ISBN 957120321-1
$ 500
2F0014
L21026
9 789571 203218
代數特論問題詳解

i. n. herstein

代數特論問題詳解

曉園
127

代數特論問題詳解

i. n. herstein

TOPICS IN ALGEBRA

nd edition

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix}$$

曉園出版社

序　言

這本書是賀司汀先生所著代數特論（Topics in Algebra by I．N．Herstein ）的習題解答。爲了方便讀者與原書對照參看，在每一題的答案前都附上了該題在原書上的頁次。例如：48.25 表示是第 48 頁上的第 25 題。在其他題目的解答中如用到此題的結果時，也都以（48.25）表示。

誠如賀司汀先生在原書序言中所說：必須是非常特出的學生才可能做出所有的習題，本書的答案中有5％左右不是我獨自思考出來的。在與老師、同學們討論或查書後，大約有五題我只列出了有關的參考書籍而沒有寫出解答。我之所以如此做，是因爲對於這幾題我既沒有好的做法而又無法整理的清楚明白，反而不如請有興趣的讀者自行查看，以免大部分的初學者望而生畏，失去了做題的興趣。我相信看過了（103.19）或（168.26）解答的初學者是會贊同我這項看法的。

在做解答時，我嘗試著不用那些未知的結果。即使那些結果就是在習題後一節的課文中，我也儘量地避免著。我想這正是賀司汀先生把那些題目故意放在那麼前面的用意。因此，像（35.9）那麼簡單的題目，我也寫了那麼會令初學者困惑的解答。但是，在第六章的一些習題中（例如（313.7），（321.17）），我無法避免地先用了定理 6.9.3 ，這是我深以爲憾的。

這本書的得以印行，除了要感謝老師、同學的指導鼓勵外，對於曉園出版社黃先生的熱心出書及該社編審部的先生、小姐們在工作上的嚴謹態度，我也是非常感激的。

程潁於台大數學系

65.8.19.

國立中央圖書館出版品預行編目資料

代數特論問題詳解 / Herstein 原著；程穎譯著.
-- 再版. -- 臺北市：曉園. 1991 [民80]印刷
面； 公分
ISBN 957-12-0321-1 (平裝)

1. 代數 - 問題集

313.022 80000572

書 名 代數特論問題詳解
著 者 Herstein
譯 者 程 穎
發行人 黃旭政
發行所 曉園出版社有限公司
臺北市青田街7巷5號
(02)3949931(六線)
門市部 北市新生南路三段96號之3(3627375)
印刷行 復大印刷廠
新聞局局版台業字第1244號
版 次 1985年10月再版第一刷
1991年3月再版第五刷

定 曉園出版社
ISB $ 500 元

Contents

1 Preliminary Notions

1.1 Set Theory 1
1.2 Mappings 7
1.3 The Integers 13

2 Group Theory

2.3 Some Preliminary Lemmas 19
2.5 A Counting Principle 30
2.6 Normal Subgroups and Quotient Groups 42
2.7 Homomorphisms 50
2.8 Automorphisms 62
2.9 Cayley's Theorem 69
2.10 Permutation Groups 74
2.11 Another Counting Principle 86
2.12 Sylow's Theorem 94
2.13 Direct Products 106
2.14 Finite Abelian Groups 113

3 Ring Theory

3.2 Some Special Classes of Rings 152
3.4 Ideals and Quotient Rings 156
3.5 More Ideals and Quotient Rings 164
3.6 The Field of Quotients of an Integral Domain 167
3.8 A Particular Euclidean Ring 174
3.9 Polynomial Rings 179
3.10 Polynomials over the Rational Field 185
3.11 Polynomial Rings over Commutative Rings 187

4 Vector Spaces and Modules

4.1 Elementary Basic Concepts 210
4.2 Linear Independence and Bases 221
4.3 Dual Spaces 230
4.4 Inner Product Spaces 236
4.5 Modules 242

5 Fields

5.1 Extension Fields 248
5.2 The Transcendence of e 256
5.3 Roots of Polynomials 259
5.4 Construction with Straightedge and Compass 267
5.5 More About Roots 275
5.6 The Elements of Galois Theory 283
5.7 Solvability by Radicals 293
5.8 Galois Groups over the Rationals 296

6 Linear Transformations

6.1 The Algebra of Linear Transformations 299
6.2 Characteristic Roots 313
6.3 Matrices 318
6.4 Canonical Forms: Triangular Form 336
6.6 Canonical Forms: A Decomposition of V: Jordan Form 350
6.7 Canonical Forms: Rational Canonical Form 371
6.8 Trace and Transpose 378
6.9 Determinants 396
6.10 Hermitian, Unitary, and Normal Transformations 409
6.11 Real Quadratic Forms 427

7 Selected Topics

7.1 Finite Fields 432
7.2 Wedderburn's Theorem on Finite Division Rings 435
7.3 A Theorem of Frobenius 441
7.4 Integral Quaternions and the Four-Square Theorem 442

1 Preliminary Notions

1.1 Set Theory

1. (a) If A is a subset of B and B is a subset of C, prove that A is a subset of C.
   (b) If $B \subset A$, prove that $A \cup B = A$, and conversely.
   (c) If $B \subset A$, prove that for any set C both $B \cup C \subset A \cup C$ and $B \cap C \subset A \cap C$.

8.1 (a) If $a \in A$, then $a \in B$ and $a \in C$, hence A is a subset of C.

(b) $x \in A$ implies $x \in A \cup B$. Hence $A \subset A \cup B$. If $x \in A \cup B$, $x \in A$ or $x \in B$. If $x \in B$, then $x \in A$. $A \cup B \subset A$. $A \cup B = A$.

(c) $x \in B \cup C$ implies $x \in B$ or $x \in C$. If $x \in B$, then $x \in A$. Hence $x \in A$ or $x \in C$, ie. $x \in A \cup C$.
$\therefore B \cup C \subset A \cup C$.
$x \in B \cap C$ implies $x \in B$ and $x \in C$ and $x \in A$, $x \in C$. $x \in A \cap C$. Hence $B \cap C \subset A \cap C$.

2. (a) Prove that $A \cap B = B \cap A$ and $A \cup B = B \cup A$.
   (b) Prove that $(A \cap B) \cap C = A \cap (B \cap C)$.

8.2 (a) $A \cap B = \{x \mid x \in A \text{ and } x \in B\} = \{x \mid x \in B \text{ and } x \in A\} = B \cap A$.
$A \cup B = \{x \mid x \in A \text{ or } x \in B\} = \{x \mid x \in B \text{ or } x \in A\} = B \cup A$.

(b) $(A \cap B) \cap C = \{x \mid x \in A \cap B \text{ and } x \in C\}$
$= \{x \mid x \in A \text{ and } x \in B \text{ and } x \in C\}$
$= \{x \mid x \in A \text{ and } x \in B \cap C\} = A \cap (B \cap C)$.

3. Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

8.3 $A \cup (B \cap C) = \{x \mid x \in A \text{ or } x \in B \cap C\} = \{x \mid x \in A \text{ or } (x \in B \text{ and } x \in C)\} = \{x \mid (x \in A \text{ and } x \in B) \text{ and } (x \in A \text{ or } x \in C)\} = \{x \mid x \in A \cup B \text{ and } x \in A \cup C\}$
$= (A \cup B) \cap (A \cup C)$.

4. For a subset C of S let C' denote the complement of C in S. For any two subsets A, B of S prove the *De Morgan rules*:
(a) $(A \cap B)' = A' \cup B'$.
(b) $(A \cup B)' = A' \cap B'$.

8.4 (a) $(A\cap B)'=\{x\in S \mid x\notin A\cap B\}=\{x\in S \mid x\notin A$ or $x\notin B\}=\{x\in S \mid x\in A'$ or $x\in B'\}=A'\cup B'$.

(b) $(A\cup B)'=\{x\in S \mid x\notin A\cup B\}=\{x\in S \mid x\notin A$ and $x\notin B\}=\{x\in S \mid x\in A'$ and $x\in B'\}=A'\cap B'$

5. For a finite set C let $o(C)$ indicate the number of elements in C. If A and B are finite sets prove $o(A \cup B) = o(A) + o(B) - o(A \cap B)$.

8.5 Let $m=o(A\cap B)$, $n=o(A)$, $p=o(B)$.
$A=\{x_1, x_2, \cdots, x_m, x_{m+1}, \cdots, x_n\}$.
$B=\{x_1, x_2, \cdots, x_m, y_{m+1}, \cdots, y_p\}$. $A\cap B=\{x_1, \cdots\cdots, x_m\}$
$A\cup B=\{x_1, \cdots, x_m, x_{m+1}, \cdots, x_n, y_{m+1}, \cdots, y_p\}$.
$o(A\cup B)=n+(p-m)=m+n-p=o(A)+o(B)-o(A\cap B)$.

6. If A is a finite set having n elements, prove that A has exactly 2^n distinct subsets.

9.6 Use induction on n. If $n=1$, A has only two subset A and ϕ. Suppose that A is a finite set having $(n+1)$ elements.
For a fixed element x in A. $o(A-\{x\})=n$. $A-\{x\}$ has exactly 2^n distinct subsets $A_1, A_2, \cdots, A_{2^n}$. Then $A_1, A_2, \cdots, A_{2^n}, A_1\cup\{x\}, A_2\cup\{x\}, \cdots, A_{2^n}\cup\{x\}$ will be all subsets of A since every subset of A either contains x or not. This completes the proof.

7. A survey shows that 63% of the American people like cheese whereas 76% like apples. What can you say about the percentage of the American people that like both cheese and apples? (The given statistics are not meant to be accurate.)

9.7 At most 63% and at least $63\%+76\%-100\%=39\%$ of American people that like both cheese and apples.

8. Given two sets A and B their *symmetric difference* is defined to be $(A - B) \cup (B - A)$. Prove that the symmetric difference of A and B equals $(A \cup B) - (A \cap B)$.

9.8 $(A-B)\cup(B-A)=\{x \mid x\in A-B$ or $x\in B-A\}$
$=\{x \mid (x\in A$ and $x\notin B)$ or $(x\in B$ and $x\notin A)\}$
$=\{x \mid (x\in A$ or $x\in B)$ and $(x\notin B$ or $x\notin A)\}$
$=\{x \mid (x\in A$ or $x\in B)$ and $x\notin(A\cap B)\}$
$=\{x \mid x\in A\cup B$ and $x\notin A\cap B\}$
$=(A\cup B)-(A\cap B)$

9. Let S be a set and let S^* be the set whose elements are the various subsets of S. In S^* we define an addition and multiplication as follows: If $A, B \in S^*$ (remember, this means that they are subsets of S):
(1) $A + B = (A - B) \cup (B - A)$.
(2) $A \cdot B = A \cap B$.
Prove the following laws that govern these operations:
(a) $(A + B) + C = A + (B + C)$.
(b) $A \cdot (B + C) = A \cdot B + A \cdot C$.
(c) $A \cdot A = A$.
(d) $A + A =$ null set.
(e) If $A + B = A + C$ then $B = C$.
(The system just described is an example of a *Boolean algebra*.)

9.9 First of all, $A-B=A\cap B'$. $A+B=(A\cap B')\cup(B\cap A')=B+A$

(a) $(A+B)+C=[(A\cap B')\cup(B\cap A')]+C$
$=[((A\cap B')\cup(B\cap A'))\cap C']\cup[((A\cap B')\cup(B\cap A'))'\cap C]$
$=[(A\cap B'\cap C')\cup(B\cap A'\cap C')]\cup[(A\cap B')'\cap(B\cap A')'\cap C]$
$=(A\cap B'\cap C')\cup(A'\cap B\cap C')\cup[(A'\cup B)\cap(A\cup B')\cap C]$
$=(A\cap B'\cap C')\cup(A'\cap B\cap C')\cup\{[((A'\cup B)\cap A)\cup((A'\cup B)\cap B')]\cap C\}$

$$=(A\cap B'\cap C')\cup(A'\cap B\cap C')\cup$$
$$\{[(A\cap B)\cup(A'\cap B')]\cap C\}$$
$$=(A\cap B'\cap C')\cup(A'\cap B\cap C')\cup$$
$$(A'\cap B'\cap C)\cup(A\cap B\cap C).$$

$A+(B+C)=(B+C)+A$
$$=(B\cap C'\cap A')\cup(B'\cap C\cap A')\cup$$
$$(B'\cap C'\cap A)\cup(B\cap C\cap A)$$
$$=(A+B)+C.$$

(b) $A\cdot(B+C)=A\cap[(B\cap C')\cup(B'\cap C)]$
$$=(A\cap B\cap C')\cup(A\cap B'\cap C)$$
$$=[(A\cap B)\cap(A\cap C)']\cup[(A'\cup B')$$
$$\cap(A\cap C)]$$
$$=A\cdot B+A\cdot C.$$

(c) $A\cdot A=A\cap A=A.$

(d) $A+A=(A\cap A')\cup(A'\cap A)=\phi$

(e) $A+B=A+C$ implies $(A+B)\cap A=(A+C)\cap A$ and $(A+B)\cap A'=(A+C)\cap A'$.

$(A+B)\cap A=((A\cap B')\cup(A'\cap B))\cap A$
$=(A\cap B'\cap A)\cup(A'\cap B\cap A)=A\cap B'.$

$(A+B)\cap A'=((A\cap B')\cup(A'\cap B))\cap A'$
$=(A\cap B'\cap A')\cup(A'\cap B\cap A')=A'\cap B.$

$(A+C)\cap A=A\cap C'$, $(A+C)\cap A'=A'\cap C.$

$A\cap B'=A\cap C'$. $A'\cap B=A'\cap C$.

$\therefore\ A'\cup B=A'\cup C.$

$A\cap B=A\cap(A'\cup B)=A\cap(A'\cup C)=A\cap C.$

$B=(A\cap B)\cup(A'\cap B)$
$=(A\cap C)\cup(A'\cap C)=C.$

10. For the given set and relation below determine which define equivalence relations.
   (a) S is the set of all people in the world today, $a \sim b$ if a and b have an ancestor in common.
   (b) S is the set of all people in the world today, $a \sim b$ if a lives within 100 miles of b.
   (c) S is the set of all people in the world today, $a \sim b$ if a and b have the same father.
   (d) S is the set of real numbers, $a \sim b$ if $a = \pm b$.

   (e) S is the set of integers, $a \sim b$ if both $a > b$ and $b > a$.
   (f) S is the set of all straight lines in the plane, $a \sim b$ if a is parallel to b.

9.10 (a), (c), (d), (e), (f), define equivalence relations.

11. (a) Property 2 of an equivalence relation states that if $a \sim b$ then $b \sim a$; property 3 states that if $a \sim b$ and $b \sim c$ then $a \sim c$. What is wrong with the following proof that properties 2 and 3 imply property 1? Let $a \sim b$; then $b \sim a$, whence, by property 3 (using $a = c$), $a \sim a$.
   (b) Can you suggest an alternative of property 1 which will insure us that properties 2 and 3 do imply property 1?

9.11 (a) The statement "let a∼b" is an assumption. It's easy to define a relation on A such that a relates without any element in A but properties 2 and 3 hold. For epample, $A=\{a, b\}$. The relation $R=\{(b, b)\}$ The a has no relation with any element of A. If x∼y, then x=y=b, b∼b implies y∼x. If x∼y and y∼z implies x=y=z=b, b∼b implies x∼z. But a∼a does not hold.

(b) Property 1′: For all a in A, a∼b for some b in A. Then, the proof of(a) is right. Hence Property 1′, 2 and 3 implies Property 1.

12. In Example 1.1.3 of an equivalence relation given in the text, prove that the relation defined is an equivalence relation and that there are exactly n distinct equivalence classes, namely, cl(0), cl(1), . . . , cl(n − 1).

9.12 (i) a−a=0 is a multiple of n. a∼.

(ii) a∼b implies n | a−b. n | b−a. b∼a.

(iii) a∼b, b∼c implies n | a−b, n | b−c.
n | (a−b)+(b−c), n | a−c. a∼c. Hence the relation defined is an equivalence relation. The equivalence class of a consists of all integers of the form a+kn where k=0, ±1, ±2 ……; there are n distinct equivalence classes since no two of 0, 1, 2, ……, n−1 are equivalent.

13. Complete the proof of the second half of Theorem 1.1.1.

9.13 As the relation defined in Theorem 1.1.1., we check that it is actually an equivalence relation defined on A. Since a and a is in the same $A\alpha$, $a\sim a$. If $a\sim b$, a and b are in the same $A\alpha$, hence b and a are in the same $A\alpha$, $b\sim a$. If $a\sim b$, $b\sim c$, then a and b are in the same $A\alpha$, b and c are in the same $A\beta$. Since $b\in A\alpha\cap A\beta$, $A\alpha=A\beta$ so that a and c are in the same $A\alpha$, $a\sim c$. Therefore, $\sim$ is actually an equivalence relation defined on A. $\alpha(a)=\{b\in A \mid b\sim a\}=\{b\in A \mid$ b and a are in the same $A\alpha\}=A\alpha$, where $A\alpha$ contains a. For any $A\alpha$, since $A\alpha\neq\phi$, say $b\in A\alpha$, $A\alpha=\alpha(b)$. This completes the proof.

1.2 Mappings.

1. In the following, where $\sigma:S\to T$, determine whether the σ is onto and/or one-to-one and determine the inverse image of any $t\in T$ under σ.
   (a) S = set of real numbers, T = set of nonnegative real numbers. $s\sigma=s^2$.
   (b) S = set of nonnegative real numbers, T = set of nonnegative real numbers, $s\sigma=s^2$.
   (c) S = set of integers, T = set of integers, $s\sigma=s^2$.
   (d) S = set of integers, T = set of integers, $s\sigma=2s$.

16.1 (a) σ is onto but is not one-to-one. The inverse image of t under σ is $\{\pm\sqrt{t}\}$.

(b) σ is onto and one-to-one. The inverse image of t under σ is $\{\sqrt{t}\}$.

(c) σ is neither onto nor one-to-one. The inverse image of t under σ is $\sqrt{t}$ when t is a square integer and ϕ when t is not a squgare integer.

(d) σ is not onto but is one-to-one. The inverse image of t under σ is $\{\frac{t}{2}\}$ when t is an even integer and ϕ when t is an odd integer.

2. If S and T are nonempty sets, prove that there exists a one-to-one correspondence between $S\times T$ and $T\times S$.

16.2 Define $\sigma:S\times T\to T\times S$ as $\sigma(s,t)=(t,s)$. σ is clearly a one-to-one correspondence between $S\times T$ and $T\times S$.

3. If S, T, U are nonempty sets, prove that there exists a one-to-one correspondence between
   (a) $(S\times T)\times U$ and $S\times(T\times U)$.
   (b) Either set in part (a) and the set of ordered triples (s,t,u) where $s\in S$, $t\in T$, $u\in U$.

16.3 (a) Define $\sigma:(S\times T)\times U\to S\times(T\times U)$ as $\sigma(((s,t),u))=(s,(t,u))$. σ is a one-to-one correspondence between $(S\times T)\times U$

and $S\times(T\times U)$.

(b) Define $\sigma:(S\times T)\times U\to\{(s,t,u)\mid s\in S,\ t\in T,\ u\in T\}$ as $\sigma(((s,t),u)))=(s,t,u)$. σ is the desired mapping between $(S\times T)\times U$ and $\{(s,t,u)\mid s\in S, t\in T, u\in U\}$.

4. (a) If there is a one-to-one correspondence between S and T, prove that there exists a one-to-one correspondence between T and S.
(b) If there is a one-to-one correspondence between S and T and between T and U, prove that there is a one-to-one correspondence between S and U.

16.4 (a) Let σ be a one-to-one correspondence between S and T . Then , for any t in T, there is exectly one elemcot s in S such that $\sigma(s)=t$. Define $\sigma^{-1}:T\to S$ as $\sigma^{-1}(t)=s$. σ^{-1} is a one-to-one correspondence between T and S .

(b) Let $\sigma:S\to T$, $\rho:T\to U$ be one-to-one correspondences between S and T , and,T and U, respectively. Then $\rho\sigma$ is a one-to-one corespondence between S and U .

5. If ι is the identity mapping on S, prove that for any $\sigma\in A(S)$, $\sigma\circ\iota=\iota\circ\sigma=\sigma$.

17.5 For any $s\in S$, $(\sigma\circ\tau)(s)=\sigma(\tau(s))=s$ $=\sigma(s)$ and $x\circ(\tau\circ\sigma)(s)=\tau\circ(\sigma(s))$ $=\sigma(s)$ Therefore $\sigma\circ\tau=\tau\circ\sigma=\sigma$.

*6. If S is any set, prove that it is *impossible* to find a mapping of S *onto* S^*.

17.6 Suppose there is a mapping σ of S into S^*. $A=\{s\in S\mid s\notin\sigma(s)\}$ can not the image of σ . For , Suppose $\sigma(t)=A$ for $t\in S$. Then, (i) if $t\in A=\sigma(t)$, $t\notin\sigma(t)$, a contradiction ;
(ii) if $t\notin A=\sigma(t)$, $t\in\sigma(t)=A$, a contradiction .

7. If the set S has n elements, prove that $A(S)$ has $n!$ (n factorial) elements.

17.7 We first claim that there are n! maps from A to B with $|A|=n$ and $|B|=n$. Let $P(A,B)=\{\rho\mid\rho:A\to B\}$. $n=1$, the identity map is the only map between A and B .
Use induction on n . Suppose $|A|=n+1$ and $|B|=n+1$ $A=\{x_1,\cdots\cdots,x_{n+1}\}$, $B=\{y_1,\cdots\cdots,y_{n+1}\}$.
Partition $P(A,B)$ by $\sim$ as $\rho\sim\sigma$ if and only if $\rho(x_i)=\sigma(x_i)$ for all x_i
Clearly $\sim$ is an equivalence relation on $P(A,B)$。 In each equivalence class E_i , $E_i=\{\rho\in P(A,B)\mid\rho(x_i)=y_i\}$, $i=1,2,\cdots,n+1$, $E_i=P(A\setminus\{x_i\}$, $B\setminus\{(y_i)\})$. $|E_i|=n!$ Hence $|P(A,B)|=\sum_{i=1}|E_i|=(n+1)|E_i|=(n+1)n!=(n+1)!$

8. If the set S has a finite number of elements, prove the following:
(a) If σ maps S onto S, then σ is one-to-one.
(b) If σ is a one-to-one mapping of S onto itself, then σ is onto.
(c) Prove, by example, that both part (a) and part (b) are false if S does not have a finite number of elements.

17.8 Let $S=\{x_1,\cdots,x_n\}$.
(a) $\{\sigma(x_1),\cdots,\sigma(x_n)\}=\{x_1,\cdots,x_n\}$ implies $\{\sigma(x_1),\cdots,\sigma(x_n)\}$ has n elements and hence all these n elements are distinct 。 σ is one - to - one .
(b) $\{\sigma(x_1),\cdots,\sigma(x_n)\}$ has n - elements and $\{x_1,\cdots,x_n\}\supset\{\sigma(x_1),\cdots,\sigma(x_n)\}$. $\{x_1,\cdots,x_n\}=\{\sigma(x_1),\cdots,\sigma(x_n)\}$ 。
(c) Let S be the set of natural numbers . $\sigma(1)=\sigma(2)=1$, $\sigma(n)=n-1$, $n=3,4,\cdots$. σ maps S onto to S , but σ is not one - to - one . $\rho(n)=n+1$, $n=1,2,\cdots\cdots$. ρ is one - to - one but is not onto .

9. Prove that the converse to both parts of Lemma 1.2.2 are false; namely,
   (a) If $\sigma \circ \tau$ is onto, it need not be that both σ and τ are onto.
   (b) If $\sigma \circ \tau$ is one-to-one, it need not be that both σ and τ are one-to-one.

17.9 (a) $S=\{1,2,3\}$, $T=\{1,2,3\}$, $U=\{1,2\}$
$\tau(1)=1, \tau(2)=2, \tau(3)=2$. $\sigma(1)=1$,
$\sigma(2)=2, \sigma(3)=2$. $\sigma\cdot\tau$ maps S onto U and τ is not onto.

(b) $S=\{1,2\}$, $T=\{1,2,3\}$, $U=\{1,2\}$.
$\tau(1)=1, \tau(2)=2, \sigma(1)=1, \sigma(2)=2$,
$\sigma(3)=2$. $\sigma\cdot\tau$ is one-to-one but σ is not one-to-one.

10. Prove that there is a one-to-one correspondence between the set of integers and the set of rational numbers.

17.10 We only show that there is a one-to-one correspondence between positive rational numbers Q^+ and positive integers N. $\sigma(\frac{q}{p})=2^p 3^q$. σ is clearly a one-to-one mapping into N. The image of σ has infinitive elements, order it as $\{x_1, x_2, \cdots, x_n, \cdots\}$ with $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n \leqslant \cdots$. Therefore, we have constract a one-to-one correspondence between Q^+ and N.

11. If $\sigma: S \to T$ and if A is a subset of S, the *restriction of* σ *to* A, σ_A, is defined by $a\sigma_A = a\sigma$ for any $a \in A$. Prove
   (a) σ_A defines a mapping of A into T.
   (b) σ_A is one-to-one if σ is.
   (c) σ_A may very well be one-to-one even if σ is not.

17.11 (a) Let $M=\{(a, a\sigma_A) \mid a \in A\}$.
$M=\{(a, a\sigma) \mid a \in A\}$ is a mapping from A to T.

(b) For $a\sigma_A = b\sigma_A$, $a\sigma = b\sigma$. Since σ is one-to-one, $a=b$, so that σ_A is one-to-one.

(c) If A has only one element, then σ_A is clearly one-to-one even if σ is not.

12. If $\sigma: S \to S$ and A is a subset of S such that $A\sigma \subset A$, prove that $(\sigma \circ \sigma)_A = \sigma_A \circ \sigma_A$.

17.12 For $a \in A$, $a(\sigma\circ\sigma)_A = a(\sigma\circ\sigma) = (a\sigma)\sigma =$
$= (a\sigma)\sigma_A = (a\sigma_A)\sigma_A = a(\sigma_A \circ \sigma_A)$.
$(\sigma\circ\sigma)_A = \sigma_A \circ \sigma_A$.

13. A set S is said to be *infinite* if there is a one-to-one correspondence between S and a proper subset of S. Prove
   (a) The set of integers is infinite.
   (b) The set of real numbers is infinite.
   (c) If a set S has a subset A which is infinite, then S must be infinite.
   (*Note:* By the result of Problem 8, a set finite in the usual sense is not infinite.)

17.13 (a) Let $\sigma(n)=n+1$, $n=0,1,2,\cdots$.
$\sigma(n)=n$, $n=-1,-2,\cdots$. σ is a one-to-one correspondence between the set of integers and the set of nonzero integers which is a proper subset of the former. Hence Z is infinite.

(b) Let $\sigma(x)=2^x$. σ is a one-to-one correspondence between R. $R^+=\{r \in R \mid r>0\}$ which is a proper subset of R. R is therefore infinite.

(c) Since A is infinite, there is a mapping σ from A onto a proper subset B of A. Define $\rho: S \to S$ as $\rho(s) = \begin{cases} s & \text{if } s \notin A \\ \sigma(s) & \text{if } s \in A. \end{cases}$ Then σ is a one-to-one correspondence between S and $B \cup (S \setminus A)$ which is a proper subset of S since B is a proper subset of A. S is infinite.

*14. If S is infinite and can be brought into one-to-one correspondence with the set of integers, prove that there is one-to-one correspondence between S and $S \times S$.

17.14 We first show that there is a one - to - one correspondence between $Z \times Z$ and Z . In (17.10), we have shown that there is a one - to - one correspondence σ between $Z^+ \times Z^+$ and Z^+ . Now define $\rho : Z \times Z \to Z$ as

$$\rho(p,q)=\begin{cases} 0, \text{ if } p=q=0 \\ 2\sigma(p,q), \text{ if } p,q>0 \\ 2\sigma(p,-q), \text{ if } p>0,\ q<0 \\ 2\sigma(-p,q)-1, \text{ if } p<0,\ q>0 \\ 2\sigma(p,q)-1, \text{ if } p<0,\ q<0. \end{cases}$$

ρ is a one - to - one correspondence between $Z \times Z$ and Z . Since there is a one - to - one correspondence τ between S and Z . Define $\mu : S \times S \to Z \times Z$ as $\mu(s,t)=(\tau(s),\tau(t))$. μ is a one - to - one correspondence between $S \times S$ and $Z \times Z$. $u^{-1} \circ \rho^{-1} \circ \tau$ is a one - to - one correspondence between S and $S \times S$.

*15. Given two sets S and T we declare $S < T$ (S is smaller than T) if there is a mapping of T *onto* S but *no* mapping of S *onto* T. Prove that if $S < T$ and $T < U$ then $S < U$.

17.15 $S < T$ and $T < U$ implies that there are $\rho : T \to S$ and $\sigma : U \to T$ such that ρ and σ are onto . By Lemma 1.2.2.1. $\rho \circ \sigma : U \to S$ is onto . Now suppose that there is a mapping τ of S onto U . Then , by Lemma 1.2.2.1. $\tau \circ \rho : T \to U$ is onto which contradicts with $T < U$.

16. If S and T are finite sets having m and n elements, respectively, prove that if $m < n$ then $S < T$.

17.16 Let $S=\{x_1,\cdots,x_m\}$, $T=\{y_1,\cdots,y_n\}$. Define $\sigma : T \to S$ by $\sigma(y_1)=x_1,\cdots,\sigma(y_m)=x_m$, and $\sigma(y_{m+1})=\cdots=\sigma(y_n)=x_1$. σ is a mapping of T onto S . Suppose there is a mapping ρ of S into T . $\rho(S)=\{\rho(x_1),\rho(x_2),\cdots,\rho(x_m)\}$. $|\rho(S)| \leqslant m < n = |T|$, ρ can not be onto . So that $S < T$.

1·3 The Integers

1. If $a \mid b$ and $b \mid a$, show that $a = \pm b$.

23.1 $a \mid b$ implies $b=ma$ for some m . $b \mid a$ implies $a=nb$ for some n . $a=nb=nma$. $a \neq 0$, $mn=1$. $m=\pm 1$, $n=\mp 1$, $a=\pm b$.

2. If b is a divisor of g and of h, show it is a divisor of $mg + nh$.

23.2 $b \mid g, b \mid h$, $g=m'b$, $h=n'b$ for some m' and n'. $mg+nh=mm'b+nn'b=(mm'+nn')b$, b is a divisor of $mg+nh$.

3. If a and b are integers, the *least common multiple* of a and b, written as $[a, b]$, is defined as that positive integer d such that
(a) $a \mid d$ and $b \mid d$.
(b) Whenever $a \mid x$ and $b \mid x$ then $d \mid x$.
Prove that $[a, b]$ exists and that $[a, b] = ab/(a, b)$, if $a > 0, b > 0$.

23.3 Since $a \mid\mid ab \mid$, $b \mid\mid ab \mid$, $M=\{d \mid a \mid b, b \mid d\} \neq \phi$. There is smallest positive integer , c , in M . $a \mid c$, $b \mid c$. Whenever $a \mid x$, $b \mid x$, $x \in M$ and $-x \in M$. We may suppose $x > 0$. $x=rc+s$. $0 \leqslant s < c$. $s=x-rc$. By (23.2) $a \mid s$ and $b \mid s$, $s \in M$. $s < c$ implies $s=0$ and $x=rc$ $c \mid x$. Therefore $[a,b]$ exists . $(a,b) \mid a$ and

$$(a,b) \mid b, \quad ab/(a,b)=a\frac{b}{(a,b)}=b\frac{a}{(a,b)},$$

$a \mid (ab/(a,b))$ and $b \mid (ab/(a,b))$.

$a \mid x$, $b \mid x$ implies $a \mid x$ and $\frac{b}{(a,b)} \mid x$.

$(a, \frac{b}{(a,b)})=1$ implies $\frac{ab}{(a,b)} \mid x$ by (23.4) . Since $[a,b]$ uniquely exists , $[a,b]=ab/(a,b)$.

4. If $a \mid x$ and $b \mid x$ and $(a, b) = 1$ prove that $(ab) \mid x$.

23.4 $a|x$ and $b|x$ implies $x=am$, $x=bn$ for some m and n. $(a,b)=1$ implies $ar+bs=1$ for some r and s. $x=arx+bsx=ar(bn)+bs(am)=ab(rn+sm)$. $(ab)|x$。。

5. If $a = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1}\cdots p_k^{\beta_k}$ where the p_i are distinct prime numbers and where each $\alpha_i \geq 0$, $\beta_i \geq 0$, prove
(a) $(a, b) = p_1^{\delta_1}\cdots p_k^{\delta_k}$ where δ_i = minimum of α_i and β_i for each i.
(b) $[a, b] = p_1^{\gamma_1}\cdots p_k^{\gamma_k}$ where γ_i = maximum of α_i and β_i for each i.

23.5 (a) Clearly, $P_1^{\delta_1}P_2^{\delta_2}\cdots P_k^{\delta_k}|(a,b)$. Whenever $x|a$ and $x|b$, $x|P_1^{\delta_1},\cdots,x|P_k^{\delta_k}$. $x|P_1^{\delta_1}P_2^{\delta_2}\cdots P_k^{\delta_k}$. Hence $(a,b)=P_1^{\delta_1}P_2^{\delta_2}\cdots P_k^{\delta_k}$.

(b) Clearly, $a|P_1^{\gamma_1}\cdots P_k^{\gamma_k}$ and $b|P_1^{\gamma_1}\cdots P_k^{\gamma_k}$. Whenever $a|x$, $b|x$. $P_1^{\gamma_1}|x,\cdots,P_k^{\gamma_k}|x$. By (23.4), $P_1^{\gamma_1}\cdots P_k^{\gamma_k}|x$. By definition of $[a,b]$, $[a,b]=P_1^{\gamma_1}\cdots P_k^{\gamma_k}$.

6. Given a, b, on applying the Euclidean algorithm successively we have

$$\begin{aligned} a &= q_0 b + r_1, & 0 \leq r_1 < |b|,\\ b &= q_1 r_1 + r_2, & 0 \leq r_2 < r_1,\\ r_1 &= q_2 r_2 + r_3, & 0 \leq r_3 < r_2,\\ &\cdots\\ r_k &= q_{k+1} r_{k+1} + r_{k+2}, & 0 \leq r_{k+2} < r_{k+1}. \end{aligned}$$

Since the integers r_k are decreasing and are all nonnegative, there is a first integer n such that $r_{n+1} = 0$. Prove that $r_n = (a, b)$. (We consider, here, $r_0 = |b|$.)

24.6 $r_{n+1}=0$ implies $r_n|r_{n-1}$, $r_n|r_{n-2}$, $\cdots$, $r_n|b$ and $r_n|a$. Whenever $x|a$ and $x|b$, $x|r_1$, $x|r_2,\cdots,x|r_{n-1}$, $x|r_n$. Hence $r_n=(a,b)$.

7. Use the method in Problem 6 to calculate
(a) (1128, 33). (b) (6540, 1206).

24.7 (a) $1128=34\cdot33+6$

$33=5\cdot6+3$
$6=2\cdot3$
$(1128,33)=3$

(b) $6540=5\cdot1206+510$
$1206=2\cdot510+186$
$510=2.186+138$
$186=1.138+48$
$138=2.48+42$
$48=1.42+6$
$42=7.6$
$(6540,1206)=6$

8. To check that n is a prime number, prove that it is sufficient to show that it is not divisible by any prime number p, such that $p \leq \sqrt{n}$.

24.8 Suppose n is not divisible by any prime number p, such that $p\leqslant\sqrt{n}$. If n not a prime number, then n must be divisible by a prime number p such that $\sqrt{n}<p<n$. $n=pm$ for some m. $m<\sqrt{n}$ otherwise $n=pm>\sqrt{n}$. $\sqrt{n}=n$. m is divisible by some prime number q, such that $q\leqslant m<\sqrt{n}$. $q|n$, a contradiction. Hence n is a prime number.

9. Show that $n > 1$ is a prime number if and only if for any a either $(a, n) = 1$ or $n \mid a$.

24.9 Suppose that for any a either $(a,n)=1$ or $n|a$. Let q be a divisor of n such that $q\neq\pm1$. Then $(q,n)=|q|\neq1$, $n|q$. By (23.1), $q=\pm n$. n is a prime number by definition. Conversely, Suppose n is a prime number. For any a, (a,n) is a divisor of n. Hence $(a,n)=1$ or $(a,n)=n$. Therefore, $(a,n)=1$ or $n|a$.

10. Assuming that any nonempty set of positive integers has a minimal element, prove
(a) If the proposition P is such that
(1) $P(m_0)$ is true,
(2) the truth of $P(m-1)$ implies the truth of $P(m)$,
then $P(n)$ is true for all $n \geq m_0$.

(b) If the proposition P is such that
(1) $P(m_0)$ is true,
(2) $P(m)$ is true whenever $P(a)$ is true for all a such that $m_0 \le a < m$,
then $P(n)$ is true for all $n \ge m_0$.

24.10(a) If not , there exists an $n \geqslant m_0$ such that $p(n)$ is not true . Let $M=\{m \mid m \geqslant m_0$, $p(m)$ is not true$\}$. $M \neq \phi$. By assumption , M has a minimal element n_0 . Since $p(m_0)$ is true , $n_0 > m_0$. $n_0-1 \geqslant m_0$, $n_0-1 \notin M$, $p(n_0-1)$ is true . By (2) $p(n_0)$ is true , a contradiction .

(b) If not , $M=\{m \mid m \geqslant m_0$, $p(m)$ is not true$\} \neq \phi$. By assumption , M has a minimal element n_0 . Since $p(m_0)$ is true , $n_0 > m_0$. For any a such that $m_0 \leqslant a < n_0$, $a \notin M$ implies $p(a)$ is true . By (2) $p(n_0)$ is true , a contradiction .

11. Prove that the addition and multiplication used in J_n are well defined.

24.11 If $[i]=[i']$, $[j]=[j']$, then $i \equiv i' \pmod n$ and $j \equiv j' \pmod n$. By Lemma 1.3.3.3, $i+j \equiv i'+j' \pmod n$ and $ij \equiv i'j' \pmod n$. Therefore, $[i+j]=[i'+j']$, $[ij]=[i'j']$, the addition and multiplication used in J_n are well-defined .

12. Prove the properties 1–7 for the addition and multiplication in J_n.

24.12(1) $[i]+[j]=[i+j]=[j+i]=[j]+[i]$.
(2) $[i][j]=[ij]=[ji]=[j][i]$.
(3) $([i]+[j])+[k]=[i+j]+[k]=[(i+j)+k]$ $=[i]+[j+k]=[i]+([j]+[k])$.
(4) $([i][j])[k]=[ij][k]=[(ij)k]$ $=[i(jk)]=[i][jk]=[i]([j][k])$.

(5) $[i]([j]+[k])=[i][j+k]=[i(j+k)]$ $=[ij+ik]=[ij]+[ik]=[i][j]+[i][k]$.
(6) $[0]+[i]=[0+i]=[i]$.
(7) $[1][i]=[1 \cdot i]=[i]$

13. If $(a, n) = 1$, prove that one can find $[b] \in J_n$ such that $[a][b] = [1]$ in J_n.

24.13 $(a,n)=1$ implies there are b and c such that $ab+cn=1$. $[1]=[ab+cn]=[ab]+[cn]$ $=[a][b]+[c][n]=[a][b]+[c][0]=[a][b]$

*14. If p is a prime number, prove that for any integer a, $a^p \equiv a \bmod p$.

24.14 $a \equiv 0 \pmod p$, $a^p \equiv 0 \equiv a \pmod p$. Suppose $a \not\equiv 0 \pmod p$. $[a],[2a],\cdots,[(p-1)a]$ are dinstinct nonzero elements in Jp . Hence $\{[a],[2a],\cdots,[(p-1)a]\}$ $=\{[1],[2],\cdots,[p-1]\}$. $[a] \cdot [2a] \cdots [(p-1)a]=[1][2]\cdots[p-1]$ implies $1 \cdot 2 \cdots (p-1)a^{p-1} \equiv 1 \cdot 2 \cdots (p-1) \pmod p$. By Lemma 1.3.3.4., $a^{p-1} \equiv 1 \pmod p$ and $a^p \equiv a \pmod p$.

15. If $(m, n) = 1$, given a and b, prove that there exists an x such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$.

24.15 By (24.13), there are r, s such that $rm \equiv 1 \pmod n$ and $sn=1 \pmod m$. Let $x=asn+brm$, Then $x \equiv asn+brm \equiv asn \equiv a \pmod m$ and $x \equiv asn+brm \equiv brm \equiv b \pmod n$.

16. Prove the corollary to Lemma 1.3.2.

24.16 Let p be a prime number which divides $a_1 \cdots a_n$. If $p \nmid a_1$, by (24.9), $(p, a_1)=1$ and $p \mid a_2 \cdots a_n$ by Lemma 1.3.2. If $p \nmid a_2$, once again , $p \mid a_3 \cdots a_n$. Continue this process , p must divides at least one a_i .

17. Prove that n is a prime number if and only if in J_n, $[a][b] = [0]$ implies that $[a] = [b] = [0]$.

24.17 Prove that n is a prime number if and only if in Jn , 〔a〕〔b〕=〔0〕 implies that 〔a〕=〔0〕 or 〔b〕=〔0〕.

Suppose n is a prime number. 〔a〕〔b〕=〔0〕 implies ab≡0 (mod n), if a≢0 (mod n), By(24,9),(a,n)=1, By Lemma 1.3.3.4., b≡(mod n).

Conversely , suppose in Jn , 〔a〕〔b〕=〔0〕 implies 〔a〕=〔0〕 or 〔b〕=〔0〕 . If n is not a prime number , say n=rs, then 〔r〕≠〔0〕 and 〔s〕≠〔0〕 in Jn . But 〔0〕=〔n〕=〔rs〕 =〔r〕〔s〕 , a contradiction . This completes the proof .

2 Group Theory

2.3 Some Preliminary Lemmas

1. In the following determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.
   (a) G = set of all integers, $a \cdot b \equiv a - b$.
   (b) G = set of all positive integers, $a \cdot b = ab$, the usual product of integers.
   (c) $G = a_0, a_1, \ldots, a_6$ where

$$a_i \cdot a_j = a_{i+j} \quad \text{if } i + j < 7,$$

$$a_i \cdot a_j = a_{i+j-7} \quad \text{if } i + j \geq 7$$

   (for instance, $a_5 \cdot a_4 = a_{5+4-7} = a_2$ since $5 + 4 = 9 > 7$).
   (d) G = set of all rational numbers with odd denominators, $a \cdot b \equiv a + b$, the usual addition of rational numbers.

35.1 (a) G is not a group since the axioms of (2), (3) and (4) fail to hold.

(b) G is not a group since the axiom of (4) fails to hold.

(c) G is a group.

(d) G is a group.

2. Prove that if G is an abelian group, then for all $a, b \in G$ and all integers n, $(a \cdot b)^n = a^n \cdot b^n$.

35.2 n = 1, $(a \cdot b)^n = a \cdot b = a^n \cdot b^n$. Suppose $(a \cdot b)^n = a^n \cdot b^n$. Then $(a \cdot b)^{n+1} = (a \cdot b)^n \cdot (a \cdot b) = (a^n \cdot b^n) \cdot (a \cdot b) = [(a^n \cdot b^n) \cdot a] \cdot b = [a \cdot (a^n \cdot b^n)] \cdot b = [(a \cdot a^n) \cdot b^n] \cdot b = (a^{n+1} \cdot b^n) \cdot b = (a^{n+1} \cdot (b^n \cdot b) = a^{n+1} \cdot b^{n+1}$.

Therefore, $(a \cdot b)^n = a^n \cdot b^n$ holds for all natural number n.

When n = 0 , $(a \cdot b)^0 = e$ and $a^0 \cdot b^0 = e \cdot e = e$. We have $(a \cdot b)^0 = a^0 \cdot b^0$.

When n is negative, $-n$ is a natural number, hence $(a \cdot b)^{-n} = a^{-n} \cdot b^{-n}$, $(a \cdot b)^n = [(a \cdot b)^{-n}]^{-1} = (a^{-n} \cdot b^{-n})^{-1} = (b^{-n})^{-1} \cdot (a^{-n})^{-1} = b^n \cdot a^n = a^n \cdot b^n$. This completes the proof.

3. If G is a group such that $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, b \in G$, show that G must be abelian.

35.3 $(a\cdot b)^2 = (a\circ b)\circ(a\circ b) = a\cdot[b\cdot(a\circ b)] = a\cdot[(b\circ a)\cdot b]$
$a^2\cdot b^2 = (a\cdot a)\cdot b^2 = a\cdot(a\cdot b^2) = a\cdot[(a(b\circ b)] = a\cdot[(a\cdot b)\circ b]$
By Lemma 2.3.2, we have $(a\cdot b)\circ b = (b\cdot a)\cdot b$.
By Lemma 2.3.2 once more, we get $a\circ b = b\circ a$. This shows that G is abelian.

*4. If G is a group in which $(a \cdot b)^i = a^i \cdot b^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian.

35.4 Suppose $(a\cdot b)^i = a^i\cdot b^i$, $(a\cdot b)^{i+1} = a^{i+1}\cdot b^{i+1}$ and $(a\cdot b)^{i+2} = a^{i+2}\circ b^{i+2}$ hold for all a,b in G.
Since $a\circ(a^i\circ b)\cdot b^i = a^{i+1}\circ b^{i+1} = (a\circ b)^{i+1} = (a\circ b)(a\circ b)^i = (a\circ b)\circ(a^i\circ b^i) = a\cdot(b\circ a^i)\cdot b^i$, We have $a^i\circ b = b\cdot a^i$ by Lemma 2.3.2.
By the same way, we get $a^{i+1}\cdot b = b\cdot a^{i+1}$ from $(a\circ b)^{i+1} = a^{i+1}\circ b^{i+1}$ and $(a\circ b)^{i+2} = a^{i+2}\cdot b^{i+2}$. Now, $a\circ(a^i\circ b) = a\circ(b\cdot a^i)\therefore(a\circ b)a^i = a^{i+1}\circ b = b\cdot a^{i+1} = (b\circ a)\,a^i$. Therefore $a\cdot b = b\cdot a$ and G is abelian.

5. Show that the conclusion of Problem 4 does not follow if we assume the relation $(a \cdot b)^i = a^i \cdot b^i$ for just two consecutive integers.

35.5 Suppose the relation $(a\circ b)^i = a^i\circ b^i$ holds for just two consecutive intergers n and n+1.
Then $(a\circ b)^n = a^n\circ b^n$, $(a\circ b)^{n+1} = a^{n+1}\,b^{n+1}$ and $(a\circ b)^{n+2} \neq a^{n+2}\cdot b^{n+2}$.
$a\cdot b^{n+1} = a^{-(n+1)}\cdot(a^{n+2}\circ b^{n+2})\circ b^{-1} \neq a^{-(n+1)}\cdot(a\cdot b)^{n+2}\circ b^{-1} = a^{-n+1}\circ(a\cdot b)^{n+1}\cdot(a\circ b)\cdot b^{-1} = a^{-(n+1)}\circ(a^{n+1}\cdot b^{n+1})\cdot(a\circ b)\circ b^{-1} = b^{n+1}\circ a$.
Since $a\cdot b^{n+1} \neq b^{n+1}\circ a$, G is not an abelian group.

6. In S_3 give an example of two elements x, y such that $(x \cdot y)^2 \neq x^2 \cdot y^2$.

35.6 In example 2.2.3, let $x = \phi$, $y = \psi$, Then $(x\circ y)^2 = (\phi\circ\psi)^2 = e$, but $x^2\cdot y^2 = \phi^2\cdot\psi^2 = e\cdot\psi^2 = \psi^2 \neq e = (x\cdot y)^2$.

7. In S_3 show that there are four elements satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.

35.7 In example 2.2.3, e, ϕ, $\phi\cdot\psi$ satisfy $x^2 = e$ and e, ψ, ψ^2 satisfy $y^3 = e$.

8. If G is a finite group, show that there exists a positive integer N such that $a^N = e$ for all $a \in G$.

35.8 Since $S = \{a, a^2, \cdots, a^n, \cdots\}$ is a subset of G, S must be finite, and therefore there exist i, j in N such that $a^i = a^j$ and $1 \leqslant i < j$. $j - i \geqslant 1$.
$a^{j-i} = a^j\circ a^{-i} = a^i\cdot a^{-i} = a^0 = e$.

9. (a) If the group G has three elements, show it must be abelian.
(b) Do part (a) if G has four elements.
(c) Do part (a) if G has five elements.

35.9 For x in G, we always have $e\cdot x = x = x\cdot e$ and $x\cdot x = x\circ x$.

(a) $G = \{e, a, b\}$. We need only to show $a\circ b = b\cdot a$. Since $a\circ b \neq a$ and $a\circ b \neq b$, we have $a\circ b = e$ and by the definition of a group we have $b\circ a = a\cdot b = e$ and hence G is abelian.

(b) $G = \{e, a, b, c, \}$. For any two elements x and y in G, if $x\circ y = e$, we have $x\cdot y = y\cdot x = e$. Therefore, We may suppose $x \neq y, x \neq e, y \neq e$ and $x\circ y \neq e$ otherwise we have $x\cdot y = y\cdot x$ already. Now $x\cdot y \neq e$, $x\cdot y \neq x$, $x\cdot y \neq y$ and $x\cdot y$ must equal the only fourth element z which differs from e, x and y. Just as the same way, $y\cdot x$ also equal z. That is xy = yx and G is abelian.

(c) $G = \{e, a, b, c, d\}$. Suppose without loss of generality that $a\circ b \neq b\cdot a$, and further more, $a\circ b = c$, $b\circ a = d$. Consider the inverse element of a in G. Clearly, $a^{-1} \neq e$, $a^{-1} \neq b$. If $a^{-1} = c$, $c^2 = c\circ c = c\cdot(a\cdot b) = (c\circ a)\circ b = b = b\cdot e = b\cdot(a\cdot c)$

$= (b \circ a) \circ c = d \circ c$, by Lemma 2.3.2 we get the contradition $c = d$. If $a^{-1} = d$, $d^2 = d \circ d = (b \circ a) \cdot d = b \circ (a \circ d) = b \circ e = b = e \circ b = (d \cdot a) \circ b = d \cdot (a \circ b) = d \circ c$, by Iemma 2.3.2 we get the contradiction $d = c$. We get the only case that $a^{-1} = a$, i.e. $a \circ a = e$. Now consider $a \circ d$. Clearly, $a \circ d \neq a$ $a \cdot d \neq d$ and $a \circ d \neq e$. If $a \circ d = c$, by our assumption $a \circ b = c$ we get the contradiction $b = d$, Therefore, we get the following conclusion, $a \circ b = c$, $b \circ a = d$, $a \circ a = e$, $a \cdot d = b$. But now $b = (a \circ a) \circ b = a \circ (a \circ b) = a \circ c$, $b = a \cdot d$ and the last contradiction $c = d$ appears. This completes the proof.

10. Show that if every element of the group G is its own inverse, then G is abelian.

35.10 Since x in G is its own inverse, $x^2 = e$. For a, b in G, $(a \cdot b)^2 = e = e \cdot e = a^2 \cdot b^2$. By (35.3), G is abelian.

11. If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.

35.11 Define an equivalence relation $\sim$ on G as following: $a \sim b$ if a is the inverse element of b. It's easy to prove that "$\sim$" is actually an equivalence relation on G and each equivalence class contains at most two distinct element. Since G is of even order and the eqiuvalence class $\{ e \}$ contains only one element, G must have another class having also only one element. now, this class $\{ a \}$ having a as it's own inverse and hence $a^2 = e$ and $a \neq e$.

12. Let G be a nonempty set closed under an associative product, which in addition satisfies:
(a) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$.

(b) Give $a \in G$, there exists an element $y(a) \in G$ such that $a \cdot y(a) = e$.
Prove that G must be a group under this product.

35.12 It's only need to prove that $a \cdot e = e \cdot a = e$ for all a in G and $y(a) \cdot a = a \circ y(a) = e$ for all a in G.
We first prove the second case. $y(a) \cdot a = (y(a) \cdot a) \cdot e = (y(a) \cdot a) \cdot [y(a) \cdot y(y(a))] = y(a) \cdot [(a \cdot y(a)) \cdot y(y(a))] = y(a) \cdot [e \circ y(y(a))] = y(a) \cdot y(y(a)) = e$. Now, $e \cdot a = (a \cdot y(a)) \cdot a = a \cdot (y(a)) \cdot a) = a \cdot e = a$. This completesthe proof.

13. Prove, by an example, that the conclusion of Problem 12 is false if we assume instead:
(a′) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$.
(b′) Given $a \in G$, there exists $y(a) \in G$ such that $y(a) \cdot a = e$.

36.13 Let G be any set containing more than one element. Define a binary operation on G by $x \cdot y = x$ for all x, y in G. Then 1. a, $b \in G$ implies $a \cdot b \in G$ (closed). 2. $a \cdot (b \circ c) = a = (a \circ b) \circ c$ for all a, b, $c \in G$. (associative law). 3. There exists an $e \in G$ (choose an arbitrary element in G) such that $a \cdot e = a$ for all $a \in G$. 4. Given $a \in G$, there exists $y(a) = e$ (the chosen element) such that $y(a) \cdot a = e \circ a = e$. But clearly, G is not a group under this operation.

14. Suppose a *finite* set G is closed under an associative product and that both cancellation laws hold in G. Prove that G must be a group.

36.14 First of all, we claim that for given a, b in G, the equation $ax = b$ and $ya = b$ have solution in G. For given a, b in G, and $G = \{ x_1, \cdots\cdots, x_n \}$, all ax_i are distinct since the left cancellation law holds. $G = \{ x_1, \cdots\cdots, x_n \} = \{ ax_1, \cdots, ax_n \}$. $b \in G$ implies $ax_i = b$ for some x_i. Therefore, $ax = b$ has solution in G. The same argument shows that $ya = b$ also has solution in G.

Now, We prove the given question by showing that (a) There exists an $e \in G$ such that $a \circ e = a$ for all $a \in G$. and (b) Given $a \in G$, there exists an element $y(a) \in G$ such that $a \cdot y(a) = e$ since we have proved (35.12).
For a fixed element a in G, there is an element e in G such that $a \circ e = a$ since $a \circ x = a$ has solution in G. Now for any element z in G, there is $y(z) \in G$ such that $z = y(z) \cdot a$ since $y \cdot a = z$ has solution y in G and $z = y(z) \circ a = y(z) \cdot (a \cdot e) = (y(z) \cdot a) \cdot e = z \circ e$. We have therefore proved (a). (b) is proved by $a \cdot y = e$ having solution y in G for all a, e in G. This completes the proof.

15. (a) Using the result of Problem 14, prove that the nonzero integers modulo p, p a prime number, form a group under multiplication mod p.
(b) Do part (a) for the nonzero integers relatively prime to n under multiplication mod n.

36.15 (a)(b) are obtained by Lemma 1.3.3. (4) and (36.14).

16. In Problem 14 show by an example that if one just assumed one of the cancellation laws, then the conclusion need not follow.

36.16 An example is given by (36.13). For that example, if $ab = cb$ then $a = ab = cb = c$, the right cancellation law holds. But clearly, G is not a group even we assume G is finite.

17. Prove that in Problem 14 infinite examples exist, satisfying the conditions, which are not groups.

36.17 Let G be the set of natural numbers. For every n in G define a binary operation $\overset{+}{n}$ on G as : $x \overset{+}{n} y = x + y + n$ for all x, y in G. Then $(G, \overset{+}{n})$ satisfies the conditions of problem 14 except G is finite and is clearly not a group. We have thus got infinite examples.

18. For any $n > 2$ construct a non-abelian group of order $2n$. (*Hint:* imitate the relations in S_3.)

36.18 Consider the mapping ϕ defined on the set $\{x_1, \cdots, x_n\}$ by
$\phi : x_1 \to x_{n-1}$, $x_2 \to x_{n-2}, \cdots\cdots, x_{\frac{n}{2}} \to x_{\frac{n}{2}}, \cdots\cdots$, $x_{n-1} \to x_1$, $x_n \to x_n$, and the mapping:
$\psi : x_1 \to x_2$, $x_2 \to x_3, \cdots\cdots, x_{n-1} \to x_n$, $x_n \to x_1$, when n is even. When n is odd, We only chang ϕ by $\phi : x_1 \to x_{n-1}$, $x_2 \to x_{n-2} \cdots\cdots, x_{n-1} \to x_1$, $x_n \to x_n$.
Then $\{\phi^i \psi^j \mid i = 0, 1, j = 1, 2, \cdots\cdots, n\}$ forms a group of order 2n nnder composition of maps.

19. If S is a set closed under an associative operation, prove that no matter how you bracket $a_1 a_2 \cdots a_n$, retaining the order of the elements, you get the same element in S (e.g., $(a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = a_1 \cdot (a_2 \cdot (a_3 \cdot a_4))$; use induction on n).

36.19 Use induction on n, when $n = 3$ by definition the statement is true. If $a_1 a_2 \cdots a_n$ is bracketed as $x = (a_1 \cdots\cdots a_i)(a_{i+1} \cdots\cdots a_n)$ then by induction hypothesis $a_1 \cdots\cdots a_i = (((a_1 \cdot a_2) a_3) \cdots a_{i-1}) a_i)$, $a_{i+1} \cdots\cdots a_n = (a_{i+1}(a_{i+2} \cdots (a_{n-1} a_n)) \cdots)$ no matter how we bracbete $a_1 \cdots a_i$ and $a_{i+1} \cdots a_n$ in x. Then $x = (\cdots ((a_1 \cdot a_2) \cdot a_3 \cdots a_{i-1}) \circ a_i)(a_{i+1} \cdot (a_{i+2} \cdots (a_{n-1} \cdot a_n)) \cdots) = (((a_1 \cdot a_2) \cdots a_{i-1})(a_i \cdot (a_{i+1} \circ (a_{i+2} \cdots (a_{n-1} \cdot a_n)) \cdots) = \cdots = (a_1 \cdot (a_2 \cdot (\cdots (a_{n-1} \circ a_n)) \cdots)$. This completes the proof.

#20. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $ad - bc \neq 0$ is a rational number. Prove that G forms a group under matrix multiplication.

36.20 Let $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \in G$.

Then $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ a_2c_1+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix}$,

$(a_1a_2 + b_1c_2)(c_1b_2 + d_1d_2) - (a_2c_1 + d_1c_2)(a_1b_2+b_1d_2)$
$= (a_1d_1 - c_1b_1)(a_2d_2 - b_2c_2) \neq 0$.

$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in G$.

$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\left[\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}\right] = \left[\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\right]\begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$

$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}.\begin{pmatrix} \frac{d_1}{a_1d_1-b_1c_1} & \frac{-b_1}{a_1d_1-b_1c_1} \\ \frac{-c_1}{a_1d_1-b_1c_1} & \frac{-a_1}{a_1d_1-b_1c_1} \end{pmatrix}$

$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. G is a group.

#21. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $ad \neq 0$.

Prove that G forms a group under matrix multiplication. Is G abelian?

36.21 Let $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}, \begin{pmatrix} a_3 & b_3 \\ 0 & d_3 \end{pmatrix} \in G$.

$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{pmatrix}$,

$(a_1a_2)(d_1d_2) \neq 0$, $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in G$.

$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\left[\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\begin{pmatrix} a_3 & b_3 \\ 0 & d_3 \end{pmatrix}\right] = \left[\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\right]$.

$\begin{pmatrix} a_3 & b_3 \\ 0 & d_3 \end{pmatrix}.\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} = 0$,

$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} \frac{d_1}{a_1d_1} & \frac{-b_1}{a_1d_1} \\ 0 & \frac{a_1}{a_1d_1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. G is a group.

Since $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}.\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 0 & 6 \end{pmatrix} \neq \begin{pmatrix} 1 & 3 \\ 0 & 6 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}.\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$,

G is not abelian.

#22. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ where $a \neq 0$.

Prove that G is an abelian group under matrix multiplication.

36.22 Let $\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}, \begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix}, \begin{pmatrix} a_3 & 0 \\ 0 & a_3^{-1} \end{pmatrix} \in G$.

$\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix} = \begin{pmatrix} a_1a_2 & 0 \\ 0 & (a_1a_2)^{-1} \end{pmatrix} \in G$.

$\left[\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix}\right]\begin{pmatrix} a_3 & 0 \\ 0 & a_3^{-1} \end{pmatrix} = \begin{pmatrix} a_1a_2a_3 & 0 \\ 0 & a_1^{-1}a_2^{-1}a_3^{-1} \end{pmatrix}$

$= \begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}\left[\begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix}\begin{pmatrix} a_3 & 0 \\ 0 & a_3^{-1} \end{pmatrix}\right]$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}$.

$\begin{pmatrix} a_1^{-1} & 0 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix} = \begin{pmatrix} a_1a_2 & 0 \\ 0 & a_1^{-1}a_2^{-1} \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix}$

$\begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}$. G is an abelian group.

#23. Construct in the G of Problem 21 a subgroup of order 4.

36.23 $H = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$ is a subgroup of G defined in (36.21).

#24. Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo 2, such that $ad - bc \neq 0$. Using matrix multiplication as the operation in G, prove that G is a group of order 6.

36.24 As we have proved in (36.20) G is a group. To find the order of G, we must find solutions of

ad−bc ≠ 0.
If a = 0, b = c = 1 and d = 0 or d = 1.
If a ≠ 0, a = 1, d = 0, b = c = 1.
If a ≠ 0, a = 1, and d = 1, then c = b = o or c = 1, b = 0, or c = 0, b = 1. There are 6 solutions of ad-bc ≠0 ,G is a group of order 6.

#25. (a) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad - bc \neq 0$ and a, b, c, d are integers modulo 3, relative to matrix multiplication. Show that $o(G) = 48$.

(b) If we modify the example of G in part (a) by insisting that $ad - bc = 1$, then what is $o(G)$?

36.25(a) Clearly, a and b can not be zero simultaneously. Now,there are (3×3−1) = 8 choices of (a,b) with (a, b) ≠ (0, 0). For a fixed pair of(a, b), (a, b) ≠ 0. We want to find the number of (c, d) such that ad−bc ≠0, For the given (a, b), ad−bc = 0 if and only if e = ra, d = rb with r = 0, 1 or 2. Therefore, there are (3×3−3) = 6 choices of (c, d). $o(G)$ = 8×6 = 48.

(b) If ad−bc ≠ 0, then ad−bc = 1 or ad−bc=2.
If ad−bc = 1, (2a) d − (2b)c = 2.
For $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, ad−bc = 1, let it correspond with $\begin{pmatrix} 2a & 2b \\ c & d \end{pmatrix}$. There is a one − to − one correspondence between $A = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | ad-bc=1 \}$ and $B = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | ad-bc=2 \}$. $|A| = |B|$, $A \cap B = \phi$. $A \cup B$ is the group define in (a). Therefore $o(G) = \frac{48}{2} = 24$.

#*26. (a) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo p, p a prime number, such that $ad - bc \neq 0$.

G forms a group relative to matrix multiplication. What is $o(G)$?

(b) Let H be the subgroup of the G of part (a) defined by

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid ad - bc = 1 \right\}.$$

What is $o(H)$?

37.26(a) Clearly, (a, b) ≠ (0, 0). For a fixed (a, b)≠ (0, 0), We want to find (c, d) such that ad−bc ≠ 0, (c, d) with ad−bc = 0 if and only if c = ra, d =rb, r = 0, 1, 2, ⋯ ,p−1. Therefore $o(G) = (p^2 - 1)(p^2 - p)$.

(b) Define a partition on G as
$A_i = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | ad-bc = i \}$, i=1, 2, ⋯ ,p−1.
Every Ai has a one − to − one correspondence with Ai defined as $\sigma: A_1 \to A_i$,

$\sigma \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \sigma \begin{pmatrix} ia & ib \\ c & d \end{pmatrix}$. $|A_i| = |A_1|$, i=1, 2, ⋯ , p−1, $A_i \cap A_j = \phi$ for i ≠ j. $G = \bigcup_{i=1}^{n} A_i$.

Therefore $o(H) = o(A_1) = \frac{o(G)}{p-1} = (p+1)p(p-1)$

2.5 A Counting Principle

1. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?)

46.1 Let H_α be subgroup of G and $\alpha \in A$, A an index set. Then $H = \bigcap H_a$ is also a subgroup of G. For if $x, y \in H$, $x, y \in H_a$ for all $\alpha \in A$ and since all H_a are subgroups of G, $x \cdot y \in H_a$ and $x^{-1} \in H_a$ for all $\alpha \in A$, i.e. $x \cdot y, x^{-1} \in H$. By Lemma 2.4.1, H is a subgroup of G.

*2. Let G be a group such that the intersection of all its subgroups which are different from (e) is a subgroup different from (e). Prove that every element in G has finite order.

46.2 Suppose G has an element g with infinite order. Then (g^n) is a subgroup of G for all $n \in N$ and $\bigcap_{n \in N} (g^n) = (e)$. But $\bigcap_{n \in N} (g^n)$ contains the intersection of all subgroups distinct from (e) which is different from (e). This is a contradiction.

3. If G has no nontrivial subgroups, show that G must be finite of prime order.

46.3 Suppose G is not finite. $a \in G$, $a \neq e$ implies $a^2 \neq e$ and a is of infinite order otherwise (a) will be a proper subgroup of G. Then (a^2) is a proper subgroup of (a) and hence a proper subgroup of G. This shows that G is finite.
Let $o(G) = n$. If $n = pq$, $p > 1$, $q > 1$, $a \in G$, $a \neq e$ implies $o(a) = n = o(a^p)$, otherwise (a) or (a^p) is a proper subgroup of G. But $(a^p)^q = a^n = e$ shows that $o(a^p) \leqslant q < n$, a contradiction.

4. (a) If H is a subgroup of G, and $a \in G$ let $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Show that aHa^{-1} is a subgroup of G.
   (b) If H is finite, what is $o(aHa^{-1})$?

47.4 (a) $x, y \in a H a^{-1}$ implies there are h and h′ in H such that $x = a h a^{-1}$, $y = a h' a^{-1}$, $x y = (a h a^{-1})(a h' a^{-1}) = a(h h') a^{-1}$, $x^{-1} = (a h a^{-1})^{-1} = a h^{-1} a^{-1}$. Since H is a subgroup of G, $h h' \in H$ and $h^{-1} \in H$, this shows that $x y, x^{-1} \in a H a^{-1}$, $a H a^{-1}$ is therefore a subgroup of G.
(b) Define $\sigma: H \to a H a^{-1}$ by $\sigma(h) = a H a^{-1}$. This mapping is 1—1 and onto. Hence $o(a H a^{-1}) = o(H)$.

5. For a subgroup H of G define the left coset aH of H in G as the set of all elements of the form ah, $h \in H$. Show that there is a one-to-one correspondence between the set of left cosets of H in G and the set of right cosets of H in G.

47.5 Define $\sigma(H a) = a^{-1} H$. σ is clearly an mapping from the set of right cosets onto the set of left cosets. To show σ is 1—1, suppose $a^{-1} H = b^{-1} H$. Then $(a^{-1})^{-1} b^{-1} \in H$, $a b^{-1} \in H$, i.e. $H a = H b$. σ is the reguired one-to-one correspondence.

6. Write out all the right cosets of H in G where
   (a) $G = (a)$ is a cyclic group of order 10 and $H = (a^2)$ is the subgroup of G generated by a^2.
   (b) G as in part (a), $H = (a^5)$ is the subgroup of G generated by a^5.
   (c) $G = A(S)$, $S = \{x_1, x_2, x_3\}$, and $H = \{\sigma \in G \mid x_1\sigma = x_i\}$.

47.6 (a) H and Ha.
(b) H, Ha, Ha^2, Ha^3, Ha^4.
(c) H, $H\psi$, $H\psi^2$, where $\psi: x_1 \to x_2$, $x_2 \to x_3$, $x_3 \to x_1$.

7. Write out all the left cosets of H in G for H and G as in parts (a), (b), (c) of Problem 6.

47.7 (a) H and aH
(b) H, aH, a^2 H, a^3 H, a^4 H.
(c) H, ϕH, ϕ^2H.

8. Is every right coset of H in G a left coset of H in G in the groups of Problem 6?

47.8 In(a) and (b) every right coset of H in G is a left coset of H in G.
But in (c), H = $\{1, \phi\cdot\phi\}$, Hϕ = $\{\phi, \phi\}$, Hϕ^2 = $\{\phi^2, \phi^2\cdot\phi\}$, and H = $\{1, \phi\cdot\phi\}$, ϕH = $\{\phi, \phi^2\phi\}$, ϕ^2H = $\{\phi^2, \phi\}$. (Example 2.2.3)
Hϕ is a right coset of H in G but is not a left coset of H in G.

9. Suppose that H is a subgroup of G such that whenever $Ha \neq Hb$ then $aH \neq bH$. Prove that $gHg^{-1} \subset H$ for all $g \in G$.

47.9 The given condition is equivalent to that whenever aH = bH then Ha = Hb. For h$\in$H, ghH = gH, therefore Hgh = Hg. and gh $g^{-1} \in$H, i.e. g H $g^{-1} \subset$H for all g$\in$G.

10. Let G be the group of integers under addition, H_n the subgroup consisting of all multiples of a fixed integer n in G. Determine the index of H_n in G and write out all the right cosets of H_n in G.

47.10 $i_G(H_n) = n$. H_n, $H_n + 1$, $H_n + 2$, ..., $H_n + (n-1)$ are all the right cosets of H_n in G.

11. In Problem 10, what is $H_n \cap H_m$?

47.11 $H_n \cap H_m = \{k[m, n] \mid k \in J\}$.

12. If G is a group and H, K are two subgroups of finite index in G, prove that $H \cap K$ is of finite index in G. Can you find an upper bound for the index of $H \cap K$ in G?

47.12 Claim (H$\cap$K)a = Ha$\cap$Ka for all a in G.
For x$\in$(H$\cap$K)a$\Leftrightarrow$ x = pa where p$\in$H$\cap$K$\Leftrightarrow$

x$\in$Ha, x$\in$Ka $\Leftrightarrow$ x$\in$Ha$\cap$Ka. Therefore $i_G(H)\cdot i_G(K)$ is an upper bound for $i_G(H\cap K)$.

13. If $a \in G$, define $N(a) = \{x \in G \mid xa = ax\}$. Show that $N(a)$ is a subgroup of G. $N(a)$ is usually called the *normalizer* or *centralizer* of a in G.

47.13 x, y$\in$N(a) $\Rightarrow$ xa = ax and ya = ay $\Rightarrow$ (xy)a = x(ya) = x(ay) = (xa)y = (ax)y = (ax)y = a(xy) and $ax^{-1} = x^{-1}a$ $\Rightarrow$ xy$\in$N(a) and $x^{-1} \in$ N(a). Therefore N(a) is a subgroup of G.

14. If H is a subgroup of G, then by the centralizer $C(H)$ of H we mean the set $\{x \in G \mid xh = hx \text{ all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

47.14 x, y$\in$C(H) $\Rightarrow$ for all h$\in$H, xh = hx and yh = hy $\Rightarrow$ for all h$\in$H, (xy)h = xyh = xhy = hxy = h(xy) and $h^{-1}x = xh^{-1} \Rightarrow$ xy, $x^{-1} \in$ C(H). C(H) is a subgroup of G.

15. The *center* Z of a group G is defined by $Z = \{z \in G \mid zx = xz \text{ all } x \in G\}$. Prove that Z is a subgroup of G. Can you recognize Z as $C(T)$ for some subgroup T of G?

47.15 Z = C(G), therefore Z is a subgroup of G.

16. If H is a subgroup of G, let $N(H) = \{a \in G \mid aHa^{-1} = H\}$ [see Problem 4(a)]. Prove that
(a) $N(H)$ is a subgroup of G. (b) $N(H) \supset H$.

47.16 (a) a, b$\in$N(H) $\Rightarrow$ aHa^{-1} = H and bHb^{-1} = H $\Rightarrow$ (ab)H(ab)$^{-1}$ = (ab)H($b^{-1}a^{-1}$) = a(bHb^{-1})a^{-1} = aHa^{-1} = H and a^{-1}H$(a^{-1})^{-1}$ = H $\Rightarrow$ ab $\in$ N(H), $a^{-1} \in$ N(H). N(H) is a subgroup of G.
(b) h $\in$ H $\Rightarrow$ hHh^{-1} = H $\Rightarrow$ h $\in$ N(H), N(H)$\supset$H.

17. Give an example of a group G and a subgroup H such that $N(H) \neq C(H)$. Is there any containing relation between $N(H)$ and $C(H)$?

47.17 $G = A(S)$, $S = \{x_1, x_2, x_3\}$, $H = (\phi)$, $N(H) = G$ $C(H) = H$, $N(H) \supset C(H)$.
Since if $x \in C(H)$, $xh = hx$ for all h in H and hence $xhx^{-1} = h$ and $xhx^{-1} \in H$ $xHx^{-1} \subset H$, $xHx^{-1} = H$, $x \in N(H)$.

18. If H is a subgroup of G let

$$N = \bigcap_{x \in G} xHx^{-1}.$$

Prove that N is a subgroup of G such that $aNa^{-1} = N$ for all $a \in G$.

48.18 $a \in G$, $aNa^{-1} = a(\bigcap_{x \in G} xHx^{-1})a^{-1} = \bigcap_{x \in G} (ax)H(ax)^{-1}$

$= \bigcap_{x \in G} (ax)H(ax)^{-1} = \bigcap_{y \in G} yHy^{-1} = N.$

By (47.4), xHx^{-1} is a subgroup of G. N, as the intersection of subgroups of G, is also a subgroup of G.

*19. If H is a subgroup of finite index in G, prove that there is only a finite number of distinct subgroups in G of the form aHa^{-1}.

48.19 If H is a subgroup of finite index in G, then N(H) containing H is also of finite index. Now define a mapping σ of right cosets of N(H) in G to subgrougs of type aHa^{-1} by $\sigma(N(H)a) = a^{-1}Ha$. If $a^{-1}Ha = b^{-1}Hb$, $ab^{-1}H(ab^{-1})^{-1} = H$ hence $ab^{-1} \in N(H)$ and $N(H)a = N(H)b$. σ is one-to-one and onto. Therefore there is only a finite number of distinct subgroups in G of the form aHa^{-1}, and clearly the number is $i_G(N(H))$.

*20. If H is of finite index in G prove that there is a subgroup N of G, contained in H, and of finite index in G such that $aNa^{-1} = N$ for all $a \in G$. Can you give an upper bound for the index of this N in G?

48.20 H is finite index in G. xHx^{-1} is also finite index in G. By (48.19) and (47.12) $N = \bigcap_{x \in G} xHx^{-1}$ is a subgroup of G contained in H, and of finite index in G such that $aNa^{-1} = N$ for all $a \in G$.
An upper bound for $i_G(H)$ is $(i_G(H))^{i_G(N(H))}$.

21. Let the mapping τ_{ab} for a, b real numbers, map the reals into the reals by the rule $\tau_{ab}: x \to ax + b$. Let $G = \{\tau_{ab} \mid a \neq 0\}$. Prove that G is a group under the composition of mappings. Find the formula for $\tau_{ab}\tau_{cd}$.

48.21 $x\,\tau ab\,\tau cd = (ax + b)\,\tau cd = c(ax + b) + d = acx + (bc + d) = x\,\tau(ac)(bc + d)$.
$\tau ab\,\tau cd = \tau(ac)(bc + d)$. If $\tau ab, \tau cd \in G$, then $a \neq 0$, $c \neq 0$ implies $ac \neq 0$ and $\tau ab\,\tau cd = \tau(ac)(bc + d) \in G$. $\tau_{ab}^{-1} = \tau_{(\frac{1}{a})(-\frac{b}{a})}$. G is a group.

22. In Problem 21, let $H = \{\tau_{ab} \in G \mid a \text{ is rational}\}$. Show that H is a subgroup of G. List all the right cosets of H in G, and all the left cosets of H in G. From this show that every left coset of H in G is a right coset of H in G.

48.22 Since $\tau ab\,\tau cd = \tau(ac)(bc + d)$ and $\tau_{ab}^{-1} = \tau_{(\frac{1}{a})(-\frac{b}{a})}$, if $\tau ab, \tau cd \in H$, then $\tau ab\,\tau cd \in H$ and $\tau_{ab}^{-1} \in H$, H is a subgroup of G. Define an equivalence relation on $R \setminus (0)$ by $x \sim y$ if and only if there is a rational r such that $x = ry$. Let $K = \{r\}$ be the set of representation elements of equivalence classes. Then $\{H\tau r o \mid r \in K\}$ is the set of all right cosets of H in G, $\{\tau r o\, H \mid r \in K\}$ is the set of all left cosets of H in G.
Let $H\tau ab$ be a right coset of H in G. $\tau xy\,\tau ab \in H\tau ab$ implies $\tau(ax)(ya + b) \in H\tau ab$. But $\tau ar\,\tau x(ya + b - rx) = \tau(ax)(ya + b)$.
Therefore $H\tau ab = \tau ar\, H$. This shows that every right coset of H in G is a left coset of H in G.

23. In the group G of Problem 21, let $N = \{\tau_{1b} \in G\}$. Prove
(a) N is a subgroup of G.
(b) If $a \in G$, $n \in N$, then $ana^{-1} \in N$.

48.23(a) $\tau_{1b}\ \tau_{1c} = \tau_{1(b+c)} \in N$ if $\tau_{1b}, \tau_{1c} \in N$
$\tau_{1b}^{-1} = \tau_{1(-b)} \in N$. N is a subgroup of G.

(b) $a = \tau_{xy}$, $x \neq 0$, $n = \tau_{1z}$. $a^{-1} = \tau_{\frac{1}{x}(-\frac{y}{x})}$,
$ana^{-1} = \tau_{xy}\ \tau_{1z}\ \tau_{\frac{1}{x}(-\frac{y}{x})} = \tau_{1(zx)} \in N$.

*24. Let G be a finite group whose order is *not* divisible by 3. Suppose that $(ab)^3 = a^3b^3$ for all $a, b \in G$. Prove that G must be abelian.

48.24 Let $o(G) = n$. There are positive integer s and integer r such that $3s + rn = 1$. $a = a^{3s+rn} = a^{3s} \cdot (a^n)^r = a^{3s}$ for all a in G. Therefore, $(ab) = (ab)^{3s} = [(ab)^3]^s = (a^3 \cdot b^3)^s =$
$\underbrace{(a^3 \cdot b^3)(a^3 \cdot b^3) \cdots\cdots (a^3 \cdot b^3)}_{s} =$
$a^3 \underbrace{(b^3 \cdot a^3)(b^3 \cdot a^3) \cdots\cdots (b^3 \cdot a^3)}_{s-1} \cdot b^3 = a^3 (b^3a^3)^s \cdot$
$a^{-3} = a^3 (ba)^{3s} a^{-3} = a^3 baa^{-3} = a^3 ba^{-2} \cdot a^2 b =$
ba^2 for all a and b in G. $a^2 \in Z(G)$ for all a in G. $(ab)(ab)(ab) = a^3b^3$ implies $baba = a^2b^2 = b^2a^2 = bbaa$ and $ab = ba$. Therefore, G is abelian.

*25. Let G be an abelian group and suppose that G has elements of orders m and n, respectively. Prove that G has an element whose order is the least common multiple of m and n.

48.25 Suppose $(m, n) = 1$, where $o(a) = m$, $o(b) = n$.
$(ab)^{mn} = a^{mn}b^{mn} = e$, $o(ab) \mid mn$. $e = (ab)^{o(ab)} = a^{o(ab)}\ b^{o(ab)}$, $a^{o(ab)} = b^{-o(ab)}$, $a^{o(ab)n} = b^{-o(ab)n} = e$, $m = o(a) \mid o(ab)n$. $(m, n) = 1$ implies $m \mid o(ab)$. As the same way, $n \mid o(ab)$. $(m, n) = 1$ implies $mn \mid o(ab)$. Hence, $o(ab) = mn$.

Now, suppose $(m, n) = d$. $o(a^d) = \frac{m}{d}$, $o(b) = n$, $(\frac{m}{d}, n) = 1$ implies $o(a^d b) = \frac{m}{d} \cdot n = \frac{mn}{d} = [m, n]$. This completes the proof.

27. Prove that any subgroup of a cyclic group is itself a cyclic group.

48.27 Suppose that G is a cyclic group generated by x. Let H be a subgroup of G. Let i be the smallest positive integer such that $x^i \in H$. For any $x^r \in H$, $r = ai + b$ for some integer a and b such that $0 \leq b < i$. $x^r = x^{ai+b} = (x^i)^a \cdot x^b$, $x^b = x^r \cdot (x^i)^{-a} \in H$, $b = 0$ and $x^r = (x^i)^a$.
H is a cyclic group generated by x^i.

28. How many generators does a cyclic group of order n have? ($b \in G$ is a generator if $(b) = G$.)

48.28 There are $\phi(n)$ generators in a cyclic group of order n.
Let $G = \{e, a, a^2, \cdots\cdots, a^{n-1}\}$. a^m is a generator of G if and only if $(m, n) = 1$.
For, if $(m, n) = 1$, there is r, s in Z such that $rm + sn = 1$. $a = a^{rm+sn} = (a^m)^r \cdot (a^n)^s = (a^m)^r \cdot e = (a^m)^r$. $a^i = (a^m)^{ri}$, a^m generates G. On the other hand, if $m = rs$ with $r \neq 1$, $s \neq 1$. Then $a^r \neq (a^m)^i$ for all i. a^m is not a generator of G. The number of generators of G is $\phi(n)$.

Let U_n denote the integers relatively prime to n under multiplication mod n. In Problem 15(b), Section 2.3, it is indicated that U_n is a group. In the next few problems we look at the nature of U_n as a group for some specific values of n.

29. Show that U_8 is not a cyclic group.

49.29 $U_8 = \{1, 3, 5, 7\}$. $3^2 \equiv 1 \pmod 8$, $5^2 \equiv 1 \pmod 8$, $7^2 \equiv 1 \pmod 8$. U_8 has no element of order 4.
U_8 is not a cyclic group.

30. Show that U_9 is a cyclic group. What are all its generators?

49.30 $U_9 = \{1, 2, 4, 5, 7, 8\}$. $o(U_9) = 6$.
$2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$. 2 is a generator of U_9. By (48.28), 2 and 5 are all generators of U_9.

31. Show that U_{17} is a cyclic group. What are all its generators?

49.31 $U_{17} = \{1, 2, \cdots, 16\}$.

a=	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3^a \equiv$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

3 is a generator of U_{17}. By (48.28), 3, 10, 5, 11, 14, 7, 12, 6 are all generators of U_{17}.

32. Show that U_{18} is a cyclic group.

49.32 $U_{18} = \{1, 5, 7, 11, 13, 17\}$. $5^1 \equiv 5$, $5^2 \equiv 7$, $5^3 \equiv 17$, $5^4 \equiv 13$, $5^5 \equiv 11$, $5^6 \equiv 1$.
U_{18} is a cyclic group.

33. Show that U_{20} is not a cyclic group.

49.33 $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. $3^4 \equiv 1$, $7^4 \equiv 1$ $9^2 \equiv 1$, $11^2 \equiv 1$, $13^4 \equiv 1$, $17^4 \equiv 1$, $19^2 \equiv 1$.
$o(U_{20}) = 8$, U is not a cyclic group.

34. Show that both U_{25} and U_{27} are cyclic groups.

49.34 U_{25}:

a=	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$2^a \equiv$	2	4	8	16	7	14	3	6	12	24	23	21	17	9	18	11	22	19	13	1

Since $o(U_{25}) = 20$, U_{25} is a cyclic group.

U_{27}

a=	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^a \equiv$	2	4	8	16	5	10	20	13	26	25	23	19	11	22	17	7	14	1

Since $o(U_{27}) = 18$, U_{27} is a cyclic group.

35. Hazard a guess at what all the n such that U_n is cyclic are. (You can verify your guess by looking in any reasonable book on number theory.)

49.35 $n = 2, 4, p^\alpha$ or $2p^\alpha$, p an old prime, if and only if U_n is cyclic.

36. If $a \in G$ and $a^m = e$, prove that $o(a) \mid m$.

49.36 There are integers i and j such that $m = io(a)+j$ and $0 \le j < o(a)$. $e = a^m = a^{io(a)+j} = (a^{o(a)})^i \cdot (a^j) = e^i \cdot a^j = a^j$. If $j \neq 0$, $j < o(a)$, contrary to the definition of $o(a)$ which says that $o(a)$ is the least positive integer n such that $a^n = 1$. Hence $j = 0$ and $m = io(a)$, $o(a) \mid m$.

37. If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for some $a, b \in G$, find $o(b)$.

49.37 $a^2ba^{-2} = a(aba^{-1})a^{-1} = ab^2a^{-1} = (aba^{-1})(aba^{-1}) = (aba^{-1})^2 = (b^2)^2 = b^4$. By induction. We can prove that $a^nba^{-n} = b^{2^n}$. For $n = 1$, it's trivial. Suppose $a^nba^{-n} = b^{2^n}$.
Then $a^{n+1}ba^{-(n+1)} = a(a^nba^{-n})a^{-1} = ab^{2^n}a^{-1} = \underbrace{(aba^{-1})(aba^{-1})}_{2^n} \cdots\cdots \underbrace{(aba^{-1})}_{2^n} = (aba^{-1})^{2^n} = (b^2)^{2^n} = b^{2^{n+1}}$. Hence, for $n = 5$, $b^{2^5} = a^5ba^{-5} = ebe = b$. $b^{31} = e$. $o(b) \mid 31$ by (49.36). $o(b) = 1$ or $o(b) = 31$.

*38. Let G be a finite abelian group in which the number of solutions in G of the equation $x^n = e$ is at most n for every positive integer n. Prove that G must be a cyclic group.

49.38 Let a be the element in G which has the largest order in G. For any element b in G, $o(b) \mid o(a)$. Otherwise, $[o(b), o(a)] > o(a)$ and G has an element of order $[o(b), o(a)]$ by (48.25), which contradicts with choice of a.
the order of any element of G is a divisor of $o(a)$.

The subgroup H generated by a has $o(a)$ elements. By Corollary 2 of Theorem 2.4.1, $x^{o(a)} = e$ has all solutians in H. For b in G, $o(b) \mid o(a)$ implies $b^{o(a)} = e$, b is a solution of $x^{o(a)} = e$ and $b \in H$. $H = G$, G is a cyclic group.

39. Let G be a group and A, B subgroups of G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$. Prove
(a) The relation so defined is an equivalence relation.
(b) The equivalence class of x is $AxB = \{axb \mid a \in A, b \in B\}$. ($AxB$ is called a *double coset* of A and B in G.)

49.39(a) $x = exe$ implies $x \sim x$. If $x \sim y$, then $y = axb$ for some a in A and b in B. $x = a^{-1}yb^{-1}$, $a^{-1} \in A$, $b^{-1} \in B$ implies $x \sim y$. Suppose $x \sim y$ and $y \sim z$. Then $y = a_1xb_1$ and $z = a_2yb_2$ for some a_1, a_2 in A and b_1, b_2 in B. $z = a_2yb_2 = a_2(a_1xb_1)b_2 = (a_2a_1)x(b_1b_2)$. $a_2a_1 \in A$, $b_1b_2 \in B$ implies $x \sim z$. $\sim$ is an equivalence relation.

(b) AxB is clearly the equivalence class of x.

40. If G is a finite group, show that the number of elements in the double coset AxB is

$$\frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

49.40 $o(AxB) = o(AxBx^{-1}) = o[A(xBx^{-1})] = \dfrac{o(A)o(xBx^{-1})}{o(A \cap xBx^{-1})} = \dfrac{o(A)o(B)}{o(A \cap xBx^{-1})}$.

41. If G is a finite group and A is a subgroup of G such that all double cosets AxA have the same number of elements, show that $gAg^{-1} = A$ for all $g \in G$.

49.41 By assumption, $o(AgA) = o(AeA)$. $o(AeA) = o(A \cdot A) = o(A) \cdot o(AgA) = \dfrac{o(A) \cdot o(A)}{o(A \cap gAg^{-1})}$. Hence $o(A) =$

$\dfrac{o(A)o(A)}{o(A \cap gAg^{-1})}$. $o(A) = o(A \cap gAg^{-1})$. $A \cap gAg^{-1} \subset A$.

$o(A \cap gAg^{-1}) = o(A)$ implies $A = A \cap gAg^{-1}$ and $A \subset gAg^{-1}$. Since $o(A) = o(gAg^{-1})$, We have $gAg^{-1} = A$.

2.6 Normal Subgroups and Quotient Groups.

1. If H is a subgroup of G such that the product of two right cosets of H in G is again a right coset of H in G, prove that H is normal in G.

53.1 For every $g \in G$, $HgHg^{-1}$ is a right coset of H in G by our assumption. Since $e = e \cdot g \cdot e \cdot g^{-1} \in HgHg^{-1} = He = H$. Hence for all $h \in H$, $ghg^{-1} = e \cdot g \cdot h \cdot g^{-1} \in HgHg^{-1} = H$. H is a normal subgroup of G.

2. If G is a group and H is a subgroup of index 2 in G, prove that H is a normal subgroup of G.

53.2 There are exactly two right cosets H, Hg of H in G and two left cosets H, gH of H in G. Therefore, the right coset $Hg = gH$ is also a left coset of H. By Lemma 2.6.2, H is normal in G.

3. If N is a normal subgroup of G and H is any subgroup of G, prove that NH is a subgroup of G.

53.3 Let $n_1h_1 \in NH$, $n_2h_2 \in NH$, where $n_1, n_2 \in N$, $h_1, h_2 \in H$.
$(n_1h_1)(n_2h_2) = [n_1(h_1n_2h_1^{-1})][h_1h_2] \in NH$.
$(n_1h_1)^{-1} = h_1^{-1}n_1^{-1} = [h_1^{-1}n_1(h_1^{-1})^{-1}]h_1^{-1}] \in NH$.
Hence NH is a subgroup of G by Lemma 2.4.1.

4. Show that the intersection of two normal subgroups of G is a normal subgroup of G.

53.4 Let M, N be normal subgroups of G. $M \cap N$ is a subgroup of G by (46.1). For all g in G and $x \in M \cap N$, $x \in M$, $x \in N$. Since M, N are normal subgroups of G, $gxg^{-1} \in M$ and $gxg^{-1} \in N$ by definition of normal subgroup. Hence $gxg^{-1} \in M \cap N$.

5. If H is a subgroup of G and N is a normal subgroup of G, show that $H \cap N$ is a normal subgroup of H.

53.5 $H \cap N$ is a subgroup of H by (46.1). For all $h \in H$ and $n \in H \cap N$, $hnh^{-1} \in H$ since $h, n, h^{-1} \in H$ and $hnh^{-1} \in N$ since N is a normal subgroup of G. $hnh^{-1} \in H \cap N$. $H \cap N$ is a normal subgroup of H.

6. Show that every subgroup of an abelian group is normal.

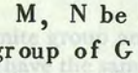
53.6 Let H be a subgroup of an abelian group G. Then for all g in G and h in H, $ghg^{-1} = gg^{-1}h = eh = h \in H$. Hence H is a normal subgroup of G.

*7. Is the converse of Problem 6 true? If yes, prove it, if no, give an example of a non-abelian group all of whose subgroups are normal.

53.7 The following group we define is called a quaternion group. Though there are many ways to define the group, we choose an explicit one.

$G = \{1, -1, i, -i, j, -j, k, -k\}$.
$i^2 = j^2 = k^2 = -1$, $ij = -ji = k$,
$jk = -kj = i$, $ki = -ik = j$.

	1	−1	i	−i	j	−j	k	−k
1	1	−1	i	−i	j	−j	k	−k
−1	−1	1	−i	i	−j	j	−k	k
i	i	−i	−1	1	k	−k	−j	j
−i	−i	i	1	−1	−k	k	j	−j
j	j	−j	−k	k	−1	1	i	−i
−j	−j	j	k	−k	1	−1	−i	i
k	k	−k	j	−j	−i	i	−1	1
−k	−k	k	−j	j	i	−i	1	−1



It's easy to check that G is a group and the subgroups of G are $\{1\}$, $\{1, -1\}$, $\{1, -1, i, -i\}$, $\{1, -1, j, -j\}$, $\{1, -1, k, -k\}$ and $\{1, -1, i, -i, j, -j, k, -k\}$ and that all these subgroups are normal in G.

8. Give an example of a group G, subgroup H, and an element $a \in G$ such that $aHa^{-1} \subset H$ but $aHa^{-1} \neq H$.

53.8 $G = \{ g^i h^j \mid i, j \text{ integers} \}$. $(g^i h^j)(g^{i'} g^{j'}) = g^{i-i'} h^{2i+j+j'}$. G is a group under this definition. Let $H = \{ h^i \mid i : \text{integer} \}$. Then $g^{-1}Hg = \{h^{2i} \mid i : \text{integer} \}$. $g^{-1}Hg \subsetneq H$

9. Suppose H is the only subgroup of order $o(H)$ in the finite group G. Prove that H is a normal subgroup of G.

53.9 By (47.4) gHg^{-1} is also a subgroup of G with order $o(H)$. By assumption, $gHg^{-1} = H$ for all g in G. By Lemma 2.6.1, H is a normal subgroup of G.

10. If H is a subgroup of G, let $N(H) = \{g \in G \mid gHg^{-1} = H\}$. Prove
(a) $N(H)$ is a subgroup of G.
(b) H is normal in $N(H)$.
(c) If H is a normal subgroup of the subgroup K in G, then $K \subset N(H)$ (that is, $N(H)$ is the largest subgroup of G in which H is normal).
(d) H is normal in G if and only if $N(H) = G$.

53.10 (a) By (47.16.(a)).
(b) By (47.16 (b)) $N(H) \supset H$ and for all $h \in N(H)$, $hHh^{-1} = H$. Hence By Lemma 2.6.1, H is a normal subgroup of N (H).
(c) $k \in K$. Since H is normal in K, $kHk^{-1} = H$ by Lemma 2.6.1. $k \in N(H)$. Hence $K \subset N(H)$.
(d) By Lemma 2.6.1, H is normal in G if and only if $N(H) = G$.

11. If N and M are normal subgroups of G, prove that NM is also a normal subgroup of G.

53.11 By (53.3), MN is a subgroup of G. For $mn \in M \cdot N$, $m \in M$, $n \in N$ and $g \in G$, $gmng^{-1} = (gmg^{-1})(gng^{-1}) \in M \cdot N$. Hence $M \cdot N$ is normal in G.

*12. Suppose that N and M are two normal subgroups of G and that $N \cap M = (e)$. Show that for any $n \in N$, $m \in M$, $nm = mn$.

53.12 For any $n \in N$, $m \in M$, $n^{-1}m^{-1}nm = (n^{-1}m^{-1}n)m \in M \cdot M = M$ and $n^{-1}(m^{-1}nm) \in N \cdot N = N$.
$\therefore n^{-1}m^{-1}nm \in M \cap N = (e)$. $\therefore n^{-1}m^{-1}nm = e$.
$\therefore nm = mn$.

13. If a cyclic subgroup T of G is normal in G, then show that every subgroup of T is normal in G.

53.13 Let S be a subgroup of T. By (48.27), S is also a cyclic group. Let $T = (a)$. $S = (a^k)$ for some integer k. Since T is a normal subgroup of G, $gag^{-1} \in (a)$ for any g in G. Let $gag^{-1} = a^m$. For any x in S, $x = a^{kr}$ for some integer r. $a = g^{-1}a^m g$, $a^{kr} = g^{-1}a^{mkr}g$, $ga^{kr}g^{-1} = (a^k)^{mr} \in S$.
S is normal in G.

*14. Prove, by an example, that we can find three groups $E \subset F \subset G$, where E is normal in F, F is normal in G, but E is *not* normal in G.

53.14 Let $E = \{ e, (12)(34) \}$, $F = \{e, (12)(34), (13)(24), (14)(23) \}$, $G = S_4$.

15. If N is normal in G and $a \in G$ is of order $o(a)$, prove that the order, m, of Na in G/N is a divisor of $o(a)$.

53.15 $(Na)^{o(a)} = Na^{o(a)} = Ne = N$. By (49.36), $m \mid o(a)$.

16. If N is a normal subgroup in the finite group such that $i_G(N)$ and $o(N)$ are relatively prime, show that any element $x \in G$ satisfying $x^{o(N)} = e$ must be in N.

54.16 $(o(N), i_G(N)) = 1$. implies $ro(N) + S\, i_G(N) = 1$ for some integers r and s.
$o(G/N) = i_G(N)$. $(Nx)^{i_G(N)} = N$.
$(Nx)^{o(N)} = Nx^{o(N)} = Ne = N$.
$Nx = (Nx)^{ro(n)+si_G(N)} = ((Nx)^{o(N)})^r((Nx)^{i_G(N)})^s$
$= N \cdot N = N$. Hence $x \in N$.

17. Let G be defined as all formal symbols $x^i y^j$, $i = 0$, $i, j = 0, 1, 2, \ldots, n-1$ where we assume

$x^i y^j = x^{i'} y^{j'}$ if and only if $i = i', j = j'$

$x^2 = y^n = e, \quad n > 2$

$xy = y^{-1}x.$

(a) Find the form of the product $(x^i y^j)(x^k y^l)$ as $x^\alpha y^\beta$.

(b) Using this, prove that G is a non-abelian group of order $2n$.

(c) If n is odd, prove that the center of G is (e), while if n is even the center of G is larger than (e).

This group is known as a *dihedral* group. A geometric realization of this is obtained as follows: let y be a rotation of the Euclidean plane about the origin through an angle of $2\pi/n$, and x the reflection about the vertical axis. G is the group of motions of the plane generated by y and x.

54.17(a) $xy = y^{-1}x$, $xy^2 = (xy)y = (y^{-1}x)y = y^{-1}(xy) = y^{-1}(y^{-1}x) = y^{-2}x$.

By induction hypothesis suppose $xy^i = y^{-i}x$.

$xy^{i+1} = (xy^i)y = (y^{-i})(xy) = y^{-i}(y^{-1}x) = y^{-(i+1)}x$. Therefore $xy^i = y^{-i}x$ for all positive integer i. $y^j x = xy^{-j}$. $y^j x^t = x^t y^{(-1)^t j}$.

$(x^i y^j)(x^t y^k) = x^t(y^j x^t)y^k = x^i(x^t y^{(-1)^t j})y^k = x^{i+t}y^{(-1)^t j+k}$.

(b) $(x^i y^j)(x^t y^k) = x^{i+t}y^{(-1)^t j+k} \in G$. (note : G is only a set at first. But in (a), we define a product on it).

$[(x^i y^j)(x^t y^k)](x^r y^s) = (x^{i+t}y^{(-1)^t j+k})(x^r y^s) = x^{i+t+r}y^{(-1)^r((-1)^t j+k)+s} = x^{i+t+r}y^{(-1)^{r+t}j+(-1)^r k+s}$.

$(x^i y^j)((x^t y^k)(x^r y^s)) = (x^i y^j)(x^{t+r}y^{(-1)^r k+s}) = x^{i+t+r}y^{(-1)^{t+r}j+(-1)^r k+s} = [(x^i y^j)(x^t y^k)](x^r y^s)$.

$e(x^i y^j) = x^i y^j$.

$(y^j)(y^{n-j}) = y^n = e$.

$(xy^j)(xy^j) = x(y^j x)y^j = x(xy^{-j})y^j = e$.

$xy = y^{-1}x$.

Therefore G is a nonabelian group of order 2n if $n > 1$.

(c) Suppose n is odd. Then if y^i lies in the center of G, $xy^i = y^i x$. $xy^i = y^{-i}x$ implies $y^i x = y^{-i}x$ and so $y^i = y^{-i}$, $y^{2i} = e$. $n \mid 2i$. n is odd implies $n \mid i$, $y^i = 1$.

If xy^i lies in the center of G, then $x(xy^i) = (xy^i)x$, $y^i = xy^i x$, $y^i x = xy^i$. As above $y^i = e$, $xy^i = x$. But x is not in the center of G if $n > 1$. Therefore the center of G is (e) if $n > 1$.

Suppose n is even. $(x^i y^j)y^{\frac{n}{2}} = x^i y^{j+\frac{n}{2}}$.

$y^{\frac{n}{2}}(x^i y^j) = x^i y^{(-1)^i \frac{n}{2}}$. $y^j = x^i y^{\frac{n}{2}} \cdot y^j$

Since $y^{\frac{n}{2}} = y^{-\frac{n}{2}}$. $y^{\frac{n}{2}}$ lies in the center of G.

The center of G is larger than (e).

18. Let G be a group in which, for some integer $n > 1$, $(ab)^n = a^n b^n$ for all $a, b \in G$. Show that

(a) $G^{(n)} = \{x^n \mid x \in G\}$ is a normal subgroup of G.

(b) $G^{(n-1)} = \{x^{n-1} \mid x \in G\}$ is a normal subgroup of G.

54.18(a) $G^{(n)}$ is clearly a subgroup of G. For $g \in G$, $gx^n g^{-1} = (gxg^{-1})^n \in G^{(n)}$.

$G^{(n)}$ is a normal subgroup of G.

(b) $(ab)^n = a^n b^n$, $\underbrace{(ab)(ab)\cdots\cdots(ab)}_{n} = a^n b^n$.

$b\underbrace{(ab)(ab)\cdots\cdots(ab)}_{n-2}a = a^{n-1}b^{n-1}$.

$(ba)^{n-1} = a^{n-1}b^{n-1}$.

For $a^{n-1}, b^{n-1} \in G^{(n-1)}$, $(a^{n-1})^{-1} = (a^{-1})^{n-1} \in G$ and $(a^{n-1})(b^{n-1}) = (ba)^{n-1} \in G^{(n-1)}$.

$G^{(n-1)}$ is a subgroup of G. For $g \in G$, $ga^{n-1}g^{-1} = (gag^{-1})^{n-1} \in G^{(n-1)}$. $G^{(n-1)}$ is a normal subgroup of G.

19. Let G be as in Problem 18. Show

(a) $a^{n-1}b^n = b^n a^{n-1}$ for all $a, b \in G$.

(b) $(aba^{-1}b^{-1})^{n(n-1)} = e$ for all $a, b \in G$.

54.19(a) $(ab)^n = a^n b^n$, $\underbrace{(ab)(ab)\cdots\cdots(ab)}_{n} = a^n b^n$,

$b\underbrace{(ab)(ab)\cdots\cdots(ab)}_{n-1} = a^{n-1}b^n$

$\underbrace{(ba)(ba)\cdots(ba)}_{n-1}b = a^{n-1}b^n$. $(ba)^n = (a^{n-1}b^n)a$

$b^n a^n = a^{n-1}b^n a$. Hence $b^n a^{n-1} = a^{n-1}b^n$.

(b) $(aba^{-1}b^{-1})^{n(n-1)} = (aba^{-1}b^{-1})^{n^2}(aba^{-1}b^{-1})^{-n}$

$= (a^{n^2}b^{n^2}a^{-n^2}b^{-n^2})(bab^{-1}a^{-1})^n =$

$(a^{n^2}b^{n^2}a^{-n^2}b^{-n^2})(b^n a^n b^{-n}a^{-n}) = (a^{n^2}b^{n^2}a^{-n^2})$

$(b^{-n})^{n-1}(a^n b^{-n}a^{-n}) = a^{n^2}b^{n^2}b^{-n(n-1)}a^{-n^2}$

$a^n b^{-n}a^{-n} = a^{n^2}b^n(a^{-n})^{n-1}b^{-n}a^{-n} = a^{n^2}$

$(a^{-n})^{(n-1)}b^n(b^{-n})(a^{-n}) = a^{n^2}a^{-n(n-1)}a^{-n}$

$= e$.

20. Let G be a group such that $(ab)^p = a^p b^p$ for all $a, b \in G$, where p is a prime number. Let $S = \{x \in G \mid x^{p^m} = e$ for some m depending on $x\}$. Prove
(a) S is a normal subgroup of G.
(b) If $\bar{G} = G/S$ and if $\bar{x} \in \bar{G}$ is such that $\bar{x}^p = \bar{e}$ then $\bar{x} = \bar{e}$.

54.20(a) For $x, y \in S$, $x^{p^m} = e$, $y^{p^n} = e$ for some nonnegative integers m and n.
$(x^{-1})^{p^m} = e$. $(xy)^{p^{m+n}} = x^{p^{m+n}}\, y^{p^{m+n}} = e$.
$x^{-1}, xy \in S$. S is a subgroup of G.
For any $g \in G$, $(gxg^{-1})^{p^m} = gx^{p^m}g^{-1} = geg^{-1} = e$. $gxg^{-1} \in S$, S is a normal subgroup of G.

(b) $x^p = \bar{e}$ implies $x^p \in S$, $(x^p)^{p^m} = e$ for some nonnegative integer m. $x^{p^{m+1}} = e$.
$x \in S$, $\bar{x} = \bar{e}$.

#21. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $ad \neq 0$, under matrix multiplication. Let $N = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right\}$. Prove that
(a) N is a normal subgroup of G.
(b) G/N is abelian.

54.21(a) For $\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} \in N$, $\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b_1 \\ 0 & 1 \end{pmatrix} \in N$. $\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_1+b_2 \\ 0 & 1 \end{pmatrix} \in N$.
N is a subgroup of G.
For $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$, $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$

$\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{a} & \frac{-b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix} = \begin{pmatrix} a & ab_1 + b \\ 0 & d \end{pmatrix}\begin{pmatrix} \frac{1}{a} & \frac{-b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix} =$

$\begin{pmatrix} 1 & -\frac{b}{d} + \frac{ab_1 + b}{d} \\ 0 & 1 \end{pmatrix} \in N$. N is a normal subgroup of G.

(b) $N\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = N\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ since $\begin{pmatrix} 1 & -\frac{b}{d} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$.

$\left[N\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix}\right]\left[N\begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix}\right] = N\begin{pmatrix} a_1a_2 & 0 \\ 0 & d_1d_2 \end{pmatrix} =$

$N\begin{pmatrix} a_2a_1 & 0 \\ 0 & d_2d_1 \end{pmatrix} = \left[N\begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix}\right]\left[N\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix}\right]$.

G/N is abelian.

2.7 Homomorphisms

1. In the following, verify if the mappings defined are homomorphisms, and in those cases in which they are homomorphisms, determine the kernel.
   (a) G is the group of nonzero real numbers under multiplication, $\bar{G} = G$, $\phi(x) = x^2$ all $x \in G$.
   (b) G, $\bar{G}$ as in (a), $\phi(x) = 2^x$.
   (c) G is the group of real numbers under addition, $\bar{G} = G$, $\phi(x) = x + 1$ all $x \in G$.
   (d) G, $\bar{G}$ as in (c), $\phi(x) = 13x$ for $x \in G$.
   (e) G is any abelian group, $\bar{G} = G$, $\phi(x) = x^5$ all $x \in G$.

64.1 (a) $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$, ϕ is a homomarphism. The kernel of ϕ is $\{\pm 1\}$.

(b) Since $\phi(xy) = 2^{xy}$ and $\phi(x)\,\phi(y) = 2^x \cdot 2^y = 2^{x+y}$, ϕ is not a homomorphism of G.

(c) Since $\phi(x+y) = (x+y)+1$ and $\phi(x)+\phi(y) = (x+1)+(y+1) = x+y+2$, ϕ is not a homomorphism of G.

(d) $\phi(x+y) = 13(x+y) = 13x+13y = \phi(x)+\phi(y)$, so that ϕ is a homomorphism of G with kernel $\{0\}$.

(e) $\phi(xy) = (xy)^5 = x^5y^5 = \phi(x)\phi(y)$ so that ϕ is a homomorphism of G with kernel $\{x \in G \mid x^5 = 1\}$.

2. Let G be any group, g a fixed element in G. Define $\phi: G \to G$ by $\phi(x) = gxg^{-1}$. Prove that ϕ is an isomorphism of G onto G.

64.2 $\phi(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \phi(x)\phi(y)$. For all x in G, $\phi(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$. If $e = \phi(x) = gxg^{-1}$, $x = e$. Therefore, ϕ is an isomorphism of G onto G.

3. Let G be a finite abelian group of order $o(G)$ and suppose the integer n is relatively prime to $o(G)$. Prove that every $g \in G$ can be written as $g = x^n$ with $x \in G$. (*Hint:* Consider the mapping $\phi: G \to G$ defined by $\phi(y) = y^n$, and prove this mapping is an isomorphism of G onto G.)

64.3 Consider the mapping $\phi : G \to G$ defined by $\phi(y) = y^n$. Then, $\phi(xy) = (xy)^n = x^n y^n = \phi(x)\,\phi(y)$, ϕ is a homomorphism of G into G. The kernel of G is $K = \{x \in G \mid x^n = e\}$. Since $(n, o(G)) = 1$, there are s, t such that $ns + o(G)t = 1$. If $x \in K$, $x = x^1 = x^{ns+o(G)t} = (x^n)^s \cdot (x^{o(G)t}) = e$. ϕ is an one-to-one mapping of G into G. Since G is finite, ϕ is onto and every $g \in G$ can be written as $g = x^n$ with $x \in G$.

4. (a) Given any group G and a subset U, let $\hat{U}$ be the smallest subgroup of G which contains U. Prove there is such a subgroup $\hat{U}$ in G. ($\hat{U}$ is called the *subgroup generated by U.*)
   (b) If $gug^{-1} \in U$ for all $g \in G$, $u \in U$, prove that $\hat{U}$ is a normal subgroup of G.

64.4 (a) $\hat{U} = \bigcap H$, where H is a subgroup of G which contains U.

(b) $gug^{-1} \in U$ for all g in G and u in U impies $gUg^{-1} = U$.

For $gUg^{-1} \subset U$ and if $u \in U$, $u = g(g^{-1}ug)g^{-1} \in gUg^{-1}$ since $g^{-1}ug \in U$. Let H be a subgroup of G. Then H contains U if and only if gHg^{-1} contains U. For, if $H \supset U$, $gHg^{-1} \supset gUg^{-1} = U$. Now, $g\hat{U}g^{-1} = \bigcap gHg^{-1}$, where the intersection ranges over all subgroups of G which contains U. Therefore $g\hat{U}g^{-1} = \bigcap gHg^{-1} = \bigcap H = \hat{U}$. $\hat{U}$ is a normal subgroup of G.

5. Let $U = \{xyx^{-1}y^{-1} \mid x, y \in G\}$. In this case $\hat{U}$ is usually written as G' and is called the *commutator subgroup of G.*
   (a) Prove that G' is normal in G.
   (b) Prove that G/G' is abelian.
   (c) If G/N is abelian, prove that $N \supset G'$.

(d) Prove that if H is a subgroup of G and $H \supset G'$, then H is normal in G.

65.5 (a) By (64.4(b)), We need only to show that $g(xyx^{-1}y^{-1})g^{-1} \in \hat{U}$ for all g in G and x, y in G. Since $gxyx^{-1}y^{-1}g^{-1} = [(gx)y(gx)^{-1}y^{-1}][ygy^{-1}g^{-1}] \in \hat{U}$, we are done.

(b) $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \overline{xyx^{-1}y^{-1}} = e$ since $xyx^{-1}y^{-1} \in G'$. Hence $\bar{x}\bar{y} = \bar{y}\bar{x}$.

(c) If G/N is abelian, $\overline{xyx^{-1}y^{-1}} = \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{x}\bar{x}^{-1}\bar{y}\bar{y}^{-1} = e$, $xyx^{-1}y^{-1} \in N$. Therefore $N \supset U$. By (64.4(a)), $N \supset \hat{U} = G'$.

(d) For all g in G and h in H, we have $ghg^{-1} = (ghg^{-1}h^{-1})h \in G' \cdot H \subset H$. Therefore H is a normal subgroup of G.

6. If N, M are normal subgroups of G, prove that $NM/M \approx N/N \cap M$.

65.6 Consider the mapping $\phi : NM \to N/(N \cap M)$ defined by $\phi(nm) = n(N \cap M)$.
First of all, ϕ is well-defind. For, if $nm = n'm'$ for $n, n' \in N$ and $m, m' \in M$. then $n^{-1}n' = mm'^{-1} \in N \cap M$ and $n(N \cap M) = n'(N \cap M)$. Now, we prove that ϕ is a homomorphism of NM onto $N/(N \cap M)$ with kernel M, by Theorem 2.7.1, we have done this excercise. Let $nm \in NM$ and $n'm' \in NM$, $(n')^{-1}mn' \in M$ sinceM is a normal subgroup of G, $(n')^{-1}mn' = m''$, $nmn'm' = nn'm''m'$.
$\phi((nm)(n'm')) = \phi(nn'm''m') = nn'(N \cap M) = (n(N \cap M))(n'(N \cap M)) = \phi(nm)\phi(n'm')$.
ϕ is a homomorphism of NM onto $N/(N \cap M)$.
If nm is in the kernel of ϕ, $n(N \cap M) = N \cap M$, $n \in M$ and $nm \in M$.
Conversely, if $m \in M$, $m = e \cdot m \in NM$, $\phi(m) = \phi(e \cdot m) = e \cdot (N \cap M) = N \cap M$, m is in the kernel of ϕ.
Hence, the kernel of ϕ is M. This completes the proof. (Note: In the proof of this exercise, we need only that M is a normal subgroup of G and N a subgroup of G.)

7. Let V be the set of real numbers, and for a, b real, $a \neq 0$ let $\tau_{ab}: V \to V$ defined by $\tau_{ab}(x) = ax + b$. Let $G = \{\tau_{ab} \mid a, b \text{ real}, a \neq 0\}$ and let $N = \{\tau_{1b} \in G\}$. Prove that N is a normal subgroup of G and that $G/N \approx$ group of nozero real numbers under multiplication.

65.7 By(48.23) N is a normal subgroup of G. Define a mapping $\phi : G \to R\setminus(0)$ by $\phi(\tau_{ab}) = a$.
Since $\phi(\tau_{ab}\tau_{cd}) = \phi(\tau_{(ac)(bc+d)}) = ac = \phi(\tau_{ab}) \cdot \phi(\tau_{cd})$, ϕ is a homomorphism of G onto $R\setminus(0)$.
The kernel of ϕ is N. Therefore, $G/N \approx$ group of nonzero real numbers under multiplication.

8. Let G be the dihedral group defined as the set of all formal symbols x^iy^j, $i = 0, 1$, $j = 0, 1, \ldots, n-1$, where $x^2 = e$, $y^n = e$, $xy = y^{-1}x$. Prove
(a) The subgroup $N = \{e, y, y^2, \ldots, y^{n-1}\}$ is normal in G.
(b) That $G/N \approx W$, where $W = \{1, -1\}$ is the group under the multiplication of the real numbers.

65.8 (a) $(xy^j)y^p(xy^j)^{-1} = xy^jy^py^{-j}x^{-1} = xy^px^{-1} = (xyx^{-1})^p = (y^{-1})^p = y^{-p} \in N$. N is normal in G.

(b) Define a mapping $\phi : G \to \{1, -1\}$ by $\phi(xy^j) = -1$, $\phi(y^j) = 1$. $j = 0, 1, 2, \cdots\cdots, n-1$. Then $\phi(xy^j \cdot xy^i) = \phi(y^{-j}y^i) = \phi(y^{i-j}) = 1 = (-1)(-1) = \phi(xy^j)\phi(xy^i)$, $\phi(xy^j \cdot y^i) = -1 = (-1) \cdot 1 = \phi(xy^j)\phi(y^i)$, $\phi(y^j \cdot xy^i) = \phi(xy^{-j}y^i) = -1 = 1 \cdot (-1) = \phi(y^j)\phi(xy^i)$, $\phi(y^jy^i) = \phi(y^{i+j}) = 1 = 1 \cdot 1 = \phi(y^j)\phi(y^i)$.
ϕ is a homomorphism of G onto $\{1, -1\}$ with kernel N. Therefore, $G/N \approx W$, where $W = \{1, -1\}$ is the group under the multiplication

of the real numbers.

9. Prove that the center of a group is always a normal subgroup.

65.9 If z is in the center of G, for all $g \in G$, $gzg^{-1} = zgg^{-1} = z \cdot e = z$ is itself in the center of G. By definition of the normal subgroup Z is normal in G.

10. Prove that a group of order 9 is abelian.

65.10 If G has an element of order 9, G is cyclic and hence abelian. Suppose now all elements different from e are of order 3. Let $a \in G$ and $b \neq e$, $b \neq a$, $b \neq a^2$, then e, a, a^2, b, b^2, ab, ab^2, a^2b, a^2b^2 are distinct element of G. We want to show that $ba = ab$. then G is abelian. $ba \neq e$, since $b \neq a^2$, $ba \neq a$, $ba \neq a^2$, $ba \neq b$, $ba \neq b^2$. Now if $ba = ab^2$, $e = (ba)^3 = (ba)(ba)(ba) = (ab^2)(ba)(ab^2) = ab^3a^2b^2 = a^3b^2 = b^2$, a contradiction. If $ba = a^2b$, $e = (ba)(ba)(ba) = (a^2b)(ba)(a^2b) = a^2b^2a^3b = a^2b^3 = a^2$, a contradiction. Therefore, $ba = ab$. This completes the proof.

11. If G is a non-abelian group of order 6, prove that $G \approx S_3$.

65.11 If G has an element of order 6, G is cyclic and hence abelian. Hence, G has no element of order 6. The order of element of G is a divisor of 6 and therefore is 1, 2 or 3. G has only e which is of order 1. If all elements other than e are of order 2, then by (35.10) G is abelian, contrary to our assumption that G is nonabelian. Therefore, G has an element, say a, which is of order 3. $H = (a)$ is of index 2 in G. H is a normal subgroup of G by (53.2). For $x \in G/H$, $\bar{x} \in G/H$, $\bar{x}^2 = \bar{e}$, $x^2 \in H$. If $x^2 \neq e$, x^2 is of order 3 and hence x is of order 6, contrary to our assumption. $x^2 = e$. Since H is a normal subgroup of G, $x^{-1}ax \in H$, $x^{-1}ax = a$ or $x^{-1}ax = a^2$. If $x^{-1}ax = a$, then $xa = xa$, then as we proved in (48.25) ax is an element of order 6. This leads to a contradiction. Hence $x^{-1}ax = a^2$. The elements of G can be represented as e, a, a^2, x, ax, a^2x since all of then are distinct. Define a mapping T of G to S_3 as $eT = (1)$, $aT = (123)$, $a^2T = (132)$, $xT = (12)$, $(ax)T = (23)$, $(a^2x)T = (13)$. It's easy to check that T is an isomorphism of G onto S_3. Hence G is isomorphic to S_3.

12. If G is abelian and if N is any subgroup of G, prove that G/N is abelian.

65.12 Let Nx, $Ny \in G/N$. $(Nx)(Ny) = Nxy = Nyx = (Ny)(Nx)$. G/N is abelian.

13. Let G be the dihedral group defined in Problem 8. Find the center of G.

65.13 If $y^i \in Z$, the center of G, $xy^i = y^ix = xy^{-i}$, $y^i = y^{-i}$, $y^{2i} = e$. $n \mid 2i$, $0 \leq i \leq n-1$. $0 \leq 2i \leq 2n-2$. $2i = 0$ or $2i = n$. Hence, if n is even $y^{\frac{n}{2}}$ is the only element of $\{y^i \mid 1 \leq i \leq n-1\}$ which lies in Z. If n is add y^i is not in Z for $1 \leq i \leq n-1$.

If $xy^i \in Z$, then $y^j(xy^i) = (xy^i)y^j$, $xy^{i-j} = xy^{i+j}$, $y^{i-j} = y^{i+j}$ for all $0 \leq j \leq n-1$. $y^{-j} = y^j$ for all $0 \leq j \leq n-1$. In particular, $y^2 = e$ $n = 1$ or 2. Hence, if $n \geq 3$. $xy^i \notin Z$ for all $0 \leq i \leq n-1$. If $n = 1$ or 2, $o(G) = 2$ or 4. $Z = G$.

In summary, we have that (i) $n = 1$, 2, $Z = G$. (ii) n is even and $n \geq 3$, $Z = \{e, y^{\frac{n}{2}}\}$. (iii) n is odd and $n \geq 3$, $Z = (e)$.

14. Let G be as in Problem 13. Find G', the commutator subgroup of G.

65.14 $(y^i)(y^j)(y^{-i})(y^{-j}) = e$

$(xy^i)(y^j)(y^{-i}x)(y^{-j}) = xy^jxy^{-j} = x(xy^{-j})y^j = y^{-2j}$

$(y^i)(xy^j)(y^{-i})(y^{-j}x) = y^ixy^{-i}x = y^i(y^ix)x = y^{2i}$

$(xy^i)(xy^j)(y^{-i}x)(y^{-j}x) = x(y^ix)(y^{j-i}x)(y^{-j}x) = y^{-i}(y^{j-i}x)(xy^j) = y^{2(j-i)}$

$0 \leq i,\ j \leq n-1$. G' contains $y^{\pm 2i}$ for all $0 \leq i \leq n-1$.

Hence $G' = \{e, y^2, \ldots\ldots, y^{n-2}\}$ if n is even and $G' = \{e, y, y^2, \ldots\ldots, y^{n-1}\}$ if n is odd.

15. Let G be the group of nonzero complex numbers under multiplication and let N be the set of complex numbers of absolute value 1 (that is, $a + bi \in N$ if $a^2 + b^2 = 1$). Show that G/N is isomorphic to the group of all positive real numbers under multiplication.

65.15 Define $T: G \longrightarrow R^+$, R^+ is the group of all positive real numbers under multiplication, as $T(a+bi) = a^2+b^2$. Since $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$, $T((a+bi)(c+di)) = (ac-bd)^2+(ad+bc)^2 = (a^2+b^2)(c^2+d^2) = T(a+bi)T(c+di)$, T is a homomorphism of G onto R^+. The kernel of T is N. Hence $G/N \approx R^+$.

#16. Let G be the group of all nonzero complex numbers under multiplication and let $\bar{G}$ be the group of all real 2×2 matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, where not both a and b are 0, under matrix multiplication. Show that G and $\bar{G}$ are isomorphic by exhibiting an isomorphism of G onto $\bar{G}$.

65.16 Let $T: G \longrightarrow \bar{G}$ as $T(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

$(a+bi)(c+di) = (ac-bd)+(ad+bc)i$.

$T((a+bi)(c+di)) = T((ac-bd)+(ad+bc)i)$

$= \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

$= T(a+bi)T(c+di)$. T is a homomorphism of G into G. Clearly T is onto. $a+bi$ in the kernel of T if and only $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, i.e., $a=1$, $b=0$, $a+bi=1$. T is one-to-one. T is an isomorphism of G onto G.

*17. Let G be the group of real numbers under addition and let N be the subgroup of G consisting of all the integers. Prove that G/N is isomorphic to the group of all complex numbers of absolute value 1 under multiplication.

66.17 Define $T: G \longrightarrow \bar{G}$, $\bar{G}$ is the group of all complex numbers of absolute value 1 under multiplication, as $T(x) = e^{i(2\pi x)}$. $T(x+y) = e^{i2\pi(x+y)} = e^{i(2\pi x)} \cdot e^{i(2\pi y)} = T(x) \cdot T(y)$. T is a homomorphism of G into G. T is clearly onto. The kernel of T is N. $G/N \approx \bar{G}$.

#18. Let G be the group of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with $ad - bc \neq 0$, under matrix multiplication, and let

$$N = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid ad - bc = 1 \right\}.$$

Prove that $N \supset G'$, the commutator subgroup of G.

66.18 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\begin{pmatrix} e & f \\ g & h \end{pmatrix}^{-1}$

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}\begin{pmatrix} \frac{h}{eh-gf} & \frac{-g}{eh-gf} \\ \frac{-f}{eh-gf} & \frac{e}{eh-gf} \end{pmatrix}$$

$$= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \cdot$$

$$\begin{pmatrix} \frac{h}{eh-gf} & \frac{-g}{eh-gf} \\ \frac{-f}{eh-gf} & \frac{e}{eh-gf} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{ade+bdg-acf-bch}{ad-bc} & \frac{-abe-b^2g+a^2f+abh}{ad-bc} \\ \frac{ade+d^2g-c^2f-cdh}{ad-bc} & \frac{-bce-bdg+acf+adh}{ad-bc} \end{pmatrix} \cdot$$

$$\begin{pmatrix} \frac{h}{eh-gf} & \frac{-g}{eh-gf} \\ \frac{-f}{eh-gf} & \frac{e}{eh-gf} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{adeh+bdgh-acfh-bch^2+abef+b^2gf-a^2f^2-abhf}{(ad-bc)(eh-gf)} & \\ \frac{cdeh+d^2gh-c^2fh-cdh^2+bcef+bdfg-acf^2-adfh}{(ad-bc)(eh-gf)} & \\ \frac{-adeg-bdg^2+acfg+bcgh-abe^2-b^2eg+a^2ef+abeh}{(ad-bc)(eh-gf)} & \\ \frac{-cdeg-d^2g^2+c^2fg+cdgh-bce^2-bdeg+acef+adeh}{(ad-bc)(eh-gf)} & \end{pmatrix}$$

By a computation, we have $N \supset G'$. In fact, We can get this result by determinant of a matrix.

*#19. In Problem 18 show, in fact, that $N = G'$.

66.19

$$\begin{pmatrix} (x+1)^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x+1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in G' \text{ for } x \neq -1.$$

$$\begin{pmatrix} 1 & 0 \\ 0 & (x+1)^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & x+1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in G' \text{ for } x \neq -1.$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in G'.$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in G'.$$

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in G', \quad \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in G'$$

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in G'.$$

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in G', \quad \begin{pmatrix} 1 & 0 \\ xy & 1 \end{pmatrix} \in G',$$

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ xy & 1 \end{pmatrix} = \begin{pmatrix} x & 0 \\ y & x^{-1} \end{pmatrix} \in G'$$

$$\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 1 & xy \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x^{-1} & y \\ 0 & x \end{pmatrix} \in G'$$

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N$, $ad-bc=1$. If $a \neq 0$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & ba^{-1} \\ 0 & 1 \end{pmatrix}$$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G'$. If $d \neq 0$, then

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d^{-1} & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d^{-1}c & 1 \end{pmatrix} \in G'$. Hence, We may suppose $a = d = 0$ and then $bc = -1$, $b \neq 0$, $c \neq 0$, $b = -c^{-1}$

$\begin{pmatrix} 0 & -c^{-1} \\ c & 0 \end{pmatrix} = \begin{pmatrix} c^{-1} & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in G'$. Therefore, $N \subset G'$, $G' \subset N$. $G' = N$.

#20. Let G be the group of all real 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, where $ad \neq 0$, under matrix multiplication. Show that G' is precisely the set of all matrices of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

66.20 $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}^{-1} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}^{-1}$

$= \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ for some x. Hence $G' \subset \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \}$.

Conversely, by the proof of (66.19), we have shown that

$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in G'$, for all x. $G' = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \}$.

21. Let S_1 and S_2 be two sets. Suppose that there exists a one-to-one mapping ψ of S_1 into S_2. Show that there exists an isomorphism of $A(S_1)$ into $A(S_2)$, where $A(S)$ means the set of all one-to-one mappings of S onto itself.

66.21 Let $T: A(S_1) \longrightarrow A(S_2)$ as $T_g = \psi g \psi^{-1}$. $\psi g \psi^{-1}$ belongs to $A(S_2)$ since ψ, g, ψ^{-1} are one-to-one. $T(gh) = \psi(gh)\psi^{-1}$ $= (\psi g \psi^{-1})(\psi h \psi^{-1}) = (Tg)(Th)$. T is a homomorphism of $A(S_1)$ into $A(S_2)$. If $\psi g \psi^{-1} = 1$, then $g = \psi^{-1} \cdot \psi = 1$. T is an isomorphism of $A(S_1)$ into $A(S_2)$.

2.8 Automorphisms

1. Are the following mappings automorphisms of their respective groups?
   (a) G group of integers under addition, $T{:}x \to -x$.
   (b) G group of positive reals under multiplication, $T{:}x \to x^2$.
   (c) G cyclic group of order 12, $T{:}x \to x^3$.
   (d) G is the group S_3, $T{:}x \to x^{-1}$.

70.1 (a), (b) are automorphisms of their respective groups.

2. Let G be a group, H a subgroup of G, T an automorphism of G. Let $(H)T = \{hT \mid h \in H\}$. Prove $(H)T$ is a subgroup of G.

70.2 Let $h_1T, h_2T \in (H)T$. $(h_1T)(h_2T) = (h_1h_2)T \in (H)T$, $(h_1T)^{-1} = h_1^{-1}T \in (H)T$.
HT is a subgroup of G.

3. Let G be a group, T an automorphism of G, N a normal subgroup of G. Prove that $(N)T$ is a normal subgroup of G.

70.3 NT is a subgroup of G by (70.2). For $g \in G$, there is $r \in G$ such that $g = rT$.
$g(nT)g^{-1} = (rT)(nT)(rT)^{-1} = (rnr^{-1})T \in (N)T$ for all $n \in N$. Hence $(N)T$ is normal in G.

4. For $G = S_3$ prove that $G \approx \mathscr{I}(G)$.

70.4 $Z(G) = (e)$. By lemma 2.8.2, $G \approx \mathscr{I}(G)$.

5. For any group G, prove that $\mathscr{I}(G)$ is a normal subgroup of $\mathscr{A}(G)$ (the group $\mathscr{A}(G)/\mathscr{I}(G)$ is called the *group of outer automorphisms* of G).

70.5 $T \in \mathscr{A}(G)$, $x \in G$. $x(T^{-1}T_gT) = (xT)^{-1}(T_gT)$
$= (g^{-1}(xT)^{-1}g)T = (gT)^{-1}(xT^{-1}T)(gT)$
$= (gT)^{-1}x(gT) = xT_{gT}$.
$T^{-1}T_gT = T_{gT} \in \mathscr{I}(G)$. $\mathscr{I}(G)$ is normal in $\mathscr{A}(G)$.

6. Let G be a group of order 4, $G = \{e, a, b, ab\}$, $a^2 = b^2 = e$, $ab = ba$. Determine $\mathscr{A}(G)$.

70.6 $I_1 : e \to e,\ a \to a,\ b \to b,\ ab \to ab.$
$I_2 : e \to e,\ a \to a,\ b \to ab,\ ab \to b.$
$I_3 : e \to e,\ a \to b,\ b \to ab,\ ab \to a.$
$I_4 : e \to e,\ a \to b,\ b \to a,\ ab \to ab.$
$I_5 : e \to e,\ a \to ab,\ b \to b,\ ab \to a.$
$I_6 : e \to e,\ a \to ab,\ b \to a,\ ab \to b.$

7. (a) A subgroup C of G is said to be a *characteristic subgroup* of G if $(C)T \subset C$ for all automorphisms T of G. Prove a characteristic subgroup of G must be a normal subgroup of G.
   (b) Prove that the converse of (a) is false.

70.7 (a) $g^{-1}cg = cT_g \in C$ for all $g \in G$ and $c \in C$.
C is normal in G.
(b) As in (70.6) $C = \{e, a\}$ is a normal subgroup of G. But $(C)I_3, (C)I_4, (C)I_5, (C)I_6 \not\subset C$.
C is not a characteristic subgroup of G.

8. For any group G, prove that the commutator subgroup G' is a characteristic subgroup of G. (See Problem 5, Section 2.7).

70.8 $xyx^{-1}y^{-1} \in G'$, $(xyx^{-1}y^{-1})T = (xT)(yT)\cdot$
$(xT)^{-1}(yT)^{-1} \in G'$ for any automorphism T of G.
$\{xyx^{-1}y^{-1} \mid x, y \in G\}$ is a set of generators of G', Hence $(G')T \subset G'$.
G' is a characteristic subgroup.

9. If G is a group, N a normal subgroup of G, M a characteristic subgroup of N, prove that M is a normal subgroup of G.

70.9 $g \in G$, $NT_g \subset N$ since N is normal in G. $T_g|_N$, the restriction of T_g on N, is an automorphism of N. Since M is a characteristic subgroup of N, $g^{-1}mg = mT_g = mT_g|_N \in M$.
M is a normal subgroup of G.

10. Let G be a finite group, T an automorphism of G with the property that $xT = x$ for $x \in G$ if and only if $x = e$. Prove that every $g \in G$ can be represented as $g = x^{-1}(xT)$ for some $x \in G$.

70.10 $h,k\in G$, If $h^{-1}(hT)=k^{-1}(kT)$, $(hT)(kT)^{-1}=hk^{-1}$. $(hk^{-1})T=hk^{-1}$, $hk^{-1}=e$ by assumption. $h=k$. The mapping $\sigma: G\longrightarrow\{h^{-1}(hT)\mid h\in G\}$ defind as $h\sigma=h^{-1}(hT)$ is one-to-one. Since G is finite, σ is also an onto mapping. Therefore, for every $g\in G$, there exists $x\in G$ such that $g=x^{-1}(xT)$.

11. Let G be a finite group, T an automorphism of G with the property that $xT = x$ if and only if $x = e$. Suppose further that $T^2 = I$. Prove that G must be abelian.

70.11 By (70.10), for $g\in G$, there exists $x\in G$ such that $g=x^{-1}(xT)$.
$gT=[x^{-1}(xT)]T=((x^{-1})T)(xT^2)=(xT)^{-1}x=(x^{-1}(xT))^{-1}=g^{-1}$. For $a,b\in G$, $(ab)=(ab)T^2=((ab)T)T=((ab)^{-1})T=(b^{-1}a^{-1})T=(b^{-1}T)(a^{-1}T)=(bT)^{-1}(aT)^{-1}=(b^{-1})^{-1}(a^{-1})^{-1}=ba$. G is abelian.

*12. Let G be a finite group and suppose the automorphism T sends more than three-quarters of the elements of G onto their inverses. Prove that $xT = x^{-1}$ for all $x \in G$ and that G is abelian.

71.12 Let $R=\{h\in G\mid hT=h^{-1}\}$. $|R|>3/4\,|G|$ by assumption. For a fixed $h\in R$, we want to show that $C(h)=\{g\in G\mid gh=hg\}$ has more than one-half of the elements of G, then since C(h) is a subgroup of G, $C(h)=G$. Then the center Z of G, $Z=\{g\in G\mid gg'=g'g$ for all g' in $G\}$ contains R and hence has more than three-quarters of the elements of G, $Z=G$. G is abelian.
Now, we have only to prove that C(h) has more than one-half elements for a fixed h in R. If $k\in R$ and $hk\in R$, then $k^{-1}h^{-1}=(hk)T=(hT)(kT)=h^{-1}k^{-1}$, $hk=kh$, $k\in C(h)$. We want to show that $K=\{k\in R\mid hk\in R\}$ has more than one-half elements. $K=R\cap h^{-1}R$. Since $|R|>3/4\,|G|$,

$|h^{-1}R|>3/4\,|G|$, $|K|>1/2|G|$. $|C(h)|\geq|K|>1/2\,|G|$. $C(h)=G$ for all $h\in R$. $Z(G)\supset R$. $|Z(G)|\geq|R|>3/4\,|G|$. $Z(G)=G$, G is abelian.

13. In Problem 12, can you find an example of a finite group which is non-abelian and which has an automorphism which maps exactly three-quarters of the elements of G onto their inverses?

71.13 Example: Let $G=\{\pm1,\pm i,\pm j,\pm k\}$: the quaternion group. Let T be an automorphism of G defined as $1\longrightarrow1$, $-1\longrightarrow-1$, $i\longrightarrow-i$, $-i\longrightarrow i$, $j\longrightarrow-j$, $-j\longrightarrow j$, $k\longrightarrow k$, $-k\longrightarrow-k$. T sends exactly three-quarters of the elements of onto their inverse.
Example 2: $G=D_4=\{x^iy^j\mid x^4=y^2=e,\ yxy^{-1}=x^{-1}\}$ as defined in (54.17). $gT=ygy$ maps $1, x, x^2, x^3, y, x^2y$ onto their inverse, respectively.

*14. Prove that every finite group having more than two elements has a nontrivial automorphism.

71.14 If G is nonabelian, say $ab=ba$ for $a, b\in G$, then T_a is a nontrivial automorphism of G. If G is abelian with an element of order different from 2, $xT=x^{-1}$ is a nontrivial automorphism of G.
Now, suppose that G is an abelian group with every element of order 2 and G has more than two elements. Let $\{a_1,\cdots\cdots a_m\}$ be a minimal set such that $\{a_1,\cdots\cdots,a_n\}$ generates G. Then clearly every element of G can be represented as $a_1^{e_1}a_2^{e_2}\cdots\cdots a_m^{e_m}$ with $e_i=0$ or 1. We claim that every element of G has only a unique representation as above. For if $g=a_1^{e_1}a_2^{e_2}\cdots\cdots a_m^{e_m}=a_1^{e_1'}a_2^{e_2'}\cdots\cdots a_m^{e_m'}$ has these two distinct representations, $a_1\cdots\cdots a_{ik}=e$ for $k\geq2$ and then $a_{i1}=a_{i2}\cdots\cdots a_{ik}$, $\{a_1,a_2,\cdots\cdots,a_m\}\setminus\{a_{i1}\}$ will be also a set which generates G, a contradiction. Now, define a mapping T as $(a_1^{e_1}a_2^{e_2}\cdots\cdots a_m^{e_m})T=a_2^{e_1}a_2^{e_2}\cdots\cdots a_m^{e_m}$. T is a nontrivial automorphism of G. This completes the proof.

*15. Let G be a group of order $2n$. Suppose that half of the elements of G are of order 2, and the other half form a subgroup H of order n. Prove that H is of odd order and is an abelian subgroup of G.

71.15 If H is even, by (35.11) H has an element of order 2, contrary to our assumption.
Let $a \in G/H$. Since H is a subgroup of G, $ah \notin H$ for all $h \in H$. Then $e = (ah)^2 = ahah$, $h^{-1} = aha$ for all h in H. For $h, k \in H$, $(hk)^{-1} = ahka = aha\,aka = h^{-1}k^{-1}$, $hk = (h^{-1}k^{-1})^{-1} = kh$, H is abelian. (Clearly, the key is that $hT_a = h^{-1}$.)

*16. Let $\phi(n)$ be the Euler ϕ-function. If $a > 1$ is an integer, prove that $n \mid \phi(a^n - 1)$.

71.16 By (36.15.(b)), $G = \{[x] \mid (x, a^n - 1) = 1\}$ is a group under nultiplication module $a^n - 1$. $o(G) = \phi(a^n - 1)$. Let $H = \{[x] \mid x = a^r, r \in N\}$. Since $(a^{n-r})(a^r) - (a^n - 1) = a^n - (a^n - 1) = 1$, $(a^r, a^{n-1}) = 1$.
$H \subset G$. H is clearly a subgroup of G with $o(H) = n$. Therefore, by Theorem 2.4.1, $n \mid \phi(a^n - 1)$.

17. Let G be a group and Z the center of G. If T is any automorphism of G, prove that $(Z)T \subset Z$.

71.17 $z \in Z$. For all g in G, there is $g' \in G$ such that $g'T = g$. $(zT)g = (zT)(g'T) = (zg')T = (g'z)T = (g'T)(zT) = g(zT)$. Hence $zT \in Z$.
(Z) $T \subset Z$.

18. Let G be a group and T an automorphism of G. If, for $a \in G$, $N(a) = \{x \in G \mid xa = ax\}$, prove that $N(aT) = (N(a))T$.

71.18 Let $gT \in (N(a))T$ with $g \in N(a)$. Then $(gT)(aT) = (ga)T = (ag)T = (aT)(gT)$, $gT \in N(aT)$. $(N(a))T \subset N(aT)$.
On the other hand, let $g \in N(aT)$. There is $g' \in G$ such that $g'T = g$.

Then $(g'a)T = (g'T)(aT) = g(aT) = (aT)g = (aT)(g'T) = (ag')T$.
Since T is an automorphism of G, $g'a = ag'$, $g' \in N(a)$ and $g = g'T \in ((N(a))T$.

19. Let G be a group and T an automorphism of G. If N is a normal subgroup of G such that $(N)T \subset N$, show how you could use T to define an automorphism of G/N.

71.19 Define $T^* : G/N \to G/N$ as $(g(G/N))T^* = (gT)(G/N)$.
First of all, we must show that T^* is well define. That is, if $g(G/N) = g'(G/N)$, is $gT(G/N) = g'T(G/N)$? Fortunately, since $g^{-1}g' \in N$, $(g^{-1}g')T = (gT)^{-1}g'T \in N$, $gT(G/N) = g'T(G/N)$. T^* is well-defined.
Now $((gG/N))(g(G/N))T^* = ((gg'G/N))T^* = (gg')TG/N = (gT)(g'T)G/N = ((gT)(G/N))((g'T)(G/N)) = (gG/N)T^*(g'G/N)T^*$. T^* is a homomorphism of G/N. T^* is clearly an onto mapping.
Now, consider the kernel of T^*. $g(G/N)$ is in the kernel if and only if $gT \in N = NT$, $g \in N$, i.e. $gG/N = e$.
T^* is an automorphism of G/N.

20. Use the discussion following Lemma 2.8.3 to construct
(a) a non-abelian group of order 55.
(b) a non-abelian group of order 203.

71.20 (a) $\{b^j a^i \mid a^{11} = b^5 = 1,\ b^{-1}ab = a^{-2}\}$.
(b) $\{b^j a^i \mid a^{29} = b^7 = 1,\ b^{-1}ab = a^{-4}.\}$
In both case, b is a symbol which we subject to the required condictions, respectively.

21. Let G be the group of order 9 generated by elements a, b, where $a^3 = b^3 = e$. Find all the automorphisms of G.

71.21 By (65.10), G is abelian. Every element of G is uniquely represented as $a^i b^j$, where $i = 0, 1, 2$ $j = 0, 1, 2$. The automorphism of G can be viewed as automorphism of vector space $\{(i, j) \mid i, j \in J_3\}$. Therefore, $\mathcal{A}(G) \approx GL(2,3)$ as in (36.25.(a)).

2.9. Cayley's Theorem.

1. Let G be a group; consider the mappings of G into itself, λ_g, defined for $g \in G$ by $x\lambda_g = gx$ for all $x \in G$. Prove that λ_g is one-to-one and onto, and that $\lambda_{gh} = \lambda_h \lambda_g$.

74.1 If $x\lambda_g = y\lambda_g$ for x, y in G, then $gx = gy$ and $x = y$, λ_g is one-to-one. For y in G, $(g^{-1}y)\lambda_g = g(g^{-1}y) = y$, λ_g is onto. $x\lambda_{gh} = ghx = g(hx) = g(x\lambda_h) = (x\lambda_h)\lambda_g = x(\lambda_h \lambda_g)$ for all x in G. Hence $\lambda_{gh} = \lambda_h \lambda_g$.

2. Let λ_g be defined as in Problem 1, τ_g as in the proof of Theorem 2.9.1. Prove that for any $g, h \in G$, the mappings λ_g, τ_h satisfy $\lambda_g \tau_h = \tau_h \lambda_g$. (*Hint:* For $x \in G$ consider $x(\lambda_g \tau_h)$ and $x(\tau_h \lambda_g)$.)

74.2 $x(\lambda_g \tau_h) = (x\lambda_g)\tau_h = (gx)\tau_h = gxh = g(xh) = g(x\tau_h) = (x\tau_h)\lambda_g = x(\tau_h \lambda_g)$, for all x in G, Hence $\lambda_g \tau_h = \tau_h \lambda_g$.

3. If θ is a one-to-one mapping of G onto itself such that $\lambda_g \theta = \theta \lambda_g$ for all $g \in G$, prove that $\theta = \tau_h$ for some $h \in G$.

74.3 $e(\lambda_g \theta) = e(\theta \lambda_g)$, $(ge)\theta = (e\theta)\lambda_g$, $g\theta = g(e\theta) = g\tau_{(e\theta)}$ for all g in G. Hence $\theta = \tau_{(e\theta)}$.

4. (a) If H is a subgroup of G show that for every $g \in G$, gHg^{-1} is a subgroup of G.
   (b) Prove that W = intersection of all gHg^{-1} is a normal subgroup of G.

74.4 (a) (47.4.(a)).
(b) (48.18).

5. Using Lemma 2.9.1 prove that a group of order p^2, where p is a prime number, must have a normal subgroup of order p.

75.5 By (46.3), the group G of order p^2 must have a proper subgroup H. $o(H) = p$. Since $p^2 \nmid p!$,

$o(G) \mid i_G(H)!$, by Lemma 2.9.1, H is a normal subgroup of G as H has no subgroup other than (e) and H.

6. Show that in a group G of order p^2 any normal subgroup of order p must lie in the center of G.

75.6 Let $H=\{e, a, a^2, \cdots, a^{p-1}\}$ be a normal subgroup of order p and $b \in G$. $b^{-1}ab \in H$, say $b^{-1}ab=a^r$.
$a=ba^rb^{-1}=b(ba^rb^{-1})^rb^{-1}=b^2a^{r^2}b^{-2}$
$=b^2(ba^rb^{-1})^{r^2}b^{-2}=b^3a^{r^3}b^{-3}=\cdots\cdots=$
$=b^{p^2}a^{rp^2}b^{-p^2}=a^{rp^2}$. $a^{rp^2-1}=e$. Hence
$r^{p^2}=1 \pmod p$. $r^p=r \pmod p$ by (24.14).
$r^{p^2}=(r^p)^p=r^p=r \pmod p$. Hence,
$r=r^{p^2}=1 \pmod p$, $b^{-1}ab=a^r=a$. $ab=ba$.
$a \in Z(G)$ and $H \subset Z(G)$. This completes the proof.

7. Using the result of Problem 6, prove that any group of order p^2 is abelian.

75.7 As in the proof of (75.5), we have show that every subgroup of order p is a normal subgroup of G, where G is a group of order p^2.
$g \in G$. If $o(g)=p^2$, then G is cyclic and abelian. If $o(g)=p$, (g), the subgroup generated by g, is a subgroup of order p and hence by (75.6) lies in Z(G). G is abelian.

8. If p is a prime number, prove that any group G of order $2p$ must have a subgroup of order p, and that this subgroup is normal in G.

75.8 By (46.3), G must have proper subgroup. By Theorem 2.4.1, every proper subgroup of G is of order 2 or p. If every proper subgroup of G is of order 2, then by (35.10) G is abelian. G must have a subgroup of order p by Cauchy's Theorem for Abelian Group on page 61. This is a contradiction. Hence G must have at least a subgroup H of order p. If $p=2$, by (75.5), G has a normal subgroup of order p. If $p>2$, $2p \nmid 2!$, $0(G)\ i_G(H)$. By Lemma 2.9.1, H is a normal subgroup of G.

9. If $o(G)$ is pq where p and q are distinct prime numbers and if G has a normal subgroup of order p and a normal subgroup of order q, prove that G is cyclic.

75.9 Let H be the normal subgroup of order p and K the normal subgroup of order q. Since p and q are distinct prime numbers, $H \cap K=(e)$. By (53,12), $hk=kh$ for any $h \in H$ and $k \in K$. Suppose $H=(h)$, $K=(k)$. As in the proof of (48,25), we have that $o(hk)=pq=o(G)$. G is cyclic.

*10. Let $o(G)$ be pq, $p > q$ are primes, prove
(a) G has a subgroup of order p and a subgroup of order q.
(b) If $q \nmid p-1$, then G is cyclic.
(c) Given two primes p, q, $q \mid p-1$, there exists a non-abelian group of order pq.
(d) Any two non-abelian groups of order pq are isomorphic.

75.10 MaKay, James, H., "Another Proof of Cauchy's Group Theorem," American Mathematical Monthly, Vol 66 (1959), page 119:
Cauchy's Theorem. If the prime p divides the order of a finite group G, then G has kp solutions to the equation $x^p=e$.
pf. Let G have order n and denote the identity by e. The set
$S=\{(a_1, \cdots, a_p) \mid a_i \in G, a_1a_2 \cdots a_p=e\}$
has n^{p-1} members. Define an equivalence relation on S by saying two p-tuples are equivalent if one is a cyclic permutation of the other.
If all components of a p-tuple are equal then its equivalence class contains only one member.
Otherwise, if two components of a p-tuple are distinct, there are p members in the equivalence class.

Let r denote the number of solutions to the equation $x^p = e$. Then r equals the number of equivalence of classes with only one member. Let s denote the number of equivalence classes with p members. Then $r+sp = n^{p-1}$ and $p \mid r$.

(a) By Cauchy Theorem, G has a subgroup H of order p and a subgroup K of order q.

(b) Let $H=(a)$, $K=(b)$. $i_G(H) = q$. $o(G) \nmid q!$. By Lemma 2.9.1, H is a normal subgroup of G. Let $b^{-1}ab = a^r$. $b^{-2}ab^2 = b^{-1}(b^{-1}ab)b = b^{-1}(a^r)b = (b^{-1}ab)^r = (a^r)^r = a^{r^2}$. $b^{-q}ab^q = a^{r^q}$. $a^{r^q-1} = e$. $r^q \equiv 1 \pmod p$ by (49.36). $r^{p-1} \equiv 1 \pmod p$ by (24.14). Since $q \nmid p-1$, $(q, p-1) = 1$. $hq+k(p-1)=1$ for some integers h and k. $r \equiv r^{hq+k(p-1)} \equiv (r^q)^h \cdot (r^{p-1})^k \equiv 1 \pmod p$. $b^{-1}ab = a$. $ab = ba$. By (48.25), $o(ab) = pq$. G is a cyclic group.

(c) $q \mid p-1$ implies $r^q \equiv 1 \pmod p$ for some r. Let H be a cyclic group of order p. $H=(a)$. The mapping $\phi : a^i \longrightarrow a^{ri}$, as can be checked trivially, is an automorphism of H of order q. Hence there is a non-abelian group of order pq as the description on page 69.

(d) Let (a), (b) be subgroups of order q and p in G and (c), (d) be subgroups of order q and p in G'. As in the proof of (b), we have $a^q = b^p = e$, $a^{-1}ba = b^r$, $r^q \equiv 1 \pmod p$. $c^q = d^p = e$, $c^{-1}dc = d^s$, $s^q \equiv 1 \pmod p$. $r, s \not\equiv 1 \pmod p$. Since $\{ x \in J_p \mid x^q \equiv 1 \pmod p \}$ is a cyclic group under multiplication modulo p, $r \equiv s^i$ for some i.

We have the relation $b^k a^j = a^j b^{rk}$, $d^k c^j = c^j d^{sjk}$.

Let $f : G \longrightarrow G'$, $f(a^{j_1}b^{k_1}) = c^{ij_1}d^{k_1}$.

$f(a^{j_2}b^{k_2}) = c^{ij_2}d^{k_2}$.

$f(a^{j_1}b^{k_1})\, f(a^{j_2}b^{k_2}) = c^{i(j_1+j_2)}b^{sj_2k_1+k_2}$

$f((a^{j_1}b^{k_1})(a^{j_2}b^{k_2})) = f(a^{j_1+j_2}b^{rj_2 \cdot k_1+k_2}) = c^{i(j_1+j_2)}b^{rj_2 \cdot k_1+k_2}$

f is a homomorphism. Since $c^{ij_1}d^{k_1} = e$ implies $d^{k_1} = e$, $b^{k_1} = e$, $c^{ij_1} = e$, $a^{j_1} = e$, f is an isomorphism of G onto G'. This completes the proof.

2.10 Permutation Groups

1. Find the orbits and cycles of the following permutations:

(a) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&4&5&1&6&7&9&8\end{pmatrix}$.

(b) $\begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&1&2\end{pmatrix}$.

80.1 (a) orbits : $\{1, 2, 3, 4, 5\}, \{6\}, \{7\}, \{8, 9\}$.
cycles : $(1,2,3,4,5), (6), (7), (89)$.

(b) orbits : $\{1, 2, 5, 6\}, \{3, 4\}$.
cycles : $(1,6,2,5), (3,4)$.

2. Write the permutations in Problem 1 as the product of disjoint cycles.

80.2 (a) $(1, 2, 3, 4, 5)(6)(7)(8,9)$.

(b) $(1,6, 2, 5)(3,4)$

3. Express as the product of disjoint cycles:
(a) $(1, 2, 3)(4, 5)(1, 6, 7, 8, 9)(1, 5)$.
(b) $(1, 2)(1, 2, 3)(1, 2)$.

80.3 (a) $(1, 2, 3, 6, 7, 8, 9, 5, 4)$

(b) $(1, 3, 2)$

4. Prove that $(1, 2, \ldots, n)^{-1} = (n, n-1, n-2, \ldots, 2, 1)$.

80.4 $(1,2, \cdots n)(n, n-1, n-2, \cdots, 2, 1) = (1)(2)\cdots(n) = e$. Hence $(1, 2, \cdots, n)^{-1} = (n, n-1, n-2, \cdots, 2, 1)$.

5. Find the cycle structure of all the powers of $(1, 2, \ldots, 8)$.

80.5 $(1, 2, \cdots, 8)^{1+8k}$

$(1, 2, \cdots, 8)^{2+8k} = (1,3,5,7)(2,4,6,8)$

$(1, 2, \cdots, 8)^{3+8k} = (1,4,7,2,5,8,3,6)$

$(1, 2, \cdots, 8)^{4+8k} = (1,5)(2,6)(3,7)(4,8)$

$(1, 2, \cdots, 8)^{5+8k} = (1,6,3,8,5,2,7,4)$

$(1, 2, \cdots, 8)^{6+8k} = (1,7,5,3)(2,8,6,4)$

$(1,2, \cdots, 8)^{7+8k} = (1,8,7,6,5,4,3,2)$

$(1, 2, \cdots, 8)^{8+8k} = (1)(2)(3)(4)(5)(6)(7)(8)$. $k \in J$.

6. (a) What is the order of an n-cycle?
(b) What is the order of the product of the disjoint cycles of lengths $m_1, m_2, \ldots, m_k$?
(c) How do you find the order of a given permutation?

80.6 (a) The order of an n-cycle is n.

(b) The order of the product of the disjoint cycles of lengths $m_1, \cdots, m_k$ is the least common multiple of $m_1, \cdots, m_k$, i.e., $[m_1, m_2, \cdots, m_k]$. For, (i) disjoint cycles are commutative, (ii) if $ab = ba$, then $\circ(ab) = [\circ(a), \circ(b)]$.

(c) Since every permutation can be uniquely expressed as a product of disjoint cycles, the order of a given permutation is the least comman multiple of lengths of disjoint cycles.

7. Compute $a^{-1}ba$, where
(1) $a = (1, 3, 5)(1, 2)$, $b = (1, 5, 7, 9)$.
(2) $a = (5, 7, 9)$, $b = (1, 2, 3)$.

80.7 (1) $a^{-1}ba = (3, 2, 7, 9)$

(2) $a^{-1}ba = (1, 2, 3)$

8. (a) Given the permutation $x = (1, 2)(3, 4)$, $y = (5, 6)(1, 3)$, find a permutation a such that $a^{-1}xa = y$.
(b) Prove that there is no a such that $a^{-1}(1, 2, 3)a = (1, 3)(5, 7, 8)$.
(c) Prove that there is no permutation a such that $a^{-1}(1, 2)a = (3; 4)(1, 5)$.

80.8 (a) $a = \begin{pmatrix}123456\\561324\end{pmatrix}, \begin{pmatrix}123456\\561342\end{pmatrix}, \begin{pmatrix}123456\\651324\end{pmatrix}, \begin{pmatrix}123456\\651342\end{pmatrix}, \begin{pmatrix}123456\\135624\end{pmatrix}, \begin{pmatrix}123456\\135642\end{pmatrix}, \begin{pmatrix}123456\\136524\end{pmatrix}$
$\begin{pmatrix}123456\\136542\end{pmatrix}, \begin{pmatrix}123456\\315624\end{pmatrix}, \begin{pmatrix}123456\\315642\end{pmatrix}, \begin{pmatrix}123456\\316524\end{pmatrix}$
$\begin{pmatrix}123456\\316542\end{pmatrix}, \begin{pmatrix}123456\\563124\end{pmatrix}, \begin{pmatrix}123456\\563142\end{pmatrix}, \begin{pmatrix}123456\\653124\end{pmatrix}$

or $\begin{pmatrix} 1&2&3&4&5&6 \\ 6&5&3&1&4&2 \end{pmatrix}$.

(b), (c) Let $a=\begin{pmatrix} 1 & 2 & \cdots\cdots & n \\ \theta(1) & \theta(2) & \cdots\cdots & \theta(n) \end{pmatrix}$.

Then $a^{-1}(r_1, r_2, \cdots\cdots, r_k)a=(\theta(r_1), \theta(r_2), \cdots, \theta(r_k))$. Therefore, there is no a such that $a^{-1}(123)a=(13)(5,7,8)$ or $a^{-1}(1,2)a=(3,4)(1,5)$.

9. Determine for what m an m-cycle is an even permutation.

30.9 $(a_1, a_2, \cdots, a_m)=(a_1, a_2)(a_1, a_3)\cdots(a_1, a_m)$, Hence, m is odd if and only if an m-cycle is an even permutation.

10. Determine which of the following are even permutations:
(a) (1, 2, 3)(1, 2).
(b) (1, 2, 3, 4, 5)(1, 2, 3)(4, 5).
(c) (1, 2)(1, 3)(1, 4)(2, 5).

81.10 Only(c) is even permutation.

11. Prove that the smallest subgroup of S_n containing (1, 2) and $(1, 2, \ldots, n)$ is S_n. (In other words, these generate S_n.)

81.11 $(a_1, a_2, \cdots, a_r)=(a_1, a_2)(a_1, a_3)\cdots(a_1, a_r)$. $(a_1, a_i)=(1, a_1)^{-1}(1, a_i)(1, a_1)$. $(1,2)$, $(1,3)$, $\cdots$, $(1,n)$ generate any 2-cycle and hence S_n. $(1,2)^{-1}(2,3)(1,2)=(1,3)$. $(1,2,\cdots,n)^{-1}(1,3)(1,2,\cdots,n)=(2,4)$, $(1,2)^{-1}(2,4)(1,2)=(1,4)$, $\cdots\cdots$. $(1,2,\cdots,n)^{-1}(1,i)(1,2,\cdots,n)=(2, i+1)$, $(1,2)^{-1}(2,i+1)(1,2)=(1,i+1)$. $\cdots\cdots$. Hence $(12), (1,2,\cdots,n)$ generate S_n.

*12. Prove that for $n \geq 3$ the subgroup generated by the 3-cycles is A_n.

8.12 For $n=3$, $A_3=\{(1,2,3), (1,3,2), e\}$. Let

$n \geq 4$. $(a,b)(a,c)=(abc)$, $(a,b)(c,d)=(acd)(cba)$, if a, b, c, d are distiact digits. $\theta \in A_n$. θ can be represented as a product of an even number of transpositions. The product of two distinct transpositions can be generated by 3-cycles as we have shown. This completes the proof.

*13. Prove that if a normal subgroup of A_n contains even a single 3-cycle it must be all of A_n.

81.13 Let H be a normal subgroup of A_n and $(a_1, a_2, a_3) \in H$. If $\{a, b, c\} \cap \{a_1, a_2, a_3\}=\phi$, then

$\theta=\begin{pmatrix} a_1 & a_2 & a_3 & a & b & c \\ a & b & c & a_1 & a_3 & a_2 \end{pmatrix}=(a_1, a)(a_2, b, a_3, c) \in A_n$ and

$\theta^{-1}(a_1, a_2, a_3)\theta=(a, b, c) \in H$.

If $\{b,c\} \cap \{a_1, a_2, a_3\}=\phi$, then

$\theta=\begin{pmatrix} a_1 & a_2 & a_3 & b & c \\ a_1 & b & c & a_2 & a_3 \end{pmatrix}=(a_2 b)(a_3 c) \in A_n$ and

$\theta^{-1}(a_1, a_2, a_3)\theta=(a_1, b, c) \in H$.

If $\{c\} \cap \{a_1, a_2, a_3\}=\phi$,

$\theta=\begin{pmatrix} a_1 & a_2 & a_3 & c \\ c & a_2 & a_1 & a_3 \end{pmatrix}=(a_1 c a_3) \in A_n$, and

$\theta^{-1}(a_1, a_2, a_3)\theta=(c, a_2, a_1) \in H$. The 3-cycle in A_n has only four choices (i) different from (a_1, a_2, a_3) by 3 digits. (ii) different from (a_1, a_2, a_3) by 2 digits. (iii) different from (a_1, a_2, a_3) by 1 digit and (iv) (a_1, a_2, a_3) itself. As we have proved, all 3-cycles are in H. By (81.12), $H=A_n$.

*14. Prove that A_5 has no normal subgroups $N \neq (e), A_5$.

81.14 Let H be a normal subgroup of A_n and $H \neq (e)$. We want to find a 3-cycle in H. Since $H \neq (e)$, H must have some elements different from e. If H contains a 5-cycle, say, $(a_1, a_2, a_3, a_4, a_5)$, then $(a_1, a_2, a_3, a_4, a_5)^2 (a_1, a_2, a_3)^{-1}(a_1, a_2, a_3,$

$a_4, a_5)(a_1, a_2, a_3) = (a_2, a_5, a_3) \in H$. $H = A_5$. If H contains an element of type $(a_1, a_2)(a_3, a_4)$ then $[(a_1, a_2)(a_3, a_4)][(a_2, a_3)(a_4, a_5)]^{-1}$ $(a_1, a_2)(a_3, a_4)[(a_2, a_3)(a_4, a_5)] = (a_1, a_5, a_2, a_3, a_4) \in H$. As we have proved, $H = A_5$. Since every element of A_5 is of type (a_1, a_2, a_3), (a_1, a_2, a_3, a_4) or $(a_1, a_2)(a_3, a_4)$, we have completes the proof。

15. Assuming the result of Problem 14, prove that any subgroup of A_5 has order at most 12.

81.15 Note : Change the problem by " Assuming the relsult of Problem 14, prove that any nontrivial subgroup of A_5 has order at most 12."
Proof. Suppose A_5 has a nontrivial subgroup H with order greater than 12. Then $o(H) = 30$, 20 or 15 by Theorem 2.4.1. If $o(H) = 30$, $i_G(H) = 2$, H must be a normal subgroup of A_5, contrary to (81.14). If $o(H) = 20$, $o(G) \nmid i(H)! = 6$. By Lemma 2.9.1, H contains a nontrivial normal subgroup of G, contrary to (81.14). If $o(H) = 15$, $o(G) \nmid i(H)! = 24$. By Lemma 2.9.1, H contains a nontrivial normal subgroup of G, contrary to (81.14). Therefore any nontrivial subgroup of A_5 has order at most 12.

16. Find all the normal subgroups in S_4.

81.16 (e), A_4 and S_4 are the only normal subgroups of S_4. There are 6 elements of type (a_1, a_2), 3 elements of the type $(a_1, a_2)(a_3, a_4)$, 8 elements of the type (a_1, a_2, a_3), 6 elements of the type (a_1, a_2, a_3, a_4) and the identity. A normal subgroup H of S_4 which contains anelement must contains all elements of the same type. The order of H is a divisor of that of S_4. Hence $o(H) = 1+3+8$, $1+6+3+8+6$, 1 are the only possible. This completes the proof.

*17. If $n \geq 5$ prove that A_n is the only nontrivial normal subgroup in S_n.

81.17 We need only to show that A_n has no normal subgroup $N \neq (e)$, A_n. For, if K is a nontrivial normal subgroup of S_n, then $K \cap A_n$ is a normal subgroup of S_n and hence a normal subgroup of An. By our assumption $K \cap A_n = (e)$ or $K \cap A_n = A_n$.
In the first case, $o(A_n K) = \frac{o(A_n) o(K)}{o(A_n \cap K)} = o(A_n) \cdot o(K)$. $o(A_n K) \mid o(G) = o(A_n) \cdot 2$. Hence $o(K) = 2$ or $o(K) = 1$. $o(K) = 1$ implies $K = (e)$. $o(K) = 2$ implies $k = (a_1 a_1')(a_2 a_2') \cdots (a_r a_r') \in K$. Let $\sigma = (a_1 b_1)(a_1' a_2)$, where b_1 is an element in $\{1, 2, \cdots, n\}$ different from a_1, a_1' and a_2. Then $\sigma^{-1} k \sigma = (b_1 a_2)(a_1' \cdots)(\cdots\cdots) \in K$, $\sigma^{-1} k \sigma \neq k$ implies $o(K) \neq 2$. Therefore $K \cap A_n \neq (e)$
In this case $K \cap A_n = A_n$, $A_n \subset K$.
$i_{S_n}(A_n) = i_{S_n}(K) \cdot i_K(A_n) = 2$ implies $K = A_n$ or $K = S_n$, This provs that if K is a nontrivial normal subgroup of S_n,, then $K = A_n$.
Now, we prove that A_n has no normal subgroup $N \neq (e)$, A_n. This clearly implies (81.14). We will get the same result by another way in (90.10.(e)). Suppose that H is an arbitrary normal subgroup of A_n other than the identity subgroup. Choose an element $\sigma \in H$, with $\sigma \neq e$, such that no element of H other than the identity fixed more symbols than does σ. If we write $\sigma = (ab)(ac) \cdots\cdots (am)$, then there must be at least two transpositions present. Since $\sigma \neq 1$, it moves at least two symbols and we may assume that it moves a and b. We now consider two cases. We may have $\sigma = (ab)(ac) = (acb)$, in which case by (81.13) we conclude that $H =$

A_n. Otherwise we have $\sigma = (ab)(ac)(ad)(ae)\cdots$ (at least four transpositions). It is no loss of generality to assume that no two consecutive transpositions are the same. However, we might have $b = d$, in which case we have $\sigma = (ae)(cb)\cdots$ If $b \neq d$ then $\sigma = (abcd)(ae)\cdots$. If we rename our symbols we see that we may assume that either $\sigma = (abc\cdots)\cdots\cdots$ or $\sigma = (ab)(cd)\cdots$. In the second case b and d may be the same. In any case, if we assume $n \geq 5$, there is a symbol e that is different from a, b, c, and d. Then $\tau = (cde) \in A_n$ and $\tau^{-1} = (ced)$. Therefore, either $\tau^{-1}\sigma\tau^{1} = (abd\cdots)\cdots$ or $\tau^{-1}\sigma\tau^{1} = (ab)(de)\cdots$ is in H. In both cases, $\sigma \neq \tau^{-1}\sigma\tau^{1}$ and so $\sigma^{-1}\tau^{-1}\sigma\tau^{1}$ belongs to H and is not the indentity element of H. However, $\sigma^{-1}\tau\sigma\tau^{-1}$ leaves fixed more symbols than σ does, which contradicts our choice of σ. Therefore, this case is impossible and we must have $H = A_n$. This completes the proof of (81.17).

Cayley's theorem (Theorem 2.9.1) asserts that every group is isomorphic to a subgroup of $A(S)$ for some S. In particular, it says that every finite group can be realized as a group of permutations. Let us call the realization of the group as a group of permutations as given in the proof of Theorem 2.9.1 the *permutation representation* of G.

18. Find the permutation representation of a cyclic group of order n.

81.18 Let $G = \{e, a, a^2, \cdots, a^{n-1}\}$ be the cyclic group of order n. $a^j \tau_{a^i} = a^j \cdot a^i = a^{i+j} = a^k$, $k \equiv i + j \pmod{n}$, $0 \leq k \leq n-1$.

19. Let G be the group $\{e, a, b, ab\}$ of order 4, where $a^2 = b^2 = e$, $ab = ba$. Find the permutation representation of G.

81.19 τ_a : e⟶a, a⟶e, b⟶ab, ab⟶b,
τ_b : e⟶b, a⟶ab, b⟶e, ab⟶a,
τ_{ab}: e⟶ab, a⟶b, b⟶a, ab⟶e,
τ_e : e⟶e, a⟶a, b⟶b, ab⟶ab.

20. Let G be the group S_3. Find the permutation representation of S_3. (*Note:* This gives an isomorphism of S_3 into S_6.)

81.20 $S_3 = \{(1), (12), (13), (23), (123), (132)\}$
$\tau_{(1)}$: (1)⟶(1), (12)⟶(12), (13)⟶(13), (23)⟶(23), (123)⟶(123), (132)⟶(132).
$\tau_{(12)}$: (1)⟶(12), (12)⟶(1), (13)⟶(132), (23)⟶(123), (123)⟶(23), (132)⟶(13)
$\tau_{(13)}$: (1)⟶(13), (12)⟶(123), (13)⟶(1), (23)⟶(132), (123)⟶(12), (132)⟶(23)
$\tau_{(23)}$: (1)⟶(23), (12)⟶(132), (13)⟶(123) (23)⟶(1), (123)⟶(13), (132)⟶(12)
$\tau_{(123)}$: (1)⟶(123), (12)⟶(13), (13)⟶(23), (23)⟶(12), (123)⟶(132), (132)⟶(1)
$\tau_{(132)}$: (1)⟶(132), (12)⟶(23), (13)⟶(12), (23)⟶(13), (123)⟶(1), (132)⟶(123)

21. Let G be the group $\{e, \theta, a, b, c, \theta a, \theta b, \theta c\}$, where $a^2 = b^2 = c^2 = \theta$, $\theta^2 = e$, $ab = \theta ba = c$, $bc = \theta cb = a$, $ca = \theta ac = b$.
(a) Show that θ is in the center Z of G, and that $Z = \{e, \theta\}$.
(b) Find the commutator subgroup of G.
(c) Show that every subgroup of G is normal.
(d) Find the permutation representation of G.
(*Note:* G is often called the group of *quaternion units*; it, and algebraic systems constructed from it, will reappear in the book.)

81.21 (a) $a^2 = \theta$, $a^2\theta = \theta^2 = e$, $(a\theta)\theta = e$, $\theta(a\theta) = e$, $\theta(a\theta) = e = a^2\theta$. Hence, $\theta_a = a\theta$. As the some way, $\theta b = b\theta$ and $\theta c = c\theta$. $\theta(a\theta) = e = (a\theta)\theta$, $\theta(b\theta) = e = (b\theta)\theta$, $\theta(c\theta) = e = (c\theta)\theta$. θ is in the center Z of G. $ab = \theta ba \neq ba$.

It's easy to check that $Z=\{e,\theta\}$.

(b) The commutator subgroup of G is $\{e,\theta\}=Z$.

(c) The subgroups of G are $\{e\}$, $\{e,\theta\}$, $\{e,\theta,a,\theta a\}$, $\{e,\theta,b,\theta b\}$, $\{e,\theta,c,\theta c\}$. Since the index of $\{e,\theta,b,\theta b\}$ in G is 2, $\{e,\theta,b,\theta b\}$ is normal in G. Therefore, every subgroup of G is normal in G.

(d)

	e	θ	a	b	c	θa	θb	θc
	↓	↓	↓	↓	↓	↓	↓	↓
τ_e :	e	θ	a	b	c	θa	θb	θc
τ_θ :	θ	e	θa	θb	θc	a	b	c
τ_a :	a	θa	θ	θc	b	e	c	θb
τ_b :	b	θb	c	θ	θa	θc	e	a
τ_c :	c	θc	θb	a	θ	b	θa	e
$\tau_{\theta a}$:	θa	a	e	c	θb	θ	θc	b
$\tau_{\theta b}$:	θb	b	θc	e	a	c	θ	θa
$\tau_{\theta c}$:	θc	c	b	θa	e	θb	a	θ

22. Let G be the dihedral group of order $2n$ (see Problem 17, Section 2.6). Find the permutation representation of G.

81.22 $(x^iy^j)\tau_{y^k}=(x^iy^j)y^k=x^iy^{j+k}$

$(x^iy^j)\tau_{xy^k}=(x^iy^j)(xy^k)=x^{i+1}y^{k-j}$, $i=0$ or 1

$j,k=0,1,\cdots,n-1$.

Let us call the realization of a group G as a set of permutations given in Problem 1, Section 2.9 the *second permutation representation* of G.

23. Show that if G is an abelian group, then the permutation representation of G coincides with the second permutation representation of G (i.e., in the notation of the previous section, $\lambda_g=\tau_g$ for all $g\in G$.)

81.23 $\forall x\in G.\ x\lambda_g=gx=xg=x\tau_g$. Hence $\lambda_g=\tau_g$.

24. Find the second permutation representation of S_3. Verify directly from the permutations obtained here and in Problem 20 that $\lambda_a\tau_b=\tau_b\lambda_a$ for all $a, b\in S_3$.

81.24 $S_3=\{(1),(12),(13),(23),(123),(132)\}$

$\lambda_{(1)}:(1)\to(1),\ (12)\to(12),\ (13)\to(13),$

$(23)\to(23),\ (123)\to(123),\ (132)\to(132)$.

$\lambda_{(12)}:(1)\to(12),\ (12)\to(1),\ (13)\to(123),$
$(23)\to(132),\ (123)\to(13),\ (132)\to(23)$.

$\lambda_{(13)}:(1)\to(13),\ (12)\to(132),\ (13)\to(1),$
$(23)\to(123),\ (123)\to(23),\ (132)\to(12)$.

$\lambda_{(23)}:(1)\to(23),\ (12)\to(123),\ (13)\to(132),$
$(23)\to(1),\ (123)\to(12),\ (132)\to(13)$.

$\lambda_{(123)}:(1)\to(123),\ (12)\to(23),\ (13)\to(12),$
$(23)\to(13),\ (123)\to(132),\ (132)\to(1)$.

$\lambda_{(132)}:(1)\to(132),\ (12)\to(13),\ (13)\to(23),$
$(23)\to(12),\ (123)\to(1),\ (132)\to(123)$.

To check that $\lambda_a\tau_b=\tau_b\lambda_a$ is a easy work.

25. Find the second permutation representation of the group G defined in Problem 21.

82.25

	e	θ	a	b	c	θa	θb	θc
	↓	↓	↓	↓	↓	↓	↓	↓
λ_e:	e	θ	a	b	c	θa	θb	θc
λ_θ:	θ	e	θa	θb	θc	a	b	c
λ_a:	a	θa	θ	c	θb	e	θc	b
λ_b:	b	θb	θc	θ	a	c	e	θa
λ_c:	c	θc	b	θa	θ	θb	a	e
λ_{θ^a}:	θa	a	e	θc	b	θ	c	θb
λ_{θ^b}:	θb	b	c	e	θa	θc	θ	a
λ_{θ^c}:	θc	c	θb	a	e	b	θa	θ

26. Find the second permutation representation of the dihedral group of order $2n$.

82.26 $(xy^j)\lambda_{x^iy^k}=(x^iy^k)(xy^j)=x^{i+1}y^{j-k}$, $i=0$ or 1,

$j,k=0,1,\cdots,n-1$.

$(y^j)\lambda_{x^iy^k}=(x^iy^k)y^j=x^iy^{k+j}$, $i=0$ or 1,

$j,k=0,1,\cdots,n-1$.

If H is a subgroup of G, let us call the mapping $\{t_g \mid g\in G\}$ defined in the discussion preceding Theorem 2.9.2 the *coset representation* of G by H.

This also realizes G as a group of permutations, but not necessarily isomorphically, merely homomorphically (see Theorem 2.9.2).

27. Let $G = (a)$ be a cyclic group of order 8 and let $H = (a^4)$ be its subgroup of order 2. Find the coset representation of G by H.

82.27 The cosets of H in G are H, Ha, Ha^2, and Ha^3.

$te : H \longrightarrow H,\ Ha \longrightarrow Ha,\ Ha^2 \longrightarrow Ha^2,\ Ha^3 \longrightarrow Ha^3.$

$ta : H \longrightarrow Ha,\ Ha \longrightarrow Ha^2,\ Ha^2 \longrightarrow Ha^3,\ Ha^3 \longrightarrow H.$

$ta^2 : H \longrightarrow Ha^2,\ Ha \longrightarrow Ha^3,\ Ha^2 \longrightarrow H,\ Ha^3 \longrightarrow Ha.$

$ta^3 : H \longrightarrow Ha^3,\ Ha \longrightarrow H,\ Ha^2 \longrightarrow Ha,\ Ha^3 \longrightarrow Ha^2.$

$ta^4 : H \longrightarrow H,\ Ha \longrightarrow Ha,\ Ha^2 \longrightarrow Ha^2,\ Ha^3 \longrightarrow Ha^3.$

$ta^5 : H \longrightarrow Ha,\ Ha \longrightarrow Ha^2,\ Ha^2 \longrightarrow Ha^3,\ Ha^3 \longrightarrow H.$

$ta^6 : H \longrightarrow Ha^2,\ Ha \longrightarrow Ha^3,\ Ha^2 \longrightarrow H,\ Ha^3 \longrightarrow Ha.$

$ta^7 : H \longrightarrow Ha^3,\ Ha \longrightarrow H,\ Ha^2 \longrightarrow Ha,\ Ha^3 \longrightarrow Ha^2.$

28. Let G be the dihedral group of order $2n$ generated by elements a, b such that $a^2 = b^n = e$, $ab = b^{-1}a$. Let $H = \{e, a\}$. Find the coset representation of G by H.

82.28 The cosets of H in G are Hb^i, $0 \leq i \leq n-1$.

$(Hb^j)\, t_{ab^i} = Hb^j ab^i = (Ha)b^{i-j} = Hb^{i-j}.$

$(Hb^j)\, t_{b^i} = (Hb^j)\, b^i = Hb^{i+j},\ 0 \leq i,\ j \leq n-1.$

29. Let G be the group of Problem 21 and let $H = \{e, \theta\}$. Find the coset representation of G by H.

82.29 The cosets of H in G are H, Ha, Hb and Hc.

	t_e	t_θ	t_a	t_b	t_c	$t_{\theta a}$	$t_{\theta b}$	$t_{\theta c}$
$H \longrightarrow$	H	H	Ha	Hb	Hc	Ha	Hb	Hc
$Ha \longrightarrow$	Ha	Ha	H	Hc	Hb	H	Hc	Hb
$Hb \longrightarrow$	Hb	Hb	Hc	H	Ha	Hc	H	Ha
$Hc \longrightarrow$	Hc	Hc	Hb	Ha	H	Hb	Ha	H

30. Let G be S_n, the symmetric group of order n, acting as permutations on the set $\{1, 2, \ldots, n\}$. Let $H = \{\sigma \in G \mid n\sigma = n\}$.
   (a) Prove that H is isomorphic to S_{n-1}.
   (b) Find a set of elements $a_1, \ldots, a_n \in G$ such that $Ha_1, \ldots, Ha_n$ give all the right cosets of H in G.
   (c) Find the coset representation of G by H.

82.30 (a) Define $T: H \longrightarrow S_{n-1}$ as the identity mapping of S_n restricted on H. Clearly, T is an isomorphism of H on S_{n-1}. H is isomorphic to S_{n-1}.

(b) Let $a_i = (n\ i)$ for $1 \leq i \leq n-1$ and $a_n = (1)$. Then $Ha_1, \cdots, Ha_n$ gives all right cosets of H in G. For, $Ha_1, \cdots, Ha_n$ are cosets of H in G and $Ha_i \cap Ha_j = \phi$ if $i \neq j$.

(c) Let $\tau \in S_n$. $(Ha_i)\, t_\tau = Ha_j$ if $\tau : i \longrightarrow j$.

2.11 Another Counting Principle.

1. List all the conjugate classes in S_3, find the c_a's, and verify the class equation.

90.1 $\{(1)\},\{(12),(13),(23)\},\{(123),(132)\}$.
$6=1+3+2$.

2. List all the conjugate classes in S_4, find the c_a's and verify the class equation.

90.2 $\{(1)\}$, $\{(12),(13),(14),(23),(24),(34)\},\{(123),(132),(124),(142),(134),(143),(234),(243)\}$, $\{(1234),(1324),(1243),(1342),(1423),(1432)\}$, $\{(12)(34),(13)(24),(14)(23)\}$. $24=1+6+8+6+3$

3. List all the conjugate classes in the group of quaternion units (see Problem 21, Section 2.10), find the c_a's and verify the class equation.

90.3 $\{e\}$, $\{\theta\}$, $\{a, \theta a\}$, $\{b,\theta b\},\{c,\theta c\}$.
$8=1+1+2+2+2$.

4. List all the conjugate classes in the dihedral group of order $2n$, find the c_a's and verify the class equation. Notice how the answer depends on the parity of n.

90.4 Dihidral group of order $2n$ has been defined in (65.8). Since $y^i x = xy^{-i}$, the conjugates of xy^i are $(xy^{i'})^{-1}(xy^i)(xy^{i'}) = xy^{-i+2i'}$ and $(y^{i'})^{-1}(xy^i)(y^{i'}) = xy^{i+2i'}$ for $i'=0,1,2,\cdots,n-1$. The conjugates of y^i are $(xy^{i'})^{-1}y^i(xy^{i'}) = y^{-i}$ and $(y^{i'})^{-1}y^i(y^{i'}) = y^i$.

$C_{xyi} = \{xyi' \mid i'=0,1,2,\cdots,n-1\}$.

$C_{yi} = \{y^i, y^{-i}\}$. $i=0,1,2,\cdots,n-1$.

When n is odd, $2n = n+\underbrace{2+2+\cdots+2}_{\frac{n-1}{2}}+\underbrace{1}_{\{e\}}$.

When n is even, $2n = n+\underbrace{2+2+\cdots+2}_{\frac{n-2}{2}}+\underbrace{1}_{\{e\}}+\underbrace{1}_{\{y^{\frac{n}{2}}\}}$.

5. (a) In S_n prove that there are $\frac{1}{r}\frac{n!}{(n-r)!}$ distinct r cycles.

(b) Using this, find the number of conjugates that the r-cycle $(1, 2, \ldots, r)$ has in S_n.

(c) Prove that any element σ in S_n which commutes with $(1, 2, \ldots, r)$ is of the form $\sigma = (1, 2, \ldots, r)^i\tau$, where $i = 0, 1, 2, \ldots, r$, τ is a permutation leaving all of $1, 2, \ldots, r$ fixed.

90.5(a) The number of distinct r cycle is

$$\frac{P(n,r)}{r} = \frac{1}{r}\frac{n!}{(n-r)!}$$

(b) The number of conjugates of $(1, 2, \cdots, r)$ is equal to the number of distinct r cycles in S_n, i.e., $\frac{1}{r}\frac{n!}{(n-r)!}$

(c) $o(N((1,2,\cdots,r))) = (n!)/\left[\frac{n!}{r(n-r)!}\right]$
$= r(n-r)!$. Every element of the form $(1,2,\cdots,r)^i\tau$, where τ is a permutation leaving all of $1, 2, \cdots, r$ fixed, commutes with $(1, 2, \cdots, r)$. The number of elements of the form $(1, 2, \cdots, r)^i\tau$ is $r\cdot(n-r)!$. Therefore, $N((1,2,\cdots,r)) = \{(1,2,\cdots,r)^i\tau \mid \tau$: a permutation leaving all $1,2,\cdots,r$ fixed$\}$.

6. (a) Find the number of conjugates of $(1, 2)(3, 4)$ in S_n, $n \geq 4$.
(b) Find the form of all elements commuting with $(1, 2)(3, 4)$ in S_n.

90.6 (a) $\frac{n!}{(n-4)!8} = \frac{n(n-1)(n-2)(n-3)}{8}$

(b) Let $S=\{e, (1,2), (3,4), (12)(34), (13)(24), (14,23), (1324), (1423)\}$
Every element in S can commute with $(12)(34)$.

$a \in S$, $a\tau$ commutes with $(12)(34)$, where τ is a permutation leaving all 1, 2, 3, 4 fixed. The number of elements of the form $a\tau$ is $8(n-4)! = 0(N((12)(34)))$. Therefore, $N((12)(34)) = \{a\tau \mid a \in S$ and τ is a permutation leaving all 1, 2, 3, 4 fixed$\}$.

7. If p is a prime number, show that in S_p there are $(p-1)! + 1$ elements x satisfying $x^p = e$.

90.7 By (80.6.(b)), $x^p = e$ implies $x = e$ or x is p cycle. There are

$\frac{p!}{p} = (p-1)!$ p cycles by (90.5.(a)). Therefore, there are $(p-1)! + 1$ elements in S_p such that $x^p = e$.

8. If in a finite group G an element a has exactly two conjugates, prove that G has a normal subgroup $N \neq (e), G$.

90.8 $i_G(N(a)) = 2$ by Theorem 2.11.1. By (53.2), $N(a)$ is a normal subgroup of G. $a \in N(a)$, $a \neq e$, $N(a) \neq (e)$. $i_G(N(a)) = 2$, $N(a) \neq G$. Let $N = N(a)$. N is the required normal subgroup.

9. (a) Find two elements in A_5, the alternating group of degree 5, which are conjugate in S_5 but not in A_5.
   (b) Find all the conjugate classes in A_5 and the number of elements in each conjugate class.

90.9 We claim first that: Let G be a finite group with subgroup H of index 2. If $x \in H$ has m conjugates in G, then x has either m or m/2 conjugates in H.

pf. $[G : H] = 2$, by (53.2), H is a normal subgroup of G. $[G : N_G(x)] = m$. $N_H(x) = N_G(x) \cap H$. By (65.6), $H/N_G(x) \cap H \approx HN_G(x)/N_G(x)$. $H \subseteq H N_G(x)$. $[G : H] = 2$ implies $HN_G(x) = G$ or $HN_G(x) = H$.

(i) $H N_G(x) = G$ implies $[H : N_H(x)] = [H : N_G(x) \cap H] = [H N_G(x) : N_G(x)] = [G : N_G(x)] = m$.

(ii) $H N_G(x) = H$ implies $N_G(x) \subset H$. $[H : N_H(x)] = [H : N_G(x) \cap H] = [H N_G(x) : N_G(x)] = [H : N_G(x)]$. $[G : N_G(x)] = [G : H][H : N_G(x)] = [G : H][H : N_H(x)]$. Hence $m = 2[H : N_H(x)]$, $[H : N_H(x)] = m/2$. This completes the proof of our claim.

Now, we are doing our exercise.

(i) There are two conjugacy classes of 5 cycles in A_5, each of which has 12 elements.

In S_5, $\alpha = (12345)$ has 24 conjugates, so that $N_{S_5}(\alpha)$ has 5 elements, and they must be the powers of α. Therefore, $|N_{A_5}(\alpha)| = 5$, and so the number of conjugates in A_5 is $60/5 = 12$.

In this case, we also show that there are two elements in A_5, which are conjugate in S_5 but not in A_5.

(ii) All products of disjoint transpositions are conjugate in A_5.

If, for example, $\alpha = (12)(34)$, then α has 15 conjugates in S_5. By our claim, α has either 15 or 15/2 conjugates in A_5, and the latter is clearly impossible.

(iii) All 3 cycles are conjugate in A_5,

In S_5 a 3 cycles α has 20 conjugates. Hence $C_{S_5}(\alpha)$ has index 20 and order 6. We can exhibit these 6 elements that commute with α. If, for example, $\alpha = (123)$, then the elements of $N_{S_5}(\alpha)$ are (1), (123), (132), (132), (45), (123)·(45), (132)(45). Now, only the first three of these are even, so that $C_{A_5}(\alpha)$ has order 3 and hence index 20 in A_5. Therefore, α has 20 conjugates in A_5, so that all 3 cycles are conjugate in A_5.

$o(A_5) = 60 = 1 + 12 + 12 + 15 + 20$.

In fact, all these conjugacy classes can be found by

actually computing.
{(1)}, {(12345), (12453), (12534), (13542), (13425), (13254), (14235), (14352), (14523), (15243), (15432), (15324)}, {(12354), (12435), (12543), (13524), (13452), (13245), (14253), (14325), (14532), (15234), (15423), (15342)}, {(12)(34), (12)(35), (12)(45), (13)(24), (13)(25), (13)(45), (14)(23), (14)(25), (14)(35), (15)(23) (15)(24), (15)(34), (23)(45), (24)(35), (25)(34)}, {(123), (132), (124), (142), (125), (152), (134), (143), (135), (153), (145), (154), (234), (243), (235), (253), (245), (254), (345), (354)}.

10. (a) If N is a normal subgroup of G and $a \in N$, show that every conjugate of a in G is also in N.
(b) Prove that $o(N) = \sum c_a$ for some choices of a in N.
(c) Using this and the result for Problem 9(b), prove that in A_5 there is no normal subgroup N other than (e) and A_5.

90.10 (a) The conjugate of a is of the form $b^{-1}ab$. Since N is normal, $b^{-1}ab \in N$. Therefore, every conjugate of a is in N.

(b) The conjugancy classes of G in N is a partition of N. Hence $0(N) = \sum Ca$. for suitable choices of a in N.

(c) $60 = 1+12+12+15+20$. If H is a normal subgroup of $A_5 \neq \{e\}$, then H is a union of conjugacy classes of A_5. The order of H is thus a sum of certain of the numbers 1, 20, 15, 12, 12. Since H contains $\{e\}$, it easily to checked that one never gets a proper divisor of 60. Therefore, $o(H) = 60$ and $H = A_5$. A_5 has no normal subgroup other than (e) and A_5.

11. Using Theorem 2.11.2 as a tool, prove that if $o(G) = p^n$, p a prime number, then G has a subgroup of order p^α for all $0 \leq \alpha \leq n$.

91.11 By theorem 2.11.2, $Z(G) \neq (e)$, $o(Z(G)) = p^k$, $k \neq 0$. By Theorem 2.11.3, Z(G) has a subgroup H of order P. By (70.7.(a)), H is a normal subgroup of G. $o(G/H) = P^{n-1}$.

Use induction on n. n=1 is a trivial case. By induction hypothese, G/H has subgroup of order p^i, $0 \leq i \leq n-1$. By lemma 2.7.5, G has subgroup of order p^{i+1}, $0 \leq i \leq n-1$. Therefore G has a subgroup of order p^α for all $0 \leq \alpha \leq n$.

12. If $o(G) = p^n$, p a prime number, prove that there exist subgroups N_i, $i = 0, 1, \ldots, r$ (for some r) such that $G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_r = (e)$ where N_i is a normal subgroup of N_{i-1} and where N_{i-1}/N_i is abelian.

91.12 n=1 is a trivial case. $o(G) = P^n$, G has a normal subgroup H of order P as we have shown in (91.11). $o(G/H) = P^{n-1} < o(G)$, By induction hypothesis, G/H has subgroups N_i', $i = 0, 1, \cdots, r'$ such that $G/H = N_0' \supset N_1' \supset \cdots\cdots \supset N'_{r'} = (\bar{e}) = H$ as desired. Let N_i be the inverse image of N_i', then $G = N_0 \supset N_1 \supset \cdots\cdots \supset N_r = H \supset (e)$, N_i is a normal subgroup of N_{i-1} and where $N_{i-1}/N_i \approx (N_{i-1}/H)/(N_i/H)$ is abelian.

13. If $o(G) = p^n$, p a prime number, and $H \neq G$ is a subgroup of G, show that there exists an $x \in G$, $x \notin H$ such that $x^{-1}Hx = H$.

91.13 n=1 is a trivial case. G has a normal subgroup K of order P, as we have shown in (91.11), which lies in the center of G. If $K \not\subseteq H$, then $x^{-1}Hx = H$ for $e \neq x \in K$ since K lies in the center of G. We may suppose $K \subseteq H$. H/K is a subgroup of G/K. By induction lypothecis, there is an element $Kx \notin H/K$ in G/K such that $(Kx)^{-1}(H/K)(Kx) = H/K$.

Since $Kx \notin H/K$, $x \notin H$. By $(Kx^{-1})(H/K)(Kx)$

$=H/K$, for all $h\in H$, $Kh\in H/K$, $(Kx^{-1})(Kh)(Kx)=Kh'$ for some $h'\in H$. $K(x^{-1}hx)=Kh'$, $x^{-1}hxh'^{-1}\in K\subset H$, $x^{-1}hx\in H$. $x^{-1}Hx\subset H$. $o(x^{-1}Hx)=o(H)$ implies that $x^{-1}Hx=H$ with $x\notin H$.

14. Prove that any subgroup of order p^{n-1} in a group G of order p^n, p a prime number, is normal in G.

91.14 Let H be a normal subgroup of G with order p^{n-1}. $N(H)=\{x\in G \mid x^{-1}Hx=H\}\supset H$. By (91.13), there is $x\notin H$ such that $x\in N(H)$. Therefore $G\supset N(H)\supset H$, $o(N(H))=o(G)$. $N(H)=G$. H is a normal subgroup of G.

*15. If $o(G)=p^n$, p a prime number, and if $N\neq(e)$ is a normal subgroup of G, prove that $N\cap Z\neq(e)$, where Z is the center of G.

91.15 By (90.10.(b)), $o(N)=\sum Ca$ for some choices of a in N. If $N\cap Z=(e)$, $o(N)=1+\sum_{a\neq e} Ca$, Ca is a power of P, a contradiction. Therefore $N\cap Z\neq(e)$.

16. If G is a group, Z its center, and if G/Z is cyclic, prove that G must be abelian.

91.16 If G/Z is cyclic, then $G/Z=\{Z, Za, Za^2, \ldots\}$ for some a in G.

Now, every element in G is of the form $z a^i$ for some integer i and z in the center Z of G. Let $z_1a^r, z_2a^s\in Z$. $(z_1a^r)(z_2a^s)=(z_1z_2)a^{r+s}=(z_2z_1)(a^sa^r)=(z_2a^s)(z_1a^r)$. G is abelian.

17. Prove that any group of order 15 is cyclic.

91.17 Proof 1. By (75.10.(b)), G is cyclic.

Proof 2. If the center Z of G is not indentity, then $o(Z)=o(G)$, $o(Z)=5$ or $o(Z)=3$.

(i) $o(Z)=o(G)$, G is abelian. By Cauchy Theorem, there are element a and b in G such that $o(a)=3$, $o(b)=5$, By (48.25), $o(ab)=15$, G is cyclic.

(ii) $o(Z)=3$ or $o(Z)=5$, G/Z is cyclic group of prime order. By (91.16), G is cyclic, a contradiction.

Now, suppose $o(Z)=1$. For $e\neq a\in G$, $o(a)=3$ or $o(a)=5$ and $o(N(a))=3$ or $o(N(a))=5$, otherwise a will be a nonidentity element in the center of G. By the Corollary of Theorem 2.11.1 $15=o(G)=1+3\cdot r+5\cdot s$ for some nonnegative integers r and s, this is impossible. Therefore $o(Z)\neq 1$ and G is cyclic.

18. Prove that a group of order 28 has a normal subgroup of order 7.

91.18 $28=7\times 4$. By Cauchy Theorem G has a subgroup H of order 7. $28\nmid 4!$, by Lemma 2.9.1, H has a nontrivial subgroup which is normal in G. Therefore, H is itself normal in G.

19. Prove that if a group G of order 28 has a normal subgroup of order 4, then G is abelian.

91.19 By (91.18), G has a normal subgroup H of order 7. Let K be a normal subgroup of order 4. By (53, 3), HK is a subgroup of G. Since $(o(H), o(K))=1$ $H\cap K=(e)$, By (53.12), for all $h\in H$, $k\in K$, $hk=kh$. Now if $h_1k_1=h_2k_2$ for $h_1, h_2\in H$ and $k_1, k_2\in K$, then $h_2^{-1}h_1=k_2k_1^{-1}\in H\cap K$, $h_1=h_2$, $k_1=k_2$. Therefore $o(HK)\geq 7\times 4=28=o(G)$, $o(HK)=o(G)$, $HK=G$. G is abelian.

2.12. Sylow's Theorem

1. Adapt the second proof given of Sylow's theorem to prove directly that if p is a prime and $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.

101.1 The second proof of Sylow's Theorem is right when we use induction on the order of the group G, that for every $P^n \mid o(G)$, G has a subgroup of order P^n.

2. If $x > 0$ is a real number, define $[x]$ to be m, where m is that integer such that $m \leq x < m + 1$. If p is a prime, show that the power of p which exactly divides $n!$ is given by

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^r}\right] + \cdots.$$

102.2 If $p^i > n$, then $\left[\frac{n}{p^i}\right] = 0$. Therefore the sum terminates; it is not really an infinite series. This exercise is easily proved by mathematical induction. It is true for 1! Assume it is true for $(n-1)!$ and let j denote the largest integer such that $p^j \mid n$. Since $n! = n \cdot (n-1)!$, we must prove that $\sum \left[\frac{n}{p^i}\right] - \sum \left[\frac{n-1}{p^i}\right] = j$. But

$$\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right] = \begin{cases} 1 & \text{if } p^i \mid n \\ 0 & \text{if } p^i \nmid n \end{cases}$$

and hence $\sum \left[\frac{n}{p^i}\right] - \sum \left[\frac{n-1}{p^i}\right] = j$

3. Use the method for constructing the p-Sylow subgroup of S_{p^k} to find generators for
(a) a 2-Sylow subgroup in S_8. (b) a 3-Sylow subgroup in S_9.

102.3 (a) By the discussion following Lemma 2,12,2, we know that $\{(13)(24), (12), (34)\}$ generates a 2-Sylow subgroup of S_4. Let $\sigma = (15)(26)(37)(48)$ and $P_1 = \{e, (12), (34), (1234), (1324), (1423), (14)(23), (13)(24)\}$. P_1 is generated by $\{(13)(24), (12), (34)\}$. Let $P_2 = \sigma^{-1} P_1 \sigma$. P_2 is generated by $\{(57)(68), (56), (78)\}$. Our 2-Sylow subgroup is then the group generated by $\sigma = (15)(26)(37)(48)$ and $T = P_1 P_2$. Theerefore, $\{(15)(26)(37)(48), (13)(24), (12)\}$ generates a 2-Sylow subgroup of S_8.

(b) $((123))$ is the 3-Sylow subgroup of S_3. Let $\sigma = (147)(258)(369)$. a 3-Sylow subgroup of S_9 is generated by σ and $T = ((123)(\sigma^{-1}((123))\sigma)(\sigma^{-2}((123))\sigma^2)$. Hence $\{(123), (147)(258)(369)\}$ generates a 3-Sylow subgroup of S_9.

4. Adopt the method used in Problem 3 to find generators for
(a) a 2-Sylow subgroup of S_6. (b) a 3-Sylow subgroup of S_6.

102.4 (a) The order of a 2-Sylow subgroup of S_6 is 2^4. Since $\{(12), (34), (56), (13)(24)\}$ generates a group of order 2^4 it really generates a 2-Sylow subgroup of S_6.

(b) The order of a 3-Sylow subgroup of S_6 is 3^2. Since $\{(123), (456)\}$ generates a group of order 3^2 it really generates a 3-Sylow subgroup of S_6.

5. If p is a prime number, give explicit generators for a p-Sylow subgroup of S_{p^2}.

102.5 $((12 \cdots\cdots p))$ is a p-Sylow subgroup of S_p. Let $\sigma = (1, p+1, 2p+1, \cdots, (p-1)(p+1)(2, p+2, \cdots, (p-1)p+2) \cdots (p, 2p, \cdots, p^2)$. By the discussion following Lemma 2.12.2, We have that σ and $(1, 2, \cdots p)$ generates a p-Sylow subgroup of S_{p^2}.

6. Discuss the number and nature of the 3-Sylow subgroups and 5-Sylow subgroups of a group of order $3^2 \cdot 5^2$.

102.6 The number of the 3-Sylow subgroups is $3k+1$ for some nonnegative integer k. $(3k+1)\mid 3^2\cdot 5^2$ implies $(3k+1)\mid 5^2$. $k=0$ or 8. Hence a group of order $3^2\cdot 5^2$ has 1 or 25 3-Sylow subgroups. In the first case the 3-Sylow subgroup is a normal subgroup. The number of the 5-Sylow subgroup is $5m+1$ for some nonnegative integer m. $(5m+1)\mid 3^2\cdot 5^2$ implies $m=0$. Hence a group of order $3^2\cdot 5^2$ has only one 5-Sylow subgroup and the 5-Sylow subgroup is a normal subgroup.

7. Let G be a group of order 30.
   (a) Show that a 3-Sylow subgroup or a 5-Sylow subgroup of G must be normal in G.
   (b) From part (a) show that every 3-Sylow subgroup and every 5-Sylow subgroup of G must be normal in G.
   (c) Show that G has a normal subgroup of order 15.
   (d) From part (c) classify all groups of order 30.
   (e) How many different nonisomorphic groups of order 30 are there?

102.7 (a) Suppose no 3-Sylow subgroup and 5-Sylow subgroup is normal in G. By Theorem 2.123, G has 10 3-Sylow subgroups and 6 5-sylow subgroups. There are $(3-1)\times 10=20$ elements of order 3 and $(5-1)\times 6=24$ elements of order 5. $20+24=44>30$, contrary to $o(G)=30$.

(b) By (a), G has a normal 5-Sylow subgroup or a normal 3-Sylow subgroup. In any case, by (53.3) G has a subgroup K of order 15. $i_G(K)=2$ implies K is normal in G. By (75.10.(b)) or (102.11.(a)) K is cyclic. The 5-Sylow subgroup and 3-Sylow subgroup of K are characteristic subgroup of K since K is cyclic. By (70.7.(a)) 5-Sylow subgroup and 3-Sylow subgroup of K are normal in G. Since $o(G)=5\times 3\times 2$, the 5-Sylow subgroup and 3-Sylow subgroup of K are actually normal 5-Sylow subgroup and 3-Sylow subgroup of G. By Theorem 2.12.2, 5-Sylow subgroup and 3-Sylow subgroup of G are unique. Hence every 5-Sylow subgroup and 3-Sylow subgroup are normal in G.

(c) In the proof of (b) we have show that G has a normal subgroup of order 15.

(d) A group of order 15 is cyclic by (75.10.(b)) or (102.11.(a)). Let $H=((a))$ be the normal subgroup of order 15 in G. Let g be an element of order 2. Then $g^{-1}ag=a^i$ for $1\leq i\leq 14$. $a=g^{-2}ag^2=g^{-1}(g^{-1}ag)g=g^{-1}a^ig=(g^{-1}ag)^i=a^{i^2}$. $i^2\equiv 1 \pmod{15}$. $i=1, 4, 11$ or 14. By the discussion following Lemma 2.8.3, there are groups of order 30 as $\{a^ig^j \mid 0\leq i\leq 14,\ 0\leq j\leq 1,\ a^{15}=e,\ g^2=e,\ g^{-1}ag=a^k\}$, $k=1, 4, 11$ or 14.

(e) There are at most 4 nonisomorphic groups of order 30, say $G_1=\{a_1^ig_1^j \mid i=0,1,\cdots,14,\ j=0,1,\ a_1^{15}=g_1^2=e,\ g_1^{-1}a_1g_1=a_1^4\}$, $G_2=\{a_2^ig_2^j\ i=0,1,\cdots,14,\ j=0,1,\ a_2^{15}=g_2^2=e,\ g_2^{-1}a_2g_2=a_2^{11}\}$, $G_3=\{a_3^ig_3^j \mid i=0,1,\cdots,14,\ j=0,1,\ a_3^{15}=g_3^2=e,\ g_3^{-1}a_3g_3=a_3^{14}\}$. G_4 is the unique abelian group of order 30. $Z(G_4)=G_4$. $Z(G_1)=(a_1^5)$, $Z(G_2)=(a_2^3)$, $Z(G_3)=(e)$. Hence G_1, G_2, G_3 and G_4 are not isomorphic. There are 4 nonisomorphic groups of order 30.

8. If G is a group of order 231, prove that the 11-Sylow subgroup is in the center of G.

102.8 $231=3\cdot 7\cdot 11$. By Theorem 2.12.3, G has $1+11k$ 11-Sylow subgroups for some nonnegative integer k. $1+11k\mid 231$, $1+11k\mid 21$, $k=0$. The 11-Sylow subgroup H is normal in G. Let $H=(a)$ and K_1 be a 3-Sylow subgroup, K_2 be a 7-Sylow subgroup. HK_1, HK_2 are subgroup of G. $o(HK_1)=33$, $o(HK_2)$

=77. By (75.10.(b)) or (102.11.(a)), HK_1 and HK_2 are cyclic group. $H \subset N(a)$. $K_1 \subset N(a)$. $K_2 \subset N(a)$. $11 \mid o(N(a))$, $3 \mid o(N(a))$, $7 \mid o(N(a))$. $231 \mid o(N(a))$. $o(N(a)) = o(G)$. $N(a) = G$. a lies in the center of G. H lies in the center of G.

9. If G is a group of order 385 show that its 11-Sylow subgroup is normal and its 7-Sylow subgroup is in the center of G.

102.9 $385 = 5 \cdot 7 \cdot 11$. There are $11k+1$ 11-sylow subgroups in G. $11k+1 \mid 385$, $11k+1 \mid 5 \cdot 7$. $k=0$. The 11-Sylow subgroup H of G is normal in G. There are $7m+1$ 7-Sylow subgroups in G. $7m+1 \mid 385$, $7m+1 \mid 5 \cdot 11$. $m=0$. The 7-Sylow subgroup K of G is normal. HK is a subgroup of G. By(75.10.(b)) or (102.11.(a)), HK is cyclic. Let S be a 5-Sylow subgroup of G. SK is a subgroup of G with order 35. By(75.10.(b)) or (102.11.(a)), SK is cyclic. Suppose $K=(a)$. $K \subset N(a)$. $H \subset N(a)$. $S \subset N(a)$. $5 \cdot 7 \cdot 11 \mid o(N(a))$. $o(G) = o(N(a))$. $G = N(a)$. a lies in the center of G. This completes the proof.

10. If G is of order 108 show that G has a normal subgroup of order 3^k, where $k \geq 2$.

102.10 $108 = 2^2 \cdot 3^3$, Let H be a 3-sylow subgroup of G. $o(H) = 3^3$. $i_G(H) = 4$. $108 \mid 4!$. By Lemma 2.9.1, H must contain a nontrivial normal subgroup K of G. $o(K) = 9$ or $o(K) = 27$ is our required case. Hence we may suppose that $o(K) = 3$. $o(G/K) = 2^2 \cdot 3^2$. $o(H/K) = 3^2$. $i_{G/H}(H/K) = 4$. $2^2 \cdot 3^2 \mid 4!$. By Lemma 2.9.1, H/K must contain a nontrivial normal subgroup of G/K. By lemma 2.7.5, H contains a normal subgroup of G with order 3^2 or 3^3. This completes the proof.

11. If $o(G) = pq$, p and q distinct primes, $p < q$, show
(a) if $p \nmid (q-1)$, then G is cyclic.

*(b) if $p \mid (q-1)$, then there exists a unique non-abelian group of order pq.

102.11 (a) There are $kq+1$ q-Sylow subgroups of G. $kq+1 \mid pq$, $kq+1 \mid p$, $p < q$ implies $k=0$ and the q-Sylow subgroup H is normal in G. Let $H=(a)$. There are $mp+1$ p-Sylow subgroups of G. $mp+1 \mid pq$, $mp+1 \mid q$. $q = s(mp+1)$ for some positive integer s. $s \mid q$. $s=1$ or $s=q$. $s=1$ implies $q = mp+1$ which leads to a contradiction with $p \nmid q-1$. Therefore $s=q$ and $mp+1=1$. The p-Sylow subgroup K is normal in G. $H \cap K = (e)$. Let $K=(b)$. By (53.12), $ab=ba$. By (48.25), $o(ab) = pq$. $G = (ab)$, G is a cyclic group.

(b) Since the proof of this exercise is the same as (75.10.(e).(d)), we do not rewrite it.

*12. Let G be a group of order pqr, $p < q < r$ primes. Prove
(a) the r-Sylow subgroup is normal in G.
(b) G has a normal subgroup of order qr.
(c) if $q \nmid (r-1)$, the q-Sylow subgroup of G is normal in G.

102.12 (a) Let H be a r-Sylow subgroup, K be a q-Sylow subgroup of G. $i_G(H) = pq$. $pqr \mid (pq)!$. By Lemma 2.7.5, H is a normal subgroup of G.

(b) HK is a subgroup of G. HK/K is a p-Sylows subgroup of the group G/K. $o(G/K) = pq$ implies HK/K is normal in G/K. Hence HK is normal in G.

(c) By (102.11.(a)), HK is a cyclic group. Every subgroup of a cyclic group is the unique subgroup with its order. Hence the subgroup of a cyclic group is a characteristic subgroup. K is a characteristic subgroup of HK. HK is a normal subgroup of G. K is a normal subgroup of G by (70.7.(a)).

13. If G is of order p^2q, p, q primes, prove that G has a nontrivial normal subgroup.

*14. If G is of order p^2q, p, q primes, prove that either a p-Sylow sub-

group or a q-Sylow subgroup of G must be normal in G.

102.13 There are mp+1 p-Sylow subgroups of G for some
102.14 nonnegative integer m. $mp+1 \mid p^2q$. $mp+1 \mid q$. $mp+1=1$ or $mp+1=q$. If $mp+1=1$, then the p-Sylow subgroup of G is normal. Suppose $mp+1=q$. There are nq+1 q-Sylow subgroups of G for some nonnegative integer n. $nq+1 \mid p^2q$. $nq+1 \mid p^2$. $nq+1=1$, $nq+1=p$ or $nq+1=p^2$. If $nq+1=1$, then the q-Sylow subgroup of G is normal. Therefore, suppose $nq+1=p$ or $nq+1=p^2$. If $nq+1=p$, then $p=nq+1=n(mp+1)+1=mnp+n+1>p$, a contradiction. Hence,

$$\begin{cases} mp+1=q \\ nq+1=p^2 \end{cases}$$

$nq=p^2-1=(p+1)(p-1)$. $q \mid p+1$ or $q \mid p-1$. If $q \mid p-1$, then $p>q=mp+1>p$, a contradiction. $q \mid p+1$. $p+1 \geq q=mp+1$, $p \geq mp$, $m=1$. $p+1=q$. If $p>2$, then p and q are add primes, contrary to $p+1=q$。 Hence $p=2$, $q=3$. $p^2q=12$. If a 3-Sylow subgroup of G is not normal in G, then there are $3 \cdot k+1=4$ 3-Sylow subgroups in G. There are $(3-1)\times 4=8$ elements of order 3 in G. The other elements forms a unique 2-Sylow subgroup of G. We have shown that, in any case, either a p-Sylow subgroup or a q-Sylow subgroup of G must be normal in G.

15. Let G be a finite group in which $(ab)^p = a^pb^p$ for every $a, b \in G$, where p is a prime dividing $o(G)$. Prove
(a) The p-Sylow subgroup of G is normal in G.
*(b) If P is the p-Sylow subgroup of G, then there exists a normal subgroup N of G with $P \cap N = (e)$ and $PN = G$.
(c) G has a nontrivial center.

103.15 Let m be the integer such that $p^m \mid o(G)$ and $p^{m+1} \nmid o(G)$.
Let $S=\{g \in G \mid o(g)$ is a power of $p\}$ and

$N=\{g^{p^m} \mid g \in G\}$
(a) S is a normal subgroup of G. Hence S is the p-Sylow subgroup of G and is normal in G.
(b) N is a normal subgroup of G.
$g^{p^m} \in N \cap S$ implies $(g^{p^m})^{p^r}=e$ for some nonnegative integer r. $g^{p^{m+r}}=e$. Since $p^{m+1} \nmid o(G)$, $r=0$ and $g^{p^m}=e$, $N \cap S=(e)$.
For any g in G, let $o(g)=p^nq$ with $(p,q)=1$. Then there are integers a and b such that $ap^m+bq=1$. $g=g^{ap^m+bq}=(g^a)^{p^m}\cdot(g^{bq})=(g^{bq})\cdot(g^a)^{p^m}$ $(g^{bq})^{p^n}=e$ implies $g^{bq} \in S$. $(g^a)^{p^m} \in N$. $g \in SN$。 $G=SN$, where S is the p-Sylow subgroup of G.
(c) By Thearem 2.11.2 $Z(S) \neq (e)$. Let $s \in Z(S)$ and $s \neq e$. For any n in N, $nsn^{-1}s^{-1} \in N \cap S=(e)$ since N and S are normal in G. $ns=sn$. For any g in G, by(b), $g=hn$ for some h in S and n in N. $gs=(hn)s=h(ns)=h(sn)=(hs)n=s(hn)=sg$. s lies in the center of G. Hence G has a nontrivial center.

**16. If G is a finite group and its p-Sylow subgroup P lies in the center of G, prove that there exists a normal subgroup N of G with $P \cap N = (e)$ and $PN = G$.

103.16 We only suggest the reader see "Larry Dornhoff Group Represention Theory (part A)" page 89-92.or "M, Hall: The Theory of Groups" page 200-204.

*17. If H is a subgroup of G, recall that $N(H) = \{x \in G \mid xHx^{-1} = H\}$. If P is a p-Sylow subgroup of G, prove that $N(N(P)) = N(P)$.

103.17 Clearly $N(P) \subset N(N(P))$. For $x \in N(N(P))$, $xN(P)x^{-1}=N(P)$. $P \subset N(P)$. $xPx^{-1} \subset xN(P)x^{-1}=N(P)$. P and xPx^{-1} are p-Sylow subgroups of N(P). By theorem 2.12.2, there is $y \in N(P)$ such that $P=y(xPx^{-1})y^{-1}=(yx)P(yx)^{-1}$ $yx \in N(P)$. $x \in y^{-1}N(P)=N(P)$. $N(N(P)) \subset N(P)$. $N(N(P))=N(P)$.

*18. Let P be a p-Sylow subgroup of G and suppose a, b are in the center of P. Suppose further that $a = xbx^{-1}$ for some $x \in G$. Prove that there exists a $y \in N(P)$ such that $a = yby^{-1}$.

103.18 $P \subseteq N(a)$, $P \subseteq N(b)$. $xPx^{-1} \subseteq xN(b)x^{-1} = N(xbx^{-1}) = N(a)$. P and xPx^{-1} are p-Sylow subgroups of $N(a)$. By Theorem 2.12.2, $P = y(xPx^{-1})y^{-1} = (yx)P(yx)^{-1}$ for some $y \in N(a)$. $yx \in N(P)$. $(yx)b(yx)^{-1} = y(xbx^{-1})y^{-1} = ya\ y^{-1} = a$.

**19. Let G be a finite group and suppose that ϕ is an automorphism of G such that ϕ^3 is the identity automorphism. Suppose further that $\phi(x) = x$ implies that $x = e$. Prove that for every prime p which divides $o(G)$, the p-Sylow subgroup is normal in G.

103.19 (i) Every element of G can be expressed in the form $x^{-1}(x\phi)$ and $(x\phi)x^{-1}$ for suitable x in G.

pf. If $x^{-1}(x\phi) = y^{-1}(y\phi)$ with x, y in G, then $xy^{-1} = (xy^{-1})\phi$. But then $xy^{-1} = e$ and $x = y$. Thus there are as many distinct elements of G of the form $x^{-1}(x\phi)$ as there are element x of G and hence every element of G can be expressed in this form. Similarly, every element of G can be expressed in the form $(x\phi)x^{-1}$, Thus(i) holds.

(ii) For every x in G, we have $x(x\phi)(x\phi^2) = (x\phi^2)(x\phi)x = e$.

pf. If $x \in G$, $x = y^{-1}(y\phi)$ for some y in G by (i). Hence

$$\begin{aligned} x(x\phi)(x\phi^2) &= y^{-1}(y\phi)(y^{-1}(y\phi))\,\phi(y^{-1}(y\phi))\phi^2 \\ &= y^{-1}(y\phi)(y\phi)^{-1}(y\phi^2)(y\phi^2)^{-1}y\phi^3 \\ &= y^{-1}\cdot y \\ &= e. \end{aligned}$$

The second relation of (ii) is proved similarly.

(iii) For every $p \mid o(G)$, ϕ leaves invariant a unique p-Sylow subgroup P of G. Further more, P contains every ϕ-invariant p-subgroup of G. (Note: a subgroup H of G is said to be ϕ-invariant if and only if $H\phi = H$.)

pf. Let Q be a p-Sylow subgroup of G. $Q\phi$ is also a p-Sylow subgroup of G, and so $Q\phi = y^{-1}Qy$ for some y in G. But then $(z^{-1}Qz)\phi = (z\phi)^{-1}y^{-1}Qy(z\phi)$ for any z in G. By(i) we can choose z so that $(z\phi)z^{-1} = y^{-1}$, in which case $y(z\phi) = z$. For this choice of z, we then have $(z^{-1}Qz)\phi = z^{-1}Qz$. and so ϕ leaves invariant the p-Sylow subgroup $P = z^{-1}Qz$.

Suppose now that P and Q′ are two ϕ-invariant p-Sylow subgroups of G. Then $Q' = x^{-1}Px$ for some x in G. Applying ϕ, it follows that also $Q' = (x\phi)^{-1}P(x\phi)$, whence $y = (x\phi)x^{-1} \in N_G(P)$. $N_G(P)$ is also ϕ-invariant. For, if $h \in N_G(P)$, $h^{-1}Ph = P$. Applying ϕ, it follows that $(h\phi)^{-1}P(h\phi) = P$, whence $h\phi \in N_G(P)$, Centainly, $n\phi = e$ implies $n = e$. By(i), applied to $N_G(P)$, we have $y = (z\phi)z^{-1}$ for some z in $N_G(P)$. But then $(x\phi)x^{-1} = (z\phi)z^{-1}$ and it follows that $x = z$. Thus $x \in N_G(P)$ and consequently $P = Q'$. Thus P is unique.

Finally, let H be a ϕ-invariant p-subgroup of G and let K be a maximal ϕ-invariant p-subgroup of G containing H. It will suffice to show that K is a p-Sylow subgroup of G, for then $K = P$ by the proceding argument and the desired conclusion $H \subseteq P$ will follow. $N_G(K)$ is also a ϕ-invariant subgroup. $N_G(K)$ possesses a unique ϕ-invariant p-Sylow subgroup Q. We have $Q \supset K$ and now our maximal choice of K implies $Q = K$. Hence if R is a p-Sylow subgroup of G containing K, we have $K = N_G(K) \cap R = N_R(K)$. Hence $R = K$ since R is a p-group. K is a p-Sylow subgroup of G, as required.

(iv) proof of the excercise.

Since $x(x\phi)(x\phi^2)=(x\phi^2)(x\phi)x=e$ by (ii), we have $x(x\phi)=(x\phi^2)^{-1}=(x\phi)x$, so x commutes with $x\phi$ for all x in G. Now let P be the unique ϕ-invariant p-Sylow subgroup of G for any $p \mid o(G)$. Assume that P is not a normal subgroup of G. Then there exists a p-Sylow subgroup Q of G with $P \neq Q$. Choose x in Q with $x \notin P$ and let H be the subgroup generated by x and $x\phi$. By the preceding paragraph, x and $x\phi$ commute, so H is abelian. Since x and $x\phi$ is of order a power of P, H is a p-subgroup. On the other hand, since $x\phi^2=(x(x\phi))^{-1}$, ϕ transforms the generators x and $x\phi$ of H into elements of H and so leaves H invariant. Thus H is a ϕ-inviant p-subgroup of G and so $H \subseteq P$ by (iii), contrary to the fact that $x \in H$, but $x \notin P$.

#20. Let G be the group of $n \times n$ matrices over the integers modulo p, p a prime, which are invertible. Find a p-Sylow subgroup of G.

103.20 $\{\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}\}$ is a p-Sylow subgroup.

21. Find the possible number of 11-Sylow subgroups, 7-Sylow subgroups, and 5-Sylow subgroups in a group of order $5^2 \cdot 7 \cdot 11$.

103.21 There are $5k+1$ 5-Sylow subgroups of G for some nonnegative integer k. $5k+1 \mid 5^2 \cdot 7 \cdot 11$ implies $5k+1 \mid 7 \cdot 11$. $k=2$ or $k=0$, that is there are one 5-Sylow subgroup or 11's 5-Sylow subgroups in G.

There are $7k'+1$ 7-Sylow subgroups of G for some nonnegative integer k'. $7k'+1 \mid 5^2 \cdot 7 \cdot 11$ implies $7k'+1 \mid 5^2 \cdot 11$. $k'=0$. There is only one 7-Sylow subgroup in G.

There are $11k''+1$ 11-Sylow subgroups of G for some nonnegative integer k''. $11k''+1 \mid 5^2 \cdot 7$ implies $k''=0$. There is only one 11-Sylow subgroup in G.

22. If G is S_3 and $A = ((1\,2))$ in G, find all the double cosets AxA of A in G.

103.22 $A(12)A=\{e,(12)\}$. $A(13)A=\{(23),(123),(132),(13)\}$.

23. If G is S_4 and $A = ((1\,2\,3\,4))$, $B = ((1\,2))$, find all the double cosets AxB of A, B in G.

103.23 $A(12)B=\{(1234),(13)(24),(1432),e,(234),(1324),(143),(12)\}$
$A(13)B=\{(12)(34),(24),(14)(23),(13),(34),(124),(1423),(132)\}$
$A(14)B=\{(123),(1342),(243),(14),(23),(134),(1243),(142)\}$.

24. If G is the dihedral group of order 18 generated by $a^2 = b^9 = e$, $ab = b^{-1}a$, find the double cosets for H, K in G, where $H = (a)$ and $K = (b^3)$.

103.24 $HaK=\{e, b^3, b^6, a, ab^3, ab^6\}$.
$HbK=\{b, b^4, b^7, ab, ab^4, ab^7\}$.
$Hb^2K=\{b^2, b^5, b^8, ab^2, ab^5, ab^8\}$.

2.13 Direct Products

1. If A and B are groups, prove that $A \times B$ is isomorphic to $B \times A$.

108.1 Define $T: A\times B \to B\times A$ as $T(a,b)=(b,a)$. Then $T((a_1,b_1)(a_2,b_2))=T(a_1a_2, b_1b_2)=(b_1b_2, a_1a_2)=(b_1,a_1)(b_2,a_2)=T(a_1b_1)\,T(a_2,b_2)$. T is a homomorphism of $A\times B$ into $B\times A$. For $(b,a)\in B\times A$, $T(a,b)=(b,a)$. T is onto. T is also one-to-one. Therefore T is an isomorphism of $A\times B$ onto $B\times A$. $A\times B$ is isomorphic to $B\times A$.

2. If G_1, G_2, G_3 are groups, prove that $(G_1 \times G_2) \times G_3$ is isomorphic to $G_1 \times G_2 \times G_3$. Care to generalize?

108.2 Define $T: (G_1\times G_2)\times G_3 \to G_1\times G_2\times G_3$ as $T((g_1,g_2), g_3)=(g_1, g_2, g_3)$. $T(((g_1,g_2),g_3)((g_1',g_2'),g_3')=T(((g_1,g_2)(g_1',g_2')), g_3g_3')=T((g_1g_1', g_2g_2'), g_3g_3')=(g_1g_1', g_2g_2', g_3g_3')=(g_1,g_2,g_3)(g_1',g_2',g_3')=T((g_1,g_2),g_3)\,T((g_1',g_2'),g_3')$. T is a homomorphism of $(G_1\times G_2)\times G_3$ into $G_1\times G_2\times G_3$. T is clearly one-to-one and onto. T is an isomorphism of $(G_1\times G_2)\times G_3$ onto $G_1\times G_2\times G_3$. $(G_1\times G_2)\times G_3$ is isomorphic to $(G_1\times G_2\times G_3)$.

As (36.19), we can prove that no matter how we bracket $G_1G_2\cdots\cdots G_n$, retaining the order of $G_1, G_2, \cdots, G_n$, they are all isomorphic to $G_1\times G_2\times \cdots\times G_n$.

3. If $T = G_1 \times G_2 \times \cdots \times G_n$ prove that for each $i = 1, 2, \ldots, n$ there is a homomorphism ϕ_i of T onto G_i. Find the kernel of ϕ_i.

108.3 Define $\phi_i: G_1\times G_2\times\cdots\times G_n \to G_i$ as $\phi_i(g_1, g_2, \cdots, g_n)=g_i$. ϕ_i is clearly a homomorphism of $G_1\times G_2\times\cdots\times G_n$ onto G_i with kernel $G_1\times G_2\times\cdots\times(e)\times\cdots\times G_n$ ((e) in the i-th position).

4. Let G be a group and let $T = G \times G$.
   (a) Show that $D = \{(g, g) \in G \times G \mid g \in G\}$ is a group isomorphic to G.
   (b) Prove that D is normal in T if and only if G is abelian.

108.4 (a) Define $\Phi: D \to G$ as $\Phi(g,g)=g$. Φ is an isomorphism of D onto G. D is isomorphic to G.

(b) Suppose that G is abelian. For $(g_1, g_2)\in T$ and $(g, g)\in D$, $(g_1, g_2)(g, g)(g_1, g_2)^{-1}=(g_1, g_2)(g, g)(g_1^{-1}, g_2^{-1})=(g_1gg_1^{-1}, g_2gg_2^{-1})=(g, g)\in D$. D is a normal subgroup of T.

Conversely, suppose that D is normal in T. For all $g_1\in G$ and $g_2\in G$, $(g_1, e)\in T$, $(g_2, g_2)\in D$. $(g_1g_2g_1^{-1}, eg_2e^{-1})=(g_1, e)(g_2, g_2)(g_1, e)^{-1}\in D$. $g_1g_2g_1^{-1}=eg_2e^{-1}=g_2$. $g_1g_2=g_2g_1$. G is abelian.

5. Le G be a finite abelian group. Prove that G is isomorphic to the direct product of its Sylow subgroups.

108.5 Let $p_1, p_2, \cdots, p_n$ be distinct prime numbers which divide $o(G)$. Let $G_1, G_2, \cdots, G_n$ be p_1-Sylow, p_2-Sylow, $\cdots$, p_n-Sylow subgroups of G.

Define $T: G_1\times G_2\times\cdots\times G_n \to G$ as $T(g_1, g_2, \cdots, g_n)=g_1g_2\cdots g_n$.

$T((g_1, g_2, \cdots, g_n)(g_1', g_2', \cdots, g_n'))=T(g_1g_1', g_2g_2', \cdots, g_ng_n')=(g_1g_1')(g_2g_2')\cdots(g_ng_n')=(g_1g_2\cdots g_n)(g_1'g_2'\cdots g_n')=T(g_1, g_2, \cdots, g_n)\,T(g_1', g_2', \cdots, g_n')$. T is a homomorphism of $G_1\times G_2\times\cdots\times G_n$ into G.

Suppose $(g_1, g_2, \cdots, g_n)$ lie in the kernel of T, i.e. $g_1g_2\cdots g_n=e$. Let $o(g_i)=p_i^{e_i}$ for some integer e_i, $i=1, 2, \cdots, n$. $g_1^{-1}=(g_2\cdots g_n)$. $o(g_1^{-1})=p_1^{e_1}$ $o(g_2\cdots g_n)=p_2^{e_2}\cdots p_n^{e_n}$ by (48.25). Since $(p_1^{e_1}, p_2^{e_2}\cdots p_n^{e_n})=1$, $g_1^{-1}=e$. $g_2\cdots g_n=e$. Continuing this process, we get that $g_1=g_2=\cdots=g_n=e$. Hence the kernel of T is (e). T is one-to-one. Since $G_1\times G_2\times\cdots\times G_n$ and G are finite, T is also onto. T is an isomorphism of $G_1\times G_2\times\cdots\times G_n$ onto G.

G is isomorphic to $G_1 \times G_2 \times \cdots \times G_n$. G is isomorphic to the direct product of its Sylow subgroups.

6. Let A, B be cyclic groups of order m and n, respectively. Prove that $A \times B$ is cyclic if and only if m and n are relatively prime.

108.6 Let $A=(a)$, $B=(b)$. $o((a,e))=m$, $o((e,b))=n$. $(a,e)(e,b)=(a,b)=(e,b)(a,e)$. Suppose that $(m,n)=1$. By (48.25), $o((a,b))=mn$. Since $o(A\times B)=mn$, $A\times B=((a,b))$, $A\times B$ is cyclic. Converisely, suppose that $A\times B$ is cyclic. Let $m=dm'$ $n=dn'$ and $A\times B=((a,b))$. $(a,b)^{dm'n'}=(a^{dm'n'}, b^{dm'n'})=(a^{mn'}, b^{nm'})=e$. $mn \mid dm'n'$. $d=1$. $(m,n)=1$.

7. Use the result of Problem 6 to prove the Chinese Remainder Theorem; namely, if m and n are relatively prime integers and u, v any two integers, then we can find an integer x such that $x \equiv u \bmod m$ and $x \equiv v \bmod n$.

108.7 $(m,n)=1$ implies $J_m \times J_n$ is cyclic under addition Let $J_m \times J_n = ((a,b))$. Clearly, $a \not\equiv 0 \pmod m$ and $b \not\equiv 0 \pmod n$. $(au, bv) \in J_m \times J_n$. $(au, bv) = x(a,b)$ for some nonnegative integer x. Hence $au \equiv xa \pmod m$, $bv \equiv xb \pmod n$. Therefore, $x \equiv u \pmod m$ and $x \equiv v \pmod n$.

8. Give an example of a group G and normal subgroups $N_1, \ldots, N_n$ such that $G = N_1 N_2 \cdots N_n$ and $N_i \cap N_j = (e)$ for $i \neq j$ and yet G is *not* the internal direct product of $N_1, \ldots, N_n$.

108.8 Let $G=\{1, (12), (34), (12)(34)\} \subset S_4$ Let $N_1=((12))$, $N_2=((34))$, $N_3=((12)(34))$. Since G is abelian, N_1, N_2, N_3 are normal subgroups of G.

$N_1 \cap N_2 = N_2 \cap N_3 = N_3 \cap N_1 = (e)$

$G = N_1 N_2 N_3$,

Since $N_1 N_2 = G$, $N_1 N_2 \cap N_3 \neq (e)$, G is not the internal direct product of N_1, N_2, N_3.

9. Prove that G is the internal direct product of the normal subgroups $N_1, \ldots, N_n$ if and only if
   1. $G = N_1 \cdots N_n$.
   2. $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n) = (e)$ for $i = 1, \ldots, n$.

108.9 Suppose that G is the internel direct product of the normal subgroups $N_1, \cdots, N_n$. By definition, $G=N_1 N_2 \cdots N_n$ and given $g \in G$ then $g=m_1 m_2 \cdots m_n$, $m_i \in N_i$ in a unique way. Let $g \in N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n)$. $g=m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_n$, $m_j \in N_j$. $g \in N_i$. $e=g^{-1} m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_n$ $=(g^{-1}m_1 g)(g^{-1}m_2 g)\cdots(g^{-1}m_{i-1}g)g^{-1}(m_{i+1})\cdots m_n$. Since N_j is normal in G, $g^{-1}m_j g \in N_j$ for $j=1, 2, \cdots, i-1$. $e=e\cdots e$. Since the representation of e as $e=e\cdots e$ is unique, we have $g^{-1}m_j g = e$ for $j=1, 2, \cdots, i-1$. $g=e$ and $m_k=e$ for $k=i+1, \cdots, n$. Hence $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n)=(e)$.

Conversely, suppose that $G=N_1 \cdots N_n$ and $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n)=(e)$ for $i=1, \cdots, n$. Let $g=m_1 m_2 \cdots m_n = m_1' m_2' \cdots m_n'$, $m_i, m_i' \in N_i$, $i=1,2, \cdots, n$.

$m_1^{-1} m_1' m_2' \cdots m_n' = m_2 \cdots m_n \in (N_2 N_3 \cdots N_n)$, $m_2' \cdots m_n' \in N_2 \cdots N_n$. $N_2 \cdots N_n$ is a normal subgroup of G by (53.3). $m_1^{-1} m_1' \in N_1 \cap (N_2 \cdots N_n) = (e)$, $m_1 = m_1'$. Continuing this process we have $m_2=m_2'$, $\cdots$, $m_n=m_n'$. This show that for given $g \in G$, $g=m_1 \cdots m_n$, $m_i \in N_i$ in a unique way. Hence G is the internel product of $N_1, N_2, \cdots, N_n$.

10. Let G be a group, $K_1, \ldots, K_n$ normal subgroups of G. Suppose that $K_1 \cap K_2 \cap \cdots \cap K_n = (e)$. Let $V_i = G/K_i$. Prove that there is an isomorphism of G into $V_1 \times V_2 \times \cdots \times V_n$.

108.10 Define $T: G \to V_1 \times V_2 \times \cdots \times V_n$ as $T(g)=(K_1 g, K_2 g, \cdots, K_n g)$. For $g_1, g_2 \in G$.

$T(g_1 g_2)=(K_1 g_1 g_2, K_2 g_1 g_2, \cdots, K_n g_1 g_2)$

$= ((K_1g_1)(K_1g_2), (K_2g_1)(K_2g_2), \cdots, (K_ng_1)(K_ng_2)) = (K_1g_1, K_2g_1, \cdots, K_ng_1)(K_1g_2, K_2g_2, \cdots K_ng_2) = T(g_1)T(g_2)$. If $T(g)=e$, then $(K_1g, \cdots, K_ng) = e = (K_1, K_2, \cdots, K_n)$. $g \in K_1 \cap K_2 \cap \cdots \cap K_n = (e)$. The kernel of T is e. T is an isomorphism of G into $V_1 \times V_2 \times \cdots \times V_n$.

*11. Let G be a finite abelian group such that it contains a subgroup $H_0 \neq (e)$ which lies in *every* subgroup $H \neq (e)$. Prove that G must be cyclic. What can you say about $o(G)$?

108.11 $o(G)$ must be a power of a prime. For, if not, we can find two elements of relatively prime orders which shows that there are two nontrivial subgroups with intersection(e). This is a contradiction.
$o(G) = p^r$ for some prime number p and positive integer r.
Let P be a subgroup of order p^{r-1} in G. By induction hypothesis $P=(a)$ for some element a. If G is not cyclic, p^{r-1} is the highest possible order of elements in G. Let $b \in G/P$. Since $o(G/P)=p$, $b^p \in P$. $b^p = a^i$ for some i.
$(a^i)^{p^{r-2}} = (b^p)^{p^{r-2}} = b^{p^{r-1}} = e$ since p^{r-1} is the highest possible order. $o(a)=p^{r-1}$ implies $p^{r-1} | ip^{r-2}$, $p | i$, $i=pj$. Let $c=a^{-j}b$, Then $c \notin P$. $c^p = e$. We want to prove that $P \cap (c) = (e)$, which is a contradiction as we have shown.
Let $c^t \in P$. $c^t = (a^{-tj}b^t) \in P$. Hence $b^t \in P$, $p | t$. $c^t = e$. This completes the proof.

12. Let G be a finite abelian group. Using Problem 11 show that G is isomorphic to a subgroup of a direct product of a finite number of finite cyclic groups.

108.12 By (108.5), we need only prove that if G is a finite abelian group of order p^n for some prime number p and positive integer n, then G is isomorphic to a subgroup of a direct product of a finite number of finite cyclic groups.

For $a \in G$. Let Ka denote the maximal subgroup M such that $M \cap (a) = (e)$. That is $Ka \cap (a) = (e)$ and if $M \cap (a) = (e)$, then $M \subset Ka$. If $Ka = (e)$, then every subgroup $H \neq (e)$, $H \cap (a) \neq (e)$, $(a^{p^{r-1}}) \subset H$ where $o(a) = p^r$. By(108.11), G is cyclic. $G \approx G$.
Now suppose that $Ka \neq (e)$ for all a in G. $\bigcap_{a \in G} Ka = (e)$
For if $x \in Ka$, then $x \notin Kx$. Every subgroup $H \supseteq Ka$, $H \cap (a) \neq (e)$, $(a^{p^{r-1}}) \subset H$. Consider the group G/Ka, $H/Ka \supsetneq Ka$, $H/Ka \supset (a^{p^{r-1}})/Ka \neq Ka$. By (108.11), G/Ka is cyclic. By (108.10), G is isomorphic to a subgroup of a direct product of a finite number of finite cyclic groups.

13. Give an example of a finite non-abelian group G which contains a subgroup $H_0 \neq (e)$ such that $H_0 \subset H$ for *all* subgroups $H \neq (e)$ of G.

109.13 Let G be the group defined on (81.21). Subgroups of G are $\{e, \theta\}$, $\{e, \theta, a, \theta a\}$, $\{e, \theta, b, \theta b\}$, $\{e, \theta, c, \theta c\}$. $H_0 = \{e, \theta\} \subset H$ for all subgroup $H \neq (e)$ of G. G is a finite non-abelian group.

14. Show that every group of order p^2, p a prime, is either cyclic or is isomorphic to the direct product of two cyclic groups each of order p.

109.14 By (75.7), any group of order p^2 is abelian. If G is not cyclic, then there are two elements a and b such that $b \notin (a)$. (a), (b) are normal subgroups of G and $(a) \cap (b) = (e)$. $o((a)(b)) = p^2$. $(a)(b) = G$. By(108, 9), G is the internal product of (a) and (b). By Theorem 2.13.1, G is isomorphic to the direct product of two cyclic groups each of order p.

*15. Let $G = A \times A$ where A is cyclic of order p, p a prime. How many automorphisms does G have?

109.15 The automorphism group of $A \times A$ is isomorphic to the group defined on (37.26.(a)). Hence $A \times A$ has

$(p^2-1)(p^2-p)$ automorphisms.

16. If $G = K_1 \times K_2 \times \cdots \times K_n$ describe the center of G in terms of those of the K_i.

109.16 Let Z_i be the center of K_i. Then the center Z of G is $Z_1 \times Z_2 \times \cdots \times Z_n$. For, if $(g_1, g_2, \cdots, g_n) \in Z$, $(g_1, g_2, \cdots, g_n)(h_1, h_2, \cdots, h_n) = (h_1, h_2, \cdots, h_n)(g_1, g_2, \cdots, g_n)$ for any $(h_1, h_2, \cdots, h_n) \in G$. $(g_1h_1, g_2h_2, \cdots, g_nh_n) = (h_1g_1, h_2g_2, \cdots, h_ng_n)$ implies $g_1h_1 = h_1g_1$, $g_2h_2 = h_2g_2, \cdots, g_nh_n = h_ng_n$ for all $h_i \in K_i$, $i = 1, 2, \cdots, n$. $g_i \in Z_i$. $(g_1g_2, \cdots, g_n) \in Z_1 \times Z_2 \times \cdots \times Z_n$. $Z \subseteq Z_1 \times Z_2 \times \cdots \times Z_n$. Clearly $Z_1 \times Z_2 \times \cdots \times Z_n \subset Z$. $Z = Z_1 \times Z_2 \times \cdots \times Z_n$.

17. If $G = K_1 \times K_2 \times \cdots \times K_n$ and $g \in G$, describe

$$N(g) = \{x \in G \mid xg = gx\}.$$

109.17 Let $g = (g_1, g_2, \cdots, g_n)$. $N_i = N(g_i) = \{x \in K_i \mid xg_i = g_ix\}$. $N(g) = N_1 \times N_2 \times \cdots\cdots \times N_n$.

18. If G is a finite group and $N_1, \ldots, N_n$ are normal subgroups of G such that $G = N_1N_2 \cdots N_n$ and $o(G) = o(N_1)o(N_2) \cdots o(N_n)$, prove that G is the direct product of $N_1, N_2, \ldots, N_n$.

109.18 $K = \{m_1m_2 \cdots m_n \mid m_i \in N_i,\ i = 1, 2, \cdots, n\}$ has at most $o(N_1)\,o(N_2) \cdots o(N_n)$ elements.

If an element of G has two representations as $m_1m_2 \cdots m_n$, $m_i \in N_i$, then $o(G) = o(K) < o(N_1)\,o(N_2) \cdots o(N_n) = o(G)$, a contradiction. Therefore, G is the internal direct product of $N_1, N_2, \cdots, N_n$.

2.14 Finite Abelian Groups

1. If G is an abelian group of order p^n, p a prime and $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, are the invariants of G, show that the maximal order of any element in G is p^{n_1}.

115.1 Let $G = A_1 \times A_2 \times \cdots \times A_k$, where each A_i is cyclic of order p^{n_i} with $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. The generator of A_k has order p^{n_1}. For $g = (a_1, a_2, \cdots a_k) \in G$, $g^{n_1} = (a_1^{n_1}, a_2^{n_2}, \cdots, a_k^{n_1}) = e$. $o(g) \mid n_1$ by (49.36). $o(g) \leq n_1$, n_1 is the maximal order of any element in G.

2. If G is a group, $A_1, \ldots, A_k$ normal subgroups of G such that $A_i \cap (A_1A_2 \cdots A_{i-1}) = (e)$ for all i, show that G is the direct product of $A_1, \ldots, A_k$ if $G = A_1A_2 \cdots A_k$.

115.2 By (108.9), we need only to show that $A_i \cap (A_1A_2 \cdots A_{i-1}A_{i+1} \cdots A_k) = (e)$ for $i = 1, 2, \cdots, k$. Let $g = a_1a_2 \cdots a_{i-1}a_{i+1} \cdots a_k \in A_i \cap (A_1A_2 \cdots A_{i-1}A_{i+1} \cdots A_k)$. $e = g^{-1}a_1a_2 \cdots a_{i-1}a_{i+1} \cdots a_k = (g^{-1}a_1g)(g^{-1}a_2g) \cdots (g^{-1}a_{i-1}g)(g^{-1})\,a_{i+1} \cdots a_k$. $a_k^{-1} = (g^{-1}a_1g)(g^{-1}a_2g) \cdots (g^{-1}a_{i-1}g)(g^{-1})\,a_{i+1} \cdots a_{k-1} \in A_k \cap (A_1A_2 \cdots A_{k-1}) = (e)$. $a_{k-1}^{-1} = (g^{-1}a_1g)(g^{-1}a_2g) \cdots (g^{-1}a_{i-1}g)(g^{-1})\,a_{i+1} \cdots a_{k-2} \in A_{k-1} \cap (A_1A_2 \cdots A_{k-2}) = (e)$. Continuing this process we have $a_{i+1}^{-1} = (g^{-1}a_1g)(g^{-1}a_2g) \cdots (g^{-1}a_{i-1}g)(g^{-1}) \in A_{i+1} \cap (A_1A_2 \cdots A_i) = (e)$, and $g = (g^{-1}a_1g)(g^{-1}a_2g) \cdots (g^{-1}a_{i-1}g) \in A_i \cap (A_1A_2 \cdots A_{i-1}) = (e)$. $g = e$.

This proves that $A_i \cap (A_1A_2 \cdots A_{i+1} \cdots A_k) = (e)$. for $i = 1, 2, \cdots, k$. By (108.9), G is the internal product of $A_1, A_2, \cdots, A_k$.

3. Using Theorem 2.14.1, prove that if a finite abelian group has subgroups of orders m and n, then it has a subgroup whose order is the least common multiple of m and n.

115.3 We use induction to show that for any k, $k \mid o(G)$, G a finite abelian group, there is a subgroup of G which is of order k.

For k=1, (e) is a subgroup of order 1.

$k>1$. If $k=p^n$, then by Sylow Theorem, G has a subgroup of order p^n.

Suppose now that k is not a power of prime number. Let $k=p^m q$, $(p,q)=1$. By induction hypothesis, G has subgroups H and K such that $o(H)=p^m$, $o(K)=q$.

$$o(HK)=\frac{o(H)\,o(K)}{o(H\cap K)}=o(H)\,o(K)=p^m q.$$

This completes the proof of our asserstion.

If G has subgroups of order m and n, then $[m,n] \mid o(G)$. Hence, G has a subgroup of order $[m, n]$.

4. Describe all finite abelian groups of order
(a) 2^6. (b) 11^6. (c) 7^5. (d) $2^4 \cdot 3^4$.

115.4 (a) $J_2 \times J_2 \times J_2 \times J_2 \times J_2 \times J_2$

$J_4 \times J_2 \times J_2 \times J_2 \times J_2$ $J_4 \times J_4 \times J_2 \times J_2$

$J_4 \times J_4 \times J_4$

$J_8 \times J_2 \times J_2 \times J_2$

$J_8 \times J_4 \times J_2$

$J_8 \times J_8$

$J_{16} \times J_2 \times J_2$

$J_{16} \times J_4$

$J_{32} \times J_2$

J_{64}.

J_n denotes the integers modulo n under addition modulo n.

(b) $J_{11} \times J_{11} \times J_{11} \times J_{11} \times J_{11} \times J_{11}$

$J_{11}^2 \times J_{11} \times J_{11} \times J_{11} \times J_{11}$

$J_{11}^2 \times J_{11}^2 \times J_{11}^2$ $J_{11}^2 \times J_{11}^2 \times J_{11} \times J_{11}$

$J_{11}^2 \times J_{11}^2 \times J_{11}^2$

$J_{11}^3 \times J_{11} \times J_{11} \times J_{11}$

$J_{11}^3 \times J_{11}^2 \times J_{11}$

$J_{11}^3 \times J_{11}^3$

$J_{11}^4 \times J_{11} \times J_{11}$

$J_{11}^4 \times J_{11}^2$

$J_{11}^5 \times J_{11}$

J_{11}^6

(c) $J_7 \times J_7 \times J_7 \times J_7 \times J_7$

$J_7^2 \times J_7 \times J_7 \times J_7$

$J_7^2 \times J_7^2 \times J_7$

$J_7^3 \times J_7 \times J_7$

$J_7^3 \times J_7^2$

$J_7^4 \times J_7$

J_7^5

(d) Let $A_{11} = J_1 \times J_1 \times J_1 \times J_1$

$A_{12} = J_1^2 \times J_1 \times J_1$

$A_{13} = J_1^2 \times J_1 \times J_1$

$A_{14} = J_1^3 \times J_1$

$A_{15} = J_1^4$ $i=2$ or 3

$E_{ij} = A_{2i} \times A_{3j}\, 1 \le i \le 5,\ 1 \le j \le 5.$

There are, under nonisomorphism, 25's groups of order $2^4 \cdot 3^4$ which are abelian.

5. Show how to get all abelian groups of order $2^3 \cdot 3^4 \cdot 5$.

115.5 There are $3 \times 5 \times 2 = 30$'s nonisomorphic abelian groups of order $2^3 \cdot 3^4 \cdot 5$.

6. If G is an abelian group of order p^n with invariants $n_1 \ge \cdots \ge n_k > 0$ and $H \neq (e)$ is a subgroup of G, show that if $h_1 \ge \cdots \ge h_s > 0$ are the invariants of H, then $k \ge s$ and for each i, $h_i \le n_i$ for $i = 1, 2, \ldots, s$.

If G is an abelian group, let $\hat{G}$ be the set of all homomorphisms of G into the group of nonzero complex numbers under multiplication. If $\phi_1, \phi_2 \in \hat{G}$, define $\phi_1 \cdot \phi_2$ by $(\phi_1 \cdot \phi_2)(g) = \phi_1(g)\phi_2(g)$ for all $g \in G$.

115.6 $G(p) \supset H(p)$. $o(G(p)) = p^k > o(H(p)) = p^s$, $k \ge s$. That is the number of invariants of a subgroup is no more than that of a group.

Let t be the first i such that $h_i > n_i$. Let $m = n_t$. Consider the subgroups, $K = \{ x^{p^m} \mid x \in G \}$ and $K' = \{ x^{p^m} \mid x \in H \}$. K' is a subgroup of K. By the proof of Theorem 2.14.2, we have that the invariants of K are $n_1 - m, n_2 - m, \cdots, n_{k-1} - m$ but the invariants of K' are $h_1 - m, h_2 - m, \cdots, h_r - m$, where r is such that $h_r > m = n_r \geq h_{r-1}$, $r \geq t$. This shows that the number of invariants of K' is greater than that of K, but what we have proved it's a contradiction. Therefore, $h_i \leq n_i$ for $i = 1, 2, \cdots, s$.

7. Show that $\hat{G}$ is an abelian group under the operation defined.

115.7 If $\phi_1, \phi_2, \phi_3 \in \hat{G}$, $(\phi_1\phi_2)(g_1g_2) = \phi_1(g_1g_2)\phi_2(g_1g_2) = \phi_1(g_1)\phi_1(g_2)\phi_2(g_1)\phi_2(g_2) = (\phi_1(g_1)\phi_2(g_1))(\phi_1(g_2)\phi_2(g_2)) = ((\phi_1\phi_2)(g_1))((\phi_1\phi_2)(g_2))$, then $\phi_1\phi_2 \in G$.

$((\phi_1\phi_2)\phi_3)(g) = ((\phi_1\phi_2)(g))(\phi_3(g)) = ((\phi_1(g))(\phi_2(g)))(\phi_3(g)) = \phi_1(g)\phi_2(g)\phi_3(g)$.

$(\phi_1(\phi_2\phi_3))(g) = (\phi_1(g))((\phi_2\phi_3)(g)) = (\phi_1(g))((\phi_2(g))(\phi_3(g))) = \phi_1(g)\phi_2(g)\phi_3(g)$.

$(\phi_1\phi_2)\phi_3 = \phi_1(\phi_2\phi_3)$.

$(\phi_1 \circ 1)g = (\phi_1(g))(1(g)) = \phi_1(g) \cdot 1 = \phi_1(g)$.

$(\phi_1\phi_2)g = \phi_1(g)\phi_2(g) = \phi_2(g)\phi_1(g) = (\phi_2\phi_1)(g)$.

Let ϕ_1^{-1} defined as $\phi_1^{-1}(g) = (\phi_1(g))^{-1}$. ϕ_1^{-1} is also in $\hat{G}$ and $\phi_1\phi_1^{-1} = 1$. $\hat{G}$ is an abelian group.

8. If $\phi \in \hat{G}$ and G is finite, show that $\phi(g)$ is a root of unity for every $g \in G$.

115.8 Let $o(g) = n$. $g^n = e$. $(\phi(g))^n = \phi(g^n) = \phi(e) = 1$. $\phi(g)$ is a root of unity.

9. If G is a finite cyclic group, show that $\hat{G}$ is cyclic and $o(\hat{G}) = o(G)$, hence G and $\hat{G}$ are isomorphic.

115.9 Let $o(G) = n$ and $G = (g)$. Let r be a primitive n

root, i.e. $r^n = 1$ and $r^m \neq 1$ for $m < n$. Define ϕ_i as $\phi_i(g) = r^i$. $\hat{G} = \{ \phi_i \}$. Clearly $\phi_i = \phi_1^i$. $\hat{G}$ is cyclic and $o(\hat{G}) = o(G)$.

10. If $g_1 \neq g_2$ are in G, G a finite abelian group, prove that there is a $\phi \in \hat{G}$ with $\phi(g_1) \neq \phi(g_2)$.

115.10 Let $G = G_1 \times G_2 \times \cdots \times G_n$, where G_i is cyclic for $i = 1, 2, \cdots, n$. $G_i = (a_i)$. $o(a_i) = e_i$. $x = g_1g_2^{-1} = (x_1, x_2, \cdots, x_n) \neq (e)$ implies $x_m \neq e$ for some m. Suppose $x_m = a_m^{\frac{e_m}{k}}$ and x_m is of order k. Define $\phi_m : G_m \longrightarrow C$ as $\phi_m(a_m) = \theta$, where θ is an e_m-th primitive root. ϕ_m is a homomorphism and $\phi_m(x_m) \neq 1$. Define $\phi_i : G_i \longrightarrow C$ as $\phi_i = 1$ for $i \neq m$. Then $(\phi_1, \cdots, \phi_m, \cdots, \phi_n) : G \longrightarrow G$ defined as $(\phi_1, \cdots, \phi_m, \cdots, \phi_n)(y_1, y_2, \cdots, y_n) = \phi_1(y_1)\phi_2(y_2) \cdots \phi_n(y_n) = \phi_m(y_m)$ is a homomorphicm with $(\phi_1, \cdots, \phi_n)x \neq 1$. $(\phi_1, \cdots, \phi_n)(g_1g_2^{-1}) \neq 1$. $(\phi_1, \cdots, \phi_n)(g_1) \neq (\phi_1, \cdots, \phi_n)(g_2)$.

11. If G is a finite abelian group prove that $o(G) = o(\hat{G})$ and G is isomorphic to $\hat{G}$.

115.11 Let $G = G_1 \times G_2 \times \cdots \times G_n$, where $G_i = (a_i)$ is a cyclic group for $i = 1, 2, \cdots, n$. Let $o(a_i) = e_i$. If $\phi \in \hat{G}$, then $\phi(a_i) = \theta_i^{r_i}$ where θ_i is an e_i-th primitive root and $0 \leq r_i \leq e_i$.

$\phi = (\phi_1, \phi_2, \cdots, \phi_n)$, where $\phi_i : G_i \longrightarrow C$ with $\phi_i(a_i) = \theta_i^{r_i}$.

Conversely, for any given $(\phi_1, \phi_2, \cdots, \phi_n)$ with $\phi_i : G_i \longrightarrow C$ with $\phi_i(a_i) = \theta_i^{r_i}$ $0 \leq r_i \leq \theta_i$, $\phi = (\phi_1, \cdots, \phi_n) : G \longrightarrow C$ is a homomorphism. Therefore $o(G) = o(\hat{G})$. $\hat{G} \approx \hat{G}_1 \times \hat{G}_2 \times \cdots \times \hat{G}_n \approx G_1 \times G_2 \times \cdots \times G_n \approx G$.

12. If $\phi \neq 1 \in \hat{G}$ where G is an abelian group, show that $\sum_{g \in G} \phi(g) = 0$.

115.12 $\phi \neq 1$ implies $\phi(g) \neq 1$ for some g in G.

$$\phi(g)\Big(\sum_{g' \in G} \phi(g')\Big) = \sum_{g' \in G} \phi(g)\phi(g') = \sum_{g' \in G} \phi(gg')$$

$$= \sum_{gg' \in G} \phi(gg') = \sum_{g' \in G} \phi(g').$$

$\phi(g) \neq 1$ implies $\sum_{g \in G} \phi(g') = 0$

Supplementary Problems

There is no relation between the order in which the problems appear and the order of appearance of the sections, in this chapter, which might be relevant to their solutions. No hint is given regarding the difficulty of any problem.

1. (a) If G is a finite abelian group with elements $a_1, a_2, \ldots, a_n$, prove that $a_1 a_2 \cdots a_n$ is an element whose square is the identity.
   (b) If the G in part (a) has no element of order 2 or more than one element of order 2, prove that $a_1 a_2 \cdots a_n = e$.
   (c) If G has one element, y, of order 2, prove that $a_1 a_2 \cdots a_n = y$.
   (d) (*Wilson's theorem*) If p is a prime number show that $(p-1)! \equiv -1(p)$.

116.1 (a) $(a_1 a_2 \cdots a_n)^2 = (a_1 b_1)(a_2 b_2) \cdots (a_n b_n)$, where b_i is the inverse of a_i in G. $(a_1 a_2 \cdots a_n)^2 = e$.

(b) Suppose G has no element of order 2. Then every element except e has an inverse different from itself. Hence $a_1 a_2 \cdots a_n = e$.

Suppose G has more than one element of order 2. It clearly that the product of all elements of order other than 2 is e. We need only to prove that the product of all elements of order 2 is e. Without loss of generality, let G be a group of order 2^n with every element of order 2. When n= 2, it is every easy to prove the result. Use induction on n, let M be a maximal subgroup of G, $o(M) = 2^{n-1}$. By induction hypothesis, $a_1 \cdots a_{2^n-1} =$ e for $M = \{a_1, \cdots, a_{2^n-1}\}$. $i_G(M) = 2$. $G = M \cup Ma$ for some a in G. $G = \{a_1, a_2, \cdots, a_{2^n-1}, aa_1, aa_2, \cdots, aa_{2^n-1}\}$. $(a_1, a_2 \cdots a_{2^n-1})(aa_1 \cdot aa_2 \cdots aa_{2^n-1}) = (a_1 \cdot a_2 \cdots a_{2^n-1})^2 \cdot a^{2^n-1} = e$. This completes the proof. We can also prove this result by writing out the structure of the abelian group.

(c) Since the product of element of order other than 2 is e, $a_1 \cdots a_n = y$.

(d) In J_p, (-1) is the only element of order 2. By (c) $1 \cdot 2 \cdots (p-1) = -1(p)$.

2. If p is an odd prime and if

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b},$$

where a and b are integers, prove that $p \mid a$. If $p > 3$, prove that $p^2 \mid a$.

116.2 $$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \cdots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{p - \frac{p-1}{2}}\right)$$

$$= \frac{p}{p-1} + \frac{p}{2(p-2)} + \cdots + \frac{p}{\frac{p-1}{2}(p - \frac{p-1}{2})} = p\left(\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)}\right)$$

The denominator of the lowest term of $\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)}$ has no p as its divisor.

Therefore, $p \mid a$.

Furthermore, when $p > 3$ we want to show that

$$p \Big| \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)}$$

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(-i)} \equiv -\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2}$$

$\frac{1}{i^2}$ are all element of Q in (116.3). By(116.3.(b)),

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} \equiv \sum_{i=1}^{\frac{p-1}{2}} i^2 .$$

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv (-)\sum_{i=1}^{\frac{p-1}{2}} i^2 \equiv -\frac{\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot p}{6}$$

$$\equiv -p\left(\frac{p^2-1}{24}\right) \equiv 0 \pmod{p}$$

This completes the proof.

3. If p is an odd prime, $a \not\equiv 0\ (p)$ is said to be a *quadratic residue of* p if there exists an integer x such that $x^2 \equiv a(p)$. Prove
   (a) The quadratic residues of p form a subgroup Q of the group of nonzero integers mod p under multiplication.
   (b) $o(Q) = (p-1)/2$.
   (c) If $q \in Q$, $n \notin Q$ (n is called a *nonresidue*), then nq is a nonresidue.
   (d) If n_1, n_2 are nonresidues, then $n_1 n_2$ is a residue.
   (e) If a is a quadratic residue of p, then $a^{(p-1)/2} \equiv +1(p)$.

116.3 (a) If $a, b \in Q$, then there are x, y in J_p such that $x^2 \equiv a$, $y^2 \equiv b(p)$. Since $(xy^{-1})^2 \equiv ab^{-1}$, $ab^{-1} \in Q$. Q is a subgroup of the group of $J_p \setminus (0)$ mod p under multiplication.

(b) If $x^2 = y^2(p)$, then $(xy^{-1})^2 \equiv 1(p)$. By (116.4), $xy^{-1} \equiv 1$ or $xy^{-1} \equiv -1$. $x \equiv y$ or $x \equiv -y$.

$Q = \{1^2, 2^2, \cdots, (\frac{p-1}{2})^2\}$. $o(Q) = \frac{p-1}{2}$.

(c) If $nq \in Q$, then $n \in Qq^{-1} = Q$, contrary to our choice of n. Hence nq is a nonresidue.

(d) By(c) $x^2 n_i^{-1} \notin Q$ for $x = 1, 2, \cdots \frac{p-1}{2}$. $1^2 n_1^{-1}$, $2^2 n_1^{-1}, \cdots, (\frac{p-1}{2})^2 n_1^{-1}$ are distinct elements in J_p. For, if $x^2 n_1^{-1} \equiv y^2 n_1^{-1}(p)$, $x \equiv y$ or $x \equiv -y$. $x, y = 1, 2, \cdots, \frac{p-1}{2}$ implies $x = y$. $n_2 \in \{x^2 n_1^{-1} \mid x = 1, 2, \cdots, \frac{p-1}{2}\}$. Hence, $n_2 \equiv x^2 n_1^{-1}$ for some nonzero element x in J_p. $x^2 \equiv n_1 n_2$, $n_1 n_2$ is a residue.

(e) $a \in Q$. Since $o(Q) = \frac{p-1}{2}$. By Corollary 1 of Theorem 2.4.1, $a^{\frac{p-1}{2}} \equiv 1(p)$.

4. Prove that in the integers mod p, p a prime, there are at most n solutions of $x^n \equiv 1(p)$ for every integer n.

116.4 Actually, we prove that if f is of degree n, then $f(x) \equiv 0$ has at most n solutions in J_p. We prove our asserstion by induction n. When $n=1$, clearly $f(x) \equiv 0$ has exactly one solution in J_p. For $n > 1$, if $f(x) \equiv 0$ has no solution in J_p, then we have proved our result. Suppose f(x) has a solution r in J_p. Then $f(x) \equiv a(x)(x-r)+b$ for some a(x) and b with a(x) a polynomial and b in J_p. $0 \equiv f(r) \equiv a(r)(0) + b$ implies $b = 0$ and $f(x) \equiv (x-r)a(x)$, a(x) is a polynomial of degree n-1. By induction hypothesis a(x) has at most n-1 solutions in J_p. Since every solution of $f(x) \equiv 0$ is r or a solution of $a(x) \equiv 0$, $f(x) \equiv 0$ has at most n solutions in J_p.

5. Prove that the nonzero integers mod p under multiplication form a cyclic group if p is a prime.

116.5 By (49.38) and (116.4), we get the result.

6. Give an example of a non-abelian group in which $(xy)^3 = x^3y^3$ for all x and y.

116.6 $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in J_3 \right\}$ is a group under multiplication. Every element of G is of order 3. $(xy)^3 = e = x^3y^3$ for all x and y in G.

$$\begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

Hence G is a nonabelian group with $(xy)^3 = x^3y^3$ for all x and y.

7. If G is a finite abelian group, prove that the number of solutions of $x^n = e$ in G, where $n \mid o(G)$ is a multiple of n.

116.7 In the proof of (115.3), we have shown that for any $m \mid o(G)$, G has a subgroup H of order m. Let $S = \{ x \in G \mid x^n = e \}$. S is clearly a subgroup of G. $n \mid o(G)$ implies there is a subgroup H of G such that $o(H) = n$. H is also a subgroup of S. Hence $o(H) \mid o(S)$ and $n \mid o(S)$. The number of solutions of $x^n = e$ in G is a multiple of n.

8. Same as Problem 7, but do not assume the group to be abelian.

116.8 We suggest the reader see "M. Hall, The Theory of Groups" Page 136-138.

9. Find all automorphisms of S_3 and S_4, the symmetric groups of degree 3 and 4.

116.9 $\mathrm{Aut}(S_3) \approx S_3$, $\mathrm{Aut}(S_4) \approx S_4$.

pf. (i) Since $Z(S_3) = (e)$, $S_3 \approx \mathscr{I}(S_3) \subset \mathrm{Aut}(S_3)$ by Lemma 2.8.2. $\sigma \in \mathrm{Aut}(S_3)$ only permutes $\{(12), (13), (23)\}$. Hence $o(\mathrm{Aut}(S_3)) \leq 6 = o(S_3)$. $S_3 \approx \mathscr{I}(S_3)$. $o(\mathscr{I}(S_3)) = 6 \geq o(\mathrm{Aut}(S_3))$. $\mathscr{I}(S_3) = \mathrm{Aut}(S_3)$. $\mathrm{Aut}(S_3) \approx S_3$.

(ii) Since $Z(S_4) = (e)$, $S_4 \approx \mathscr{I}(S_4) \subset \mathrm{Aut}(S_4)$ by Lemma 2.8.2. S_4 has four 3-Sylow subgroups $P_1 = \{e, (123), (132)\}$, $P_2 = \{e, (124), (142)\}$, $P_3 = \{e, (234), (243)\}$ and $P_4 = \{e, (134), (143)\}$. $\sigma \in \mathrm{Aut}(S_4)$ permutes $\{P_1, P_2, P_3, P_4\}$. If σ fix P_1, P_2, P_3, P_4, then $\sigma = e$. Therefore $o(\mathrm{Aut}(S_4)) \leq o(S_4) = o(\mathscr{I}(S_4))$. $\mathrm{Aut}(S_4) = \mathscr{I}(S_4) \approx S_4$.

DEFINITION *A group G is said to be* solvable *if there exist subgroups $G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_r = (e)$ such that each N_i is normal in N_{i-1} and N_{i-1}/N_i is abelian.*

10. Prove that a subgroup of a solvable group and the homomorphic image of a solvable group must be solvable.

116.10 Let H be a subgroup of a solvable group G. To prove H is solvable, by (117, 13. (b)), we have to show that $H^{(k)} = (e)$ for some $k \geq 1$. $H^{(i)} \subseteq G^{(i)}$ for $i = 1$ If $H^{(i)} \subseteq G^{(i)}$ is true for some positive integer i, then by definition of $H^{(i)}$ and $G^{(i)}$ we have $H^{(i+1)} \subseteq G^{(i+1)}$. Therefore, $H^{(i)} \subseteq G^{(i)}$ for all positive integer i. Since G is solvable, $G^{(k)} = (e)$ for some $k \geq 1$, $H^{(k)} \subseteq G^{(k)} = (e)$. This proves that every subgroup of a solvable group must be solvable. By Theorem 2.7.1, for every homomarphic image $\bar{G}$ of G, there is a normal subgroup N of G such that $G/N \approx \bar{G}$. We want to show that $(G/N)^{(k)} = (\bar{e})$ for some $k \geq 1$. We can prove by induction that

$(G/N)^{(i)}=G^{(i)}/N$. Since $G^{(k)}=(e)$ for some $k\geq 1$, $(G/N)^{(k)}\subseteq G^{(k)}/N=N$. G/N is solvable and hence $\bar{G}$ is solvable.

11. If G is a group and N is a normal subgroup of G such that both N and G/N are solvable, prove that G is solvable.

116.11 By (117.13.(b)), We have $N^{(k)}=(e)$ and $(G/N)^{(h)}=(\bar{e})$ for some $k\geq 1$ and $h\geq 1$. $G^{(h)}/N=(G/N)^{(h)}=(\bar{e})$, $G^{(h)}\subseteq N$, $G^{(h+i)}\subseteq N^{(i)}$, $G^{(h+k)}\subseteq N^{(k)}=(e)$, G is solvable.

12. If G is a group, A a subgroup of G and N a normal subgroup of G, prove that if both A and N are solvable then so is AN.

116.12 $AN/N\approx A/A\bigcap N$ by (65.6). Since A is solvable, $A/A\bigcap N$ is solvable. N is solvable. By (116.11), AN is solvable.

13. If G is a group, define the sequence of subgroups $G^{(i)}$ of G by
(1) $G^{(1)}$ = commutator subgroup of G = subgroup of G generated by all $aba^{-1}b^{-1}$ where $a, b \in G$.
(2) $G^{(i)}$ = commutator subgroup of $G^{(i-1)}$ if $i > 1$.
Prove
(a) Each $G^{(i)}$ is a normal subgroup of G.
(b) G is solvable if and only if $G^{(k)} = (e)$ for some $k \geq 1$.

117.13(a) In fact, we want to prove that $G^{(1)}$ is a characteristic subgroup of $G^{(i-1)}$. Then by (70.7.(a)), each $G^{(i)}$ is a normal subgroup of G.
$G^{(1)}$ is the subgroup of $G^{(i-1)}$ generated by all $aba^{-1}b^{-1}$ where $a, b\in G^{(i-1)}$. For any automorphism ϕ of $G^{(i-1)}$, $\phi(aba^{-1}b^{-1})=\phi(a)\phi(b)(\phi(a))^{-1}(\phi(b))^{-1}\in G^{(1)}$, $\phi(G^{(1)})\subseteq G^{(1)}$. Hence $G^{(1)}$ is a characteristic subgroup of $G^{(i-1)}$.

(b) Suppose that there exist subgroups $G=N_0\supset N_1\supset N_2\supset\cdots\supset N_r=(e)$ such that each N_i is normal in N_{i-1} and N_{i-1}/N_i is abelian. We want to show that $G^{(i)}\subset N_i$. $G^{(0)}=G=N_0$. Suppose $G^{(i)}\subset N_i$. Since N_i/N_{i+1} is abelian, by (65,5,(c)), $N_{i+1}\supset N_i'\supset (G^{(i)})'=G^{(i+1)}$. $G^{(i)}\subset N_i$ for all i. $G^{(r)}\subset N_r=(e)$.
Conversely, suppose that $G^{(k)}=1$ for some $k\geq 1$. Then $G=G^{(0)}\supset G^{(1)}\supset G^{(2)}\supset\cdots\supset G^{(k)}=(e)$, $G^{(i)}$ is normal in $G^{(i-1)}$ and $G^{(i-1)}/G^{(i)}$ is abelian by (65.5.(b)). G is solvable.

14. Prove that a solvable group always has an abelian normal subgroup $M \neq (e)$.

117.14 By(117.13.(b)), $G^{(k)}=(e)$ for some $k\geq 1$. Let r be the smallest positive integer such that $G^{(r)}=(e)$. $G^{(r-1)}\neq(e)$. By (117.13.(a)), $G^{(r-1)}$ is normal in G. $G^{(r)}=(G^{(r-1)})'=(e)$ implies $aba^{-1}b^{-1}=e$ for all $a, b\in G^{(r-1)}$, i.e. $ab=ba$ for all $a, b\in G^{(r-1)}$. $G^{(r-1)}$ is an abelian normal subgroup of G. $G^{(r-1)}\neq(e)$.

If G is a group, define the sequence of subgroups $G_{(i)}$ by
(a) $G_{(1)}$ = commutator subgroup of G.
(b) $G_{(i)}$ = subgroup of G generated by all $aba^{-1}b^{-1}$ where $a \in G$, $b \in G_{(i-1)}$.
G is said to be *nilpotent* if $G_{(k)} = (e)$ for some $k \geq 1$

15. (a) Show that each $G_{(i)}$ is a normal subgroup of G and $G_{(i)} \supset G^{(i)}$.
(b) If G is nilpotent, prove it must be solvable.
(c) Give an example of a group which is solvable but not nilpotent.

117.15(a) $G^{(1)}=G_{(1)}$ by definition. Suppose $G^{(i)}\subset G_{(i)}$. $G^{(i+1)}$ is the subgroup of $G^{(i)}$ generated by all $aba^{-1}b^{-1}$ where $a, b\in G^{(i)}$. Hence $G^{(i+1)}\subset G_{(i+1)}$. Sinci $xaba^{-1}b^{-1}x^{-1}=xax^{-1}xbx^{-1}xa^{-1}x^{-1}xb^{-1}x^{-1}$ and (64.4.(b)), we can prove that G(i) is normal by induction way.

(b) If G is nilpotent, then $G_{(k)}=(e)$ for some $k\geq 1$. $G^{(k)}\subseteq G_{(k)}=(e)$. By (117.13.(b)), G is solvable.

(c) Let $G=S_3=\{(1),(12),(13),(23),(123),(132)\}$. $G^{(1)}$ is a normal subgroup of G. G has only three normal subgroups G, (e) and $\{(1),(123),(132)\}$.

$(a_1a_2)(a_1a_3)(a_1a_2)^{-1}(a_1a_3)^{-1}=(a_2a_3)(a_1a_3)$
$=(a_1a_3a_2)$. Hence $G^{(1)}=\{(1),(123),(132)\}$.
$G^{(2)}=(e)$ since $G^{(1)}$ is abelian. G is solvable.
$(13)(123)(13)^{-1}(123)^{-1}=(321)(123)^{-1}=(123)$.
$G_{(2)}\neq(e)$. $G_{(2)}=G_{(1)}$, $G_{(k)}=G_{(1)}\neq(e)$ for all $k\geq 1$. G is not nilpotent.

16. Show that any subgroup and homomorphic image of a nilpotent group must be nilpotent.

117.16 Let H be a subgroup of a nilpotent group G. $G_{(k)}=(e)$ for some $k\geq 1$. $H_{(1)}\subseteq G_{(1)}$. $H_{(k)}\subseteq G_{(k)}=(e)$ H is nilpotent.
By Theorem 2.7.1, for every homomorphic image $\bar{G}$ of G, there is a normal subgroup N of G such that $G/N\approx\bar{G}$. $(G/N)_{(1)}\subseteq G_{(1)}/N$. $(G/N)_{(k)}=G_{(k)}/N=(e)$. G/N is nilpotent. G is nilpotent.

17. Show that every homomorphic image, different from (e), of a nilpotent group has a nontrivial center.

117.17 Since any homomorphic image of a nilpotent group is also nilpotent, we need only to show that a nilpotent group different frome(e) has a nontrivial center. Let G be a nilpotent group and $G\neq(e)$. $G_{(k)}=(e)$ for some $k\geq 1$. Let r be the smallest positive integer such that $G_{(r)}=(e)$. $G_{(r-1)}\neq(e)$. Let $g\in G_{(r-1)}$, $g\neq e$. Then $aga^{-1}g^{-1}\in G_{(r)}=(e)$ for all a in G. $aga^{-1}g^{-1}=e$ implies $ag=ga$. Hence g lies in the center of G. This completes the proof.

18. (a) Show that any group of order p^n, p a prime, must be nilpotent.
(b) If G is nilpotent, and $H\neq G$ is a subgroup of G, prove that $N(H)\neq H$ where $N(H)=\{x\in G\mid xHx^{-1}=H\}$.

117.18 (a) We define a chain of subgroups inductively: $Z^0(G)=(e)$; $Z^{(i+1)}(G)$ is the subgroup of G corresponding to the center of $G/Z^i(G)$:

$G\longrightarrow G/Z^1(G)$
$Z^{i+1}(G)\longrightarrow$ center $=Z^{i+1}/Z^i$
$Z^i(G)\longrightarrow(e)$.
$Z^i(G)$ is the ith higher center of G.
We first prove the following
Lemma: $Z^m(G)=G$ implies $G_{(m+1)}=(e)$. moreover, $G_{(i+1)}\subset Z^{m-i}(G)$ for all i.
pf: Assuming $Z^m=G$, we shall prove the inclusion holds by an induction on i.
Both terms equal G when $i=0$, so the induction begins. If $G_{(i+1)}\subset Z^{m-i}$, then $G_{(i+2)}\subset H$, where H is the subgroup of G generated by all $aba^{-1}b^{-1}$ with $a\in G$ and $b\in Z^{m-i}$. $Z^{m-i}/Z^{m-i-1}\subset Z(G/Z^{m-i-1})$ implies $H\subset Z^{m-i-1}$. $G_{(i+2)}\subset Z^{m-i-1}$. Since the inclusion holds for all i, it holds for $i=m$, Therefore, $G_{(m+1)}\subset Z^0=(e)$.
Proof of the exercise: By Theorem 2.11.2, G and all its nontrivial quotients have nontrivial centers. Therefore, if $Z^i\neq G$ for some i, then $Z^i\subseteq Z^{i+1}$. Since G is finite, itfollows that $Z^i=G$ for some i, i.e. G is nilpotent.
(b) Since $H\neq G$, there exists an i such that $G_{(i+1)}\subset H$, but $G_{(i)}\not\subset H$. Now, the subgroup of G generated by all $aba^{-1}b^{-1}$ with $a\in G_{(i)}$, $b\in H$ is contained in $G_{(i+1)}$ and hence H. Therefore $G_{(i)}\subset N(H)$ and $N(H)\neq H$.

19. If G is a finite group, prove that G is nilpotent if and only if G is the direct product of its Sylow subgroups.

117.19 We first prove that
Lemma: a direct product of a finite number of nilpotent groups is nilpotent.
pf: An induction on the number of direct factors allows us to assume that $G=H\times K$. Another

induction proves that $(H\times K)_{(i)} \subset H_{(i)} \times K_{(i)}$ for all i. Let $M=\max\{m,n\}$, where $H_{(m)}=K_{(m)}=(e)$. Then $(H\times K)_m=(e)$, so that $H\times K$ is nilpotent.

Proof of the exercise:

If G is the direct product of its Sylow subgroups, then G is nilpotent, by (117.18.(a)) and the above Lemma.

Conversely, suppose that G is nilpotent. By (117.18.(b)), if $H\neq G$, then $N(H)\neq H$. Let P be a p-Sylow subgroup of G. By (103.17), $N(N(P))=N(P)$. If $N(P)\neq G$, then $N(N(P))=N(P)$ and $N(N(P))\neq N(P)$, a contradiction. Hence $N(P)=G$. P is a normal subgroup of G. This shows that every p-Sylow subgroup of G is nomal. G is therefore the internal direct product of all its Sylow Subgroups.

20. Let G be a finite group and H a subgroup of G. For A, B subgroups of G, define A to be conjugate to B relative to H if $B = x^{-1}Ax$ for some $x \in H$. Prove
(a) This defines an equivalence relation on the set of subgroups of G.
(b) The number of subgroups of G conjugate to A relative to H equals the index of $N(A) \cap H$ in H.

117.20(a) $A=e^{-1}Ae$ implies $A\sim A$. If $B\sim A$, then there is an x in H such that $B=x^{-1}Ax$. $(x^{-1})^{-1}B(x^{-1})=A$, $x^{-1}\in H$. $A\sim B$. If $B\sim A$ and $C\sim B$, then there are x, y in H such that $B=x^{-1}Ax$, $C=y^{-1}By$. $C=y^{-1}By=y^{-1}(x^{-1}Ax)y=(xy)^{-1}A(xy)$, $xy\in H$. $C\sim A$. Therefore $\sim$ is an equivalence relation on the set of subgroups of G.

(b) Define $\phi(x^{-1}Ax)=(N(A)\cap H)x$ for all x in H. Then $x^{-1}Ax=y^{-1}Ay \Leftrightarrow (xy^{-1})^{-1}A(xy^{-1})=A \Leftrightarrow xy^{-1}\in H$ and $xy^{-1}\in N(A) \Leftrightarrow xy^{-1}\in H\cap N(A) \Leftrightarrow (H\cap N(A))x=(H\cap N(A))y \Leftrightarrow \phi(x^{-1}Ax)=\phi(y^{-1}Ay)$. Therefore, ϕ is well-defined and ϕ is one-to-one. For any $(N(A)\cap H)x$, $x\in H$, we have $\phi(x^{-1}Ax)=(N(A)\cap H)x$. Therefore, ϕ is a one-to-one correspondence between the set of subgroups of G conjugate to A relative to H and the set of right cosets of $N(A)\cap H$ in H. This completes the proof.

21. (a) If G is a finite group and if P is a p-Sylow subgroup of G, prove that P is the only p-Sylow subgroup in $N(P)$.
(b) If P is a p-Sylow subgroup of G and if $a^{p^k}=e$ then, if $a\in N(P)$, a must be in P.
(c) Prove that $N(N(P))=N(P)$.

117.21(a) Since $P\subset N(P)$ and $o(N(P))\mid o(G)$, P is a p-Sylow subgroup of N(P). By definition of N(P), P is a normal subgroup of N(P). Let Q be a p-Sylow subgroup of N(P). PQ is also a subgroup of N(P) by (53.3). By Theorem 2.5.1,

$$o(PQ)=\frac{o(P)\,o(Q)}{o(P\cap Q)}=\frac{p^{2m}}{Q(P\cap Q)},$$

where $o(P)=p^m$. If $o(P\cap Q)<p^m$, then $(PQ)>p^m$, contrary to the fact that $p^m\mid o(G)$, $p^{m+1}\nmid o(G)$. Hence, $o(P\cap Q)\geq p^m$, $o(P\cap Q)=p^m=o(P)$, $P\cap Q=P$, $P=Q$. P is the only p-Sylow subgroup in N(P).

(b) Let Q be the subgroup generated by a and let $o(Q)=p^k$. Then

$$o(PQ)=\frac{o(P)\,o(Q)}{o(P\cap Q)}=\frac{p^m\cdot p^k}{o(P\cap Q)}$$

If $o(P\cap Q)<p^k$, then $o(PQ)>p^m=o(P)$, a contradiction. $o(P\cap Q)\geq p^k=o(Q)$.
$o(P\cap Q)=o(Q)$, $P\cap Q=Q$, $Q\subset P$. $a\in P$.

(c) Clearly, we have $N(P)\subset N(N(P))$. For x in $N(N(P))$, $x^{-1}N(P)x=N(P)$. $P\subset N(P)\subset x^{-1}N(P)x$, $xPx^{-1}\subset N(P)$. xPx^{-1} is also a p-Sylow

subgroup in N(P). By(a), $xPx^{-1} = P$ and $x \in N(P)$. $N(N(P)) \subset N(P)$. This completes the proof.

22. (a) If G is a finite group and P is a p-Sylow subgroup of G, prove that the number of conjugates of P in G is *not* a multiple of p.
(b) Breaking up the conjugate class of P further by using conjugacy relative to P, prove that the conjugate class of P has $1 + kp$ distinct subgroups. (*Hint:* Use part (b) of Problem 20 and Problem 21. Note that together with Problem 23 this gives an alternative proof of Theorem 2.12.3, the third part of Sylow's theorem.)

117.22(a) In (117.20), let H=G. By (117.20.(b)), the number of conjugates of P in G is $i_G(N(P))$. Since $P \subset N(P)$, $p \nmid i_G(N(P))$. The number of conjugates of P is not a multiple of P.

(b) As above, let H = G in (117.20). Then
$$i_G(N(P)) = \sum i_P(N(A) \cap P),$$
where the sum extends over a set of representatives $\{A\}$ of the classes of subgroups of G conjugate to A relative to P. If A=P, $i_P(N(A) \cap P) = i_P(P) = 1$. For all others A, $N(A) \cap P = A \cap P$ by (117.21.(b)). $p \mid i_P(N(A) \cap P)$ for $A \neq P$. Therefore, the conjugate class of P has $1+kp$ distinct subgroups.

23. (a) If P is a p-Sylow subgroup of G and B is a subgroup of G of order p^k, prove that if B is not contained in some conjugate of P, then the number of conjugates of P in G is a multiple of p.
(b) Using part (a) and Problem 22, prove that B must be contained in some conjugate of P.
(c) Prove that any two p-Sylow subgroups of G are conjugate in G. (This gives another proof of Theorem 2.12.2, the second part of Sylow's theorem.)

Note : Change "some" by "any" in (118.23.(a)).

118.23(a) For any conjugate Q of P, $N(Q) \cap B \neq B$. For, if $N(Q) \cap B = B$, $B \subset N(Q)$. By (117.21.(b)), $B \subset Q$, contrary to our assumption that B is not contained in any conjugate of P. Since $N(Q) \cap B \neq B$, $P \mid i_B(N(Q) \cap B)$. The number of subgroups of G conjugate to Q relative to B is therefore a multiple of P by (117.20.(b)). The number of conjugates of P in G is the sum of $i_B(N(Q) \cap B)$ for some Q which conjugate to P in G. Hence, the number of conjugates of P in G is a multiple of P.

(b) By (117.22.(a)), B must be contained in some conjugate of P.

(c) Let P, Q be two p-Sylow subgroup of G. By (b), Q is conjugate to P in G.

24. Combine Problems 22 and 23 to give another proof of all parts of Sylow's theorem.

(Note : change " all" by " the second and third" in (118.24).)

118.24 By (118.23.(c)), all p-Sylow subgroups of G are conjugate. By (117.22.(b)), the number of them are $1+kp$ for some integer k. This prove the second and third part of Sylow Theorem.

25. Making a case-by-case discussion using the results developed in this chapter, prove that any group of order less than 60 either is of prime order or has a nontrivial normal subgroup.

118.25 In the following, we assume all p, q, r are distinct prime number. By (91.11) and (91.14), any group of order p^n has a nontrivial normal subgroup for $n > 1$. By (102.12) and (102.13), any group of order pqr and p^2q has a nontrivial normal subgroup. For groups of order pq, with $p < q$. $pq \mid p!$, by Lemma 2.9.1, these groups also have nontrivial normal subgroups. The groups of prime order is also in our argument. The above cases cover all subgroups of order 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,

13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 37, 38, 39, 41, 42, 43, 44, 45, 46, 47, 49, 50, 51, 52, 53, 55, 57, 58, 59. The exceptional cases are groups of order 24, 36, 40, 48, 54, 56.

(i) $o(G)=24$, G has a 2-Sylow subgroup H of order 8. $o(G) \nmid i_G(H)! = 3!$
By Lemma 2.9.1., G has a nontrivial normal subgroup.

(ii) $o(G)= 36$, G has a 3-Sylow subgroup H of order 9. $o(G) \nmid i_G(H)! = 4!$
By Lemma 2.9.1, G has a nontrivial normal subgroup.

(iii) $o(G)= 40$, the number of 5-Sylow subgroups of G is $5k+1$ for some k. Moreover, $5k+1 \mid 40$. This implies $5k+1=1$. 5-Sylow subgroup is a normal subgroup of G since G has a unique 5-Sylow subgroup.

(iv) $o(G)=48$. G has a 2-Sylow subgroup H of order 16. Since $o(G) \nmid i_G(H)=3!$, by Lemma 2.9.1., G has a nontrivial nomal subgroup.

(v) $o(G)=54$. G has a 3-Sylow subgroup H of order 27. Since $o(G) \nmid i_G(H)=2!$, by Lemma 2.9.1., G has a nontrivial normal subgroup.

(vi) $o(G)=56$. Suppose the 7-Sylow subgroup H of G is not normal. There are $7k+1$ 7-Sylow subgroups in G. $7k+1 \mid o(G)$ implies $7k+1=8$. Therefore, there are $(7-1)\times 8=48$ elements of order 7. Since $56-48=8$, the elements of G which is of order different from 7 forms the only 2-Sylow subgroup of G. Hence, the 2-Sylow subgroup is normal in G. We have now completed the proof.

26. Using the result of Problem 25, prove that any group of order less than 60 is solvable.

118.26 Use induction on the order of G. $o(G)=1$ is trivial.

Now, if $o(G)$ is prime, G is cyclic and hence solvable. If G is not prime, by (118.25), G has a nontrivial normal subgroup H. $o(G/H)$ and $o(H)$ are less than $o(G)$. By induction hypothesis G/H and H are solvable. By (116.11), G is solvable.

27. Show that the equation $x^2ax = a^{-1}$ is solvable for x in the group G if and only if a is the cube of some element in G.

118.27 Suppose there is an x in G such that $x^2ax=a^{-1}$. Then $xax=x^{-1}a^{-1}$. $xa=x^{-1}a^{-1}x^{-1}=(xax)^{-1}=(x^{-1}a^{-1})^{-1}=ax$. $x^3a=x^2ax=a^{-1}$, $(xa)^3=x^3a^3=(x^3a)a^2=a^{-1}\cdot a^2=a$. a is the cube of some element in G.
Conversely, suppose that $a=y^3$ for some element in G. Let $x=y^{-2}$. Then $x^2ax=(y^{-2})^2(y^3)(y^{-2})=y^{-3}=a^{-1}$. The equation $x^2ax=a^{-1}$ is solvable.

28. Prove that (1 2 3) is not a cube of any element in S_n.

118.28 Suppose a is the cube of some element in S_n. By (118.27), the equation $x^2ax=a^{-1}$ is solvable. As the proof in (118.27), we know that the solution x commutes with a and $a=(xa)^3=x^3a^3=x^3$. By (90.5.(c)), $x=(123)^i\tau$, where $i=0,1$, τ is a permutation leaving all 1, 2, 3 fixed. $x^3=(123)^{3i}\tau^3=\tau^3\neq a$, a contradiction. Hence a is not a cube of any element in S_n.

29. Prove that $xax = b$ is solvable for x in G if and only if ab is the square of some element in G.

118.29 Suppose that x is a solution of the equation $xax=b$ in G. Then $(ax)^2=axax=ab$. ab is the square of some element in G.
Conversely, let $ab=c^2$. Let $x=a^{-1}c$. Then $xax=(a^{-1}c)(a)(a^{-1}c)=a^{-1}c^2=b$, the equation $xax=b$ is solvable in G.

30. If G is a group and $a \in G$ is of finite order and has only a finite number of conjugates in G, prove that these conjugates of a generate a finite normal subgroup of G.

118.30 Let $o(a)=n$ and $H=\{b_1^{-1}ab_1, b_2^{-1}ab_2, \cdots, b_m^{-1}ab_m\}$ be the set of all conjugates of a in G. Every element in K which is generated by H is of the form $(b_{i_1}^{-1}ab_{i_1})(b_{i_2}^{-1}ab_{i_2})\cdots(b_{i_k}^{-1}ab_{i_k})$. If $k > n^m$, since $(c^{-1}ac)(b^{-1}ab)=(b^{-1}ab)[(b^{-1}a^{-1}b)(a^{-1}ac)(b^{-1}ab)]$, there is a $b_i^{-1}ab_i$ which appears n times and by changing the position $(b^{-1}ab)^n=1$. Hence k is bounded by n^m. $o(K)\leq n^m$.

31. Show that a group cannot be written as the set-theoretic union of two proper subgroups.

118.31 Suppose $G=A\cup B$ with $A\neq G$ and $B\neq G$. Let $a\in G\setminus A$ and $b\in G\setminus B$. $ab\in G=A\cup B$. If $ab\in A$, since $b\in A$, $a\in A$, a contradiction. If $ab\in B$, since $b\in A$, $a\in A$, a contradiction. Hence G can not be written as the set-theoretic union of two proper subgroups.

32. Show that a group G is the set-theoretic union of three proper subgroups if and only if G has, as a homomorphic image, a noncyclic group of order 4.

118.32 Suppose G has as a homomorphic image, a noncyclic group of order 4. $G/H\approx\{e, a, b, ab\}$ for some normal subgroup H of G with $a^2=b^2=(ab)^2=e$. Let K_1, K_2, K_3 b be the preimage of (a), (b) and (ab). The $G=K_1\cup K_2\cup K_3 b$. G is the union of three proper subgroups.

Conversely, suppose $G=A\cup B\cup C$ with A, B, C be three proper subgroups of G. We first claim that $A\cap B=A\cap C=B\cap C=A\cap B\cap C$. We need only to show that $x\in A\cap B$ implies $x\in C$. Choose an element $y\in G\ (A\cup B)$. Then $y\in C$ and $y\notin A$, $y\notin B$. $xy\in A$ or $xy\in B$ implies $y\in A$ or $y\in B$, contrary to our choice of y. Hence $xy\in C$. Since $y\in C$, $x\in C\cdot y^{-1}=C$. This proves that $A\cap B\subset A\cap B\cap C$ and $A\cap B=A\cap B\cap C$. Therefore, $A\cap B=A\cap C=B\cap C=A\cap B\cap C$. $A\cap B\cap C$ is a normal subgroup of G.

Let $K=\{e, a, b, ab\}$ be the noncyclic group of order 4. Define a mapping ϕ from G to K as.

$$\phi(x)=\begin{cases} e & \text{if } x\in A\cap B\cap C=A\cap B=A\cap C=B\cap C \\ a & \text{if } x\in G\setminus(B\cup C) \\ b & \text{if } x\in G\setminus(A\cup C) \\ ab & \text{if } x\in G\setminus(A\cup B). \end{cases}$$

It's easy to check that ϕ is a homomorphism of G onto K. This completes the proof.

#33. Let p be a prime and let Z_p be the integers mod p under addition and multiplication. Let G be the group $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in Z_p$ are such that $ad-bc=1$. Let

$$C=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$$

and let $LF(2,p)=G/C$.

(a) Find the order of $LF(2,p)$.

(b) Prove that $LF(2,p)$ is simple if $p\geq 5$.

118.33 (a) $o(G)=(p+1)p(p-1)$ by (37.26.(b). Hence

$$o(LF(2,p))=\frac{(p+1)p(p-1)}{2}$$

(b) If fact, we prove that G has no normal subgroup H such that $C\subsetneq H\subsetneq G$. Then, by Lemma 2.7.5, $LF(2,p)$ is simple for $p\geq 5$.

Lemmal. G is geneated by

$$\left\{\begin{pmatrix}1&\alpha\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\\beta&1\end{pmatrix} \mid \alpha, \beta\in Z_p\right\}$$ whose

element is called transvection. (Note: transvection in G is like 3-cycle in A_n as we prove A_n

is simple).

pf. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. $ad-bc=1$.

(i) If $c \neq 0$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & c^{-1}(a-1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & c^{-1}(d-1) \\ 0 & 1 \end{pmatrix}.$$

(ii) If $c=0$, then $a \neq 0$ and

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ a & b+d \end{pmatrix}.$$

By (i), $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is also generated by transvections.

This proves the Lemma.

Lemma 2. If a normal subgroup H of G contains a transvection $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$ with $u \neq 0$, then $H=G$.

pf. By Lemma 1, it suffices to prove that H contains every transvection.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$= \begin{pmatrix} 1-uac & ua^2 \\ -uc^2 & 1+uac \end{pmatrix} \in H.$$

$c=0$ implies $\begin{pmatrix} 1 & ua^2 \\ 0 & 1 \end{pmatrix} \in H$ for all $a \in Z_p$.

Since $ua^2 = ub^2$ implies $a = \pm b$, $\Gamma = \{ \lambda \in F \mid \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \in H \}$ is a subgroup of Z_p under addition with elements more than half the elements of Z_p. $\Gamma = K$, by Lagrange's Theorem. Hence, H

contains all transvections of the form $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$.

As the same way, let $a=0$, we know that H contains all transvections of the form $\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$. Hence, if the given transvection is $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, $H=G$. The other case is proved by the same way.

Proof of the exercise: Let H be a normal subgroup of G, which contains a matrix not in C. Suppose H contains $A = \begin{pmatrix} r & 0 \\ s & t \end{pmatrix}$ where $r \neq \pm 1$. Let $S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, then H contains $SAS^{-1}A^{-1} = \begin{pmatrix} 1 & 0 \\ 1-t^2 & 1 \end{pmatrix}$.

$1-t^2 = r^{-2}(r^2-1) \neq 0$. Suppose H contains $A = \begin{pmatrix} r & s \\ 0 & t \end{pmatrix}$ where $r \neq \pm 1$. Let $s = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, then H contains $SAS^{-1}A^{-1} = \begin{pmatrix} 1 & 1-t^2 \\ 0 & 1 \end{pmatrix}$. In both cases, by Lemma 2, we have $G=H$.

To complete the proof, we have only to produce a matrix in H whose top row is $(r \ \ 0)$ where $r \neq \pm 1$ or whose first column is $\begin{pmatrix} r \\ 0 \end{pmatrix}$ where $r \neq \pm 1$. If H contains $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, without loss of generality, we may suppose $a+d \neq 0$ Since otherwise $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2$ will be required. (i) Suppose $c \neq 0$. Let $U = \begin{pmatrix} 0 & -c^{-1} \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -c^{-1} \\ c & d \end{pmatrix}^{-1}$

$= \begin{pmatrix} 0 & -c^{-1} \\ c & a+d \end{pmatrix} \in H.$

$T = \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix}$, H contains $P = TUT^{-1}U^{-1}$

$= \begin{pmatrix} \alpha^{-2} & 0 \\ c(a+d)(\alpha^2-1) & \alpha^2 \end{pmatrix}$. If $p > 5$, Z_p contains an element α with $\alpha^{-2} \neq \pm 1$, i.e. $\alpha^4 \neq 1$ since Z_p has at most four nonzero elements satisfies $x^4 = 1$. In this case, $G = H$. If $p = 5$, then take an α in Z_p with $\alpha^2 - 1 \neq 0$. $\alpha^2 = -1$,

$P = \begin{pmatrix} -1 & 0 \\ x & -1 \end{pmatrix}$, $x \neq 0$. $P^2 = \begin{pmatrix} 1 & 0 \\ -2x & 1 \end{pmatrix}$, $-2x \neq 0$. By Lemma 2, we also have $H = G$.

(ii) Suppose $c = 0$, $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. If $a \neq \pm 1$, then $G = H$. If $a = 1$, then $d = 1$ and $b \neq 0$ since A is not in C. If $a = -1$, then $d = -1$ and $b \neq 0$.

$A = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}$, $A^2 = \begin{pmatrix} 1 & -2b \\ 0 & 1 \end{pmatrix}$, $-2b \neq 0$.

Hence $G = H$. This completes the proof.

#34. Prove that $LF(2, 5)$ is isomorphic to A_5, the alternating group of degree 5.

119.34 In fact, we will show that any simple group G of order 60 is isomorphic to A_5. Since $o(LF(2,5)) = 60$, $LF(2,5) \approx A_5$.

In the following, let G be a simple group of order 60.

Every homomorphism of G is an isomorphism or maps G onto (e) since the kernel of the homomorphism is (e) or G.

There are $3k+1$ 3-Sylow subgroups in G. $3k+1 \mid 60$ implies $3k+1 = 1$, 4 or 10, If $3k+1 = 1$, then the 3-Sylow subgroup is normal in G, contrary to the fact that G is simple. If $3k+1 = 4$, then G can be embeded into S_4 as a permutating group on these four 3-Sylow subgroups. Since $o(S_4) = 24$, G cannot be embedded into S_4. There are 10 3-Sylow subgroups in G. There are 6 5-Sylow subgroups. There are $(3-1) \times 10 = 20$ elements of order 3 and $(5-1) \times 6 = 4 \times 6 = 24$ elements of order 5. $60-20-24-1=15$. G has 15 elements of order different 1, 3 and 5.

In the following, we want to show that there are exactly 5 2-Sylow subgroups in G. Hence G can be embedded into S_5. Since $o(S_5) = 60 = o(G)$. $G \approx S_5$. There are 3, 5 or 15 2-Sylow subgroups.

(i) If there are exactly 3 2-Sylow subgroups, then G can be embedded into S_3. Since $o(S_3) = 3! = 6$, G can not be embedded into S_3.

(ii) If there are exactly 15 2-Sylow subgroups, then at least two such subgroups have a nontrivial intersection, otherwise G has more than 15 elements of order different from 1, 3 and 5 which contradicts a fact we have shown.

Let $h \neq e$ be in the intersection of two dinstinct 2-Sylow subgroups. $o(C_G(h)) > 4$, $4 \mid o(C_G(h))$. $o(C_G(h)) = 4 \cdot 3 = 12$, $o(C_G(h)) = 4 \cdot 5 = 20$ or $o(C_G(h)) = 60$.

(α) $o(C_G(h)) = 60$, $h \in Z(G)$. $Z(G)$ is a nontrivial normal subgroup of G, contrary to the fact that G is simple.

(β) $o(C_G(h)) = 20$. By Theorem 2.9.2, G can be embedded into S_3, a contradiction.

(γ) $o(C_G(h)) = 12$. By Theorem2. 9. 2, G can be

embedded into S_5. Since $o(G) = 60 = o(S_5)$. $G \approx S_5$. But S_5 has only 5 2-Sylow subgroups, a contradiction.

(iii) There are exactly 5's 2-Sylow subgroups. Hence G can be embedded into S_5. $G \approx S_5$.

This completes the proof.

#35. Let $G = LF(2, 7)$; according to Problem 33, G is a simple group of order 168. Determine exactly how many 2-Sylow, 3-Sylow, and 7-Sylow subgroups there are in G.

119.35 $168 = 2^3 \cdot 3 \cdot 7$

(i) There are $7k+1$ 7-Sylow subgroup in G. $7k+1 \mid 168$ implies $7k+1 \mid 24$, $7k+1 = 8$.

(ii) There are $3m+1$ 3-Sylow subgroups in G. $3m+1 \mid 168$ implies $3m+1 \mid 56$. $3m+1 = 4$, 7 or 28.

(α) $3m+1 = 4$, G can be embeded into S_4 as a permutation group acting on the four conjugate 3-Sylow subgroups. Since G is simple, G is isomorphic to a subgroup of S_4. $o(S_4) = 24 < 168$, a contradiction.

(β) $3m+1 = 7$. G can be embedded into S_7 as a permutation group acting on the seven conjugate 3-Sylow subgroups. By (117.20), $o(N(H)) = 168/7 = 2^3 \cdot 3$, where H is a 3-Sylow subgroup of G. N(H) can be viewed as an automorphism group of H. That is, $N(H) \longrightarrow Aut(H)$, the kernel of this homomorphism is C(H). N(H)/C(H) is isomorphic to a subgroup of Aut(H). Since $o(Aut(H)) = 2$ and $o(N(H)) = 2^3 \cdot 3$, $2 \mid o(C(H))$. $o(H) = 3$ implies there is an element g of order 6 in C(H). G isemmbedded into S_7 by σ. $\sigma(g)$ is of order 6. $\sigma(g)$ has fixed H as it acts on the seven conjugate 3-Sylow subgroups. Hence $\sigma(g)$ is a 6-cycle or a product of a 3-cycle and a transposition. In any case, $\sigma(g)$ is an add permutation, which implies that G has a subgroup of index 2, against the simplicity of G.

(γ) Therefore, there are 28 3-Sylow subgroups in G.

(iii) There are $2n+1$ 2-Sylow subgroups in G. $2n+1 \mid 168$, $2n+1 \mid 3 \cdot 7$, $2n+1 = 3$, 7 or 21.

(α) If $2n+1 = 3$, then G can be embedded into S_3. $o(S_3) = 6 < 168$, a contradiction.

(β) Suppose $2n+1 = 7$, G can be embedded into S_7 as a permutation group acting on the seven conjugate 2-Sylow subgroups. The order of any element is the power of a prime. For, there is no element of order $7r$, $r \neq 1$ since G can be viewed as a subgroup of S_7. To prove there is no element of order 3^s with $s > 1$, it suffices to show that G has no element of order 6. Let H be a 3-Sylow subgroup of G. By (β), we have $o(N(H)) = 6$. Assume that G has an element g of order 6. $o(g^2) = 3$. (g^2) is a 3-Sylow subgroup of G. H is conjngate to (g^2) by Sylow's Theorem. Hence, N(H) is conjugate to $N((g^2))$. $o(N((g^2))) = 6$. $(g) \subseteq N((g^2))$. $N((g^2)) = (g)$ is a cyclic subgroup of G. Therefore, N(H) is also a cyclic subgroup of order 6. Let K be a 3-Sylow subgroup of G and $H \neq K$. Then $N(H) \neq N(K)$, otherwise N(H) and N(K) have the same element of order 3 and $H = K$, a contradiction. This shows that for distinit 3-Sylow subgroup H of G we get N(H), the normalizer of H in G, which is a cyclic subgroup of order 6. Thus, we have at least

28·2=56 elements of order 6 in G. There are 168−(7−1)×8−(3−1)·28−56=8 elements of order distinct from 7,3,6. Those elements form the unique 2-Sylow subgroup of G and hence a normal subgroup of G, against the simplicity of G. This meane that G has no element of order 6 and proved our assertion that the order of any element of G is a power of a prime. Hence G contains 168−(7−1)×8−(3−1)×28=64 elements of order 1, 2, 4 or 8. 2n+1=7 implies G contains at most (8−1)×7+1=50 elements of order 1, 2, 4 or 8. This contradiction shows that G contains 21 2-Sylow subgroups.

Topics for Class Discussion

ALPERIN, J. L., "A classification of n-abelian groups," *Canadian Journal of Mathematics*, Vol. XXI (1969), pages 1238–1244.

MCKAY, JAMES, H., "Another proof of Cauchy's group theorem," *American Mathematical Monthly*, Vol. 66 (1959), page 119.

SEGAL, I. E., "The automorphisms of the symmetric group," *Bulletin of the American Mathematical Society*, Vol. 46 (1940), page 565.

A CLASSIFICATION OF n-ABELIAN GROUPS

J. L. ALPERIN

1. Introduction. The concept of an abelian group is central to group theory. For that reason many generalizations have been considered and exploited. One, in particular, is the idea of an n-abelian group (**6**). If n is an integer and $n > 1$, then a group G is n-abelian if, and only if,

$$(xy)^n = x^n y^n$$

for all elements x and y of G. Thus, a group is 2-abelian if, and only if, it is abelian, while non-abelian n-abelian groups do exist for every $n > 2$.

Many results pertaining to the way in which groups can be constructed from abelian groups can be generalized to theorems on n-abelian groups (**1**; **2**). Moreover, the case of $n = p$, a prime, is useful in the study of finite p-groups (**3**; **4**; **5**). Moreover, a recent result of Weichsel (**9**) gives a description of all p-abelian finite p-groups. It is this classification that we wish to extend and simplify. We shall prove the following result.

THEOREM 1. *A group is n-abelian if, and only if, it is a homomorphic image of a subgroup of the direct product of an abelian group, a group of exponent dividing n, and a group of exponent dividing $n - 1$.*

Abelian groups and groups of exponent dividing n are clearly n-abelian. Moreover, if G is a group of exponent dividing $n - 1$ and x is an element of G, then $x^n = x$, the nth power map is the identity map and again G is n-abelian. Furthermore, direct products, subgroups, and homomorphic images of n-abelian groups are also n-abelian so that half of the theorem is now obvious. It remains to show that an arbitrary n-abelian group can be so described. This can also be rephrased in terms of varieties of groups: The join of the varieties of abelian groups, groups of exponent dividing n, and groups of exponent dividing $n - 1$ is the variety of n-abelian groups. Here, as always, we implicitly assume that $n > 1$.

We shall also derive two consequences of the above theorem for finite groups.

COROLLARY 1. *A finite group is n-abelian if, and only if, it is a homomorphic image of a subgroup of the direct product of a finite abelian group, a finite group of exponent dividing n and a finite group of exponent dividing $n - 1$.*

Received May 15, 1968. This work has been partially supported by NSF Grant NSF GP 6379

While the statement of the preceding result is just that of the theorem with "group" replaced by "finite group", it is not an immediate consequence and requires a lemma which may be of some independent interest.

The next assertion is a direct consequence of the corollary just given.

COROLLARY 2 (Weichsel (9)). *A finite p-group is p-abelian if, and only if, it is a homomorphic image of a subgroup of the direct product of a finite abelian p-group and a finite p-group of exponent p.*

Our notation is all quite standard. For example, if x and y are elements of the group G, then

$$[x, y] = x^{-1}y^{-1}xy, \qquad x^y = y^{-1}xy.$$

Moreover, if k is a positive integer, then G^k is the subgroup of G generated by all kth powers of elements of G.

The remainder of this paper is organized in the following manner. Section 2 contains a proof of Theorem 1, § 3 is devoted to a useful lemma and the derivation of the two corollaries, while § 4 contains a short and direct proof of the last of these corollaries.

2. The proof of Theorem 1. The heart of the argument is contained in two lemmas, the first of which consists of a number of identities while the second is, in fact, a special case of the theorem.

LEMMA 1. *If x and y are elements of an n-abelian group, then*

(a) $(xy)^{n-1} = y^{n-1}x^{n-1}$,
(b) $[x, y]^n = [x^n, y]$,
(c) $[x, y]^{n-1} = [y, x^{-(n-1)}]$,
(d) $[x^n, y^{n-1}] = 1$,
(e) $[x, y]^{n(n-1)} = 1$.

The results in this lemma are more or less contained in (**1**; **2**); we give the proofs for the convenience of the reader.

Proof. Each assertion follows from a direct and simple calculation.

(a) $(xy)^{n-1} = ((yx)^y)^{n-1} = ((yx)^{n-1})^y = ((yx)^n x^{-1}y^{-1})^y$
$= (y^n x^n x^{-1}y^{-1})^y = y^{n-1}x^{n-1}$.

(b) $[x, y]^n = (x^{-1}x^y)^n = x^{-n}(x^y)^n = (x^n)^{-1}(x^n)^y = [x^n, y]$.

(c) $[x, y]^{n-1} = (x^{-1}x^y)^{n-1} = (x^y)^{n-1}x^{-(n-1)}$ (by (a))
$= (x^{n-1})^y x^{-(n-1)} = [y, x^{-(n-1)}]$.

(d) $(x^n)^y = (x^y)^n = (y^{-1}xy)^n = (y^n)^{-1}x^n y^n$ so that $y^{n-1}x^n = x^n y^{n-1}$, as desired.

(e) $[x, y]^{n(n-1)} = [y, x^{-(n-1)}]^n$ (by (c)) $= [y^n, x^{-(n-1)}]$ (by (b)) $= 1$ (by (d)).

LEMMA 2. *If G is an n-abelian group and G/G' is torsion-free, then*

$$G' \cap G^n \cap G^{n-1} = 1.$$

Proof. Let g be any element of the intersection; we shall prove that g is the identity. First, $g \in G^n$, hence g equals a product of nth powers of elements of G. However, G is n-abelian, thus g is an nth power and $g = h^n$, for some h in G. Moreover, $h \in G^{n-1}$. Indeed, if $h \notin G^{n-1}$, then $g = h^n \notin G^{n-1}$ since n and $n - 1$ are relatively prime. Thus, h equals a product of $(n - 1)$st powers, thus $h = k^{n-1}$, $k \in G$, by Lemma 1 (a). Furthermore, $k \in G'$ as $g \in G'$, $k^{n(n-1)} = g$ and G/G' is torsion-free. Thus, there is a positive integer r and elements x_i, y_i, $1 \leqq i \leqq r$, of G such that

$$k = [x_1, y_1] \cdots [x_r, y_r].$$

Hence, as G is n-abelian,

$$k^n = [x_1, y_1]^n \cdots [x_r, y_r]^n$$

and, by Lemma 1 (a),

$$k^{n(n-1)} = [x_r, y_r]^{n(n-1)} \cdots [x_1, y_1]^{n(n-1)}.$$

However, each factor of this product is the identity, by Lemma 1 (e), thus $g = k^{n(n-1)} = 1$, as desired. This proves the lemma.

Proof of Theorem 1. Let H be an arbitrary n-abelian group and let F be a free group which has H as a homomorphic image. Furthermore, let R be the least normal subgroup of F with n-abelian quotient group and set $G = F/R$. Since H is n-abelian, it follows that H is a homomorphic image of G. Hence, we need only prove that G is isomorphic with a subgroup of the direct product of an abelian group, a group of exponent dividing n, and a group of exponent dividing $n - 1$.

However, $F' \supseteq R$ as F/F' is certainly n-abelian, thus $G/G' \simeq F/F'$ and is torsion-free. Thus, Lemma 2 yields

$$G' \cap G^n \cap G^{n-1} = 1.$$

Thus, the kernel of the homomorphism of H into the direct product of G/G', G/G^n, and G/G^{n-1} is trivial, and the proof is complete.

3. Derivation of the corollaries. At this point we need to recall a few elementary definitions and facts. A quotient of a subgroup of a group G is called a *section* of G. Moreover, if H is a group isomorphic with a section of G, then we shall say that H *is* a section of G.

We also have to review the description of subgroups of a direct product. Let A_1 and A_2 be groups and assume that H is a subgroup of the direct product $A_1 \times A_2$. The projection of H in A_1 is the subgroup P_1 of A_1 consisting of all $a_1 \in A$ such that there is $a_2 \in A_2$ with $(a_1, a_2) \in H$. The intersection I_1 of H

and A_1 is the subgroup of A_1 consisting of all $a_1 \in A_1$ with $(a_1, 1) \in H$. The projection P_2 and intersection I_2 of H with A_2 are defined similarly. It follows that I_i is normal in P_i, $i = 1, 2$, the corresponding quotients are isomorphic, and there is an isomorphism θ of P_1/I_1 onto P_2/I_2 such that (a_1, a_2) is in H if, and only if, $a_i \in P_i$, $i = 1, 2$, and $(I_1 a_1)\theta = I_2 a_2$.

The key step in the derivation of Corollary 1 from Theorem 1 is an application of the following result.

LEMMA 3. *If G is a finite group which is a section of the direct product $A_1 \times A_2$ of groups A_1 and A_2, then G is a section of the direct product of finite sections S_1 and S_2 of A_1 and A_2, respectively, provided any finitely generated group which is a section of A_1 and A_2 is finite.*

We have been unable to remove the condition on finitely generated groups and we strongly suspect the lemma is false without some such hypothesis.

Proof. Let G be isomorphic with X/K, where X is a subgroup of $A_1 \times A_2$ and K is a normal subgroup of X. We assert that we may assume that X is finitely generated. Indeed, given an isomorphism of X/K onto G, choose for each $g \in G$ an element of X mapped to g and let X_0 be the subgroup of X generated by this finite set of elements. It follows that the given map of X/K onto G induces an isomorphism of $X_0/X_0 \cap K$ onto G so that we may replace X by X_0.

Let X_i and Y_i be the projection and intersection, of X with A_i, $i = 1, 2$, respectively. Let $Y = Y_1 \times Y_2$ so that Y is a normal subgroup of X as Y_i is normal in X_i, $i = 1, 2$, and $X \subseteq X_1 \times X_2$. Let $L = Y \cap K$ so that L is also a normal subgroup of X. Moreover, let L_i be the intersection of L and A_i, $i = 1, 2$, thus $L_i \subseteq Y_i$ as $L \subseteq Y$. We now claim that the following assertions hold:

(1) L_i is a normal subgroup of X_i, $i = 1, 2$;
(2) The index of L_i in X_i is finite, $i = 1, 2$;
(3) G is a section of $X_1/L_1 \times X_2/L_2$.

Once these three statements are established, our proof will be complete by taking $S_i = X_i/L_i$, $i = 1, 2$.

The last assertion is easy to prove. Indeed $L_1 \times L_2 \subseteq L \subseteq K$, thus we have

$$L_1 \times L_2 \subseteq K \subseteq X \subseteq X_1 \times X_2$$

and X/K is a section of $X_1 \times X_2/L_1 \times L_2$ which is isomorphic with $X_1/L_1 \times X_2/L_2$.

As for the first statement, $L_i \subseteq X_i$ as we have just seen. Moreover,

$$L_1 \times 1 = (A_1 \times 1) \cap L,$$

hence $L_1 \times 1$ is normal in X. Thus, the image X_1 of X in the projection on A_1 normalizes the image L_1 of $L_1 \times 1$. Similarly, L_2 is normal in X_2.

Finally, we establish (2). First, we know that X_1/Y_1 and X_2/Y_2 are isomorphic, by the remarks preceding the statement of the lemma. Moreover, X is finitely generated, hence X_i is also, $i = 1, 2$, being a homomorphic image of X. Thus, by our hypothesis, X_i/Y_i is finite. However, $L \subseteq Y$ hence $L_i \subseteq Y_i$ and we, therefore, only need to demonstrate that Y_i/L_i is finite.

For this purpose, let M_i be the projection of L on A_i, $i = 1, 2$, thus $L_i \subseteq M_i \subseteq Y_i$, L_i is normal in M_i, and there is an isomorphism θ of M_1/L_1 onto M_2/L_2 so that $(m_1, m_2) \in M_1 \times M_2$ lies in L if, and only if, $(L_1 m_1)\theta = L_2 m_2$. We set $M = M_1 \times M_2$.

Now Y/L is finite since $Y/L = Y/Y \cap K$ is isomorphic with a subgroup of X/K. Hence, the projection M_i of L on A_i has finite index in the projection Y_i of Y on A_i. Moreover, $L_i \subseteq M_i \subseteq Y_i$, thus it remains only to show that M_i/L_i is finite, $i = 1, 2$. However, M/L is finite, being a subgroup of Y/L. Hence, it suffices to show that there is a one-to-one map of M_1/L_1 into M/L.

If $t \in M_1$, we map $L_1 t \in M_1/L_1$ to $L(t, 1)$ and $L(t, 1) \in M/L$ since $M = M_1 \times M_2$. This is well-defined since $x \in L_1$ yields $L(xt, 1) = L(t, 1)$ as $(x, 1) \in L$. Moreover, suppose that $s \in M_1$ and $L(t, 1) = L(s, 1)$. This implies that $(ts^{-1}, 1) \in L$. Hence $(L_1 ts^{-1})\theta = L_2$, and thus $ts^{-1} \in L_1$ and $L_1 s = L_1 t$ and the map is one-to-one. This proves the second assertion and establishes the lemma.

We are now ready to prove the corollaries.

Proof of Corollary 1. As for the theorem, we need only show that a finite n-abelian group has the desired structure. However, if G is such a group, then G is a section of the direct product of an abelian group A, a group A_n of exponent dividing n, and a group A_{n-1} of exponent dividing $n - 1$. A finitely generated group which is a section of A and a section of $A_n \times A_{n-1}$ is finite as it is finitely generated, abelian, and of finite exponent. Thus, by Lemma 3, G is a section of $B \times C$, where B is a finite section of A and C is a finite section of $A_n \times A_{n-1}$. Moreover, any group which is a section of A_n and a section of A_{n-1} is the identity, as n and $n - 1$ are relatively prime, thus again by Lemma 3, C is a section of $B_n \times B_{n-1}$, where B_n is a finite section of A_n and B_{n-1} is a finite section of A_{n-1}. Thus, G is a section of $B \times B_n \times B_{n-1}$, and the result is established.

Proof of Corollary 2. Let P be a p-abelian finite p-group. By the previous result, P is a section of the direct product of a finite abelian group B, a finite group B_p of exponent dividing p, and a finite group B_{p-1} of exponent dividing $p - 1$. Now B is the direct product of a p-subgroup B_0 and a subgroup B' of order prime to p, thus P is a section of $A_p \times A'$, where $A_p = B_0 \times B_p$ and $A' = B' \times B_{p-1}$. We need only see that P is a section of A_p.

However, suppose that P is isomorphic to X/Y, where X and Y are subgroups of $A_p \times A'$ and Y is normal in X. However, A_p and A' are of coprime orders, thus $X = X_p \times X'$ and $Y = Y_p \times Y'$, where X_p and X' are the projections of X on A_p and A', and Y_p and Y' are the projections of Y on A and A'. Thus,

$$P \simeq X_p/Y_p \times X'/Y'.$$

However, X'/Y' has order prime to p, thus $Y' = X'$, $P \simeq X_p/Y_p$, and P is a section of A_p.

As in all the above cases, the other half of the corollary is obvious and the proof is, therefore, complete.

4. Another proof of Corollary 2. The arguments we have developed give a short direct proof of Weichsel's theorem and avoid the appeal to stronger results. For this reason, we sketch the quick argument.

Let P be a p-abelian finite p-group. Suppose that P is a d-generator group of class of nilpotence c and exponent p^e, where c, d, and e are positive integers. Let F be a free group on a set of d free generators. Let R be the least normal subgroup of F whose quotient is nilpotent of class at most c, has exponent dividing p^e, and is p-abelian. Let $G = F/R$, thus G is a finite p-group as it is finitely generated, nilpotent, and of exponent dividing p^e. Moreover, P is a homomorphic image of G since P is an image of F and the corresponding kernel must contain R. Hence, we need only show that G is isomorphic with a subgroup of the direct product of a finite abelian p-group and a finite p-group of exponent dividing p.

However, there is a homomorphism of G into $G/G' \times G/G^p$ constructed from the natural maps of G onto G/G' and G onto G/G^p. The kernel of this homomorphism is $G' \cap G^p$, thus we need only prove that $G' \cap G^p = 1$ inasmuch as G/G' is a finite abelian p-group and G/G^p is finite and of exponent p.

To do this we first remark that $G\ G'$ is the direct product of d cyclic groups of order p^e. Indeed, such a direct product is a d-generator p-abelian group of class one and exponent p^e and hence is a homomorphic image of G and consequently of G/G'. On the other hand, G/G' is an abelian p-group on d generators and of exponent dividing p^e, thus it is as described. In particular, any element of $G\ G'$ of order dividing p is equal to the p^{e-1}st power of an element of G/G'.

Finally, suppose that $g \in G' \cap G^p$; we shall show that $g = 1$ and conclude the proof. Since $g \in G^p$ and G is p-abelian, we have: $g = h^p$ for some h in G. However, $g \in G'$, thus $(G'h)^p = 1$ and $h = x^{p^{e-1}}y$, where $x \in G$, $y \in G'$, by our remarks above. Hence $h^p = x^{p^e}y^p = y^p$ as G is p-abelian of exponent p^e. However,

$$y = [x_1, y_1] \cdots [x_r, y_r]$$

for suitable x_i, y_i in G, $1 \leqq i \leqq r$. Thus

$$g = h^p = y^p = [x_1, y_1]^p \cdots [x_r, y_r]^p.$$

However, $[x_i, y_i]^p = 1$, by Lemma 1 (e), since G is a p-group. Thus, $g = 1$, as desired.

5. Concluding remarks. Our main result also has some consequences in a slightly different direction. Indeed, it is an easy consequence of Theorem 1 that a group, in which the taking of nth powers is an automorphism, is a homomorphic image of a subgroup of the direct product of an abelian group and a group of exponent dividing $n - 1$. This result, in turn, leads to easy derivations of the results of Trotter (8).*

REFERENCES

1. Reinhold Baer, *Endlichkeitskriterien für Kommutatorgruppen*, Math. Ann. *124* (1952), 161–167
2. ——— *Factorizations of n-soluble and n-nilpotent groups*, Proc. Amer. Math. Soc. *4* (1953), 15–26.
3. Otto Grün, *Beiträge zur Gruppentheorie. IV. Über eine Charakteristische Untergruppe*, Math. Nach. *3* (1949), 77–94.
4. ——— *Beiträge zur Gruppentheorie. V*, Osaka Math. J. *5* (1953), 117–146.
5. C. Hobby, *A characteristic subgroup of a p-group*, Pacific J. Math. *10* (1960), 853–858.
6. F. Levi, *Notes on group theory. I*, J. Indian Math. Soc. *8* (1944), 1–7.
7. ——— *Notes on group theory. VII*, J. Indian Math. Soc. *9* (1945), 37–42.
8. H. F. Trotter, *Groups in which raising to a power is an automorphism*, Can. Math. Bull. *8* (1965), 825–827.
9. P. M. Weichsel, *On p-abelian groups*, Proc. Amer. Math. Soc. *18* (1967), 736–737.

Northeastern University.
Boston, Massachusetts;
University of Chicago,
Chicago, Illinois

*I thank the referee for pointing out this paper to me.

MATHEMATICAL NOTES

EDITED BY ROY DUBISCH, Fresno State College

Material for this department should be sent to Roy Dubisch, Department of Mathematics, Fresno State College, Fresno 26, California

ANOTHER PROOF OF CAUCHY'S GROUP THEOPEM

JAMES H McKAY, Seattle University

Since $ab=1$ implies $ba=b(ab)b^{-1}=1$, the identities are symmetrically placed in the group table of a finite gronp. Each tow of a group table contains exactly one identity and thus if the group has even order, there are an even number of identities on the main diagonal Therefore, $x^2=1$ has an even number of solutions.

Generalizing this observation, we obtain a simple proof of Cauchy's theorem. For another proof see [1].

CAUCHY'S THEOREM. *If the prime p divides the order of a finite group G, then G has kp solutions to the equation $x^p=1$.*

Let G have order n and denote the identity of G by 1. The set

$$S=\{(a_1,\cdots,a_p)\mid a_i\in G,\ a_1a_2\cdots a_p=1\}$$

has n^{p-1} members. Define an equivalence relation on S by saying two p-tuples are equivalent if one is a cyclic permutation of the other.

If all components of a p-tuple are equal then its equivalence class coatains only one member. Otherwise, if two components of a p-tuple are distinct, there are p members in the equivalence class.

Let r denote the number of solutions to the equation $x^n=1$. Then r equals the number of equivalence classes with only one member. Let s denote the number of equivalence classes with p members. Then $r+sp=n^{p-1}$ and thas $p\mid r$.

Reference

1. G A. Miller, On an extension of Sylow's theorem, Bull Amer. Math. Soc., vol. 4, 1898, pp. 323–327.

A REMARK ON BOUNDED FUNCTIONS

V. F. COWLING, University of Kentucky

Denote by E the class of functions regular and bounded by unity in $|z|<1$. Denote by E^* the subclass of functions of E which are in addition univalent in $|z|<1$. Analogies of various inequalities which are known to hold for functions in the class E have been obtained for functions of the class E^*. For example, it is known [3] that there exist functions in E for which the sequence $\{a_0+\cdots+a_n\}$ $(f(z)=\sum a_nz^n)$ is unbounded. On the other hand, it is shown by Fejer in [1] that if $f\in E^*$ then $|a_0+\cdots+a_n|<1+(1/\sqrt{2})$ for all n.

THE AUTOMORPHISMS OF THE SYMMETRIC GROUP

IRVING E. SEGAL

The purpose of this note is to give a proof of the following well known theorem. *The group of automorphisms of the symmetric group S_n on n letters is isomorphic with S_n, except when $n=6$.* The proofs of this in the literature are complicated[1] and involve the use of lemmas whose relevance is not plain.

Let A be an automorphism of S_n. Then it is clear that A takes a class of similar elements into a class of similar elements, and that it takes an element of order m into an element with the same order. Hence suppose $A(1r)=t_1(r)\cdot t_2(r)\cdot\cdots\cdot t_k(r)$ $(k\geqq 1)$, where the $t_i(r)$ are disjoint transpositions. A simple calculation shows that there are $n(n-1)/2$ elements similar to $(1r)$, and that there are $n!/2^kk!(n-2k)!$ elements similar to $t_1(r)\cdot t_2(r)\cdot\cdots\cdot t_k(r)$. Hence

$$\frac{n(n-1)}{2}=\frac{n!}{2^kk!(n-2k)!}.$$

If $n\neq 6$ this equation is satisfied for no k $(k\geqq 1)$ except $k=1$.

Suppose now that $n\neq 6$. Then $A(1r)=(a_rb_r)$ say. If $r\neq 2$, $(12)(1r)=(12r)$ (multiplying from right to left), and evidently, $A(12r)=(12r)$ $=(a_2b_2)(a_rb_r)$. Since $(12r)$ has the order 3, so has $(a_2b_2)(a_rb_r)$ and the transpositions (a_2b_2) and (a_rb_r) must have a letter in common. Then it is no loss to assume $a_2=a_r$ or $b_2=b_r$. However, if $a_2=a_r$ and $b_2=b_s$ $(r\neq 2,\ s\neq 2)$, then $r\neq s$ and $A(12r)=A(12)\cdot A(1r)=(a_2b_2)(a_2b_r)$ $=(b_ra_2b_2)$. Similarly $A(12s)=(a_sb_2a_2)$. Hence $A((12r)\cdot(12s))=A(12r)$ $\cdot A(12s)=(b_ra_2b_2)(a_sb_2a_2)=(b_ra_sb_2)$ which is of order 3, while $(12r)$ $\cdot(12s)=(1s)(2r)$, which is of order 2. Hence one must have $a_2=a_r$ for all r or $b_2=b_r$ for all r; of course one can let $a_2=a_r$ $(r=2,3,\cdots,n)$. Then $A(1r)=(a_2b_r)$. Hence A is precisely the automorphism A defined by $Ax=t^{-1}xt$, where

$$t=\begin{pmatrix}1 & 2 & \cdots & r & \cdots & n\\ a_2 & b_2 & \cdots & b_r & \cdots & b_n\end{pmatrix}.$$

For $Ax=t^{-1}xt$ when $x=(1r)$, and the elements $\{(1r)\}$ $(r=2,3,\cdots,n)$ generate S_n.

YALE UNIVERSITY

[1] The first proof is by O. Hölder, Mathematische Annalen, vol. 46 (1895), especially pp. 340–345.

3 Ring Theory

3.2 Some Special Classes of Rings

R is a ring in all the problems.

1. If $a, b, c, d \in R$, evaluate $(a + b)(c + d)$.

130.1 $(a+b)(c+d) = (a+b)c+(a+b)d = ac+bc+ad+bd$.

2. Prove that if $a, b \in R$, then $(a + b)^2 = a^2 + ab + ba + b^2$, where by x^2 we mean xx.

130.2 In (130.1) let $c=a$, $d=b$ we have
$(a+b)^2 = (a+b)(a+b) = a\cdot a+b\cdot a+a\cdot b+b\cdot b$
$= a^2+ab+ba+b^2$

3. Find the form of the binomial theorem in a general ring; in other words, find an expression for $(a + b)^n$, where n is a positive integer.

130.3 $(a+b)^n = \sum (x_1 \cdots\cdots x_n)$, where the summation runs over all elements of length n with $x_1 = a$ or b.

4. If every $x \in R$ satisfies $x^2 = x$, prove that R must be commutative. (A ring in which $x^2 = x$ for all elements is called a *Boolean* ring.)

130.4 $x, y \in R$, $x+y = (x+y)^2 = x^2+xy+yx+y^2$
$= x+xy+yx+y$, $xy+yx = 0$, $xy = -yx$,
$(-yx) = (-yx)^2 = (-yx)(-yx) = (yx)^2$
$= yx$, $xy = -yx = yx$ for all x, y in R. R is commutative.

5. If R is a ring, merely considering it as an abelian group under its addition, we have defined, in Chapter 2, what is meant by na, where $a \in R$ and n is an integer. Prove that if $a, b \in R$ and n, m are integers, then $(na)(mb) = (nm)(ab)$.

130.5 We prove $a(mb) = m(ab)$ at first.
$m = 0$ is a trivial case. Suppose it holds for $m \in N$, ie. $a(mb) = m(ab)$.

Then $a(mb) = m(ab)$, $a((m+1)b)$
$= a(mb+b) = a(mb)+ab = m(ab)+ab$
$= (m+1)ab$.
Therefore, $a(mb) = m(ab)$ holds for all nonnegative integers. If $m < 0$, $-m > 0$,
$a((-m)b) = (-m)(ab)$, $(-m)b = -(mb)$,
$(-m)(ab) = -(mab)$, $a(-(mb)) = -(mab)$
$\therefore -(a(mb)) = -(m(ab))$
$\therefore a(mb) = m(ab)$.
As the same way, $(na)b = n(ab)$.
Hence $(na)(mb) = n(a(mb)) = n(m(ab))$
$= mn(ab)$.

6. If D is an integeral domain and D is of finite characteristic, prove that the characteristic of D is a prime number.

130.6 Let p be the smallest pozitive integer such that $pa = 0$ for all $a \in D$. Suppose $na = 0$, n a positive integer $a \in D \setminus (0)$.
Then $a(nb) = n(ab) = (na)b = 0\cdot b = 0$ for all b in D. Since D is an integral domain $nb = 0$ for all b in D. Now, suppose $p = rs$. $r > 1$, $s > 1$, then let $x \in D \setminus 0$,
$0 = px = (rs)x = r(sx)$. If $sx \neq 0$, by our above argument $rb = 0$ for all b in D, $0 < r < p$, a contradiction.
Hence $sx = 0$, but also $sb = 0$ for all b in D, $0 < s < p$, a contradiction.
Therefore, p is a prime number.

7. Give an example of an integral domain which has an infinite number of elements, yet is of finite characteristic.

130.7 $J_p[x]$: the polynomial ring over the ring J_p.

8. If D is an integral domain and if $na = 0$ for some $a \neq 0$ in D and some integer $n \neq 0$, prove that D is of finite characteristic.

130.8 $na=0$, $\forall b\in D$, $(na)b=0$ $\therefore a(nb)=0$,
$a\neq 0$, $nb=0$. ie. $nb=0$ for all b in D.
D is of finite characteristic.

9. If R is a system satisfying all the conditions for a ring with unit element with the possible exception of $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring. (*Hint:* Expand $(a + b)(1 + 1)$ in two ways.)

130.9 $(a+b)(1+1)=(a+b)\cdot 1+(a+b)\cdot 1$
$=a+b+a+b$
$(a+b)(1+1)=a(1+1)+b(1+1)$
$=a+a+b+b$ $\therefore b+a=a+b$.

10. Show that the commutative ring D is an integral domain if and only if for $a, b, c \in D$ with $a \neq 0$ the relation $ab = ac$ implies that $b = c$.

130.10 If D is an integral domain , $ab=ac$
implies $ab-ac=0$. $a(b-c)=0$, $a\neq 0$
hence $b-c=0$ and $b=c$.
Suppose for $a, b, c\in D$ with $a\neq 0$ the relation
$ab=ac$ implies $b=c$.
Suppose $ab=0$ and $a\neq 0$. Let $c=0$,
then $ab=0=a\cdot 0=a\cdot c$ Hence $b=c=0$.
D is an integral domain.

11. Prove that Lemma 3.2.2 is false if we drop the assumption that the integral domain is finite.

130.11 Rational integers form an infinite integral domain but not a field.

12. Prove that any field is an integral domain.

130.12 A field R is a commutative division ring.
$x, y\in R\setminus(0)$, Since the nonzero elements of
R form a group under multiplication.
$x\cdot y\in R\setminus(0)$ by closed law. $x\cdot y\neq 0$.
Hence R is an integral domain.

13. Useing the pigeonhole principle, prove that if m and n are relatively prime integers and a and b are any integers, there exists an integer x such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$. (*Hint:* Consider the remainders of $a, a + m, a + 2m, \ldots, a + (n - 1)m$ on division by n.)

130.13 Consider the remainders of a , $a+m$, $a+2m$,
$\cdots\cdots$, $a+(n-1)m$ on division by n.
All the remainders of a , $a+m$, $\cdots\cdots$, $a+(n-1)m$
on division by n are distinct.
For if $a+im\equiv a+jm \pmod n$,
$im\equiv jm \pmod n$, $i\equiv j \pmod n$ since
$(m,n)=1$. $i=j$.
The remainder of b on division by n equals one
of that of a , $a+m$, $\cdots\cdots$, $a+(n-1)m$,
say $a+im$.
Then let $x=a+im$. $x\equiv a \pmod m$,
$x\equiv a+im\equiv b \pmod n$.

14. Using the pigeonhole principle, prove that the decimal expansion of a rational number must, after some point, become repeating.

130.14 Let $a.a_1a_2\cdots\cdots a_k\cdots\cdots$ be the decimal expansion of the rational number $\frac{m}{n}$, m , n be natural numbers. Then

$$\begin{aligned}
m &= a\,n+b_1 && , \quad 0\leq b_1<n\\
10\,b_1 &= a_1n+b_2 && , \quad 0\leq b_2<n\\
10\,b_2 &= a_2n+b_3 && , \quad 0\leq b_3<n\\
&\vdots && \vdots\\
10\,b_k &= a_kn+b_{k+1} && , \quad 0\leq b_{k+1}<n\\
&\vdots && \vdots
\end{aligned}$$

Since there are only n nonnegative integers less than n, by pigeonhole principle, we have
$b_i=b_j$ for some $i\neq j$.
Then $10b_{i+1}=10b_{j+1}$ implies $a_{i+1}=b_{j+1}$ and $a_{i+2}=b_{j+2}\cdots\cdots$, The decimal expansion of m/n must , after some point, become repeating.

3.4 Ideals and Quotient Rings.

1. If U is an ideal of R and $1 \in U$, prove that $U = R$.

135.1 For any x in R, $x = 1 \cdot x$. Since $1 \in U$ and U is an ideal of R, $x \in U$ by definition of "ideal". $R \subset U$, $U \subset R$. Hence $U = R$.

2. If F is a field, prove its only ideals are (0) and F itself.

135.2 Let U be a nonzero ideal of F. Since $U \neq (0)$, there is $x \in U$ with $x \neq 0$, $x^{-1} \in F$. $1 = x \cdot x^{-1} \in U$. By (135.1), $U = F$. (0) and F are actually ideals of F. Therefore, the only ideals of F are (0) and F.

3. Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.

135.3 Since the kernel of any homomorphism is an ideal. By (135.2), the kernel is (0) or the field itself. If the kernel is (0), the homomorphism is an isomorphism. If the kernel is the field itself, then it takes each element into 0.

4. If R is a commutative ring and $a \in R$,
   (a) Show that $aR = \{ar \mid r \in R\}$ is a two-sided ideal of R.
   (b) Show by an example that this may be false if R is not commutative.

135.4 (a) $ar, ar' \in aR$, $ar - ar' = a(r - r') \in aR$. $ar \in aR$, $r' \in R$, imply $(ar)r' = a(rr') \in aR$ and $r'(ar) = (ar)r' = a(rr') \in aR$. By definition, aR is an ideal of R.

(b) Let $R = \left\{ \begin{pmatrix} x & y \\ z & u \end{pmatrix} \mid x, y, z, u \in F \right\}$, F is a field. $a = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $aR = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in F \right\}$ is not an ideal of R since $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} a = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin aR$.

5. If U, V are ideals of R, let $U + V = \{u + v \mid u \in U, v \in V\}$. Prove that $U + V$ is also an ideal.

135.5 $(u+v)-(u'+v') = (u-u')+(v-v') \in U+V$ for all $u, u' \in V$ and $v, v' \in V$. $a(u+v) = au+av \in U+V$ for all $u \in U$, $v \in V$ and $a \in R$. $(u+v)a = ua+va \in U+V$ for all $u \in U$, $v \in V$ and $a \in R$. Hence $U+V$ is an ideal of R.

6. If U, V are ideals of R let UV be the set of all elements that can be written as finite sums of elements of the form uv where $u \in U$ and $v \in V$. Prove that UV is an ideal of R.

135.6 $x, y \in U \cdot V$, then $x = \sum uv$ $y = \sum u'v'$, $x - y = \sum uv - u'v'$. $x - y \in U \cdot V$. $x \in U$, then $x = \sum uv$, $a \in R$, $ax = \sum auv = \sum (au)v \in U \cdot V$ and $xa = \sum uva = \sum u(va) \in U \cdot V$.

7. In Problem 6 prove that $UV \subset U \cap V$.

135.7 $x \in U \cdot V$. Then $x = u_1v_1 + \cdots\cdots + u_nv_n$, where $u_1, \cdots\cdots, u_n \in U$ and $v_1, \cdots\cdots, v_n \in V$. $u_iv_i \in U$, $u_iv_i \in V$. Hence $\sum u_iv_i \in U$ and $\sum u_iv_i \in V$, $x = \sum u_iv_i \in U \cap V$. $U \cdot V \subset U \cap V$.

8. If R is the ring of integers, let U be the ideal consisting of all multiples of 17. Prove that if V is an ideal of R and $R \supset V \supset U$ then either $V = R$ or $V = U$. Generalize!

135.8 If R is the ring of all integers, let U be the ideal consisting of all multiplies of p (p is a prime number), then if V is an ideal of R and $R \supset V \supset U$, we have $V = R$ or $V = U$.
pf. If $V \neq U$, let $a \in V \setminus U$. $a = rp + s$, $0 < s < p$. $rp \in U \subset V$, $a \in V$ implies $s \in V$. $(s, p) = 1$, There are h, k such that $hs + kp = 1$ $hs \in V$, $kp \in V$ since V is an ideal of R. By (135.1), $V = R$.

9. If U is an ideal of R, let $r(U) = \{x \in R \mid xu = 0 \text{ for all } u \in U\}$. Prove that $r(U)$ is an ideal of R.

136.9 $x, y \in r(U)$. $(x-y)u = xu - yu = 0$ for all $u \in U$ hence $x-y \in r(U)$. $x \in r(U)$.
$(xr)u = x(ru) = 0$ for all $r \in R$, $u \in U$ $ru \in U$.
$xr \in r(U)$, $x \in r(U)$. $(rx)u = r(xu) = 0$ for all $r \in R$, $u \in U$. $rx \in r(U)$.
$r(U)$ is an ideal of R.

10. If U is an ideal of R let $[R:U] = \{x \in R \mid rx \in U \text{ for every } r \in R\}$. Prove that $[R:U]$ is an ideal of R and that it contains U.

136.10 $r(x-y) = rx - ry \in U$ for all $x, y \in [R,U]$ and $r \in R$. $r(ax) = (ra)x \in U$, $r(x \cdot a) = (rx) \cdot a \in U$, $[R:U]$ is an ideal of R. Since U is an ideal of R, for all x in U and r in R, we have $rx \in U$, $x \in [R:U]$, $[R:U]$ contains U.

11. Let R be a ring with unit element. Using its elements we define a ring $\tilde{R}$ by defining $a \oplus b = a + b + 1$, and $a \cdot b = ab + a + b$, where $a, b \in R$ and where the addition and multiplication on the right-hand side of these relations are those of R.
(a) Prove that $\tilde{R}$ is a ring under the operations $\oplus$ and $\cdot$
(b) What acts as the zero-element of $\tilde{R}$?
(c) What acts as the unit-element of $\tilde{R}$?
(d) Prove that R is isomorphic to $\tilde{R}$.

136.11 (a) It's very easy to check that $[\widetilde{R}; \oplus, \odot]$ is a ring.
(b) -1
(c) $a \odot 0 = a \cdot 0 + a + 0 = a$,
$0 \odot a = 0 \cdot a + 0 + a = a$.
Hence 0 is the unit-element of $\widetilde{R}$.
(d) Define $\theta(a) = a - 1$ for all $a \in R$.
$\theta(a \cdot b) = a \cdot b - 1$.
$\theta(a) \odot \theta(b) = (a-1) \odot (b-1)$
$= (a-1)(b-1) + (a-1) + (b-1)$
$= ab - a - b + 1 + a + b - 1 - 1 = ab - 1$.
$\theta(a \cdot b) = \theta(a) \odot \theta(b)$.
$\theta(a) \oplus \theta(b) = (a-1) \oplus (b-1)$
$= (a-1) + (b-1) + 1 = a + b - 1 = \theta(a+b)$.
If $\theta(a) = \theta(b)$, $a-1 = b-1$, $a = b$,
θ is an isomophism of R into $\widetilde{R}$.
For any x in $\widetilde{R}$, $\theta(x+1) = (x+1) - 1 = x$
θ is onto. θ is an isomorphism of R onto $\widetilde{R}$. Therefore R is isomphic to $\widetilde{R}$.

*12. In Example 3.1.6 we discussed the ring of rational 2 × 2 matrices. Prove that this ring has no ideals other than (0) and the ring itself.

136.12 Suppose U is a nonzero ideal of R.
$a = \sum_{i,j=1}^{2} \alpha_{ij} e_{ij} \in U \setminus 0$. let's say $\alpha_{rs} \neq 0$.
Now, $e_{rr} a e_{ss} = \alpha_{rs} e_{rs} \in U$,
$(\alpha_{rs}) e_{rs} \cdot (\alpha_{rs}^{-1} \cdot 1) = e_{rs} \in U$,
$e_{hr} e_{rs} e_{sk} = e_{hk} \in U$, $h = 1, 2$, $k = 1, 2$,
$\therefore e_{11}, e_{22}$ $e \in U$, $1 = e_{11} + e_{22} \in U$.
By (135.1), $U = R$.

*13. In Example 3.1.8 we discussed the real quaternions. Using this as a model we define the quaternions over the integers mod p, p an odd prime number, in exactly the same way; however, now considering all symbols of the form $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, where $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are integers mod p.
(a) Prove that this is a ring with p^4 elements whose only ideals are (0) and the ring itself.
**(b) Prove that this ring is *not* a division ring.

136.13 (a) R is clearly a ring with p^4 elements.
Let U be a nonzero ideal of R.
$a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in U \setminus 0$.
Without loss of generality, we may suppose that $\alpha_0 \neq 0$. Since, for example, if
$\alpha_1 \neq 0$, $-ai \in U$, $-ai = \alpha_1 - \alpha_0 i - \alpha_3 j + \alpha_2 k$.
$ia - ai = 2(\alpha_2 k - \alpha_3 j) \in U$. Since $p \neq 2$

$2^{-1}(ia-ai)=(\alpha_2 k-\alpha_3 j)\in U$,
$(\alpha_2 k-\alpha_3 j)i=\alpha_2 j+\alpha_3 k\in U$, Hence
$a-(\alpha_2 j+\alpha_3 k)=\alpha_0+\alpha_1 i\in U$.
$j(\alpha_0+\alpha_1 i)+(\alpha_0+\alpha_1 i)j=2\alpha_0 j\in U$,
$(-2^{-1})(2\alpha_0 j)j=\alpha_0\in U$,
$1=(\alpha_0^{-1})(\alpha_0)\in U$, $U=R$ by (135.1).

(b) We want to find x, y such that
$x^2+y^2+1=mp$, $0\le x$, $y\le\frac{1}{2}(p-1)$.
Then $(1+xi+yj)(1-xi-yj)=1+x^2+y^2$
$=0$ with $1+xi+yj\neq 0$ and
$1-xi-yj\neq 0$, R is not a division ring.
Consider $S_1=\{0^2, 1^2, \cdots\cdots, (\frac{p-1}{2})^2\}$,
$S_2=\{0^2-1, -1^2-1, \cdots\cdots, -(\frac{p-1}{2})^2-1\}$.
$|S_1|=|S_2|=\frac{p+1}{2}$. For if $i^2\equiv j^2 \pmod p$,
then $i\equiv -j$ or $i\equiv j \pmod p$.
$|S_1|+|S_2|=p+1>p=|\{0, 1, 2, \cdots\cdots, p\}$
Therefore, under module p , there are
$x\in S_1$, $y\in S_2$ such that $x\equiv y$ by pigeonhole principle, ie. $x^2\equiv -y^2-1 \pmod p$, $x^2+y^2+1=mp$.
This completes the proof.

If R is any ring a subset L of R is called a *left-ideal* of R if
1. L is a subgroup of R under addition.
2 $r\in R$, $a\in L$ implies $ra\in L$.
(One can similarly define a *right-ideal*.) An ideal is thus simultaneously a left- and right-ideal of R.

14. For $a\in R$ let $Ra=\{xa \mid x\in R\}$. Prove that Ra is a left-ideal of R.

136.14 $xa-ya=(x-y)a\in Ra$ for all x, y in R.
$r(xa)=(rx)a\in Ra$ for all $r, x\in R$.
Hence Ra is a left ideal of R.

15. Prove that the intersection of two left-ideals of R is a left-ideal of R.

136.15 Let L_1, L_2 be two left ideals of R.
$L=L_1\cap L_2$. $x, y\in L$ implies $x, y\in L_1$ and $x, y\in L_2$ so that $x-y\in L_1$ and $x-y\in L_2$ and $x-y\in L_1\cap L_2=L$.
For all $r\in R$, $rx\in L_1$ and $rx\in L_2$, so that $rx\in L_1\cap L_2=L$.
L is a left ideal of R.

16. What can you say about the intersection of a left-ideal and right-ideal of R?

136.16 If R is commutative, there is not distinguish between one-sided ideal and two-sided ideal. Therefore the intersection of a left ideal and right ideal are again an ideal of R. But, ingeneral, we can not get this conclusion.
For example, $R=\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d\in F\}$, F a field. $\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b\in F\}$ is a right ideal of R. $\{\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \mid c, d\in F\}$ is a left ideal of R. the intersection of these two sets is $\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a\in F\}$ which is neither a right ideal nor a left ideal.

17. If R is a ring and $a\in R$ let $r(a)=\{x\in R \mid ax=0\}$. Prove that $r(a)$ is a right-ideal of R.

136.17 $x, y\in r(a)$ implies $ax=0$ and $ay=0$ so that $a(x-y)=ax-ay=0$, $x-y\in r(a)$.
$p\in R$, $a(xp)=(ax)p=0\cdot p=0$ so that $xp\in R$. $r(a)$ is a right ideal of R.

18. If R is a ring and L is a left-ideal of R let $\lambda(L)=\{x\in R \mid xa=0$ for all $a\in L\}$. Prove that $\lambda(L)$ is a two-sided ideal of R.

136.18 $x, y\in\lambda(L)$ implies $xa=0$ and $ya=0$ for all a in L. Hence $(x-y)a=xa-ya=0$, $x-y\in\lambda(L)$. For all $r\in R$, $(xr)a=x(ra)=0$

since L is a left ideal and $ra \in L$.
$xr \in \lambda(L)$. $(rx)a = r(xa) = r \cdot 0 = 0$.
$rx \in \lambda(L)$. $\lambda(L)$ is a two-sided ideal of R.

*19. Let R be a ring in which $x^3 = x$ for every $x \in R$. Prove that R is a commutative ring.

136.19 Note : an element a in R is called nilpotent if for some positive integer m we have $a^m = 0$, an element a in R is called an idempotent if $a^2 = a$, $Z(R) = \{a \in R \mid ax = xa \text{ for all } x \text{ in } R\}$ is called the center of R.
We first claim that "R is a ring with no non-zero nilpotent element, then Z(R) contains all idempotent of R.
Pf. Suppose $a^2 = a$, $x \in R$. $(ax - axa)^2 = 0$, $(xa - axa)^2 = 0$. $ax = axa$ and $xa = axa$.
Hence $ax = xa$. $a \in Z(R)$.
Now, we prove the exercise R has no nonzero nilpotent element for if $a^m = 0$, $m \geq 1$.
We can choose the smallest m with $a^m = 0$.
$m = 3n$ implies $a^n = (a^n)^3 = a^{3n} = a^m = 0$.
$m = 3n+1$, $a^{n+1} = a^{3n+3} = (a^{3n+1})a^2 = 0$.
$m = 3n+2$, $a^{n+1} = a^{3n+3} = (a^{3n+2})a = 0$. This implies $a = 0$. Therefore $a^2 = a$ implies $a \in Z(R)$
$(x^2)^2 = x^4 = x^3 \cdot x = x \cdot x = x^2 \in Z(R)$ for all x in R.
$xyxy = x^2(xy)^2 = x(xy)^2x = x^2yxyx = yxyx$
$\therefore (xy)^2 = (yx)^2$.
$xy = (xy)^3 = (xy)(yx)^2 = xy(yx)(yx)$
$= xy^2xyx = x^2yx = yx^3 = yx$.
Hence R is commutative.

20. If R is a ring with unit element 1 and ϕ is a homomorphism of R *onto* R' prove that $\phi(1)$ is the unit element of R'.

136.20 Since ϕ is onto, for an $r' \in R'$, there is an $r \in R$ such that $\phi(r) = r'$.

$r' = \phi(r) = \phi(1 \cdot r) = \phi(1)\phi(r) = \phi(1)r'$
$= \phi(r \cdot 1) = \phi(r)\phi(1) = r'\phi(1)$.
Therefore, $\phi(1)$ is the unit element of R.

21. If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that $I(\phi) \neq R$, prove that $\phi(1)$ is the unit element of R'.

137.21 Since $I(\phi) \neq R$, there is an $a \in R$ such that $\phi(a) \neq 0$. Let $r \in R'$,
$(\phi(1)r - r)\phi(a) = \phi(1)r\phi(a) - r\phi(a)$
$= r\phi(1)\phi(a) - r\phi(a) = r\phi(1 \cdot a) - r\phi(a)$
$= r\phi(a) - r\phi(a) = 0$
Hence $\phi(1)r = r$, $r\phi(1) = r\phi(1) = r$.
$\phi(1)$ is the unit element of R'.

3.5 More Ideals and Quotient Rings.

1. Let R be a ring with unit element, R not necessarily commutative, such that the only right-ideals of R are (0) and R. Prove that R is a division ring.

139.1 To prove that R is a division ring, we must show that its nonzero elements form a group under multiplication. Now, we need only to show that every nonzero element has a right inverse by (35.12). Let $x \in R \setminus (0)$. xR is a right ideal of R and $x = x \cdot 1 \in xR$, $xR \neq (0)$. By our assumption $xR = R$. There exists $y \in R$ such that $x \cdot y = 1$. This shows that every nonzero element has a right inverse. R is therefore a division ring.

*2. Let R be a ring such that the only right ideals of R are (0) and R. Prove that either R is a division ring or that R is a ring with a prime number of elements in which $ab = 0$ for every $a, b \in R$.

140.2 $M = \{ x \in R \mid xR = 0 \}$ is a right ideal of R. $M = 0$ or $M = R$. (i) If $M = R$, $\forall x \in R = M$, $xR = 0$, and $xy = 0$ for all $y \in R$. In this case, any additive subgroup of R is a right ideal of R and hence is 0 or R. This shows that R has no proper subgroup under addition. By (46.3) R must be finite of prime order. Hence R is a ring with a prime number of elements in which $ab = 0$ for every $a, b \in R$.
(ii) $M = 0$. This means that $xR = 0$ implies $x = 0$. Hence, if $xy = 0$ and $y \neq 0$ then for all $z \in R$, there is $z' \in R$ such that $y \cdot z' = z$ by $yR = R$, and $x \cdot z = x \cdot y \cdot z' = 0$ i.e. $xR = 0$, and $x = 0$, that is $xy = 0$ implies $x = 0$ or $y = 0$. Let a be a fixed nonzero element of R, and e an element of R, necessarily different from zero, such that $ae = a$. From this, it follows that $ae^2 = ae$, and hence $e^2 = e$ since $a \neq 0$. Now if t is any element of R, we see that $(t - te)e = 0$. Hence $t = te$. Since $t \neq 0$ implies $tR = R$, there is $t' \in R$ such that $t \cdot t' = e$. By (35.12), the nonzero elements of R form a group under multiplication. R is a division ring.

3. Let J be the ring of integers, p a prime number, and (p) the ideal of J consisting of all multiples of p. Prove
(a) $J/(p)$ is isomorphic to J_p, the ring of integers mod p.
(b) Using Theorem 3.5.1 and part (a) of this problem, that J_p is a field.

140.3 (a) $\varphi : J \to J_p$. $\varphi(n) = n \pmod p$. This is a homomorphism of J onto Jp with kernel (p). Hence $J/(p) \cong J_p$.
(b) (p) is a maximal ideal of J, $J/(p)$ is a field. Hence Jp is a field.

**4. Let R be the ring of all real-valued continuous functions on the closed unit interval. If M is a maximal ideal of R, prove that there exists a real number γ, $0 \leq \gamma \leq 1$, such that $M = M_\gamma = \{f(x) \in R \mid f(\gamma) = 0\}$.

140.4 Suppose that for all r, $0 \leq r \leq 1$, there is an $f_r \in M$ such that $f_r(r) \neq 0$. Since f_r is continuous, there is an open interval I_r containing r such that $0 \notin f_r(I_r)$. Now $\bigcup_{0 \leq r \leq 1} I_r \supseteq [0,1]$. $[0,1]$ is a compact set in R, there are finite intervals say $I_{r_1}, \cdots\cdots, I_{r_n}$, such that $\bigcup_{i=1}^{n} I_{r_i} \supseteq [0,1]$. Let $f = f_{r_1}^2 + \cdots\cdots + f_{r_n}^2$, $f \in M$. $f(x) > 0$ for all $x \in [0,1]$, since $x \in I_{r_i}$, $f_{r_i}^2(x) > 0$ for some i. For any $g \in R$, $g/f \in R$,

$g=(g/f)f\in M$, $R\subseteq M$, $R=M$, a contradiction. Hence, there is an r, $0\le r\le 1$, such that for all $f\in M$, $f(r)=0$.
Let $M_r=\{f\in R \mid f(r)=0\}$.
M_r is an ideal of R which contains M.
Since $M_r\neq R$, and M is a maximal ideal of R, $M_r=M$, i.e. $M=M_r=\{f(x)\in R \mid f(r)=0\}$.

3.6 Field of Quotients of Integeral Domain

1. Prove that if $[a, b] = [a', b']$ and $[c, d] = [c', d']$ then $[a, b][c, d] = [a', b'][c', d']$.

142.1 $[a,b]=[a',b']$ means $ab'=a'b$.
$[c,d]=[c',d']$ means $cd'=c'd$.
$[a,b]\cdot[c,d]=[ac,bd]$,
$[a',b'][c',d']=[a'c',b'd']$.
Since $acb'd'=ab'cd'=a'bc'd=a'c'bd$,
$[ac,bd]=[a'c',b'd']$.
$[a,b][c,d]=[ac,bd]=[a'c',b'd']$
$=[a',b'][c',d']$.

2. Prove the distributive law in *F*.

142.2 $[a,b]([c,d]+[e,f])=[a,b][cf+de, df]=[acf+ade, bdf]$.
$[a,b][c,d]+[a,b][e,f]$
$=[ac,bd]+[ae,bf]=[acbf+bdae, b^2df]$
$=[b(acf+ade), b(bdf)]=[acf+ade, bdf]$
$=[a,b]([c,d]+[e,f])$.

3. Prove that the mapping $\phi:D\to F$ defined by $\phi(a)=[a,1]$ is an isomorphism of *D* into *F*.

142.3 $\phi(a+b)=[a+b,1]$,
$\phi(a)+\phi(b)=[a,1]+[b,1]=[a+b,1]$
$=\phi(a+b)$.
$\phi(ab)=[ab,1]=[ab,1\cdot 1]$
$=[a,1][b,1]=\phi(a)\cdot\phi(b)$.
If $\phi(a)=[a,1]=[0,b]$, $ab=0$, $a=0$.
So that ϕ is an isomorphism of D into F.

4. Prove that if *K* is any field which contains *D* then *K* contains a subfield isomorphic to *F*. (*In this sense F is the smallest field containing D.*)

142.4 Let the mapping $\phi: F\to K$ defined by

$\phi([a,b]) = ab^{-1}$.
Then $\phi([a,b]+[c,d])$
$=\phi([ad+bc, bd]) = (ad+bc)b^{-1}d^{-1}$
$= ab^{-1} + cd^{-1} = \phi([a,b]) + \phi([c,d])$.
$\phi([a,b]\cdot[c,d]) = \phi([ac,bd]) = acb^{-1}d^{-1}$
$= (ab^{-1})(cd^{-1}) = \phi([a,b])\cdot\phi([c,d])$.
$\phi \neq 0$. By (136.3), K contains a subfield isomorphic to F.

*5. Let R be a commutative ring with unit element. A nonempty subset S of R is called a multiplicative system if
1. $0 \notin S$.
2. $s_1, s_2 \in S$ implies that $s_1 s_2 \in S$.
Let $\mathcal{M}$ be the set of all ordered pairs (r, s) where $r \in R$, $s \in S$. In $\mathcal{M}$ define $(r, s) \sim (r', s')$ if there exists an element $s'' \in S$ such that

$$s''(rs' - sr') = 0.$$

(a) Prove that this defines an equivalence relation on $\mathcal{M}$.
Let the equivalence class of (r, s) be denoted by $[r, s]$, and let R_S be the set of all the equivalence classes. In R_S define $[r_1, s_1] + [r_2, s_2] = [r_1 s_2 + r_2 s_1, s_1 s_2]$ and $[r_1, s_1][r_2, s_2] = [r_1 r_2, s_1 s_2]$.
(b) Prove that the addition and multiplication described above are well defined and that R_S forms a ring under these operations.
(c) Can R be imbedded in R_S?
(d) Prove that the mapping $\phi: R \to R_s$ defined by $\phi(a) = [as, s]$ is a homomorphism of R into R_S and find the kernel of ϕ.
(e) Prove that this kernel has no element of S in it.
(f) Prove that every element of the form $[s_1, s_2]$ (where $s_1, s_2 \in S$) in R_S has an inverse in R_S.

142.5 (a) (i) $(r,s) \sim (r,s)$ since
$s'(rs - sr) = s'(rs - rs) = 0$
(ii) $(r,s) \sim (r',s')$ means there exists an element $s'' \in S$ such that $s''(rs' - sr') = 0$.
$s''(r's - s'r) = 0$ implies $(r',s') \sim (r,s)$
(iii) $(r,s) \sim (r',s')$, $(r',s') \sim (r'',s'')$
means there are $s_1, s_2 \in S$
such that $s_1 \cdot (rs' - sr') = 0$
and $s_2 \cdot (r's'' - s'r'') = 0$.

Then, $s_1 s_2 s'(rs'' - sr'')$
$= s_1 s_2 s' ts'' - s_1 s_2 sr' s'' + s_1 s_2 sr' s''$
$- s_1 s_2 ss' r''$
$= s_2 s'' s_1 (rs' - sr') + s_1 ss_2 (r's'' - s'r'')$
$= 0$.
That is $(r,s) \sim (r'',s'')$.
This completes the proof.

(b) $[r_1, s_1] = [r_1', s_1']$, $[r_2, s_2] = [r_2', s_2']$ implies there are s', $s'' \in S$ such that
$s'(r_1 s_1' - r_1' s_1) = 0$ and $s''(r_2 s_2' - r_2' s_2) = 0$.
$[r_1, s_1] + [r_2, s_2] = [r_1 s_2 + r_2 s_1, s_1 s_2]$,
$[r_1', s_1'] + [r_2', s_2'] = [r_1' s_2' + r_2' s_1', s_1' s_2']$.
$s's''((r_1 s_2 + r_2 s_1) s_1' s_2' - s_1 s_2 (r_1' s_2' + r_2' s_1'))$
$= s's''(r_1 s_2 s_1' s_2' + r_2 s_1 s_1' s_2' - s_1 s_2 r_1' s_2' - s_1 s_2 r_2' s_1')$
$= s_2 s_2' s'' s'(r_1 s_1' - s_1 r_1') + s' s_1 s_1' s''(r_2 s_2' - s_2 r_2')$
$= 0$.
Hence $[r_1 s_2 + r_2 s_1, s_1 s_2]$
$= [r_1' s_2' + r_2' s_1', s_1' s_2']$, i.e.,
$[r_1, s_1] + [r_2, s_2] = [r_1', s_1'] + [r_2', s_2']$.
$[r_1, s_1][r_2, s_2] = [r_1 r_2, s_1 s_2]$,
$[r_1', s_1'][r_2', s_2'] = [r_1' r_2', s_1' s_2']$.
$s's''(r_1 r_2 s_1' s_2' - r_1' r_2' s_1 s_2)$
$= s''s'(r_1 s_1' r_2 s_2' - r_1' s_1 r_2 s_2' + r_1' s_1 r_2 s_2'$
$- r_1' s_1 r_2' s_2)$
$= s'' r_2 s_2' s'(r_1 s_1' - r_1' s_1) + r_1' s_1 s' s''(r_2 s_2'$
$- r_2' s_2)$
$= 0$.
Hence $[r_1 r_2, s_1 s_2] = [r_1' r_2', s_1' s_2']$, i.e.
$[r_1, s_1][r_2, s_2] = [r_1', s_1'][r_2', s_2']$.
The addition and multiplication described above are well defined. All the other works are just like Theorem 3.6.1.

(c) If $rs = 0$ for $r \in R$ and $s \in S$ implies $r = 0$, then R can be imbedded into Rs by $\phi: R \to Rs$ as $\phi(r) = [r, 1]$.

(d) $\phi(a+b)=[(a+b)s,s]=[as+bs,s]$
$=[ass+bss,ss]=[a,s]+[b,s]$
$=\phi(a)\phi(b)$.
$\phi(ab)=[abs,s]=[abss,ss]$
$=[(as)(bs),ss]=[as,s][bs,s]$
$=\phi(a)\phi(b)$.
ϕ is a homomorphism of R into Rs. The kernel K of ϕ is $\{a\in R \mid$ there is an $s\in S$ such that $as=0\}$.

(e) If $s\in K\cap S$ then there is an $s'\in S$ such that $ss'=0\in S$, a contradiction.

(f) The unit element of Rs is $[s,s]$ for $[s,s][r',s']=[r's,s's]=[r',s']$. The inverse element of $[s_1,s_2]$ is $[s_2,s_1]$ since $[s_1,s_2][s_2,s_1]$ $=[s_1s_2,s_1s_2]$.

6. Let D be an integral domain, $a, b \in D$. Suppose that $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n. Prove that $a = b$.

143.6 $(m,n)=1$ implies there are integers r,s such that $rm+sn=1$.
D can be imbedded in F. Hence, if $a\neq 0$, $b\neq 0$, a, b have inverse elements in F.
$a^1=a^{rm+sn}=(a^m)^r\cdot(a^n)^s=(b^m)^r(b^n)^s$
$=b^{mr+ns}=b$ in F, and hence in D.

7. Let R be a ring, possibly noncommutative, in which $xy = 0$ implies $x = 0$ or $y = 0$. If $a, b \in R$ and $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n, prove that $a = b$.

143.7 $(m,n)=1$ implies there are integers r,s such that $rm+sn=1$. If $r=0$ or $s=0$, then we are done.
Let's say $r>0$ and $s<0$. $rm=1-sn$.
$a\cdot b^{-sn}=a\cdot a^{-sn}=a^{1-sn}=a^{rm}=b^{rm}$
$=b^{1-sn}=bb^{-sn}$. $(a-b)b^{-sn}=0$.
If $b=0$, we are done.
If $b\neq 0$, $b^{-sn}\neq 0$, $(a-b)=0$, $a=b$.

3.7 Euclidean Rings

Note: Lemma 3.7.7 must be changed by
"The ideal $A=(a_0)\neq(0)$ is a maximal ideal of the Euclidean ring R if and only if a_0 is a prime element of R."

1. In a commutative ring with unit element prove that the relation a is an associate of b is an equivalence relation.

149.1 Since $a=1\cdot a$, a is an associate of a. If a is an associate of b, then $b=ua$ for some unit u in R. There is u' in R such that $u'u=1$. $u'b=u'(ua)=(u'u)a=1\cdot a=a\cdot a$ is an associate of b. If a is an associate of b and b is an associate of c, then $a=ub$, $b=u'c$ for some u and u' in R. $a=ub=u(u'c)=(uu')c$. Since uu' is also a unit of R, c is an associate of a. This completes the proof.

2. In a Euclidean ring prove that any two greatest common divisors of a and b are associates.

149.2 Let c, d be greatest common divisors of a and b. By definition, $c\mid d$ and $d\mid c$. By Lemma 3.7.2., c and d are associates.

3. Prove that a necessary and sufficient condition that the element a in the Euclidean ring be a unit is that $d(a) = d(1)$.

149.3 Suppose a is a unit in R. $ab=1$ for some b in R. $d(a)\leq d(ab)=d(1)$.
On the other hand, since $a=1\cdot a$, $d(1)\leq d(1\cdot a)=d(a)$. Hence $d(a)=d(1)$.
Conversely, suppose $d(a)=d(1)$. For 1, a, there exist $t,r\in R$ such that $1=ta+r$ where either $r=0$ or $d(r)<d(a)$.
Since $d(a)=d(1)\leq d(r)$, $d(r)\not< d(a)$, so $r=0$, i.e. $1=ta$, a is a unit.

4. Prove that in a Euclidean ring (a, b) can be found as follows:

$$b = q_0 a + r_1, \quad \text{where} \quad d(r_1) < d(a)$$
$$a = q_1 r_1 + r_2, \quad \text{where} \quad d(r_2) < d(r_1)$$
$$r_1 = q_2 r_2 + r_3, \quad \text{where} \quad d(r_3) < d(r_2)$$
$$\vdots \qquad\qquad \vdots$$
$$r_{n-1} = q_n r_n$$

and $r_n = (a, b)$.

149.4 $r_n \mid r_{n-1}$ by $r_{n-1} = q_n r_n$.
$r_n \mid r_{n-2}$ by $r_{n-2} = q_{n-1} r_{n-1} + r_n$.
Continue this process, we have that $r_n \mid r_2$, $r_n \mid r_1$, $r_n \mid a$ and $r_n \mid b$. And if $r \mid a$ and $r \mid b$.
By $b = q_0 a + r_1$ we have $r \mid r_1$.
By $a = q_1 r_1 + r_2$ we have $r \mid r_2$.
Continue this process, we have $r \mid r_n$.
By definition $r_n = (a, b)$.

5. Prove that if an ideal U of a ring R contains a unit of R, then $U = R$.

149.5 Let $u \in U$ be a unit in R. By definition $uu' = 1$ for some u' in R.
Since U is an ideal of R, $1 = uu' \in U$.
By (135.1), $U = R$.

6. Prove that the units in a commutative ring with a unit element form an abelian group.

149.6 If u, u' are units in R, there are v, v' in R such that $uv = 1$ and $u'v' = 1$.
$(uu')(v'v) = u(u'v')v = u \cdot 1 \cdot v = uv = 1$.
v, uu' are also units R. Since R is commutative, $uu' = u'u$. By (35.12), the units in a commutative ring with a unit element form an abelian group under multiplication.

7. Given two elements a, b in the Euclidean ring R their *least common multiple* $c \in R$ is an element in R such that $a \mid c$ and $b \mid c$ and such that whenever $a \mid x$ and $b \mid x$ for $x \in R$ then $c \mid x$. Prove that any two elements in the Euclidean ring R have a least common multiple in R.

8. In Problem 7, if the least common multiple of a and b is denoted by $[a, b]$, prove that $[a, b] = ab/(a, b)$.

149.7 $ab/(a, b)$ has a and b as divisors.

149.8 If $a \mid x$ and $b \mid x$, then $(a/(a, b)) \mid x$ and $b \mid x$. $(a/(a, b), b) = 1$ implies $ab/(a, b) \mid x$.
By definition, the least common multiple of a and b exists and is $ab/(a, b)$.

3.8 A Particular Euclidean Ring

1. Find all the units in $J[i]$.

152.1 By (149.3), $x+yi$ is a unit if and only if $d(x+yi)=x^2+y^2=1$. Hence $1, -1, i, -i$ are the units in $J[i]$.

2. If $a + bi$ is not a unit of $J[i]$ prove that $a^2 + b^2 > 1$.

152.2 Note: Chang the problem by "If $a+bi\neq 0$ is not a unit of $J[i]$ prove that $a^2+b^2>1$."
Pf. By (149.3),
$d(a+bi)=a^2+b^2\neq 1$, $a^2+b^2\neq 0$,
$a^2+b^2>1$.

3. Find the greatest common divisor in $J[i]$ of
(a) $3 + 4i$ and $4 - 3i$. (b) $11 + 7i$ and $18 - i$.

152.3 (a) Since $3+4i=(4-3i)i$ and i is a unit, the greatest common divisor in $J[i]$ of $3+4i$ and $4-3i$ is $\in(4-3i)$, where $\in$ is a unit in $J[i]$.
(b) $18-i=(11+7i)(1-i)+3i$
$11+7i=(3i)(-4i+2)+(-1+i)$
$3i=(-1+i)(1-i)+i$
$-1+i=i(1+i)$.
By (149.4), the greatest common divisor of $11+7i$ and $18-i$ is the unit in $J[i]$.

4. Prove that if p is a prime number of the form $4n + 3$, then there is no x such that $x^2 \equiv -1 \bmod p$.

152.4 If there is an x such that $x^2\equiv -1 \pmod p$, then $x^4\equiv 1 \pmod p$. x is of order 4.
$4 \mid p-1$ since (x) is a subgroup of $\{1, 2, \cdots\cdots, p-1\}$ under multiplication mod p.
This completes the proof.

5. Prove that no prime of the form $4n + 3$ can be written as $a^2 + b^2$ where a and b are integers.

152.5 If there are a and b such that $p=a^2+b^2$, where p is a prime of the form $4n+3$, then $a\not\equiv 0$ and $b\not\equiv 0 \pmod p$. $a^2+b^2\equiv 0 \pmod p$.
$a^2\equiv -b^2 \pmod p$ $(ab^{-1})^2\equiv -1 \pmod p$.
This contradicts with (152.4).

6. Prove that there is an infinite number of primes of the form $4n + 3$.

152.6 Suppose there is only a finite number of primes of the form $4n+3$.
Let these primes be $x_1, x_2, \cdots\cdots, x_m$.
$P=4x_1x_2\cdots\cdots x_m-1$ is also of the form $4n+3$ since $m\geq 2$, $2\nmid p$. $x_i\nmid P$.
Therefore, the prime divisors of P are all of the form $4n+1$. Since $(4n+1)(4m+1)=4r+1$, P must be of the form $4n+1$, a contradiction.

*7. Prove there exists an infinite number of primes of the form $4n + 1$.

152.7 Let $x_1, x_2, \cdots\cdots, x_m$ be all the distinct primes of the form $4n+1$.
$P=4x_1^2\cdots\cdots x_m^2+1$. $2\nmid p$, $x_i\nmid P$.
The prime divisors of P are all of the form $4n+3$. But then $(2x_1\cdots\cdots x_m)^2\equiv -1 \pmod q$ for some prime number q of the form $4n+3$ which contradicts with (152.4). P is a prime number. But $P>x_i$, $i=1, \cdots\cdots, m$, a contradiction.

*8. Determine all the prime elements in $J[i]$.

152.8 To do this exercises we show first that any prime r in $J[i]$ divides exactly one positive

rational prime p.
For $d(r)= r\bar{r}$, so $r|d(r)$. Let $d(r)= p_1 \cdots p_t$ be the decomposition in J of $d(r)$ into positive primes. Then $r|p_1 \cdots p_t$. By corollary of Lemma 3.7.6. , r divides one of the p_i.
So r divides some positive rational prime.
It cannot divide two, p and q. For we can find rational integers l and m such that $lp+mq=1$. If $r|p$, $r|q$ then $r|1$, so r is a unit, not a prime, contrary to hypothesis.
Hence, we can get each prime in $J[i]$ once and only once by considering the factorization of all positive rational primes, treated as elements of $J[i]$.
Now, let r be a prime in $J[i]$, and p the positive prime for which $r|p$. Then $d(r)|\, d(p)$. But $d(p)= p^2$, since p is a rational integer. Hence $d(r)= p$ or $d(r)= p^2$.
If $r=x+yi$, then $x^2+y^2=p$ or $x^2+y^2=p^2$.
Case 1. $p\equiv 3 \pmod 4$. By (152.5), $x^2+y^2=p^2$. $d(r)= d(p)$. Since $r|p$, $p=rs$, $p=rs$, where $s\in J[i]$.
$p^2 = d(p)= d(rs) = d(r)d(s)= p^2\, d(s)$, $d(s)= 1$, s is a unit in $J[i]$. p and r are associates.
Case 2. $p=2$. $2=(1+i)(1-i)$, and $r|2$. So $r|1+i$ or $r|1-i$.
But $d(1+i)=d(1-i)=2$, a rational prime. So $1+i$, $1-i$ are prime. Hence r associates with $1+i$ or $1-i$. Since $(1+i)/(1-i)= i$, $1+i$ and $1-i$ are associates.
Case 3. $p\equiv 1 \pmod 4$. $p|n^2+1$ for some rational integer n by Lemma 3.8.2.
But $n^2+1=(n+i)(n-i)$ and $r|p$,

so $r|n+i$ or $r|n-i$. But p does not divide $n+i$ or $n-i$, for otherwise one of $\frac{n}{p}\pm\frac{1}{p}i$ would be a Gaussian integer; this cannot be, for $1/p$ is not a rational integer.
Hence r and p are not associated. It follows that $d(r)\neq d(p)$, so $x^2+y^2\neq p^2$.
From our earlier remarks, this leaves only the alternative $x^2+y^2=p$.
Then $r\bar{r}=p$. moreover $r=x+iy$ and $\bar{r}=x-iy$ are primes, since $Nr=N\bar{r}=p$.
They are not associated, for otherwise $x+yi=\in(x-yi)$, where $\in=\pm 1$ or $\pm i$.
If $\in=1$, $y=0$, $x^2=p$, so p is not a prime.
If $\in=-1$, $x=0$, $y^2=p$, and the same conclusion follows. If $\in=\pm i$, $x=\pm y$, and p is even. All these eventualites are impossible, so $x+yi$ and $x-yi$ are not associated.
Finally, since $x^2+y^2=p$, one of x and y must be even, the other odd. Therefore, Gaussian primes fall into the following three classes :

(1) all positive rational primes of the form $4n+3$ and the associates.
(2) the number $1+i$ and its associates.
(3) all integers associated with either $x+yi$ or $x-yi$ where $x>0$, $y>0$, x is even, and x^2+y^2 is a rational prime of the form $4n+1$.

*9. Determine all positive integers which can be written as a sum of two squares (of integers).

152.9 The integer m can be written as a sum of two squares of integers if and only if $m=2^r n^2 p_1 p_2 \cdots p_k$, where n is an integer and p_i is a prime of the form $4n+1$, $r=0$ or $r=1$.

Pf. Since $(a^2+b^2)(c^2+d^2)$
$=(ac-bd)^2+(bc+ad)^2$,
$(\because d(a+bi)d(c+di)=d((a+bi)(c+di))$
$=d((ac-bd)+(bc+ad)i).)$
and $2^r, n^2, p_1, \cdots\cdots, p_k$ all can be written as a sum of two squares of integers, there product $m=2^r n^2 p_1 p_2 \cdots\cdots p_k$ is also a sum of two squares of integers.
Conversely, if $a^2+b^2=2^r n^2 p_1 \cdots\cdots p_k \cdot q'$, where q' is a product of primes of the form $4m+3$. Then $a^2+b^2 \equiv 0 \pmod{q}$ for some prime q of the form $4m+3$. $a \not\equiv 0$, $b \not\equiv 0 \pmod{q}$. $(ab^{-1})^2 \equiv -1 \pmod{q}$. contrary to (152.4). This completes the proof.

3.9. Polynomial Rings.

1. Find the greatest common divisor of the following polynomials over F, the field of rational numbers:
(a) $x^3 - 6x^2 + x + 4$ and $x^5 - 6x + 1$.
(b) $x^2 + 1$ and $x^6 + x^3 + x + 1$.

158.1 (a) $x^3-6x^2+x+4=(x-1)(x^2-5x-4)$.
x^5-6x+1 is not divisible by $x-1$ and x^2-5x-4. Hence, the greatest common divisor of x^3-6x^2+x+4 and x^5-6x+1 is 1.

(b) $x^6+x^3+x+1=(x^2+1)(x^4-x^2+x+1)$.
The greatest common divisor of x^2+1 and x^6+x^3+x+1 is x^2+1.

2. Prove that
(a) $x^2 + x + 1$ is irreducible over F, the field of integers mod 2.
(b) $x^2 + 1$ is irreducible over the integers mod 7.
(c) $x^3 - 9$ is irreducible over the integers mod 31.
(d) $x^3 - 9$ is reducible over the integers mod 11.

158.2 A polynomial of degree no more than three is reducible if and only if it has a linear factor, i.e. it is solvable over the given field.

(a) If x^2+x+1 is reducible over J_2, it has a root 0 or 1. Since $0^2+0+1=1 \neq 0$ and $1^2+1+1=1 \neq 0$, x^2+x+1 is irreducible.

(b) If x^2+1 is reducible, there is an $a \in J_7$ such that $a^2+1=0 \pmod{7}$, by (152.4) this is impossible. Hence x^2+1 is irreducible.

(c) If x^3-9 is reducible, there is an $a \in J_{31}$ such that $a^3-9 \equiv 0 \pmod{31}$.
By (24.14), $a^{30} \equiv 1 \pmod{31}$.
But $a^{30} \equiv (a^3)^{10} \equiv 9^{10} \equiv 5 \pmod{31}$,

contrary to $a^{30} \equiv 1 \pmod{31}$.
Hence, x^3-9 is irreducible.

(d) $x^3 - 9 = (x-4)(x^2+4x+5)$,
$x^3 - 9$ is reducible.

3. Let F, K be two fields $F \subset K$ and suppose $f(x), g(x) \in F[x]$ are relatively prime in $F[x]$. Prove that they are relatively prime in $K[x]$.

158.3 $a(x), b(x) \in L[x]$, L a field, are relatively prime if and only if there are $c(x), d(x) \in L[x]$ such that $a(x)c(x)+b(x)d(x)=1$.
Now, $f(x), g(x) \in F[x]$ are relatively prime implies there are $h(x), k(x) \in F[x]$, hence $h(x), k(x) \in K[x]$, such that $f(x)h(x)+g(x)k(x)=1$. Therefore, $f(x)$ and $g(x)$ are relatively prime in $K[x]$.

4. (a) Prove that $x^2 + 1$ is irreducible over the field F of integers mod 11 and prove directly that $F[x]/(x^2 + 1)$ is a field having 121 elements.
(b) Prove that $x^2 + x + 4$ is irreducible over F, the field of integers mod 11 and prove directly that $F[x]/(x^2 + x + 4)$ is a field having 121 elements.
*(c) Prove that the fields of part (a) and part (b) are isomorphic.

158.4 (a) Since $x^2+1=0$ has no solution in J_{11} by (152.4), x^2+1 is irreducible over J_{11}.
To prove that $F[x]/(x^2+1)$ is a field, we need only prove that for $a_1x+b_1 \notin (x^2+1)$ there is a_2x+b_2 such that
$(a_1x+b_1)(a_2x+b_2)=1$.
$(a_1x+b_1)(a_2x+b_2)$
$=(a_1b_2+b_1a_2)x+(b_1b_2-a_1a_2)$:

$$\begin{cases} a_1b_2+b_1a_2=0 \\ b_1b_2-a_1a_2=1 \end{cases}$$

We get a solution (a_2, b_2) if and only if $a_1^2+b_1^2 \neq 0$. Since $a_1x+b_1 \neq 0$, $a_1 \neq 0$ and $b_1 \neq 0$.
If $a_1^2+b_1^2 \equiv 0 \pmod{11}$,

$(a_1b_1^{-1})^2 \equiv -1 \pmod{11}$, contrary to (152.4). Hence we can find a_2x+b_2 such that $(a_1x+b_1)(a_2x+b_2)=1$.
$F[x]/(x^2+1)$ is a field. Since every element of $F[x]/(x^2+1)$ can be uniquely represented as $(ax+b)+(x^2+1)$, $F[x]/(x^2+1)$ has $(11)^2=121$ elements.

(b) $x^2+x+4=x^2+12x+36+1=(x+6)^2+1$ has no solution in J_{11}. Hence x^2+x+4 is irreducible. As above, we only show that for a given $a_1x+b_1 \neq 0$, there is a_2x+b_2 such that $(a_1x+b_1)(a_2x+b_2)=1$.
$(a_1x+b_1)(a_2x+b_2)$
$=a_1a_2x^2+(b_1a_2+a_1b_2)x+b_1b_2$
$=a_1a_2(-x-4)+(b_1a_2+a_1b_2)x+b_1b_2$
$=(b_1a_2+a_1b_2-a_1a_2)x+(b_1b_2-4a_1a_2)$
$=1$

$$\begin{cases} (b_1-a_1)a_2+a_1b_2=0 \\ -4a_1a_2+b_1b_2=1 \end{cases}$$

We get a solution (a_2, b_2) if and only if $(b_1-a_1)b_1+4a_1^2 \neq 0$, i.e.
$4a_1^2-a_1b_1+b_1^2 \neq 0$.
If $4a_1^2-a_1b_1+b_1^2=0$.
$4a_1^2-12a_1b_1+9b_1^2-8b_1^2$
$=(2a_1-3b_1)^2-8b_1^2=0$.
$(2a_1-3b_1)^2=8b_1^2$.
$\{x^2 \mid x \in J_{11}\}=\{0,1,3,4,5,9\}$.
$\{8x^2 \mid x \in J_{11}\}=\{0,8,2,10,7,6\}$.
Since $\{x^2 \mid x \in J_{11}\} \cap \{8x^2 \mid x \in J_{11}\}$
$=\{0\}$. $a_1=b_1=0$.
Hence $(b_1-a_1)b_1+4a_1^2 \neq 0$, if $a_1x+b_1 \neq 0$.
Therefore $F[x]/(x^2+x+4)$ is a field having 121 elements.

(c) Define $\sigma : F[x]/(x^2+1) \to F[x]/(x^2+x+4)$ as $\sigma(ax+b)=a(x+6)+b$.

Clearly, $\sigma((a_1x+b_1)+(a_2x+b_2))$
$=\sigma(a_1x+b_1)+\sigma(a_1x+b_1)$

$(a_1x+b_1)(a_2x+b_2)$
$=(a_1b_2+a_2b_1)x+(b_1b_2-a_1a_2)$
in $F[x]/(x^2+1)$ and
$(a_1(x+6)+b_1)(a_2(x+6)+b_2)$
$=(a_1b_2+a_2b_1)(x+6)+(b_1b_2-a_1a_2)$
in $F[x]/(x^2+x+4)$.
Hence $\sigma((a_1x+b_1)(a_2x+b_2))$
$=(a_1b_2+a_2b_1)(x+6)+(b_1b_2-a_1a_2)$
$=(a_1(x+6)+b_1)(a_2(x+6)+b_2)$
$=\sigma(a_1x+b_1)\sigma(a_2x+b_2)$.
σ is a homomorphism of $F[x]/(x^2+1)$ into $F[x]/(x^2+x+4)$. σ is clearly one-to-one and onto. $F[x]/(x^2+1)\approx F[x]/(x^2+x+4)$.

5. Let F be the field of real numbers. Prove that $F[x]/(x^2+1)$ is a field isomorphic to the field of complex numbers.

158.5 x^2+1 is irreducible over F. $F[x]/(x^2+1)$ is a field. Define $\sigma: F[x]/(x^2+1)\to C$ as $\sigma(ax+b)=ai+b$, σ is an isomorphism of $F[x]/(x^2+1)$ onto C. $F[x]/(x^2+1)\approx C$.

*6. Define the *derivative* $f'(x)$ of the polynomial

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

as $$f'(x)=a_1+2a_2x+3a_3x^2+\cdots+na_nx^{n-1}.$$

Prove that if $f(x)\in F[x]$, where F is the field of rational numbers, then $f(x)$ is divisible by the square of a polynomial if and only if $f(x)$ and $f'(x)$ have a greatest common divisor $d(x)$ of positive degree.

158.6 Note: Change the Problem by "$f(x)$ is divisible by the square of a polynomial of positive degree if and only if $f(x)$ and $f'(x)$ have a greatest common divisor $d(x)$ of positive degree."

Let $g(x)=b_0+b_1x+b_2x^2+\cdots\cdots+b_mx^m$.
$f(x)g(x)=(a_0+a_1x+\cdots\cdots+a_nx^n)$
$(b_0+b_1x+b_2x^2+\cdots\cdots+b_mx^m)$
$=a_0b_0+(a_0b_1+a_1b_0)x$
$+(a_0b_2+a_1b_1+a_2b_0)x^2$
$+\cdots\cdots+a_nb_mx^{n+m}$
$(f(x)g'(x))=(a_0b_1+a_1b_0)+2(a_0b_2+a_1b_1+a_2b_2)x$
$+\cdots\cdots+(m+n)a_nb_mx^{n+m-1}$
$f'(x)g(x)=(a_1+2a_2x+3a_3x^2+\cdots\cdots+na_nx^{n-1})$
$(b_0+b_1x+\cdots\cdots+b_mx^m)$
$=a_1b_0+(a_1b_1+2a_2b_0)x$
$+(3a_3b_0+2a_2b_1+a_1b_2)x^2$
$+\cdots\cdots+na_nb_mx^{n+m-1}$
$f(x)g'(x)=b_1a_0+(b_1a_1+2b_2a_0)x$
$+(3b_3a_0+2b_2a_1+b_1a_2)x^2$
$+mb_ma_nx^{n+m-1}$
$f'(x)g(x)+f(x)g'(x)=(a_0b_1+a_1b_0)$
$+2(a_0b_2+a_1b_1+a_2b_2)x$
$+3(a_0b_3+a_1b_2+a_2b_1+a_3b_0)x^2$
$+\cdots\cdots+na_nb_mx^{n+m-1}$
$=(f(x)g(x))'$
Hence, $(f_1(x)f_2(x)\cdots\cdots f_n(x))'=f_1'(x)f_2(x)\cdots f_n(x)$
$+f_1(x)(f_2(x)\cdots\cdots f_2(x))'$
$=f_1'(x)f_2(x)\cdots\cdots f_n(x)+f_1(x)f_2'(x)f_3(x)\cdots$
$\cdots f_n(x)+\cdots\cdots+f_1(x)f_2(x)\cdots\cdots f_n'(x)$
by induction hypothesis.
If $f(x)$ is divisible by $(h(x))^2$, then
$f(x)=(h(x))^2k(x)$ for some $k(x)$ in $F[x]$.
$f'(x)=h'(x)h(x)k(x)+h(x)h'(x)k(x)+h(x)h(x)k'(x)$
$=h(x)(2h'(x)k(x)+h(x)k'(x))$. $f(x)$ and $f'(x)$ have at least $h(x)$ as their common divisor, so that $f(x)$ and $f'(x)$ have a greatest common divisor $d(x)$ of posetive degree.
Conversely, suppose that $f(x)$ and $f'(x)$ have a greatest common divisor $d(x)$ of positive

degree . Let r(x) be an irreducible polynomial as a divisor of d(x) . Then $f(x)=r(x)h(x)$ for some h(x) in F[x] . $f'(x)=r(x)h'(x)+r'(x)h(x)$. Since r(x) is irreducible , $(r(x), r'(x))=1$. $r(x)|f'(x)$, $r(x)|r'(x)h(x)$, $r(x)|h(x)$. Hence $r^2(x)|f(x)$. This completes the proof .

7. If $f(x)$ is in $F[x]$, where F is the field of integers mod p, p a prime, and $f(x)$ is irreducible over F of degree n prove that $F[x]/(f(x))$ is a field with p^n elements.

159.7 F[x]/(f(x)) is clearly a field . Since every element of it can be uniquely represented as $a_0+a_1x+\cdots\cdots+a_{n-1}x^{n-1}+(f(x))$, F[x]/(f(x)) has p^n elements .

3.10. Polynomials over Rational Field

1. Let D be a Euclidean ring, F its field of quotients. Prove the Gauss Lemma for polynomials with coefficients in D factored as products of polynomials with coefficients in F.

161.1 Since the proof of lemma 3.10.1 and Theorem 3.10.1 can be carried out if we replace integers by Euclidean ring and rational numbers by its field of quotients , the Gauss Lemma is true for Euclidean ring case .

2. If p is a prime number, prove that the polynomial $x^n - p$ is irreducible over the rationals.

161.2 By Theorem 3.10.2, x^n-p is irreducible over the rationals .

3. Prove that the polynomial $1 + x + \cdots + x^{p-1}$, where p is a prime number, is irreducible over the field of rational numbers. (*Hint:* Consider the polynomial $1 + (x + 1) + (x + 1)^2 + \cdots + (x + 1)^{p-1}$, and use the Eisenstein criterion.)

161.3 The polynomial $1+x+\cdots\cdots+x^{p-1}$ is irreducible if and only if $1+(1+x)+(1+x)^2+\cdots\cdots+(1+x)^{p-1}$ is irreducible .

$$1+(1+x)+\cdots\cdots+(1+x)^{p-1}=\frac{(1+x)^p-1}{(1+x)-1}$$

$$=\frac{(1+x)^p-1}{x}=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\cdots+\binom{p}{p-1}.$$

By Theorem 3.10.2 , $1+(1+x)+\cdots\cdots+(1+x)^{p-1}$ is irreducible , so that $1+x+\cdots\cdots+x^{p-1}$ is irreducible .

4. If m and n are relatively prime integers and if

$$\left(x-\frac{m}{n}\right)|(a_0+a_1x+\cdots+a_rx^r),$$

where the a's are integers, prove that $m \mid a_0$ and $n \mid a_r$.

161.4 $a_0+a_1(\frac{m}{n})+a_2(\frac{m}{n})^2+\cdots\cdots+a_r(\frac{m}{n})^r=0$

$n^r a_0+a_1 m n^{r-1}+a_2 m^2 n^{r-2}+\cdots\cdots+a_{r-1}m^{r-1}n+a_r m^r=0$
$n\mid(n^r a_0+a_1 m n^{r-1}+\cdots\cdots+a_{r-1}m^{r-1}n)$ implies $n\mid a_r m^r$.
$(n,m)=1$ implies $(n,m^r)=1$ and $n\mid a_r$. On the other hand, $m\mid(a_1 m n^{r-1}+a_2 m^2 n^{r-2}+\cdots+a_r m^r)$ implies $m\mid n^r a_0$. $(n,m)=1$ implies $(n^r,m)=1$ and $m\mid a_0$.

5. If a is rational and $x-a$ divides an integer monic polynomial, prove that a must be an integer.

161.5 By (161.4), let $a=\frac{m}{n}$, then $n\mid a_r$, $a_r=1$ and $n=1$. $a=m$ is an integer.

3.11 Polynomial Rings over Commutative Rings

1. Prove that $R[x]$ is a commutative ring with unit element whenever R is.

166.1 Suppose $f(x)=a_0+a_1x+\cdots\cdots+a_rx^r$, $g(x)=b_0+b_1x+\cdots\cdots+b_sx^s$, $h(x)=c_0+c_1x+\cdots\cdots+c_tx^t\in R[x]$. $f(x)+g(x)\in R[x]$, $f(x)g(x)\in R[x]$. $(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$, $0+f(x)=f(x)$, $f(x)+(-f(x))=0$, $f(x)+g(x)=g(x)+f(x)$. $(f(x)g(x))h(x)=f(x)(g(x)h(x))$, $f(x)g(x)=g(x)f(x)$, $1\cdot f(x)=f(x)$, $f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$. $R[x]$ is a commutative ring with unit element.

2. Prove that $R[x_1,\ldots,x_n]=R[x_{i_1},\ldots,x_{i_n}]$, where $(i_1,\ldots,i_n)$ is a permutation of $(1,2,\ldots,n)$.

166.2 Every element of $R[x_1,\cdots\cdots,x_n]$ is of the from

$$\Sigma a_{j_1 j_2\cdots\cdots j_n}x_1^{j_1}x_2^{j_2}\cdots\cdots x_n^{j_n}=\Sigma a_{j_1 j_2\cdots\cdots i_1}x^{j_{i_1}}x_{i_2}^{j_{i_2}}\cdots\cdots x_{i_n}^{j_{i_n}}$$

and is also in $R[x_{i_1},x_{i_2},\cdots\cdots,x_{i_n}]$. $R[x_1,\cdots\cdots,x_n]\subset R[x_{i_1},\cdots\cdots,x_{i_n}]$. $R[x_{i_1},\cdots\cdots,x_{i_n}]\subset R[x_1,\cdots\cdots,x_n]$. $R[x_{j_{i_1}},\cdots\cdots,x_n]=R[x_{i_1},\cdots\cdots,x_{i_n}]$.

3. If R is an integral domain, prove that for $f(x)$, $g(x)$ in $R[x]$, $\deg(f(x)g(x))=\deg(f(x))+\deg(g(x))$.

166.3 Let $f(x)=a_0+a_1x+\cdots\cdots+a_nx^n$, $g(x)=b_0+b_1x+\cdots\cdots+b_mx^m$. $\deg f(x)=n$, $\deg g(x)=m$. $f(x)g(x)=a_0b_0+(a_1b_0+a_0b_1)x+\cdots\cdots+a_nb_mx^{n+m}$. $a_n\neq 0$, $b_m\neq 0$ implies that $a_nb_m\neq 0$ and $\deg(f(x)g(x))=m+n=\deg f(x)+\deg g(x)$.

4. If R is an integral domain with unit element, prove that any unit in $R[x]$ must already be a unit in R.

166.4 Let $f(x)=a_0+a_1x+\cdots\cdots+a_nx^n$ be a unit in $R[x]$. There is $g(x)=b_0+b_1x+\cdots\cdots+b_mx^m$ in $R[x]$ such that $f(x)g(x)=1$. $\deg f(x)+\deg g(x) = \deg(f(x)g(x))=\deg(1)=0$. $\deg f(x)=0$, $\deg g(x)=0$. $f(x)\in R$, $g(x)\in R$. $f(x)g(x)=1$. $f(x)$ is a unit in R.

5. Let R be a commutative ring with no nonzero *nilpotent* elements (that is, $a^n = 0$ implies $a = 0$). If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ in $R[x]$ is a zero-divisor, prove that there is an element $b \neq 0$ in R such that $ba_0 = ba_1 = \cdots = ba_m = 0$.

166.5 There is a nonzero polynomial $g(x)=b_ix^i+b_{i+1}x^{i+1}+\cdots\cdots+b_nx^n$ in $R[x]$ such that $f(x)g(x)=0$ and $b_i\neq 0$. $f(x)g(x)=a_0b_ix^i+(a_0b_{i+1}+a_1b_i)x^{i+1}+(a_0b_{i+2}+a_1b_{i+1}+a_2b_i)x^{i+2}+\cdots\cdots+a_mb_nx^{m+n}=0$ implies

$$a_0b_i=0$$
$$a_0b_{i+1}+a_1b_i=0$$
$$a_0b_{i+2}+a_1b_{i+1}+a_2b_i=0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_0b_{i+k}+a_1b_{i+k-1}+a_2b_{i+k-2}+\cdots\cdots+a_kb_i=0$$
$$k=0,1,2,\cdots\cdots,m.$$

Let $b=b_i^{m+1}$. Since $b_i\neq 0$, $b\neq 0$. Claim $a_kb_i^{k+1}=0$. $k=0$ is trivial. Suppose $a_kb_i^{k+1}=0$ for $k=0,1,2,\cdots\cdots,r-1$. Then $0=(a_0b_{i+r}+a_1b_{i+r-1}+a_2b_{i+r-2}+\cdots\cdots+a_{r-1}b_{i+1}+a_rb_i)b_i^r=a_0b_i^rb_{i+r}+a_1b_i^rb_{i+r-1}+\cdots\cdots+a_{r-1}b_i^rb_{i+1}+a_rb_i^{r+1}=a_rb_i^{r+1}$. Therefore $a_rb_i^{r+1}=0$.

Hence $a_0b=a_1b=\cdots\cdots=a_mb=0$.

*6. Do Problem 5 dropping the assumption that R has no nonzero nilpotent elements.

166.6 There is $g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots\cdots+b_0$ $(b_n\neq 0)$ in $R[x]$ such that $f(x)g(x)=0$. we chaim that either we can find the required b or for a given $g(x)$ such that $f(x)g(x)=0$

there exists an $h(x)\neq 0$ in $R[x]$ such that $\deg h(x)<\deg g(x)$ and $h(x)f(x)=0$. For, if $a_mg(x)$, $a_{m-1}g(x)$, $\cdots\cdots$, $a_0g(x)$ are all zero, then $a_mb_n=a_{m-1}b_n=a_{m-2}b_n=\cdots\cdots=a_0b_n=0$ and $b_n\neq 0$. In this case, we have proved this exercise. If not, i.e. $a_mg(x)=a_{m-1}g(x)=\cdots\cdots=a_{i+1}g(x)=0$ but $a_ig(x)\neq 0$. Let $h(x)=a_ig(x)$. Since $g(x)f(x)=0$, $h(x)f(x)=(a_ig(x))f(x)=a_i(g(x)f(x))=0$.

$0=g(x)(a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_ix^i+a_{i-1}x^{i-1}+\cdots\cdots+a_0)=g(x)(a_ix^i+a_{i-1}x^{i-1}+\cdots\cdots+a_0)$, $a_ib_n=0$, $\deg h(x)=\deg a_ig(x)<\deg g(x)$.

Continue this process for $h(x)$, we can find a $b\in R$ such that $bf(x)=0$ with $b\neq 0$. This completes the proof.

*7. If R is a commutative ring with unit element, prove that $a_0 + a_1x + \cdots + a_nx^n$ in $R[x]$ has an inverse in $R[x]$ (i.e., is a unit in $R[x]$) if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent elements in R.

166.7 Suppose a_0 is a unit in R and $a_1,\cdots\cdots,a_n$ are nilpotent elements in R. We first show that the sum of two nilpotent elements in a commutative ring is also nilpotent. For, if r,s is nilpotent, then $r^l=s^m=0$ for some positive integers l and m. Then $(r+s)^{l+m+1}=0$. Hence, the sum of finite number of nilpotent elements in a commutative ring is also nilpotent. Now, $(a_1x+a_2x^2+\cdots\cdots+a_nx^n)$ is nilpotent since $a_1x, a_2x^2,\cdots\cdots,a_nx^n$ are. Say, $(a_1x+a_2x^2+\cdots\cdots+a_nx^n)^m=0$. Since a_0 is a unit in R, there is b_0 in R such that $a_0b_0=1$. $0=[b_0(f(x)-a_0)]^m=(b_0f(x)-1)^m$, $(1-b_0f(x))^m=0$, $1=f(x)g(x)$ for some $g(x)$. $f(x)$ has an inverse in $R[x]$.

Conversely, suppose $f(x)$ has an inverse $g(x)$ in

in $R[x]$ such that $f(x)g(x)=0$. We claim that $R[x]$. $g(x)=b_0+b_1x+\cdots\cdots+b_mx^m$ is of degree $m>0$. By what we have proved , we know that the set of all nilpotent elements in a commutative ring is an ideal . Now , let $k\leqslant n$ be a positive integer such that every coefficient a_i of $f(x)$ with $i>k$ is nilpotent , and let us show that a_k is nilpotent .
By considering the coefficients of $x^{k+m},\cdots\cdots,x^k$ in $f(x)g(x)=1$, we find that each of the following is nilpotent

$$a_kb_m ,$$
$$a_kb_{m-1}+a_{k-1}b_m$$
$$\vdots$$
$$a_kb_0+a_{k-1}b_1+\cdots\cdots$$

If we multiply the second of these expressions by a_k and use the fact that a_kb_m is nilpotent , we conclude that $a_k^2b_{m-1}$ is also nilpotent . Similarly , by multiplying the third expression by a_k^2 , we find that $a_k^3b_{m-2}$ is nilpotent . A continuation of this procedure shows that $a_k^{m+1}b_0$ is nilpotent . Since $a_0b_0=1$, it follows that $a_k^{m+1}b_0a_0$ is nilpotent and a_k^{m+1} is nilpotent , therefore a_k is nilpotent . This completes the proof .

8. Prove that when F is a field, $F[x_1, x_2]$ is not a principal ideal ring.

166.8 We will show that (x_1,x_2) , the ideal of $F[x_1,x_2]$ generated by x_1 and x_2 , is not a principal ideal , i.e. $(x_1,x_2)\neq(f(x_1,x_2))$ for $f(x_1,x_2)$ in $F[x_1,x_2]$. If $(x_1,x_2)=(f(x_1,x_2))$, then since x_1 and x_2 are irreducible elements in $F[x_1,x_2]$. $x_1=c_1f(x_1,x_2)$, $x_2=c_2f(x_1,x_2)$, a contradiction .

9. Prove, completely, Lemma 3.11.2 and its corollary.

166.9 Lemma 3.11.2: If R is a unique foctorization domain and if a,b are in R , then a and b have a greatest common divisor (a,b) in R . Moreover , if a and b are relatively prime (i.e.,(a,b)=1) , whenever $a\mid bc$ then $a\mid c$.

pf . Let $a=u_1p_1^{\alpha_1}\cdots\cdots p_k^{\alpha_k}$ and $b=u_2p_1^{\beta_1}\cdots\cdots p_k^{\beta_k}$ where the p_i are distinct prime elements and where each $\alpha_i\geqslant 0$ and $\beta_i\geqslant 0$. As in the proof of (23.5) we know that $p_1^{\delta_1}p_2^{\delta_2}\cdots\cdots p_k^{\delta_k}$ (where $\delta_i=$ minimum of α_i and β_i for each i) is a greatest common divisor of a and b .
If a and b are relatively prime , whenever $a\mid bc$, let $b=u_2p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_k^{\beta_k}$, $c=u_3p_1^{\gamma_1}p_2^{\gamma_2}\cdots\cdots p_k^{\gamma_k}$. $bc=u_2u_3p_1^{\beta_1+\gamma_1}p_2^{\beta_2+\gamma_2}\cdots\cdots p_k^{\beta_k+\gamma_k}$. Since $(a,b)=1$, $\alpha_i=0$ whenever $\beta_i\neq 0$ and $\beta_j=0$ whenever $\alpha_j\neq 0$. Therefore $a\mid c$.
Corollary . If $a\in R$ is an irreducible element and $a\mid bc$, then $a\mid b$ or $a\mid c$.
pf. If $a\nmid b$, then $(a,b)=1$. Hence $a\mid c$, by Lemma 3.11.2.

10. (a) If R is a unique factorization domain, prove that every $f(x)\in R[x]$ can be written as $f(x)=af_1(x)$, where $a\in R$ and where $f_1(x)$ is primitive.
(b) Prove that the decomposition in part (a) is unique (up to associates).

166.10 (a) Let $f(x)=a_0+a_1x+\cdots\cdots+a_nx^n$ and a is the greatest common divisor of $a_0,a_1\cdots\cdots$,

and a_n . Then $f(x)=af_1(x)$, where

$f_1(x)=\frac{a_0}{a}+\frac{a_1}{a}x+\cdots\cdots+\frac{a_n}{a}x^n$.

$f_1(x)$ is primitive .

(b) If $af_1(x)=bf_2(x)$ with $f_1(x)$ and $f_2(x)$ primitive and $f_1(x)=a_0+a_1x+\cdots\cdots+a_nx^n$, $f_2(x)=b_0+b_1x+\cdots\cdots+b_nx^n$, then $aa_0=bb_0$, $aa_1=bb_1$, $\cdots\cdots$, $aa_n=bb_n$. The greatest common divisor of $aa_0\ aa_1\cdots$, aa_1 is a and hence b . $a=bu$, where u is a unit in R . This completes the proof .

11. If R is an integral domain, and if F is its field of quotients, prove that any element $f(x)$ in $F[x]$ can be written as $f(x) = (f_0(x)/a)$, where $f_0(x) \in R[x]$ and where $a \in R$.

166.11 Let $f(x)=\frac{a_0}{b_0}+\frac{a_1}{b_1}x+\cdots\cdots+\frac{a_n}{b_n}x^n$. Then ; let $a=b_0b_1\cdots\cdots b_n$ we have $f(x)=\frac{1}{a}(a_0b_1b_2\cdots\cdots b_n+b_0a_1b_2\cdots\cdots b_nx+\cdots\cdots+b_0b_1b_2\cdots\cdots a_nx^n)$. This completes the proof .

12. Prove the converse part of Lemma 3.11.4.

166.12 Suppose $f(x)$ is primitive in $R[x]$ and irreducible in $F[x]$. If $f(x)=g(x)h(x)$ for $g(x)$, $h(x)$ in $R[x]$, then since $g(x)$, $h(x)$ is also in $F[x]$ and $f(x)$ is irreducible in $F[x]$, $g(x)\in F$ or $h(x)\in F$.

Let's say $h(x)=\frac{m}{n}\in F$. $h(x)\in R[x]$ implies (x) , $h(x)\in R$. Hence $f(x)$ is irreducible as an element of $R[x]$.

13. Prove Corollary 2 to Theorem 3.11.1.

166.13 We know that $F[x_1]$ is a unique factorization domain . $F[x_1,x_2,\cdots\cdots,x_n]=F[x_1][x_2,\cdots,x_n]$ is a unique factorization domain by Corollary 1 to Theorem 3.11.1 .

14. Prove that a principal ideal ring is a unique factorization domain.

166.14 For an element a in R , R a principal ideal ring , if a is not irreducible $a=b_1c_1$ with b_1 and c_1 not units in R . $(a)\subsetneq(b_1)$. If b_1 is not irreducible , $b_1=b_2c_2$ with b_2 and c_2 not units in R . $(b_1)\subsetneq(b_2)$, continuing the process , we get an irreducible element b_n . Otherwise , there is an infinite sequence $(a)\subsetneq(b_1)\subsetneq(b_2)\subsetneq\cdots\cdots$. $\bigcup_{i=1}^{\infty}(b_i)$ is also an ideal of R , $\bigcup_{i=1}^{\infty}(b_i)=(c)$ since R is a principal ideal ring . $c\in\bigcup_{i=1}^{\infty}(b_i)$ implies $c\in(b_k)$ for some k . $(c)\subset(b_k)$. $(b_k)=(c)$, contrary to $(b_k)\subsetneq(b_{k+1})$. Using this method , we can factorize a as a product of finite number of irreducible elements of R .

For a, b in R , $(a)+(b)=(c)$ for some c in R since R is a principal ideal ring . $c=ua+vb$ for some u, v in R . Since $a,b\in(c)$, c is a common divisor of a and b. On the other hand, any common divisor of a and b is also a divisor of c . Therefore, for any two elements a , b in R , there is a greatest common divisor c of a and b . Now , if π is a prime element in R and $\pi\mid bc$ and $\pi\nmid b$, then $(\pi,b)=1$, and hence $\pi\mid c$ since $c=c\cdot1=c(u\pi+vb)=cu\pi+vbc$. As in the proof of Theorem 3.7.2, we have completed the proof .

15. If J is the ring of integers, prove that $J[x_1, \ldots, x_n]$ is a unique factorization domain.

166.15 Since J is a unique factorization domain , by corollary 1 of Theorem 3.11.1 , $J[x_1, \cdots, x_n]$ is a unique factorization domain .

Supplementary Problems

Supplementary Problems

1. Let R be a commutative ring; an ideal P of R is said to be a *prime ideal* of R if $ab \in P$, $a, b \in R$ implies that $a \in P$ or $b \in P$. Prove that P is a prime ideal of R if and only if R/P is an integral domain.

167. Suppose P is a prime ideal of R and $(a+P)(b+P)=0$. Then $ab+P=0$, $ab \in P$ hence $a \in P$ or $b \in P$ and $a+P=0$ or $b+P=0$, i.e. R/P is an integral domain . Suppose , conversely , R/P is an integral domain and $ab \in P$. Then $(a+P)\cdot(b+P)=ab+P=0$, $a+P=0$ or $b+P=0$ i.e. $a \in P$ or $b \in P$. P is a prime ideal of R .

2. Let R be a commutative ring with unit element; prove that every maximal ideal of R is a prime ideal.

167.2 R/M is a commutative ring with unit element whose only ideals are (0) and R/M itself . Hence , by Theorem 3.5.1 , R/M is a field and therefore an integral domain . By (167.1) M is a prime ideal of R .

3. Give an example of a ring in which some prime ideal is not a maximal ideal.

167.3 The ring J of rational integers has (0) as a prime ideal since for $ab=0$ we have $a=0$ or $b=0$. But clearly (0) is not a maximal ideal of J .

4. If R is a finite commutative ring (i.e., has only a finite number of elements) with unit element, prove that every prime ideal of R is a maximal ideal of R.

167.4 Let P be a prime ideal of R . By (167.1) R/P is an integral domain . Since R/P is a finite integral domain , by Lemma 3.2.2., R/P is a field . Hence , by Theorem 3.5.1 , P is a maximal ideal of R .

5. If F is a field, prove that $F[x]$ is isomorphic to $F[t]$.

167.5 Define $\sigma : F[x] \longrightarrow F[t]$ by $\sigma(f(x)) = f(t)$, i.e. $\sigma : a_n x^n + a_n x^{n-1} + \cdots\cdots + a_0 \longrightarrow a_n t^n + a_{n-1} t^{n-1} + \cdots\cdots + a_0$. This is a one - to - one and onto homomorphism . Hence , $F[x]$ is isomormphic to $F[t]$.

6. Find all the automorphisms σ of $F[x]$ with the property that $\sigma(f) = f$ for every $f \in F$.

167.6 Such an automorphism σ of $F[x]$ must be linear , i.e. $\sigma(h(x)) = h(ax+b)$ for some $a, b \in F$ and $a \neq 0$. For , let $\sigma(x) = g(x) \in F[x]$. Then , clearly , $\sigma(k(x)) = k(g(x))$ for all $k(x)$ in $F[x]$. Since σ is an onto mapping , $g(x) = ax+b$ for some $a, b \in F$. Otherwise $x \notin \sigma(F[x])$. Conversely , every $\sigma : \sigma(h(x)) = h(ax+b)$ with $a, b \in F$ and $a \neq 0$, is an automormphism of $F[x]$.

7. If R is a commutative ring, let $N = \{x \in R \mid x^n = 0 \text{ for some integer } n\}$. Prove
   (a) N is an ideal of R.
   (b) In $\bar{R} = R/N$ if $\bar{x}^m = 0$ for some m then $\bar{x} = 0$.

167.7 (a) $a, b \in N$, then $a^n = 0$, $b^m = 0$ for some positive integers m and n . $(a+b)^{m+n+1} = 0$ and $(ac)^n = a^n c^n = 0$ for all $c \in R$. Hence N is an ideal of R .

(b) If $\bar{x}^m = 0$, then $x^m \in N$ and $(x^m)^n = 0$ for some positive integer n . Hence $x \in N$

and $\bar{x} = 0$.

8. Let R be a commutative ring and suppose that A is an ideal of R. Let $N(A) = \{x \in R \mid x^n \in A \text{ for some } n\}$. Prove
(a) $N(A)$ is an ideal of R which contains A.
(b) $N(N(A)) = N(A)$.
$N(A)$ is often called the *radical* of A.

168.8 (a) It's clear that $A \subset N(A)$. Suppose $a, b \in N(A)$ and $c \in R$, then $a^n, b^m \in A$ for some n , m . Now $(a+b)^{m+n+1} \in A$. For every term of the expression for $(a+b)^{m+n}$ is of the form ka^ib^j with $i+j=m+n+1$, therefore $n > i$ or $m > j$ and $ka^ib^j \in A$ since A is an ideal of R . $a+b \in N(A)$. $(ac)^n = a^n c^n \in A$, $ac \in N(A)$. $N(A)$ is an ideal of R .

(b) $N(N(A)) \supset N(A)$. Now, suppose $\in N(N(A))$. $x^n \in N(A)$ for some n and $(x^n)^m \in A$ for some m . Hence $x \in N(A)$. $N(N(A)) \subset N(A)$. $N(N(A)) = N(A)$.

9. If n is an integer, let J_n be the ring of integers mod n. Describe N (see Problem 7) for J_n in terms of n.

167.9 Let $p_1, p_2, \cdots\cdots, p_m$ be the prime divisors of n. $N = (p_1 p_2 \cdots\cdots p_m)$. (mod n). Let $n = p_1^{e_1} p_2^{e_2} \cdots\cdots p_m^{e_m}$. If $x \in (p_1 \cdots\cdots p_m)$ then $x = r p_1 \cdots\cdots p_m$ for some r . $x^{\max(e_1 \cdots\cdots e_m)}$ has n as a divisor . $x^{\max(e_1, \cdots\cdots, e_m)} = 0$ (mod n) . $x \in N$. Conversely , if $x \in N$, then $x^k = 0$ (mod n) for some k . $n \mid x^k$ $p_i \mid x^k$. $p_i \mid x$ $\therefore$ $p_1 p_2 \cdots\cdots p_m \mid x$. $\therefore$ $x \in (p_1 p_2 \cdots\cdots p_m)$ $\therefore$ $(p_1 \cdots\cdots p_m) = N$.

10. If A and B are ideals in a ring R such that $A \cap B = (0)$, prove that for every $a \in A$, $b \in B$, $ab = 0$.

167.10 $a \in A$, $b \in B$ implies $ab \in A$ since A is an ideal of R and $ab \in B$ since B is an ideal of R . $ab \in A \cap B = (0)$. Hence $ab = 0$.

11. If R is a ring, let $Z(R) = \{x \in R \mid xy = yx \text{ all } y \in R\}$. Prove that $Z(R)$ is a subring of R.

167.11 $x, y \in Z(R)$ implies $xz = zx$ and $yz = zy$ for all z in R . $(x-y)z = xz - yz = zx - zy = z(x-y)$ for all z in R and $(xy)z = xzy = z(xy)$. Hence $Z(R)$ is a subring of R .

12. If R is a division ring, prove that $Z(R)$ is a field.

167.12 $Z(R)$ is a commutative subgring of R . If $x \in Z(R) \setminus 0$, $xz = zx$ for all z in R . Since R is a division ring $x^{-1}z = zx^{-1}$ for all z in R . Hence $x^{-1} \in Z(R)$ for all $x \in Z(R) \setminus 0$. Therefore , the nonzero elements of $Z(R)$ form a subgroup of $R \setminus 0$ under multiplication . Hence $Z(R)$ is a field .

13. Find a polynomial of degree 3 irreducible over the ring of integers, J_3, mod 3. Use it to construct a field having 27 elements.

167.13 $x^3 - x + 1$ is a polynomial of degree 3 irreducible over the ring of integers , J_3 , mod 3 . $J_3[x]/(x^3 - x + 1)$ is a field having 27 elements by (159.7) .

14. Construct a field having 625 elements.

167.14 $x^4 + x - 1$ is an irreducible polynomial of degree 4 over the ring of integers , J_5 , mod 5 . To prove this fact , we first show that all $1, 2, 3, 4$ are not roots of $x^4 + x - 1$ in J_5 and (x^2+2) , (x^2+3) , (x^2+x+1) , (x^2+x+2) , (x^2+2x+3) , (x^2+2x+4) , (x^2+3x+3) , (x^2+3x+4) , (x^2+4x+1) , (x^2+4x+2) are

all irreducible polynomials of degree two in $J_5[x]$. Then show that x^4+x-1 is not the product of two irreducible polynomials of degree two . Hence x^4+x-1 is irreducible . $J_5[x]/(x^4+x-1)$ is a field having 625 elements by (159.7) .

15. If F is a field and $p(x) \in F[x]$, prove that in the ring

$$R = \frac{F[x]}{(p(x))},$$

N (see Problem 7) is (0) if an only if $p(x)$ is not divisible by the square of any polynomial of positive degree.

167.15 Suppose $p(x)$ is divisible by the square of a polynomial of positive degree , say $p(x)=p_1^2(x)q(x)$, then $p_1(x)q(x)+(p(x)) \neq 0$, and $(p_1(x)q(x))^2+(p(x)) = 0$. Hence $p_1(x)q(x)+(p(x)) \in N \setminus 0$. Therefore , if $N=(0)$, $p(x)$ is not divisible by the square of any polynomial . Conversely , suppose $p(x)$ is not divisible by the square of any polynomialof positive degree , i.e. $p(x)=p_1(x)p_2(x)\cdots\cdots p_n(x)$, where $p_i(x)'$s are distinct irreducible polynomials . Then $q(x)+(p(x)) \in N$. implies $(q(x))^m+(p(x)) = 0$ for some m . $q(x)^m \in (p(x))$ $p_i(x) \mid (q(x))^m$, $p_i(x) \mid q(x)$, $p_1(x) \cdots p_n(x) \mid q(x)$, $p(x) \mid q(x)$, $q(x) \in (p(x))$,. $q(x)+(p(x)) = 0$ $N=(0)$.

16. Prove that the polynomial $f(x) = 1 + x + x^3 + x^4$ is not irreducible over any field F.

168.16 $f(x)= 1+x+x^3+x^4=(1+x)^2(1-x+x^2)$.

17. Prove that the polynomial $f(x) = x^4 + 2x + 2$ is irreducible over the field of rational numbers.

168.17 By Theorem 3.10.2 (The Eisenstein Criterion) $f(x)$ is irreducible over the field of rational numbers .

18. Prove that if F is a finite field, its characteristic must be a prime number p and F contains p^n elements for some integer. Prove further that if $a \in F$ then $a^{p^n} = a$.

168.18 By (130.6) the characteristic of F must be a prime number p . Consider the additive group of F , since F is a p-group , F contains p^n elements for some integer n . Now , consider the multiplicative group of nonzero elements of F , it's of order p^n-1 . Hence , for all $a \in F \setminus 0$, $a^{p^n-1}=1$ and $a^{p^n}=a$. If $a=0$, $a^{p^n}=a$. $a^{p^n}=a$ holds for all a in F .

19. Prove that any nonzero ideal in the Gaussian integers $J[i]$ must contain some positive integer.

168.19 Let N be a nonzero ideal of $J[i]$. $a+bi \in N \setminus 0$. Since $a-bi \in J[i]$ and N is an ideal of $J[i]$, $a^2+b^2=(a+bi)(a-bi) \in N \setminus 0$.

20. Prove that if R is a ring in which $a^4 = a$ for every $a \in R$ then R must be commutative.

168.20 $(-x)=(-x)^4=x^4=x$. R has no nonzero nilpotent element and hence every idempotent is in Z(R) by (136.19).
$(x^2+x)^2=x^4+x^2+2x^3=x^4+x^2=x+x^2$ since $2a=0$ for all a in R . x^2+x is an idempotent . Hence $x^2+x \in Z(R)$ for all x in R .
$(a+b)+(a+b)^2 \in Z(R)$. i.e. $(a+a^2)+(b+b^2)+(ab+ba) \in Z(R)$, $a+a^2$, $b+b^2 \in Z(R)$ since Z(R) is a subring of R . $ab+ba \in Z(R)$ for all a, b in R . $(ab+ba)a=a(ab+ba)$, $a^2b=ba^2$. Hence $a^2 \in Z(R)$, $a^4 \in Z(R)$. $a=a^4 \in Z(R)$. R is commutative .

21. Let R and R' be rings and ϕ a mapping from R into R' satisfying (a) $\phi(x + y) = \phi(x) + \phi(y)$ for every $x, y \in R$.

(b) $\phi(xy) = \phi(x)\phi(y)$ or $\phi(y)\phi(x)$.
Prove that for all $a, b \in R$, $\phi(ab) = \phi(a)\phi(b)$ or that, for all $a, b \in R$, $\phi(a) = \phi(b)\phi(a)$. (*Hint:* If $a \in R$, let

$$W_a = \{x \in R \mid \phi(ax) = \phi(a)\phi(x)\}$$

and

$$U_a = \{x \in R \mid \phi(ax) = \phi(x)\phi(a)\}.)$$

168.21 It's easy to check that Wa and Ua are additive subgroups of R and R=Wa $\cup$ Ua for all a in R . By (118.31) Wa = R or Ua = R for all a in R .
Now , let W= { a$\in$R| Wa = R} , U= { a$\in$R| Ua=R} . It's also easy to check that W and U are additive subgroups of R and R = W $\cup$ U . By (118.31) W=R or U=R . Hence for all a,b$\in$R , ϕ(a b)=ϕ(a)ϕ(b) or for all a,b$\in$R , ϕ(a b)=ϕ(b) ϕ(a) .

22. Let R be a ring with a unit element, 1, in which $(ab)^2 = a^2b^2$ for all $a, b \in R$. Prove that R must be commutative.

168.22 By (a(b+1))^2=a^2(b+1)^2 and (a b)^2=a^2 b^2 we can get aba=a^{2}b for all a ,b in R . By (a+1)b (a+1) =(a+1)^{2}b and aba = a^{2}b we can get ab =ba . Hence R is commutative .

23. Give an example of a noncommutative ring (of course, without 1) in which $(ab)^2 = a^2b^2$ for all elements a and b.

168.23 $R = \left\{ \begin{pmatrix} 0 & \alpha \\ 0 & \beta \end{pmatrix} \mid \alpha, \beta \in F \right\}$, where F is a field .

24. (a) Let R be a ring with unit element 1 such that $(ab)^2 = (ba)^2$ for all $a, b \in R$. If in R, $2x = 0$ implies $x = 0$, prove that R must be commutative.
(b) Show that the result of (a) may be false if $2x = 0$ for some $x \neq 0$ in R.
(c) Even if $2x = 0$ implies $x = 0$ in R, show that the result of (a) may be false if R does not have a unit element.

168.24 (a) By (a(b+1))^2=((b+1)a)^2 and (ab)^2=(ba)^2 we have a^{2}b=ba^2 for all a,b in R . By (a+1)^{2}b=b(a+1)^2 and a^{2}b=ba^2 we have ab = ba . Hence R is commutative .

(b) $R = \left\{ \begin{pmatrix} d & a & b \\ 0 & d & c \\ 0 & 0 & d \end{pmatrix} \mid a, b, c, d \in J_2 \right\}$.

(c) $R = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \mid a, b, c \in F \right\}$, where F is a field .

25. Let R be a ring in which $x^n = 0$ implies $x = 0$. If $(ab)^2 = a^2b^2$ for all $a, b \in R$, prove that R is commutative.

168.25 ((a+b) b)^2=(a+b)^2 b^2 implies b^{2}ab= bab^2, i.e. b(ba$-$ ab)b= 0 ·····①
(ab)^2=a^{2}b^2 implies a (ba$-$a b) b= 0·····②.
a b (b a$-$a b) b= 0 ·····③
b a (b a$-$a b) b= 0 ·····④ . By ④ $-$ ③
(b a$-$ a b)^2 b= 0 , (b a$-$ a b)^2 b a= 0 ·····⑤
Change the places of a and we have
(a b$-$ b a)^2 a b= 0 ·····⑥ . By ⑤ $-$ ⑥
(b a$-$ a b)^2(b a$-$ a b) = 0 , i.e. (b a$-$ a b)^3 = 0.
By assumption ba=ab . This completes the proof .

26. Let R be a ring in which $x^n = 0$ implies $x = 0$. If $(ab)^2 = (ba)^2$ for all $a, b \in R$, prove that R must be commutative.

168.26 (i) $0 = ((ab)^2b)^2 - ((ab)b(ab))^2$
$= (ab)^2b(ab)^2b - (ab)b(ab)^2b(ab)$
$= (ab)^2(baba)b^2 - (ab)(baba)b^2ab$
$= (ab)^2(ab)^2b^2 - (ab)(ab)^2b^2ab$
$= (ab)^3(ab^3 - b^2ab)b$
$= (ab)^3(ab^2 - b^2a)b.$
Let $x = ab^2 - b^2a$. Then $(ab)^3xb = 0$.
(ii) uv=0 implies vu=0 and u^{n}v=0 implies

$uv=vu=0$.

pf. $(vu)^2=(vu)(vu)=v(uv)u=0$. Hence $vu=0$.

Suppose $u^nv=0$ for $n \geq 2$. We want to show that $u^{n-1}v=0$. $u^nv=0$ implies $u^{n-1}vu=0$.

$(u^{n-1}v)^2=(u^{n-1}v)(u^{n-1}v)=(u^{n-1}vu)(u^{n-2}v)=0$.

Hence $u^{n-1}v=0$. By induction, we have $uv=0$.

(iii) For all a in R. we have $a^2 \in Z(R)$.

pf. It suffices to show that $x=0$ in (i)

$(ab)^3xb=0$ implies $abxb=0$ and $xbab=0$.

$xbaba=0$. $x(ba)^2=0$. $xba=0$. $axb=0$. $axb^2=0$.

$xb^2a=0$.

$xba=0$. $bax=0$. $baxab=0$. $xab^2a=0$. $xab^2ab^2=0$.

$x(ab^2)^2=0$. $xab^2=0$. $x^2=x(ab^2-b^2a)=$

$xab^2-xb^2a=0-0=0$. $x=0$. $a^2 \in Z(R)$.

(iv) $y \in R$. $2y=0$ implies $y \in Z(R)$.

pf. $z \in R$. $(yz-zy)^2$

$=(yz)(yz)-yz^2y-zy^2z+(zy)(zy)$

$=((-y)(z))(yz)-(-y)z^2y-zy^2z+(zy)(zy)$

$=-(yz)(yz)+yz^2y-zy^2z+(zy)^2$

$=-(yz)^2+y^2z^2-y^2z^2+(zy)^2$

$=0$.

$yz-zy=0$. $y \in Z(R)$.

(v) $a^2, b^2, (ab+ba)^2 \in Z(R)$. Hence $ab+ba \in Z(R)$ for all a,b in R. $a^2b+ba^2=2a^2b \in Z(R)$.

$2a^2bc=(2a^2b)c=c(2a^2b)=2a^2cb$, $2a^2(bc-bc)=0$ for all a,b, c in R. Hence $2(bc-cb)^2(bc-cb)=0$.

$2(bc-cb)^3=0$. $8(bc-cb)^3=0$. $2(bc-cb)=0$.

$bc-cb \in Z(R)$ by (iv). $2b(bc-cb)=0$. $b(bc-cb) \in Z(R)$.

$(bc-cb)bc=((bc-cb)b)c=c((bc-cb)b)$

$=c(b(bc-cb))=(cb)(bc-cb)=(bc-cb)(cb)$. 0

$=(bc-cb)(bc-cb)=(bc-cb)^2$ implies $bc-cb=0$ for all b, c in R. This completes the proof of the exercise.

27. Let $p_1, p_2, \ldots, p_k$ be distinct primes, and let $n = p_1p_2 \cdots p_k$. If R is the ring of integers modulo n, show that there are exactly 2^k elements a in R such that $a^2 = a$.

168.27 We first prove Chinese Remainder Theorem. Let $m_1, m_2, \ldots\ldots, m_k$ denote positive integers that are relatively prime in pairs, and let $a_1, a_2, \ldots\ldots, a_k$ denote any k integers. Then the congruences $x \equiv a_i \pmod{m_i}$, $i=1,2,\cdots,k$, have common solutions. Any two solutions are congruent modulo m_1m (c.f. the proof of (108.7))

Proof of Chinese Remainder Theorem: Writting $m=m_1 \cdots\cdots m_k$ we see that m/m_j is an integer and that $(m/m_j, m_j)=1$. Therefore, by (36.15.(b)), there are integers b_j such that $(m/m_j)b_j \equiv 1 \pmod{m_j}$. Clearly $(m/m_j)b_j \equiv 0 \pmod{m_i}$ if $i \neq j$. Now, if we define x_0 as

$$x_0 = \sum_{j=1}^{k} \frac{m}{m_j} b_j a_j$$

we have $x_0 \equiv \sum_{j=1}^{k} \frac{m}{m_j} b_j a_j \equiv \frac{m}{m_i} b_i a_i \equiv a_i \pmod{m_i}$

so that x_0 is a common solution of the original congruences. If x_0 and x_1 are both common solutions of $x \equiv a_i \pmod{m_i}$, $i=1,\ldots\ldots,k$, then $x_0 \equiv x_1 \pmod{m_i}$ for $i=1,2,\ldots\ldots,k$ and hence $x_0 \equiv x_1 \pmod{m}$ since $m_1m_2 \cdots\cdots m_k \mid x_0 - x_1$. This completes the proof.

proof of the exercise: The equation $x^2 \equiv x \pmod{n}$ is equivalent to $x^2 \equiv x \pmod{p_i}$ for $i=1,2,\ldots\ldots,k$. Hence $x \equiv 0$ or $1 \pmod{p_i}$, $i=1,2,\ldots\ldots,k$.

Therefore, there are exactly 2^k solutions modulo n.

28. Construct a polynomial $q(x) \neq 0$ with integer coefficients which has no rational roots but is such that for any prime p we can solve the congruence $q(x) \equiv 0 \bmod p$ in the integers.

168.28 $q(x)=(x^2-3)(x^2-5)(x^2-15)$. $q(x)$ has clearly no rational roots. For any prime p, $x^2 \equiv a \pmod p$ has roots if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ by (116.3). If $x^2 \equiv 3$ and $x^2 \equiv 5 \pmod p$ has no roots, then $3^{\frac{p-1}{2}} \equiv -1$ and $5^{\frac{p-1}{2}} \equiv -1$, $(3\cdot 5)^{\frac{p-1}{2}} \equiv 3^{\frac{p-1}{2}} \cdot 5^{\frac{p-1}{2}} \equiv (-1)\cdot(-1) \equiv 1 \pmod p$. $x^2 \equiv 15$ has solution. $(x^2-3)(x^2-5)(x^2-15)$ has solution in modulo p.

Topic for Class Discussion

MOTZKIN, T., "The Euclidean algorithm," *Bulletin of the American Mathematical Society*, Vol. 55 (1949), pages 1142–1146.

THE EUCLIDEAN ALGORITHM

TH. MOTZKIN

In this note a constructive criterion for the existence of a Euclidean algorithm within a given integral domain is derived, and from among the different possible Euclidean algorithms in an integral domain one is singled out. The same is done for "transfinite" Euclidean algorithms. The criterion obtained is applied to some special rings, in particular rings of quadratic integers. By an example it is shown that there exist principal ideal rings with no Euclidean algorithm. Finally, different sets of axioms for the Euclidean algorithm and related notions are compared, and the possible implications for the classification of principal ideal rings, and other integral domains, indicated.

The question of the relationship between different Euclidean algorithms in the same integral domain was raised (orally) by O. Zariski.

1. The derived sets. Let Q be an integral domain. A subset P of $Q-0$ (Q except zero) shall be called a *product ideal* if $P(Q-0)\subseteq P$.

For any subset S of Q, the set B of all b in Q for which there exists an a in Q such that $a+bQ\subseteq S$ is called the *total derived set* of S, and the intersection $B\cap S$ is called the *derived set* S'. With S also S' is a product ideal. If $S_1\subseteq S$, then $S_1'\subseteq S'$.

A *Euclidean algorithm* (or process) is given by a norm $|a|$ defined in $Q-0$, with positive integral (or zero) values and such that $|a| \geqq |b|$ for b dividing a and that for any b in $Q-0$ and any a not divisible by b there exist q and r in Q satisfying $a=qb+r$, $|r|<|b|$.

Let P_i, $i=0, 1, 2, \cdots$, be the set of all b in Q with $|b| \geqq i$. Obviously P_i is a product ideal. For any b in P_i', let a be an element with $a+bQ\subseteq P_i$, whence $a-bq\neq 0$ and (for any $r=a-bq$ with $|r|<|b|$) $|r|\geqq i$, $|b|\geqq i+1$; we see that $P_i'\subseteq P_{i+1}$. Conversely, given a sequence $Q-0=P_0\supseteq P_1\supseteq \cdots$ of product ideals with empty intersection $\bigcap P_i$ such that $P_i'\subseteq P_{i+1}$, the norm defined by $|b|=i$ for every b in P_i-P_{i+1} will fulfil the conditions for a Euclidean algorithm. Hence *there is a one-one correspondence between sequences of this kind and Euclidean algorithms.*

If for another Euclidean algorithm, with the sequence $\overline{P}_i$, always $P_i\subseteq \overline{P}_i$, we say that the first algorithm is the *faster* one (under cer-

Presented to the Society, October 30, 1948; received by the editors September 28, 1948.

tain additional conditions, indeed less algorithm steps are needed).

If there exists at all a Euclidean algorithm in Q, then *there exists a fastest Euclidean algorithm* defined by the sequence $P_0, P_0', P_0'', \cdots$. Hence *the emptiness of the intersection* $\cap P_0^{(i)}$ *is a criterion* (n.a.s.c.) *for the existence of a Euclidean algorithm in* Q.

Any sequence (P_i) as above may be changed to a new sequence $P_1, \cdots, P_{i-1}, \overline{P}_i, \overline{P}_i', \overline{P}_i'' \cdots$, where $\overline{P}_i$ is a product ideal with $P_{i-1} \supseteq \overline{P}_i \supseteq (P_{i-1})'$, so (besides the trivial repetition of identical product ideals) there always exist, if any, different Euclidean algorithms except if there are no product ideals between any $P_0^{(i)}$ and $P_0^{(i+1)}$.

2. Generalization. These considerations may be generalized as follows. Let a *tea* (*transfinite Euclidean algorithm*) be an algorithm as before but where (1) we allow $|b|$ to take any ordinal numbers as values; (2) we do not require $|a| \geqq |b|$ for b dividing a. Then it is seen in the usual way that the existence of a *tea* implies that Q is a principal ideal ring.

Further, such a *tea* determines, and is determined by, a transfinite sequence S_λ, $0 \leqq \lambda \leqq \mu$, of subsets of $Q-0$ with (1) $S_\lambda' \subseteq S_{\lambda+1}$, (2) $S_\lambda \subseteq S_{\lambda-1}$, but $S_\lambda = \cap S_i$, $i<\lambda$, if $\lambda-1$ does not exist, (3) empty S_μ.

Defining "faster" as before there is again a *fastest tea* given by $P_0^{(\lambda)}$, where $S^{(\lambda)}$ is defined as $(S^{(\lambda-1)})'$ or $\cap S^{(i)}$, $i<\lambda$.

Hence *the criterion for the existence of a tea is the emptiness of some* $P_0^{(\omega)}$.

For the fastest *tea* the sequence consists of product ideals, so that the monotonity condition $|a| \geqq |b|$ for b dividing a is automatically fulfilled.

If no $P_0^{(\lambda)}$ vanishes then there is no *tea*. If Q is not a principal ideal ring this is certainly so, but even for a principal ideal ring the constant $P_0^{(\omega)}$ (which is the largest subset S of Q with $S=S'$, and therefore never a principal ideal) may not be empty, as shown by some of the following examples.

3. Examples. The derived set S' of a given set S may also be defined as the set obtained from S by exemption of all b such that for every a, b divides some $a+c$ with c not in S. In particular P_0' is the set of all non-units except 0. Now call a non-unit $b \neq 0$ a *side divisor* of a if b divides some $a+e$, where e is a unit or 0. Then P_0'' is obtained from P_0' by exemption of the *universal side divisors*, that is, of those elements b which are side divisors of every a in Q, or equivalently for which there is a unit, or 0, in every residue class mod b. Such an element is obviously prime; the principal ideal (b) must even be

maximal. If no universal side divisors exist, then $P_0'' = P'$, and there is, except for the trivial case of a field, no *tea* in Q.

For the ring of rational integers, $Q-P_0'$ has three elements $0, \pm 1$. Hence the universal side divisors are ± 2 and ± 3, and $Q-P_0''$ contains all c with $|c| < 2^2$. By induction, b is in $P_0^{(i)}$ if and only if $|b| \geqq 2^i$. The fastest Euclidean algorithm is given by $a = bq+r$ with minimal $|r|$ (in a fixed algorithm q and r need not be unique).

$P_0'' = P_0'$ holds for the algebraic integers of every quadratic number field with negative discriminant d except $-1, -2, -3, -7, -11$. This can be seen as follows. It is well known that the above integers are the numbers $f+gd^{1/2}$, where f and g denote arbitrary rational integers, and in addition, if 4 divides $d-1$, the numbers $f+1/2+(g+1/2)d^{1/2}$. It follows easily that, except for the five stated values of d, 2 and 3 are irreducible and ± 1 the only units, so that the only side divisors of 2 are ± 2, ± 3; but these are not side divisors of $(1+d^{1/2})/2$, and if this is not an integer, of $d^{1/2}$. Hence there are no universal side divisors. For the excepted values of d there are respectively 12, 4, 24 4, 4 universal side divisors, among which all the 22 non-real quadratic integers b with $1 < b\bar{b} \leqq 3$ occur. (Dedekind [2, Supplement XI, §159 (4th ed., 1894, p. 451)][1] stated that the usual norm gives no Euclidean algorithm for the principal ideal ring belonging to $d=-19$. Hasse [4, p. 11] asked whether a Euclidean algorithm might be obtained by another norm, retaining the multiplicativity condition $|ab| = |a||b|$. We see that this is not the case, even without this condition and allowing ordinal numbers as norm values. Hence we have an example of a principal ideal ring with no Euclidean algorithm. The given result for arbitrary negative discriminant generalizes, and contains a new proof of, the similar result of Dickson [3, pp. 150–151] for the usual norm. For this norm and positive discriminant the question is not entirely solved, see Chatland [1], with further references.)

We have also $P_0' = P_0'$ for the ring of all polynomials, or power series, of one variable over an integral domain that is not a field. Likewise, for a valuation ring with no smallest positive value, $P_0' = P_0'$. If a smallest positive value v exists, then $P_0^{(i)}$ is the set of all elements whose value is at least i, and $P_0^{(\omega)} = P_0^{(\omega+1)}$. In particular for the power series of one variable over a field, $P_0^{(\omega)} = 0$. Similarly for the polynomials of one variable over a field, $P_0^{(i)}$ is the set of all polynomials of degree not less than i. This is a special case of the next example.

[1] Numbers in brackets refer to the references cited at the end of the paper.

Quotient rings. If, within the affine space over an algebraically closed field K of arbitrary characteristic, C is a rational curve with no singular point at finite distance, then the ring of all rational functions on C with no poles at finite distance is a principal ideal ring (for example, since we shall see that it has a Euclidean algorithm). The ring consists of all those rational functions with coefficients in K, of a parameter t on C, whose poles belong to a given finite set $(t_1, \cdots, t_r)$. Subjecting t, if necessary, to a broken linear transformation, we may suppose $t_1 = \infty$. In this case $P^{(i)}$ is the set of all the functions in the ring that have at least i zeros (with due counting of multiplicities) outside $(t_1, \cdots, t_r)$. Indeed, define $|a|$ accordingly as the number of zeros of a outside $(t_1, \cdots, t_k)$; to prove that $|a - bq| < |b|$ can be solved we may (multiplying both by a polynomial c with $|c| = 0$) suppose that a and b are polynomials and (shifting other factors of b to q) that b has no zero in $(t_1, \cdots, t_k)$, in which case the usual polynomial q will do. And obviously, since for $|a_1| < |b|$, $|a_2| < |b|$, $a_1 \neq a_2$, never $a_1 - a_2 = bq$, no faster Euclidean algorithm exists.

Similarly a *tea* may be defined in any quotient ring of an integral domain with a given *tea* by letting $|a|$ be the smallest value of $|am/n|$ in the original ring, where m and n are elements of a fixed multiplicatively closed set of denominators that yields the quotient ring considered.

5. **Related notions.** If we modify the definition of the derived set by demanding the existence of an a (not divisible by b) such that $aM + bN \subseteq (S, 0)$, where M and N are given subsets of Q (for instance, the set $0, \pm 1, \pm 2, \cdots$), we obtain sequences of subsets quite similar to those obtained before, which contract the faster the larger the sets M and N are. Here too P_0 is the set of non-units except 0. For $M = N = Q$ and if Q is a principal ideal ring, $P_0^{(\omega)}$ is the set of all elements that are products of at least i primes, so $P_0^{(\omega)} = 0$; the corresponding (multiplicative) norm being γ^i with fixed $\gamma > 1$.

Comparing the strength of different notions similar to the usual Euclidean algorithm, we may consider an algorithm (j, k, l), where $j = 1$ means that the norm shall be a positive integer, $j = 2$ that it be within a set of real positive numbers with no limit point except ∞, $j = 3$ that it be an ordinal number; $k = 1$ that $|ab| = |a|\,|b|$, $k = 2$ that $|a| \geqq |b|$ for b dividing a, $k = 3$ no such condition; $l = 1$ that, for any $b \neq 0$ and a not divisible by b, there exists some q with $|a - bq| < |b|$, $l = 2$ that, in the only relevant case $|a| \geqq |b|$, there only need exist m and q with $|am - bq| < |b|$ and m prime to b (that is, b shall divide mn only if it divides n), $l = 3$ the same, demanding only $|am - bq| < |a|$, $l = 4$ again demanding that $|am - bq| < |b|$, but with no restriction for m. So l determines the stepping down condition characteristic for the "descente infinie" application of Euclidean algorithms. We exclude the case $j = 3$, $k = 1$.

Then the existence of any algorithm (j, k, l) clearly implies that the integral domain Q is a principal ideal ring. It is easily seen that in every principal ideal ring the before mentioned norm γ^i fulfils (1, 1, 2) (see, for example, [4, pp. 7–8]), so that every combination with $l > 1$ gives a n.a.s.c. for principal ideal rings. On the other hand, even the weakest condition with $l = 1$, which is (3, 3, 1), is not always fulfilled in principal ideal rings, as we have shown; and (3, 3, 1) as equivalent to (3, 2, 1), (2, 3, 1) is equivalent to (2, 2, 1), (1, 3, 1), and (1, 2, 1), and finally (2, 1, 1) to (1, 1, 1), while it remains open whether these three sets of conditions are really of different strength.

A further classification of integral domains may be made according to the number μ of §2, or by (M, N)-stepping down conditions. That the fact that (1, 1, 3) is fulfilled for $M = (1)$, $N = (\pm 1)$ in the ring of rational integers is the essence of the simple Kronecker-Zermelo proof [4, p. 3] of unique decomposition into primes. For a similar, still weaker condition than $l = 4$ characterizing integral domains with unique decomposition into primes, see Krull [5, pp. 107–108]; also with respect to that condition derived sets may be defined and integral domains grouped according to whether the constant $P^{(\omega)}$ is or is not empty, and according to μ.

References

1. H. Chatland, *On the Euclidean Algorithm in quadratic number fields* Bull Amer. Math. Soc. vol. 55 (1949) pp. 948–953.

2. L. Dickson, *Algebren und ihre Zahlentheorie*, Zürich and Leipzig, 1927.

3. P. G. Lejeune Dirichlet, *Vorlesungen über Zahlentheorie*, ed. by R. Dedekind.

4. H. Hasse, *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen*, J. Reine Angew. Math. vol. 159 (1928) pp. 3–12.

5. W. Krull, *Idealtheorie*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vols. 4, no. 3, 1935.

Hebrew University and
Harvard University

4 Vector Spaces and Modules

4.1 Elementary Basic Concepts

1. In a vector space show that $\alpha(v - w) = \alpha v - \alpha w$.

175.1 $\alpha\omega + \alpha(-\omega) = \alpha(\omega + (-\omega)) = \alpha \cdot 0 = 0$

$\alpha(-\omega) = -\alpha\omega$.

$\alpha(v - \omega) = \alpha(v + (-\omega)) = \alpha v + \alpha(-\omega)$

$= \alpha v + (-\alpha\omega) = \alpha v - \alpha\omega$.

2. Prove that the vector spaces in Example 4.1.4 and Example 4.1.2 are isomorphic.

175.2 Define $f : V_n \to V$ as

$f(a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots\cdots + a_0)$

$= (a_{n-1}, a_{n-2}, \cdots\cdots, a_0)$.

Evidently, f is an isomorphism of V_n onto V.

V_n and V are isomorphic.

3. Prove that the kernel of a homomorphism is a subspace.

175.3 Let W be the kernel of a homomorphism T.

$u, v \in W$ implies $f(u + v) = f(u) + f(v)$

$= 0 + 0 = 0$,

$u + v \in w$, $\alpha \in F$. $f(\alpha \cdot v) = \alpha f(v) = \alpha \cdot 0$

$= 0$, $\alpha v \in W$.

W is a subspace.

4. (a) If F is a field of real numbers show that the set of real-valued, continuous functions on the closed interval [0, 1] forms a vector space over F.

(b) Show that those functions in part (a) for which all nth derivatives exist for $n = 1, 2, \ldots$ form a subspace.

175.4 (a) Let f and g be real continuous functions on $[0, 1]$.

$f + g$ is also a real continuous functions on $[0, 1]$. If h is also a real continuous functions on $[0, 1]$, then $(f + g) + h = f + (g + h)$. 0, a real function which maps

every point of $[0, 1]$ to 0, is a continuous function and $0 + f = f + 0 = 0$. $-f$, a real function which maps x on $[0, 1]$ to $-f(x)$, is a continuous function. $f + (-f) = 0$, $f + g = g + f$. The set C of all real continuous functions on $[0, 1]$ forms an abelian group.

$\alpha, \beta \in F$. $\alpha f \in C$, $\alpha(f + g) = \alpha f + \alpha g$.

$(\alpha + \beta)f = \alpha f + \beta f$ $(\alpha\beta)(f) = \alpha(\beta f)$

$1 \cdot f = f$ C is a vector space over F.

(b) $X = \{f \in C \mid$ the n-th derivatives exist for $n = 1, 2, \cdots\cdots\}$

$\alpha \in F$, $f \in X$, $g \in X$ then the n-th derivatives of $f + g$, αf exist for $n = 1, 2, \cdots\cdots$, X is a subspace of C.

5. (a) Let F be the field of all real numbers and let V be the set of all sequences $(a_1, a_2, \ldots, a_n, \ldots)$, $a_i \in F$, where equality, addition and scalar multiplication are defined componentwise. Prove that V is a vector space over F.

(b) Let $W = \{(a_1, \ldots, a_n, \ldots) \in V \mid \lim_{n\to\infty} a_n = 0\}$. Prove that W is a subspace of V.

*(c) Let $U = \{(a_1, \ldots, a_n, \ldots) \in V \mid \sum_{i=1}^{\infty} a_i^2$ is finite$\}$. Prove that U is a subspace of V and is contained in W.

175.5 (a) $\alpha = (a_1, a_2, \cdots\cdots, a_n, \cdots\cdots)$,

$\beta = (b_1, b_2, \cdots\cdots, b_n, \cdots\cdots) \in V$

implies

$\alpha + \beta = (a_1 + b_1, a_2 + b_2, \cdots\cdots, a_n + b_n, \cdots\cdots) \in V$.

If $\gamma = (c_1, c_2, \cdots, c_n, \cdots) \in V$,

then $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$,

$0 = (0, 0, \cdots\cdots, 0, \cdots) \in V$. $\alpha + 0 = \alpha$

$-\alpha = (-a_1, -a_2, \cdots, -a_n, \cdots\cdots) \in V$,

$\alpha + (-\alpha) = 0$. $\alpha + \beta = \beta + \alpha$.

V is an abelian group.

$a, b \in F$. $a(\alpha + \beta) = a(a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n, \cdots\cdots)$

$$= (a (a_1 + b_1), a (a_2 + b_2), \cdots, a (a_n + b_n), \cdots\cdots)$$
$$= a\alpha + a\beta .$$

$(a+b)\alpha = a\alpha + b\alpha$, $a(b\alpha) = (ab)\alpha$, $1\alpha = \alpha$, V is a vector space over F.

(b) $\alpha = (a_1, a_2, \cdots, a_n, \cdots)$,
$\beta = (b_1, b_2, \cdots, b_n, \cdots) \in W$.

$$\lim_{n\to\infty} (a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n = 0 + 0 = 0.$$

$$\alpha + \beta = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n, \cdots\cdots) \in W$$

$$a \in F , \lim_{n\to\infty} a a_n = a \lim_{n\to\infty} a_n = a \cdot 0 = 0$$

$$a\alpha = (a a_1, a a_2, \cdots, a a_n, \cdots\cdots) \in W,$$

W is a subspace of V.

(c) $\alpha = (a_1, a_2, \cdots, a_n, \cdots) \in U$

$\sum_{i=1}^{\infty} a_i^2$ is finite $\lim_{n\to\infty} a_n^2 = 0$,

$\lim_{n\to\infty} a_n = 0$, $\alpha \in W$, $U \subset W$.

$\beta = (b_1, b_2, \cdots, b_n, \cdots) \in U$,

$\sum_{i=1}^{\infty} b_i^2$ is finite .

$$(\sum_{i=1}^{n} a_i b_i)^2 \le (\sum_{i=1}^{n} a_i^2) (\sum_{i=1}^{n} b_i^2)$$
$$\le (\sum_{i=1}^{\infty} a_i^2) (\sum_{i=1}^{\infty} b_i^2)$$

$$\therefore \sum_{i=1}^{\infty} a_i b_i \le (\sum_{i=1}^{\infty} a_i^2) (\sum_{i=1}^{\infty} b_i^2) < \infty .$$

$$(a_i + b_i)^2 = a_i^2 + b_i^2 + 2 a_i b_i$$

$$\sum_{i=1}^{n} (a_i + b_i)^2 = \sum_{i=1}^{n} a_i^2 + \sum_{i=1}^{n} b_i^2 + 2 \sum_{i=1}^{n} a_i b_i$$

$$\therefore \sum_{i=1}^{\infty} (a_i + b_i)^2 = \sum_{i=1}^{\infty} a_i^2 + \sum_{i=1}^{\infty} b_i^2 + 2 \sum_{i=1}^{\infty} a_i b_i < \infty$$

$$\therefore \alpha + \beta \in U$$

$$a \in F , \sum_{i=1}^{\infty} (a a_i)^2 = a^2 \sum_{i=1}^{\infty} a_i^2 < \infty$$

$$a\alpha \in U$$

U is a subspace of W.

6. If U and V are vector spaces over F, define an addition and a multiplication by scalars in Hom (U, V) so as to make Hom (U, V) into a vector space over F.

176.6 $T , S \in \mathrm{Hom}(U , V)$, $\alpha \in F$. Define
$T + S : U \to V$
as $(T + S)(u) = Tu + Su$ for all u in U.
$(T + S)$ is a homomorphism of U into V.
$T + S \in \mathrm{Hom}(U , V)$.
Define $(\alpha T) : U \to V$
as $(\alpha T)(u) = \alpha (T u)$.
(αT) is a homomorphism of U into V.
$\alpha T \in \mathrm{Hom}(U , V)$. It's easy to show that Hom (U , V) is a vector space over F under the addition and multiplication by scalars.

*7. Using the result of Problem 6 prove that Hom $(F^{(n)}, F^{(m)})$ is isomorphic to F^{nm} as a vector space.

176.7 Let $e_i = (0 , 0 , \cdots , 0 , i , 0 , \cdots\cdots 0)$.
Every element of $F^{(n)}$ has one and only one representation as $\sum_{i=1}^{n} \alpha_i e_i$, $\alpha_i \in F$

For $T \in \mathrm{Hom}(F^{(n)} , F^{(m)})$,
$Te_i = \sum_{j=1}^{m} a_{ij} e_j$.
Define $\sigma : \mathrm{Hom}(F^{(n)}, F^{(m)}) \to F^{(mn)}$ as
$\sigma(T) = (a_{11} , a_{12} , \cdots , a_{1m} , a_{21} , a_{22} , \cdots , a_{2m} , \cdots\cdots , a_{n1} , a_{n2} , \cdots\cdots , a_{nm})$.
If $S \in \mathrm{Hom}(F^{(n)} , F^{(m)})$ and
$Se_i = \sum_{j=1}^{m} b_{ij} e_j$, then

$$(T+S)e_i = Te_i + Se_i = \sum_{j=1}^{m} a_{ij}e_j + \sum_{j=1}^{m} b_{ij}e_j$$
$$= \sum_{j=1}^{m} (a_{ij}+b_{ij})e_j$$
$$\sigma(T+S) = (a_{11}+b_{11}, a_{12}+b_{12}, \cdots, a_{1m}+b_{1m}, \cdots, a_{n1}+b_{n1}, a_{n2}+b_{n2}, \cdots, a_{nm}+b_{nm})$$
$$= (a_{11}, a_{12}, \cdots, a_{1m}, \cdots, a_{n1}, a_{n2}, \cdots, a_{nm}) + (b_{11}, b_{12}, \cdots, b_{1m}, \cdots, b_{n1}, b_{n2}, \cdots, b_{nm})$$
$$= \sigma(T) + \sigma(S)$$

$\alpha \in F$, $(\alpha T)e_i = \alpha(Te_i)$

$$= \alpha \sum_{j=1}^{m} a_{ij}e_j = \sum_{j=1}^{m} \alpha a_{ij}e_j .$$

$$\sigma(\alpha T) = (\alpha a_{11}, \alpha a_{12}, \cdots, \alpha a_{1m}, \cdots, \alpha a_{n1}, \alpha a_{n2}, \cdots, \alpha a_{nm})$$
$$= \alpha(a_{11}, a_{12}, \cdots, a_{1m}, \cdots, a_{n1}, a_{n2}, \cdots, a_{nm}) = \alpha\sigma(T).$$

σ is a homomorphism of $\mathrm{Hom}(F^{(n)}, F^{(m)})$ into $F^{(mn)}$.

If $\sigma(T) = 0$, then $a_{ij} = 0$ for all i and j. Hence $Te_i = 0$ for all i. Since every element of $F^{(n)}$ can be represented as $\sum_{i=1}^{n} \alpha_i e_i$,

$$T\left(\sum_{i=1}^{n} \alpha_i e_i\right) = \sum_{i=1}^{n} \alpha_i T(e_i)$$
$$= \sum_{i=1}^{n} \alpha_i \cdot 0 = 0 .$$

σ is an isomorphism.

Finally, we want to show that σ is onto. For any element $a = (a_{11}, a_{12}, \cdots, a_{1m}, a_{21}, a_{22}, \cdots, a_{2m}, \cdots, a_{n1}, a_{n2}, \cdots, a_{nm})$ in $F^{(nm)}$. Define $T: F^{(n)} \to F^{(m)}$ as

$$T\left(\sum_{i=1}^{n} \alpha_i e_i\right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_i a_{ij} e_j .$$

There is no difficult to show that $T \in \mathrm{Hom}(F^{(n)}, F^{(m)})$ and $\sigma(T) = a$.

Therefore σ is onto and an isomorphism of $\mathrm{Hom}(F^{(n)}, F^{(m)})$ onto $F^{(nm)}$.

8. If $n > m$ prove that there is a homomorphism of $F^{(n)}$ onto $F^{(m)}$ with a kernel W which is isomorphic to $F^{(n-m)}$.

176.8 Define $\sigma: F^{(n)} \to F^{(m)}$ as

$\sigma(a_1, a_2, \cdots, a_m, a_{m+1}, \cdots, a_n) = (a_1, a_2, \cdots, a_m)$.

σ is clearly a homomorphism of $F^{(n)}$ onto $F^{(m)}$ with kernel $\{(0, 0, \cdots, 0, a_{m+1}, \cdots, a_n) \mid a_i \in F, i = m+1, \cdots, n\}$ which is isomorphic to $F^{(n-m)}$.

9. If $v \neq 0 \in F^{(n)}$ prove that there is an element $T \in \mathrm{Hom}(F^{(n)}, F)$ such that $vT \neq 0$.

176.9 Let $v = (a_1, a_2, \cdots, a_n)$. Since $v \neq 0$, $a_i \neq 0$ for some i. Define $T: F^{(n)} \to F$ as $T(x_1, x_2, \cdots, x_n) = x_i$.

T is clearly a homomorphism of $F^{(n)}$ onto F. $T \in \mathrm{Hom}(F^{(n)}, F)$ and $Tv \neq 0$.

10. Prove that there exists an isomorphism of $F^{(n)}$ into $\mathrm{Hom}(\mathrm{Hom}(F^{(n)}, F), F)$.

176.10 By 178.7 $\mathrm{Hom}(\mathrm{Hom}(F^{(n)}, F), F)$ is isomorphie to $\mathrm{Hom}(F^{(n)}, F)$ and $F^{(n)}$.

11. If U and W are subspaces of V, prove that $U + W = \{v \in V \mid v = u + w, u \in U, w \in W\}$ is a subspace of V.

176.11 $v, v' \in U+W$ implies $v = u+w$, $v' = u'+w'$ for some u, u' in U and w, w' in W. $v + v' = (u+w)+(u'+w') = (u+u')+(w+w') \in U+W$. $\alpha \in F$, $\alpha v = \alpha(u+w)$

$= \alpha u + \alpha w \in U + W$,

$U + W$ is a subspace of V .

12. Prove that the intersection of two subspaces of V is a subspace of V.

176.12 Let U , W be subspaces of V. u , $u' \in U \cap W$ implies $u + u' \in U \cap W$. $\alpha \in F$, $\alpha u \in U \cap W$. $U \cap W$ is a subspace of V.

13. If A and B are subspaces of V prove that $(A + B)/B$ is isomorphic to $A/(A \cap B)$.

176.13 As in the proof of (65.6), we can easily show that $A + B / B$ is isomorphic to $A / A \cap B$.

14. If T is a homomorphism of U onto V with kernel W prove that there is a one-to-one correspondence between the subspaces of V and the subspaces of U which contain W.

176.14 As in the proof of Lemma 2.7.5 , we can find that there is a one-to-one correspondence between the subspaces of V and the subspaces of U which contains W .

15. Let V be a vector space over F and let $V_1, \ldots, V_n$ be subspaces of V. Suppose that $V = V_1 + V_2 + \cdots + V_n$ (see Problem 11), and that $V_i \cap (V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_n) = (0)$ for every $i = 1, 2, \ldots, n$. Prove that V is the internal direct sum of $V_1, \ldots, V_n$.

176.15 We suggest the reader to check the proof of (108.9).

16. Let $V = V_1 \oplus \cdots \oplus V_n$; prove that in V there are subspaces $\bar{V}_i$ isomorphic to V_i such that V is the internal direct sum of the $\bar{V}_i$.

176.16 Let $\overline{V}_i = \{ (0 , 0 , \cdots , v_i , 0 , \cdots , 0) \mid v_i \in V_i \}$. $\overline{V}_i$. is isomorphic to V_i and V is the internel direct sum of the $\overline{V}_i$.

17. Let T be defined on $F^{(2)}$ by $(x_1, x_2)T = (\alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2)$ where $\alpha, \beta, \gamma, \delta$ are some fixed elements in F.

(a) Prove that T is a homomorphism of $F^{(2)}$ into itself.
(b) Find necessary and sufficient conditions on $\alpha, \beta, \gamma, \delta$ so that T is an isomorphism.

176.17 (a) $(x_1 , x_2) , (y_1 , y_2) \in F^{(2)}$.

$$
\begin{aligned}
&((x_1 , x_2) + (y_1 , y_2)) T \\
&= (x_1 + y_1 , x_2 + y_2) T \\
&= (\alpha (x_1 + y_1) + \beta (x_2 + y_2) , \\
&\quad \gamma (x_1 + y_1) + \delta (x_2 + y_2)) \\
&= (\alpha x_1 + \beta x_2 , \gamma x_1 + \delta x_2) + (\alpha y_1 + \beta y_2 , \\
&\quad \gamma y_1 + \delta y_2) = (x_1 , x_2) T + (y_1 , y_2) T .
\end{aligned}
$$

$a \in F$,

$$
\begin{aligned}
&(a (x_1 , x_2)) T \\
&= (a x_1 , a x_2) T \\
&= (\alpha a x_1 + \beta a x_2 , \gamma a x_1 + \delta a x_2) \\
&= a (\alpha x_1 + \beta x_2 , \gamma x_1 + \delta x_2) \\
&= a ((x_1 , x_2) T) .
\end{aligned}
$$

T is a homomorphism of $F^{(2)}$ into itself.

(b) T is an isomorphism if and only if $\alpha\delta - \beta\gamma \neq 0$.

(i) Suppose T is an isomorphism. Then (x_1, x_2) $T = (0 , 0)$ implies $x_1 = x_2 = 0$.

Therefore $\begin{cases} \alpha x_1 + \beta x_2 = 0 \\ \gamma x_1 + \delta x_2 = 0 \end{cases}$ has no nonzero solution and $\alpha\delta - \beta\gamma \neq 0$

(ii) If $\alpha\delta - \beta\gamma = 0$, then

$\begin{cases} \alpha x_1 + \beta x_2 = 0 \\ \gamma x_1 + \delta x_2 = 0 \end{cases}$ has nonzero solution.

Hence T is not isomorphism.

18. Let T be defined on $F^{(3)}$ by $(x_1, x_2, x_3)T = (\alpha_{11}x_1 + \alpha_{12}x_2 + \alpha_{13}x_3, \alpha_{21}x_1 + \alpha_{22}x_2 + \alpha_{23}x_3, \alpha_{31}x_1 + \alpha_{32}x_2 + \alpha_{33}x_3)$. Show that T is a homomorphism of $F^{(3)}$ into itself and determine necessary and sufficient conditions on the α_{ij} so that T is an isomorphism.

176.18 T is clearly a homomorphism of $F^{(3)}$ into itself . T is an isomorphism if and only if

the determinant of $\begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix}$ is not zero. The proof of this condition is the same as (176 , 17 , (b)) .

19. Let T be a homomorphism of V into W. Using T, define a homomorphism T^* of Hom (W, F) into Hom (V, F).

177.19 Define $T^* : \mathrm{Hom}(W, F) \to \mathrm{Hom}(V, F)$ as $v(hT^*) = (vT)h$ for all h in Hom (W , F) and v in V. There is no difficult to show that T^* is a homomorphism of Hom (W , F) into Hom (V , F) .

20. (a) Prove that $F^{(1)}$ is not isomorphic to $F^{(n)}$ for $n > 1$.
(b) Prove that $F^{(2)}$ is not isomorphic to $F^{(3)}$.

177.20 (a) Suppose that T is an isomorphism of $F^{(1)}$ onto $F^{(n)}$, Let (1) $T = (x_1 , \cdots , x_n)$, the image of $1.(\alpha)\ T = (\alpha \cdot 1)T$
$= \alpha ((1) T)$
$= \alpha (x_1 , \cdots , x_n)$.
Since T is an onto mapping , every element is of the form $\alpha (x_1 , \cdots , x_n)$, $\alpha \in F$.
If $X_i = 0$ for some $1 \leq i \leq n$, then
$(0 , 0 , \cdots , \overset{i}{1} , 0 , \cdots , 0) \neq \alpha (x_1 , \cdots , x_n)$
for all α in F. Hence $X_i \neq 0$ for all $i = 1, 2 \cdots , n$
Clearly , $(x_1 + x_2 , x_2 , \cdots , x_n) \neq \alpha (x_1 , x_2 , \cdots , x_n)$ for all α in F, a contradiction . Therefore , there is no isomorphism of $F^{(1)}$ onto $F^{(n)}$.
$F^{(1)}$ is not isomorphic to $F^{(n)}$.

(b) Suppose that T is an isomorphism of $F^{(3)}$ onto $F^{(2)}$.
Let $(1, 0, 0)T = (a_1 , a_2)$,
$(0, 1, 0)T = (b_1 , b_2)$.

$(\alpha , \beta , 0)T = (\alpha(1, 0, 0) + \beta(0, 1, 0))T$
$= (\alpha a_1 + \beta b_1 , \alpha a_2 + \beta b_2)$.
Since T is one-to-one , there is no nonzero α , β such that

$$\begin{cases} \alpha a_1 + \beta b_1 = 0 \\ \alpha a_2 + \beta b_2 = 0 \end{cases}$$

Therefore $a_1 b_2 - a_2 b_1 \neq 0$, and for all $(x , y) \in F^{(2)}$ there are α and β in F such that

$$\begin{cases} \alpha a_1 + \beta b_1 = x \\ \alpha a_2 + \beta b_2 = y \end{cases}$$

T mapps $\{ (\alpha , \beta , 0) \mid \alpha , \beta \in F \} \subsetneq F^{(3)}$ onto $F^{(2)}$. T cannot be a one-one correspondence between $F^{(3)}$ and $F^{(2)}$, a contradiction.

21. If V is a vector space over an *infinite* field F, prove that V cannot be written as the set-theoretic union of a finite number of proper subspaces.

177.21 Note : In the definition of vector space we required the vector space is over a field. We can also define a vector space over a division ring as the same way. We prove this exercise without requring F to be a field . In fact , the conclusion is also true for F being a division ring. We need this result to prove (368.9).

Suppose $V = \bigcup_{i=1}^{n} V_i$ and $V_1 \not\subset \bigcup_{i=2}^{n} V_i$,

$\bigcup_{i=2}^{n} V_i \not\subset V_1$, where V_j are proper subspace of V. Let $0 \neq u \in V_1 \setminus \bigcup_{i=2}^{n} V_i$ and $0 \neq \omega \in \bigcup_{i=2}^{n} V_i \setminus V_1$. $S = \{ \omega + \alpha u \mid \alpha \in F \}$ is an infinite set . If $\omega + \alpha u$, $\omega + \beta u \in V_i$,

$i = 2, 3, \cdots$ or n, then
$(\alpha - \beta)u = (\omega + \alpha u) - (\omega + \beta u) \in V_i$.
$u \neq 0$ implies $\alpha = \beta$.
This shows that there is at most one element of S in V_i for all $i = 2, \cdots, n$.

Since $V = \bigcup_{i=1}^{n} V_i$ and S is infinite,
there are $\omega + \alpha u$, $\omega + \beta u \in V_1$ with
$\alpha \neq 0$, $\beta \neq 0$ and $\alpha \neq \beta$.
$\alpha^{-1}(\omega + \alpha u) = \alpha^{-1}\omega + u$,
$\beta^{-1}(\omega + \beta u) = \beta^{-1}\omega + u \in V_1$.
$(\alpha^{-1} - \beta^{-1})\omega = (\alpha^{-1}\omega + u) - (\beta^{-1}\omega + u) \in V_1$,
$\alpha^{-1} - \beta^{-1} \neq 0$ implies $\omega \in V_1$ a contradiction.
Therefore, V cannot be written as the set-theoretic union of a finite number of proper subspaces.

4.2 Linear Independence and Bases.

1. Prove Lemma 4.2.2.

183.1 (1) $v \in L(S)$ implies
$v = \sum_{i=1}^{n} \alpha_i v_i$, where $\alpha_i \in F$ and $v_i \in S$
Since $S \subset T$, $v_i \in S$ and $v \in L(T)$.
$L(S) \subset L(T)$.

(2) $v \in L(S \cup T)$ implies $v = \sum_{i=1}^{n} \alpha_i v_i$,
where $\alpha_i \in F$ and $v_i \in S \cup T$.
$v = \sum_{i=1}^{n} \alpha_i v_i = \sum_{v_i \in S} \alpha_i v_i + \sum_{v_i \in T} \alpha_i v_i$
$\in L(S) + L(T)$.
$L(S \cup T) \subset L(S) + L(T)$
$v \in L(S) + L(T)$ implies
$v = \sum_{i=1}^{n} \alpha_i v_i + \sum_{i=1}^{m} \beta_i u_i$,
where $\alpha_i, \beta_i \in F$ and $v_i \in S$, $u_i \in T$.
$v \in L(S \cup T)$. $L(S) + L(T) \subset L(S \cup T)$.
$L(S \cup T) = L(S) + L(T)$.

(3) By (1) and $S \subset L(S)$ we have
$L(S) \subset L(L(S))$. If $v \in L(L(S))$
then $v = \sum_{i=1}^{n} \alpha_i V_i$, where $\alpha_i \in F$ and
$v_i \in L(S)$ $v_i \in L(S)$ implies
$v_i = \sum_{j=1}^{m_i} b_{ij} u_{ij}$, where $b_{ij} \in F$ and
$U_{ij} \in S$.
$v = \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \alpha_i \left(\sum_{j=1}^{m_i} B_{ij} u_{ij} \right)$
$= \sum_{i=1}^{n} \sum_{j=1}^{m_i} \alpha_i \beta_{ij} u_{ij} \in L(S)$
$L(L(S)) \subset L(S)$.

$$L(L(S)) = L(S).$$

2. (a) If F is the field of real numbers, prove that the vectors (1, 1, 0, 0), (0, 1, −1, 0), and (0, 0, 0, 3) in $F^{(4)}$ are linearly independent over F.
   (b) What conditions on the characteristic of F would make the three vectors in (a) linearly dependent?

183.2 (a) Suppose $a(1,1,0,0) + b(0,1,-1,0) + c(0,0,0,3) = 0$, $a, b, c \in F$

$(a, a+b, -b, 3c) = 0$, $a = b = c = 0$.

Hence $(1,1,0,0)$, $(0,1,-1,0)$ and $(0,0,0,3)$ in $F^{(4)}$ are linearly independent over F

(b) If F is of characteristic 3, then

$0 \cdot (1,1,0,0) + 0 \cdot (0,1,-1,0) + 1 \cdot (0,0,0,3) = 0$

$(1,1,0,0)$, $(0,1,-1,0)$ and $(0,0,0,3)$ are linearly dependent.

3. If V has a basis of n elements, give a detailed proof that V is isomorphic to $F^{(n)}$.

183.3 Let $v_1, v_2, \cdots, v_n$ be one basis of V. Every element of V is a linear combination of $v_1, \cdots\cdots, v_n$. Since $v_1, \cdots\cdots, v_n$ are linearly indenpendent, every element of V has one and only one repesentation as linear combination of $v_1, \cdots\cdots, v_n$. For $v = \sum_{i=1}^{n} \alpha_i V_i \in V$, define $vT = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in F^{(n)}$.

T is clearly an isomorphism of V onto $F^{(n)}$.

V is isomorphic to $F^{(n)}$.

4. If T is an isomorphism of V onto W, prove that T maps a basis of V onto a basis of W.

183.4 Let $S \subset V$ be a basis of V. $ST = \{sT \mid s \in S\} \subset W$. If $\sum_{i=1}^{n} \alpha_i (v_i T) = 0$ for $\alpha_i \in F$ and $v_i \in S$, then $(\sum_{i=1}^{n} \alpha_i v_i) T = 0$.

Since T is one-to-one, $\sum_{i=1}^{n} \alpha_i v_i = 0$.

The linear independence of $v_1, \cdots, v_n$ implies $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

$v_1 T, v_2 T, \cdots, v_n T$ are linearly independent.

This shows that any finite number of elements in ST is linearly indenpendent.

On the other hand, if $\omega \in W$, then $\omega = vT$ for some v in V since T is an onto mapping.

$v = \sum_{i=1}^{m} \beta_i v_i$, where $\beta_i \in F$, $v_i \in S$ since S spans V.

$w = vT = (\sum_{i=1}^{m} \beta_i v_i) T = \sum_{i=1}^{m} \beta_i (v_i T)$.

ST spans W. ST is a basis of W.

5. If V is finite-dimensional and T is an isomorphism of V into V, prove that T must map V *onto* V.

183.5 Let $v_1, v_2, \cdots, v_n$ be one basis of V.

$v_1 T, v_2 T, \cdots, v_n T$ are linearly independent.

For, if $\sum_{i=1}^{n} \alpha_i (v_i T) = 0$ for $\alpha_i \in F$, then $(\sum_{i=1}^{n} \alpha_i v_i) T = 0$. Since T is an isomorphism so $\sum_{i=1}^{n} \alpha_i v_i = 0$. The linear indenpendence of $v_1, \cdots, v_n$ implies $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

$v_1 T, v_2 T, \cdots, v_n T$ are linearly indenpendent.

By Lemma 4.2.5, we can find vectors $u_{n+1}, \cdots$

, u_{r+n} in V such that v_1T, v_2T, $\cdots$, v_nT, u_{n+1}, $\cdots$, u_{n+r} is a basis of V. By Corollary 1 of Lemma 4.2.4, r=0 and v_1T, $\cdots$, v_nT is a basis of V. v_1T, $\cdots$, v_nT span V. For $v \in V$, $v = \sum_{i=1}^{n} \beta_i (v_i T)$

for some $\beta_i \in F$, $v = \sum_{i=1}^{n} \beta_i (v_i T)$

$= (\sum_{i=1}^{n} \beta_i v_i) T$

T must map V onto V.

6. If V is finite-dimensional and T is a homomorphism of V *onto* V, prove that T must be one-to-one, and so an isomorphism.

183.6 Let $v_1, v_2, \cdots, v_n$ be one basis of V. $v_1T, v_2T, \cdots, v_nT$ span V. For, if $v \in V$, then $v = \omega T$ for some ω in V since T is an onto mapping. $\omega = \sum_{i=1}^{n} \alpha_i v_i$ for some α_i in F.

$v = \omega T = (\sum_{i=1}^{n} \alpha_i v_i) T = \sum_{i=1}^{n} \alpha_i (v_i T)$.

$v_1T, \cdots, v_nT$ Span V. By Corollary 3 of Theorem 4.2.1 and Corollary 1 of Lemma 4.2.4, $v_1T, \cdots\cdots, v_nT$ are linearly independent. $v \in V$, $v = \sum_{i=1}^{n} \beta_i v_i$. If $vT = 0$, then

$vT = (\sum_{i=1}^{n} \beta_i v_i) T = \sum_{i=1}^{n} \beta_i (v_i T) = 0$.

Since $v_1T, \cdots, v_nT$ are linearly independent, $\beta_1 = \beta_2 = \cdots\cdots = \beta_n = 0$, $v = \sum_{i=1}^{n} \beta_i v_i = 0$.

T is one-to-one. T is an isomorphism of V onto V.

7. If V is of dimension n, show that any set of n linearly independent vectors in V forms a basis of V.

183.7 Let $v_1, v_2, \cdots, v_n$ be linearly independent. By Lemma 4.2.5, we can find vectors u_{n+1}, u_{n+2}, $\cdots$, u_{n+r} in V such that $v_1, v_2, \cdots, v_n, u_{n+1}, u_{n+2}, \cdots, u_{n+r}$ is a basis of V. By Corollary 1 of Lemma 4.2.4, r=0 and $v_1, v_2 \cdots, v_n$ is a basis of V.

8. If V is finite-dimensional and W is a subspace of V such that dim V = dim W, prove that $V = W$.

184.8 Let dim V = dim W = n. By definition of the dimension of W, there is a basis $v_1, \cdots, v_n$ in W. $v_1, \cdots, v_n$ are linearly independent. By (183.7), $v_1, \cdots, v_n$ forms a basis of V. Every element of V can be written as $\sum_{i=1}^{n} \alpha_i v_i$ for some α_i in F. $\sum_{i=1}^{n} \alpha_i v_i \in W$

$V \subset W$, $V = W$.

9. If V is finite-dimensional and T is a homomorphism of V into itself which is not onto, prove that there is some $v \neq 0$ in V such that $vT = 0$.

184.9 Suppose $vT = 0$ implies $v = 0$, Then T is an isomorphism of V into itself. By (183.5), T is onto, a contradiction. Hence, there is some $v \neq 0$ in V such that $vT = 0$.

10. Let F be a field and let $F[x]$ be the polynomials in x over F. Prove that $F[x]$ is not finite-dimensional over F.

184.10 If F[x] is finite-dimensional over F, then there is a finite set $\{f_1(x), f_2(x), \cdots, f_n(x)\}$ which spans F[x]. Let $k = \max\{\deg f_i(x)\}$ clearly, x^{k+1} can not written as linear combination of $f_1(x)$,

$\cdots$, $f_n(x)$, a contradiction. Hence $F[x]$ is not finite-dimensional over F.

11. Let $V_n = \{p(x) \in F[x] \mid \deg p(x) < n\}$. Define T by

$$(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1})T = \alpha_0 + \alpha_1(x+1) + \alpha_2(x+1)^2 + \cdots + \alpha_{n-1}(x+1)^{n-1}.$$

Prove that T is an isomorphism of V_n onto itself.

184.11 $1, x, \cdots, x^{n-1}$ forms a basis of V_n. V_n is of finite-dimension.

T is clearly a homomorphism of V_n into itself.

If $(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1})T = 0$, then $\alpha_0 + \alpha_1(x+1) + \alpha_2(x+1)^2 + \cdots + \alpha_{n-1}(x+1)^{n-1} = 0$

The coefficient of x^{n-1} is α_{n-1}, so $\alpha_{n-1} = 0$

The coefficient of x^{n-2} is α_{n-2}, so $\alpha_{n-2} = 0$, $\cdots\cdots$, $\alpha_0 = \alpha_1 = \cdots\cdots = \alpha_{n-1} = 0$.

T is one-to-one. T is an isomorphism of V_n onto itself by (183.5).

12. Let $W = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1} \in F[x] \mid \alpha_0 + \alpha_1 + \cdots + \alpha_{n-1} = 0\}$. Show that W is a subspace of V_n and find a basis of W over F.

184.12 $\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}$,
$\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1} \in W$ implies
$\alpha_0 + \alpha_1 + \cdots + \alpha_{n-1} = \beta_0 + \beta_1 + \cdots + \beta_{n-1} = 0$.
$(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}) + (\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1})$
$= (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)x + \cdots + (\alpha_{n-1} + \beta_{n-1})x^{n-1}$
$(\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) + \cdots + (\alpha_{n-1} + \beta_{n-1})$
$= (\alpha_0 + \alpha_1 + \cdots + \alpha_{n-1}) + (\beta_1 + \beta_2 + \cdots + \beta_n)$
$= 0 + 0 = 0$.

$(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}) + (\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1}) \in W$. $\alpha \in F$,
$\alpha(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1})$
$= \alpha\alpha_0 + \alpha\alpha_1 x + \cdots + \alpha\alpha_{n-1} x^{n-1}$, $\alpha\alpha_0 + \alpha\alpha_1 + \cdots + \alpha\alpha_{n-1} = \alpha(\alpha_0 + \cdots + \alpha_{n-1})$
$= \alpha \cdot 0 = 0$, $\alpha(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} + x^{n-1}) \in W$, W is a subspace of V_n.

Suppose $n > 1$. $1 - x$, $1 - x^2$, $\cdots\cdots$, $1 - x^{n-1}$ form a basis of W. For, if $\sum_{i=1}^{n-1} \alpha_i (1 - x^i) = 0$,

then $(\sum_{i=1}^{n-1} \alpha_i) - \sum_{i=1}^{n-1} \alpha_i x^i = 0$,

$\alpha_1 = \alpha_2 = \cdots = \alpha_{n-1} = 0$,

$1-x$, $1-x^2$, $\cdots$, $1-x^{n-1}$ are linearly independent. If $1-x, 1-x^2, \cdots\cdots, 1-x^{n-1}$ do not span W, then by Lemma 4.2.5, $\dim W > n-1$, $W \subset V_n$.

$n = \dim V \geq \dim W > n-1$.

$\dim W = \dim V = n$. By (184.8), $V = W$, contrary to $1 \in V \setminus W$. Therefore, $1-x, 1-x^2, \cdots, 1-x^{n-1}$ form a basis of W. If $n=1$, then $W=(0)$. W has no basis.

13. Let $v_1, \ldots, v_n$ be a basis of V and let $w_1, \ldots, w_n$ be any n elements in V. Define T on V by $(\lambda_1 v_1 + \cdots + \lambda_n v_n)T = \lambda_1 w_1 + \cdots + \lambda_n w_n$.
(a) Show that R is a homomorphism of V into itself.
(b) When is T an isomorphism?

184.13 (a) $((\alpha_1 v_1 + \cdots + \alpha_n v_n) + (\beta_1 v_1 + \cdots + \beta_n v_n))$
$T = ((\alpha_1 + \beta_1)v_1 + \cdots + (\alpha_n + \beta_n)v_n)T$
$= (\alpha_1 + \beta_1)w_1 + \cdots + (\alpha_n + \beta_n)w_n$
$= (\alpha_1 w_1 + \cdots + \alpha_n w_n) + (\beta_1 w_1 + \cdots + \beta_n w_n)$
$= (\alpha_1 v_1 + \cdots + \alpha_n v_n)T + (\beta_1 v_1 + \cdots + \beta_n v_n)T$. $(\alpha(\alpha_1 v_1 + \cdots + \alpha_n v_n))T$

$= (\alpha\alpha_1 v_1 + \alpha\alpha_2 v_2 + \cdots + \alpha\alpha_n v_n)T$
$= \alpha\alpha_1 w_1 + \alpha\alpha_2 w_2 + \cdots + \alpha\alpha_n w_n$
$= \alpha(\alpha_1 w_1 + \cdots + \alpha_n w_n) = \alpha((\alpha_1 v_1 + \cdots + \alpha_n v_n)T)$. T is a homomorphism of V into itself .

(b) T is an isomorphism if and only if w_1, w_2, ... , w_n is a basis of V. For , if T is an isomorphism , then by (183.4) $w_1 = v_1 T$, $\cdots$, $w_n = v_n T$ is a basis of V. Conversely , if w_1 , $\cdots$, w_n is a basis of V , then T is an onto mapping. By (183.6) , T is an isomorphism.

14. Show that any homomorphism of V into itself, when V is finite-dimensional, can be realized as in Problem 13 by choosing appropriate elements $w_1, \ldots, w_n$.

184.14 Let v_1 , v_2 , $\cdots$, v_n be a basis of V. Let $w_i = v_i T$, $i = 1 , 2 , \cdots n$.

$(\lambda_1 v_1 + \cdots + \lambda_n v_n)T = \lambda_1 (v_1 T) + \cdots + \lambda_n (v_n T)$

$= \lambda_1 w_1 + \cdots + \lambda_n w_n$.

15. Returning to Problem 13, since $v_1, \ldots, v_n$ is a basis of V, each $w_i = \alpha_{i1}v_1 + \cdots + \alpha_{in}v_n$, $\alpha_{ij} \in F$. Show that the n^2 elements α_{ij} of F determine the homomorphism T.

184.15 Since $(\lambda_1 v_1 + \cdots + \lambda_n v_n)T$

$= \lambda_1 w_1 + \cdots + \lambda_n w_n$

$= \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \alpha_{ij} v_j$, so

T is determined by the n^2 elements α_{ij} of F.

*16. If $\dim_F V = n$ prove that $\dim_F (\mathrm{Hom}\ (V,V)) = n^2$.

184.16 By Corollary 3 of Lemma 4.2.4 , V is isomorphic to $F^{(n)}$. By (176.7), Hom (V , V) is isomorphic to $F^{(n^2)}$.

Hence $\dim_F (\mathrm{Hom} (V , V)) = n^2$.

17. If V is finite-dimensional and W is a subspace of V prove that there is a subspace W_1 of V such that $V = W \oplus W_1$.

184.17 Let v_1 , $\cdots$, v_n be a basis of W. v_1 , v_2 , $\cdots$, v_n are linearly independent. By Lemma 4.2.5 , we can find vectors u_{n+1} , u_{n+2} , $\cdots u_{n+r}$ in V such that v_1 , $\cdots$, v_n , u_{n+1} , u_{n+2} , $\cdots$, u_{n+r} is a basis of V.

Let $W_1 = L (u_{n+1} , \cdots , u_{n+r})$.

$V = W \oplus W_1$.

4.3. Dual Spaces

1. Prove that $A(W)$ is a subspace of $\hat{V}$.

190.1 $f, g \in A(W)$ implies $f(w)=g(w)=0$ for all $w \in W$. $(f+g)(w)=f(w)+g(w)=0+0=0$ for all $w \in W$. $\alpha \in F$, $(\alpha F)(w)=\alpha(f(w))=\alpha \cdot 0=0$ $f+g \in A(w)$, $\alpha F \in A(w)$, $A(w)$ is a subspace of V.

2. If S is a subset of V let $A(S) = \{f \in \hat{V} \mid f(s) = 0 \text{ all } s \in S\}$. Prove that $A(S) = A(L(S))$, where $L(S)$ is the linear span of S.

190.2 $S \subset L(S)$ implies $A(L(S)) \subset A(S)$. Conversely, if $f \in A(S)$, then $f(s)=0$ for all s in S. $v \in L(S)$ implies $v=\sum_{i=1}^{n} \alpha_i s_i$ for some α_i in F and s_i in S.

$f(v)=f(\sum_{i=1}^{n} \alpha_i s_i)=\sum_{i=1}^{n} \alpha_i f(s_i)=0$.

$f \in A(L(S))$. $A(S) \subset A(L(S))$

$A(S)=A(L(S))$.

3. If $S, T \in \text{Hom}(V, W)$ and $v_i S = v_i T$ for all elements v_i of a basis of V, prove that $S = T$.

191.3 $v \in V$ implies $v=\sum_{i=1}^{n} \alpha_i v_i$ for some $\alpha_i \in F$ and v_i in the given basis of V.

$$vS=(\sum_{i=1}^{n} \alpha_i v_i)S=\sum_{i=1}^{n} \alpha_i (v_i S)$$

$$=\sum_{i=1}^{n} \alpha_i (v_i T)=(\sum_{i=1}^{n} \alpha_i v_i) T = vT$$

Hence $vS = vT$ for all v in V. $S = T$.

4. Complete the proof, with all details, that Hom (V, W) is a vector space over F.

191.4 As on page 185, we only prove that $\lambda S \in \text{Hom}(V, W)$ and $(\lambda+\mu)S=\lambda S+\mu S$, $\lambda(S+T)=\lambda S+\lambda T$, $\lambda(\mu S)=(\lambda\mu)S$ and $1 \cdot S = S \cdot$ For $v_1, v_2 \in V$ and $\alpha \in F$,

$(v_1+v_2)(\lambda S)=\lambda((v_1+v_2)S)$

$=\lambda(v_1 S+v_2 S)=\lambda(v_1 S)+\lambda(v_2 S)$

$=v_1(\lambda S)+v_2(\lambda S)$.

$(\alpha v_1)(\lambda S)=\lambda((\alpha v_1)S)=\lambda(\alpha(v_1 S))$

$=(\lambda\alpha)(v_1 S)=\alpha(\lambda(v_1 S))=\alpha(v_1(\lambda S))$

$\lambda S \in \text{Hom}(V, W)$. For $v \in V$,

$v((\lambda+\mu)S)=(\lambda+\mu)(vS)$

$=\lambda(vS)+\mu(vS)=v(\lambda S)+v(\mu S)$

$=v(\lambda S+\mu S)$, $(\lambda+\mu)S=\lambda S+\mu S$.

$v(\lambda(S+T))=\lambda(v(S+T))=\lambda(vS+vT)$

$=\lambda(vS)+\lambda(vT)=v(\lambda S)+v(\lambda T)$

$=v(\lambda S+\lambda T)$, $\lambda(S+T)=\lambda S+\lambda T$.

$v(\lambda(\mu S))=\lambda(v(\mu S))=\lambda(\mu(vS))$

$=(\lambda\mu)(vS)=v((\lambda\mu)S)$,

$\lambda(\mu S)=(\lambda\mu)S$. $v(1 \cdot S)=1 \cdot (vS)=vS$,

$1 \cdot S = S$. Hom (V, W) is a vector space over F.

5. If ψ denotes the mapping used in the text of V into $\hat{V}$, give a complete proof that ψ is a vector space homomorphism of V into $\hat{V}$.

191.5 As on page 188, we need only show that $(\alpha v)\Psi=\alpha(v\Psi)$. $(\alpha v)\Psi = T_{\alpha v}$,

$\alpha(v\Psi)=\alpha T v$. $T_{\alpha v}(f)=f(\alpha v)=\alpha f(v)$

$=\alpha(Tv(f))=(\alpha Tv)(f)$

for all f in $\hat{V}$, $T_{\alpha v}=\alpha Tv$ and $(\alpha v)\Psi$

$=\alpha(v\Psi)$.

Ψ is a vector space homomorphism of V into $\hat{\hat{V}}$.

6. If V is finite-dimensional and $v_1 \neq v_2$ are in V, prove that there is an $f \in \hat{V}$ such that $f(v_1) \neq f(v_2)$.

191.6 $v_1 \neq v_2$ implies $v_1 - v_2 \neq 0$. By Lemma 4.3.2 , there is an element f in $\hat{V}$ such that
$f(v_1 - v_2) \neq 0$. $f(v_1) - f(v_2) = f(v_1 - v_2) \neq 0$
implies $f(v_1) \neq f(v_2)$.

7. If W_1 and W_2 are subspaces of V, which is finite-dimensional, describe $A(W_1 + W_2)$ in terms of $A(W_1)$ and $A(W_2)$.

191.7 $A(W_1 + W_2) = A(W_1) \cap A(W_2)$.
For , W_1 , $W_2 \subset W_1 + W_2$, $A(W_1 + W_2) \subset A(W_1)$ and $A(W_1 + W_2) \subset A(W_2)$.
$A(W_1 + W_2) \subset A(W_1) \cap A(W_2)$
Conversely , if $f \in A(W_1) \cap A(W_2)$, then for $v \in W_1 + W_2$, $v = w_1 + w_2$ for some $w_1 \in W_1$ and $w_2 \in W_2$,
$f(v) = f(w_1 + w_2) = f(w_1) + f(w_2)$
$= 0 + 0 = 0$. $f \in A(W_1 + W_2)$.
$A(W_1) \cap A(W_2) \subset A(W_1 + W_2)$.
$A(W_1 + W_2) = A(W_1) \cap A(W_2)$.

8. If V is a finite-dimensional and W_1 and W_2 are subspaces of V, describe $A(W_1 \cap W_2)$ in terms of $A(W_1)$ and $A(W_2)$.

191.8 $A(W_1 \cap W_2) = A(W_1) + A(W_2)$. For $W_1 \cap W_2 \subset W_1$, $W_1 \cap W_2 \subset W_2$ imply $A(W_1) \subset A(W_1 \cap W_2)$ and $A(W_2) \subset A(W_1 \cap W_2)$
$A(W_1) + A(W_2) \subset A(W_1 \cap W_2)$.
By the Corollary of Lemma 4.2.6 . ,
$\dim W_1 + \dim W_2 = \dim(W_1 + W_2) + \dim(W_1 \cap W_2)$ .....(*)
$\dim A(W_1) + \dim A(W_2)$
$= \dim(A(W_1) + A(W_2)) + \dim(A(W_1) \cap A(W_2))$.
$\dim W_1 = \dim A(W_1)$, $\dim W_2 = \dim A(W_2)$.
By (191.7), $\dim A(W_1 + W_2) = \dim(A(W_1) \cap A(W_2))$.

By (*) , $\dim(A(W_1) \cap A(W_2)) + \dim A(W_1 \cap W_2)$
$= \dim A(W_1 + W_2) + \dim A(W_1 \cap W_2)$
$= \dim(W_1 + W_2) + \dim(W_1 \cap W_2)$
$= \dim W_1 + \dim W_2$
$= \dim A(W_1) + \dim A(W_2)$
$= \dim(A(W_1) \cap A(W_2)) + \dim(A(W_1) + A(W_2))$.
Hence $\dim A(W_1 \cap W_2) = \dim(A(W_1) + A(W_2))$.
By (184.8) , $A(W_1 \cap W_2) = A(W_1) + A(W_2)$

9. If F is the field of real numbers, find $A(W)$ where
(a) W is spanned by (1, 2, 3) and (0, 4, −1).
(b) W is spanned by (0, 0, 1, −1), (2, 1, 1, 0), and (2, 1, 1, −1).

191.9 (a) $\dim W = 2$, $\dim A(W) = \dim F^{(3)} - \dim W$
$= 3 - 2 = 1$.
Define $f : F^{(3)} \to F$ as
$f(\alpha, \beta, \gamma) = -14\alpha + \beta + 4\gamma$,
$f \in \hat{V}$ and $f(1, 2, 3) = -14 \cdot 1 + 2 + 4 \cdot 3 = 0$,
$f(0, 4, -1) = -14 \cdot 0 + 4 + 4 \cdot (-1) = 0$
By (190.2), $f \in A(W)$, $f \neq 0$.
Hence $A(W) = \{\lambda f \mid \lambda \in F\}$.
(b) $\dim W = 3$, $\dim A(W) = \dim F^{(4)} - \dim W$
$= 4 - 3 = 1$
Define $f : F^{(4)} \to F$ as
$f(a, b, c, d) = a - 2b$. $f \in \hat{V}$ and
$f(0, 0, 1, -1) = 0 - 2 \cdot 0 = 0$,
$f(2, 1, 1, 0) = 2 - 2 \cdot 1 = 0$,
$f(2, 1, 1, -1) = 2 - 2 \cdot 1 = 0$.
By (190.2), $f \in A(w)$, $f \neq 0$.
Hence $A(W) = \{\lambda f \mid \lambda \in F\}$.

10. Find the ranks of the following systems of homogeneous linear equations over F, the field of real numbers, and find all the solutions.

(a) $x_1 + 2x_2 - 3x_3 + 4x_4 = 0,$
$x_1 + 3x_2 - x_3 = 0,$
$6x_1 + x_3 + 2x_4 = 0.$

(b) $x_1 + 3x_2 + x_3 = 0,$
$x_1 + 4x_2 + x_3 = 0.$

(c) $x_1 + x_2 + x_3 + x_4 + x_5 = 0,$
$x_1 + 2x_2 = 0,$
$4x_1 + 7x_2 + x_3 + x_4 + x_5 = 0,$
$x_2 - x_3 - x_4 - x_5 = 0.$

191.10 (a) Since $(1,2,-3,4)$, $(1,3,-1,0)$ and $(6,0,1,2)$ are linearly independent, the rank of (a) is 3.

$(x_1, x_2, x_3, x_4) = (26, -32, -70, -43)$ is a solution of (a).

By Theorem 4.3.3, the solutions of (a) are $\alpha(26, -32, -70, -43)$, $\alpha \in F$

(b) Since $(1,3,1)$ and $(1,4,1)$ are linearly independent, the rank of (b) is 2. $(x_1, x_2, x_3) = (1,0,-1)$ is a solution of (b).

By theorem 4.3.3, the solutions of (b) are $\alpha(1,0,-1)$, $\alpha \in F$.

(c) $(4,7,1,1,1) = (1,1,1,1,1) + 3(1,2,0,0,0)$

$(0,1,-1,-1,-1) = -(1,1,1,1,1) + (1,2,0,0,0)$

$(1,1,1,1,1)$ and $(1,2,0,0,0)$ are linearly independent.

The rank of (c) is 2.

$(0,0,1,-1,0)$, $(0,0,1,0,-1)$ and $(-2,1,1,0,0)$ are linearly independent and are solutions of (c).

By Theorem 4.3.3, The solutions of (c) are $\alpha(0,0,1,-1,0) + \beta(0,0,1,0,-1) + \gamma(-2,1,1,0,0)$,

$\alpha, \beta, \gamma \in F$

11. If f and g are in $\hat{V}$ such that $f(v) = 0$ implies $g(v) = 0$, prove that $g = \lambda f$ for some $\lambda \in F$.

191.11 If $f = 0$, then $g = 0$, and $f = g$.

Suppose $f \neq 0$. Let $f(v_0) \neq 0$.

$$\lambda = \frac{g(v_0)}{f(v_0)}.$$

$$f(f(v_0)v - f(v)v_0) = f(v_0)f(v) - f(v)f(v_0) = 0$$

implies $g(f(v_0)v - f(v)v_0) = 0$.

$$0 = g(f(v_0)v - f(v)v_0) = f(v_0)g(v) - f(v)g(v_0)$$

$$g(v) = \frac{g(v_0)}{f(v_0)} f(v) = \lambda f(v) \quad \text{for all } v \text{ in } V.$$

Hence $g = \lambda f$.

4.4. Inner Product Spaces.

In all the problems V is an inner product space over F.

1. If F is the real field and V is $F^{(3)}$, show that the Schwarz inequality implies that the cosine of an angle is of absolute value at most 1.

199.1 $v=(x_1, x_2, x_3)$, $w=(y_1, y_2, y_3)$.

$v \cdot w = x_1y_1 + x_2y_2 + x_3y_3$

$v \cdot v = x_1^2 + x_2^2 + x_3^2$, $w \cdot w = y_1^2 + y_2^2 + y_3^2$.

By Schwarz inequality, we have

$(x_1y_1 + x_2y_2 + x_3y_3)^2 \leq (x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2)$.

$$\frac{v \cdot w}{\sqrt{v \cdot v}\sqrt{w \cdot w}} = \frac{x_1y_1 + x_2y_2 + x_3y_3}{\sqrt{x_1^2 + x_2^2 + x_3^2}\sqrt{y_1^2 + y_2^2 + y_3^2}}$$

Hence $\left| \frac{v \cdot w}{\sqrt{v \cdot v}\sqrt{w \cdot w}} \right| \leq 1$

2. If F is the real field, find all 4-tuples of real numbers (a, b, c, d) such that for $u = (\alpha_1, \alpha_2)$, $v = (\beta_1, \beta_2) \in F^{(2)}$, $(u, v) = a\alpha_1\beta_1 + b\alpha_2\beta_2 + c\alpha_1\beta_2 + d\alpha_2\beta_1$ defines an inner product on $F^{(2)}$.

199.2 $\{(a, b, c, d) \mid a>0, b>0, c=d=0\}$

clearly, $(u, v) = a\alpha_1\beta_1 + b\alpha_2\beta_2$, $a>0$, $b>0$, defines an inner product on $F^{(2)}$.

Conversely, suppose $(u, v) = a\alpha_1\beta_1 + b\alpha_2\beta_2 + c\alpha_1\beta_2 + d\alpha_2\beta_1$ defines an inner product on $F^{(2)}$.

Since $(u, v) = (v, u)$ for all vectors u, v in $F^{(2)}$, $(u, v) = a\alpha_1\beta_1 + b\alpha_2\beta_2 + c\alpha_1\beta_1 + d\alpha_2\beta_1 = (v, u) = a\beta_1\alpha_1 + b\beta_2\alpha_2 + c\beta_1\alpha_2 + d\beta_2\alpha_1$,

for all $\alpha_1, \alpha_2, \beta_1, \beta_2$ in F.

Hence $c=d$

$(u, u) = a\alpha_1^2 + b\alpha_2^2 + 2c\alpha_1\alpha_2 \geq 0$

for all α_1, α_2 in F and $(u, u)=0$ if and only if $\alpha_1=\alpha_2=0$. Therefore $a>0$, $b>0$ and $c=0$.

3. In V define the *distance* $\zeta(u, v)$ from u to v by $\zeta(u, v) = \|u - v\|$. Prove that
   (a) $\zeta(u, v) \geq 0$ and $\zeta(u, v) = 0$ if and only if $u = v$.
   (b) $\zeta(u, v) = \zeta(v, u)$.
   (c) $\zeta(u, v) \leq \zeta(u, w) + \zeta(w, v)$ (triangle inequality).

199.3 (a) $\zeta(u, v) = \|u - v\| \geq 0$, $\|u - v\| = 0$ if and only $u - v = 0$

(b) $\zeta(u, v) = \|u - v\| = \|v - u\| = \zeta(v, u)$

(c) We first prove that $\|x + y\| \leq \|x\| + \|y\|$ for all x, y in V.

$\|x + y\|^2 = (x + y, x + y) = (x, x) + (y, y) + (x, y) + (x, y)$

$= \|x\|^2 + \|y\|^2 + (x, y) + \overline{(x, y)}$.

The sum $(x, y) + \overline{(x, y)}$ is real.

The Schwarz inequality shows that $|(x, y)| \leq \|x\|\|y\|$ and $|\overline{(x, y)}| \leq \|x\|\|y\|$, so we have

$\|x + y\|^2 \leq \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| = (\|x\| + \|y\|)^2$.

This proves $\|x + y\| \leq \|x\| + \|y\|$.

Hence $\|u - v\| = \|(u - w) + (w - v)\| \leq \|u - w\| + \|w - v\|$

Therefore $\zeta(u, v) \leq \zeta(u, w) + \zeta(w, v)$

4. If $\{w_1, \ldots, w_m\}$ is an orthonormal set in V, prove that

$$\sum_{i=1}^{m} |(w_i, v)|^2 \leq \|v\|^2 \text{ for any } v \in V.$$

(Bessel inequality)

200.4 Let $u = v - \sum_{i=1}^{m} (v, w_i) w_i$

$$0 \leq (u, u) = \left(v - \sum_{i=1}^{m} (v, w_i) w_i, \; v - \sum_{j=1}^{m} (v, w_j) w_j\right)$$

$$= (v, v) + \Big(\sum_{i=1}^{m} (v, w_i)\, w_i, \sum_{j=1}^{m} (v, w_j)\, w_j\Big)$$
$$-\Big(v, \sum_{j=1}^{m} (v, w_j)\, w_j\Big) - \Big(\sum_{i=1}^{m} (v, w_i)\, w_i, v\Big)$$
$$= (v, v) + \sum_{i=1}^{m}\sum_{j=1}^{m} (v, w_i)\overline{(v, w_j)}\,(w_i, w_j)$$
$$- \sum_{j=1}^{m} \overline{(v, w_j)}\,(v, w_j) - \sum_{i=1}^{m} (v, w_i)(w_i, v)$$
$$= (v, v) + \sum_{i=1}^{m} (v, w_i)\,\overline{(v, w_i)}\,(w_i, w_i)$$
$$- \sum_{j=1}^{m} (v, w_j)\,\overline{(v, w_j)} - \sum_{i=1}^{m} (v, w_i)\overline{(v, w_i)}$$
$$= (v, v) - \sum_{i=1}^{m} (v, w_i)\overline{(v, w_i)}$$
$$= (v, v) - \sum_{i=1}^{m} |(v, w_i)|^2$$

Hence $\sum_{i=1}^{m} |(w_i, v)|^2 \leq \|v\|^2$ for any $v \in V$.

5. If V is finite-dimensional and if $\{w_1, \ldots, w_m\}$ is an orthonormal set in V such that

$$\sum_{i=1}^{m} |(w_i, v)|^2 = \|v\|^2$$

for every $v \in V$, prove that $\{w_1, \ldots, w_m\}$ must be a basis of V.

200.5 The equality sign holds in (200.4) if and only if $(u, u) = 0$. That is $u = v - \sum_{i=1}^{m} (v, w_i)\, w_i = 0$. Therefore $w_1, \cdots, w_m$ span V. By Lemma 4.4.4., $w_1, w_2, \cdots, w_m$ are linearly independent. This shows that $\{w_1, \cdots, w_m\}$ is a basis of V.

6. If $\dim V = n$ and if $\{w_1, \ldots, w_m\}$ is an orthonormal set in V, prove that there exist vectors $w_{m+1}, \ldots, w_n$ such that $\{w_1, \ldots, w_m, w_{m+1}, \ldots, w_n\}$ is an orthonormal set (and basis of V).

200.6 By Lemma 4.2.5, there are vectors $U_{m+1}, U_{m+2}, \cdots, U_n$ such that $\{w_1, w_2, \cdots, w_m, U_{m+1}, \cdots, U_n\}$ is a basis of V. By Gram-Schmidt Orthogonalization Process, there exist vectors $w_{m+1}, \cdots, w_n$ such that $\{w_1, \cdots, w_m, w_{m+1}, \cdots, w_n\}$ is an orthonormal set.

7. Use the result of Problem 6 to give another proof of Theorem 4.4.3.

200.7 Let $\{w_1, \cdots, w_m\}$ be one orthonormal basis of W. By (200.6), there exist vectors $w_{m+1}, \cdots, w_n$ such that $\{w_1, \cdots, w_m, w_{m+1}, \cdots, w_n\}$ is a orthonormal set and a basis of V. $v \in V$ implies

$$v = \sum_{i=1}^{m} \alpha_i w_i + \sum_{i=m+1}^{n} \beta_i w_i \in W + W^{\perp}$$

$V = W + W^{\perp}$; Since $W \cap W^{\perp} = (0)$, this sum is direct.

8. In V prove the parallelogram law:

$$\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2).$$

Explain what this means geometrically in the special case $V = F^{(3)}$, where F is the real field, and where the inner product is the usual dot product.

200.8
$$\|u + v\|^2 + \|u - v\|^2$$
$$= (u + v, u + v) + (u - v, u - v)$$
$$= ((u, u) + (v, v) + (u, v) + (v, u))$$
$$+ ((u, u) + (v, v) - (u, v) - (v, u))$$
$$= 2((u, u) + (v, v))$$
$$= 2(\|u\|^2 + \|v\|^2).$$

Geometric meaning: the sum of the squares of the diagonals of a parallelogram is equal to the sum of the squares of its sides.

9. Let V be the real functions $y = f(x)$ satisfying $d^2y/dx^2 + 9y = 0$.
(a) Prove that V is a two-dimensional real vector space.
(b) In V define $(y, z) = \int_0^\pi yz\,dx$. Find an orthonormal basis in V.

200.9 (a) $\{\cos 3t, \sin 3t\}$ is a basis of V.
(b) $\left\{\sqrt{\frac{2}{\pi}}\cos 3t, \sqrt{\frac{2}{\pi}}\sin 3t\right\}$ is an orthonormal basis in V.

10. Let V be the set of real functions $y = f(x)$ satisfying

$$\frac{d^3y}{dx^3} - 6\frac{d^2y}{dx^2} + 11\frac{dy}{dx} - 6y = 0.$$

(a) Prove that V is a three-dimensional real vector space.
(b) In V define

$$(u, v) = \int_{-\infty}^{0} uv\,dx.$$

Show that this defines an inner product on V and find an orthonormal basis for V.

200.10 (a) $\{e^x, e^{2x}, e^{3x}\}$ is a basis of V.
(b) $\{\sqrt{2}\,e^x, 6e^{2x} - 4e^x, \sqrt{3}(10e^{3x} - 12e^{2x} + 3e^x)\}$ is an orthonormal basis in V.

11. If W is a subspace of V and if $v \in V$ satisfies $(v, w) + (w, v) \leq (w, w)$ for every $w \in W$, prove that $(v, w) = 0$ for every $w \in W$.

200.11 $\frac{1}{m}w \in W$ for all $w \in W$ and $m \in N$.

$$(v, \tfrac{1}{m}w) + (\tfrac{1}{m}w, v) \leq (\tfrac{1}{m}w, \tfrac{1}{m}w).$$

$$\tfrac{1}{m}((v, w) + (w, v)) \leq \tfrac{1}{m^2}(w, w).$$

$$((v, w) + (w, v)) \leq \tfrac{1}{m}(w, w)$$

$$(v, w) + (w, v) \leq 0 \text{ for all } w \in W.$$

$$(v, -w) + (-w, v) \leq 0$$
$$-((v, w) + (w, v)) \leq 0$$
$$0 \leq (v, w) + (w, v) \leq 0$$
$$(v, w) + (w, v) = 0$$

If F is the field of real numbers, then $(v, w) = (w, v) = 0$ for all w in W.

If F is the field of complex numbers, then $iw \in W$.

$$(v, iw) + (iw, v) = 0$$
$$-i(v, w) + i(w, v) = 0$$
$$-(v, w) + (w, v) = 0$$
$$(v, w) + (w, v) = 0$$

Hence $(v, w) = 0$ for all w in W.

12. If V is a finite-dimensional inner product space and if f is a linear functional on V (i.e., $f \in V$), prove that there is a $u_0 \in V$ such that $f(v) = (v, u_0)$ for all $v \in V$.

200.12 Let $\{v_1, \cdots, v_n\}$ be an orthonormal basis of V. Let $u_0 = \sum_{i=1}^{n} \overline{f(v_i)}\,v_i$.

$$(v_j, u_0) = (v_j, \sum_{i=1}^{n} \overline{f(v_i)}\,v_i)$$
$$= \sum_{i=1}^{n} f(v_i)(v_j, v_i)$$
$$= f(v_j)(v_j, v_j) = f(v_j)$$

$v \in V$, $v = \sum_{j=1}^{n} \alpha_j v_j$

$$(v, u_0) = (\sum_{j=1}^{n} \alpha_j v_j, u_0)$$
$$= \sum_{j=1}^{n} \alpha_j (v_j, u_0)$$
$$= \sum_{j=1}^{n} \alpha_j f(v_j)$$
$$= f(\sum_{j=1}^{n} \alpha_j v_j) = f(v).$$

4.5 modules

1. Verify that the statement made in Example 4.5.1 that every abelian group is a module over the ring of integers is true.

205.1 Let R be the ring of integers . G is an abelian group. $r(a+b)=ra+rb$ by (35.2). $r(sa)=(rs)a$, $(r+s)a=ra+sa$ by (1)(2) on page 29. G is a module over R .

2. Verify that the set in Example 4.5.4 is an R-module.

205.2 M is an abelian group.
$r((a+\lambda)+(b+\lambda))=r((a+b)+\lambda)$
$=r(a+b)+\lambda=(ra+rb)+\lambda$
$=(ra+\lambda)+(rb+\lambda)=r(a+\lambda)+r(b+\lambda)$.
$r(s(a+\lambda))=r(sa+\lambda)=(r(sa)+\lambda)$
$=((rs)a+\lambda)=(rs)(a+\lambda)$.
$(r+s)(a+\lambda)=(r+s)a+\lambda=(ra+sa)+\lambda$
$=(ra+\lambda)+(sa+\lambda)=r(a+\lambda)+s(a+\lambda)$.
M is an R-module.

3. Suppose that R is a ring with a unit element and that M is a module over R but is not unital. Prove that there exists an $m \neq 0$ in M such that $rm = 0$ for all $r \in R$.

205.3 Since M is not unital R-module , there exists an m' in M such that $1 \cdot m' \neq m'$.
$m = 1 \cdot m' - m' \neq 0$.
$rm = r(1 \cdot m' - m') = r(1 \cdot m') - rm'$
$= (r \cdot 1)m' - rm' = rm' - rm' = 0$
for all r in R .

Given two R-modules M and N then the mapping T from M into N is called a *homomorphism* (or *R-homomorphism* or *module homomorphism*) if

1. $(m_1 + m_2)T = m_1T + m_2T$;
2. $(rm_1)T = r(m_1T)$;

for all $m_1, m_2 \in M$ and all $r \in R$.

4. If T is a homomorphism of M into N let $K(T) = \{x \in M \mid xT = 0\}$. Prove that $K(T)$ is a submodule of M and that $I(T) = \{xT \mid x \in M\}$ is a submodule of N.

205.4 $x, y \in K(T)$ implies $xT = yT = 0$.
$(x-y)T = xT - yT = 0 - 0 = 0$
$x - y \in K(T)$, $r \in R$, $(rx)T = r(xT) = r \cdot 0 = 0$,
$rx \in K(T)$. $K(T)$ is a submodule of M.
$xT, yT \in I(T)$ implies
$xT - yT = (x-y)T \in I(T)$, $r \in R$,
$r(xT) = (rx)T \in I(T)$, $I(T)$ is a submodule of M.

5. The homomorphism T is said to be an *isomorphism* if it is one-to-one. Prove that T is an isomorphism if and only if $K(T) = (0)$.

205.5 If T is an isomorphism, then $xT = 0$ implies $x = 0$ since T is one-to-one . Hence $K(T) = (0)$. Conversely , Suppose $K(T) = 0$. If $xT = yT$ for some x , y in M , then $(x-y)T = xT - yT = 0$, $(x-y) \in K(T) = (0)$, $x = y$, T is one-to-one . Hence T is an isomorphism if and only if $K(T) = (0)$

6. Let M, N, Q be three R-modules, and let T be a homomorphism of M into N and S a homomorphism of N into Q. Define $TS: M \to Q$ by $m(TS) = (mT)S$ for any $m \in M$. Prove that TS is an R-homomorphism of M into Q and determine its kernel, $K(TS)$.

205.6 $(m_1 + m_2)(TS) = ((m_1 + m_2)T)S$
$= (m_1T + m_2T)S = (m_1T)S + (m_2T)S$
$= m_1(TS) + m_2(TS)$, $(rm_1)(TS) = ((rm_1)T)S$
$= (r(m_1T))S = r((m_1T)S)$
$= r(m_1(TS))$,
for all m_1 , m_2 in M and all r in R . TS is an R-homomorphism of M into Q .
$K(TS) = \{m \mid m(TS) = 0\} = \{m \mid mT \in K(S)\}$.

7. If M is an R-module and A is a submodule of M, define the quotient module M/A (use the analogs in group, rings, and vector spaces as a guide) so that it is an R-module and prove that there is an R-homomorphism of M onto M/A.

205.7 Let M/A consist of all the coset , $m+A$, where $m \in M$, of A in M . In M/A define $(m_1+A)+(m_2+A)=(m_1+m_2)+A$ and $r(m+A)=rm+A$ Since A is a submodule of M, these definitions are well-defined. There is no difficult to show that M/A is an R-module .
Define $T: M \to M/A$ as $mT=m+A$. T is an R-homomorphism of M onto M/A .

8. If T is a homomorphism of M onto N with $K(T) = A$, prove that N is isomorphic (as a module) to M/A.

205.8 Define $S: M/A \to N$ as $(m+A)S = mT$
If $m+A=m'+A$, then $m-m' \in A = K(T)$, $(m-m')T = 0$, $mT = m'T$, the definition of S is well-defined . S is clearly an R-homomorphism of M/A onto N.
$m+A \in K(S)$ implies $(m+A)S = mT = 0$, $m \in A$, $m+A = A = 0$, $K(S)=(0)$.
S is an isomorphism of M/A onto N . N is isomorphic to M/A .

9. If A and B are submodules of M prove
(a) $A \cap B$ is a submodule of M.
(b) $A + B = \{a + b \mid a \in A, b \in B\}$ is a submodule of M.
(c) $(A + B)/B$ is isomorphic to $A/(A \cap B)$.

205.9 (a) $x, y \in A \cap B$, $x \pm y \in A$, $x \pm y \in B$, $x \pm y \in A \cap B$. $r \in R$, $rx \in A$, $rx \in B$, $rx \in A \cap B$, $A \cap B$ is a submodule of M .
(b) $a+b \in A+B$, $a'+b' \in A+B$, where a , $a' \in A$, b , $b' \in B$. Then $(a+b)-(a'+b')=(a-a')+(b-b')$

$\in A + B$.
$r \in R$, $r(a+b) = ra+rb \in A+B$
$A+B$ is a submodule of M .
(c) Define $T: A+B \to A/A \cap B$ as $(a+b)T = a+(A \cap B)$. If $a+b=a'+b'$, then $a-a' = b'-b \in A \cap B$, $a+(A \cap B) = a'+(A \cap B)$, the definition of T is well-defined. T is clearly an R-homomorphism of $A+B$ onto $A/A \cap B$, $K(T) = B$. For , if $b \in B$, then $bT = 0 + (A \cap B) = A \cap B = 0$, $b \in K(T)$, $B \subset K(T)$, On the other hand, if $a + b \in K(T)$, $(a+b)T = a + A \cap B = 0$ implies $a \in A \cap B$, $a + b \in B$, $K(T) = B$ By (205.8) , $A + B / B$ is isomorphic to $A/A \cap B$.

10. An R-module M is said to be *irreducible* if its only submodules are (0) and M. Prove that any unital, irreducible R-module is cyclic.

206.10 Let M be a unital , irreducible R-module . Let $m \neq 0$ in M . Then $Rm = \{ rm \mid r \in R \}$ is a submodule of M . Since $m = 1 \cdot m \in Rm$, $Rm \neq (0)$, $Rm = M$. M is cyclic .

11. If M is an irreducible R-module, prove that either M is cyclic or that for every $m \in M$ and $r \in R$, $rm = 0$.

206.11 Let $N = \{ m \in M \mid rm = 0$ for all r in R $\}$.
N is a submodule of M . Hence $N = M$ or $N = (0)$. If $N = M$, then for every $m \in M$ and $r \in R$, $rm = 0$. Consider the case $N = 0$. Let $m \neq 0$ in M . $m \notin N$.
There is an r in R such that $rm \neq 0$.
Rm is a submodule of M , $Rm = (0)$ or $Rm = M$. Since $rm \in Rm$, $Rm \neq (0)$.
$Rm = M$. M is cyclic .

*12. If M is an irreducible R-module such that $rm \neq 0$ for some $r \in R$ and $m \in M$, prove that any R-homomorphism T of M into M is either an *isomorphism* of M *onto* M or that $mT = 0$ for every $m \in M$.

206.12 Suppose $T \neq 0$, By (205.4), $K(T)$ and $I(T)$ are submodule of M. $T \neq 0$ implies $K(T) \neq M$ and $I(T) \neq 0$. Since M is irreducible, $K(T) = 0$ and $I(T) = M$. T is an isomorphism of M onto M.

13. Let M be an R-module and let $E(M)$ be the set of all R-homomorphisms of M into M. Make appropriate definitions of addition and multiplication of elements of $E(M)$ so that $E(M)$ becomes a ring. (*Hint:* imitate what has been done for Hom (V, V), V a vector space.)

206.13 For $S, T \in E(M)$, define $TS : M \to M$ by $m(TS) = (mT)S$ for any $m \in M$. By (205.6), $TS \in E(M)$. Define $(T+S) : M \to M$ by $m(T+S) = mT + mS$. $T+S \in E(M)$. There is no difficult to show that $E(M)$ is a ring.

*14. If M is an irreducible R-module such that $rm \neq 0$ for some $r \in R$ and $m \in M$, prove that $E(M)$ is a division ring. (This result is known as *Schur's lemma.*)

206.14 We need only show that every element $T \neq 0$ in $E(M)$ has an inverse in $E(M)$. By (206.12), $0 \neq T \in E(M)$ implies T is one-to-one and onto. Define $T^{-1} : M \to M$ as $mT^{-1} = m'$ if $m = m'T$. Since T is one-to-one and onto, the definition of T^{-1} is well-defined and $T^{-1} \in E(M)$. $E(M)$ is a division ring.

15. Give a complete proof of Theorem 4.5.1 for finitely generated modules over Euclidean rings.

206.15 modify the proof given for the integers to M for R.

16. Let M be an R-module; if $m \in M$ let $\lambda(m) = \{x \in R \mid xm = 0\}$. Show that $\lambda(m)$ is a left-ideal of R. It is called the *order* of m.

206.16 $x, y \in \lambda(m)$ implies $xm = 0$, $ym = 0$. $(x-y)m = xm - ym = 0$, $r \in R$, $(rx)m = r(xm) = 0$, $x - y \in \lambda(M)$, $rx \in \lambda(M)$. $\lambda(M)$ is a left ideal of R.

17. If λ is a left-ideal of R and if M is an R-module, show that for $m \in M$, $\lambda m = \{xm \mid x \in \lambda\}$ is a submodule of M.

206.17 $x, y \in \lambda$, $xm - ym = (x-y)m \in \lambda m$. $r(xm) = (rx)m \in \lambda m$ λm is a submodule of M.

*18. Let M be an irreducible R-module in which $rm \neq 0$ for some $r \in R$ and $m \in M$. Let $m_0 \neq 0 \in M$ and let $\lambda(m_0) = \{x \in R \mid xm_0 = 0\}$.
(a) Prove that $\lambda(m_0)$ is a maximal left-ideal of R (that is, if λ is a left-ideal of R such that $R \supset \lambda \supset \lambda(m_0)$, then $\lambda = R$ or $\lambda = \lambda(m_0)$).
(b) As R-modules, prove that M is isomorphic to $R - \lambda(m_0)$ (see Example 4.5.4).

206.18 (a) Let λ be a left ideal of R such that $R \supset \lambda \supset \lambda(m_0)$ and $\lambda \neq \lambda(m_0)$. By (206.17), $\lambda m_0 \neq (0)$ is a submodule of M. Since M is irreducible, $\lambda m_0 = M$. For $r \in R$, $rm_0 = am_0$ for some a in λ. $(r-a)m_0 = 0$ implies $r - a \in \lambda(m_0) \subset \lambda$. $a \in \lambda$. $r \in \lambda$. $R \subset \lambda$. $R = \lambda$. Hence $\lambda(m_0)$ is a maximal left-ideal of R.

(b) Define $T : R \to M$ by $rT = rm_0$. Clearly, T is an R-homomorphism of R into M. By the proof of (206.11), T is onto $K(T) = \lambda(m_0)$. By (205.7), M is isomorphic to $R - \lambda(m_0)$.

5 Fields

5.1 Extension Fields

1. Prove that the mapping $\psi: F[x] \to F(a)$ defined by $h(x)\psi = h(a)$ is a homomorphism.

214.1 $h(x), k(x) \in F(x)$, $(h(x)+k(x))\Psi = h(a)+k(a) = h(x)\Psi + k(x)\Psi$.
$(h(x)k(x))\Psi = h(a)k(a) = [(h(x)\Psi][(k(x)\Psi]$.
Ψ is a homomorphism.

2. Let F be a field and let $F[x]$ be the ring of polynomials in x over F. Let $g(x)$, of degree n, be in $F[x]$ and let $V = (g(x))$ be the ideal generated by $g(x)$ in $F[x]$. Prove that $F[x]/V$ is an n-dimensional vector space over F.

214.2 $1+V, x+V, \cdots\cdots, x^{n-1}+V$ is a basis of $F[x]/V$ over F. For, if $f(x) \in F[x]$, then there exist $a(x), b(x)$ in $F[x]$ such that $f(x) = a(x)g(x)+b(x)$ and $b(x) = 0$ or $\deg b(x) < \deg g(x)$. $a(x)g(x) \in V$, $f(x)+V = b(x)+V$. Let $b(x) = a_0+a_1x+\cdots\cdots+a_{n-1}x^{n-1}$. $f(x)+V = b(x)+V = (a_0+a_1x+\cdots\cdots+a_{n-1}x^{n-1})+V = a_0(1+V)+a_1(x+V)+\cdots\cdots+a_{n-1}(x^{n-1}+V)$. $1+V, x+V, \cdots\cdots, x^{n-1}+V$ span $F[x]/V$. To prove $1+V, x+V, \cdots\cdots, x^{n-1}+V$ are linearly independent over F, suppose $\alpha_0(1+V)+\alpha_1(x+V)+\cdots\cdots+\alpha_{n-1}(x^{n-1}+V)=0$.
$0=\alpha_0(1+V)+\alpha_1(x+V)+\cdots\cdots+\alpha_{n-1}(x^{n-1}+V)$
$=(\alpha_0+\alpha_1x+\cdots\cdots+\alpha_{n-1}x^{n-1})+V$.
$\alpha_0+\alpha_1x+\cdots\cdots+\alpha_{n-1}x^{n-1} \in V = (g(x))$. Since $\deg g(x) = n > n-1$, $\alpha_0=\alpha_1=\cdots\cdots=\alpha_{n-1}=0$. $1+V, x+V, \cdots\cdots, x^{n-1}+V$ is a basis of $F[x]/V$ over F. $F[x]/V$ is an n-dimensional vector space over F.

3. (a) If V is a finite-dimensional vector space over the field K, and if F is a subfield of K such that $[K:F]$ is finite, show that V is a finite-dimensional vector space over F and that moreover $\dim_F(V) = (\dim_K(V))([K:F])$.
(b) Show that Theorem 5.1.1 is a special case of the result of part (a).

214.3 (a) Since F is a subfield of K and V is a vector space over K, V is a vector space over F. Let $\dim_K V = m$ and $v_1, v_2, \cdots\cdots, v_m$ be a basis of V over K. Let $[K:F]=n$ and $a_1, a_2, \cdots\cdots, a_n$ be a basis of K over F. Then, $S = \{a_i v_j \mid i=1,2,\cdots\cdots,n.\ j=1,2,\cdots\cdots,m\}$ is a basis of V over F. For, if $v \in V$, then $v = \sum_{j=1}^{m} \alpha_j v_j$, $\alpha_j \in K$.
$\alpha_j = \sum_{i=1}^{n} a_{ij}a_i$. $v = \sum_{j=1}^{m}(\sum_{i=1}^{n} a_{ij}a_i)v_j = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}a_iv_j$.
$\{a_i v_j \mid i=1,2,\cdots\cdots,n.\ j=1,2,\cdots\cdots,m\}$ spans V over F. To prove S is a linearly independent set, suppose that $\sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}a_iv_j=0$. Since $v_1, \cdots\cdots, v_n$ are linearly independent over K, $\sum_{i=1}^{n} a_{ij}a_i=0$. Since $a_1, \cdots\cdots, a_n$ are linearly independent over F, $a_{ij}=0$. Hence $\dim_F(V)=mn=(\dim_K(V))([K:F])$.
(b) That L is a finite extension of K implies L is a finite-dimensional vector space over K. By (a), L is a finite-dimensional vector space over F and $[L:F]=\dim_F(L)=(\dim_K(L))([K:F])=[L:K][K:F]$.

4. (a) Let R be the field of real numbers and Q the field of rational numbers. In R, $\sqrt{2}$ and $\sqrt{3}$ are both algebraic over Q. Exhibit a polynomial of degree 4 over Q satisfied by $\sqrt{2}+\sqrt{3}$.
(b) What is the degree of $\sqrt{2}+\sqrt{3}$ over Q? Prove your answer.
(c) What is the degree of $\sqrt{2}\sqrt{3}$ over Q?

215.4 (a) Let $a=\sqrt{2}+\sqrt{3}$. $a-\sqrt{2}=\sqrt{3}$. $(a-\sqrt{2})^2=3$. $a^2-2\sqrt{2}a+2=3$. $a^2-1=2\sqrt{2}a$. $(a^2-1)^2=8a^2$. $a^4-2a^2+1=8a^2$. $a^4-10a^2+1=0$.
$\sqrt{2}+\sqrt{3}$ satisfies x^4-10x^2+1.

(b) By (161.4), x^4-10x^2+1 has no linear divisor. Let $p(x)$ be the minimal, monic polynomial for $\sqrt{2}+\sqrt{3}$ over Q. $p(x) \mid x^4-10x^2+1$. $\deg p(x)=2$ or 4. Suppose $\deg p(x)=2$. Let $P(x)=x^2+\alpha x+\beta, \alpha, \beta \in Q$.

Then $\sqrt{2}+\sqrt{3}$ and $\frac{\beta}{\sqrt{2}+\sqrt{3}}=\beta(\sqrt{3}-\sqrt{2})$ are two roots of $p(x)$ and $(\sqrt{2}+\sqrt{3})+\beta(\sqrt{3}-\sqrt{2})=-\alpha$, a contradiction. Hence $\deg p(x)=4$.

(c) $\sqrt{2}\sqrt{3}$ satisfies x^2-6. The degree of $\sqrt{2}\sqrt{3}$ orer Q is 2.

5. With the same notation as in Problem 4, show that $\sqrt{2}+\sqrt[3]{5}$ is algebraic over Q of degree 6.

215.5 Let $a=\sqrt{2}+\sqrt[3]{5}$.

$(a-\sqrt{2})^3=5$.

$a^3-3\sqrt{2}a^2+6a-2\sqrt{2}=5$.

$(a^3+6a-5)=5\sqrt{2}$. $(a^3+6a-5)^2=50$.

$a^6+12a^4-10a^3+36a^2-60a-25=0$.

a satisfies $p(x)=x^6+12x^4-10x^3+36x^2-60x-25$ and satisfies also $q(x)=x^3-3\sqrt{2}x^2+6x-(2\sqrt{2}+5)$. Let $f(x)$ be the minimal polynomial for a over Q. $\deg f(x) \mid 6$. $\deg f(x) \neq 1$. $\deg f(x) \neq 2$. If $\deg f(x)=3$, then $f(x)=q(x)$ since $q(x)$ is the minimal polynomial for a over $Q(\sqrt{2})$, a contradiction. Hence $\deg f(x)=6$. $\sqrt{2}+\sqrt[3]{5}$ is algebraic over Q of degree 6.

*6. (a) Find an element $u \in R$ such that $Q(\sqrt{2}, \sqrt[3]{5}) = Q(u)$.

(b) In $Q(\sqrt{2}, \sqrt[3]{5})$ characterize all the elements w such that $Q(w) \neq Q(\sqrt{2}, \sqrt[3]{5})$.

215.6 (a) By (215.8), $Q(\sqrt{2}, \sqrt[3]{5})$ is of degree 6. Since $\sqrt{2}+\sqrt[3]{5}$ is of degree 6 over Q. $Q(\sqrt{2}+\sqrt[3]{5})=Q(\sqrt{2}, \sqrt[3]{5})$.

(b) $\omega \in Q(\sqrt{2}) \cup Q(\sqrt[3]{5})$. ω is of degree 1, 2 or 3, $Q(\omega) \neq Q(\sqrt{2}, \sqrt[3]{5})$. If $\omega \notin Q(\sqrt{2}) \cup Q(\sqrt[3]{5})$, $\omega=\alpha_0+\alpha_1\sqrt{2}+\alpha_2\sqrt[3]{5}+\alpha_3\sqrt[3]{5}^2+\alpha_4\sqrt{2}\sqrt[3]{5}+\alpha_5\sqrt{2}\sqrt[3]{5}^2$ is not of degree 1, 2 or 3. Hence ω is of degree 6, $Q(\omega)=Q(\sqrt{2}, \sqrt[3]{5})$.

7. (a) Prove that $F(a, b) = F(b, a)$.

(b) If $(i_1, i_2, \ldots, i_n)$ is any permutation of $(1, 2, \ldots, n)$, prove that

$$F(a_1, \ldots, a_n) = F(a_{i_1}, a_{i_2}, \ldots, a_{i_n}).$$

215.7 (a) $F(a,b)=(F(a))(b)$, $F(b,a)=(F(b))(a)$. $F \subset (F(b))(a)$, $a \in (F(b))(a)$. $F(a) \subseteq (F(b))(a)$. $b \in (F(b))(a)$. $((F(a))(b)) \subseteq (F(b))(a)$. Hence $F(a,b) \subset F(b,a)$.

Similarly $F(b,a) \subset F(a,b)$. $F(a,b)=F(b,a)$

(b) If $i_n=n$, then $F(a_1, \cdots\cdots, a_{n-1}, a_n)=(F(a_1, \cdots\cdots, a_{n-1}))(a_n)=(F(a_{i_1}, \cdots\cdots, a_{i_{n-1}}))(a_{i_n})$ $= F(a_{i_1}, \cdots\cdots, a_{i_n})$ by induction hypothesis.

Suppose $i_{n-1} < n$. $F(a_1, \cdots\cdots, a_n)=(F(a_1, \cdots\cdots, a_{n-1}))(a_n)=(F(a_1, \cdots\cdots, \hat{a}_{i_n}, \cdots\cdots, a_{n-1}, a_{i_n}))(a_n)$ (by induction hypothesis)

$=(F(a_1, \cdots\cdots \hat{a}_{i_n}, \cdots\cdots, a_{n-1}))(a_{i_n}, a_n)$

$=(F(a_1, \cdots\cdots \hat{a}_{i_n}, \cdots\cdots, a_{n-1}))(a_n, a_{i_n})$ (by (a)) $=(F(a_1 \cdots\cdots, \hat{a}_{i_n} \cdots\cdots, a_{n-1})(a_n))(a_{i_n})$

$= (F(a_1, \cdots\cdots, \hat{a}_{i_n}, \cdots\cdots, a_{n-1}, a_n))(a_{i_n})$

$=(F(a_{i_1}, \cdots\cdots, a_{i_{n-1}}))(a_{i_n})$ (by induction hypothesis)

$=F(a_{i_1}, \cdots\cdots, a_{i_n})$.

8. If $a, b \in K$ are algebraic over F of degrees m and n, respectively, and if m and n are relatively prime, prove that $F(a, b)$ is of degree mn over F.

215.8 By the proof of Theorem 5.1.4, we know that $[F(a,b):F] \leq mn$. On the other hand, since $[F(a,b):F]=[F(a,b):F(a)][F(a):F]=[F(a,b):F(a)]m$, we have $m \mid [F(a,b):F]$. Similarly, $n \mid [F(a,b):F]$. Since m and n are relatively prime,

$mn \mid [F(a,b):F]$. $mn \leq [F(a,b):F] \leq mn$ implies $[F(a,b):F]=mn$.

9. Suppose that F is a field having a finite number of elements, q.
   (a) Prove that there is a prime number p such that $\underbrace{a+a+\cdots+a}_{p\text{-times}}=0$ for all $a \in F$.
   (b) Prove that $q = p^n$ for some integer n.
   (c) If $a \in F$, prove that $a^q = a$.
   (d) If $b \in K$ is algebraic over F, prove $b^{q^m} = b$ for some $m > 0$.

215.9 (a) By (130.6), there is a prime number p such that $pa=0$ for all a in F.

(b) By (24.14) and (a), $\{0,1,2,\cdots\cdots,p-1\}$ forms a subfield P of F. Suppose $[F:P]=n$. $q=p^n$.

(c) Since the set of all nonzero elements of F is a group of order $q-1$, $a^{q-1}=e$ for all $a \in F$, $a \neq 0$. Hence $a^q=a$ for $a \neq 0$. If $a=0$, then $a^q=0=a$. $a^q=a$ for all a in F.

(d) Suppose $b \neq 0$. By Theorem 5.1.2., $[F(b):F]=m < \infty$. F(b) is of order q^m. By (c), $b^{q^m} = b$ and $m > 1$. If $b=0$, $b^q=0=b$. Hence $b^{q^m}=b$ for some $m > 0$.

An algebraic number a is said to be an *algebraic integer* if it satisfies an equation of the form $a^m + \alpha_1 a^{m-1} + \cdots + \alpha_m = 0$, where $\alpha_1, \ldots, \alpha_m$ are integers.

10. If a is any algebraic number, prove that there is a positive integer n such that na is an algebraic integer.

215.10 Since a is an algebraic number, there are integers $\alpha_0, \alpha_1, \cdots\cdots, \alpha_m$, $\alpha_m \neq 0$, such that $\alpha_m a^m + \alpha_{m-1} a^{m-1} + \cdots\cdots + \alpha_0 = 0$. Multiplying the equation by α_m^m, we have $(\alpha_m a)^m + \alpha_{m-1}\alpha_m(\alpha_m a)^{m-1} + \alpha_{m-2}\alpha_m^2(\alpha_m a)^{m-2} + \cdots\cdots + \alpha_0\alpha_m^m = 0$. $\alpha_m a$ is an algebraic integer.

11. If the rational number r is also an algebraic integer, prove that r must be an ordinary integer.

215.11 Let $r = \frac{q}{p}$, where $(p,q)=1$. Since r is an algebraic integer, there are integers $\alpha_1, \cdots\cdots, \alpha_m$ such that $r^m + \alpha_1 r^{m-1} + \cdots + \alpha_m = 0$.
$q^m + \alpha_1 q^{m-1} p + \alpha_2 q^{m-2} p^2 + \cdots\cdots + \alpha_m p^m = 0$.
$q^m = -p(\alpha_1 q^{m-1} + \alpha_2 q^{m-2} p + \cdots + \alpha_m p^{m-1})$.
$p \mid q^m$ implies $(p,q) \neq 1$ if $p=1$. Therefore $p=1$ and $r=q$ is an integer.

12. If a is an algebraic integer and m is an ordinary integer, prove
   (a) $a + m$ is an algebraic integer.
   (b) ma is an algebraic integer.

215.12 There are integers $\alpha_1, \alpha_2, \cdots\cdots, \alpha_n$ such that $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$.

(a) Let $b=a+m$. $a=b-m$. b satisfies $(b-m)^n + \alpha_1(b-m)^{n-1} + \cdots\cdots + \alpha_n = 0$. Since the coeficient of b^n is 1, $b=a+m$ is an algebraic integer.

(b) $m^n(a^n + \alpha_1 a^{n-1} + \cdots\cdots + \alpha_n) = 0$.
$(ma)^n + \alpha_i m(ma)^{n-1} + \cdots\cdots + \alpha_n = 0$.
ma is an algebraic integer.

13. If α is an algebraic integer satisfying $\alpha^3 + \alpha + 1 = 0$ and β is an algebraic integer satisfying $\beta^2 + \beta - 3 = 0$, prove that both $\alpha + \beta$ and $\alpha\beta$ are algebraic integers.

215.13 By (215.14), $\alpha+\beta$ and $\alpha\beta$ are algebraic integers.

**14. (a) Prove that the sum of two algebraic integers is an algebraic integer.

(b) Prove that the product of two algebraic integers is an algebraic integer.

215.14 Let α and β be algebraic integers. There are integers $a_1, a_2, \cdots\cdots, a_m, b_1, b_2, \cdots\cdots, b_n$ such that
$\alpha^m = a_1\alpha^{m-1} + a_2\alpha^{m-2} + \cdots\cdots + a_m$

$\beta^n=b_1\beta^{n-1}+b_2\beta^{n-2}+\cdots\cdots+b_n$.

Form the mn=N numbers $\alpha^i\beta^j$, $0\leq i\leq m-1$, $0\leq j\leq n-1$, which, arranged in some fixed order, we denote by $\omega_1,\omega_2,\cdots\cdots,\omega_N$.

α^m and high powers of α can be expressed as polynomials in α of degree less than m. Similarly for β. Hence $\omega_i(\alpha+\beta)$ can be expressed in the form

$\omega_i(\alpha+\beta)=c_{i1}\omega_1+c_{i2}\omega_2+\cdots\cdots+c_{iN}\omega_N$, $i=1,2,\cdots\cdots,N$, in which each c_{ij} is an integer.

But the above equations form a system of linear homogeneous equation for the ω_i:

$(c_{11}-(\alpha+\beta))\omega_1+c_{12}\omega_2+\cdots\cdots+c_{1N}\omega_N=0$

$c_{11}\omega_1+(c_{22}-(\alpha+\beta))\omega_2+\cdots\cdots+c_{2N}\omega_N=0$

.....

$c_{N1}\omega_1+c_{N2}\omega_2+\cdots\cdots+(c_{NN}-(\alpha+\beta))\omega_N=0$.

Since the ω_i are not all zero, the determinant of the coefficients must vanish. Multiplying by $(-1)^N$ we get the equation,

$(\alpha+\beta)^N-(c_{11}+c_{22}+\cdots\cdots+c_{NN})(\alpha+\beta)^{N-1}+\cdots\cdots=0$,

whose coefficients are integers. Thus $(\alpha+\beta)$ is an algebraic integer. Replace $\alpha+\beta$ by $\alpha\beta$, we have $\alpha\beta$ is also an algebrace integer.

Note that, modifying this, for α and β being algebraic over a field F we can also prove that $\alpha+\beta$ and $\alpha\beta$ are algebraic over F.

15. (a) Prove that sin 1° is an algebraic number.
(b) From part (a) prove that sin m° is an algebraic number for any integer m.

216.15

$$\sin m^0=\frac{1}{2i}\left(e^{\frac{m\pi}{180}i}-e^{-\frac{m\pi}{180}i}\right).$$

$(e^{\frac{m\pi}{180}i})^{2\cdot 180}=e^{2m\pi i}=1$. $e^{\frac{m\pi}{180}i}$ and $e^{-\frac{m\pi}{180}i}$ are al-

gebraic numbers, $\frac{1}{2i}$ is an algebraic number.

By the Corollary to Theorem 5.1.4, sin m° is an algebraic number for any integer m.

5.2. Transcendence of e.

1. Using the infinite series for e,

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{m!} + \cdots,$$

prove that e is irrational.

219.1 If e is rational, then there is a positive integer m such that $(m!)e$ is an integer.

$(m!)e = r + \frac{1}{m+1} + \frac{1}{(m+2)(m+1)} + \frac{1}{(m+3)(m+2)(m+1)} + \cdots\cdots$, where r is an integer. $s = (m!)e - r$ is also a positive integer.

$$0 < \frac{1}{m+1} + \frac{1}{(m+2)(m+1)} + \frac{1}{(m+3)(m+2)(m+1)} + \cdots\cdots$$

$$< \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots\cdots = 1.$$

$0 < s < 1$, a contradiction.

2. If $g(x)$ is a polynomial with integer coefficients, prove that if p is a prime number then for $i \geq p$,

$$\frac{d^i}{dx^i}\left(\frac{g(x)}{(p-1)!}\right)$$

is a polynomial with integer coefficients each of which is divisible by p.

219.2 $\frac{d^i}{dx^i}\left(\frac{x^n}{(p-1)!}\right) = 0$ if $n < i$.

$\frac{d^i}{dx^i}\left(\frac{x^n}{(p-1)!}\right) = \frac{n(n-1)\cdots\cdots(n-i+1)}{(p-1)!}x^{n-i}$ if $n \geq i$. $n \geq i \geq p$. $n(n-1)\cdots\cdots(n-i+1)$ is divisible by p!. Hence $\frac{di}{dx^i}\left(\frac{x^n}{(p-1)!}\right)$ is a polynomial with integer coefficients each of which is divisible. Since

$\frac{d^i}{dx^i}\left(\frac{f(x)+g(x)}{(p-1)!}\right) = \frac{d^i}{dx^i}\left(\frac{f(x)}{(p-1)!}\right) + \frac{d^i}{dx^i}\left(\frac{g(x)}{(p-1)!}\right)$ and

$\frac{d^i}{dx^i}\left(\frac{\alpha f(x)}{(p-1)!}\right) = \alpha \frac{d^i}{dx^i}\left(\frac{f(x)}{(p-1)!}\right)$,

we can prove that $\frac{d^i}{dx^i}\left(\frac{g(x)}{(p-1)!}\right)$ is a polynomial with integer coefficients each of which is divisible by p.

3. If a is any real number, prove that $(a^m/m!) \to 0$ as $m \to \infty$.

219.3 Since $\sum_{n=0}^{\infty} \frac{a^m}{m!}$ converges to e^a, $\lim_{m\to\infty} \frac{a^m}{m!} = 0$.

Another proof of $\frac{a^m}{m!} \longrightarrow 0$ as $m \longrightarrow \infty$.

Suppose $a > 0$. There is an integer n such that $n \geq a$.

$$\frac{a^{n+1}}{(n+1)!} \Big/ \frac{a^n}{n!} = \frac{a}{n+1} \leq \frac{a}{n+1}$$

$$\frac{a^{n+2}}{(n+2)!} \Big/ \frac{a^{n+1}}{(n+1)!} = \frac{a}{n+2} < \frac{a}{n+1}$$

$$\frac{a^{n+2}}{(n+2)!} \Big/ \frac{a^n}{n!} < \left(\frac{a}{n+1}\right)^2$$

$$\vdots$$

$$\frac{a^{n+k}}{(n+k)!} \Big/ \frac{a^n}{n!} < \left(\frac{a}{n+1}\right)^k$$

$$\vdots$$

$$0 < \frac{a^{n+k}}{(n+k)!} < \frac{a^n}{n!}\left(\frac{a}{n+1}\right)^k$$

Since $\left(\frac{a}{n+1}\right)^k \to 0$ as $k \to 0$ we have $\frac{a^m}{m!} \to 0$ as $m \to \infty$. When $a < 0$, we consider the sequence $\left|\frac{a^m}{m!}\right|$. $\left|\frac{a^m}{m!}\right| \to 0$ as $m \to \infty$. Hence $\frac{a^m}{m!} \to 0$ as $m \to \infty$.

4. If $m > 0$ and n are integers, prove that $e^{m/n}$ is transcendental.

219.4 we may suppose $n > 0$ and m is an integer.

If $e^{\frac{m}{n}}$ is algebraic, then $(e^{\frac{m}{n}})^n = (e^{\frac{m}{n}})(e^{\frac{m}{n}})\cdots(e^{\frac{m}{n}})$ (n factors)

is also algebraic. e^m is algebraic. e^m satisfies $f(x)$ with coefficients are rationals.

$f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots\cdots + a_0$.

$0 = f(e^m) = a_k e^{mk} + a_{k-1} e^{m(k-1)} + \cdots\cdots + a_0$ Either e or e^{-1} also satisfies a polymial with rational coefficients. e or e^{-1} is algebraic . e is algebraic, a contradiction.

5.3. Roots of Polynomials

1. In the proof of Lemma 5.3.1, prove that the degree of $q(x)$ is one less than that of $p(x)$.

227.1 In Lemma 5.3.1, we must suppose that $p(x)$ is not of degree 0 or $p(x) = 0$ since we do not define the degree of the zero polynomial.

If $q(x) = 0$, then $p(x) = (x-b)\, q(x) + p(b) = p(b)$, deg $p(x) = 0$. Hence $q(x) \neq 0$. Suppose deg $q(x) = r$ and $q(x) = a_r x^r + a_{r-1} x^{r-1} + \cdots\cdots + a_0$.

$r+1$ is the largest i for which the ith coefficient of $p(x) = (x-b)q(x) + p(b)$ is not zero. Hence deg $p(x) = r+1 =$ deg $q(x) + 1$. deg $q(x) =$ deg $p(x) - 1$.

2. In the proof of Theorem 5.3.1, prove in all detail that the elements $1 + V, x + V, \ldots, x^{n-1} + V$ form a basis of E over F.

227.2 For $f(x)+V$ in E, $f(x) = p(x)\, q(x) + r(x)$, where $q(x), r(x) \in F[x]$ and $r(x) = 0$ or deg $r(x) <$ deg $p(x)$. $p(x)\, q(x) + V = V$.

$f(x) + V = p(x)\, q(x) + r(x) + V = r(x) + V$. $f(x)+V$ is a linear combination of $1+V$, $x+V$, $\cdots\cdots$, $x^{n-1}+V$.

If $\alpha_0(1+V) + \alpha_1(x+V) + \cdots\cdots + \alpha_{n-1}(x^{n-1}+V) = 0$, for $\alpha_0, \alpha_1, \cdots\cdots, \alpha_{n-1}$ in F, then $(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}) + V = 0$. $\alpha_0 + \alpha_1 x + \cdots\cdots + \alpha_{n-1} x^{n-1} \in V = (p(x))$. $\alpha_0 + \alpha_1 x + \cdots\cdots + \alpha_{n-1} x^{n-1} = 0$. $\alpha_0 = \alpha_1 = \cdots\cdots = \alpha_{n-1} = 0$. $1+V, x+V, \cdots\cdots, x^{n-1}+V$ forms a basis of E over F .

3. Prove Lemma 5.3.3 in all detail.

227.3 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_0$, $g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots\cdots + b_0 \in F[x]$. $f(x) + g(x) = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \cdots\cdots + (a_0 + b_0)$.

$f(x)\, g(x) = c_0 + c_1 x + \cdots\cdots + c_k x^k$, where $c_t = a_t b_0 + a_{t-1} b_1 + \cdots\cdots + a_0 b_t$.

$(f(x)+g(x))\tau^* = (a_n+b_n)\tau t^n+(a_{n-1}+b_{n-1})\tau t^{n-1}$
$+\cdots\cdots+(a_0+b_0)\tau=(a_n\tau+b_n\tau)t^n+(a_{n-1}\tau+b_{n-1}\tau)$
$t^{n-1}+\cdots\cdots+(a_0\tau+b_0\tau)=(a_n\tau t^n+a_{n-1}\tau t^{n-1}+\cdots$
$\cdots+a_0\tau)+(b_n\tau t^n+b_{n-1}\tau t^{n-1}+\cdots\cdots+b_0\tau)=f(x)\tau^*$
$+g(x)\tau^*$.

$(f(x)g(x))\tau^*=c_k\tau t^k+c_{t-1}\tau t^{t-1}+\cdots\cdots+c_0\tau$.

$c_t\tau=(a_tb_0+a_{t-1}b_1+\cdots\cdots+a_0bt)\tau$
$=(a_t\tau)(b_0\tau)+(a_{t-1}\tau)(b_1\tau)+\cdots\cdots+(a_0\tau)$.
$(b_t\tau)$.

$(f(x)g(x))\ \tau^*=(f(x)\tau^*)(g(x)\tau^*)$. τ^* is clearly one-to-one and onto. For $\alpha\in F$, $\alpha\tau^*=\alpha\tau=\alpha'$. This completes the proof.

4. Show that τ^{**} in Lemma 5.3.4 is well defined and is an isomorphism of $F[x]/(f(x))$ onto $F[t]/(f'(t))$.

227.4 For $g(x)+(f(x))$ in $F[x]/(f(x))$, define $(g(x)+(f(x))\tau^{**}=g'(t)+(f'(t))$.
It's easy to show that τ^{**} is well-defined and is an isomorphism of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$ with the property that for every α in F, $\alpha\tau^{**}=\alpha^t$, $(x+(f(x))\ \tau^{**}=t+(f'(t))$.

5. In Example 3 at the end of this section prove that $F(\omega)$ is the splitting field of x^4+x^2+1.

227.5 The four roots of x^4+x^2+1 in the field of complex numbers are w, w^2, $-w$, $-w^2$. Hence $F(w)$ is the splitting field of x^4+x^2+1.

6. Let F be the field of rational numbers. Determine the degrees of the splitting fields of the following polynomials over F.
(a) x^4+1. (b) x^6+1.
(c) x^4-2. (d) x^5-1.
(e) x^6+x^3+1.

227.6 (a) Let $a=\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}$.
$a,-a,a^{-1},-a^{-1}$ are the four roots of x^4+1 in the field of complex numbers. x^4+1 is crreducible over F since it has no linear factor and quadratic factor over F. F(a) is the splitting field of x^4+1. The degree of the splitting field of x^4+1 is 4.

(b) Let $a=\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}$. $i,-i,a,-a,a^{-1},-a^{-1}$ are the six roots of x^6+1.

$a-a^{-1}=(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6})-(\cos\frac{\pi}{6}-i\sin\frac{\pi}{6})$
$=2i\sin\frac{\pi}{6}=i$.

F(a) is the splitting field of x^6+1. a satisfies x^4-x^2+1. x^4-x^2+1 is irreducible over F since it has no linear and quadratic factors over F. F(a) is of degree 4. The splitting field of x^6+1 is of degree 4.

(c) $\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}$, $-\sqrt[4]{2}i$ are the four roots of x^4-2. $F(\sqrt[4]{2},i)$ is the spitting field of x^4-2. For, $F(\sqrt[4]{2},i)\supset F(\sqrt[4]{2},\sqrt[4]{2}i,-\sqrt[4]{2},-\sqrt[4]{2}i)$ and $i=(\sqrt[4]{2}i)/\sqrt[4]{2}$ implies $F(\sqrt[4]{2},i)\subset F(\sqrt[4]{2},\sqrt[4]{2}i,-\sqrt[4]{2},-4\sqrt{2}i)$. $F(\sqrt[4]{2},i)=(F(\sqrt[4]{2}))(i)$.
$[F(\sqrt[4]{2},i):F]=[F(\sqrt[4]{2},i):F(\sqrt[4]{2})]\,[F(\sqrt[4]{2}):F]$
$=2\cdot4=8$.
The splitting field of x^4-2 is of degree 8.

(d) Let $a=\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$.
$1,a,a^2,a^3,a^4$ are five roots of x^5-1. a satisfies $x^4+x^3+x^2+x+1$. By(161.3), $x^4+x^3+x^2+x+1$ is irreducible over F. $[F(a):F]=4$. F(a) is the splitting field of x^5-1. The splitting of x^5-1 is of degree 4.

(e) Let $a=\cos\frac{2}{9}\pi+i\sin\frac{2}{9}\pi$.
$a,a^2,a^4,a^{-1},a^{-2},a^{-4}$ are the six roots of x^6+x^3+1. F(a) is the splitting field of x^6+x^3

+1. Since the product of a with any two of $\{a^2, a^4, a^{-1}, a^{-2}, a^{-4}\}$ is not rational, x^6+x^3+1 has no divisors of degree 3 which has a as a root. a clearly satisfies no polynomial of degree 1 or 2. x^6+x^3+1 is irreducible. $[F(a):F]=6$. The degree of the splitting field of x^6+x^3+1 is 6.

7. If p is a prime number, prove that the splitting field over F, the field of rational numbers, of the polynomial $x^p - 1$ is of degree $p - 1$.

227.7 Let $a=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$. $1, a, \cdots\cdots, a^{p-1}$ are the roots of x^p-1. $F(a)$ is the splitting field of x^p-1 over F. a satisfies $x^{p-1}+x^{p-2}+\cdots\cdots+x+1$. By (161.3), $x^{p-1}+x^{p-2}+\cdots\cdots+x+1$ is irreducible. Hence $[F(a):F]=p-1$. The splitting field of x^p-1 over F is p-1.

**8. If $n > 1$, prove that the splitting field of $x^n - 1$ over the field of rational numbers is of degree $\Phi(n)$ where Φ is the Euler Φ-function. (This is a well-known theorem. I know of no easy solution, so don't be disappointed if you fail to get it. If you get an easy proof, I would like to see it. This problem occurs in an equivalent form as Problem 15, Section 5.6.)

*9. If F is the field of rational numbers, find necessary and sufficient conditions on a and b so that the splitting field of $x^3 + ax + b$ has degree exactly 3 over F.

227.9 The splitting feld of x^3+ax+b has degree 3 over F if and only if x^3+ax+b is irreducible and $D=-4a^3-27b^2$ is the square of a rational number. Suppose that x^3+ax+b is irreducible over Q. Let x_1, x_2, x_3 be three roots of x^3+ax+b. $D=((x_1-x_2)(x_1-x_3)(x_2-x_3))^2=-4a^3-27b^2$. The splitting field of x^3+ax+b is $K=F(\sqrt{D}, x_1)$. $F(x_1, x_2, x_3)$ is the splitting field of x^3+ax+b. $K\subset F(x_1, x_2, x_3)$. Conversely, since $x_1+x_2+x_3=0$, $x_2+x_3\in K$. $(x-x_2)(x-x_3)=x^2-(x_2+x_3)x+x_2x_3=(x^3+ax+b)/(x-x_1)$ has coefficients in K. Hence $(x_1-x_2)(x_1-x_3)\in K$. $\sqrt{D}=(x_1-x_2)(x_1-x_3)(x_2-x_3)$. $x_2-x_3=\sqrt{D}/(x_1-x_2)(x_1-x_3)$ lies in K. Since x_2+x_3 and x_2-x_3 are in K. x_2 and x_3 lie in K. $F(x_1, x_2, x_3)\subset K$. $K=F(x_1, x_2, x_3)$ is the splitting field of x^3+ax+b. x_1 is of degree 3 over Q. Hence K is of degree 3 if and only if $D=-4a^3-27b^2$ is a square of an element in $Q(x_1)$. Since x_1 is of degree 3 and $D=-4a^3-27b^2\in Q$, K is of degree 3 if and only if $D=-4a^3-27b^2$ is a square of a rational number. If x^3+ax+b is not irreducible, the splitting field of x^3+ax+b can not be of degree 3. Thiscompletesthe proof of our assertion.

10. Let p be a prime number and let $F = J_p$, the field of integers mod p.
(a) Prove that there is an irreducible polynomial of degree 2 over F.
(b) Use this polynomial to construct a field with p^2 elements.
*(c) Prove that any two irreducible polynomials of degree 2 over F lead to isomorphic fields with p^2 elements.

227.10 (a) There are $(p-1)\cdot p\cdot p=(p-1)p^2$ polynomials of degree 2 over F. If $p(x)=ax^2+bx+c$ $(a\neq 0)$ is not irreducible, then $p(x)=a(x-\alpha)(x-\beta)$ for some α and β in F. There are at most $(p-1)[p\cdot p-p]$ reducible polynomials of degree 2 over F since $a(x-\alpha)(x-\beta)=a(x-\beta)(x-\alpha)$ if $\alpha=\beta$. This shows that there are at least $(p-1)p^2-(p-1)(p^2-p)=(p-1)p$ irreducible polynomials of degree 2 over F. Hence there is an irreducible polynomial $p(x)$ of degree 2 over F.
(b) $F[x]/(p(x))$ is a field with p^2 elements.
(c) In fact, we prove that any finite field of order p^2 is the splitting field of $x^{p^2}-x$ over F

and thus any two fields of order p^2 are isomorphic.

Let K be a field of order p^2. Consider $x^{p^2}-x$. By (168.18), if $a \in K$, then $a^{p^2}=a$. Hence every element of K is a root of $x^{p^2}-x$. $x^{p^2}-x$ has at most p^2 distinct roots in K by Lemma 5.3.2. Thus $x^{p^2}-x$ certainly splits in K. However, it can not split in any smaller field For, that field would have to have all the roots of $x^{p^2}-x$ and so would bave to have at least p^2 elements in K. Thus K is the splitting field of $x^{p^2}-x$ over F. This completes the proof. (Note : we suggest the reader prove this exercise by modefying the proof of (158.4.(c)).

11. If E is an extension of F and if $f(x) \in F[x]$ and if ϕ is an automorphism of E leaving every element of F fixed, prove that ϕ must take a root of $f(x)$ lying in E into a root of $f(x)$ in E.

228.11 Let $f(x)=a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_0$, a_n, a_{n-1}, $a_0 \in F$. If b is a root of f(x), then $a_n b^n + a_{n-1} b^{n-1} + \cdots\cdots + a_1 b + a_0 = 0$.

$0 = \phi(a_n b^n + a_{n-1} b^{n-1} + \cdots\cdots + a_1 b + a_0)$

$= a_n(\phi(b))^n + a_{n-1}(\phi(b))^{n-1} + \cdots\cdots + a_1 \phi(b) + a_0$

$\phi(b)$ is also a root of f(x).

12. Prove that $F(\sqrt[3]{2})$, where F is the field of rational numbers, has no automorphisms other than the identity automorphism.

228.12 If ϕ is an automorphism of $F(\sqrt[3]{2})$, then $\phi(\alpha)=\alpha$ for all α in F since $\phi(1)=1$. $(\phi(\sqrt[3]{2}))^3 = \phi((\sqrt[3]{2})^3) = \phi(2) = 2$. Since $\sqrt[3]{2}$ is the only root of x^3-2 in F, $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$. ϕ fixes $\sqrt[3]{2}$ and any element in F. Hence ϕ fixes every element of $F(\sqrt[3]{2})$.

13. Using the result of Problem 11, prove that if the complex number α is a root of the polynomial $p(x)$ having *real* coefficients then $\bar{\alpha}$, the

complex conjugate of α, is also a root of $p(x)$.

228.13 $\phi : a \longrightarrow \bar{a}$ is an automorphism of the field of complex numbers. By(228.11), if α is a root of P(x), then $\phi(\alpha)=\bar{\alpha}$ is alos a root of P(x).

14. Using the result of Problem 11, prove that if m is an integer which is not a perfect square and if $\alpha + \beta\sqrt{m}$ (α, β rational) is the root of a polynomial $p(x)$ having *rational coefficients*, then $\alpha - \beta\sqrt{m}$ is also a root of $p(x)$.

228.14 $\phi : a+b\sqrt{m} \longrightarrow a-b\sqrt{m}$ is an automorphism of $F(\sqrt{m})$, where F is the field of rational numbers. If $\alpha+\beta\sqrt{m}$ is a root of P(x), then $\phi(\alpha+\beta\sqrt{m}) = \alpha-\beta\sqrt{m}$ is also a root of P(x) by (228.11).

*15. If F is the field of real numbers, prove that if ϕ is an automorphism of F, then ϕ leaves every element of F fixed.

228.15 If $r>0$, then $\phi(r)=\phi(\sqrt{r}\sqrt{r}) = (\phi(\sqrt{r}))^2 \geq 0$. $\phi(r) \neq 0$. $\phi(r)>0$. If $a>b$, then $a-b>0$. $\phi(a)-\phi(b)=\phi(a-b)>0$ $\phi(a)>\phi(b)$.

For x in F, if $\phi(x) \neq x$, then $\phi(x)>x$ or $\phi(x)<x$. If $\phi(x)>x$, then there is a rational number m such that $\phi(x)>m>x$. Then $m=\phi(m)>\phi(x)$, a contradiction. Similarly, $\phi(x)<x$ is impossible. $\phi(x)=x$. ϕ leaves every element of F fixed.

16 (a) Find *all* real quaternions $t = a_0 + a_1 i + a_2 j + a_3 k$ satisfying $t^2 = -1$

*(b) For a t as in part (a) prove we can find a real quaternion s such that $sts^{-1} = i$.

228.16 (a) $t^2 = (a_0^2 - a_1^2 - a_2^2 - a_3^2) + 2a_0 a_1 i + 2a_0 a_2 j + 2a_0 a_3 k$. $a_0^2 - a_1^2 - a_2^2 - a_3^2 = -1$.

$2a_0a_1=2a_0a_2=2a_0a_3=0$. If $a_0\neq 0$, then $a_1=a_2=a_3=0$, $a_0^2=-1$, a contradiction . Hence $a_0=0$ and $a_1^2+a_2^2+a_3^2=1$. $\{a_1i+a_2j+a_3k \mid a_1^2+a_2^2+a_3^2=1\}$ is the set of solutions of $t^2=-1$.

(b)Let $s=t+i$. Suppose $t\neq -i$. Then $s\neq 0$.

$st\ (t+i)t=t^2+it=-1+it$

$is=i(t+i)=it-1=-1+it=st$.

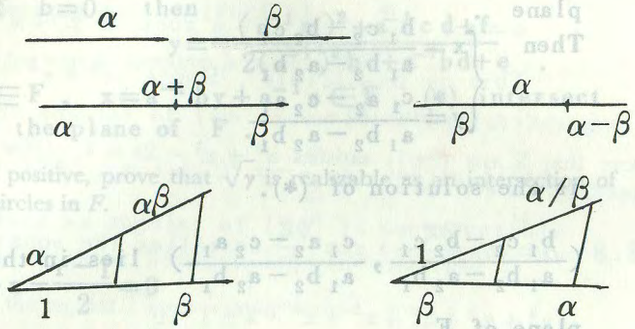
$sts^{-1}=i$.

For $t=-i$. Let $s=j$. $sts^{-1}=j(-i)j^{-1}$ $=k(-j)=i$.

5.4. Construction with Straighedge and Compass.

1. Prove that if α, β are constructible, then so are $\alpha \pm \beta$, $\alpha\beta$, and α/β (when $\beta \neq 0$).

231.1



2. Prove that a line in F has an equation of the form $ax + by + c = 0$ with a, b, c in F.

231.2 Let $(p,q),(r,s)$ be distinct points of the plane of F. The equation of the line through these two points is

$(s-q)(x-p)=(r-p)(y-q)$

$(s-q)x-(r-p)y-p(s-q)+q(r-p)=0$.

$s-q, -(r-p), -p(s-q)+q(r-p)\in F$.

3. Prove that a circle in F has an equation of the form

$$x^2 + y^2 + ax + by + c = 0,$$

with a, b, c in F.

231.3 Let (t,u) be a point of the plane of F. $w\in F$. The circle centre C , radiusw, is

$(x-t)^2+(y-u)^2=w^2$.

$x^2+y^2-2tx-2uy+(t^2+u^2-w^2)=0$,

$-2t$, $-2u$, $t^2+u^2-w^2\in F$.

4. Prove that two lines in F, which intersect in the real plane, intersect at a point in the plane of F.

231.4 Let

$$\begin{cases} a_1x+b_1y+c_1=0 \\ a_2x+b_2y+c_2=0 \end{cases} \quad \cdots\cdots\cdots(*)$$

be two lines in F, which intersect in the real plane .

Then $\begin{cases} x=\dfrac{b_1c_2-b_2c_1}{a_1b_2-a_2b_1} \\ y=\dfrac{c_1a_2-c_2a_1}{a_1b_2-a_2b_1} \end{cases}$

is the solution of (*).

$\left(\dfrac{b_1c_2-b_2c_1}{a_1b_2-a_2b_1}, \dfrac{c_1a_2-c_2a_1}{a_1b_2-a_2b_1}\right)$ lies in the plane of F .

5. Prove that a line in F and a circle in F which intersect in the real plane do so at a point either in the plane of F or in the plane of $F(\sqrt{\gamma})$ where γ is a positive number in F.

231.5 Let $\begin{cases} ax+by+c=0 \\ x^2+y^2+dx+ey+f=0 \end{cases} \quad \cdots\cdots\cdots(*)$

be the given line and circle , respeetively .

$a \neq 0$ or $b \neq 0$. Suppose $a \neq 0$.

$x=a^{-1}by+a^{-1}c$.

$(a^{-1}by+a^{-1}c)^2+y^2+d(a^{-1}by+a^{-1}c)+ey+f=0$

$(a^{-1}b)^2y^2+(2(a^{-1})bc+a^{-1}bd+e)y$

$+((a^{-1}c)+a^{-1}cd+f)=0$.

If $b \neq 0$, then

$$y=\frac{-(2(a^{-1})^2bc+a^{-1}bd+e)}{2(a^{-1}b)^2} \pm \frac{\sqrt{(2(a^{-1})bc+a^{-1}bd+e)^2-4(a^{-1}b)^2((a^{-1}c)^2+a^{-1}cd+f)}}{2(a^{-1}b)^2}$$

Let

$\gamma=(2(a^{-1})bc+a^{-1}bd+e)^2-4(a^{-1}b)^2((a^{-1}c)^2+a^{-1}cd+f)$.

$\gamma \geq 0$ since (*) has intersection in the real plane .

$y \in F(\sqrt{\gamma})$, $x=a^{-1}by+a^{-1}c \in F(\sqrt{\gamma})$.

(*) intersect in the plane of $F(\sqrt{\gamma})$.

If $b=0$, then

$$y=-\frac{(a^{-1}c)^2+a^{-1}cd+f}{2(a^{-1})^2bc+a^{-1}bd+e} .$$

$y \in F$, $x=a^{-1}by+a^{-1}c \in F$. (*) intersect in the plane of F .

6. If $\gamma \in F$ is positive, prove that $\sqrt{\gamma}$ is realizable as an intersection of lines and circles in F.

231.6

$$\begin{cases} x-\dfrac{r-1}{2}=0 \\ x^2+y^2-\left(\dfrac{1+r}{2}\right)^2=0 \end{cases}$$

have intersection $\left(\dfrac{r-1}{2}, \sqrt{r}\right)$ and

$\left(\dfrac{r-1}{2}, -\sqrt{r}\right)$.

7. Prove that the following polynomials are irreducible over the field of rational numbers.
   (a) $8x^3 - 6x - 1$.
   (b) $x^3 - 2$.
   (c) $x^3 + x^2 - 2x - 1$.

231.7 (a) If $8x^3-6x-1$ is not irreducible , then it has a linear factor $x-\dfrac{m}{n}$, where m and n are integers . By (161.4) $m=\pm 1$ and $n \mid 8$.

$\dfrac{m}{n}=\pm 1$, $\pm\dfrac{1}{2}$, $\pm\dfrac{1}{4}$ or $\pm\dfrac{1}{8}$ is a root of $8x^3-6x-1$. This is clearly impossible . Hence $8x^3-6x-1$ is irreducible .

(b) By Theorem 3.10.2 , (The Eisenstein Criterion) , x^3-2 is irreducible .

(c) If x^3+x^2-2x-1 is not irreducible, then it has a linear factor $x-\frac{m}{n}$, where m and n are integers. By (161.4), $m=\pm 1$ and $n=\pm 1$. $\frac{m}{n}=\pm 1$ is a root of x^3+x^2-2x-1. This is impossible. Hence x^3+x^2-2x-1 is irreducible.

8. Prove that $2\cos(2\pi/7)$ satisfies x^3+x^2-2x-1. (*Hint:* Use $2\cos(2\pi/7)=e^{2\pi i/7}+e^{-2\pi i/7}$.)

232.8 $\alpha=\cos\frac{2\pi}{7}+i\sin\frac{2\pi}{7}$ satisfies the equation

$$x^6+x^5+x^4+x^3+x^2+x+1=0$$

$$2\cos\frac{2\pi}{7}=\alpha+\alpha^{-1}$$

$$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+1=0 .$$

$$(\alpha^3+\frac{1}{\alpha^3})+(\alpha^2+\frac{1}{\alpha^2})+(\alpha+\frac{1}{\alpha})+1=0 .$$

$$\alpha^2+\frac{1}{\alpha^2}=(\alpha+\frac{1}{\alpha})^2-2 .$$

$$\alpha^3+\frac{1}{\alpha^3}=(\alpha+\frac{1}{\alpha})^3-3(\alpha+\frac{1}{\alpha}) .$$

Hence $[(\alpha+\frac{1}{\alpha})^3-3(\alpha+\frac{1}{\alpha})]+[(\alpha+\frac{1}{\alpha})^2-2]+(\alpha+\frac{1}{\alpha})+1=0 .$

$$(\alpha+\frac{1}{\alpha})^3+(\alpha+\frac{1}{\alpha})^2-2(\alpha+\frac{1}{\alpha})-1=0 .$$

$2\cos\frac{2\pi}{7}=\alpha+\alpha^{-1}$. satisfies x^3+x^2-2x-1.

9. Prove that the regular pentagon is constructible.

232.9 The angular of two sides of a regular pentagon is 108°.

$\cos 108^\circ=\frac{-\sqrt{5}+1}{4}$. $\sqrt{5}$ is constructible. $\cos 108^\circ$ is also constructible. The angular of 108° is thus constructible. The regular pentagon is constructible.

10. Prove that the regular hexagon is constructible.

232.10 The angular of two sides of a regular hexagon is 120°. $\cos 120^\circ=-\frac{1}{2}$ is contructible. Hence an angular of 120° is constructible. The regular hexagon is constructible.

11. Prove that the regular 15-gon is constructible.

232.11 $\cos 18^\circ=\frac{\sqrt{5}-1}{4}$ is constructible. The angular of 18° is constructible. The angular of $2\times 18^\circ=36^\circ$ is constructible. $\cos 60^\circ=\frac{1}{2}$. The angular of 60° is constructible. Hence the angular of $60^\circ-36^\circ=24^\circ$ is also constructible. Of course, the angular of $180^\circ-24^\circ=156^\circ$ is constructible. The angular of two sides of a regular 15 - gon is 156°. Thus the regular 15 - gon is constructible.

12. Prove that it is possible to trisect 72°.

232.12 As in the proof of (232.11), we know that the angular of 24° is constructible. $\frac{1}{3}(72^\circ)=24^\circ$. Hence, it is possible to trisect 72°.

13. Prove that a regular 9-gon is not constructible.

232.13 The angular of two sides of the regular 9 - gon

is $140°$. If a regular 9-gon is constructible, then the angular of $180° - 140° = 40°$ is constructible . Hence $2\cos 40°$ is constructible . Let $\alpha = \cos 40° + i \sin 40°$.

$2\cos 20° = \alpha + \alpha^{-1}$. α satisfies

$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$.

$\alpha^6 + \alpha^3 + 1 = 0$

$(\alpha^3 + \frac{1}{\alpha^3}) + 1 = 0$.

$(\alpha + \frac{1}{\alpha})^3 - 3(\alpha + \frac{1}{\alpha}) + 1 = 0$.

$2\cos 40°$ satisfies $x^3 - 3x + 1$.

$x^3 - 3x + 1$ is irreducible over the field of rational numbers . For , if $x^3 - 3x + 1$ is reducible , then it has a linear factor $x - \frac{m}{n}$, where m and n are integer . By (161.4)

$m = \pm 1$, $n = \pm 1$. $\frac{m}{n} = \pm 1$ is a root of $x^3 - 3x + 1$. This is impossible . Hence $x^3 - 3x + 1$ is irreducible . This contradicts with Corollary 2 to Theorem 5.4.1.

*14. Prove a regular 17-gon is constructible.

232.14 We want to show that $\cos\frac{2\pi}{17}$ is constructible and hence a regular 17-gon is constracuible .

Consider

$$\frac{t^{17} - 1}{t - 1} = t^{16} + \cdots\cdots + t + 1 \quad \cdots\cdots\cdots(1)$$

Let $\theta = \frac{2\pi}{17}$, $a_k = \cos k\theta + i \sin k\theta$

The zeros of (1) in the field of complex numbers are $a_1, \cdots\cdots, a_{16}$.

The powers of 3 reduced mod 17 are as follows:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^m	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

We define

$x_1 = a_1 + a_9 + a_{13} + a_{15} + a_{16} + a_8 + a_4 + a_2$

$x_2 = a_3 + a_{10} + a_5 + a_{11} + a_{14} + a_7 + a_{12} + a_6$

$y_1 = a_1 + a_{13} + a_{16} + a_4$

$y_2 = a_9 + a_{15} + a_8 + a_2$

$y_3 = a_3 + a_5 + a_{14} + a_{12}$

$y_4 = a_{10} + a_{11} + a_7 + a_6$

Now $a_k + a_{17-k} = 2\cos k\theta$ ·····(2)

for $k = 1, 2, \cdots\cdots, 16$, so that

$x_1 = 2(\cos\theta + \cos 8\theta + \cos 4\theta + \cos 2\theta)$ ···(3)

$x_2 = 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta)$

$y_1 = 2(\cos\theta + \cos 4\theta)$

$y_2 = 2(\cos 8\theta + \cos 2\theta)$

$y_3 = 2(\cos 3\theta + \cos 5\theta)$

$y_4 = 2(\cos 7\theta + \cos 6\theta)$

From (1) it follows that $x_1 + x_2 = -1$.

Using (3) and the equation $2\cos m\theta \cos n\theta = \cos(m+n)\theta + \cos(m-n)\theta$ we find that

$$\begin{aligned} x_1 x_2 = 2\{&\cos 4\theta + \cos 2\theta + \cos 8\theta + \cos 6\theta + \cos 4\theta \\ &+ \cos 6\theta + \cos 5\theta + \cos 7\theta + \cos 11\theta + \cos 5\theta \\ &+ \cos 15\theta + \cos\theta + \cos 13\theta + \cos 3\theta + \cos 14\theta \\ &+ \cos 2\theta + \cos 7\theta + \cos\theta + \cos 3\theta + \cos 11\theta \\ &+ \cos\theta + \cos 9\theta + \cos 2\theta + \cos 10\theta + \cos 5\theta \\ &+ \cos\theta + \cos 9\theta + \cos 5\theta + \cos 7\theta + \cos 3\theta \\ &+ \cos 4\theta + \cos 8\theta\} = -4 \end{aligned}$$

using (2). Hence x_1 and x_2 are zeros of the quadratic polynomial

$t^2 + t - 4$.·····(4)

Further, $x_1 > 0$ so that $x_1 > x_2$. By trigonometric expansions similar to that above , we find that

$$y_1 + y_2 = x_1$$
$$y_1 y_2 = -1$$

and y_1, y_2 are the zeros of

$$t^2 - x_1 t - 1 \cdots\cdots\cdots\cdots (5)$$

Further, $y_1 > y_2$. Similarly, y_3 and y_4 are zeros of

$$t^2 - x_2 t - 1 \cdots\cdots\cdots\cdots (6)$$

and $y_3 > y_4$.

Now $$2\cos\theta + 2\cos 4\theta = y_1$$
$$4\cos\theta\cos 4\theta = 2(\cos 5\theta + \cos 3\theta) = y_3$$

so that $z_1 = 2\cos\theta$, $z_2 = 2\cos 4\theta$ are zeros of $t^2 - y_1 t + y_3 \cdots\cdots\cdots\cdots (7)$ and $z_1 > z_2$.

Solving the series of quadratics (4), (5), (6) and (7) and using the inequalities to decide which zero is which we obtain the equation

$$\cos\theta = \frac{1}{16}\{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2(1 - \sqrt{17})\sqrt{34 - 2\sqrt{17}}}\}.$$

Hence $\cos\theta$ is constructible. This completes the proof.

5.5. More About Roots

1. If F is of characteristic 0 and $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = \alpha \in F$.

236.1 Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_0 \in F[x]$, $a_n, a_{n-1}, \cdots\cdots, a_0 \in F$.

$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots\cdots + a_1 = 0$.

$n a_n = (n-1) a_{n-1} = \cdots\cdots = a_1 = 0$.

Since F is of characteristic 0,

$a_n = a_{n-1} = \cdots\cdots = a_1 = 0$.

$f(x) = a_0 \in F$.

2. If F is of characteristic $p \neq 0$ and if $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$.

236.2 Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_0 \in F[x]$, $a_n, a_{n-1}, \cdots\cdots, a_0 \in F$.

$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots\cdots + a_1 = 0$.

$n a_n = (n-1) a_{n-1} = \cdots\cdots = a_1 = 0$.

$j a_j = 0$ for $j = 1, 2, \cdots\cdots, n$. If $p \nmid j$, then $a_j = 0$. Hence

$$f(x) = a_{pr} x^{pr} + a_{p(r-1)} x^{p(r-1)} + \cdots\cdots + a_p x^p + a_0$$
$$= a_{pr}(x^p)^r + a_{p(r-1)}(x^p)^{r-1} + \cdots + a_p(x^p) + a_0.$$

Let $g(x) = a_{pr} x^r + a_{p(r-1)} x^{r-1} + \cdots a_p x + a_0$.

Then $f(x) = g(x^p)$.

3. Prove that $(f(x) + g(x))' = f'(x) + g'(x)$ and that $(\alpha f(x))' = \alpha f'(x)$ for $f(x), g(x) \in F[x]$ and $\alpha \in F$.

236.3 Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_0$,

$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots\cdots + b_0$,

where $a_n, a_{n-1}, \cdots\cdots, a_0, b_n, b_{n-1}, \cdots\cdots, b_0 \in F$.

$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots\cdots + a_1$.

$g'(x) = n b_n x^{n-1} + (n-1) b_{n-1} x^{n-2} + \cdots\cdots + b_1$.

$f(x) + g(x) = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \cdots\cdots + (a_0 + b_0)$.

$\alpha f(x) = \alpha a_n x^n + \alpha a_{n-1} x^{n-1} + \cdots\cdots + \alpha a_0$.

$$(f(x)+g(x))' = n(a_n+b_n)x^{n-1} + (n-1)(a_{n-1}+b_{n-1})x^{n-2} + \cdots\cdots + (a_1+b_1)$$
$$= na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 + nb_nx^{n-1} + (n-1)b_{n-1}x^{n-2} + \cdots + b_1$$
$$= f'(x) + g'(x).$$
$$(\alpha f(x))' = n\alpha a_nx^{n-1} + (n-1)\alpha a_{n-1}x^{n-2} + \cdots + \alpha a_1$$
$$= \alpha(na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1)$$
$$= \alpha f(x).$$

4. Prove that there is no rational function in $F(x)$ such that its square is x.

236.4 Suppose there is a rational function $\frac{f(x)}{g(x)}$ in $F(x)$ such that $(\frac{f(x)}{g(x)})^2 = x$.

Furthermore, we may suppose $(f(x), g(x)) = 1$.

$f(x)f(x) = xg(x)g(x)$.

$2\deg f(x) = 1 + 2\deg g(x)$.

$2\deg f(x)$ is an even integer.

But $1 + 2\deg g(x)$ is an odd integer. Hence There is no rational function in $F(x)$ such that its square is x.

5. Complete the induction needed to establish the corollary to Theorem 5.5.1.

236.5 $F(\alpha_1, \cdots\cdots, \alpha_n) = (F(\alpha_1, \cdots\cdots, \alpha_{n-1}))(\alpha_n)$
$= (F(c_1))(\alpha_n) = F(c_1, \alpha_n) = F(c)$ for some c_1 in $F(\alpha_1, \cdots\cdots, \alpha_{n-1})$ by induction and c in $F(c_1, \alpha_n)$ by Theorem 5.5.1.

An element a in an extension K of F is called *separable over* F if it satisfies a polynomial over F having no multiple roots. An extension K of F is called *separable* over F if all its elements are separable over F. A field F is called *perfect* if all finite extensions of F are separable.

6. Show that any field of characteristic 0 is perfect.

236.6 Any finite extension K of F is also of characteristic 0.
For a in K, the minimal polynomial f(x) for a over F is irreducible over F. By corollary 1.1. to Lemma 5.5.2, f(x) has no multiple root. a is seperable over F. Hence K is seperable over F. F is perfect.

7. (a) If F is of characteristic $p \neq 0$ show that for $a, b \in F$, $(a+b)^{p^m} = a^{p^m} + b^{p^m}$.
(b) If F is of characteristic $p \neq 0$ and if K is an extension of F let $T = \{a \in K \mid a^{p^n} \in F \text{ for some } n\}$. Prove that T is a subfield of K.

236.7 (a) $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots\cdots + \binom{p}{p-1}ab^{p-1} + b^p$.

$p \mid \binom{p}{i}$ for $i = 1, 2, \cdots\cdots, p-1$.

$(a+b)^p = a^p + b^p$.

For $m > 1$, $(a+b)^{p^m} = ((a+b)^{p^{m-1}})^p$
$= (a^{p^{m-1}} + b^{p^{m-1}})^p$ (by induction)
$= (a^{p^{m-1}})^p + (b^{p^{m-1}})^p$
$= a^{p^m} + b^{p^m}$.

Hence $(a+b)^{p^m} = a^{p^m} + b^{p^m}$ for all $m = 0, 1, 2, \cdots\cdots$.

(b) Let $a, b \in T$. Then $a^{p^n}, b^{p^m} \in F$ for some m and n. $(a^{-1})^{p^n} = (a^{p^n})^{-1} \in F$.
$(-a)^{p^n} = (-1)^{p^n}a^{p^n} \in F$. Let $k = \max(m, n)$
$(a+b)^{p^k} = a^{p^k} + b^{p^k} \in F$.
$(ab)^{p^k} = a^{p^k}b^{p^k} \in F$. $a^{-1}, -a, a+b, ab \in T$.
T is a subfield of K.

8. If K, T, F are as in Problem 7(b) show that any automorphism of K

leaving every element of F fixed also leaves every element of T fixed.

236.8 For $a \in T$, $a^{p^n} \in F$ for some n. Let σ be the automorphism of K leaving every element of F fixed. $a^{p^n} = \sigma(a^{p^n}) = (\sigma(a))^{p^n}$.
$(\sigma(a) - a)^{p^n} = (\sigma(a))^{p^n} - a^{p^n} = 0$.
$\sigma(a) - a = 0$.
$\sigma(a) = a$.

*9. Show that a field F of characteristic $p \neq 0$ is perfect if and only if for every $a \in F$ we can find a $b \in F$ such that $b^p = a$.

236.9 An element a in an extension K of F is seperable if and only if the minimal p(x) for a over F has no multiple roots. For, if p(x) has no multiple roots, then a is seperable by definition. Conversely, if a satisfies a polynomial f(x) over F having no multiple roots, then p(x) has no multiple root since $p(x) \mid f(x)$.
Suppose that for every a in F we can find a b in F such that $b^p = a$. If K is a finite extension such that K is not seperable over F, then there is an element a in K which is not seperable over F. Let p(x) be the minimal polynomial for a over F.
p(x) has a multiple root by what we have proved in the first paragraph. By corollary 1, (2) to Lemma 5.5.2,

$$p(x) = \sum_{r=0}^{n} a_r x^{pr},$$

$a_r \in F$ for $r = 1, 2, \cdots\cdots, n$. $a_r = b_r^p$ for some b_r in F by our assumption.

$$p(x) = \sum_{r=0}^{n} b_r^p x^{pr} = \left(\sum_{r=0}^{n} b_r x^r\right)^p,$$

which contradicts the fact that p(x) is irreducible in $F[x]$. Thus F must be perfect.
Conversely, suppose that F is perfect. Let $a \in F$ and consider the polynomial $x^p - a \in F[x]$. If this polynomial has a root b in F then $a = b^p$. Suppose it has not root in F and let p(x) be one of its nonconstant monic irreducible factors in $F[x]$. Consider the extension F(b) where $p(b) = 0$. In $F(b)[x]$ we have $x^p - a = x^p - b^p = (x - b)^p$ and since p(x) divides this polynomial we have $p(x) = (x - b)^m$ for some m. If $m = 1$ then $x - b \in F[x]$ and so $b \in F$ which is not true. Hence $m > 1$. But b is not a simple root of p(x) and since p(x) is the minimal polynomial for b over F, F(b) is not seperable over F. This contradicts the fact that F is perfect. Therefore we must have a b in F such that $a = b^p$.

10. Using the result of Problem 9, prove that any finite field is perfect.

236.10 Let F be a finite field with characteristic p. $\sigma : F \to F$ defined as $\sigma(a) = a^p$ is a ring homomorphism of F into F.
σ is one-to-one. For, if $\sigma(a) = 0$, then $a^p = \sigma(a) = 0$ and so $a = 0$.
Hence σ is onto. For every a in F, we can find b in F such that $b^p = a$. F is perfect by (236.9).

**11. If K is an extension of F prove that the set of elements in K which are separable over F forms a subfield of K.

237.11 We suggest the student see McCarthy, P.J., Algebraic Extensions of Field, page 10 ~ 13. or Zariski, Oscar, and Samuel, Pierre, Commutative Algebra, Vol. 1. page 65 ~ 70.

12. If F is of characteristic $p \neq 0$ and if K is a finite extension of F, prove that given $a \in K$ either $a^{p^n} \in F$ for some n or we can find an integer m such that $a^{p^m} \notin F$ and is separable over F.

237.12 Suppose that $a^{p^m} \notin F$ implies a^{p^m} is not seperable over F . Let $p_1(x)$ be the minimal polynomial for a over F .Either $a \in F$ or a is not seperable . Suppose a is not seperable . By Corollary 1.(2) to Lemma 5.5.2. , $p_1(x) = g_1(x^p)$ for some $g_1(x)$ in $F[x]$. deg $p_1(x) >$ deg $g_1(x)$. a^p satisfies $g_1(x)$. Let $p_2(x)$ be the minimal polynomial for a^p over F . If $a^{p^2} \notin F$, then a^{p^2} is not seperable over F . By Corollary 1.(2) to Lemma 5.5.2. , $p_2(x) = g_2(x^p)$ for some $g_2(x)$ in $F[x]$. deg $g_1(x) \geq$ deg $p_2(x) >$ deg $g_2(x)$. a^{p^2} satisfies $g_2(x)$. Continuing this process , $a^{p^n} \in F$ for some n since deg $p_1(x)$ is a finite number .

13. If K and F are as in Problem 12, and if no element which is in K but not in F is separable over F, prove that given $a \in K$ we can find an integer n, depending on a, such that $a^{p^n} \in F$.

237.13 Since there is no integer m such that $a^{p^m} \notin F$ and a^{p^m} is seperable over F , so $a^{p^m} \in F$ for some integer n .

14. If K is a finite, separable extension of F prove that K is a simple extension of F.

237.14 If $K = F(a_1, a_2)$, then K is a simple extension of F by (237.15) .
$K = F(a_1, a_2, \cdots\cdots, a_n)$.
$F(a_1, \cdots\cdots, a_n) = (F(a_1, a_2, \cdots\cdots, a_{n-1}))(a_n)$.
$F(a_1, a_2, \cdots\cdots, a_{n-1})$ is seperable over F .
$F(a_1, \cdots\cdots, a_{n-1}) = F(c_1)$ by induction hypothesis .$K = (F(c_1))(a_n) = F(c_1, a_n) = F(c)$.
K is a simple extension of F .

15. If one of a or b is separable over F, prove that $F(a, b)$ is a simple extension of F.

237.15 Let $K = F(a, b)$. If F is finite , then K is finite and the multiplicative group of nonzero elements of K is cyclic by (49.38) and Lemma 5.3.2. Hence K is a simple extension of F . It follows that we may suppose that F is not finite . Suppose b is seperable . Let p(x) and q(x) be the minimal polynomial for a and b over F , respectively . We take a field in which f(x) and g(x) split over K . Let the distinct zeros of f(x) be $\alpha_1, \cdots\cdots, \alpha_r$ and let those of g(x) be $\beta_1, \cdots\cdots, \beta_s$, for example , $\alpha_1 = a$, $\beta_1 = b$. For $k \neq 1$, we have $\beta_k \neq \beta_1$ so that the equation $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ has at most one root x in F for every i and every $k \neq 1$. If we take c different from the roots of all these linear equations , we have $\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$ for every i and $k \neq 1$. We let $\theta = \alpha_1 + c\beta_1 = a + cb$. Then θ is an element of K . We assert that $F(\theta) = K$.
The element b satisfies the equations g(x) and $f(\theta - cx)$, whose coefficient in $F(\theta)$. The polynomials g(x) and $f(\theta - cx)$ have only the root b in common ; for we have the others β_k ($k \neq 1$) of the first equation $\theta - c\beta_k \neq \alpha_i$ ($i = 1, \cdots\cdots, r$), and so $f(\theta - c\beta_k) \neq 0$. β_1 is a simple root of g(x); therefore, g(x) and $f(\theta - cx)$ have but one linear factor $x - \beta_1$ in common . The coefficients of this greatest common divisor

must lie in $F(\theta)$ already ; thus $\beta_1 = b$ lies in $F(\theta)$. From $a = \theta - cb$, $a \in F(\theta)$. $F(a,b) = F(\theta)$. This completes the proof .

5.6. Elements of Galois Theory

1. If K is a field and S a set of automorphisms of K, prove that the fixed field of S and that of $\bar{S}$ (the subgroup of the group of all automorphisms of K generated by S) are identical.

249.1 Let K_S and $K_{\bar{S}}$ be the fixed field of S and $\bar{S}$, respectively . If $a \in K_{\bar{S}}$, then $\sigma(a) = a$ for σ in $\bar{S}$, in particular , $\sigma(a) = a$ for all σ in S . So $a \in K_S$. $K_{\bar{S}} \subset K_S$. On the other hand , if $a \in K_S$, then $\sigma(a) = a$ for all σ in S . If $p \in \bar{S}$, then $\rho = \sigma_1 \sigma_2 \cdots\cdots \sigma_n$, where $\sigma_i \in S$ or $\sigma_i^{-1} \in S$. $\rho(a) = \sigma_1 \sigma_2 \cdots\cdots \sigma_n(a)$ $= \sigma_1 \sigma_2 \cdots\cdots \sigma_{n-1}(a) = a$. $a \in K_{\bar{S}}$. Hence $K_S = K_{\bar{S}}$.

2. Prove Lemma 5.6.2.

249.2 σ , $\rho \in G(K,F)$. σ^{-1}, $\sigma\rho$ are also automorphisms of K . $\sigma(a) = a$ $\rho(a) = a$ for all a in F . $\sigma^{-1}(a) = a$. $\sigma\rho(a) = \sigma(\rho(a)) = \sigma(a) = a$. σ^{-1}, $\sigma\rho \in G(K,F)$. $G(K,F)$ is a subgroup of the group of all automorphisms of K .

3. Using the Eisenstein criterion, prove that $x^4 + x^3 + x^2 + x + 1$ is irreducible over the field of rational numbers.

249.3 c.f. (161.3) .

4. In Example 5.6.3, prove that each mapping σ_i defined is an automorphism of $F_0(\omega)$.

249.4 $\sigma_i(\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3) = \alpha_0 + \alpha_1\omega^i + \alpha_2(\omega^i)^2 + \alpha_3(\omega^i)^3$, $i = 1,2,3,4$.

$\sigma_i((\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3) + (\beta_0 + \beta_1\omega + \beta_2\omega^2 + \beta_3\omega^3))$
$= \sigma_i((\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)\omega + (\alpha_2 + \beta_2)\omega^2 + (\alpha_3 + \beta_3)\omega^3)$
$= (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)\omega^i + (\alpha_2 + \beta_2)(\omega^i)^2 + (\alpha_3 + \beta_3)(\omega^i)^3$

$$=(\alpha_0+\alpha_1\omega^i+\alpha_2(\omega^i)^2+\alpha_3(\omega^i)^3)$$
$$+(\beta_0+\beta_1\omega^i+\beta_2(\omega^i)^2+\beta_3(\omega^i)^3)$$
$$=\sigma_i(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)$$
$$+\sigma_i(\beta_0+\beta_1\omega+\beta_2\omega^2+\beta_3\omega^3).$$
$$(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)(\beta_0+\beta_1\omega+\beta_2\omega^2+\beta_3\omega^3)$$
$$=(\alpha_0\beta_0-\alpha_1\beta_3-\alpha_2\beta_2+\alpha_2\beta_3-\alpha_3\beta_1+\alpha_3\beta_2)$$
$$+(\alpha_0\beta_1+\alpha_1\beta_0-\alpha_1\beta_3-\alpha_2\beta_2-\alpha_3\beta_1+\alpha_3\beta_3)\omega$$
$$+(\alpha_0\beta_2+\alpha_1\beta_2-\alpha_1\beta_3+\alpha_2\beta_0-\alpha_2\beta_2-\alpha_3\beta_1)\omega^2$$
$$+(\alpha_0\beta_3-\alpha_1\beta_3+\alpha_2\beta_1-\alpha_2\beta_2+\alpha_3\beta_0-\alpha_3\beta_1)\omega^3$$

By a computation, we have

$$\sigma_i((\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)(\beta_0+\beta_1\omega+\beta_2\omega^2+\beta_3\omega^3))$$
$$=\sigma_i(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)\sigma_i(\beta_0+\beta_1\omega+\beta_2\omega^2+\beta_3\omega^3)$$

5. In Example 5.6.3, prove that the fixed field of $F_0(\omega)$ under σ_1, σ_2, σ_3, σ_4 is precisely F_0.

249.5 Suppose $\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$ is fixed by $\sigma_1,\sigma_2,\sigma_3$ and σ_4.

$$\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$$
$$=\sigma_2(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)$$
$$=\alpha_0+\alpha_1\omega^2+\alpha_2\omega^4+\alpha_3\omega^6$$
$$=(-\alpha_2+\alpha_0)+(\alpha_3-\alpha_2)\omega+(\alpha_1-\alpha_2)\omega^2-\alpha_2\omega^3,$$
$$\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$$
$$=\sigma_3(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)$$
$$=\alpha_0+\alpha_1\omega^3+\alpha_2\omega^6+\alpha_3\omega^9$$
$$=(-\alpha_3+\alpha_0)+(\alpha_2-\alpha_3)\omega+(-\alpha_3)\omega^2+(\alpha_1-\alpha_3)\omega^3.$$

$$\begin{cases}\alpha_0=-\alpha_2+\alpha_0=-\alpha_3+\alpha_0\\ \alpha_1=\alpha_3-\alpha_2=\alpha_2-\alpha_3\\ \alpha_2=\alpha_1-\alpha_2=-\alpha_3\\ \alpha_3=-\alpha_2=\alpha_1-\alpha_3\end{cases}.$$

$\alpha_2=\alpha_3=0$, $\alpha_1=0$. Hence $\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3=\alpha_0$. $\sigma_i(\alpha_0)=\alpha_0$.

The fixed field of $F_0(\omega)$ under $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ is precisely F_0.

6. Prove directly that any automorphism of K must leave every rational number fixed.

249.6 The characteristic of K is 0. Let σ be an automorphism of K. $\sigma(1)=1$. $\sigma(n)=n$ for all positive integers.

$\sigma(-n)=-\sigma(n)=-n$. Hence $\sigma(m)=m$ for all integers.

$\sigma(\frac{m}{n})=\sigma(m)(\sigma(n))^{-1}=m(n^{-1})=\frac{m}{n}$. Hence

$\sigma(r)=r$ for all rational numbers.

*7. Prove that a symmetric polynomial in $x_1,\ldots,x_n$ is a polynomial in the elementary symmetric functions in $x_1,\ldots,x_n$.

249.7 We first prove

Lemma. If $b_0,b_1,\cdots\cdots,b_{n-1}$ are symmetric polynomials in $x_1,\cdots\cdots,x_n$ and

$b_0x_1^{n-1}+b_1x_1^{n-2}+\cdots\cdots+b_{n-1}=0$,

then $b_0=b_1=\cdots\cdots=b_{n-1}=0$.

pf. Consider the polynomial

$g(x)=b_0X^{n-1}+b_1X^{n-2}+\cdots\cdots+b_{n-1}$

in $F(x_1,x_2,\cdots\cdots,x_n)$. The polynomial g(X) has n roots in $F(x_1,x_2,\cdots\cdots,x_n)$. By Lemma 5.3.2, $b_0=b_1=\cdots\cdots=b_{n-1}=0$.

This completes the proof of the Lemma.

We are now prepared to prove this exercise by induction. Let $g_1(x_1,\cdots\cdots,x_n)$ be a symmetric polynomial with coefficients in F. We may cosider g as a polynomial in x_1 with coefficients in $F[x_2,\cdots\cdots,x_n]$. Clearly, the coefficients are symmetric polynomials in $x_2,x_3,\cdots\cdots,x_n$. Denote the elementary symmetric functions in $x_2,\cdots\cdots,x_n$ by $a_1',a_2',\cdots\cdots,a_{n-1}'$ we have by induction

$g(x_1,\cdots\cdots,x_n)=g_1(x_1,a_1',a_2',\cdots\cdots,a_{n-1}')$ ……(*).

The identities $a_1=x_1+a_1'$, $a_i=x_1a_{i-1}'+a_i'$ $(i=2,\cdots\cdots,n-1)$ permit us to eliminate $a_1',\cdots\cdots,a_{n-1}'$ from the right side of (*) and we obtain.

$g(x_1,\cdots\cdots,x_n)=g_2(x_1,a_1,\cdots\cdots,a_{n-1})$ ……(**).

By means of the identity

$x_1^n-a_1x_1^{n-1}+a_2x_1^{n-2}+\cdots\cdots+(-1)^na_n=0$,

we can reduce the right side of (**) to a polynomial of degree at most $n-1$ in x_1.

Thus we finally get:

$g_3(x_1,a_1,\cdots\cdots,a_n)-g(x_1,\cdots\cdots,x_n)=0$,

where g_3 is a polynomial in x_1 of degree at most $n-1$.

Consider g_3 as a polynomial in x_1 with coefficients in $F[a_1,a_2,\cdots\cdots,a_n]$.

It follows from the Lemma that

$g_3(0,a_1,\cdots\cdots,a_n)=g(x_1,\cdots\cdots,x_n)$,

since $g_3(0,a_1,\cdots\cdots,a_n)-g(x_1,\cdots\cdots,x_n)$ is the constant term of

$g_3(x_1,a_1,\cdots\cdots,a_n)-g(x_1,\cdots\cdots,x_n)$.

8. Express the following as polynomials in the elementary symmetric functions in x_1, x_2, x_3:
(a) $x_1^2+x_2^2+x_3^2$.
(b) $x_1^3+x_2^3+x_3^3$.
(c) $(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$.

249.8 (a) $x_1^2+x_2^2+x_3^2=(x_1+x_2+x_3)^2-2(x_1x_2+x_2x_3+x_3x_1)$.

(b) $x_1^3+x_2^3+x_3^3=(x_1+x_2+x_3)^3$
$-3(x_1+x_2+x_3)(x_1x_2+x_2x_3+x_3x_1)+3x_1x_2x_3$.

(c) $(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$
$=(x_1+x_2+x_3)^2(x_1x_2+x_2x_3+x_3x_1)^2+$
$18(x_1+x_2+x_3)(x_1x_2+x_2x_3+x_3x_1)(x_1x_2x_3)$
$-4(x_1x_2+x_2x_3+x_3x_1)^3-27(x_1x_2x_3)^2$
$-4(x_1+x_2+x_3)^3(x_1x_2x_3)$.

9. If $\alpha_1, \alpha_2, \alpha_3$ are the roots of the cubic polynomial x^3+7x^2-8x+3, find the cubic polynomial whose roots are
(a) $\alpha_1^2, \alpha_2^2, \alpha_3^2$. (b) $\frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \frac{1}{\alpha_3}$. (c) $\alpha_1^3, \alpha_2^3, \alpha_3^3$.

249.9 (a) $x^3-65x^2+22x-9$
(b) $3x^3-8x^2+7x+1$
(c) $x^3+520x^2+19x+27$

*10. Prove *Newton's identities*, namely, if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of $f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n$ and if $s_k=\alpha_1^k+\alpha_2^k+\cdots+\alpha_n^k$ then
(a) $s_k+a_1s_{k-1}+a_2s_{k-2}+\cdots+a_{k-1}s_1+ka_k=0$ if $k=1,2,\ldots,n$.
(b) $s_k+a_1s_{k-1}+\cdots+a_ns_{k-n}=0$ for $k>n$.
(c) For $n=5$, apply part (a) to determine s_2, s_3, s_4, and s_5.

249.10 (a) $f'(x)=\frac{f(x)}{x-\alpha_1}+\frac{f(x)}{x-\alpha_2}+\cdots\cdots+\frac{f(x)}{x-\alpha_n}$
$=nx^{n-1}+(n-1)a_1x^{n-2}+\cdots\cdots+2a_{n-2}x+a_{n-1}$

$\frac{f(x)}{x-\alpha}=x^{n-1}+(\alpha+a_1)x^{n-2}+(\alpha^2+a_1\alpha+a_2)x^{n-3}$
$+(\alpha^3+a_1\alpha^2+a_2\alpha+a_3)x^{n-4}+\cdots\cdots+$
$(\alpha^{n-1}+a_1\alpha^{n-2}+a_2\alpha^{n-3}+\cdots\cdots+a_{n-2}\alpha+a_{n-1})$.

In this equation we replace α by each of the quantities $\alpha_1,\cdots\cdots,\alpha_n$ in succession, and put $s_p=\alpha_1^p+\cdots\cdots+\alpha_n^p$, we have, by adding all these results, the following value for $f'(x)$; — $f'(x)=nx^{n-1}+(s_1+na_1)x^{n-2}$
$+(s_2+a_1s_1+na_2)x^{n-3}+(s_3+a_1s_2+a_2s_1+na_3)x^{n-4}$
$+\cdots+(s_{n-1}+a_1s_{n-2}+a_2s_{n-3}+\cdots+a_{n-2}s_1+na_{n-1})$;
whence, comparing this value of $f'(x)$ with the former, we obtain the following relations;

$$\begin{aligned}
&s_1+a_1=0\\
&s_2+a_1s_1+2a_2=0\\
&s_3+a_1s_2+a_2s_1+3a_3=0 \quad\cdots\cdots\cdots(*)\\
&s_4+a_1s_3+a_2s_2+a_3s_3+4a_4=0\\
&\cdots\cdots\\
&s_{n-1}+a_1s_{n-2}+a_2s_{n-3}+\cdots+a_{n-2}s_1+(n-1)a_{n-1}=0.
\end{aligned}$$

(b) $\alpha_i^n+a_1\alpha_i^{n-1}+a_2\alpha_i^{n-2}+\cdots\cdots+a_n=0$. Multipling

this equation by α_1^{k-n} we have

$\alpha_1^k+a_1\alpha_1^{k-1}+a_2\alpha_1^{k-2}+\cdots\cdots+a_n\alpha_1^{k-n}=0$.

Adding these equations , we have

$s_k+a_1 s_{k-1}+a_2 s_{k-2}+\cdots\cdots+a_n s_{k-n}=0$.

(c) Solving (*) , we have $s_1=-a_1$

$s_2=a_1^2-2a_2$

$s_3=-a_1^3+3a_1a_2-3a_3$

$s_4=a_1^4-4a_1^2a_2+4a_1a_3-4a_4+2a_2^2$

$s_5=-a_1^5+5a_1^3a_2+5a_1a_4-5a_3a_1^2-5a_1a_2^2+5a_2a_3-5a_5$

11. Prove that the elementary symmetric functions in $x_1,\ldots,x_n$ are indeed symmetric functions in $x_1,\ldots,x_n$.

249.11 $a_k=\sum_{i_1 i_2\cdots i_k} x_{i_1}x_{i_2}\cdots\cdots x_{i_k}$.

For any σ in S_n , $x_{\sigma(i_1)}x_{\sigma(i_2)}\cdots\cdots x_{\sigma(i_k)}$ is also a term of a_k . Hence a_k is a symmetric funetion in $x_1,x_2,\cdots\cdots,x_n$.

12. If $p(x)=x^n-1$ prove that the Galois group of $p(x)$ over the field of rational, numbers is abelian.

249.12 Let $\xi=e^{\frac{2\pi i}{n}}$; note that $\xi^n=1$ but $\xi^m\neq 1$ for $0<m<n$. $1,\xi^1,\cdots\cdots,\xi^{n-1}$ are all the roots of x^n-1 . Thus $F(\xi)$ is the splitting field of x^n-1 . If σ , τ are any two elements in the Galois group of x^n-1 , that is , if σ and τ are automorphisms of $F(\xi)$ leaving every element of F fixed , then since both $\sigma(\xi)$ and $\tau(\xi)$ are roots of x^n-1 , $\sigma(\xi)=\xi^i$ and $\tau(\xi)=\xi^j$.

$(\sigma\tau)(\xi)=\sigma(\xi^j)=(\sigma(\xi))^j=(\xi^i)^j=\xi^{ij}$.

$(\tau\sigma)(\xi)=\tau(\xi^i)=(\tau(\xi))^i=(\xi^j)^i=\xi^{ij}$.

$\sigma\tau$ and $\tau\sigma$ agree on ξ and on F hence all of $F(\xi)$. But then $\sigma\tau=\tau\sigma$ whence the Galois group is abelian .

The complex number ω is a *primitive nth root of unity* if $\omega^n=1$ but $\omega^m\neq 1$ for $0<m<n$. F_0 will denote the field of rational numbers.

13. (a) Prove that there are $\phi(n)$ primitive nth roots of unity where $\phi(n)$ is the Euler ϕ-function.
(b) If ω is a primitive nth root of unity prove that $F_0(\omega)$ is the splitting field of x^n-1 over F_0 (and so is a normal extension of F_0).
(c) If $\omega_1,\ldots,\omega_{\phi(n)}$ are the $\varphi(n)$ primitive nth roots of unity, prove that any automorphism of $F_0(\omega_1)$ takes ω_1 into some ω_i.
(d) Prove that $[F_0(\omega_1):F_0]\leq\phi(n)$.

250.13 (a) Let $\xi=e^{\frac{2\pi i}{n}}$; note that $\xi^n=1$ but $\xi^m\neq 1$ for $0<m<n$. $1,\xi^1,\cdots\cdots,\xi^{n-1}$ are all the roots of x^n-1 . ξ^k is also a primitive n th roots of unity if $(n,k)=1$. Hence there are $\phi(n)$ primitive nth roots of unity .

(b) If w is a primitive nth root of unity , then $w=\xi^k$ for some integer k , $(n,k)=1$. $\{1,w,w^2,\cdots\cdots,w^{n-1}\}=\{1,\xi^1,\xi^2,\cdots\cdots,\xi^{n-1}\}$. $F(w)$ contains all roots of x^n-1 . w is a root of x^n-1 . Hence $F(w)$ is the splitting field of x^n-1 over F_0 .

(c) Let σ be an automorphism of $F_0(w_1)$. $(\sigma(w_1))^n=1$ and $(\sigma(w_1))^m\neq 1$ for $0<m<n$. For , if $(\sigma(w_1)^m=1$ for $0<m<n$, then $\sigma(w_1^m)=1$ and $w_1^m=1$, contrary to the fact that w_1 is a primitive nth root of unity . Hence $\sigma(w_1)=w_i$ for some $i=1,2,\cdots\cdots,\phi(n)$.

(d) $[F_0(w_1):F_0]=o(G(F_0(w_1),F_0))$ by Theorem 5.6.4. $G(F(w_1),F_0)$ is equal to the group of all automorphisms of $F_0(w_1)$. By (250.13.(c)) . $[F_0(w_1):F_0]<\phi(n)$.

14. The notation is as in Problem 13.

*(a) Prove that there is an automorphism σ_i of $F_0(\omega_1)$ which takes ω_1 into ω_i.

(b) Prove the polynomial $p_n(x) = (x - \omega_1)(x - \omega_2)\cdots(x - \omega_{\phi(n)})$ has rational coefficients. (The polynomial $p_n(x)$ is called the *nth cyclotomic polynomial.*)

*(c) Prove that, in fact, the coefficients of $p_n(x)$ are integers.

**15. Use the results of Problems 13 and 14 to prove that $p_n(x)$ is irreducible over F_0 for all $n \geq 1$. (See Problem 8, Section 3.)

250.14 We suggest the reader see

250.15 McCarty , P.J. Algebraic Extensions of Fields. page 39 ~ 42 . or Serge Lang . Algebra . page 203 ~ 206 .

16. For $n = 3, 4, 6$, and 8, calculate $p_n(x)$ explicitly, show that it has integer coefficients and prove directly that it is irreducible over F_0.

250.16 $p_3(x)=x^2+x+1$. $p_4(x)=x^2+1$. $p_6(x)=x^2-x+1$. $p_8(x)=x^4+1$.

17. (a) Prove that the Galois group of $x^3 - 2$ over F_0 is isomorphic to S_3, the symmetric group of degree 3.

(b) Find the splitting field, K, of $x^3 - 2$ over F_0.

(c) For every subgroup H of S_3 find K_H and check the correspondence given in Theorem 5.6.6.

(d) Find a normal extension in K of degree 2 over F_0.

250.17 Let K be the splitting field of $f(x)=x^3-2$ over F_0 . We may consider K as a subfield of the field of complex numbers . To obtain K we first adjoin $\sqrt[3]{2}$ (real) to F_0 . In $F_0(\sqrt[3]{2})[x]$ we have

$$f(x)=(x-\sqrt[3]{2})[x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2]$$
$$=(x-\sqrt[3]{2})\,g(x) .$$

The field $F_0(\sqrt[3]{2})$ is a subfield of the field of real numbers and $g(x)$ has no real roots , so that $g(x)$ is irreducible in $F_0(\sqrt[3]{2})[x]$. The roots of $g(x)$ are $\sqrt[3]{2}\,\alpha$ and $\sqrt[3]{2}\,\beta$

where $\alpha=\dfrac{-1+\sqrt{3}i}{2}$ and $\beta=\dfrac{-1-\sqrt{3}i}{2}$.

Hence $K=F_0(\sqrt[3]{2}, \sqrt{3}i)$.

We have $[K:F_0]=6$ and, since K is a normal extension of F_0 , the order of $G(K,F_0)$ is 6 . Thus , if we can find six distinct automorphism of K they will constitute all of $G(K,F_0)$; one element of this group is its identity element 1 .

An element of $G(K,F_0)$ is completely determined by what it does to $\sqrt[3]{2}$ and $\sqrt{3}i$.

Let σ be the automorphism of K which leaves $\sqrt[3]{2}$ fixed and maps $\sqrt{3}i$ to $-\sqrt{3}i$.

Let τ be the automorphism of K which maps $\sqrt[3]{2}$ to $\sqrt[3]{2}\,\alpha$ and $\sqrt{3}i$ to $-\sqrt{3}i$. We have the following table which gives the images of $\sqrt[3]{2}$ and $\sqrt{3}i$ under the indicated automorphisms of K .

	1	σ	τ	$\sigma\tau$	$\tau\sigma$	$\sigma\tau\sigma$	
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}\alpha$	$\sqrt[3]{2}\beta$	$\sqrt[3]{2}\alpha$	$\sqrt[3]{2}\beta$	
$\sqrt{3}i$	$\sqrt{3}i$	$-\sqrt{3}i$	$-\sqrt{3}i$	$\sqrt{3}i$	$\sqrt{3}i$	$-\sqrt{3}i$	

Thus $G(K,F_0)=\{1,\sigma,\tau,\sigma\tau,\tau\sigma,\sigma\tau\sigma\}$.

The subgroups of $G(K,F_0)$ are

$H_1=\{1,\sigma\}$, $H_2=\{1,\tau\}$, $H_3=\{1,\sigma\tau\sigma\}$, $H_4=\{1,\sigma\tau,\tau\sigma\}$.

The fixed fields of these subgroups are , respectively ,

$L_1=F_0(\sqrt[3]{2})$, $L_2=F_0(\sqrt[3]{2}\beta)$, $L_3=F_0(\sqrt[3]{2}\alpha)$, $L_4=F_0(\sqrt{3}i)$.

$G(K,F_0)$ is of order 6 and not cyclic so that $G(K,F_0)$ is isomorphic to S_3 by (65.11) .

L_4 is normal over F_0 .

18. If the field F contains a primitive nth root of unity, prove that the Galois group of $x^n - a$, for $a \in F$, is abelian.

250.18 Since F contain all nth roots of unity , it contains $\xi = e^{\frac{2\pi i}{n}}$ note that $\xi^n = 1$ but $\xi^m \neq 1$ for $0 < m < n$.

If $u \in K$ is any root of $x^n - a$, then $u, \xi u, \xi^2 u, \cdots\cdots, \xi^{n-1} u$ are all the roots of $x^n - a$. F(u) is the splitting field of $x^n - a$ over F . If σ , τ are any two elements in the Galois group of $x^n - a$, that is , if σ , τ are automorphisms of F(u) leaving every element of F fixed , then since both $\sigma(u)$ and $\tau(u)$ are roots of $x^n - a$, $\sigma(u) = \xi^i u$ and $\tau(u) = \xi^j u$ for some i and j . Thus $\sigma\tau(u) = \sigma(\xi^j u) = \xi^j \sigma(u) = \xi^j \xi^i u = \xi^{i+j} u$; similarly , $\tau\sigma(u) = \xi^{i+j} u$. Therefore , $\sigma\tau$ and $\tau\sigma$ agree on u and on F herce all of F(u) . But then $\sigma\tau = \tau\sigma$ whence the Galois group is abelian .

5.7. Solvability by Radicals

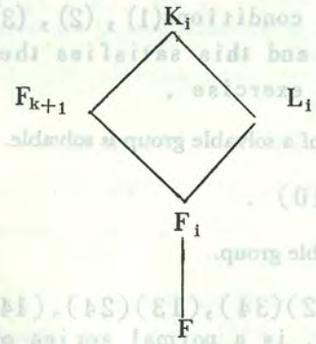
*1. If $p(x)$ is solvable by radicals over F, prove that we can find a sequence of fields

$$F \subset F_1 = F(\omega_1) \subset F_2 = F_1(\omega_2) \subset \cdots \subset F_k = F_{k-1}(\omega_k),$$

where $\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1, \ldots, \omega_k^{r_k} \in F_{k-1}$, F_k containing all the roots of $p(x)$, such that F_k is *normal* over F.

256.1 We call the sequence of fields $F = F_1 \subset F_2 = F_1(\omega_1) \subset F_3 = F_2(\omega_2) \subset \cdots \subset F_{k+1} = F_k(\omega_k)$ a root tower for F_{k+1} over F if $\omega_i^{n_i} \in F_i$ for $i = 1, 2, \cdots\cdots, k$.

Suppose that we are given $F = F_1 \subset F_2 = F_1(\omega_1) \subset \cdots\cdots \subset F_{k+1} = F_k(\omega_k)$ with $\omega_i^{n_i} = \alpha_i \in F_i$. We shall show that there exists a field $K_i \supset F_{k+1}$ which also contains a subfield L_i such that (1) $L_i \supset F_i$, (2) L_i is normal over F (3) L_i has a root tower over F :



Now for $i = 1$ we take $K_1 = F_{k+1}$, $L_1 = F_1 = F$ and we suppose we are given K_i and L_i for a certain i . Let $\sigma_1 = 1, \sigma_2, \cdots\cdots, \sigma_{k_i}$ be the elements of $G(L_i, F)$. Set

$$g_i(x) = \prod_{j=1}^{k_i} (x^{n_i} - \sigma_j(\alpha_i)) .$$

Then $g_i(x) \in F[x]$ since L_i is normal over F .

Let K_{i+1} be the splitting field of $g_i(x)$ over K_i and let $\omega_i, \omega_i', \omega_i'', \cdots\cdots$ be the roots of $g_i(x)$ in K_{i+1}. Note that one of these is ω_i such that $F_{i+1} = F_i(\omega_i)$ since $g_i(\omega_i) = 0$ and $K_{i+1} \supset K_i \supset F_{k+1}$. Set $L_{i+1} = L_i(\omega_i, \omega_i', \omega_i'', \cdots\cdots)$. Since L_i is a splitting field of a polynomial $f_i(x) \in F[x]$ (Theorem 5.6.5), L_{i+1} is a splitting field of $f_i(x)\, g_i(x)$ over F, L_{i+1} is normal over F. Since $L_{i+1} \supset L_i$ and $\omega_i \in L_i$, $L_{i+1} \supset F_{i+1} = F_i(\omega_i)$. Let $\omega_i^{(h)}$ be any one of the elements $\omega_i, \omega_i', \omega_i'', \cdots\cdots$; then $g_i(\omega_i^{(h)}) = 0$ and

$$g_i(x) = \prod_{j=1}^{k_i} (x^{n_i} - \sigma_j(\alpha_i))$$

show that $(\omega_i^{(h)})^{n_i}$ is one of the $\sigma_j(\alpha_i)$. Hence $L_{i+1} = L_i(\omega_i, \omega_i', \omega_i'', \cdots\cdots)$ has a root tower over F. This shows that K_{i+1} and L_{i+1} satisfies the conditions(1), (2), (3). We now tabe $K = L_{k+1}$ and this satisfies the conditions stated in the exercise.

2. Prove that a subgroup of a solvable group is solvable.

256.2 See (116.10).

3. Prove that S_4 is a solvable group.

256.3 $(1) \subset \{1, (12)(34), (13)(24), (14)(23)\} = K \subset A_4 \subset S_4$ is a normal series of S_4. K, A_4/K, S_4/A_4 are abelian. Hence S_4 is solvable.

4. If G is a group, prove that all $G^{(k)}$ are normal subgroups of G.

256.4 See (117.13.(a)).

5. If N is a normal subgroup of G prove that N' must also be a normal subgroup of G.

256.5 N' is a normal subgroup of G'. G' is a characteristic subgroup of G. Hence N' is a normal subgroup of G.

6. Prove that the alternating group (the group of even permutations in S_n) A_n has no nontrivial normal subgroups for $n \geq 5$.

256.6 See (81.17).

5.8. Galois Groups over the Rationals

1. In S_5 show that (1 2) and (1 2 3 4 5) generate S_5.

259.1 See (81.11) .

2. In S_5 show that (1 2) and (1 3 2 4 5) generate S_5.

259.2 $(13245)^2=(12534)$. (12) and (12534) generate S_5 .

3. If $p > 2$ is a prime, show that (1 2) and $(1\,2\cdots p-1\,p)$ generate S_p.

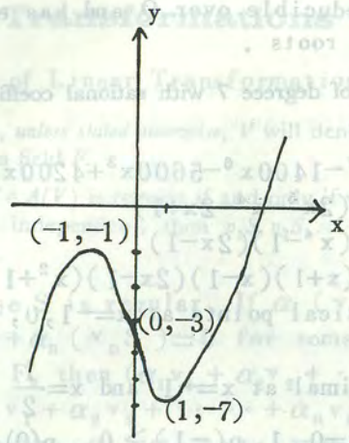
259.3 See (81.11) .

4. Prove that any transposition and p-cycle in S_p, p a prime, generate S_p.

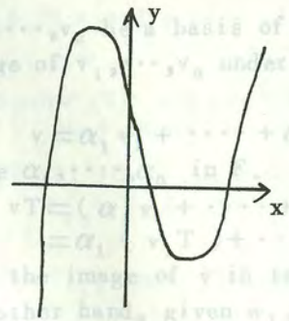
259.4 Without loss of generality , we may suppose that the transposition is (1 i) and the p - cycle is (12 ····· p) .
$(12\cdots\cdots p)^i=(1i\cdots\cdots)$ is also a p - cycle .
(1 i) and (1 i ·····) generate Sp .

5 Show that the following polynomials over Q are irreducible and have exactly two nonreal roots.
(a) $p(x) = x^3 - 3x - 3$,
(b) $p(x) = x^5 - 6x + 3$,
(c) $p(x) = x^5 + 5x^4 + 10x^3 + 10x^2 - x - 2$.

259.5 (a) By Theorem 3.10.2 (The Eisenstein Criterion), x^3-3x-3 is irreducible over Q.
$p'(x)=3x^2-3$.
p (x) has a maximum at $x=-1$ and a minimum at $x=1$. As the graph clearly indicates , p(x) cross the x - axis exactly one times , so p(x) has exactly 1 root which is real .



(b) By Theorem 3.10.2 (The Eisensten Criterion), $p(x)= x^5-6x+3$ is irreducible over Q .
$p'(x)=5x^4-6$.
p(x) has a maximal at $x=-\sqrt[4]{\frac{6}{5}}$ and a minimal at $x=\sqrt[4]{\frac{6}{5}}$. $p(-\sqrt[4]{\frac{6}{5}})>0$, $p(\sqrt[4]{\frac{6}{5}})<0$. Hence p(x) cross the x - axis exactly three times , so p(x) has exactly two nonreal roots .



(c) $p(x)=(x+1)^6-6(x+1)+3$. By (259.5.(b)),

$p(x)$ is irreducible over Q and has exactly two nonreal roots .

7. Construct a polynomial of degreee 7 with rational coefficients whose Galois group over Q is S_7.

259.7 $p(x)=2400x^7-1400x^6-5600x^3+4200x^2-84$.

$p'(x)=8400x(2x^5-x^4-2x+1)$

$=8400x(x^4-1)(2x-1)$

$=8400x(x+1)(x-1)(2x-1)(x^2+1)$.

$p(x)$ has critical points at $x=-1, 0, \frac{1}{2}$ and 1 .

$p(x)$ has maximal at $x=-1$ and $x=\frac{1}{2}$ and has minimal at $x=0, 1$. $p(-1)>0$, $p(0)<0$, $p(\frac{1}{2})>0$, $p(1)<0$.

$p(x)$ crooss the x-axis exactly 5 times , so $p(x)$ has exactly 5 roots which are real . $p(x)$ has exactly two nonreal roots . By Theorem 3.10.2 (The Eisenstein Criterion), $p(x)$ is irreducible over Q . By Theorem 5.8.1, the Galois group of $p(x)$ over Q is S_7 .

6 Linear Transformations

6.1. Algebra of Linear Transformations

In all problems, *unless stated otherwise*, V will denote a finite-dimensional vector space over a field F.

1. Prove that $S \in A(V)$ is regular if and only if whenever $v_1, \ldots, v_n \in V$ are linearly independent, then $v_1S, v_2S, \ldots, v_nS$ are also linearly independent.

267.1 Suppose S is regular. If $\alpha_1(v_1S)+\alpha_2(v_2S)+\cdots\cdots+\alpha_n(v_nS)=0$ for some $\alpha_1, \alpha_2, \cdots\cdots, \alpha_n$ in F, then $(\alpha_1v_1+\alpha_2v_2+\cdots\cdots+\alpha_nv_n)S=0$. $\alpha_1v_1+\alpha_2v_2+\cdots\cdots+\alpha_nv_n=0$ since S is one-to-one. $\alpha_1=\alpha_2=\cdots\cdots=\alpha_n=0$ since $v_1, v_2, \cdots\cdots, v_n$ are linearly independent.

Conversely, suppose that whenever $v_1, \cdots, v_n \in V$ are linearly independent, then $v_1S, v_2S, \cdots v_nS$ are also linearly independent. If S is singular, then there is a $v \neq 0$ in V such that $vS=0$ by Theorem 6.1.3. v is itself linearly independent and 0 is not linearly independent. This contradicts with our assumption. Hence S is regular.

2. Prove that $T \in A(V)$ is completely determined by its values on a basis of V.

267.2 Let $v_1, \cdots, v_n$ be a basis of V over F. If we know the image of $v_1, \cdots, v_n$ under T, then for every v in V,

$$v=\alpha_1v_1+\cdots\cdots+\alpha_nv_n$$

for some $\alpha_1, \cdots, \alpha_n$ in F.

$$vT=(\alpha_1v_1+\cdots\cdots+\alpha_nv_n)T$$
$$=\alpha_1(v_1T)+\cdots\cdots+\alpha_n(v_nT).$$

We have the image of v in terms of $v_1T, \cdots, v_nT$. On the other hand, given $w_1, \cdots\cdots, w_n$ in V. Let $(\alpha_1v_1+\cdots\cdots+\alpha_nv_n)S=\alpha_1w_1+\cdots\cdots+\alpha_nw_n$.

S is a linear transformation on V over F and $v_1S = w_1, \cdots, v_nS = w_n$.
This shows that $T \in A(w)$ is completely determined by its values on a basis of V.

3. Prove Lemma 6.1.1 even when A does not have a unit element.

267.3 Let $W = \{(\alpha, a) \mid \alpha \in F, a \in A\}$. Define an addition on W as $(\alpha, a) + (\beta, b) = (\alpha+\beta, a+b)$.
W is an abelian group under this definition. Define
$$\alpha \cdot (\beta, b) = (\alpha\beta, \alpha b) \text{ for } \alpha \in F.$$
W is a vector space over F. Define a product on W as
$$(\alpha, a) \cdot (\beta, b) = (\alpha\beta, \alpha b + \beta a + ab).$$
W is an algebra over F with identity $(1, 0)$.
A can be embedded into W by $a \longrightarrow (0, a)$. By Lemma 6.1.1, W is isomorphic to a subalgebra of $A(V)$ for some vector space V over F.
Hence A is isomorphic to a subalgebra of $A(V)$.

4. If A is the field of complex numbers and F is the field of real numbers, then A is an algebra over F of dimension 2. For $a = \alpha + \beta i$ in A, compute the action of T_a (see Lemma 6.1.1) on a basis of A over F.

267.4 A satisfies all the given axioms. Thus A is an algebra over F. 1, i is a basis of A over F.
$1Ta = a$. $iTa = ia$.

5. If V is two-dimensional over F and $A = A(V)$, write down a basis of A over F and compute T_a for each a in this basis.

267.5 Let v_1, v_2 be a basis of V. Define $T_1 : V \longrightarrow V$ as
$$(\alpha_1 v_1 + \alpha_2 v_2) T_1 = \alpha_1 v_1,$$
$T_2 : V \longrightarrow V$ as
$$(\alpha_1 v_1 + \alpha_2 v_2) T_2 = \alpha_1 v_2,$$
$T_3 : V \longrightarrow V$ as
$$(\alpha_1 v_1 + \alpha_2 v_2) T_3 = \alpha_2 v_1,$$

$T_4 : V \longrightarrow V$ as
$$(\alpha_1 v_1 + \alpha_2 v_2) T_4 = \alpha_2 v_2.$$
T_1, T_2, T_3, T_4 form a basis of V.
For $a \in A(V)$, let $(\alpha_1 v_1 + \alpha_2 v_2) a = (\alpha_1\beta_{11} + \alpha_2\beta_{21}) v_1 + (\alpha_1\beta_{12} + \alpha_2\beta_{22}) v_2$.
$(\alpha_1 v_1 + \alpha_2 v_2)(T_1) Ta = \alpha_1\beta_{11} v_1 + \alpha_1\beta_{12} v_2$.
$(\alpha_1 v_1 + \alpha_2 v_2)(T_2)(Ta) = \alpha_1\beta_{21} v_1 + \alpha_1\beta_{22} v_2$.
$(\alpha_1 v_1 + \alpha_2 v_2)(T_3)(Ta) = \alpha_2\beta_{11} v_1 + \alpha_2\beta_{12} v_2$.
$(\alpha_1 v_1 + \alpha_2 v_2)(T_4)(Ta) = \alpha_2\beta_{21} v_1 + \alpha_2\beta_{22} v_2$.

6. If $\dim_F V > 1$ prove that $A(V)$ is not commutative.

267.6 Let $v_1, \cdots, v_n$ be a basis of V over F. Define $T_1 : V \longrightarrow V$ as
$$(\alpha_1 v_1 + \cdots + \alpha_n v_n) T_1 = \alpha_1 v_1.$$
Define $T_2 : V \longrightarrow V$ as
$$(\alpha_1 v_1 + \cdots + \alpha_n v_n) T_2 = \alpha_1 v_2$$
Then $v_1(T_1T_2) = (v_1T_1)T_2 = v_1T_2 = v_2$ but
$v_1(T_2T_1) = (v_1T_2)T_1 = v_2T_1 = 0$.
$T_1T_2 \neq T_2T_1$. $A(V)$ is not commutative.

7. In $A(V)$ let $Z = \{T \in A(V) \mid ST = TS \text{ for all } S \in A(V)\}$. Prove that Z merely consists of the multiples of the unit element of $A(V)$ by the elements of F.

267.7 Let $v_1, v_2, \cdots, v_n$ be a basis of V over F. Let $T \in Z$. Define
$E_{ij} : V \longrightarrow V$ as
$$(\alpha_1 v_1 + \cdots + \alpha_n v_n) E_{ij} = \alpha_i v_j.$$
$E_{ij} \in A(V)$.
Suppose $v_i T = \beta_{i1} v_1 + \beta_{i2} v_2 + \cdots + \beta_{in} v_n$.
$v_i(TE_{ij}) = (v_iT) E_{ij} = (\beta_{i1} v_1 + \beta_{i2} v_2 + \cdots + \beta_{in} v_n) E_{ij} = \beta_{ii} v_j = v_i(E_{ij}T) = (v_iE_{ij})T = v_jT = \beta_{j1} v_1 + \cdots + \beta_{jn} v_n$. $\cdots$ (*)
for all $i, j = 1, 2, \cdots, n$.
By (*) $\beta_{ji} = 0$ if $i \neq j$ and $\beta_{ii} = \beta_{jj}$ for all i,j.

Hence $v_i T = \beta_{11} v_i$. $T = \beta_{11} I$. This completes the proof.

*8. If $\dim_F (V) > 1$ prove that $A(V)$ has no two-sided ideals other than (0) and $A(V)$.

268.8 Let $v_1, \cdots, v_n$ be a basis of V. Define E_{ij} as in (268.7). Suppose R is a nonzero two-sided ideal of A(V). Let T be a nonzero element in R. $v_i T \neq 0$ for some v_i, otherwise $T = 0$. Let $v_i T = \alpha_{i1} v_1 + \alpha_{i2} v_2 + \cdots\cdots + \alpha_{ij} v_j + \cdots\cdots + \alpha_{in} v_n$. $\alpha_{ij} \neq 0$ for some α_{ij}, otherwise $v_i T = 0$. Claim

$$\alpha_{ij} I = E_{1i} T E_{j1} + E_{2i} T E_{j2} + \cdots\cdots + E_{ni} T E_{jn}.$$

For, $v_l (E_{1i} T E_{j1} + E_{2i} T E_{j2} + \cdots\cdots + E_{ni} T E_{jn})$

$= v_l E_{1i} T E_{j1} + v_l E_{2i} T E_{j2} + \cdots\cdots + v_l E_{ni} T E_{jn}$

$= v_l E_{li} T E_{jl}$

$= v_i T E_{jl}$

$= (\alpha_{i1} v_1 + \alpha_{i2} v_2 + \cdots\cdots + \alpha_{in} v_n) E_{jl}$

$= \alpha_{ij} v_l$

for all $l = 1, 2, \cdots, n$.

$\alpha_{ij} I \in R$, $I = (\alpha^{-1}{}_{ij} I)(\alpha_{ij} I) \in R$.

$R = A(V)$. This completes the proof.

**9. Prove that the conclusion of Problem 8 is false if V is not finite-dimensional over F.

268.9 Let V be a vector space and not finite-dimensional over F. Define

$$R = \{ T \in A(V) \mid \dim VT < \infty \}.$$

If $S, T \in R$, then

$$V(S+T) = VS + VT.$$

$\dim V(S+T) \leq \dim VS + \dim VT < \infty$,

$S + T \in R$.

$\dim V(-S) = \dim VS < \infty$,

$-S \in R$.

If $T' \in A(V)$, then

$\dim V(ST') \leq \dim VS < \infty$,

and $\dim V(T'S) \leq \dim VS < \infty$.

ST' and $T'S \in R$.

R is a two-sided ideal of A(V). $R \neq A(V)$ since $1 \in A(V) \setminus R$. $R \neq (0)$, for, let $\{v_\alpha\}$ be a basis of V, define $T : v_\alpha \to v_\alpha$ and $T : v_\beta \to 0$ if $\alpha \neq \beta$. Then $\dim VT = 1 < \infty$, $T \in R \setminus (0)$. This shows that the conclusion of Problem 8 is false if V is not finite-dimension over F. Note that, when we say that $\{v_\alpha\}$ is a basis of V, we have not shown that in an infinite-dimensional vector space, it has also a basis. In fact, we can prove it by Zorn's Lemma. We don't prove this here.

10. If V is an arbitrary vector space over F and if $T \in A(V)$ is both right- and left-invertible, prove that the right inverse and left inverse must be equal. From this, prove that the inverse of T is unique.

268.10 Suppose $AT = TB = 1$.

$A = A \cdot 1 = A(TB) = (AT)B = 1 \cdot B = B$.

The right and left inverse of T are equal. Hence the inverse of T is unique.

11. If V is an arbitrary vector space over F and if $T \in A(V)$ is right-invertible with a *unique* right inverse, prove that T is invertible.

268.11 Let B be the uniqul right inverse of T. $TB = 1$

$T(BT + B - 1) = (TB)T + TB - T = 1 \cdot T + 1 - T = 1$.

$BT + B - 1 = B$ since B is the unique right inverse of T.

$BT - 1 = 0$, $BT = 1$, $TB = BT = 1$. T is invertible.

12. Prove that the regular elements in $A(V)$ form a group.

268.12 If T is regular, then there is an S in A(V) such that $TS = ST = 1$, $T^{-1} = S$ is also regular

by definition.

If A is also regular, and $AB = BA = 1$, then

$(AT)(SB) = A(TS)B = A \cdot 1 \cdot B = AB = 1$,

$(SB)(AT) = S(BA)T = S \cdot 1 \cdot T = ST = 1$

AT is regular. Hence the regular elements of $A(V)$ form a group.

13. If F is the field of integers modulo 2 and if V is two-dimensional over F, compute the group of regular elements in $A(V)$ and prove that this group is isomorphic to S_3, the symmetric group of degree 3.

*14. If F is a finite field with q elements, compute the order of the group of regular elements in $A(V)$ where V is two-dimensional over F.

*15. Do Problem 14 if V is assumed to be n-dimensional over F.

268.13, 268.14, 268.15

$(q^n-1)(q^n-q)(q^n-q^2)\cdots\cdots(q^n-q^{n-1})$.

Let $v_1, v_2, \cdots\cdots, v_n$ be a basis of V. For a regular element T of $A(V)$, v_1T must be nonzero.

v_1T has (q^n-1) choices.

v_2T and v_1T are linearly independent. v_2T has (q^n-q) choices.

That is $v_2T \neq \alpha v_1T$ for all α in F. v_3T, v_1T, v_2T are linearly independent. $v_3T \neq \alpha v_1T + \beta v_2T$ for all α, β in F. v_3T has (q^n-q^2) choices.

Continuing this process. There are $(q^n-1)(q^n-q)\cdots\cdots(q^n-q^{n-1})$ elements of regular elements in $A(V)$. The order of the group of regular elements in $A(V)$ is $(q^n-1)(q^n-q)\cdots\cdots(q^n-q^{n-1})$.

*16. If V is finite-dimensional, prove that every element in $A(V)$ can be written as a sum of regular elements.

268.16 Let E_{ij} be defined as in (267.7). Since $\{E_{ij}\}$ forms a basis of $A(V)$, we need only show that E_{ij} is a sum of regular elements.

$E_{ij} = (E_{ij}+I)+(-I)$ for $i \neq j$.

For given i, chose $j \neq i$.

$$E_{ii} = [(E_{ii}+E_{ij}+E_{ji}) + \sum_{k\neq i,j} E_{kk}] + [-E_{ij} - E_{ji} - \sum_{k\neq i,j} E_{kk}].$$

$(E_{ij}+I)(-E_{ij}+I) = I$, $(-I)(-I) = I$,

$$[(E_{ii}+E_{ij}+E_{ji}+\sum_{k\neq i,j} E_{kk})][E_{ij}+E_{ji}-E_{jj}+\sum_{k\neq i,j} E_{kk}]$$

$= I$,

$$[(-E_{ij}-E_{ji}-\sum_{k\neq i,j} E_{kk})][(-E_{ij}-E_{ji}-\sum_{k\neq i,j} E_{kk})] = I.$$

This completes the proof.

17. An element $E \in A(V)$ is called an *idempotent* if $E^2 = E$. If $E \in A(V)$ is an idempotent, prove that $V = V_0 \oplus V_1$ where $v_0E = 0$ for all $v_0 \in V_0$ and $v_1E = v_1$ for all $v_1 \in V_1$.

268.17 $vE = vE^2 = (vE)E$, $vE \in V_1$ for all v in V.

$(v-vE)E = vE - vE^2 = vE - vE = 0$, $v - vE \in V_0$ for all v in V. $v - vE = v' \in V_0$.

$v = v' + vE \in V_0 + V_1$. $V = V_0 + V_1$.

Consider $V_0 \cap V_1$. Let $v \in V_0 \cap V_1$.

$v = vE$ (since $v \in V_1$)

$= 0$ (since $v \in V_0$).

$V_0 \cap V_1 = (0)$. $V = V_0 \oplus V_1$.

18. If $T \in A_F(V)$, F of characteristic not 2, satisfies $T^3 = T$, prove that $V = V_0 \oplus V_1 \oplus V_2$ where
(a) $v_0 \in V_0$ implies $v_0T = 0$.
(b) $v_1 \in V_1$ implies $v_1T = v_1$.
(c) $v_2 \in V_2$ implies $v_2T = -v_2$.

268.18 For v in V, $v = (v - vT^2) + (\frac{1}{2}vT + \frac{1}{2}vT^2) + (-\frac{1}{2}vT + \frac{1}{2}vT^2)$.

$(v - vT^2)T = vT - vT^3 = vT - vT = 0$, $v - vT^2 \in V_0$.

$(\frac{1}{2}vT + \frac{1}{2}vT^2)T = \frac{1}{2}vT^2 + \frac{1}{2}vT^3 = \frac{1}{2}vT^2 + \frac{1}{2}$

$vT = \frac{1}{2}vT + \frac{1}{2}vT^2 \in V_1$.

$(-\frac{1}{2}vT + \frac{1}{2}vT^2)T = -\frac{1}{2}vT^2 + \frac{1}{2}vT^3 = -(-\frac{1}{2}vT + \frac{1}{2}vT^2)$, $-\frac{1}{2}vT + \frac{1}{2}vT^2 \in V_2$.

Hence $V = V_0 + V_1 + V_2$. Suppose $v_0 + v_1 + v_2 = 0$, $v_0 \in V_0, v_1, \in V_1$, $v_2 \in V_2$. $0 = (v_0 + v_1 + v_2)T = v_0T + v_1T + v_2T = v_1 - v_2$.

$0 = (v_1 - v_2)T = v_1T - v_2T = v_1 + v_2$.

$v_0 = 0$. $v_1 = 0$. $v_2 = 0$.

$V = V_0 \oplus V_1 \oplus V_2$.

*19. If V is finite-dimensional and $T \neq 0 \in A(V)$, prove that there an $S \in A(V)$ such that $E = TS \neq 0$ is an idempotent.

268.19 Let V_0 be the kernel of T and $\{v_1, \cdots\cdots, v_k\}$ be a basis of V_0 and $\{v_1, \cdots\cdots, v_k, v_{k+1}, \cdots, v_n\}$ be a basis of V. $n > k$ since $T \neq 0$. $v_{k+1}T, \cdots\cdots v_nT$ are linearly independent. For, if $\alpha_{k+1}(v_{k+1}T) + \cdots\cdots + \alpha_n(v_nT) = 0$ for some $\alpha_{k+1}, \cdots\cdots, \alpha_n$ in F, then $(\alpha_{k+1}v_{k+1} + \cdots\cdots + \alpha_n v_n)T = 0$

$\alpha_{k+1}v_{k+1} + \cdots\cdots + \alpha_n v_n \in V_0$. $\alpha_{k+1}v_{k+1} + \cdots\cdots + \alpha_n v_n = \alpha_1 v_1 + \cdots\cdots + \alpha_k v_k$ for some $\alpha_1, \cdots\cdots, \alpha_k$ in F since $v_1, \cdots\cdots, v_k$ is a basis of V_0. $(-\alpha_1)v_1 + (-\alpha_2)v_2 + \cdots\cdots + (-\alpha_k)v_k + \alpha_{k+1}v_{k+1} + \cdots\cdots + \alpha_n v_n = 0$.

$-\alpha_1 = -\alpha_2 = \cdots\cdots = -\alpha_k = \alpha_{k+1} = \cdots\cdots = \alpha_n = 0$ since $v_1, \cdots v_n$ are linearly independent. Let $\{v_{k+1}T, \cdots\cdots, v_nT, w_1, \cdots\cdots, w_k\}$ be a basis of V over F. Define $S : V \to V$ as

$(v_{k+1}T)S = v_{k+1}, \cdots\cdots, (v_nT)S = v_n$,

$w_1S = w_2S = \cdots\cdots = w_kS = 0$.

By (267.2), we can define S such that $S \in A(V)$.

$v_{k+1}(TS) = (v_{k+1}T)S = v_{k+1} \neq 0$, $TS \neq 0$.

$(TS)^2 = TS$. For $v_1(TS)^2 = v_1TSTS = 0, \cdots\cdots, v_k(TS)^2 = v_kTSTS = 0$.

$v_{k+1}(TS)^2 = (v_{k+1}TS)(TS) = v_{k+1}(TS), \cdots\cdots, v_n(TS)^2 = (v_nTS)(TS) = v_n(TS)$.

$v_i(TS)^2 = v_i(TS)$ for $i = 1, 2 \cdots\cdots, n$.

$(TS)^2 = TS$ by (267.2). This completes the proof.

20. The element $T \in A(V)$ is called *nilpotent* if $T^m = 0$ for some m. If T is *nilpotent* and if $vT = \alpha v$ for some $v \neq 0$ in V, with $\alpha \in F$, prove that $\alpha = 0$.

268.20 T is nilpotent. $T^m = 0$ for some m. $vT = \alpha v$. $vT^2 = (\alpha v)T = \alpha(vT) = \alpha^2 v, \cdots\cdots, vT^m = \alpha^m v = 0$. $v \neq 0$ implies $\alpha^m = 0$ and $\alpha = 0$.

21. If $T \in A(V)$ is nilpotent, prove that $\alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_k T^k$ is regular, provided that $\alpha_0 \neq 0$.

268.21 If $A, B \in A(V)$, A, B are nilpotent and $AB = BA$, then $A + B$ is nilpotent. For, if $A^m = 0$ and $B^n = 0$, then $(A+B)^{m+n+1} = 0$. By induction, $S = \alpha_1 T + \alpha_2 T^2 + \cdots\cdots + \alpha_k T^k$ is nilpotent. Suppose $S^r = 0$. Let $N = \alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots\cdots + \alpha_k T^k = \alpha_0 + S$. $S = N - \alpha_0$. $(N - \alpha_0)^r = 0$. ${\alpha_0}^r = Nf(N)$, where f(x) is a polynomial over F. $\alpha_0 \neq 0$, ${\alpha_0}^r \neq 0$. $1 = N({\alpha_0}^{-r} f(N))$. $N = \alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots\cdots + \alpha_k T^k$ is regular.

22. If A is a finite-dimensional algebra over F and if $a \in A$, prove that for some integer $k > 0$ and some polynomial $p(x) \in F[x]$, $a^k = a^{k+1}p(a)$.

268.22 Let $\alpha_k x^k + \alpha_{k+1}x^{k+1} + \cdots + \alpha_n x^n$ be a minimal polynomial for a over F with $\alpha_k \neq 0$. $\alpha_k a^k = -(\alpha_{k+1}a^{k+1} + \cdots\cdots + \alpha_n a^n)$.

$a^k = a^{k+1}[-\alpha_k^{-1}(\alpha_{k+1}a^0 + \cdots + \alpha_n a^{n-k-1})]$.

23. Using the result of Problem 22, prove that for $a \in A$ there is a polynomial $q(x) \in F[x]$ such that $a^k = a^{2k}q(a)$.

268.23 $a^k = a^{k+1}\,p(a) = (ap(a))\,a^k = (ap(a))\,(a^{k+1}p(a)) = a^{k+2}(p(a))^2 = \cdots\cdots = a^{2k}(p(a))^k$.

24. Using the result of Problem 23, prove that given $a \in A$ either a is nilpotent or there is an element $b \neq 0$ in A of the form $b = ah(a)$, where $h(x) \in F[x]$, such that $b^2 = b$.

269.24 $a^k = a^{2k}q(a)$. If a is not nilpotent, then $b = a^k q(a) \neq 0$. Otherwise $a^k = a^{2k}q(a) = a^k(a^k q(a)) = 0$. $b^2 = a^{2k}(q(a))^2 = (a^{2k}q(a))(q(a)) = a^k q(a) = b$.

25. If A is an algebra over F (not necessarily finite-dimensional) and if for $a \in A$, $a^2 - a$ is nilpotent, prove that either a is nilpotent or there is an element b of the form $b = ah(a) \neq 0$, where $h(x) \in F[x]$, such that $b^2 = b$.

269.25 Since $a^2 - a$ is nilpotent, $(a^2 - a)^n = 0$ for some n and a satisfies a polynomial as in the proof of (268.22). By (268.22), (268.23), (268.24), we get the conclusion.

*26. If $T \neq 0 \in A(V)$ is singular, prove that there is an element $S \in A(V)$ such that $TS = 0$ but $ST \neq 0$.

269.26 $VT \neq (0)$. Let $\{v_1T, v_2T, \cdots\cdots v_mT\}$ be a basis of VT. There are vectors $u_{m+1}, \cdots, u_n$ such that $v_1T, \cdots, v_mT, u_{m+1}, \cdots, u_n$ be a basis of V by Lemma 4.2.5. Since T is singular, $n > m > 0$ by Theorem. 6.1.4. By 267.2, we can find an S in A(V) such that
$(v_1T)S = (v_2T)S = \cdots = (v_mT)S = u_{m+1}S = \cdots = u_{n-1}S = 0$ and $u_nS = v_1$.
Then $u_n(ST) = (u_nS)T = v_1T \neq 0$ and $v \in V$,
$vT \in VT$, $vT = \sum_{i=1}^{m} \alpha_i (v_iT)$,

$$v(TS) = (vT)S = \left(\sum_{i=1}^{m} \alpha_i (v_iT)\right)S$$
$$= \sum_{i=1}^{m} \alpha_i (v_iT)S = 0.$$
Thus $TS = 0$ but $ST \neq 0$.

27. Let V be two-dimensional over F with basis v_1, v_2. Suppose that $T \in A(V)$ is such that $v_1T = \alpha v_1 + \beta v_2$, $v_2T = \gamma v_1 + \delta v_2$, where $\alpha, \beta, \gamma, \delta \in F$. Find a nonzero polynomial in $F[x]$ of degree 2 satisfied by T.

269.27 $x^2 - (\alpha + \delta)x + (\alpha\delta - \beta\gamma)$ is satisfied by T.
For
$$v_1T^2 = (v_1T)T = (\alpha v_1 + \beta v_2)T$$
$$= \alpha(\alpha v_1 + \beta v_2) + \beta(\gamma v_1 + \delta v_2)$$
$$= (\alpha^2 + \beta\gamma)v_1 + (\alpha\beta + \beta\delta)v_2.$$
$$v_1[T^2 - (\alpha + \delta)T + (\alpha\delta - \beta\gamma)I)$$
$$= v_1T^2 - (\alpha + \delta)v_1T + (\alpha\delta - \beta\gamma)v_1$$
$$= [(\alpha^2 + \beta\gamma)v_1 + (\alpha\beta + \beta\delta)v_2] - (\alpha + \delta)(\alpha v_1 + \beta v_2) + (\alpha\delta - \beta\gamma)v_1$$
$$= 0$$
Similarly, $v_2(T^2 - (\alpha + \delta)T + (\alpha\delta - \beta\gamma)I) = 0$.
Thus T satisfies, $x^2 - (\alpha + \delta)x + (\alpha\delta - \beta\gamma)$.

28. If V is three-dimensional over F with basis v_1, v_2, v_3 and if $T \in A(V)$ is such that $v_iT = \alpha_{i1}v_1 + \alpha_{i2}v_2 + \alpha_{i3}v_3$ for $i = 1, 2, 3$, with all $\alpha_{ij} \in F$, find a polynomial of degree 3 in $F[x]$ satisfied by T.

269.28 $x^3 - (\alpha_{11} + \alpha_{22} + \alpha_{33})x^2 + (\alpha_{11}\alpha_{22} + \alpha_{22}\alpha_{33} + \alpha_{33}\alpha_{11} - \alpha_{31}\alpha_{13} - \alpha_{32}\alpha_{23} - \alpha_{12}\alpha_{21})x - (\alpha_{11}\alpha_{22}\alpha_{33} + \alpha_{21}\alpha_{32}\alpha_{13} + \alpha_{12}\alpha_{23}\alpha_{31} - \alpha_{31}\alpha_{22}\alpha_{13} - \alpha_{21}\alpha_{12}\alpha_{33} - \alpha_{11}\alpha_{23}\alpha_{32})$ is satisfied by T. As the proof in (269, 27), we can prove this fact.

29. Let V be n-dimensional over F with a basis $v_1, \ldots, v_n$. Suppose that $T \in A(V)$ is such that
$$v_1T = v_2, v_2T = v_3, \ldots, v_{n-1}T = v_n,$$
$$v_nT = -\alpha_n v_1 - \alpha_{n-1}v_2 - \cdots - \alpha_1 v_n,$$
where $\alpha_1, \ldots, \alpha_n \in F$. Prove that T satisfies the polynomial

$p(x) = x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + \alpha_n$ over F.

269.29 $v_1 T^n = v_2 T^{n-1} = v_3 T^{n-2} = \cdots\cdots = v_n T = -\alpha_n v_1 - \alpha_{n-2} v_2 - \cdots - \alpha_1 v_n = -\alpha_n v_1 - \alpha_{n-2} v_1 T - \cdots - \alpha_1 v_1 T^{n-1}$.

$v_1 (T^n + \alpha_1 T^{n-1} + \alpha_2 T^{n-2} + \cdots + \alpha_n) = 0$.

$v_1 p(T) = 0$. $v_2 p(T) = v_1 T p(T) = v_1 p(T)\, T = 0$

.....

$v_n p(T) = v_1 T^{n-1} p(T) = v_1 p(T)\, T^{n-1} = 0$.

For v in V,

$$v = \sum_{i=1}^{m} a_i v_i .$$

$$v\, p(T) = \Big(\sum_{i=1}^{n} a_i v_i \Big) p(T)$$

$$= \sum_{i=1}^{n} a_i (v_i p(T))$$

$$= 0 .$$

$p(T) = 0$. T satisfies $p(x)$.

30. If $T \in A(V)$ satisfies a polynomial $q(x) \in F[x]$, prove that for $S \in A(V)$, S regular, STS^{-1} also satisfies $q(x)$.

269.30 Let $q(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots\cdots + \alpha_0$.

$\alpha_n T^n + \alpha_{n-1} T^{n-1} + \cdots + \alpha_0 I = 0$

$S (\alpha_n T^n + \alpha_{n-1} T^{n-1} + \cdots + \alpha_0 I) S^{-1} = 0$

$\alpha_n S T^n S^{-1} + \alpha_{n-1} S T^{n-1} S^{-1} + \cdots + \alpha_0 S I S^{-1} = 0$.

$\alpha_n (STS^{-1})^n + \alpha_{n-1} (STS^{-1})^{n-1} + \cdots + \alpha_0 I = 0$.

Thus STS^{-1} also satisfies $q(x)$.

31. (a) If F is the field of rational numbers and if V is three-dimensional over F with a basis v_1, v_2, v_3, compute the rank of $T \in A(V)$ defined by

$$v_1 T = v_1 - v_2,$$
$$v_2 T = v_1 + v_3,$$
$$v_3 T = v_2 + v_3.$$

(b) Find a vector $v \in V$, $v \neq 0$, such that $vT = 0$.

269.31 (a) Since $v_1 - v_2$ and $v_1 + v_3$ are linearly independent

and $v_2 + v_3 = -(v_1 - v_2) + (v_1 + v_3)$, VT is of dimension 2. The rank of T is 2.

(b) $(v_1 - v_2 + v_3) T = v_1 T - v_2 T + v_3 T$

$= (v_1 - v_2) - (v_1 + v_3) + (v_2 + v_3)$

$= 0$

32. Prove that the range of T and $U = \{v \in V \mid vT = 0\}$ are subspaces of V.

269.32 v_1, v_2 belong to the range of T implies there are vectors ω_1 and ω_2. such that $\omega_1 T = v_1$, $\omega_2 T = v_2$, $(\omega_1 + \omega_2) T = \omega_1 T + \omega_2 T = v_1 + v_2$, $v_1 + v_2$ lies in the range of T. $\alpha \in F$, $(\alpha \omega_1) T = \alpha (\omega_1 T) = \alpha v_1$ αv_1 lies in the range of T. The range of T is a subspace of V.

$v_1, v_2 \in U$, $(v_1 + v_2) T = v_1 T + v_2 T = 0 + 0 = 0$.

$v_1 + v_2 \in U$. $\alpha \in F$. $(\alpha v_1) T = \alpha (v_1 T)$

$= \alpha \cdot 0 = 0$.

$\alpha v_1 \in U$. U is a subspace of V.

33. If $T \in A(V)$, let $V_0 = \{v \in V \mid vT^k = 0 \text{ for some } k\}$. Prove that V_0 is a subspace and that if $vT^m \in V_0$, then $v \in V_0$.

269.33 $v_1, v_2 \in V_0$. $v_1 T^{k_1} = v_2 T^{k_2} = 0$ for some k_1 and k_2.

$(v_1 + v_2) T^{k_1 + k_2}$

$= v_1 T^{k_1 + k_2} + v_2 T^{k_1 + k_2} = 0 + 0 = 0$.

$v_1 + v_2 \in V_0$. $\alpha \in F$.

$(\alpha v_1) T^{k_1} = \alpha (v_1 T^{k_1}) = \alpha \cdot 0 = 0$,

$\alpha v_1 \in V_0$. V_0 is a subspace of V.

$vT^m \in V_0$ implies $(vT^m) T^k = 0$

for some k. $vT^{m+k} = 0$. Hence $v \in V_0$.

34. Prove that the minimal polynomial of T over F divides all polynomials satisfied by T over F.

269.34 Let $p(x)$ be the minimal polynomial of T. Suppose $q(x)$ satisfies by T.

$q(x) = a(x) p(x) + b(x)$ for some $a(x)$,

b(x) in F[x] and b(x) = 0 or deg b(x) < deg P(x). 0 = q(T)
= a(T) p(T) + b(T)
= a(T) · 0 + b(T) = b(T)
T also satisfies b(x). If b(x) ≠ 0, then deg b(x) < deg p(x) and T satisfies b(x), contrary to the fact that p(x) is the minimal polynomial of T. Hence b(x) = 0 and q(x) = a(x) p(x). p(x) divides q(x). This completes the proof.

*35. If $n(T)$ is the dimension of the U of Problem 32 prove that $r(T) + n(T) = \dim V$.

269.35 By (205.7), V/U is isomorphic to VT.
r(T) = dim VT = dim V − dim U = dim V − n(T).
r(T) + n(T) = dim V.

6.2 Characteristic Roots

In all the problems V is a vector space over F.

1. If $T \in A(V)$ and if $q(x) \in F[x]$ is such that $q(T) = 0$, is it true that every root of $q(x)$ in F is a characteristic root of T? Either prove that this is true or give an example to show that it is false.

272.1 Let V be the set of all complex numbers. V is a vector space over F, the set of all real numbers. Let T : V → V as (a+ib)T = a − ib T ∈ A(V). Let q(x) = x³ + 2x² − x − 2
= (x² − 1)(x + 2).
q(T) = 0. −2 is a root of q(x) in F but not a characteristic root of T. For, if −2 is a characteristic root of T, then there is a + ib ∈ V, a + ib ≠ 0 such that (a + ib)T = (−2)(a + ib) by Theorem 6.2.1. But a − ib = (−2)(a + ib) implies a + ib = 0, a contradiction. Therefore, the statement of (272.1) is not true.

2. If $T \in A(V)$ and if $p(x)$ is the minimal polynomial for T over F, suppose that $p(x)$ has all its roots in F. Prove that every root of $p(x)$ is a characteristic root of T.

272.2 Let λ be a root of p(x). Let f(x) be the minimal polynomial for λ − T over F. We want to show that λ − T is singular and then λ is a characteristic root of T by Theorem 6.2.1. By the definition of f(x). T satisfies f(λ − x). Since p(x) is a minimal polynomial for T. p(x) | f(λ − x). f(0) = f(λ − λ)
= p(λ) · k = 0.
The constant term of f(x) is 0.
By Theorem 6.1.2., T is singular.
This completes the proof.

3. Let V be two-dimensional over the field F, of real numbers, with a basis v_1, v_2. Find the characteristic roots and corresponding characteristic vectors for T defined by
(a) $v_1T = v_1 + v_2$, $v_2T = v_1 - v_2$.
(b) $v_1T = 5v_1 + 6v_2$, $v_2T = -7v_2$.
(c) $v_1T = v_1 + 2v_2$, $v_2T = 3v_1 + 6v_2$.

272.3 (a) $\sqrt{2}$, $(-1-\sqrt{2})v_1 - v_2$.
$-\sqrt{2}$, $(-1+\sqrt{2})v_1 - v_2$
(b) 5, $(-12v_1 - 6v_2)$, -7, v_2
(c) 0, $3v_1 - v_2$. 7, $-v_1 - 2v_2$.

4. Let V be as in Problem 3, and suppose that $T \in A(V)$ is such that $v_1T = \alpha v_1 + \beta v_2$, $v_2T = \gamma v_1 + \delta v_2$, where $\alpha, \beta, \gamma, \delta$ are in F.
(a) Find necessary and sufficient conditions that 0 be a characteristic root of T in terms of $\alpha, \beta, \gamma, \delta$.
(b) In terms of $\alpha, \beta, \gamma, \delta$ find necessary and sufficient conditions that T have two distinct characteristic roots in F.

272.4 (a) The necessary and sufficient conditions that 0 be characteristic root of T is $\alpha\delta = \beta\gamma$
For, 0 is a characteristic root of T, if and only if there are a, b in F such that
$(av_1 + bv_2)T = a(\alpha v_1 + \beta v_2) + b(\gamma v_1 + \delta v_2)$
$= (\alpha a + \gamma b)v_1 + (\beta a + \delta b)v_2 = 0$
with $av_1 + bv_2 \neq 0$ by Theorem 6.2.1.

$$\begin{cases} \alpha a + \gamma b = 0 \\ \beta a + \delta b = 0 \end{cases}$$

has nonzero solutions if and only if
$\alpha\delta = \beta\gamma$

(b) The necessary and sufficient condition that T have two distinct characteristic roots in F is $(\alpha - \delta)^2 + 4\beta\gamma > 0$. By (269.27), T satisfies $f(x) = x^2 - (\alpha + \delta)x + (\alpha\delta - \beta\gamma)$. If T has two distinct characteristic roots in F, then $f(x)$ is the minimal polynomial for T by Theorem 6.2.2. and $f(x)$ has two distinct roots in F. Hence

$(\alpha + \delta)^2 - 4(\alpha\delta - \beta\gamma)$
$= (\alpha - \delta)^2 + 4\beta\gamma > 0$. Conversely, suppose $(\alpha - \delta)^2 + 4\beta\gamma > 0$.
Let $p(x)$ be the monic minimal polynomial for T. $p(x) \mid f(x)$. If $f(x) = p(x)$, then by (272.2), T has two distinct characteristic roots in F. If $f(x) \neq p(x)$ then $p(x) = x - \lambda$ for some λ in F.
Since $P(x)$ is the minimal polynomial for T, $T = \lambda$.

$$\begin{cases} v_1T = \alpha v_1 + \beta v_2 = \lambda v_1 \\ v_2T = \gamma v_1 + \delta v_2 = \lambda v_2 \end{cases}$$

$\beta = \gamma = 0$, $\alpha = \delta = \lambda$, $(\alpha - \delta)^2 + 4\beta\gamma = 0$, contrary to our assumption that $(\alpha - \delta)^2 + 4\beta\gamma > 0$.

5. If V is two-dimensional over a field F prove that every element in $A(V)$ satisfies a polynomial of degree 2 over F.

273.5 By (269.27), we have that every element in A(V) satisfies a polynomial of degree 2 over F.

*6. If V is two-dimensional over F and if $S, T \in A(V)$, prove that $(ST - TS)^2$ commutes with all elements of $A(V)$.

273.6 Let v_1, v_2 be a basis of V over F. Let

$$\begin{cases} v_1T = a_1v_1 + b_1v_2 \\ v_2T = c_1v_1 + d_1v_2 \end{cases}$$

and

$$\begin{cases} v_1S = a_2v_1 + b_2v_2 \\ v_2S = c_2v_1 + d_2v_2 \end{cases}$$

Then

$$\begin{cases} v_1(TS) = (a_1a_2 + b_1c_2)v_1 \\ \qquad + (a_1b_2 + b_1d_2)v_2, \\ v_2(TS) = (c_1a_2 + d_1c_2)v_1 \\ \qquad + (c_1b_2 + d_1d_2)v_2, \end{cases}$$

$$\begin{cases} v_1(ST) = (a_2a_1 + b_2c_1)v_1 + (a_2b_1 + b_2d_1)v_2 \\ v_2(ST) = (c_2a_1 + d_2c_1)v_1 + (c_2b_1 + d_2d_1)v_2, \end{cases}$$

$$\begin{cases} v_1(ST-TS) = (b_2c_1 - b_1c_2)v_1 + (a_2b_1 \\ \qquad + b_2d_1 - (a_1b_2 + b_1d_2))v_2 \\ v_2(ST-TS) = (c_2a_1 + d_2c_1 - (c_1a_2 + d_1c_2))v_1 \\ \qquad + (c_2b_1 - c_1b_2)v_2, \end{cases}$$

$$\begin{cases} v_1(ST-TS)^2 = \lambda v_1 \\ v_2(ST-TS)^2 = \lambda v_2, \end{cases}$$

where $\lambda = (b_2c_1 - b_1c_2)^2 + (a_2b_1 + b_2d_1 - (a_1b_2 + b_1d_2))(c_2a_1 + d_2c_1 - (c_1a_2 + d_1c_2))$.

Hence $(ST-TS)^2 = \lambda \cdot (ST-TS)^2$ commutes with all elements of $A(V)$.

7. Prove Corollary 2 to Theorem 6.2.3.

273.7 By Theorem 6.2.3 and Theorem 6.2.2, we get the Corollary.

8. If V is n-dimensional over F and $T \in A(V)$ is nilpotent (i.e., $T^k = 0$ for some k), prove that $T^n = 0$. (*Hint:* If $v \in V$ use the fact that v, vT, $vT^2, \ldots, vT^n$ must be linearly dependent over F.)

273.8 If $T = 0$, them $T^n = 0$. Let $T \neq 0$ and $T^l = 0$ $T^{l-1} \neq 0$. $V \supset VT \supset VT^2 \supset \cdots\cdots \supset VT^{l-1} \supset VT^l = (0)$.

In this sequence, VT^{i+1} is properly contained in VT^i for $i = 0, 1, \cdots, \ell - 1$, For, if $VT^{i+1} = VT^i$, then

$VT^i = VT^{i+1}$, $VT^{i+1} = VT^{i+2}$

$VT^i = VT^{i+1} = VT^{i+2} = \cdots\cdots = VT^l = (0)$

$T^i = 0$, $i \geq \ell$.

$n = \dim V \geq \dim VT \geq \dim VT^2 \geq \cdots\cdots \geq \dim VT^{l-1} \geq \dim VT^l = 0$.

Therefore, $\ell \leq n$ and $T^n = 0$.

Another proof of this exercises. $v \in V$.

Let $VT^l = 0$ and $VT^{l-1} \neq 0$.

$v, vT, \cdots\cdots, vT^{l-1}$ are linearly independent. For, if

$\alpha_0 v + \alpha_1 vT + \cdots\cdots + \alpha_{l-1} vT^{l-1} = 0$, then

$$\begin{aligned} 0 &= (\alpha_0 v + \alpha_1 vT + \cdots\cdots + \alpha_{l-1} vT^{l-1})T^{l-1} \\ &= \alpha_0 vT^{l-1} + \alpha_1 vT^l + \cdots\cdots + \alpha_{l-1} vT^{2l-2} \\ &= \alpha_0 VT^{l-1}. \end{aligned}$$

Since $vT^{l-1} \neq 0$, $\alpha_0 = 0$. $\alpha_1 vT + \cdots + \alpha_{l-1} vT^{l-1} = 0$.

$$\begin{aligned} 0 &= (\alpha_1 vT + \cdots + \alpha_{l-1} vT^{l-1})T^{l-2} \\ &= \alpha_1 vT^{l-1} + \cdots + \alpha_{l-1} vT^{2l-3} \\ &= \alpha_1 vT^{l-1}. \end{aligned}$$

Since $vT^{l-1} \neq 0$, $\alpha_1 = 0$. Repeating this process, we have $\alpha_0 = \alpha_1 = \cdots\cdots = \alpha_{l-1} = 0$. $v, vT, \cdots\cdots, vT^{l-1}$ are linearly independent and $l \leq n = \dim V$.

6.3. Matrices

1. Compute the following matrix products:

(a) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & -1 & 2 \\ 3 & 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 3 \\ -1 & -1 & -1 \end{pmatrix}$.

(b) $\begin{pmatrix} 1 & 6 \\ -6 & 1 \end{pmatrix}\begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix}$.

(c) $\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}^2$.

(d) $\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}^2$.

281.1(a) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & -1 & 2 \\ 3 & 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 3 \\ -1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} -2 & 1 & 4 \\ -1 & -4 & -4 \\ -2 & 3 & 10 \end{pmatrix}$.

(b) $\begin{pmatrix} 1 & 6 \\ -6 & 1 \end{pmatrix}\begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 15 & 16 \\ -16 & 15 \end{pmatrix}$.

(c) $\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}^2 = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$.

(d) $\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

2. Verify all the computations made in the example illustrating Theorem 6.3.2.

281.2 $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$,

$$C^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}.$$

$$Cm_1(D)C^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -2 & 2 & 0 & 0 \\ -3 & 0 & 3 & 0 \end{pmatrix} = m_2(D).$$

3. In F_n prove directly, using the definitions of sum and product, that
(a) $A(B + C) = AB + AC$;
(b) $(AB)C = A(BC)$;
for $A, B, C \in F_n$.

282.3 Let $A=(\alpha_{ij})$, $B=(\beta_{ij})$, $C=(\gamma_{ij})$

(a) $A(B+C)=A(\beta_{ij}+\gamma_{ij})=(\alpha_{ij})(\beta_{ij}+\gamma_{ij})$

$$=\left(\sum_{k=1}^{n}\alpha_{ik}(\beta_{kj}+\gamma_{kj})\right)=\left(\sum_{k=1}^{n}(\alpha_{ik}\beta_{kj}+\alpha_{ik}\gamma_{kj})\right)$$

$$=\left(\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}+\sum_{k=1}^{n}\alpha_{ik}\gamma_{kj}\right)$$

$$=\left(\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}\right)+\left(\sum_{k=1}^{n}\alpha_{ik}\gamma_{kj}\right)$$

$$=(\alpha_{ij})(\beta_{ij})+(\alpha_{ij})(\gamma_{ij})$$

$$=AB+AC.$$

(b) $(AB)C=((\alpha_{ij})(\beta_{ij}))(\gamma_{ij})$

$$=\left(\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}\right)(\gamma_{ij})$$

$$=\left(\sum_{l=1}^{n}\left(\sum_{k=1}^{n}\alpha_{ik}\beta_{kl}\right)\gamma_{lj}\right)$$

$$=\Big(\sum_{l=1}^{n}\sum_{k=1}^{n}\alpha_{ik}(\beta_{kl}\gamma_{lj})\Big)$$
$$=\Big(\sum_{k=1}^{n}\alpha_{ik}\Big(\sum_{l=1}^{n}\beta_{kl}\gamma_{lj}\Big)\Big)$$
$$=(\alpha_{ij})\Big(\sum_{l=1}^{n}\beta_{il}\gamma_{li}\Big)$$
$$=A(BC).$$

4. In F_2 prove that for any two elements A and B, $(AB - BA)^2$ is a scalar matrix.

282.4 By(273.6), $(AB-BA)^2$ is a scalar matrix.

5. Let V be the vector space of polynomials of degree 3 or less over F. In V define T by $(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3)T = \alpha_0 + \alpha_1(x + 1) + \alpha_2(x + 1)^2 + \alpha_3(x + 1)^3$. Compute the matrix of T in the basis
(a) $1, x, x^2, x^3$.
(b) $1, 1 + x, 1 + x^2, 1 + x^3$.
(c) If the matrix in part (a) is A and that in part (b) is B, find a matrix C so that $B = CAC^{-1}$

282.5 (a)(1) $T=1$, $xT=x+1=1+x$, $x^2T=(x+1)^2=1+2x+x^2$, $x^3T=(x+1)^3=1+3x+3x^2+x^3$.

$$A=\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&2&1&0\\1&3&3&1\end{pmatrix}.$$

(b)(1) $T=1$, $(1+x)T=1+(x+1)$, $(1+x^2)T=1+(x+1)^2=2+2x+x^2=-1+2(1+x)+(1+x^2)$, $(1+x^3)T=1+(x+1)^3=2+3x+3x^2+x^3=-5+3(1+x)+3(1+x^2)+(1+x^3)$.

$$B=\begin{pmatrix}1&0&0&0\\1&1&0&0\\-1&2&1&0\\-5&3&3&1\end{pmatrix}.$$

(c)(1) $S=1$, $xS=1+x$, $x^2S=1+x^2$, $x^3S=1+x^3$,

$$C=\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}.$$

$$C^{-1}=\begin{pmatrix}1&0&0&0\\-1&1&0&0\\-1&0&1&0\\-1&0&0&1\end{pmatrix}.$$

$$CAC^{-1}=\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&2&1&0\\1&3&3&1\end{pmatrix}$$
$$\begin{pmatrix}1&0&0&0\\-1&1&0&0\\-1&0&1&0\\-1&0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0&0\\2&1&0&0\\2&2&1&0\\2&3&3&1\end{pmatrix}$$
$$\begin{pmatrix}1&0&0&0\\-1&1&0&0\\-1&0&1&0\\-1&0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0&0\\1&1&0&0\\-1&2&1&0\\-5&3&3&1\end{pmatrix}$$
$$=B.$$

6. Let $V = F^{(3)}$ and suppose that

$$\begin{pmatrix}1&1&2\\-1&2&1\\0&1&3\end{pmatrix}$$

is the matrix of $T \in A(V)$ in the basis $v_1 = (1, 0, 0)$, $v_2 = (0, 1, 0)$, $v_3 = (0, 0, 1)$. Find the matrix of T in the basis
(a) $u_1 = (1, 1, 1)$, $u_2 = (0, 1, 1)$, $u_3 = (0, 0, 1)$.
(b) $u_1 = (1, 1, 0)$, $u_2 = (1, 2, 0)$, $u_3 = (1, 2, 1)$.

282.6
(a) $u_1T=(1,1,1)\begin{pmatrix}1&1&2\\-1&2&1\\0&1&3\end{pmatrix}=(0,4,6)$
$=4u_2+2u_3$

$$u_2T=(0,1,1)\begin{pmatrix}1&1&2\\-1&2&1\\0&1&3\end{pmatrix}=(-1,3,4)$$

$$=-u_1+4u_2+u_3$$

$$u_3T=(0,0,1)\begin{pmatrix}1&1&2\\-1&2&1\\0&1&3\end{pmatrix}=(0,1,3)$$

$$=u_2+2u_3.$$

The matrix of T in the basis u_1,u_2,u_3 is

$$\begin{pmatrix}0&4&2\\-1&4&1\\0&1&2\end{pmatrix}.$$

(b) $$u_1T=(1,1,0)\begin{pmatrix}1&1&2\\-1&2&1\\0&1&3\end{pmatrix}=(0,3,3)$$

$$=-3u_1+3u_3$$

$$u_2T=(1,2,0)\begin{pmatrix}1&1&2\\-1&2&1\\0&1&3\end{pmatrix}=(-1,5,4)$$

$$=-7u_1+2u_2+4u_3$$

$$u_3T=(1,2,1)\begin{pmatrix}1&1&2\\-1&2&1\\0&1&3\end{pmatrix}=(-1,6,7)$$

$$=-8u_1+7u_3.$$

The matrix of T in the basis u_1,u_2,u_3 is

$$\begin{pmatrix}-3&0&3\\-7&2&4\\-8&0&7\end{pmatrix}.$$

7. Prove that, given the matrix

$$A=\begin{pmatrix}0&1&0\\0&0&1\\6&-11&6\end{pmatrix}\in F_3$$

(where the characteristic of F is not 2), then
(a) $A^3-6A^2+11A-6=0$.
(b) There exists a matrix $C\in F_3$ such that

$$CAC^{-1}=\begin{pmatrix}1&0&0\\0&2&0\\0&0&3\end{pmatrix}$$

282.7

(a) $$A=\begin{pmatrix}0&1&0\\0&0&1\\6&-11&6\end{pmatrix}$$

$$A^2=\begin{pmatrix}0&1&0\\0&0&1\\6&-11&6\end{pmatrix}^2=\begin{pmatrix}0&0&1\\6&-11&6\\36&-60&25\end{pmatrix}$$

$$A^3=\begin{pmatrix}6&-11&6\\36&-60&25\\150&-239&90\end{pmatrix}$$

$$A^3-6A^2+11A-6=\begin{pmatrix}6&-11&6\\36&-60&25\\150&-239&90\end{pmatrix}$$

$$\begin{pmatrix}0&0&6\\36&-66&36\\216&-360&150\end{pmatrix}+\begin{pmatrix}0&11&0\\0&0&11\\66&-121&66\end{pmatrix}$$

$$-\begin{pmatrix}6&0&0\\0&6&0\\0&0&6\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}=0.$$

(b) $$C=\begin{pmatrix}6&-5&1\\3&-4&1\\2&-3&1\end{pmatrix}.\quad\begin{pmatrix}6&-5&1\\3&-4&1\\2&-3&1\end{pmatrix}.$$

$$\begin{pmatrix}\frac{1}{2}&-1&\frac{1}{2}\\\frac{1}{2}&-2&\frac{3}{2}\\\frac{1}{2}&-4&\frac{9}{2}\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}.$$

$$C^{-1}=\begin{pmatrix}\frac{1}{2}&-1&\frac{1}{2}\\\frac{1}{2}&-2&\frac{3}{2}\\\frac{1}{2}&-4&\frac{9}{2}\end{pmatrix}$$

$$CAC^{-1}=\begin{pmatrix}6&-5&1\\3&-4&1\\2&-3&1\end{pmatrix}\begin{pmatrix}0&1&0\\0&0&1\\6&-11&6\end{pmatrix}$$

$$\begin{pmatrix}\frac{1}{2}&-1&\frac{1}{2}\\ \frac{1}{2}&-2&\frac{3}{2}\\ \frac{1}{2}&-4&\frac{9}{2}\end{pmatrix}=\begin{pmatrix}6&-5&1\\6&-8&2\\6&-9&3\end{pmatrix}$$

$$\begin{pmatrix}\frac{1}{2}&-1&\frac{1}{2}\\ \frac{1}{2}&-2&\frac{3}{2}\\ \frac{1}{2}&-4&\frac{9}{2}\end{pmatrix}=\begin{pmatrix}1&0&0\\0&2&0\\0&0&3\end{pmatrix}$$

8. Prove that it is impossible to find a matrix $C \in F_2$ such that

$$C\begin{pmatrix}1&1\\0&1\end{pmatrix}C^{-1}=\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix},$$

for any $\alpha, \beta \in F$.

282.8 If there is a $C=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in F_2$ such that $C\begin{pmatrix}1&1\\0&1\end{pmatrix}C^{-1}=\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}$ for some α,β in F, then

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}.$$

$$\begin{pmatrix}a&a+b\\c&c+d\end{pmatrix}=\begin{pmatrix}\alpha a&\alpha b\\\beta c&\beta d\end{pmatrix}.$$

$$\begin{cases}a=\alpha a\\ c=\beta c\\ a+b=\alpha b\\ c+d=\beta d.\end{cases}$$

If $a\neq 0$, then $\alpha=1$ and $a+b=\alpha b=b$ implies $a=0$. Hence $a=0$. If $c\neq 0$, then $\beta=1$ and $c+d=\beta d=d$ implies $c=0$. Hence $c=0$.

$C=\begin{pmatrix}0&b\\0&d\end{pmatrix}$. C is not invertible. Thus, it is impossible to find a matrix c in F_2 such that

$$C\begin{pmatrix}1&1\\0&1\end{pmatrix}C^{-1}=\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix},$$

for any $\alpha,\beta\in F$.

9. A matrix $A \in F_n$ is said to be a *diagonal* matrix if all the entries off the main diagonal of A are 0, i.e., if $A = (\alpha_{ij})$ and $\alpha_{ij} = 0$ for $i \neq j$. If A is a diagonal matrix all of whose entries on the main diagonal are distinct, find all the matrices $B \in F_n$ which commute with A, that is, all matrices B such that $BA = AB$.

282.9 Let $B=(\beta_{ij})$. $AB=(\alpha_{ij})(\beta_{ij})=(\sum_{k=1}^{n}\alpha_{ik}\beta_{kj})$ $=(\alpha_{ii}\beta_{ij})$, $BA=(\beta_{ij})(\alpha_{ij})=(\sum_{k=1}^{n}\beta_{ik}\alpha_{kj})$ $=(\beta_{ij}\alpha_{jj})$.

$\alpha_{ii}\beta_{ij}=\beta_{ij}\alpha_{jj}$ for all $i=1,\cdots\cdots,n$ $,j=1,\cdots\cdots,n$. $i\neq j$ implies $\beta_{ij}=0$.
Hence B is a diagonal matrix.
Conversely, if B is a diagonal matrix, then clearly AB=BA. Hence BA=AB if and only if B is a diagonal matrix.

10. Using the result of Problem 9, prove that the only matrices in F_n which commute with all matrices in F_n are the scalar matrices.

283.10 By (267.7), the only matrices in F_n which commute with all matrices in F_n are the scalar matrices.
Note that, since the number of elements in F may be less than n, we can not use the result of (283.9).

11. Let $A \in F_n$ be the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

whose entries everywhere, except on the superdiagonal, are 0, and whose entries on the superdiagonal are 1's. Prove $A^n = 0$ but $A^{n-1} \neq 0$.

283.11

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots\cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots\cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots\cdots & 0 & 0 \\ \vdots & & & & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots\cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots\cdots & 0 & 0 \end{pmatrix}$$

$$A^2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & \cdots\cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots\cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \cdots\cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots\cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots\cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots\cdots & 0 & 0 \end{pmatrix}$$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

$$A^{n-1} = \begin{pmatrix} 0 & 0 & \cdots\cdots & 0 & 1 \\ 0 & 0 & \cdots\cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots\cdots & 0 & 0 \\ 0 & 0 & \cdots\cdots & 0 & 0 \end{pmatrix} \neq 0, \quad A^n = 0.$$

*12. If A is as in Problem 11, find all matrices in F_n which commute with A and show that they must be of the form $\alpha_0 + \alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_{n-1} A^{n-1}$ where $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in F$.

283.12 $A=(\alpha_{ij})$, $\alpha_{ij}=0$ if $j \neq i+1$, $\alpha_{i,i+1}=1$, $i=1, \cdots\cdots, n-1$.

Suppose $B=(\beta_{ij})$, $BA=BA$. $\sum_{k=1}^{n} \alpha_{ik}\beta_{kj} = \sum_{k=1}^{n} \beta_{ik}\alpha_{kj}$ $i, j=1, 2, \cdots\cdots, n$.

For $1 \leq i \leq n-1$ and $2 \leq j \leq n$, we have $\beta_{i+1,j} = \beta_{ij-1}$.

For $j=1$ and $1 \leq i \leq n-1$, we have $\beta_{i+11}=0$.

$B_{21}=\beta_{31}=\cdots\cdots=\beta_{n1}=0$. $\beta_{ij}=\beta_{i-1\,j-1}$, $2 \leq i \leq n$, $2 \leq j \leq n$.

$\beta_{11}=\beta_{22}=\cdots\cdots=\beta_{nn}=\alpha_0$.

$\beta_{12}=\beta_{23}=\cdots\cdots=\beta_{n-1\,n}=\alpha_1$.

$\beta_{13}=\beta_{24}=\cdots\cdots=\beta_{n-2\,n}=\alpha_2$.

$\vdots$

$\beta_{1n}=\alpha_{n-1}$.

For $i > j$, $\beta_{ij}=\beta_{i-1\,j-1}=\beta_{i-2\,j-2}=\cdots\cdots=\beta_{i-j+11}$ $=0$ since $i-j+1 \leq 2$

$$B = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots\cdots & \alpha_{n-1} & \alpha_n \\ 0 & \alpha_0 & \alpha_1 & \cdots\cdots & \alpha_{n-2} & \alpha_{n-1} \\ 0 & 0 & \alpha_0 & & \alpha_{n-3} & \alpha_{n-2} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots\cdots & \alpha_0 & \alpha_1 \\ 0 & 0 & 0 & & 0 & \alpha_0 \end{pmatrix}$$

$= \alpha_0 + \alpha_1 A + \alpha_2 A^2 + \cdots\cdots + \alpha_{n-1} A^{n-1}$. Conversely, if $B = \alpha_0 + \alpha_1 A + \cdots\cdots + \alpha_{n-1} A^{n-1}$, then $BA=AB$.

13. Let $A \in F_2$ and let $C(A) = \{B \in F_2 \mid AB = BA\}$. Let $C(C(A)) = \{G \in F_2 \mid GX = XG \text{ for all } X \in C(A)\}$. Prove that if $G \in C(C(A))$ then G is of the form $\alpha_0 + \alpha_1 A$, $\alpha_0, \alpha_1 \in F$.

14. Do Problem 13 for $A \in F_3$, proving that every $G \in C(C(A))$ is of the form $\alpha_0 + \alpha_1 A + \alpha_2 A^2$.

283.13 283.14 we suggest the reader see Jacobson , N. Lectures in Abstract Algebra (Vol 2) page 113.

15. In F_n let the matrices E_{ij} be defined as follows: E_{ij} is the matrix whose only nonzero entry is the (i, j) entry, which is 1. Prove
(a) The E_{ij} form a basis of F_n over F.
(b) $E_{ij}E_{kl} = 0$ for $j \neq k$; $E_{ij}E_{jl} = E_{il}$.

(c) Given i, j, there exists a matrix C such that $CE_{ii}C^{-1} = E_{jj}$.
(d) If $i \neq j$ there exists a matrix C such that $CE_{ij}C^{-1} = E_{12}$.
(e) Find all $B \in F_n$ commuting with E_{12}.
(f) Find all $B \in F_n$ commuting with E_{11}.

283.15 (a) $A=(\alpha_{ij}) \in F_n$. $A=\sum_{i,j}\alpha_{ij}E_{ij}$, $\{E_{ij}\}$ spans Fn.

Clearly, E_{ij} are linearly independent. Hence E_{ij} form a basis of F_n.

(b) $E_{ij}=(\alpha_{ij})$, $\alpha_{rs}=0$ if $r \neq i$, $s \neq j$ and $\alpha_{ij}=1$.
$E_{kl}=(\beta_{ij})$, $\beta_{rs}=0$ if $r \neq k$, $s \neq l$ and $\beta_{kl}=1$.
$E_{ij}E_{kl}=(r_{ij})$

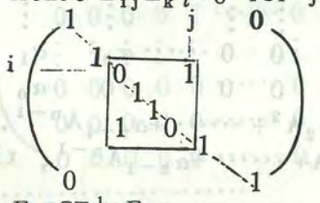
$$r_{rs}=\sum_{t=1}^{n}\alpha_{rt}\beta_{ts}.$$

If $r \neq i$, then $\alpha_{rt}=0$ for $t=1, \cdots\cdots, n$. $r_{rs}=0$.
If $s \neq l$, then $\beta_{ts}=0$ for $t=1, \cdots\cdots, n$. $\gamma_{rs}=0$.

$$\gamma_{il}=\sum_{t=1}^{n}\alpha_{it}\beta_{tl}=\alpha_{ij}\beta_{jl}.$$

If $j \neq k$, then $\beta_{jl}=0, \gamma_{il}=0$, If $j=k$, then $\gamma_{il}=1$. Hence $E_{ij}E_{kl}=0$ for $j \neq k$; $E_{ij}E_{jl}=E_{il}$.

(c) Let C=



Then, $C E_{ii} C^{-1}=E_{jj}$.

(d) Let $C=(\alpha_{ij})$ such that
$\alpha_{i1}=\alpha_{1i}=\alpha_{2j}=\alpha_{j2}=1$, $\alpha_{rr}=1$ if $r \neq 1, 2, i, j$, and any other entry is 0. Then $CE_{ij}C^{-1}=E_{12}$.

(e) Let $B=(\beta_{ij})=\sum_{i,j}\beta_{ij}E_{ij}$.

$$E_{12}B=\sum_{j=1}^{n}\beta_{2j}E_{1j}. \quad BE_{12}=\sum_{i=1}^{n}\beta_{i1}E_{12}.$$

$E_{12}B=BE_{12}$ if and only if

$$\begin{cases}\beta_{2j}=\beta_{i1}=0 \text{ if } i \neq 1 \text{ and } j \neq 2\\ \beta_{11}=\beta_{22}.\end{cases}$$

(f) Let $B=(\beta_{ij})=\sum_{i,j}\beta_{ij}E_{ij}$.

$$E_{11}B=\sum_{j=1}^{n}\beta_{1j}E_{1j}. \quad BE_{11}=\sum_{i=1}^{n}\beta_{i1}E_{11}.$$

$E_{11}B=BE_{11}$ if and only if
$\beta_{1j}=\beta_{i1}=0$ for $i \neq 1$ and $j \neq 1$.

16. Let F be the field of real numbers and let C be the field of complex numbers. For $a \in C$ let $T_a: C \to C$ by $xT_a = xa$ for all $x \in C$. Using the basis 1, i find the matrix of the linear transformation T_a and so get an isomorphic representation of the complex numbers as 2×2 matrices over the real field.

283.16 Let $a=\alpha+i\beta$.
(1) $Ta=\alpha+i\beta$
(i) $Ta=i(\alpha+i\beta)=-\beta+i\alpha$.
Define $T: C \to F_2$ as $aT=\begin{pmatrix}\alpha & \beta\\ -\beta & \alpha\end{pmatrix}$

17. Let Q be the division ring of quaternions over the real field. Using the basis 1, i, j, k of Q over F, proceed as in Problem 16 to find an isomorphic representation of Q by 4×4 matrices over the field of real numbers.

283.17 Let $a=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$.
(1) $Ta=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$.
(i) $Ta=-\alpha_1+\alpha_0 i-\alpha_3 j+\alpha_2 k$.
(j) $Ta=-\alpha_2+\alpha_3 i+\alpha_0 j-\alpha_1 k$.
(k) $Ta=-\alpha_3-\alpha_2 i+\alpha_1 j+\alpha_0 k$.

Define $T: Q \to F_4$ as $aT=\begin{pmatrix}\alpha_0 & \alpha_1 & \alpha_2 & \alpha_3\\ -\alpha_1 & \alpha_0 & -\alpha_3 & \alpha_2\\ -\alpha_2 & \alpha_3 & \alpha_0 & -\alpha_1\\ -\alpha_3 & -\alpha_2 & \alpha_1 & \alpha_0\end{pmatrix}$

*18. Combine the results of Problems 16 and 17 to find an isomorphic representation of Q as 2×2 matrices over the field of complex numbers.

283.18 Define $T: Q \to C_2$ as

$$(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)T=\begin{pmatrix}\alpha_0+\alpha_1 i & \alpha_2+\alpha_3 i\\ -\alpha_2+\alpha_3 i & \alpha_0-\alpha_1 i\end{pmatrix}.$$

This representation is obtained as we identify $\begin{pmatrix}\alpha_0 & \alpha_1\\ -\alpha_1 & \alpha_0\end{pmatrix}$ with $\alpha_0+\alpha_1 i$. We can get this by

using the basis $1, j$ over C.

$a=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k=(\alpha_0+\alpha_1 i)+(\alpha_2+\alpha_3 i)j$.

$1Ta=(\alpha_0+\alpha_1 i)+(\alpha_2+\alpha_3 i)j$

(j) $Ta=-\alpha_2+\alpha_3 i+\alpha_0 j-\alpha_1 k$

$=(-\alpha_2+\alpha_3 i)+(\alpha_0-\alpha_1 i)j$.

19. Let $\mathcal{M}$ be the set of all $n \times n$ matrices having entries 0 and 1 in such a way that there is one 1 in each row and column. (Such matrices are called *permutation matrices*.)
(a) If $M \in \mathcal{M}$, describe AM in terms of the rows and columns of A.
(b) If $M \in \mathcal{M}$, describe MA in terms of the rows and columns of A.

284.19 (a) If the (i,j) entry of M is 1, then the j-th column of AM is the i-th column of A.

(b) If the (i,j) entry of M is 1, then the i-th row of MA is the j-th row of A.

20. Let $\mathcal{M}$ be as in Problem 19. Prove
(a) $\mathcal{M}$ has $n!$ elements.
(b) If $M \in \mathcal{M}$, then it is invertible and its inverse is again in $\mathcal{M}$.
(c) Give the explicit form of the inverse of M.
(d) Prove that $\mathcal{M}$ is a group under matrix multiplication.
(e) Prove that $\mathcal{M}$ is isomorphic, as a group, to S_n, the symmetric group of degree n.

284.20 (a) By the definition of $\mathcal{M}$, $\mathcal{M}$ has n! elements.

(b)(c) $M \in \mathcal{M}$, $M^t=(\beta_{ij})$, $M=(\alpha_{ij})$, $\beta_{ij}=\alpha_{ji}$.

$MM^t=1$. For $M=\sum_{i,j}\alpha_{ij}E_{ij}$, $M^t=\sum_{i,j}\beta_{ij}E_{ij}$.

$$MM^t=\sum_{i,j}\left(\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}E_{ij}\right)=\sum_{i,j}\left(\sum_{k=1}^{n}\alpha_{ik}\alpha_{jk}E_{ij}\right).$$

If $i \neq j$, then $\sum_{k=1}^{n}\alpha_{ik}\alpha_{jk}=0$ and $\sum_{k=1}^{n}\alpha_{ik}\alpha_{ik}=1$ since $M=(\alpha_{ij}) \in \mathcal{M}$. $M^t=M^{-1}$

(d) By (284.19 (a)) or (284.19 (b)), $\mathcal{M}$ is a group under matrix multiplication.

(e) $\mathcal{M}$ is a permutation group on $P=\{(1,0,0,\cdots\cdots,0),(0,1,0,\cdots\cdots,0),\cdots\cdots,(0,0,\cdots\cdots,0,1)\}$. $\mathcal{M}$ is isomorphic to a subgroup of Sn.

Since $o(\mathcal{M})=n!=o(S_n)$. $\mathcal{M}$ is isomorphic to S_n.

21. Let $A=(\alpha_{ij})$ be such that for each i, $\sum_j \alpha_{ij}=1$. Prove that 1 is a characteristic root of A (that is, $1-A$ is not invertible).

284.21 Since $(AB)^t=B^tA^t$ for A,B in F_n, A and A^t have the same minimal polynomial. For, if p(x) and q(x) are the minimal polynomials for A and A^t, respectively, then $p(A)=0$, $0=(p(A))^t=p(A^t)=0$, $q(x) \mid p(x)$. Similarly, $p(x) \mid q(x)$. By (284.22) 1 is a characteristic root of A^t. 1 is a root of the minimal polynomial for A^t and hance for A. By the proof of (272.2), 1 is a characteristic root of A.

22. Let $A=(\alpha_{ij})$ be such that for every j, $\sum_i \alpha_{ij}=1$. Prove that 1 is a characteristic root of A.

284.22 Since $(1,1,1,\cdots\cdots,1)A=(1,1,1,\cdots\cdots,1),1$ is a characteristic root of A.

23. Find necessary and sufficient conditions on $\alpha, \beta, \gamma, \delta$, so that $A=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ is invertible. When it is invertible, write down A^{-1} explicitly.

284.23 $A=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ is invertible if and only if $\alpha\delta-\beta r \neq 0$.

For, if $\alpha\delta-\beta\gamma \neq 0$, then

$$\begin{pmatrix} (\alpha\delta-\beta\gamma)^{-1}\delta & -(\alpha\delta-\beta\gamma)^{-1}\beta \\ -(\alpha\delta-\beta\gamma)^{-1}\gamma & (\alpha\delta-\beta\gamma)^{-1}\alpha \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = 1.$$

Conversely, if $A=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is invertible, then there is $B=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

That $\begin{cases} \alpha a+\beta c=1 \\ \gamma a+\delta c=0 \end{cases}$ has solutions a, c implies $\alpha\delta-\beta\gamma\neq 0$. Clearly, when A is invertible,

$$A^{-1}=\begin{pmatrix} (\alpha\delta-\beta\gamma)^{-1}\delta & -(\alpha\delta-\beta\gamma)^{-1}\beta \\ -(\alpha\delta-\beta\gamma)^{-1}\gamma & (\alpha\delta-\beta\gamma)^{-1}\alpha \end{pmatrix}.$$

24. If $E\in F_n$ is such that $E^2 = E \neq 0$ prove that there is a matrix $C\in F_n$ such that

$$CEC^{-1} = \left(\begin{array}{cccc|ccc} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & & & \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ \hline 0 & & \dots & 0 & 0 & \dots & 0 \\ 0 & & \dots & 0 & 0 & \dots & 0 \end{array}\right)$$

where the unit matrix in the top left corner is $r \times r$, where r is the rank of E.

284.24 By (268.17) and Theorem 6.3.2, we can get this result.

25. If F is the real field, prove that it is impossible to find matrices $A, B \in F_n$ such that $AB - BA = 1$.

284.25 Suppose there are $A=(\alpha_{ij})$, $B=(\beta_{ij})$ in F_n such that $AB-BA=1$.

$$AB=\left(\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}\right),\quad BA=\left(\sum_{k=1}^{n}\beta_{ik}\alpha_{kj}\right).$$

The (i,i) entry of $AB-BA$ is

$$\sum_{k=1}^{n}\alpha_{ik}\beta_{ki}-\sum_{k=1}^{n}\beta_{ik}\alpha_{ki}=1.$$

$$\sum_{i=1}^{n}\left(\sum_{k=1}^{n}\alpha_{ik}\beta_{ki}-\sum_{k=1}^{n}\alpha_{ki}\beta_{ik}\right)=n.$$

$$n=\sum_{i=1}^{n}\sum_{k=1}^{n}\alpha_{ik}\beta_{ki}-\sum_{i=1}^{n}\sum_{k=1}^{n}\alpha_{ki}\beta_{ik}$$

$$=\sum_{i=1}^{n}\sum_{k=1}^{n}\alpha_{ik}\beta_{ki}-\sum_{k=1}^{n}\sum_{i=1}^{n}\alpha_{ik}\beta_{ki}=0,$$

a contradiction. Therefore, it is impossible to find matrices A, B in F_n such that $AB-BA=1$.

26. If F is of characteristic 2, prove that in F_2 it is possible to find matrices A, B such that $AB - BA = 1$.

284.26 $$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}-\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$=\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}-\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

27. The matrix A is called *triangular* if all the entries above the main diagonal are 0. (If all the entries below the main diagonal are 0 the matrix is also called triangular).
   (a) If A is triangular and no entry on the main diagonal is 0, prove that A is invertible.
   (b) If A is triangular and an entry on the main diagonal is 0, prove that A is singular.

284.27 (a) Let $A=(\alpha_{ij})$. If $(a_1, \dots\dots, a_n)A=0$, then

$$0=\sum_{k=1}^{n}a_k\alpha_{ki}=\sum_{k=i}^{n}a_k\alpha_{ki} \quad \text{for } i=1, \dots\dots, n.$$

$0=a_n\alpha_{nn}$ implies $a_n=0$.

$0=a_n\alpha_{nn-1}+a_{n-1}\alpha_{n-1}=a_{n-1}\alpha_{n-1}$ implies $a_{n-1}=0$

$\vdots$

Repeating this process, we have $(a_1, \dots\dots, a_n)=0$. A is one-to-one and hence A is invertible.

(b) If $A=\begin{pmatrix} 0 & & 0 \\ & \alpha_{22} & \\ * & & \alpha_{nn} \end{pmatrix}$, then $(1,0, \dots\dots, 0)A=0$,

A is singular. If $A=\begin{pmatrix} \alpha_{11} & & 0 \\ & \ddots & \\ * & & \alpha_{k-1\,k-1} \end{pmatrix}$ and $\alpha_{11}\neq 0$, $\alpha_{k-1\,k-1}\neq 0$, then rank $A\leqslant k$. By Theorem 4.3.3, there is a nonzero element $(x_1, \cdots\cdots, x_k)$ such that $(x_1, \cdots\cdots, x_k)A=0$. Hence A is singular.

If $A=\begin{pmatrix} \alpha_{11} & & & 0 \\ & \alpha_{22} & & \\ & & \alpha_{k-1\,k-1} & \\ * & & & 0 \\ & & & \alpha_{nn} \end{pmatrix}$, then $(x_1, \cdots\cdots, x_k, 0, \cdots\cdots, 0)A=0$. A is singular.

28. If A is triangular, prove that its characteristic roots are precisely the elements on its main diagonal.

285.28 Let α lie on the main diagonal of A. α-A is also triangular and an entry on the main diagonal is 0 . By (284.27.(b)) , α-A is siugular. Hence every element on the main diagonal of A is a characteristic root of A. Conversely, if α is a chacteristic root of A, then α-A is singular by dcfinition. By (284.27(a)) , one entry on the main diagonal of α-A is 0. α equals to one entry on the main diagonal of A. This completes the proof.

29. If $N^k = 0$, $N \in F_n$, prove that $1 + N$ is invertible and find its inverse as a polynomial in N.

285.29 $(1+N)(1-N+N^2-\cdots\cdots+(-1)^{k-1}N^{k-1})=1+(-1)^{k-1}N^k=1$.

$1+N$ is invertible and $(1+N)^{-1}=1-N+N^2-\cdots\cdots+(-1)^{k-1}N^{k-1}$.

30. If $A \in F_n$ is triangular and all the entries on its main diagonal are 0, prove that $A^n = 0$.

285.30 Let $(\alpha_1, \cdots\cdots, \alpha_n)\in F^{(n)}$. $A=\begin{pmatrix} 0 & & 0 \\ \alpha_{21} & \ddots & \\ \alpha_{n1} & \alpha_{n2} & 0 \end{pmatrix}$.

$(\alpha_1, \cdots\cdots, \alpha_n)A=(\beta_1, \cdots\cdots, \beta_{n-1}, 0)$, $(\alpha_1, \cdots\cdots, \alpha_n)A^2=(\beta_1, \cdots\cdots, \beta_{n-1}, 0)A=(r_1, \cdots\cdots, r_{n-2}, 0, 0)$. Continuing the process, we have $(\alpha_1, \cdots\cdots, \alpha_n)A^n=0$ and $A^n=0$.

31. If $A \in F_n$ is triangular and all the entries on its main diagonal are equal to $\alpha \neq 0 \in F$, find A^{-1}.

285.31 By (284.27.(a)) , A is invertible. By (285.30) , $(A-\alpha)^n=0$.

$\alpha^n-\binom{n}{1}\alpha^{n-1}A+\binom{n}{2}\alpha^{n-2}A^2-\cdots\cdots+(-1)^nA^n=0$.

$A^{-1}=\alpha^{-n}\left\{\binom{n}{1}\alpha^{n-1}-\binom{n}{2}\alpha^{n-2}A+\cdots\cdots+(-1)^{n-1}A^{n-1}\right\}$.

32. Let S, T be linear transformations on V such that the matrix of S in one basis is equal to the matrix of T in another. Prove there exists a linear transformation A on V such that $T = ASA^{-1}$.

285.32 Let $m_1(S)$ be the matrix of S in the basis $v_1, \cdots\cdots, v_n$ and $m_2(T)$ be the matrix of T in the basis $w_1, \cdots\cdots, w_n$ and $m_1(S)=m_2(T)$. By Theorem 6.3.2 , there is a linear transformation A on V such that $m_1(S)=m_2(A)m_2(S)m_2(A^{-1})$.

Hence $m_2(T)=m_2(A)m_2(S)m_2(A^{-1})=m_2(ASA^{-1})$.

Therefore, $T=ASA^{-1}$.

6.4. Canonical Forms: Triangular Form.

1. Prove that the relation of similarity is an equivalence relation in $A(V)$.

290.1 For $A \in A(V)$, $IAI^{-1}=IAI=A$, A and A are similar.
If A and B are similar, then there is an invertible element C in A(V) such that $B=CAC^{-1}$, $A=C^{-1}B(C^{-1})^{-1}$. B and A are similar.
If S and T are similar, T and U are similar, then there are C and D in A(V) such that $T=CSC^{-1}$ and $U=DTD^{-1}$. $U=DTD^{-1}=D(CSC^{-1})D^{-1}=(DC)S(DC)^{-1}$. S and U are similar. The relation of similarity is an equivalence relation in A(V).

2. If $T \in F_n$ and if $K \supset F$, prove that as an element of K_n, T is invertible if and only if it is already invertible in F_n.

290.2 If T is invertible in F_n, then there is S in F_n such that $TS=I$. $S \in F_n \subset K_n$. T is invertible in K_n.
Conversely, if T is invertible in K_n, then $T: K^{(n)} \to K^{(n)}$ is one-to-one. $T \in F_n$, $T: F^{(n)} \to F^{(n)}$ is also one-to-one. Hence T is invertible in F_n.

3. In the proof of Theorem 6.4.1 prove that $v_1, \ldots, v_n$ is a basis of V.

290.3 If $\alpha_1 v_1+\alpha_2 v_2+\cdots\cdots+\alpha_n v_n=0$ for some $\alpha_1 \cdots\cdots, \alpha_n$ in F, then
$\alpha_1 \bar{v}_1+\alpha_2 \bar{v}_2+\cdots\cdots+\alpha_n \bar{v}_n=0$.
$\bar{v}_1=0$, $\alpha_2 \bar{v}_2+\cdots\cdots+\alpha_n \bar{v}_n=0$.
$\bar{v}_2, \cdots\cdots, \bar{v}_n$ is a basis of $\bar{V}$. $\alpha_2=\cdots\cdots=\alpha_n=0$.
$0=\alpha_1 v_1+\alpha_2 v_2+\cdots\cdots+\alpha_n v_n=\alpha_1 v_1$. $\alpha_1=0$.
$v_1, \cdots\cdots, v_n$ are linearly independent. $v_1, \cdots \cdots, v_n$ is a basis of V since dim V=n.

4. Give a proof, using matrix computations, that if A is a triangular $n \times n$ matrix with entries $\lambda_1, \ldots, \lambda_n$ on the diagonal, then

$$(A-\lambda_1)(A-\lambda_2)\cdots(A-\lambda_n)=0.$$

290.4 Let $A=\begin{pmatrix} \lambda_1 & & & 0 \\ a_{21} & \lambda_2 & & \\ a_{31} & a_{32} & \lambda_3 & \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots\cdots & \lambda_n \end{pmatrix}$

$$(A-\lambda_1)(A-\lambda_2)=\begin{pmatrix} 0 & & & \\ a_{21} & (\lambda_2-\lambda_1) & & \\ a_{31} & a_{32} & (\lambda_3-\lambda_1) & \\ \vdots & & & \\ a_{n1} & a_{n2} & & (\lambda_n-\lambda_1) \end{pmatrix}\cdot$$

$$\begin{pmatrix} (\lambda_1-\lambda_2) & & & \\ a_{21} & 0 & & \\ a_{31} & a_{32} & (\lambda_3-\lambda_2) & \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots\cdots & (\lambda_n-\lambda_2) \end{pmatrix}$$

$$=\begin{pmatrix} & & 0 & \\ & & 0 & \\ a_{31}(\lambda_1-\lambda_2)+a_{32}a_{21}+(\lambda_3-\lambda_1)a_{31} & & 0 & \\ a_{n1}(\lambda_1-\lambda_2)+a_{n2}a_{21}+\cdots+(\lambda_n-\lambda_1)a_{n1} & \cdots & (\lambda_n-\lambda_1)(\lambda_n-\lambda_2) & \end{pmatrix}.$$

$\cdots\cdots, (A-\lambda_1)(A-\lambda_2)\cdots\cdots(A-\lambda_n)=0$,

*5. If $T \in F_n$ has minimal polynomial $p(x)$ over F, prove that every root of $p(x)$, in its splitting field K, is a characteristic root of T.

290.5 Let $(K:F)=m$ and $e_1, \cdots\cdots, e_n$ be a basis of K over F. Let p(x) be the minimal polyomial for T over F and q(x) the minimal polynomid for T over K. Clearly $q(x) \mid p(x)$. Suppose deg $q(x)=l$.
$q(x)=a_l x^l+a_{l-1}x^{l-1}+\cdots\cdots+a_0$, $a_i \in K$.

$$a_i=\sum_{t=1}^{m} a_{it}e_t,\quad a_{it} \in F,\quad 0 \le i \le l,\quad 1 \le t \le m.$$

$$0=q(A)=\sum_{t=1}^{m} a_{lt}e_t A^l+\sum_{t=1}^{m} a_{l-1\,t}e_t A^{l-1}+\cdots\cdots+\sum_{t=1}^{m} a_{0t}e_t$$

$=(\sum_{i=0}^{l} a_{i1}A^i)e_1+(\sum_{i=0}^{l} a_{i2}A^i)e_2+\cdots\cdots+(\sum_{i=0}^{l} a_{im}A^i)e_m$.

Hence $\sum_{i=0}^{l} a_{ik}A^i=0$, $1\leq k\leq m$.

$a_l\neq 0$ implies $a_{lt}\neq 0$ for some t.

A satisfies $\sum_{i=0}^{l} a_{it}x^i=a_{lt}x^l+a_{l-1\,t}x^{l-1}+\cdots\cdots+a_{0t}$.

$l\geq$ degree of p(x). deg q(x)$\geq$ deg p(x). q(x)= p(x)(suppose p(x) and q(x) are both monic). Hence the root of p(x) must be a characteristic root of T over K by the proof of (272.2).

6. If $T\in A(V)$ and if $\lambda\in F$ is a characteristic root of T in F, let $U_\lambda=\{v\in V\mid vT=\lambda v\}$. If $S\in A(V)$ commutes with T, prove that U_λ is invariant under S.

290.6 $v\in U\lambda$, $(vS)T=v(ST)=v(TS)=(vT)S=(\lambda v)S=\lambda(vS)$, $vS\in U\lambda$. $U\lambda$ is invariant under S.

*7. If $\mathscr{M}$ is a commutative set of elements in $A(V)$ such that every $M\in\mathscr{M}$ has all its characteristic roots in F, prove that there is a $C\in A(V)$ such that every CMC^{-1}, for $M\in\mathscr{M}$, is in triangular form.

290.7 Use induction on dim V=k. If k=1, we are done.

(i) Suppose for all M in $\mathscr{M}$, $U\lambda=V$ for a characteristic root λ of M, $U\lambda=V$ implies $M=\lambda$ and every element in M is scalar. In this case we are done.

(ii) Suppose that there is an M in $\mathscr{M}$ such that $U\lambda\neq V$ for a characteristic root of M. By (290.6), $U\lambda$ is invariant under $\mathscr{M}$. Every element S of $\mathscr{M}$ induces a linear transformation $\overline{S}$ on $V/U\lambda$, defined by $(v+U\lambda)\overline{S}=vS+U\lambda$ and the minimal polynomial of $\overline{S}$ divides that for S.

$\overline{\mathscr{M}}=\{\overline{M}\mid M\in\mathscr{M}\}$ is a commutative set of elements in A ($V/U\lambda$) and every element $\overline{M}$ in $\overline{\mathscr{M}}$ has all its characteristic roots in F. r=dim $V/U\lambda$

$<$ dim V. By induction hypothesis, there is a basis $\bar{v}_{n-r+1}$, $\bar{v}_{n-r+2}$, $\cdots\cdots$, $\bar{v}_n$ of $V/U\lambda$ over F such that for all S in $\mathscr{M}$ we have

$\bar{v}_{n-r+1}\overline{S}=\alpha^{(s)}_{n-r+1\;n-r+1}\bar{v}_{n-r+1}$

$\bar{v}_{n-r+2}\overline{S}=\alpha^{(s)}_{n-r+2\;n-r+1}\bar{v}_{n-r+1}+\alpha^{(s)}_{n-r+2\;n-r+2}\bar{v}_{n-r+2}$

$\vdots$

$\bar{v}_n\overline{S}=\alpha^{(s)}_{n\,n-r+1}\bar{v}_{n-r+1}+\alpha^{(s)}_{n\,n-r+2}\bar{v}_{n-r+2}+\cdots\cdots+\alpha^{(s)}_{n\,n}\bar{v}_n$.

Eeery element S of $\mathscr{M}$ induces a linear transformation $\overline{S}$ on $U\lambda$, defined by $v\overline{S}=vS$. The characteristic roots of $\overline{S}$ are also characteristic roots of S.

$\overline{\mathscr{M}}=\{\overline{M}\mid M\in\mathscr{M}\}$ is a commutative set of elements in A($U\lambda$) and every element $\overline{M}$ in $\overline{\mathscr{M}}$ has all its characteristic roots in F.

dim $U\lambda<$ dim V since $U\lambda\neq V$.

By induction hypothesis, there is a basis $v_1, v_2, \cdots\cdots, v_{n-r}$ of $U\lambda$ over F such that for all S in M we have

$v_1\overline{S}=\alpha^{(s)}_{11}v_1$

$v_2\overline{S}=\alpha^{(s)}_{21}v_1+\alpha^{(s)}_{22}v_2$

$\vdots$

$v_{n-r}\overline{S}=\alpha(s)_{n-r\,1}v_1+\alpha(s)_{n-r\,2}v_2+\cdots\cdots+\alpha^{(s)}_{n-r\,n-r}v_{n-r}$

Then $v_1, \cdots\cdots, v_n$ form a basis of V. For, if $\alpha_1v_1+\alpha_2v_2+\cdots\cdots+\alpha_nv_n=0$ for some α_i in F, then

$0=\alpha_1\bar{v}_1+\alpha_2\bar{v}_2+\cdots\cdots+\alpha_n\bar{v}_n$

$=\alpha_{n-r+1}\bar{v}_{n-r+1}+\cdots\cdots+\alpha_n\bar{v}_n$.

$\alpha_{n-r+1}=\alpha_{n-r+2}=\cdots\cdots=\alpha_n=0$ since $\bar{v}_{n-r+1}, \cdots\cdots, \bar{v}_n$ are linearly independent over F.

$0=\alpha_1 v_1+\cdots\cdots+\alpha_n v_n=\alpha_1 v_1+\cdots\cdots+\alpha_{n-r} v_{n-r}$.
$\alpha_1=\cdots\cdots=\alpha_{n-r}=0$ since $v_1, \cdots\cdots, v_{n-r}$ are linearly independent over F.
Hence $v_1, \cdots\cdots, v_n$ are linearly independent over F. dim V=n. $v_1, \cdots\cdots, v_n$ form a basis of V over F. For any S in $\mathcal{M}$,

$v_1 S=v_1\overline{S}=\alpha_{11}^{(s)} v_1$

$\vdots$

$v_{n-r} S=v_{n-r}\overline{S}=\alpha_{n-r\,1}^{(s)} v_1+\alpha_{n-r\,2}^{(s)} v_2+\cdots\cdots+\alpha_{n-r\,n-r}^{(s)} v_{n-r}$.

$v_{n-r+1}\overline{S}-\alpha_{n-r+1\,n-r+1}^{(s)}\overline{v}_{n-r+1}=0$

$v_{n-r+1} S-\alpha_{n-r+1\;n+r+1}^{(s)} v_{n-r+1}\in U_\lambda$,

$v_{n-r+1} S=\alpha_{n-r+1\,1}^{(s)} v_1+\alpha_{n-r+1\;2}^{(s)} v_2+\cdots\cdots+\alpha_{n-r+1\;n-r+1}^{(s)} v_{n-r+1}$.

Similarly, $v_1 S=\alpha_{11}^{(s)} v_1+\cdots\cdots+\alpha_{1\,1}^{(s)} v_1$
Therefore, the matrix of S in this basis is triangular. This completes the induction and proves this exercic .

8. Let W be a subspace of V invariant under $T\in A(V)$. By restricting T to W, T induces a linear transformation $\tilde{T}$ (defined by $w\tilde{T}=wT$ for every $w\in W$). Let $\tilde{p}(x)$ be the minimal polynomial of $\tilde{T}$ over F.
   (a) Prove that $\widetilde{p(x)}\mid p(x)$, the minimal polynomial of T over F.
   (b) If T induces $\bar{T}$ on V/W satisfying the minimal polynomial $\bar{p}(x)$ over F, prove that $p(x)\mid\tilde{p}(x)\bar{p}(x)$.
   *(c) If $\tilde{p}(x)$ and $\bar{p}(x)$ are relatively prime, prove that $p(x)=\tilde{p}(x)\bar{p}(x)$.
   *(d) Give an example of a T for which $p(x)\neq\tilde{p}(x)\bar{p}(x)$.

290.8 (a) $p(T)=0$, $p(\widetilde{T})=p(T)=0$, $p(\widetilde{x})\mid p(x)$.
(b) For $v\in V$, $0=\overline{v}\,\overline{p}(\overline{T})=v\bar{p}(T)+W$.
$v\bar{p}(T)\in W$.

$0=(v\bar{p}(T))\,\widetilde{p}(\widetilde{T})=v\bar{p}(T)\widetilde{p}(T)$.

$v\bar{p}(T)\widetilde{p}(T)=0$ for all v in V.

$p(x)\mid\widetilde{p}(x)\overline{p}(x)$ since $p(x)$ is the minimal polynomial for T.
(c) By Lemma 6.4.1 and (290.8(a)), $\bar{p}(x)\mid p(x)$ and $\widetilde{p}(x)\mid p(x)$.
Since $\bar{p}(x)$ and $\widetilde{p}(x)$ are relatively prime, $\widetilde{p}(x)\bar{p}(x)\mid p(x)$. By (290.8.(b)),
$p(x)=\widetilde{p}(x)\bar{p}(x)$.
(d) Let $W=\{(\alpha,0,0)\mid\alpha\in F\}$.

$$T=\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}.$$

$p(x)=(x-1)(x+1)$. $\widetilde{T}=I$, $\widetilde{p}(x)=x-1$.

$$\bar{T}=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad \bar{p}(x)=(x+1)(x-1).$$

$\bar{p}(x)\widetilde{p}(x)=(x+1)(x-1)^2\neq(x+1)(x-1)=p(x)$.

9. Let $\mathcal{M}$ be a nonempty set of elements in $A(V)$; the subspace $W\subset V$ is said to be *invariant under* $\mathcal{M}$ if for every $M\in\mathcal{M}$, $WM\subset W$. If W is invariant under $\mathcal{M}$ and is of dimension r over F, prove that there exists a basis of V over F such that every $M\in\mathcal{M}$ has a matrix, in this basis, of the form

$$\left(\begin{array}{c|c}M_1&0\\\hline M_{12}&M_2\end{array}\right),$$

where M_1 is an $r\times r$ matrix and M_2 is an $(n-r)\times(n-r)$ matrix.

290.9 Let $\{w_1, \cdots\cdots, w_r\}$ be a basis of W.
By Lemma 4.2.5, we can find vectors $w_{r+1}, \cdots\cdots, w_n$ in V such that $\{w_1, \cdots\cdots, w_n\}$ form a basis of V.
Under this basis, every M in $\mathcal{M}$ is of the form

$$\begin{pmatrix}M_1&0\\M_{12}&M_2\end{pmatrix},$$

where M_1 is an $r\times r$ matrix and M_2 is an $(n-r)\times(n-r)$ matrix.

10. In Problem 9 prove that M_1 is the matrix of the linear transformation $\tilde{M}$ induced by M on W, and that M_2 is the matrix of the linear transformation $\bar{M}$ induced by M on V/W.

291.10 It's clear that M_1 is the matrix of the linear transformation $\tilde{M}$ induced by M on W.
Since $\{w_{r+1}+W, w_{r+2}+W, \cdots\cdots, w_n+W\}$ foms a basis of V/W, the matrix of the linear transformation $\bar{M}$ induced by M on V/W is M_2.

*11. The nonempty set, $\mathscr{M}$, of linear transformations in $A(V)$ is called an *irreducible* set if the only subspaces of V invariant under $\mathscr{M}$ are (0) and V. If $\mathscr{M}$ is an irreducible set of linear transformations on V and if

$$D = \{T \in A(V) \mid TM = MT \text{ for all } M \in \mathscr{M}\},$$

prove that D is a division ring.

291.11 Evidently, D is a subring of A(V). We need to prove that for every nonzero element T in D, there is an element T^{-1}, the inverse of T, in D. In fact, we need only show that T^{-1} exists in A(V). For, if $T^{-1} \in A(V)$, $TM=MT$ implies $MT^{-1}=T^{-1}M$ for all M in $\mathscr{M}$ and $T^{-1} \in D$.
$VT \neq 0$. VT is invariant under $\mathscr{M}$.
For $(VT)M=V(TM)=V(MT)=(VM)T \subset VT$.
Since $\mathscr{M}$ is irreducible and $VT \neq 0$, we have $VT=V$ and T is onto. The kernel W of T is a subspace of V. W is invariant under $\mathscr{M}$. For, if $\omega \in W$ and $M \in \mathscr{M}$, then $(\omega M)T=(\omega T)M=0$, $\omega M \in W$. $W \neq V$, otherwise $T=0$. Since M is irreducible, $W=0$ and T is one-to-one.
T has an inverse in A(V). This compltes the proof.

*12. Do Problem 11 by using the result (Schur's lemma) of Problem 14, end of Chapter 4, page 206.

291.12 First of all, V can be viewed as a right A(V)-module. Since $\mathscr{M}$ is irreducible, $\bar{\mathscr{M}}$, the subalgebra of A(V) genertd by $\mathscr{M}$, is also irreducible. V can be viewed as a right $\bar{\mathscr{M}}$-module. V is an irreducible $\bar{\mathscr{M}}$-module. Now, we say that E(V) is just D. For, $E \in E(V)$, $v(ME)=(vM)E=(vE)M=v(EM)$ for all v in V. $ME=EM$ for all M in $\bar{\mathscr{M}}$. $E \in D$.
If $E' \in D$, then $(vM)E'=v(ME')=v(E'M)=(vE')M$, E' is an $\bar{\mathscr{M}}$-homomorphism, $E' \in E(M)$. By Schur's Lemma $D=E(M)$ is a division ring since $V\bar{\mathscr{M}} \neq 0$.

*13. If F is such that all elements in $A(V)$ have all their characteristic roots in F, prove that the D of Problem 11 consists only of scalars.

291.13 $T \in D$, $T \neq 0$. Let λ be one characteristic root of T. By (290.6), $U\lambda \neq 0$ is invariant under $\mathscr{M}$. $U\lambda=V$. $T=\lambda$.

14. Let F be the field of real numbers and let

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in F_2.$$

(a) Prove that the set $\mathscr{M}$ consisting only of

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

is an irreducible set.

(b) Find the set D of all matrices commuting with

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and prove that D is isomorphic to the field of complex numbers.

291.14 (a) Let $U \neq 0$ be an $\mathscr{M}$ invariant subspace of $V=F^{(2)}$. Let $0 \neq (\alpha, \beta) \in U$.

$$(\alpha, \beta)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (-\beta, \alpha) \in U.$$

(α, β), $(-\beta, \alpha)$ are linearly independent.
$U=V$. $\mathscr{M}$ is irreducible.

(b) $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in D$.

$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}\alpha&\gamma\\\beta&\delta\end{pmatrix}=\begin{pmatrix}\alpha&\gamma\\\beta&\delta\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}.$$

$$\begin{pmatrix}\beta&\delta\\-\alpha&-\gamma\end{pmatrix}=\begin{pmatrix}-\gamma&\alpha\\-\delta&\beta\end{pmatrix}.$$

$\gamma=-\beta$, $\delta=\alpha$.

$$\begin{pmatrix}\alpha&\gamma\\\beta&\delta\end{pmatrix}=\begin{pmatrix}\alpha&-\beta\\\beta&\alpha\end{pmatrix}.$$

By (283.16), D is isomorphic to the field of complex numbers.

15. Let F be the field of real numbers.

(a) Prove that the set

$$\mathscr{M}=\left\{\begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&1\\0&0&-1&0\end{pmatrix},\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&-1&0&0\\-1&0&0&0\end{pmatrix}\right\}$$

is an irreducible set.

(b) Find all $A\in F_4$ such that $AM=MA$ for all $M\in\mathscr{M}$.

(c) Prove that the set of all A in part (b) is a division ring isomorphic to the division ring of quaternions over the real field.

291.15 (a)

Let $i=\begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&1\\0&0&-1&0\end{pmatrix}$,

$j=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&-1&0&0\\-1&0&0&0\end{pmatrix}$.

$k=ij=\begin{pmatrix}0&0&1&0\\0&0&0&-1\\-1&0&0&0\\0&1&0&0\end{pmatrix}$.

A simple computation shows that $i^2=j^2=k^2=-1$, $ij=-ji=k$, $jk=-kj=i$, $ki=-ik=j$.

Suppose $U\neq 0$ is an $\mathscr{M}$-invariant subspace of $V=F^{(4)}$. $0\neq v\in U$. vi, vj, vk are also in U since U is $\mathscr{M}$-invariant. We can show that v, vi, vj, vk are linearly indendent. For, if $\alpha v+\beta vi+\gamma vj+\delta vk=0$ for some $\alpha,\beta,\gamma,\delta$ in F, then $v(\alpha+\beta i+\gamma j+\delta k)(\alpha-\beta i+\gamma j+\delta k)=0$.

$v(\alpha^2+\beta^2+\gamma^2+\delta^2)\cdot 1=0$.

$(\alpha^2+\beta^2+\gamma^2+\delta^2)v=0$.

$v\neq 0$ implies $\alpha^2+\beta^2+\gamma^2+\delta^2=0$ and $\alpha=\beta=\gamma=\delta=0$.

$v, vi, vj, vk\in U$ are linearly independence over F. $U=F^{(4)}$. $\mathscr{M}$ is irreducible.

(b)(c)

$$\begin{pmatrix}\alpha_{11}&\alpha_{12}&\alpha_{13}&\alpha_{14}\\\alpha_{21}&\alpha_{22}&\alpha_{23}&\alpha_{24}\\\alpha_{31}&\alpha_{32}&\alpha_{33}&\alpha_{34}\\\alpha_{41}&\alpha_{42}&\alpha_{43}&\alpha_{44}\end{pmatrix}\in D$$

$$\begin{pmatrix}\alpha_{11}&\alpha_{12}&\alpha_{13}&\alpha_{14}\\\alpha_{21}&\alpha_{22}&\alpha_{23}&\alpha_{24}\\\alpha_{31}&\alpha_{32}&\alpha_{33}&\alpha_{34}\\\alpha_{41}&\alpha_{42}&\alpha_{43}&\alpha_{44}\end{pmatrix}\begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&1\\0&0&-1&0\end{pmatrix}$$

$$=\begin{pmatrix}-\alpha_{12}&\alpha_{11}&-\alpha_{14}&\alpha_{13}\\-\alpha_{22}&\alpha_{21}&-\alpha_{24}&\alpha_{23}\\-\alpha_{32}&\alpha_{31}&-\alpha_{34}&\alpha_{33}\\-\alpha_{42}&\alpha_{41}&-\alpha_{44}&\alpha_{43}\end{pmatrix}$$

$$=\begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&1\\0&0&-1&0\end{pmatrix}\begin{pmatrix}\alpha_{11}&\alpha_{12}&\alpha_{13}&\alpha_{14}\\\alpha_{21}&\alpha_{22}&\alpha_{23}&\alpha_{24}\\\alpha_{31}&\alpha_{32}&\alpha_{33}&\alpha_{34}\\\alpha_{41}&\alpha_{42}&\alpha_{43}&\alpha_{44}\end{pmatrix}$$

$$=\begin{pmatrix}\alpha_{21}&\alpha_{22}&\alpha_{23}&\alpha_{24}\\-\alpha_{11}&-\alpha_{12}&-\alpha_{13}&-\alpha_{14}\\\alpha_{41}&\alpha_{42}&\alpha_{43}&\alpha_{44}\\-\alpha_{31}&-\alpha_{32}&-\alpha_{33}&-\alpha_{34}\end{pmatrix}$$

Hence $\alpha_{21}=-\alpha_{12}$, $\alpha_{22}=\alpha_{11}$, $\alpha_{23}=-\alpha_{14}$, $\alpha_{24}=\alpha_{13}$ $\alpha_{41}=-\alpha_{32}$, (*)……

$\alpha_{42}=\alpha_{31}$ $\alpha_{43}=-\alpha_{34}$, $\alpha_{44}=\alpha_{33}$

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} -\alpha_{14} & -\alpha_{13} & \alpha_{12} & \alpha_{11} \\ -\alpha_{24} & -\alpha_{23} & \alpha_{22} & \alpha_{21} \\ -\alpha_{34} & -\alpha_{33} & \alpha_{32} & \alpha_{31} \\ -\alpha_{44} & -\alpha_{43} & \alpha_{42} & \alpha_{41} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ -\alpha_{21} & -\alpha_{22} & -\alpha_{23} & -\alpha_{24} \\ -\alpha_{11} & -\alpha_{12} & -\alpha_{13} & -\alpha_{14} \end{pmatrix}$$

Hence $\alpha_{14}=-\alpha_{41}$, $\alpha_{13}=-\alpha_{42}$, $\alpha_{43}=\alpha_{12}$, $\alpha_{44}=\alpha_{11}$, $\alpha_{24}=-\alpha_{31}$, $\alpha_{32}=-\alpha_{23}$, $\alpha_{33}=\alpha_{22}$, $\alpha_{34}=\alpha_{21}$, ... (**)

By (*) and (**) we have

$\alpha_{21}=-\alpha_{12}=-\alpha_{43}=\alpha_{34}=-\beta$

$\alpha_{11}=\alpha_{22}=\alpha_{33}=\alpha_{44}=\alpha$

$\alpha_{23}=-\alpha_{14}=\alpha_{41}=-\alpha_{32}=-\delta$

$\alpha_{24}=\alpha_{13}=-\alpha_{42}=-\alpha_{31}=\gamma$.

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} \\ \alpha_{41} & \alpha_{42} & \alpha_{43} & \alpha_{44} \end{pmatrix} = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ -\beta & \alpha & -\delta & \gamma \\ -\gamma & \delta & \alpha & -\beta \\ -\delta & -\gamma & \beta & \alpha \end{pmatrix}$$

By (283.17), D is isomorphic to the division ring of quaternions over the real field.

16. A set of linear transformations, $\mathscr{M} \subset A(V)$, is called *decomposable* if there is a subspace $W \subset V$ such that $V = W \oplus W_1$, $W \neq (0)$, $W \neq V$, and each of W and W_1 is invariant under $\mathscr{M}$. If $\mathscr{M}$ is not decomposable, it is called *indecomposable*.

(a) If $\mathscr{M}$ is a decomposable set of linear transformations on V, prove that there is a basis of V in which every $M \in \mathscr{M}$ has a matrix of the form

$$\left(\begin{array}{c|c} M_1 & 0 \\ \hline 0 & M_2 \end{array}\right),$$

where M_1 and M_2 are square matrices.

(b) If V is an n-dimensional vector space over F and if $T \in A(V)$ satisfies $T^n = 0$ but $T^{n-1} \neq 0$, prove that the set $\{T\}$ (consisting of T) is indecomposable.

291.16 (a) $V=W\oplus W_1$, $W\neq(0)$, $W\neq V$. Let $\{w_1, \ldots, w_r\}$, $\{w_{r+1}, \ldots, w_n\}$ be bases of W and W_1, respectively. $\{w_1, \ldots, w_n\}$ is a basis of V. Under this basis, every element is of the form

$$\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix}$$

where M_1 is an $r\times r$ matrix and M_2 is an $(n-r)\times(n-r)$ matrix.

(b) If $\{T\}$ is decomposable, then $V=W_1\oplus W_2$, $W_1\neq(0)$, $W_1\neq V$. T can be induced to T_1, the linear transformation of W_1, and to T_2, the linear transformation of W_2. Since $W_1\neq(0)$, $W_1\neq V$, $\dim W_1=r_1$, $\dim W_2=r_2$, $0<r_1, r_2<n$. Since $T^n=0$, ${T_1}^n={T_2}^n=0$. By (273.8), ${T_1}^{r_1}{T_1}^{r_2}=0$. Every element v of V is the form $v=w_1+w_2$, where $w_1\in W_1$, $w_2\in W_2$. Let $r=\max(r_1,r_2)$, $r<n$. $vT^r=w_1T^r+w_2T^r=w_1{T_1}^r+w_2{T_2}^r=0+0=0$. Hence $T^r=0$, contrary to the fact that $T^{n-1}\neq 0$. Hence $\{T\}$ is indecomposable.

17. Let $T \in A(V)$ and suppose that $p(x)$ is the minimal polynomial for T over F.

(a) If $p(x)$ is divisible by two distinct irreducible polynomials $p_1(x)$ and $p_2(x)$ in $F[x]$, prove that $\{T\}$ is decomposable.

(b) If $\{T\}$, for some $T \in A(V)$ is indecomposable. prove that the minimal polynomial for T over F is the power of an irreducible

polynomial.

292.17 (a) Since $p(x)$ is divisible by two distinct irreducible polynomials $p_1(x)$ and $p_2(x)$ in $F[x]$, $p(x)=r(x)s(x)$ for some $r(x), s(x)$ in $F[x]$ such that $\deg r(x) < \deg p(x)$, $\deg s(x) < \deg p(x)$ and $r(x)$ and $s(x)$ are relatively prime. Let W_1 be the kernel of $r(T)$ and W_2 the kernel of $s(T)$. W_1 and W_2 are subspace of V. $W_1 \neq V$ and $W_2 \neq V$. For, if $W_1 = V$, then $r(T)=0$, $p(x) \mid r(x)$. $r(x) \mid p(x)$. $\deg r(x) = \deg p(x)$, a contradiction. Hence $W_1 \neq V$ and similarly $W_2 \neq V$. Since $r(x)$ and $s(x)$ are relatively prime, there are $a(x)$ and $b(x)$ in $F[x]$ such that $1=r(x)a(x)+s(x)b(x)$. $I=r(T)a(T)+s(T)b(T)$. For $v \in V$, $v=vr(T)a(T)+vs(T)b(T)$. $(vr(T)a(T))s(T)=(va(T))r(T)s(T)=(va(T))(p(T))=v(a(T))0=0$, $vr(T)a(T) \in W_2$. Similarly, $vs(T)b(T) \in W_1$. $V=W_1+W_2$. If $v \in W_1 \cap W_2$, then $v=vr(T)a(T)+vs(T)b(T) = 0a(T)+0b(T)=0+0=0$. $W_1 \cap W_2 = (0)$. $V=W_1 \oplus W_2$. $\{T\}$ is decomposable.

(b) If $p(x)$ is not the power of an irreducible polynomial, then, by (a), $\{T\}$ is decomposable. Hence, $p(x)$ is the power of an irreducible polynomial.

18. If $T \in A(V)$ is nilpotent, prove that T can be brought to triangular form over F, and in that form all the elements on the diagonal are 0.

292.18 That T is nilpotent implies $T^r=0$ for some positive integer r. T satisfies x^r. Let $p(x)$ be the minimal polynomial for T. $p(x) \mid x^r$. $p(x)=x^s$ for some positive integer s. Hence, all the charateristic roots of T are in F. By Theorem 6.4.1. and the proof of

Theorem 6.4.2, we get the result of this exercise.

19. If $T \in A(V)$ has only 0 as a characteristic root, prove that T is nilpotent.

292.19 By the proof of Theorem 6.4.2, we have that $T^n=0$. T is nilpotent.

6.6. Canonical Forms: Decomposition of V: Jordan Form.

1. If S and T are nilpotent linear transformations which commute, prove that ST and $S+T$ are nilpotent linear transformations.

303.1 Suppose $S^m=0$, $T^n=0$. $(ST)^m=S^mT^m=0$. $(S+T)^{m+n+1}=0$. ST and S+T are nilpotent.

2. By a direct matrix computation, show that

$$\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \text{ and } \begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\0&0&0&0\end{pmatrix}$$

are not similar.

303.2 Suppose there is an $A=(a_{ij})$ in F_4 such that

$$A\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&0\\0&0&0&0\end{pmatrix}A^{-1}=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\0&0&0&0\end{pmatrix}$$

$$A\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&0\\0&0&0&0\end{pmatrix}=\begin{pmatrix}0&a_{11}&a_{12}&0\\0&a_{21}&a_{22}&0\\0&a_{31}&a_{32}&0\\0&a_{41}&a_{42}&0\end{pmatrix}$$

$$=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\0&0&0&0\end{pmatrix}A=\begin{pmatrix}a_{21}&a_{22}&a_{23}&a_{24}\\a_{31}&a_{32}&a_{33}&a_{34}\\a_{41}&a_{42}&a_{43}&a_{44}\\0&0&0&0\end{pmatrix}$$

$a_{41}=a_{44}=0$, $a_{42}=a_{31}=0$, $a_{43}=a_{32}=a_{21}=0$.
A cannot be invertible, a contradiction.

3. If $n_1 \geq n_2$ and $m_1 \geq m_2$, by a direct matrix computation prove that

$$\begin{pmatrix}M_{n_1}&\\&M_{n_2}\end{pmatrix} \text{ and } \begin{pmatrix}M_{m_1}&\\&M_{m_2}\end{pmatrix}$$

are similar if and only if $n_1 = m_1$, $n_2 = m_2$.

303.3 Suppose there is an $A=(a_{ij})$ in F_n such that

$$A\begin{pmatrix}M_{n_1}&\\&M_{n_2}\end{pmatrix}A^{-1}=\begin{pmatrix}M_{m_1}&\\&M_{m_2}\end{pmatrix}.$$

$$A\begin{pmatrix}M_{n_1}&\\&M_{n_2}\end{pmatrix}$$

$$=\begin{pmatrix}0&a_{11}&a_{12}&\cdots&a_{1n_1-1}&0&a_{1n_1+1}&\cdots\cdots&a_{1n-1}\\0&a_{21}&a_{22}&\cdots&a_{2n_1-1}&)&a_{2n_1+1}&\cdots\cdots&a_{2n-1}\\\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots&&\vdots\\0&a_{n1}&a_{n2}&\cdots&a_{nn_1-1}&0&a_{nn_1+1}&\cdots\cdots&a_{nn-1}\end{pmatrix}$$

$$=\begin{pmatrix}M_{m_1}&\\&M_{m_2}\end{pmatrix}A=\begin{pmatrix}a_{21}&a_{22}&\cdots\cdots\cdots&a_{2n}\\a_{31}&a_{32}&\cdots\cdots\cdots&a_{3n}\\\vdots&\vdots&&\vdots\\a_{m_1 1}&a_{m_1 2}&\cdots\cdots\cdots&a_{m_1 n}\\0&0&\cdots\cdots\cdots&0\\a_{m_1+21}&a_{m_1+22}&\cdots\cdots&a_{m_1+2n}\\\vdots&\vdots&&\vdots\\a_{n1}&a_{n2}&&a_{nn}\\0&0&&0\end{pmatrix}$$

Suppose $m_1 > n_1 \geq n_2$. $a_{m_1 1}=0$, $a_{m_1 2}=a_{m_1-11}=0$, $a_{m_1 3}=a_{m_1-12}=a_{m_1-21}=0$, $\cdots\cdots$, $a_{m_1 n_1}=a_{m_1-1\,n_1-1}=\cdots=a_{m_1-n_1+11}=0$. $a_{m_1 n_1+1}=0$, $a_{m_1 n_1+2}=a_{m_1-1\,n_1+1}=0$, $\cdots$, $a_{m_1 n}=a_{m_1-1\,n-1}=\cdots\cdots=a_{m_1-n_2+1\,n_1+1}=0$. $a_{m_1 1}=a_{m_1 2}=\cdots\cdots=a_{m_1 n}=0$. A can not be inver-tible, a contradiction.

Hence $m_1 \geq n_1$. Similarly, $n_1 \geq m_1$. $n_1=m_1$. $n_2=n-n_1=n-m_1=m_2$. Conversely, if $n_1=m_1$, $n_2=m_2$, then $\begin{pmatrix}M_{n_1}&\\&M_{n_2}\end{pmatrix}=\begin{pmatrix}M_{m_1}&\\&M_{m_2}\end{pmatrix}$. This complctes the proof.

*4. If $n_1 \geq n_2 \geq n_3$ and $m_1 \geq m_2 \geq m_3$, by a direct matrix computation prove that

$$\begin{pmatrix}M_{n_1}&&\\&M_{n_2}&\\&&M_{n_3}\end{pmatrix} \text{ and } \begin{pmatrix}M_{m_1}&&\\&M_{m_2}&\\&&M_{m_3}\end{pmatrix}$$

are similar if and only if $n_1 = m_1$, $n_2 = m_2$, $n_3 = m_3$.

303.4 Suppose there is an $A=(a_{ij})$ in F_n such that

$$A\begin{pmatrix} M_{n_1} & & \\ & M_{n_2} & \\ & & M_{n_3} \end{pmatrix}A^{-1}=\begin{pmatrix} M_{m_1} & & \\ & M_{m_2} & \\ & & M_{m_3} \end{pmatrix}.$$

$$A\begin{pmatrix} M_{n_1} & & \\ & M_{n_2} & \\ & & M_{n_3} \end{pmatrix} = \begin{pmatrix} M_{m_1} & & \\ & M_{m_2} & \\ & & M_{m_3} \end{pmatrix} A$$

$$\begin{pmatrix} 0 & a_{11} & a_{12} & \cdots & a_{1n_1-1} & 0 & a_{1n_1+1} & \cdots & a_{1n_1+n_2-1} & \cdots & 0 \\ 0 & a_{21} & a_{22} & \cdots & a_{2n_1-1} & 0 & a_{2n_1+1} & \cdots & a_{2n_1+n_2-1} & & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & a_{n1} & a_{n2} & \cdots & a_{nn_1-1} & 0 & a_{nn_1+1} & \cdots & a_{nn_1+n_2-1} & & 0 \end{pmatrix}$$

$$\begin{pmatrix} a_{1n_1+n_2+1} & \cdots & a_{1n-1} \\ a_{2n_1+n_2+1} & \cdots & a_{2n-1} \\ & \vdots & \\ a_{nn_1+n_2+1} & \cdots & a_{nn-1} \end{pmatrix}$$

$$= \begin{pmatrix} a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & & \vdots \\ a_{m_1 1} & a_{m_1 2} & \cdots & a_{m_1 n} \\ 0 & 0 & \cdots & 0 \\ a_{m_1+21} & a_{m_1+22} & \cdots & a_{m_1+2n} \\ \vdots & \vdots & & \vdots \\ a_{m_1+m_2 1} & a_{m_1+m_2 2} & \cdots & a_{m_1+m_2 n} \\ 0 & 0 & \cdots & 0 \\ a_{m_1+m_2+21} & a_{m_1+m_2+22} & \cdots & a_{m_1+m_2+2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

If $m_1 > n_1$, then $m_1 > n_1 \geq n_2 \geq n_3$.

$a_{m_1 1}=0$, $a_{m_1 2}=a_{m_1-1\,1}=0$, $\cdots\cdots$, a_{m_1,n_1}
$=a_{m_1-1\,n_1-1}=\cdots\cdots=a_{m_1-n_1+1\,1}=0$, $a_{m_1 n_1+1}=0$,
$a_{m_1 n_1+2}=a_{m_1-1\,n_1+1}=0$, $\cdots\cdots$, $a_{m_1 n_1+n_2}=$

$a_{m_1-1\,n_1+n_2-1}=\cdots\cdots=a_{m_1-n_2+1\,n_1+1}=0$,
$a_{m_1 n_1+n_2+1}=0$, $a_{m_1 n_1+n_2+2}=a_{m_1-1\,n_1+n_2+1}=0$,
$a_{m_1 n_1+n_2+n_3}=a_{m_1-1\,n_1+n_2+n_3-1}=\cdots\cdots\cdots\cdots$
$=a_{m_1-n_3+1\;n_1+n_2+1}=0$.
$a_{m_1 1}=a_{m_1 2}=\cdots\cdots=a_{m_1 n}=0$. A cannot be invertible, a contradiction. Hence $m_1 \leq n_1$. Similarly, $m_1 \geq n_1$. $m_1=n_1$. If $m_2 > n_2$, then $m_2 > n_2 \geq n_3$.
$a_{m_1+m_2 1}=0$, $a_{m_1+m_2 2}=a_{m_1+m_2-1\,1}=0$, $\cdots\cdots$
$a_{m_1+m_2\;n_1}=a_{m_1+m_2-n_1+1\,1}=0$.
$a_{m_1+m_2 n_1+1}=0$, $a_{m_1+m_2 n_1+2}=a_{m_1+m_2-1\,n_1+1}=0$, $\cdots\cdots$,
$a_{m_1+m_2 n}=0$.

$a_{m_1+m_2 1}=a_{m_1+m_2 2}=\cdots\cdots=a_{m_1+m_2 n}=0$. A can not be invertible, a contradiction. Hence $m_2 \leq n_2$.
Similarly $m_2 \geq n_2$. $m_2=n_2$. $m_3=n-(m_1+m_2)$
$=n-(n_1+n_2)=n_3$. $n_1=m_1$, $n_2=m_2$, $n_3=m_3$.
Conversely, if $n_1=m_1$, $n_2=m_2$, $n_3=m_3$, then

$$\begin{pmatrix} M_{n_1} & & \\ & M_{n_2} & \\ & & M_{n_3} \end{pmatrix} = \begin{pmatrix} M_{m_1} & & \\ & M_{m_2} & \\ & & M_{m_3} \end{pmatrix}$$

This completes the proof.

5. (a) Prove that the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$$

is nilpotent, and find its invariants and Jordan form.

(b) Prove that the matrix in part (a) is not similar to

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix}$$

303.5 (a) $$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix} \text{ is nilpotent.}$$

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 & -1 \\ 1 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

The invariant of $\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$ is 3.

(b) $$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix} \neq 0.$$

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix} \text{ is not nilpotent.}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix} \text{ are not similar.}$$

6. Prove Lemma 6.6.1 and its corollary even if the sums involved are not direct sums.

304.6 If $p(x)$ is the minimal polynomial for T over F, as we have seen above, both $p(T_1)$ and $p(T_2)$ are zero, whence $p_1(x) \mid p(x)$ and $p_2(x) \mid p(x)$.
But then the least common multiple of $p_1(x)$ and $p_2(x)$ must also divide $p(x)$
On the other hand, if $q(x)$ is the least common multiple of $p_1(x)$ and $p_2(x)$, consider $q(x)$.
For $v_1 \in V_1$, since $p_1(x) \mid q(x)$, $v_1 q(T) = v_1 q(T_1) = 0$; similarly, for $v_2 \in V_2$, $vq(T) = 0$, Given any v in V, v can be written as $v = v_1 + v_2$, where $v_1 \in V_1$ and $v_2 \in V_2$, in concequence of which $vq(T) = (v_1 + v_2)\, q(T) = v_1 q(T) + v_2 q(T) = 0$.
Thus $q(T) = 0$ and T satisfies $q(x)$. Combined with the result of the first paragraph, this yields the lemma.
The result of the corollary is also true by induction.

7. Prove the statement made to the effect that two linear transformations in $A_F(V)$ all of whose characteristic roots lie in F are similar if and only if their Jordan forms are the same (except for a permutation in the ordering of the characteristic roots).

304.7 Let S, T be linear transformations in $A(V)$.
Suppose S and T have the same Jordan forms. Then there is a basis $\{v_1, \cdots\cdots, v_n\}$ and a basis $\{w_1, \cdots\cdots, w_n\}$ in which S and T have the matrices S and T have the same forms.
That is $m_2(T) = m_1(S)$. By Theorem 6.3.2, there is a B in $A(V)$ such that $m_2(T) = m_1(B) m_1(T)\, m_1(B)^{-1} = m_1(S)$. $BTB^{-1} = S$.
T and S are similar.
Conversely, if S and T are similar, then there is a C in $A(V)$ such that $CTC^{-1} = S$.
There is a basis $\{v_1, \cdots\cdots, v_n\}$ in which the matrix T has its Jordan form. In the basis $\{v_1 C^{-1}, \cdots, v_n C^{-1}\}$, the matrix has the same Jordan form as T.

8. Complete the proof of the matrix version of Theorem 6.6.2, given in the text.

304.8 It follows from Theorem 6.6.2 and Theorem 6.3.2 that: Let A in F_n and suppose that K is the splitting field of the minimal polynomial of A over F; then an invertible matrix C in K_n can be found so that CAC^{-1} is in Jordan form.

9. Prove that the $n \times n$ matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & 1 & 0 \end{pmatrix}$$

having entries 1's on the subdiagonal and 0's elsewhere, is similar to M_n.

304.9

$$\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ 1 & \iddots & & \\ & & & \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ 1 & \iddots & & \\ & & & \end{pmatrix}$$

$$\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ 1 & \iddots & & \\ & & & \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & & \\ 0 & 0 & & 1 \end{pmatrix} \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ 1 & \iddots & & \\ & & & \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ 1 & \iddots & & \\ & & & \end{pmatrix} \begin{pmatrix} 0 & \cdots & \cdots & 0 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ & & & 1 & 0 \\ & & & \vdots & \\ 0 & 1 & & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \vdots \\ & & & & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} = M_n .$$

10. If F has characteristic $p > 0$ prove that $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ satisfies $A^p = 1$.

304.10 $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, $A^2 = \begin{pmatrix} 1 & 2\alpha \\ 0 & 1 \end{pmatrix}$, $A^3 = \begin{pmatrix} 1 & 3\alpha \\ 0 & 1 \end{pmatrix}$ $\cdots$

$$A^p = \begin{pmatrix} 1 & p\alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A^p = 1 .$$

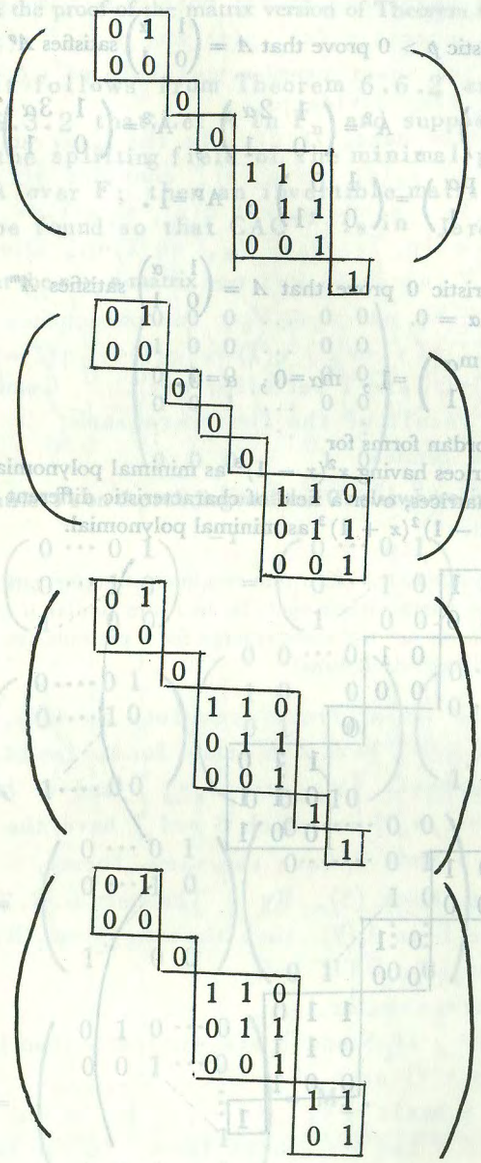
11. If F has characteristic 0 prove that $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ satisfies $A^m = 1$, for $m > 0$, only if $\alpha = 0$.

304.11 $A^m = \begin{pmatrix} 1 & m\alpha \\ 0 & 1 \end{pmatrix} = 1$, $m\alpha = 0$, $\alpha = 0$.

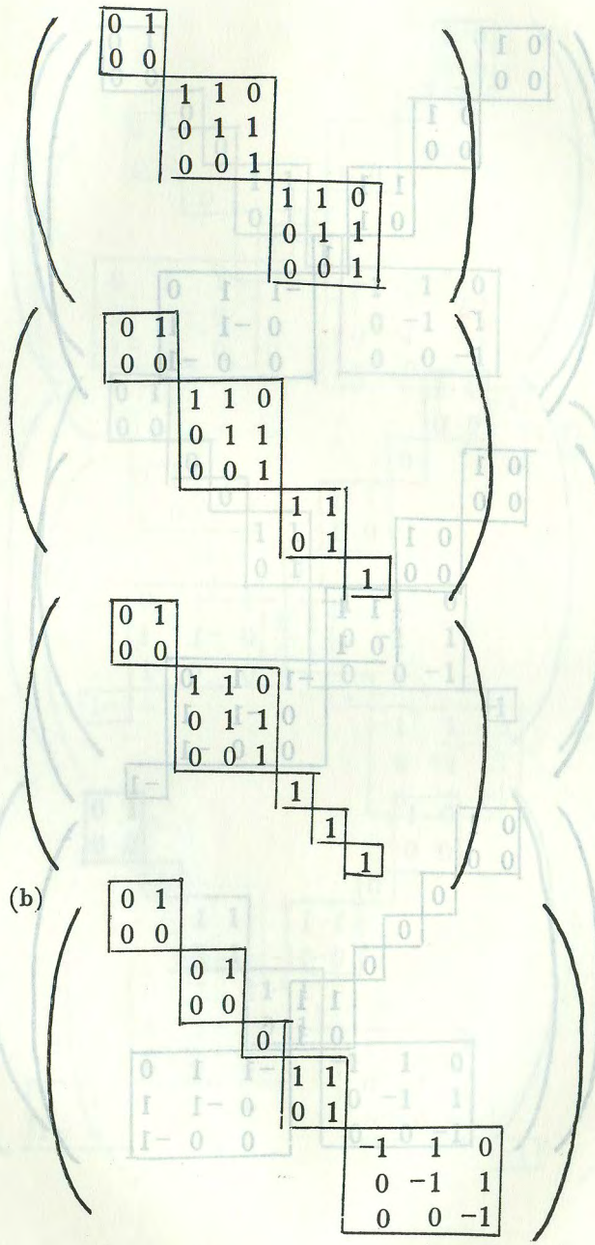
12. Find all possible Jordan forms for
(a) All 8×8 matrices having $x^2(x-1)^3$ as minimal polynomial.
(b) All 10×10 matrices, over a field of characteristic different from 2, having $x^2(x-1)^2(x+1)^3$ as minimal polynomial.

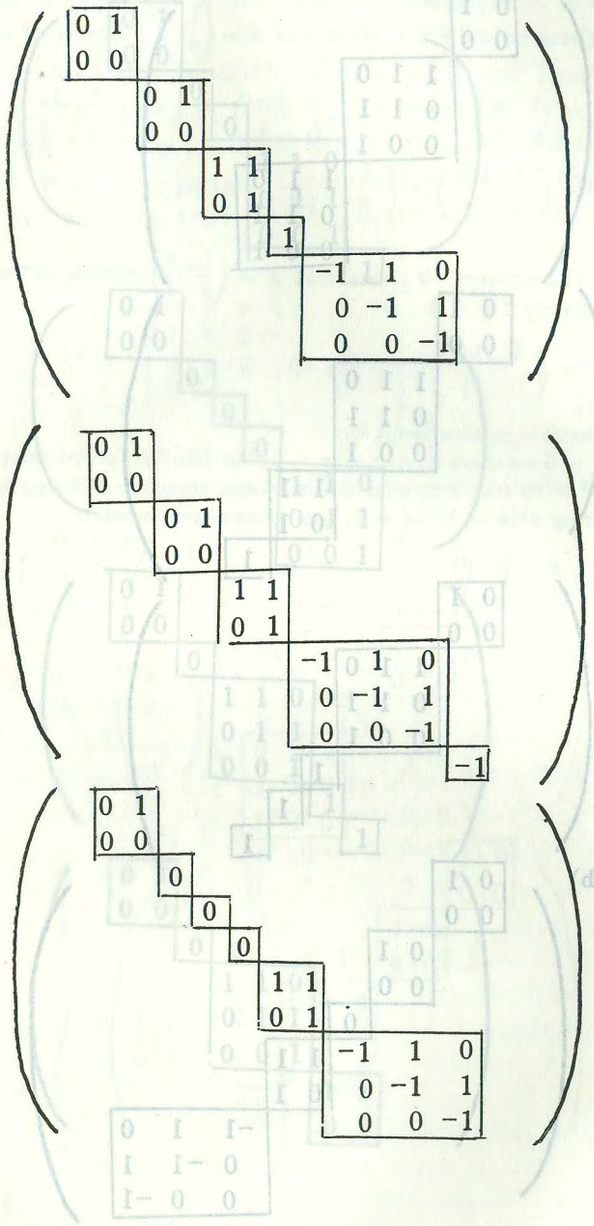
304.12 (a)

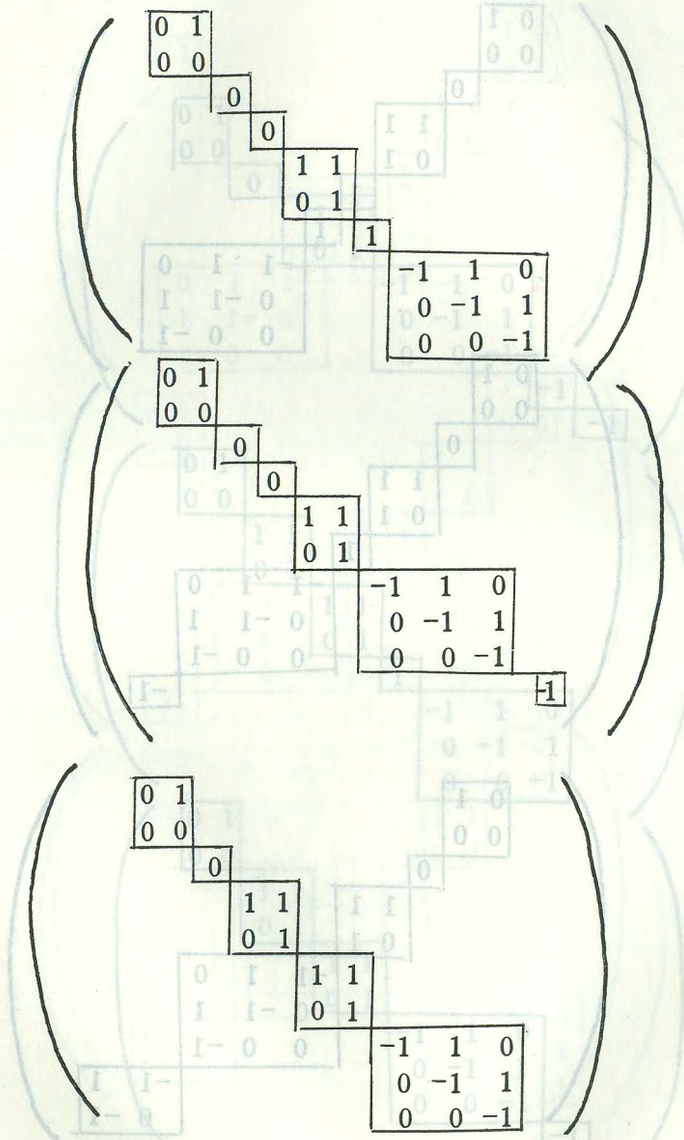
$$\begin{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & & & \\ & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & & \\ & & (0) & \\ & & & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{pmatrix} \begin{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & & & \\ & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & & \\ & & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} & \\ & & & (1) \end{pmatrix}$$

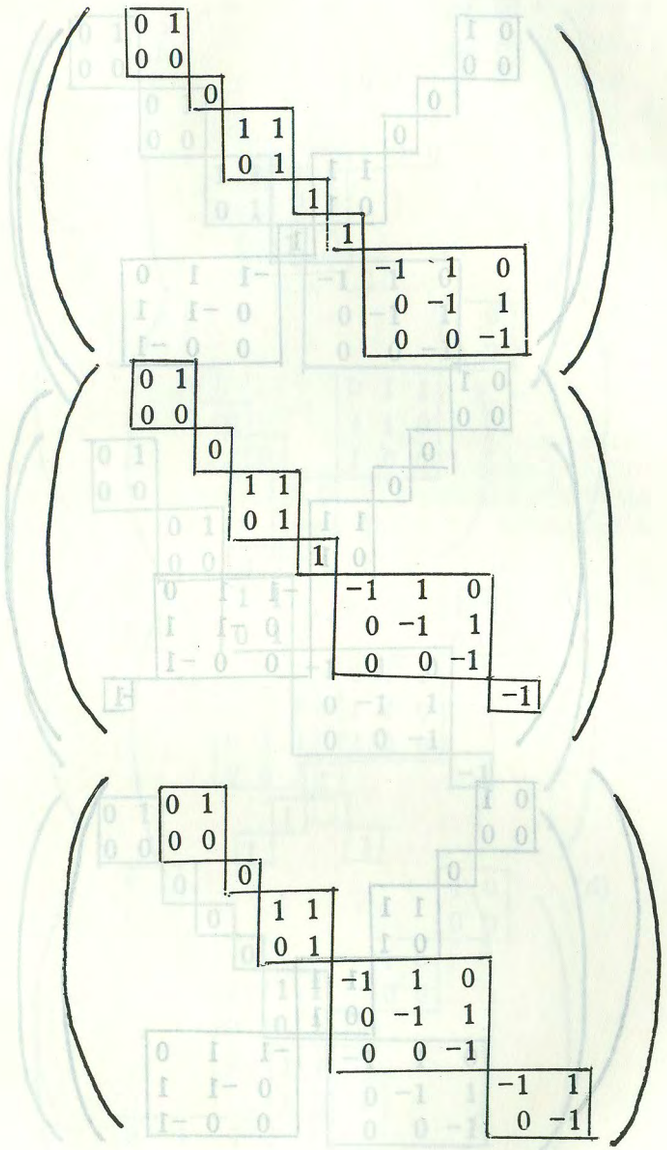


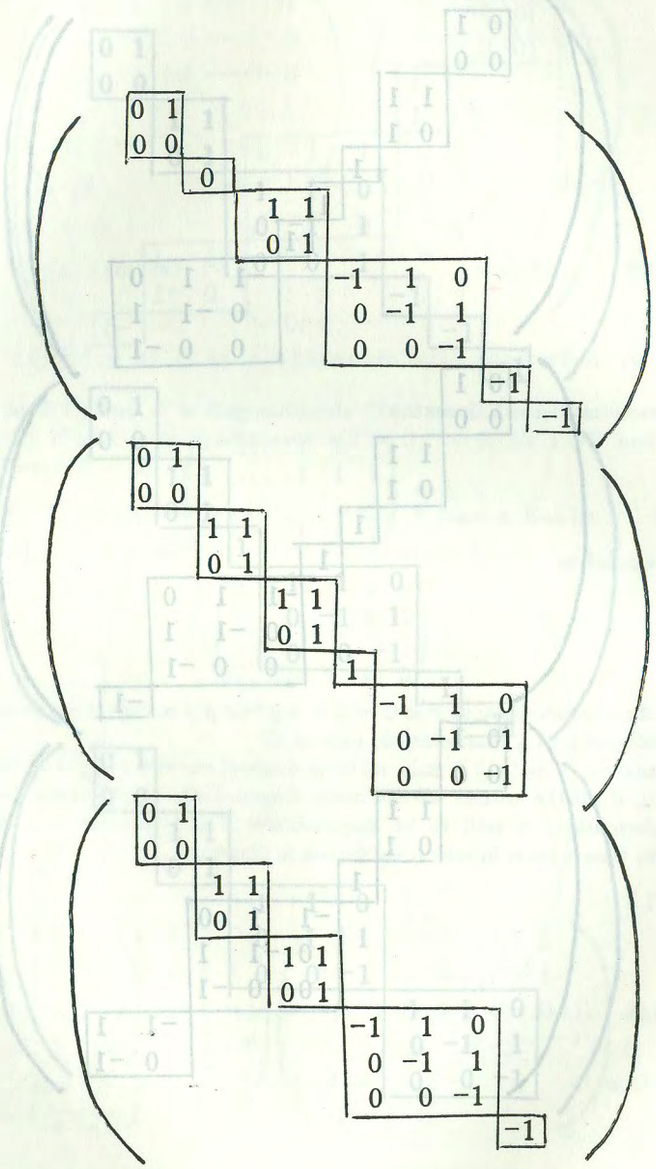
(b)

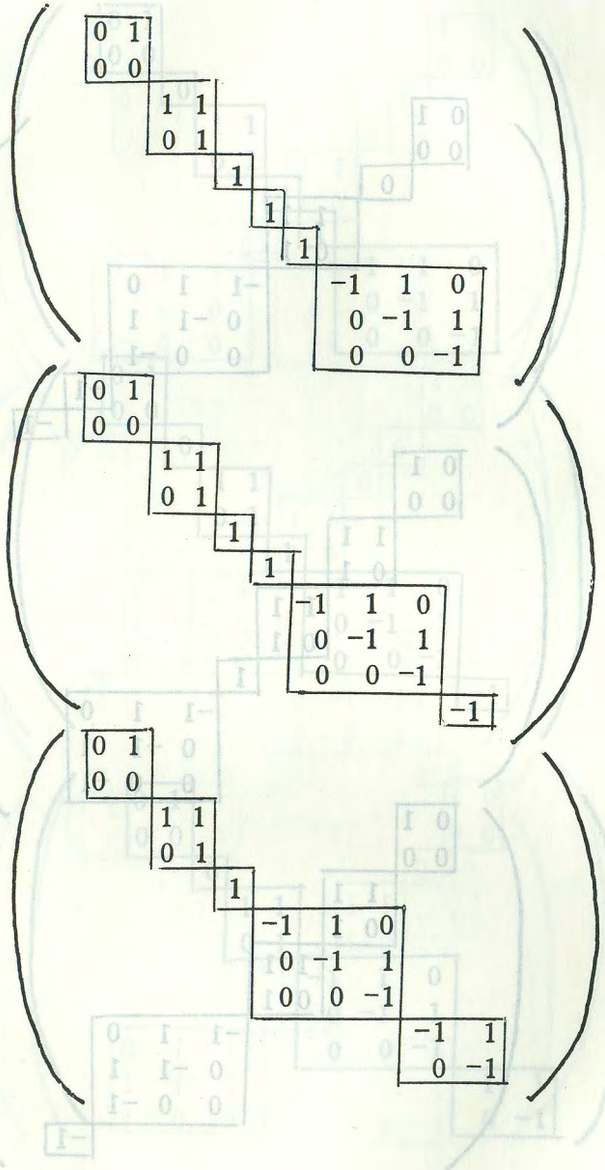


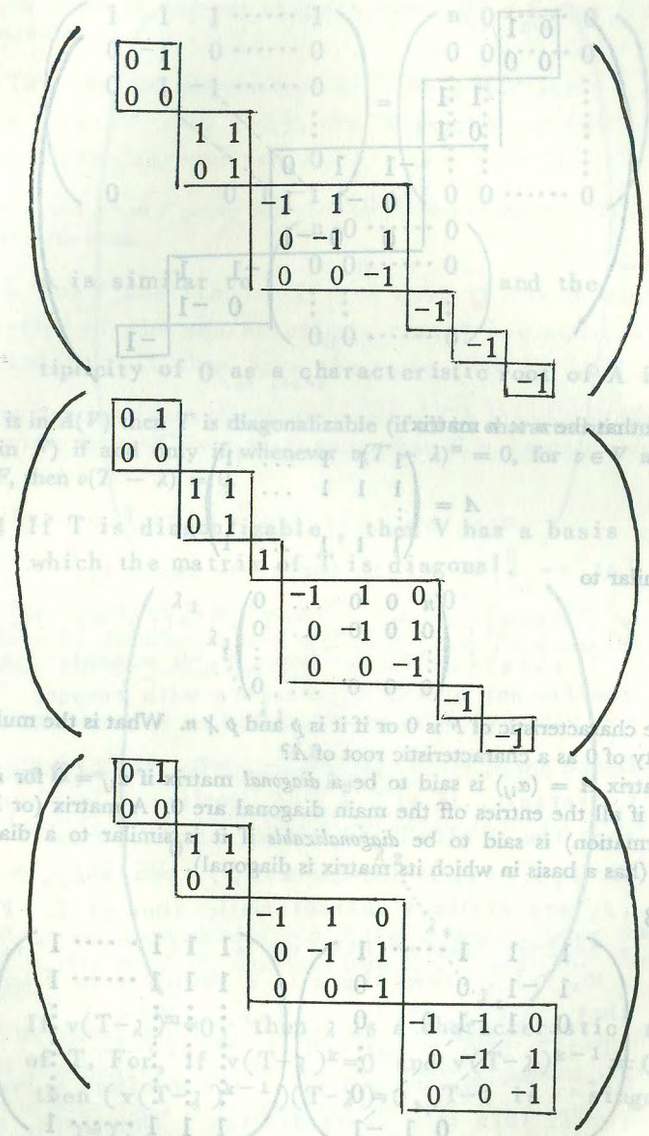

0 1
0 0
0 1
0 0
1 1
0 1
1
-1 1 0
0 -1 1
0 0 -1
0 1
0 0
0 1
0 0
1 1
0 1
-1 1 0
0 -1 1
0 0 -1
-1
0 1
0 0
0
0
0
1 1
0 1
-1 1 0
0 -1 1
0 0 -1


0 1
0 0
0
0
1 1
0 1
1
-1 1 0
0 -1 1
0 0 -1
0 1
0 0
0
0
1 1
0 1
-1 1 0
0 -1 1
0 0 -1
-1
0 1
0 0
0
1 1
0 1
1 1
0 1
-1 1 0
0 -1 1
0 0 -1


0 1
0 0
0
1 1
0 1
1
1
-1 1 0
0 -1 1
0 0 -1
0 1
0 0
0
1 1
0 1
1
-1 1 0
0 -1 1
0 0 -1
-1
0 1
0 0
0
1 1
0 1
-1 1 0
0 -1 1
0 0 -1
-1 1
0 -1


0 1
0 0
0
1 1
0 1
-1 1 0
0 -1 1
0 0 -1
-1
-1
0 1
0 0
1 1
0 1
1 1
0 1
1
-1 1 0
0 -1 1
0 0 -1
0 1
0 0
1 1
0 1
1 1
0 1
-1 1 0
0 -1 1
0 0 -1
-1


0 1
0 0
1 1
0 1
1
1
1
-1 1 0
0 -1 1
0 0 -1
0 1
0 0
1 1
0 1
1
1
-1 1 0
0 -1 1
0 0 -1
-1
0 1
0 0
1 1
0 1
1
-1 1 0
0 -1 1
0 0 -1
-1 1
0 -1


0 1
0 0
1 1
0 1
-1 1 0
0 -1 1
0 0 -1
-1
-1
-1
0 1
0 0
1 1
0 1
1
-1 1 0
0 -1 1
0 0 -1
-1
-1
0 1
0 0
1 1
0 1
-1 1 0
0 -1 1
0 0 -1
-1 1 0
0 -1 1
0 0 -1

$$\begin{pmatrix} \boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}} & & & & \\ & \boxed{\begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}} & & & \\ & & \boxed{\begin{matrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{matrix}} & & \\ & & & \boxed{\begin{matrix} -1 & 1 \\ 0 & -1 \end{matrix}} & \\ & & & & \boxed{-1} \end{pmatrix}$$

13. Prove that the $n \times n$ matrix

$$A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ \vdots & & & & \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}$$

is similar to

$$\begin{pmatrix} n & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

if the characteristic of F is 0 or if it is p and $p \nmid n$. What is the multiplicity of 0 as a characteristic root of A?

A matrix $A = (\alpha_{ij})$ is said to be a *diagonal* matrix if $\alpha_{ij} = 0$ for $i \neq j$, that is, if all the entries off the main diagonal are 0. A matrix (or linear transformation) is said to be *diagonalizable* if it is similar to a diagonal matrix (has a basis in which its matrix is diagonal).

305.13

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 0 & & 0 \\ 0 & 1 & -1 & 0 & 0 \\ & & \ddots & \ddots & \vdots \\ & & & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ & \ddots & & & \vdots \\ 0 & & 0 & 1 & -1 \end{pmatrix} = \begin{pmatrix} n & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

A is similar to $\begin{pmatrix} n & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$ and the multiplicity of 0 as a characteristic root of A is n-1.

14. If T is in $A(V)$ then T is diagonalizable (if all its characteristic roots are in F) if and only if whenever $v(T - \lambda)^m = 0$, for $v \in V$ and $\lambda \in F$, then $v(T - \lambda) = 0$.

305.14 If T is diagonlizable, then V has a basis in which the matrix of T is diagonal.

$$m(T) = \begin{pmatrix} \lambda_1 & & & & & 0 \\ & \lambda_1 & & & & \\ & & \ddots & & & \\ & & & \lambda_1 & & \\ & & & & \lambda_2 & \\ & & & & & \lambda_2 \\ & & & & & & \ddots \\ & & & & & & & \lambda_2 \\ & & & & & & & & \ddots \\ & & & & & & & & & \lambda_t \\ & & & & & & & & & & \ddots \\ 0 & & & & & & & & & & & \lambda_t \end{pmatrix}$$

If $v(T-\lambda)^m=0$, then λ is a characteristic root of T. For, if $v(T-\lambda)^k=0$ and $v(T-\lambda)^{k-1} \neq 0$, then $(v(T-\lambda)^{k-1})(T-\lambda)=0$, $T-\lambda$ is singular. $\lambda=\lambda_1$.

$$m(T-\lambda)^k = \begin{pmatrix} (\lambda_1-\lambda_i)^k & & & & & & \\ & \ddots & & & & & \\ & & (\lambda_1-\lambda_i)^k & & & & \\ & & & (x_2-\lambda_i)^k & & & \\ & & & & \ddots & & \\ & & & & & (\lambda_2-\lambda_i)^k & \\ & & & & & & \ddots \\ & & & & & & 0 \\ & & & & & & & \ddots \\ & & & & & & & & 0 \\ & & & & & & & & & (\lambda_{i+1}-\lambda_i)^k \\ & & & & & & & & & & \ddots \\ & & & & & & & & & & & (\lambda_{i+1}-\lambda_i)^k \\ & & & & & & & & & & & & \ddots \\ & & & & & & & & & & & & & (\lambda_t-\lambda_i)^k \end{pmatrix}$$

Let $v=\sum_{i=1}^{n}\alpha_i v_i$ in the given basis $v_1, \cdots\cdots, v_n$. $0=(\alpha_1, \cdots\cdots, \alpha_n)m(T-\lambda)^k=((\lambda_1-\lambda_i)^k\alpha_1, \cdots\cdots, (\lambda_t-\lambda_i)^k\alpha_n)$. Hence $\alpha_j=0$ except the coefficient of the eignvectors with respect to λ_i.

Hence $(\alpha_1, \cdots\cdots, \alpha_n)m(T-\lambda)=0$. $v(T-\lambda)=0$. Conversely, if $v(T-\lambda)^m=0$ implies $v(T-\lambda)=0$, then the minimal polynomial $p(x)$ of T must be $(x-\lambda_1)(x-\lambda_2)\cdots\cdots(x-\lambda_t)$, where $\lambda_1, \cdots\cdots, \lambda_t$ are distinct characteristic root of T. For, if not, suppose $p(x)=(x-\lambda_1)^{m_1}\cdots\cdots(x-\lambda_t)^{m_t}$, $m_t>1$, then there is a vector v in V such that $(v(T-\lambda_1)^{m_1}\cdots\cdots(T-\lambda_{t-1})^{m_{t-1}})(T-\lambda_t)\neq 0$, but $v(T-\lambda_1)^{m_1}\cdots\cdots(T-\lambda_t)^{m_t}=0$ since $p(x)$ is the minimal polynomial for T. This is a contradiction. Therefore, the minimal polynomial of T is $(x-\lambda_1)\cdots\cdots(x-\lambda_t)$. The Jordan Form of T is a diagonal matrix. This completes the proof.

15. Using the result of Problem 14, prove that if $E^2 = E$ then E is diagonalizable.

305.15 The minimal polynomial of E is a divisor of x^2-x. $x^2-x=x(x-1)$. By the proof of (305.14), E is diagonalizable.

16. If $E^2 = E$ and $F^2 = F$ prove that they are similar if and only if they have the same rank.

305.16 E and F are similar if and only if the multiplici-ties of the characteristic root 1 are equal, and, if and only if they have the same rank by (284.28).

17. If the multiplicity of each characteristic root of T is 1, and if all the characteristic roots of T are in F, prove that T is diagonalizable over F.

305.17 By the proof of (305.14), we can this fact.

18. If the characteristic of F is 0 and if $T \in A_F(V)$ satisfies $T^m = 1$, prove that if the characteristic roots of T are in F then T is diagonalizable. (*Hint:* Use the Jordan form of T.)

305.18 The minimal polynomial p(x) of T is a divisor of x^m-1. Since x^m-1 has no multiple root, the multiplicity of each characteristic root of T is 1. By (307.17), T is diagonalizable.

*19. If $A, B \in F$ are diagonalizable and if they commute, prove that there is an element $C \in F_n$ such that both CAC^{-1} and CBC^{-1} are diagonal.

305.19 Use induction on n. n=1 we are done. If A and B are scalar, then take C=1, we are done.
Suppose that A is not scalar.
$U_\lambda = \{ v \in F^{(n)} \mid vA=\lambda v \}$, where λ is a charcteristic root of A.
$V=U_{\lambda_1} \oplus U_{\lambda_2} \oplus \cdots\cdots \oplus U_{\lambda_k}$,

where $\lambda_1, \cdots\cdots, \lambda_k$ are all characteristic roots of A. Every $U\lambda_i$ is invariant under B by (290.6). B induces a linear tranformation $\overline{B}$ on $U\lambda_i$ and the minimal polynomial for $\overline{B}$ divides that for B. $\overline{B}$ is also diagonal. Similarly, $\overline{A}$ is diagonal. By induction hypothesis, there is a basis $\{ v_1^{(i)}, \cdots\cdots, v_{ir}^{(i)} \}$ of $U\lambda_i$ such that $\overline{A}$ and $\overline{B}$ are diagonal. $\{ v_1^{(1)}, \cdots\cdots, v_{i1}^{(1)}, \cdots\cdots, v_1^{(k)}, \cdots\cdots, v_{ik}^{(k)} \}$ forms a basis of $F^{(n)}$ and A, B are diagonal in this basis. By Theorem 6.3.2, there is a C in F_n such that CAC^{-1} and CBC^{-1} are diagonal. This completes the proof.

20. Prove that the result of Problem 19 is false if *A* and *B* do not commute.

305.20 Let $A=\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}$, $B=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$. Suppose there is a C in F_2 such that $CAC^{-1}=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$ and CBC^{-1} $\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$ or $CAC^{-1}=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$ and $CBC^{-1}=\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}$.

The first case can not happen, otherwise A=B.

Suppose $CA=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}C$,

$CB=\begin{pmatrix}2 & 0\\ 1 & 0\end{pmatrix}C$. Let $C=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$

$$CA=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}=\begin{pmatrix}a & a+2b\\ c & c+2d\end{pmatrix}$$

$$=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}C=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}a & b\\ 2c & 2d\end{pmatrix},\ \begin{matrix}c=0,\\ a+b=0.\end{matrix}$$

$$CB=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}=\begin{pmatrix}a & 2b\\ c & 2d\end{pmatrix}=\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}C$$

$$=\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}2a & 2b\\ c & d\end{pmatrix}$$

$a=0$, $d=0$. $b=-a=0$. $C=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$, a contradiction.

6.7. Canonical Forms: Rational Canonical Form.

1. Verify that V becomes an $F[x]$-module under the definition given.

312.1 V isan abelian group under additon by definition.

$v_1, v_2 \in V$, $f(x), g(x) \in F[x]$.

$(v_1+v_2)f(x)=(v_1+v_2)f(T)=v_1f(T)+v_2f(T)$

$=v_1f(x)+v_2f(x)$.

$v_1(f(x)+g(x))=v_1(f(T)+g(T))=v_1f(T)+v_1g(T)$

$=v_1f(x)+v_2g(x)$.

$(v_1f(x))g(x)=(v_1f(T))g(x)=(v_1f(T))g(T)$

$=v_1(f(T)g(T))=v_1(f(x)g(x))$.

V is an $F[x]$-module.

2. In the proof of Theorem 6.7.3 provide complete proof at all points marked "(Prove)."

312.2 We left the first "(Prove)" to the reader and only prove the second one.

Let $\{ u, uT, \cdots\cdots, uT^{d-1}$

$\vdots \quad \vdots \quad \vdots$

$uT^{(f_1-f_m)d}, \cdots\cdots, uT^{(f_1-f_m)d+(d-1)}$

$\vdots \quad \vdots$

$uT^{(f_i-1)d}, \cdots\cdots, uT^{(f_i-1)d+d-1} \}$

be a basis of U_i.

$U_i q(T)^{f_m}$ is spaned by

$\{ uq(T)^{f_m}, uTq(T)^{f_m}, \cdots\cdots uT^{d-1}q(T)^{f_m},$

$\vdots$

$uT^{(f_i-f_m)d}q(T)^{f_m}, \cdots\cdots, uT^{(f_i-f_m)d+(d-1)}q(T)^{f_m},$

$uT^{(f_i-1)d}q(T)^{f_m}, \cdots\cdots, uT^{f_id-1}q(T)^{f_m} \}$.

If $(\alpha_{11}u+\cdots\cdots+\alpha_{1d}uT^{d-1}+\cdots\cdots\cdots\cdots$

$+\alpha_{(f_1-f_m),d}uT^{(f_i-f_m)d-1})q(T)^{f_m}=0$, then

$\alpha_{f_i-f_m,d}=0$ since $u, \cdots\cdots, uT^{f_id-1}$ are linearly independent. Similarly, we can prove that $\alpha_{11}=\cdots\cdots=\alpha_{(f_1-f_m),d}=0$. If $uq(T)^{f_i-f_m}q(T)^{f_m}=0$ then

$uT^{(f_i-f_m)}q(T)^{f_m} \in \{ uq(T)^{f_m}, uTq(T)^{f_m}, \cdots\cdots,$

$uT^{(f_i-f_m)d-1}q(T)^{f_m}\}$.

Therefore, dim $U_i q(T)^{f_m}=d(f_i-f_m)$.

*3. (a) Prove that every root of the characteristic polynomial of T is a characteristic root of T.

(b) Prove that the multiplicity of any root of $p_T(x)$ is equal to its multiplicity as a characteristic root of T.

312.3 (a) Let the minimal polymomial for T is $f(x)=(q_1(x))^{e_1}\cdots\cdots(q_n(x)^{e_n})$, where $q_i(x)$ is irreducible over F. $p_T(x)=(q_1(x))^{l_1}\cdots\cdots(q_n(x))^{l_n}$, where $l_1\geq e_1\cdots l_n\geq e_n$. Hence every root of $p_T(x)$ is a root of $f(x)$ and so a characteristic root of T by (290.5).

(b) Suppose the matrix of T under some basis is

$$\begin{pmatrix} R_1 & & \\ & R_2 & \\ & & \ddots \\ & & & R_n \end{pmatrix}, \text{ wher } R_i =$$

$$= \begin{pmatrix} C(q_i(x)^{e_{i1}}) & & \\ & \ddots & \\ & & C(q_i(x)^{e_{ir_i}}) \end{pmatrix}.$$

Since $q_i(x)$ is irreduible, so the multiplicity of every root of $q_i(x)$ is $(e_{i1}+e_{i2}+\cdots+e_{ir_i})$ (by Corollary 1 to Lemma 5.5.2).

Let K be the splitting field of $f(x)$. In a basis of V, the matrix of T is triangular over K and the the main diagonal entries are the characteristic rootsof T. We may consider only $C(q_j(x)^{e_{i1}})$.

$C(q_i(x)^{e_{i1}})$ is simlar to $S=\begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix}$.

By (312.4), $q_i(x)^{e_{i1}}$ is the minimal polynomial for $C((q_i(x))^{e_{i1}})$. The main diagonal entries of S are roos of $q_i(x)^{e_{i1}}$.

Hence the multiplicity of any roots of $p_T(x)$ is equal to its multiplicity as a charart eristic root of T.

4. Prove that for $f(x)\in F[x]$, $C(f(x))$ satisfies $f(x)$ and has $f(x)$ as its minimal polynomial. What is its characteristic polynomial?

312.4 By (269.29), T=C(f(x)) satisfies f(x). Let $v=(1,0,0,\cdots\cdots,0)$. v, $vT=(0,1,0,\cdots\cdots 0)$, $vT^2=(0,0,1,0)$, $\cdots\cdots$ $vT^{n-1}=(0,0,\cdots\cdots,0,1)$ is a basis of $V=F^{(n)}$. If the degree of the minimal polynomial p(x) for T is less than f(x), then vp(T)=0. This contradicts with the fact that $v, vT, \cdots\cdots, vT^{n-1}$ are linearly independent. Hence the minimal polynomial for T is f(x). The characteristic polynomial for T is also f(x).

5. If F is the field of rational numbers, find all possible rational canonical forms and elementary divisors for

(a) The 6×6 matrices in F_6 having $(x-1)(x^2+1)^2$ as minimal polynomial.

(b) The 15×15 matrices in F_{15} having $(x^2+x+1)^2(x^3+2)^2$ as minimal polynomial.

(c) The 10×10 matrices in F_{10} having $(x^2+1)^2(x^3+1)$ as minimal polynomial.

312.5 (a) $\begin{pmatrix} 1 & & \\ & 1 & \\ & & C((x^2+1)^2) \end{pmatrix}$

(b) $\begin{pmatrix} C((x^2+x+1)^2) & & \\ & C(x^2+x+1) & \\ & & C((x^3+2)^2) \\ & & & C(x^3+2) \end{pmatrix}$

(c) $\begin{pmatrix} C((x^2+1)^2) & & & \\ & C(x^2+1) & & \\ & & C(x^3+1) & \\ & & & C(-1) \end{pmatrix}$

$$\begin{pmatrix} C((x^2+1)^2) & & & \\ & C(x^3+1) & & \\ & & -1 & \\ & & & -1 \\ & & & & -1 \end{pmatrix}$$

$$\begin{pmatrix} C((x^2+1)^2) & & \\ & C(x^3+1) & \\ & & C(x^3+1) \end{pmatrix}$$

6. (a) If K is an extension of F and if A is in K_n, prove that A can be written as $A = \lambda_1 A_1 + \cdots + \lambda_k A_k$ where $A_1, \ldots, A_k$ are in F_n and where $\lambda_1, \ldots, \lambda_k$ are in K and are linearly independent over F.

   (b) With the notation as in part (a), prove that if $B \in F_n$ is such that $AB = 0$ then $A_1B = A_2B = \cdots = A_kB = 0$.

   (c) If C in F_n commutes with A prove that C commutes with each of $A_1, A_2, \ldots, A_k$.

313.6 (a) Let $A=(a_{ij})$. $M=\{a_{ij} \mid i=1,2,\cdots\cdots,n,\ j=1,2,\cdots\cdots,n\}$. Let $\{\lambda_1,\lambda_2,\cdots\cdots,\lambda_k\}$ be a maximal subset of M such that $\lambda_1,\cdots\cdots,\lambda_k$ are linearly independent over F. Then

$$a_{ij}=\sum_{r=1}^{k}\alpha_{ijr}\lambda_r$$

since $\lambda_1,\cdots\cdots,\lambda_k, a_{ij}$ are linearly dependent over F. Let $A_r=(\alpha_{ijr})$. $A=\lambda_1A_1+\lambda_2A_2+\cdots\cdots+\lambda_kA_k$.

(b) $AB=(\lambda_1A_1+\lambda_2A_2+\cdots\cdots+\lambda_kA_k)B$
$=\lambda_1A_1B+\lambda_2A_2B+\cdots\cdots+\lambda_kA_kB$
$=0$.

$A_rB\in F_n$. $\lambda_1,\cdots\cdots,\lambda_k$ are linearly independent over F. Consider the (i,j) entry of $\lambda_1A_1B+\cdots\cdots+\lambda_kA_kB$, we have that the (i,j) entry of A_rB is zero. Hence $A_rB=0$, $r=1,\cdots\cdots,k$. $A_1B=A_2B=\cdots\cdots=A_kB=0$.

(c) $0=AC-CA=\lambda_1(A_1C-CA_1)+\lambda_2(A_2C-CA_2)+\cdots\cdots+\lambda_k(A_kC-CA_k)$. $\lambda_1,\cdots\cdots,\lambda_k$ are linearly independent over F. Consider the (i,j) entry of $\lambda_1(A_1C-CA_1)+\lambda_2(A_2C-CA_2)+\cdots\cdots+\lambda_k(A_kC-CA_k)$, we have that the (i,j) entry of A_rC-CA_r is zero. Hence $A_rC-CA_r=0$. $A_rC=CA_r$. C commutes with each of $A_1,A_2,\cdots\cdots A_k$.

*7. If $A_1, \ldots, A_k$ are in F_n and are such that for some $\lambda_1, \ldots, \lambda_k$ in K, an extension of F, $\lambda_1A_1 + \cdots + \lambda_kA_k$ is invertible in K_n, prove that *if F has an infinite number of elements* we can find $\alpha_1, \ldots, \alpha_k$ *in* F such that $\alpha_1A_1 + \cdots + \alpha_kA_k$ is invertible in F_n.

313.7 In this exercise, we use the fact that A is invertible if and only if $\det A \neq 0$ (Theoren 6.9.3.).

Let $f_k(x)=\det(\lambda_1A_1+\lambda_2A_2+\cdots\cdots+\lambda_{k-1}A_{k-1}+xA_k)\in K[x]$. $\deg f_k(x)=n$. $f_k(x)$ has at most n solutions in F by Lemma 5.3.2. Since F has infinite elements, there is an α_k in F such that $f_k(\alpha_k)\neq 0$. Otherwise $f_k(x)\equiv 0$.
This contradicts with $f_k(\lambda_k)\neq 0$.
Hence $\lambda_1A_1+\lambda_2A_2+\cdots\cdots+\lambda_{k-1}A_{k-1}+\alpha_kA_k$ is invertible. Let $f_{k-1}(x)=\det(\lambda_1A_1+\lambda_2A_2+\cdots\cdots+\lambda_{k-2}A_{k-2}+xA_{k-1}+\alpha_kA_k)$.
As above, there is an α_{k-1} in F such that $f_{k-1}(\alpha_{k-1})\neq 0$. Otherwise $f_{k-1}(x)\equiv 0$. This contradicts with $f_{k-1}(\lambda_{k-1})\neq 0$. Hence $\lambda_1A_1+\lambda_2A_2+\cdots\cdots+\lambda_{k-2}A_{k-2}+\alpha_{k-1}A_{k-1}+\alpha_{k-2}A_{k-2}$ is invertible. Continuing this proeess,we have that there are $\alpha_1,\cdots\cdots,\alpha_k$ in F such that $\alpha_1A_1+\alpha_2A_2+\cdots\cdots+\alpha_kA_k$ is invertible.

*8. If F is a *finite field* prove the result of Problem 7 is false.

313.8 Let $A_1=\begin{pmatrix}1&0&0\\1&0&0\\0&0&1\end{pmatrix}$, $A_2=\begin{pmatrix}1&0&0\\0&1&0\\1&0&0\end{pmatrix}\in(J_2)_3$.

$$A=\begin{pmatrix}1+x & 0 & 0\\ 1 & x & 0\\ x & 0 & 1\end{pmatrix}=\begin{pmatrix}1&0&0\\1&0&0\\0&0&1\end{pmatrix}+x\begin{pmatrix}1&0&0\\0&1&0\\1&0&0\end{pmatrix}$$

is invertible in $(J_2[x]/(x^2+x+1))_3$.

In fact, $A^{-1}=\begin{pmatrix}x & 0 & 0\\ 1 & 1+x & 0\\ 1+x & 0 & 1\end{pmatrix}$.

But $\alpha\begin{pmatrix}1&0&0\\1&0&0\\0&0&1\end{pmatrix}+\beta\begin{pmatrix}1&0&0\\0&1&0\\1&0&0\end{pmatrix}$ is not invertible in $(J_2)_3$ for all $\alpha,\beta=0,1$.

*9. Using the results of Problems 6(a) and 7 prove that if F has an infinite number of elements then whenever $A, B \in F_n$ are similar in K_n, where K is an extension of F, then they are familiar in F_n. (This provides us with a proof, independent of canonical forms of Corollary 1 to Theorem 6.7.3 in the special case when F is an infinite field.)

313.9 If A,B are similar in K_n, then there is an invertible element C in K_n such that $A=CBC^{-1}$.

By (313.6.(a)), $C=\lambda_1C_1+\lambda_2C_2+\cdots\cdots+\lambda_kC_k$, where $C_1,C_2,\cdots\cdots,C_k$ are in F_n and where $\lambda_1,\cdots\cdots,\lambda_k$ are in K and are linearly independent over F.

$0=AC-CB=A(\lambda_1C_1+\lambda_2C_2+\cdots\cdots+\lambda_kC_k)-(\lambda_1C_1+\lambda_2C_2+\cdots\cdots+\lambda_kC_k)B=\lambda_1(AC_1-C_1B)+\lambda_2(AC_2-C_2B)+\cdots\cdots+\lambda_k(AC_k-C_kB)$.

Since $\lambda_1,\cdots\cdots,\lambda_k$ are linearly independent over F, $AC_1=C_1B$, $AC_2=C_2B$, $\cdots\cdots$, $AC_k=C_kB$.

By(313.7), there are $\alpha_1,\alpha_2,\cdots\cdots\alpha_k$ in F such that $\alpha_1C_1+\alpha_2C_2+\cdots\cdots+\alpha_kC_k=D$ is invertible in F_n.

$AD=A(\alpha_1C_1+\cdots\cdots+\alpha_kC_k)=\alpha_1AC_1+\cdots\cdots+\alpha_kAC_k$
$=\alpha_1C_1B+\cdots\cdots+\alpha_kC_kB$
$=(\alpha_1C_1+\cdots\cdots+\alpha_kC_k)B$
$=DB$,

$A=DBD^{-1}$. A and B are similar in F_n.

10. Using matrix computations (but following the lines laid out in Problem 9), prove that if F is the field of real numbers and K that of complex numbers, then two elements in F_2 which are similar with K_2 are already similar in F_2.

313.10 Suppose A, B in F_2 are similar in K_2. There is a C in K_2 such that $A=CBC^{-1}$. Let

$A=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}$, $B=\begin{pmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{pmatrix}$,

$C=\begin{pmatrix}c_{11}+id_{11}&c_{12}+id_{12}\\c_{21}+id_{21}&c_{22}+id_{22}\end{pmatrix}=\begin{pmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{pmatrix}+i\begin{pmatrix}d_{11}&d_{12}\\d_{21}&d_{22}\end{pmatrix}$.
$=C_1+iD_1$

C is invertible in K_2.

$AC=CB$. $AC_1+iAD_1=C_1B+iD_1B$.

$AC_1=C_1B$, $AD_1=D_1B$.

If C_1 is invertible in F_2, that is, $c_{11}c_{22}-c_{21}c_{12}\neq 0$, then A and B are similar in F_2.

If D_1 is inveofible in F_2 that is, $d_{11}d_{22}-d_{22}d_{12}\neq 0$ then A and B are similar in F_2. Suppose now that

$c_{11}c_{22}-c_{21}c_{12}=d_{11}d_{22}-d_{21}d_{12}=0$. $f(x)=\det(C_1+xD_1)=(d_{11}d_{22}-d_{21}d_{12})x^2+(d_{11}c_{22}+d_{22}c_{11}-c_{21}d_{12}-d_{21}c_{12})x+(c_{11}c_{22}-c_{21}c_{12})=(d_{11}c_{22}+d_{22}c_{11}-c_{21}d_{12}-d_{21}c_{12})x$.

Since $f(i)\neq 0$. $f(1)\neq 0$. $\det(C_1+D_1)\neq 0$.

C_1+D_1 is invertible in F_2.

$AC_1=C_1B$, $AD_1=D_1B$.

$A(C_1+D_1)=(C_1+D_1)B$.

$A=(C_1+D_1)B(C_1+D_1)^{-1}$.

A and B are simlar in F_2.

6.8. Trace and Transpose.

Unless otherwise specified, symmetric and skew-symmetric refer to transpose.

1. Prove that $\operatorname{tr}(A + B) = \operatorname{tr} A + \operatorname{tr} B$ and that for $\lambda \in F$, $\operatorname{tr}(\lambda A) = \lambda \operatorname{tr} A$.

319.1 Let $A=(\alpha_{ij})$, $B=(\beta_{ij})$. $A+B=(\alpha_{ij}+\beta_{ij})$. $\lambda A=(\lambda\alpha_{ij})$.

$$\operatorname{tr}(A+B)=\sum_{i=1}^{n}(\alpha_{ii}+\beta_{ii})=\sum_{i=1}^{n}\alpha_{ii}+\sum_{i=1}^{n}\beta_{ii}=\operatorname{tr}A+\operatorname{tr}B.$$

$$\operatorname{tr}(\lambda A)=\sum_{i=1}^{n}\lambda\alpha_{ii}=\lambda\sum_{i=1}^{n}\alpha_{ii}=\lambda\operatorname{tr}A.$$

2. (a) Using a trace argument, prove that if the characteristic of F is 0 then it is impossible to find $A, B \in F_n$ such that $AB - BA = 1$.
   (b) In part (a), prove, in fact, that $1 - (AB - BA)$ cannot be nilpotent.

319.2 (a) Suppose there are A,B in F_n such that $AB-BA=1$. Then $0=\operatorname{tr}(AB)-\operatorname{tr}(BA)=\operatorname{tr}(AB-BA)=\operatorname{tr}1=n$, a contradiction.

(b) If $1-(AB-BA)$ is nilpotent, then $0=\operatorname{tr}(1-(AB-BA))=\operatorname{tr}1-\operatorname{tr}AB-\operatorname{tr}BA=\operatorname{tr}1=n$, a contradiction. Hence $1-(AB-BA)$ can not be nilpotent.

3. (a) Let f be a function defined on F_n having its values in F such that
   1. $f(A + B) = f(A) + f(B)$;
   2. $f(\lambda A) = \lambda f(A)$;
   3. $f(AB) = f(BA)$;

   for all $A, B \in F_n$ and all $\lambda \in F$. Prove that there is an element $\alpha_0 \in F$ such that $f(A) = \alpha_0 \operatorname{tr} A$ for every A in F_n.
   (b) If the characteristic of F is 0 and if the f in part (a) satisfies the additional property that $f(1) = n$, prove that $f(A) = \operatorname{tr} A$ for all $A \in F_n$.

Note that Problem 3 characterizes the trace function.

320.3 (a) Let E_{ij} be defined as in (283.15). If $i \neq j$, then $f(E_{ij})=f(E_{ij}E_{jj})=f(E_{jj}E_{ij})=f(0)=0$. (By $1.\ f(0)=f(0+0)=f(0)+f(0)$, $f(0)=0$).
$f(E_{11})=f(E_{11}E_{11})=f(E_{11}E_{11})=f(E_{ii})$ for

$i=1,2,\cdots\cdots,n$. Let $\alpha_0=f(E_{11})=\cdots\cdots\cdots f(E_{nn})$. For $A\in F_n$, $A=\sum_{i,j}\alpha_{ij}E_{ij}$.

$$f(A)=f\Big(\sum_{i,j}\alpha_{ij}E_{ij}\Big)=\sum_{i,j}\alpha_{ij}f(E_{ij})$$

$$=\sum_{i=1}^{n}\alpha_{ii}f(E_{ii})=\alpha_0\sum_{i=1}^{n}\alpha_{ii}=\alpha_0\operatorname{tr}A.$$

(b) $n=f(1)=\alpha_0\operatorname{tr}1=\alpha_0 n$, $n(1-\alpha_0)=0, \alpha_0=1$. $f(A)=\operatorname{tr}A$.

*4. (a) If the field F has an infinite number of elements, prove that every element in F_n can be written as the sum of regular matrices.
   (b) If F has an infinite number of elements and if f, defined on F_n and having its values in F, satisfies
   1. $f(A + B) = f(A) + f(B)$;
   2. $f(\lambda A) = \lambda f(A)$;
   3. $f(BAB^{-1}) = f(A)$;

   for every $A \in F_n$, $\lambda \in F$ and invertible element B in F_n, prove that $f(A) = \alpha_0 \operatorname{tr} A$ for a particular $\alpha_0 \in F$ and all $A \in F_n$.

320.4 (a) Let $A\in F_n$, $A=(\alpha_{ij})$. Since F has infinite number of elements, there is a nonzero α in F sach that $\alpha+\alpha_{ii}\neq 0$ for all $i=1,2,\cdots\cdots n$.

$$A=\begin{pmatrix}\alpha_{11} & & **\\ & \alpha_{22} & \\ & & \\ * & & \alpha_{nn}\end{pmatrix}=\begin{pmatrix}1 & & 0\\ & 1 & \\ & & \\ * & & 1\end{pmatrix}+$$

$$\begin{pmatrix}-1 & & **\\ & -1 & \\ & & \\ 0 & & -1\end{pmatrix}+\begin{pmatrix}\alpha+\alpha_{11} & & 0\\ & \alpha+\alpha_{22} & \\ & & \\ 0 & & \alpha+\alpha_{nn}\end{pmatrix}$$

$$+\begin{pmatrix}-\alpha & & 0\\ & -\alpha & \\ & & \\ 0 & & -\alpha\end{pmatrix}.$$

Since $\begin{pmatrix} 1 & & 0 \\ & 1 & \\ * & & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & & ** \\ & -1 & \\ 0 & & -1 \end{pmatrix}$, $\begin{pmatrix} \alpha+\alpha_{11} & & 0 \\ & \alpha+\alpha_{22} & \\ 0 & & \alpha+\alpha_{nn} \end{pmatrix}$ and $\begin{pmatrix} -\alpha & & 0 \\ & -\alpha & \\ 0 & & -\alpha \end{pmatrix}$ are regular matrices, A is a sum of regular matrices. Note: review(268.16).

(b) For $i \neq j$, $E_{ij}+I$ is invertible and $(E_{ij}+I)^{-1}$
$=-E_{ij}+I$. $(E_{ij}+I)E_{ii}(-E_{ij}+I)=E_{ii}(-E_{ij}+I)$
$=-E_{ij}+E_{ii}$.
$f(E_{ii})=f((E_{ij}+I)E_{ii}(-E_{ij}+I))=f(-E_{ij}+E_{ii})$
$=-f(E_{ij})+f(E_{ii})$, $f(E_{ij})=0$.
By Theorem 6.7.2 and Theorem 6.7.3.,
$f(E_{ii})=f(E_{jj})$ for all $i, j=1, \cdots\cdots, n$. Let
$\alpha_0=f(E_{11})=\cdots\cdots=f(E_{nn})$. For $A \in F_n$,
$A=\sum_{i,j}\alpha_{ij}E_{ij}$, $f(A)=f(\sum_{i,j}\alpha_{ij}E_{ij})=\sum_{i,j}\alpha_{ij}f(E_{ij})$
$=\sum_{i=1}^{n}\alpha_{ii}f(E_{ii})=\alpha_0\sum_{i=1}^{n}\alpha_{ii}=\alpha_0 \operatorname{tr} A$.

5. Prove the Jacobson lemma for elements $A, B \in F_n$ if n is less than the characteristic of F.

320.5 Since Lemma 6.8.3. is true when $n < p$, p is the characteric of F, Jacobson Lemma is also true when $n < p$.

6. (a) If $C \in F_n$, define the mapping d_C on F_n, by $d_C(X) = XC - CX$ for $X \in F_n$. Prove that $d_C(XY) = (d_C(X))Y + X(d_C(Y))$. (Does this remind you of the derivative?)

(b) Using (a), prove that if $AB - BA$ commutes with A, then for any polynomial $q(x) \in F[x]$, $q(A)B - Bq(A) = q'(A)(AB - BA)$, where $q'(x)$ is the derivative of $q(x)$.

320.6 (a) $d_c(XY)=XYC-CXY=X(YC-CY)+(XCY-CXY)$
$=X(d_c(Y))+(XC-CX)Y=(d_c(X))Y+X(d_c(Y))$.
(b) $d_B(A^2)=d_B(A)A+Ad_B(A)=2Ad_B(A)$.
$d_B(A^n)=d_B(A)A^{n-1}+Ad_B(A^{n-1})$
$=A^{n-1}d_B(A)+d_B(A^{n-1})A$
$=A^{n-1}d_B(A)+(n-1)A^{n-2}d_B(A)A$ (by induction hypothesis)
$=nA^{n-1}d_B(A)$.

$d_B(\sum_{i=1}^{n}a_iA^i)=\sum_{i=1}^{n}a_i d_B(A^i)$
$=\sum_{i=1}^{n}a_i iA^{i-1}d_B(A)$.

Hence $q(A)B-Bq(A)=d_B(q(A))=q'(A)d_B(A)=q'(A)\cdot(AB-BA)$.

*7. Use part (b) of Problem 6 to give a proof of the Jacobson lemma. (*Hint:* Let $p(x)$ be the minimal polynomial for A and consider $0 = p(A)B - Bp(A)$.)

320.7 Let P(x) be the minimal polynomial for A.
$0=P(A)B-BP(A)=P'(A)(AB-BA)=(AB-BA)P'(A)$.
$0=(AB-BA)(P'(A)B-BP'(A))(AB-BA)$
$=(AB-BA)(P''(A)(AB-BA))(AB-BA)$
$=P''(A)(AB-BA)^3=(AB-BA)^3P''(A)$.
In general, $P^{(k)}(A)(AB-BA)^{2^k-1}=(AB-BA)^{2^k-1}$.
$P^{(k)}(A)=0$. For,
$0=(AB-BA)^{2k-1}(P^{(k)}(A)B-BP^{(k)}(A))(AB-BA)^{2^k-1}$
(by induction hypothesis)
$=(AB-BA)^{2^k-1}(P^{(k+1)}(A)(AB-BA))(AB-BA)^{2^k-1}$
$=P^{(k+1)}(A)(AB-BA)^{2^{k+1}-1}=(AB-BA)^{2^{k+1}-1}P^{(k+1)}(A)$.
If deg $p(x)=n$, then $(n!)(AB-BA)^{2^n-1}=0$,
$(AB-BA)^{2^k-1}=0$. AB-BA is nilpotent.

8. (a) If A is a triangular matrix, prove that the entries on the diagonal

of A are exactly all the characteristic roots of A.

(b) If A is triangular and the elements on its main diagonal are 0, prove that A is nilpotent.

320.8 (a) By (285.28), we have the result.

(b) By Theorem 6.4.2, T satisfies x^n. Hence $T^n=0$. T is nilpotent.

9. For any $A, B \in F_n$ and $\lambda \in F$ prove that $(A')' = A$, $(A + B)' = A' + B'$, and $(\lambda A)' = \lambda A'$.

320.9 Let $A=(\alpha_{ij})$, $B=(\beta_{ij})$. $A+B=(\alpha_{ij}+\beta_{ij})$, $\lambda A=(\lambda\alpha_{ij})$. $A'=(\gamma_{ij})$, where $\gamma_{ij}=\alpha_{ji}$. $(A')'=(\delta_{ij})$, where $\delta_{ij}=\gamma_{ji}=\alpha_{ij}$. $(A')'=A$. $(A+B)'=(\theta_{ij})$, where $\theta_{ij}=\alpha_{ji}+\beta_{ji}$. $(A+B)'=A'+B'$. $(\lambda A)'=(\eta_{ij})$, $\eta_{ij}=\lambda\alpha_{ji}$. $(\lambda A)'=\lambda A'$.

10. If A is invertible, prove that $(A^{-1})' = (A')^{-1}$.

320.10 $I=(AA^{-1})'=(A^{-1})'A'$. $(A^{-1})^1=(A^1)^{-1}$.

11. If A is skew-symmetric, prove that the elements on its main diagonal are all 0.

320.11 If A is skew-symmetric, $A=(\alpha_{ij})$, then $A'=-A$. $\alpha_{ii}=-\alpha_{ii}$. $2\alpha_{ii}=0$.

On page 318, we have required that the characteristic of F is different from 2. $\alpha_{ii}=0$.

12. If A and B are symmetric matrices, prove that AB is symmetric if and only if $AB = BA$.

321.12 If AB is symmetric, then $(AB-BA)'=(AB)'-(BA)'=AB-A'B'=AB-AB=0$. $AB-BA=((AB-BA)')'=0'=0$. $AB=BA$.

Conversely, if $AB=BA$, then $(AB)'=(BA)'=A'B'=AB$. AB is symmetric.

13. Give an example of an A such that $AA' \neq A'A$.

321.13 Let $A=\begin{pmatrix}1&1\\0&0\end{pmatrix}$, $A'=\begin{pmatrix}1&0\\1&0\end{pmatrix}$. $AA'=\begin{pmatrix}2&0\\0&0\end{pmatrix}$, $A'A=\begin{pmatrix}1&1\\1&1\end{pmatrix}$. $AA' \neq A'A$.

*14. Show that A and A' are similar.

321.14 First we prove that

$J=\begin{pmatrix}\lambda&1&&0\\&\lambda&1&\\&&\ddots&1\\0&&&\lambda\end{pmatrix}$ is similar to $J'=\begin{pmatrix}\lambda&&&0\\1&\lambda&&\\&1&\lambda&\\0&&1&\lambda\end{pmatrix}$. For, let $C=\begin{pmatrix}0&&&1\\&&1&\\&\ddots&&\\1&&&0\end{pmatrix}$ then $CJC^{-1}=CJC=J'$.

Let K be the splitting field of the minimal poly-nomial for A. By Theorem 6.6.2., there is a B in K_n such that

$BAB^{-1}=\begin{pmatrix}J_1&&&0\\&J_2&&\\&&\ddots&\\0&&&J_k\end{pmatrix}$,

where J_i is Jordan form of A.

$(B')^{-1}A'B'=(B^{-1})'A'B'=(BAB^{-1})'=\begin{pmatrix}J_1'&&&0\\&J_2'&&\\&&\ddots&\\0&&&J_k'\end{pmatrix}$

A' is similar to $\begin{pmatrix}J_1'&&&0\\&J_2'&&\\&&\ddots&\\0&&&J_k'\end{pmatrix}$ and hence

similar to $\begin{pmatrix} J_1 & & 0 \\ & J_2 & \\ & \ddots & \\ 0 & & J_k \end{pmatrix}$. A and A′ are similar in K_n. By the Corollay to Theorem 6.7.3, A and A′ are similar in F_n.

15. The symmetric elements in F_n form a vector space; find its dimension and exhibit a basis for it.

321.15 $\{E_{ij}+E_{ji}, E_{ii} \mid i, j=1, \cdots\cdots, n,\ i \neq j\}$ forms a basis of the space of all symmetric elements in F_n. The dimension of the space is $\frac{n(n+1)}{2}$.

*16. In F_n let S denote the set of symmetric elements; prove that the subring of F_n generated by S is all of F_n.

321.16 $E_{ij}=E_{ii}(E_{ij}+E_{ji})$ for $i \neq j$. Therefore $\{E_{ij} \mid i, j=1, \cdots\cdots, n\} \subset S$. The subring of F_n generated by S is all of F_n.

*17. If the characteristic of F is 0 and $A \in F_n$ has trace 0 ($\mathrm{tr}\, A = 0$) prove that there is a $C \in F_n$ such that CAC^{-1} has only 0's on its main diagonal.

321.17 Use induction on n. n=1 is a trial case.

(i) Suppose there is a ω in $F^{(n)}$ such that $\omega, \omega A$ are linearly independent. By Lemma 4,2.5., there are vectors $v_3, \cdots\cdots, v_n$ such that $\{\omega, \omega A, v_3, \cdots\cdots, v_n\}$ forms a basis of $F^{(n)}$. Under this basis, the matrix of A is of the form

$$\begin{pmatrix} 0 & * \\ * & B \end{pmatrix}.$$

That is, there is a matrix C_1 in F_n such that

$$C_1AC_1^{-1}=\begin{pmatrix} 0 & * \\ * & B \end{pmatrix}.$$

$0=\mathrm{tr}\, A=\mathrm{tr}\,(C_1AC_1^{-1})=0+\mathrm{tr}\, B=\mathrm{tr}\, B$. By induction, there is a matrix C_2 in F_{n-1} such that

$$C_2BC_2^{-1}=\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}.$$

Let $C_3=\begin{pmatrix} 1 & 0 \cdots\cdots 0 \\ 0 & \\ \vdots & C_2 \\ 0 & \end{pmatrix}$. $C_3^{-1}=\begin{pmatrix} 1 & 0 \cdots\cdots 0 \\ 0 & \\ \vdots & C_2^{-1} \\ 0 & \end{pmatrix}$

$$(C_3C_1)A(C_3C_1)^{-1}=C_3(C_1AC_1^{-1})C_3^{-1}$$

$$=C_3\begin{pmatrix} 0 & * \\ * & B \end{pmatrix}C_3^{-1}$$

$$=\begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}.$$

$$=\begin{pmatrix} & \\ * & 0 \end{pmatrix}.$$

(ii) Suppose that $\omega, \omega A$ are linearly dependent for all ω in $F^{(n)}$.

$vA=\lambda_v v$ for some λ_v in F.

Let $v_1, \cdots\cdots, v_n$ be a basis of $F^{(n)}$ and $v_iA=\lambda_i v_i$, $i=1, \cdots\cdots, n$. For $i \neq 1$, $(v_i-v_1)A=\lambda(v_i-v_1)$ for some λ in F.

$\lambda_i v_i-\lambda_1 v_1=\lambda v_i-\lambda v_1$. $\lambda_i=\lambda=\lambda_1$ since v_i and v_1 are linearly indendent.

Hence $v_1A=\lambda_1 v_1$, $0=\mathrm{tr}A=n\lambda_1$, $\lambda_1=0$. $v_1A=0$.

$A=0$. This completes the proof.

*18. If F is of characteristic 0 and $A \in F_n$ has trace 0, prove that there exist $B, C \in F_n$ such that $A = BC - CB$. (*Hint:* First step, assume, by result of Problem 17, that all the diagonal elements of A are 0.)

321.18 In this exercise, as (313.7), we suppose the fact (Theorem 6.9.3) that A is invertible if and only if $\det A \neq 0$.

We first prove the case that the main diagonal entries of A are all zero. Let

$A=\begin{pmatrix} 0 & a_{12} \\ a_{21} & A_{22} \end{pmatrix}$,

where A_{22} is a $(n-1)\times(n-1)$ matrix and a_{12} a row vector of $F^{(n-1)}$ and a_{21} a column vector. By induction hypothesis, there are B_1, C_1 in F_{n-1} such that $A_{22}=B_1C_1-C_1B_1$. $\det(C_1-\lambda)$ is a polynomial of degree $n-1$. Therefore there is a c_{11} in F such that $\det(C_1-c_{11})\neq 0$. $C_1-c_{11}I$ is invertible. Let $b_{12}=a_{12}(C-c_{11}I)^{-1}$ and $b_{21}=(C-c_{11}I)^{-1}a_{21}$. Then, let

$$B=\begin{pmatrix} 0 & b_{12} \\ b_{21} & B_1 \end{pmatrix}, \quad C=\begin{pmatrix} c_{11} & 0 \\ 0 & C_1 \end{pmatrix}.$$

$$BC-CB=\begin{pmatrix} 0 & b_{12} \\ b_{21} & B_1 \end{pmatrix}\begin{pmatrix} c_{11} & 0 \\ 0 & C_1 \end{pmatrix}-\begin{pmatrix} c_{11} & 0 \\ 0 & C_1 \end{pmatrix}\begin{pmatrix} 0 & b_{12} \\ b_{21} & B_1 \end{pmatrix}$$

$$=\begin{pmatrix} 0 & b_{21}C \\ b_{21}c_{11} & BC \end{pmatrix}-\begin{pmatrix} 0 & c_{11}b_{12} \\ Cb_{21} & CB \end{pmatrix}$$

$$=\begin{pmatrix} 0 & b_{12}C-c_{11}b_{12} \\ b_{21}c_{11}-Cb_{21} & A_{22} \end{pmatrix}=\begin{pmatrix} 0 & a_{12} \\ a_{21} & A_{22} \end{pmatrix}=A.$$

Suppose now that $\operatorname{tr}A=0$. By (321.17), there is a D in F_n such that the main diagonal entries of DAD^{-1} are all zero. $DAD^{-1}=BC-CB$ for some B,C in F_n by the above paragraph. $A=D^{-1}(BC-CB)D=(D^{-1}BD)(D^{-1}CD)-(D^{-1}CD)(D^{-1}BD)$. This comletes the proof.

19. (a) If F is of characteristic not 2 and if $*$ is any adjoint on F_n, let $S=\{A\in F_n \mid A^*=A\}$ and let $K=\{A\in F_n \mid A^*=-A\}$. Prove that $S+K=F_n$.
(b) If $A\in F_n$ and $A=B+C$ where $B\in S$ and $C\in K$, prove that B and C are unique and determine them.

321.19 (a) For $A\in F_n$, $A=\dfrac{A+A^*}{2}+\dfrac{A-A^*}{2}$.

$$\left(\frac{A+A^*}{2}\right)=\left(\frac{A^*+A}{2}\right)=\frac{A+A^*}{2}\in S.$$

$$\left(\frac{A-A^*}{2}\right)^*=\left(\frac{A^*-A}{2}\right)=-\frac{A-A^*}{2}, \quad \frac{A-A^*}{2}\in K.$$

$A\in S+K$. $S+K=F_n$.

(b) Suppose $A=B+C=B_1+C_1$, $B,B_1\in S$, $C,C_1\in K$. $B-B_1=C_1-C$.

$C_1-C=B-B_1=B^*-B_1^*=(B-B_1)^*=(C_1-C)^*=C_1^*-C^*=-C_1+C=-(C_1-C)$. $2(C_1-C)=0$. $C_1-C=0$. $B-B_1=C_1-C=0$. $B=B_1$, $C=C_1$. B and C are uniqiue.

By (a) $B=\dfrac{A+A^*}{2}$, $C=\dfrac{A-A^*}{2}$.

20. (a) If $A, B\in S$ prove that $AB+BA\in S$.
(b) If $A, B\in K$ prove that $AB-BA\in K$.
(c) If $A\in S$ and $B\in K$ prove that $AB-BA\in S$ and that $AB+BA\in K$.

321.20 (a) $(AB+BA)^*=(AB)^*+(BA)^*=B^*A^*+A^*B^*=BA+AB=AB+BA$. $AB+BA\in S$.

(b) $(AB-BA)^*=(AB)^*-(BA)^*=B^*A^*-A^*B^*=(-B)(-A)-(-A)(-B)=BA-AB=-(AB-BA)$.

$AB-BA\in K$.

(c) $(AB-BA)^*=(AB)^*-(BA)^*=B^*A^*-A^*B^*=(-B)(A)-(A)(-B)=-BA+AB=AB-BA$. $AB-BA\in S$.

$(AB+BA)^*=(AB)^*+(BA)^*=B^*A^*+A^*B^*=(-B)(A)+(A)(-B)=-BA-AB=-(AB+BA)$. $AB+BA\in K$.

21. If ϕ is an automorphism of the field F we define the mapping Φ on F_n by: If $A=(\alpha_{ij})$ then $\Phi(A)=(\phi(\alpha_{ij}))$. Prove that $\Phi(A+B)=\Phi(A)+\Phi(B)$ and that $\Phi(AB)=\Phi(A)\Phi(B)$ for all $A, B\in F_n$.

321.21 Let $A=(\alpha_{ij})$, $B=(\beta_{ij})$. $\Phi(A)=(\phi(\alpha_{ij}))$, $\Phi(B)=(\phi(\beta_{ij}))$. $\Phi(A+B)=\Phi((\alpha_{ij}+\beta_{ij}))=(\phi(\alpha_{ij}+\beta_{ij}))=(\phi(\alpha_{ij})+\phi(\beta_{ij}))=(\phi(\alpha_{ij}))+(\phi(\beta_{ij}))=\Phi(A)+\Phi(B)$

$AB=(\gamma_{ij})$, $\gamma_{ij}=\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}$.

$$\phi(\gamma_{ij})=\phi\left(\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}\right)=\sum_{k=1}^{n}\phi(\alpha_{ik}\beta_{kj})$$

$= \sum_{k=1}^{n} \phi(\alpha_{ik})\phi(\beta_{kj})$.

$\Phi(AB) = (\phi(\gamma_{ij})) = (\phi(\alpha_{ij}))(\phi(\beta_{ij})) = \Phi(A)\Phi(B)$.

22. If $*$ and $\circledast$ define two adjoints on F_n, prove that the mapping $\psi: A \to (A^*)^{\circledast}$ for every $A \in F_n$ satisfies $\psi(A + B) = \psi(A) + \psi(B)$ and $\psi(AB) = \psi(A)\psi(B)$ for every $A, B \in F_n$.

321.22 $\phi(A+B) = ((A+B)^*)^{\circledast} = (A^*+B^*)^{\circledast} = (A^*)^{\circledast} + (B^*)^{\circledast}$
$= \phi(A) + \phi(B)$.
$\phi(AB) = ((AB)^*)^{\circledast} = (B^*A^*)^{\circledast} = (A^*)^{\circledast}(B^*)^{\circledast}$
$= \phi(A)\phi(B)$.

23. If $*$ is any adjoint on F_n and λ is a scalar matrix in F_n, prove that λ^* must also be a scalar matrix.

321.23 $A\lambda^* = (A^*)^* \lambda^* = (\lambda A^*)^* = (A^*\lambda)^* = \lambda^*(A^*)^* = \lambda^* A$ for all A in F_n. By (267.7) or (291.13), λ^* is a scalar matrix.

*24. Suppose we know the following theorem: If ψ is an automorphism of F_n (i.e., ψ maps F_n onto itself in such a way that $\psi(A + B) = \psi(A) + \psi(B)$ and $\psi(AB) = \psi(A)\psi(B)$) such that $\psi(\lambda) = \lambda$ for every scalar matrix λ, then there is an element $P \in F_n$ such that $\psi(A) = PAP^{-1}$ for every $A \in F_n$. On the basis of this theorem, prove: If $*$ is an adjoint of F_n such that $\lambda^* = \lambda$ for every scalar matrix λ then there exists a matrix $P \in F_n$ such that $A^* = PA'P^{-1}$ for every $A \in F_n$. Moreoever, $P^{-1}P'$ must be a scalar.

321.24 By definition of an adjoint, we know that $*$ is an anti-automorphism of F_n onto F_n. Define $\phi: F_n \to F_n$ as $\phi(A) = (A^*)'$. By (321.22), ϕ is a homomorphism of F_n into F_n. Clearly, ϕ is one-to-one and onto. ϕ is an automorphism of F_n onto F_n. By the given theorem, there is a P_1 is F_n such that $\phi(A) = P_1 A P_1^{-1}$ for all A in F_n.
$A^* = (P_1 A P_1^{-1})' = (P_1^{-1})' A' P_1' = (P_1')^{-1} A' P_1'$.
Let $P = (P_1^{-1})'$ we have $A^* = PA'P^{-1}$ for all A in F_n.

$A = (A^*)^* = P(A^*)'P^{-1} = P(PA'P^{-1})'P^{-1} = P(P^{-1})'AP'P^{-1}$.
$P(P^{-1})'A = A(P'P^{-1})^{-1} = A(P(P^{-1})')$ for all A in F_n.
By (267.7) or (291.13), $P(P^{-1})'$ is a scalar and $P^{-1}P' = (P(P^{-1})')'$ is a scalar.

25. If $P \in F_n$ is such that $P^{-1}P' \neq 0$ is a scalar, prove that the mapping defined by $A^* = PA'P^{-1}$ is an adjoint on F_n.

321.25 $(A^*)^* = (PA'P^{-1})^* = P(PA'P^{-1})'P^{-1}$
$= P(P^{-1})'AP'P^{-1} = A(P(P^{-1})')P'P^{-1}$
$= A$ since $((P^{-1})'P)^{-1} = P^{-1}P'$ is a scalar.
$(A+B)^* = P(A+B)'P^{-1} = P(A'+B')P^{-1}$
$= PA'P^{-1} + PB'P^{-1} = A^* + B^*$.
$(AB)^* = P(AB)'P^{-1} = PB'A'P^{-1} = (PB'P^{-1})(PA'P^{-1})$
$= B^* A^*$.
$*$ is an adjoint on F_n.

*26. Assuming the theorem about automorphisms stated in Problem 24, prove the following: If $*$ is an adjoint on F_n there is an automorphism ϕ of F of period 2 and an element $P \in F_n$ such that $A^* = P(\Phi(A))'P^{-1}$ for all $A \in F_n$ (for notation, see Problem 21). Moreover, P must satisfy $P^{-1}\Phi(P)'$ is a scalar.

Problems 24 and 26 indicate that a general adjoint on F_n is not so far removed from the transpose as one would have guessed at first glance.

322.26 Define $\phi: F \to F$ as $\phi(\lambda) = \lambda^*$. ϕ is an automorp-hism of F of period 2. For, by (321.23),
$\phi(\lambda) = \lambda^* \in F$. $\phi^2(\lambda) = \phi(\lambda^*) = (\lambda^*)^* = \lambda$.
ϕ is clearly onto. If $\phi(\lambda_1) = \phi(\lambda_2)$, $\lambda_1^* = \lambda_2^*$.
$\lambda_1 = (\lambda_1^*)^* = (\lambda_2^*)^* = \lambda_2$. ϕ is one-to-one.
$\phi(\lambda_1 + \lambda_2) = (\lambda_1 + \lambda_2)^* = \lambda_1^* + \lambda_2^* = \phi(\lambda_1) + \phi(\lambda_2)$.
$\phi(\lambda_1\lambda_2) = (\lambda_1\lambda_2)^* = \lambda_2^*\lambda_1^* = \lambda_1^*\lambda_2^* = \phi(\lambda_1)\phi(\lambda_2)$.
Define $\phi: F_n \to F_n$ as $\phi(A) = (\Phi(A)')^*$. ϕ is an automorphism of F_n with $\phi(\lambda) = \lambda$ for $\lambda \in F$.
By the given theorem, there is a P_1 in F_n such that

$\psi(A)=P_1AP_1^{-1}$.
$(\Phi(A)')^*=P_1AP_1^{-1}$. $P_1^{-1}(\Phi(A)')^*P_1=A$.
$A^*=P_1^*(\Phi(A))'(P_1^{-1})^*$. $I=I^*=(P_1P_1^{-1})^*$
$=(P_1^{-1})^*P_1^*$. $(P_1^*)^{-1}=(P_1^{-1})^*$. Let $P=P_1^*$.
$A^*=P(\Phi(A))'P^{-1}$,
for all A in F_n.
$A=(A^*)^*=P(\Phi(A^*))'P^{-1}=P[\Phi(P(\Phi(A))'P^{-1})]P^{-1}$
$=P[\Phi(P)\Phi((\Phi(A)')\Phi(P^{-1}))]'P^{-1}$
$=P[\Phi(P)A(\Phi(P))^{-1}]'P^{-1}$
$=P(\Phi(P)^{-1})'A(\Phi(P))'P^{-1}$.
By (267.7) or (291.13), $(\Phi(P))'P^{-1}=\lambda\in F$.
If $\lambda=0$, then $\Phi(P)=0$, $P=0$, a contradiction.
$\lambda\neq 0$. $\frac{1}{\lambda}(\Phi(P))'P^{-1}=1$. $P^{-1}(\frac{1}{\lambda}(\Phi(P))')=I$,
$P^{-1}(\Phi(P))'=\lambda$. This completes the proof.

*27. If ψ is an automorphism of F_n such that $\psi(\lambda)=\lambda$ for all scalars, prove that there is a $P\in F_n$ such that $\psi(A)=PAP^{-1}$ for every $A\in F_n$.

322.27 Define E_{ij} as we have done in (283.15). Let
$\delta_{ij}=1$ if $i=j$ and $\delta_{ij}=0$ if $i\neq j$.
$\psi(E_{ii})\psi(E_{jj})=\psi(E_{ii}E_{jj})=\psi(\delta_{ij}E_{ii})$
$=\delta_{ij}\psi(E_{ii})$ ……①

$\sum_{i=1}^{n}\psi(E_{ii})=\psi(\sum_{i=1}^{n}E_{ii})=\psi(I)=I$ ……②
$\psi(E_{ii})\neq 0$, $1\leq i\leq n$.
Claim that $V=F^{(n)}$ is a direct sum of $V\psi(E_{ii})$, $i=1,2,\cdots\cdots,n$. For, $v\in V$, by ②, we have

$v=vI=v\sum_{i=1}^{n}\psi(E_{ii})=\sum_{i=1}^{n}v\psi(E_{ii})$.

If $\sum_{i=1}^{n}v_i\psi(E_{ii})=0$ for some $v_1,\cdots\cdots,v_n$ in V, then

$0=(\sum_{i=1}^{n}v_i\psi(E_{ii}))\psi(E_{jj})$

$=\sum_{i=1}^{n}v_i\psi(E_{ii})\psi(E_{jj})$

$=v_j\psi(E_{jj})$
for $j=1,2,\cdots\cdots,n$. Hence V is the direct sum of $V\psi(E_{ii})$, $i=1,2,\cdots\cdots,n$.
Since $\psi(E_{ii})\neq 0$, $\dim_F V\psi(E_{ii})\geq 1$. That V is a sum of $V\psi(E_{ii})$ implies $\dim_F V\psi(E_{ii})=1$
$i=1,2,\cdots\cdots,n$.
Let $v_1=v\psi(E_{11})\in V\psi(E_{11})\setminus(0)$. Let
$v_i=v\psi(E_{ii})=v\psi(E_{ii}E_{ii})$
$=(v\psi(E_{ii}))\psi(E_{ii})\in V\psi(E_{ii})$
for $i=1,2,\cdots\cdots,n$.
$v_i\neq 0$. For, if $v_i=0$, then $v\psi(E_{ii})=0$.
$0=(v\psi(E_{ii}))\psi(E_{ii})=v\psi(E_{ii}E_{ii})=v\psi(E_{ii})=v_i\neq 0$
, a contradiction. Hence $\{v_1,v_2,\cdots\cdots,v_n\}$ forms a basis of V.
$v_i\psi(E_{kl})=(v\psi(E_{ii}))\psi(E_{kl})$
$=v\psi(E_{ii}E_{kl})$
$=\delta_{ik}v\psi(E_{il})$
$=\delta_{ik}v_l$.
Under the basis $\{v_1,\cdots\cdots,v_n\}$, the matrix of $\psi(E_{kl})$ is E_{kl}, for all $1\leq k,l\leq n$.
Therefore, by Theorem 6.3.2., there is an invertible matrix P such that
$\psi(E_{kl})=PE_{kl}P^{-1}$.
For A in F_n, $A=\sum_{i,j}a_{ij}E_{ij}$.

$\psi(A)=\psi(\sum_{i,j}a_{ij}E_{ij})=\sum_{i,j}a_{ij}\psi(E_{ij})=\sum_{i,j}a_{ij}PE_{ij}P^{-1}$

$=P(\sum_{i,j}a_{ij}E_{ij})P^{-1}=PAP^{-1}$.

*In the remainder of the problems, F will be the field of complex numbers and * the Hermitian adjoint on F_n.*

28. If $A\in F_n$ prove that there are unique Hermitian matrices B and C such that $A=B+iC$ $(i^2=-1)$.

322.28 Let $B=\frac{A+A^*}{2}$, $C=\frac{A^*-A}{2}i$. Then $A=B+iC$ and

$B^* = (\frac{A+A^*}{2})^* = \frac{A^*+A}{2} = B, C^* = (\frac{A^*-A}{2} i)^*$
$= (-i)(\frac{A-A^*}{2}) = C$, B and C are Hermitian.
If $A = B+iC = B_1+iC_1$ and B, B_1, C, C_1 are Hermitian, then $B-B_1 = i(C_1-C)$. $i(C_1-C) = B-B_1 = B^*-B_1^* = (B-B_1)^* = (i(C_1-C))^* = (C_1-C)^* i^* = (C_1^*-C^*)(-i) = -(C_1-C)i$. $C_1-C=0$. $C_1=C$. $B-B_1 = i(C_1-C) = 0$. $B=B_1$. There are unique Hermitian matrices B and C such that $A=B+iC$.

29. Prove that $\operatorname{tr} AA^* > 0$ if $A \neq 0$.

322.29 Let $A=(\alpha_{ij})$. $A^*=(\gamma_{ij})$, $\gamma_{ij}=\bar{\alpha}_{ji}$. $AA^* = (\sum_{k=1}^{n} \alpha_{ik} \gamma_{kj})$. $\operatorname{tr} AA^* = \sum_{i=1}^{n} (\sum_{k=1}^{n} \alpha_{ik} \gamma_{ki}) = \sum_{i=1}^{n} \sum_{k=1}^{n} \alpha_{ik} \bar{\alpha}_{ik} \geq 0$, and if $A \neq 0$, $\operatorname{tr} AA^* > 0$.

30. By directly computing the matrix entries, prove that if $A_1A_1^* + \cdots + A_kA_k^* = 0$, then $A_1 = A_2 = \cdots = A_k = 0$.

322.30 Let $A_r = (\alpha_{ij}^{(r)})$. Then $A_rA_r^* = (\sum_{k=1}^{n} \alpha_{ik}^{(r)} \bar{\alpha}_{jk}^{(r)})$. The (i,j) entry of $A_1A_1^* + \cdots + A_kA_k^*$ is $\sum_{r=1}^{k} (\sum_{k=1}^{n} \alpha_{ik}^{(r)} \bar{\alpha}_{jk}^{(r)}) = 0$.
Consider the (i,i) entry, we have $\sum_{r=1}^{k} \sum_{k=1}^{n} \alpha_{ik}^{(r)} \bar{\alpha}_{ik}^{(r)} = 0$. $\alpha_{ik}^{(r)} \bar{\alpha}_{ik}^{(r)} = 0$ for all r and k, $i=1,2,\cdots,n$. Hence $A_1 = \cdots = A_k = 0$.

31. If A is in F_n and if $BAA^* = 0$, prove that $BA = 0$.

322.31 $BAA^* = 0$. $BAA^*B^* = 0$. $(BA)(BA)^* = 0$. $BA = 0$.

32. If A in F_n is Hermitian and $BA^k = 0$, prove that $BA = 0$.

322.32 $k=1$, $BA=0$. $BA^k = 0$. $(BA^{k-2})AA^* = (BA^{k-2})AA = 0$. $(BA^{k-2})A = BA^{k-1} = 0$ by (322.31). $BA=0$ by induction.

33. If $A \in F_n$ is Hermitian and if λ, μ are two distinct (real) characteristic roots of A and if $C(A-\lambda) = 0$ and $D(A-\mu) = 0$, prove that $CD^* = DC^* = 0$.

322.33 $C(A-\lambda) = 0$. $C(A-\lambda)D^* = 0$. $C(A-\mu+(\mu-\lambda))D^* = 0$. $D(A-\mu) = 0$. $0 = 0^* = (D(A-\mu))^* = (A-\mu)^* D^* = (A-\mu)D^*$. $C(\mu-\lambda)D^* = 0$. $(\mu-\lambda)CD^* = 0$. $\mu-\lambda \neq 0$ implies $CD^* = 0$. $0 = 0^* = (CD^*)^* = DC^*$. $CD^* = DC^* = 0$.

*34. (a) Assuming that all the characteristic roots of the Hermitian matrix A are in the field of complex numbers, combining the results of Problems 32, 33, and the fact that the roots, then, must all be real and the result of the corollary to Theorem 6.6.1, prove that A can be brought to diagonal form; that is, there is a matrix P such that PAP^{-1} is diagonal.

(b) In part (a) prove that P could be chosen so that $PP^* = I$

322.34 (a) Let λ be a characteristic root of A. Suppose $(a_1, a_2, \cdots, a_n)(A-\lambda)^k = 0$ for some $k \geq 1$. Then

$$\begin{array}{c} \begin{matrix} a_1 & a_2 & \cdots & a_n \end{matrix} \\ \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \end{array} (A-\lambda)^k = 0.$$

$(A-\lambda)$ is Hermition. By (322.32),

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} (A-\lambda) = 0.$$

$(a_1, a_2, \cdots, a_n)(A-\lambda) = 0$. It follows from (305.14) that A is diagonalizable.
Hence there is a matrix P such that PAP^{-1} is diagonal.

(b) Let $\lambda_1, \cdots, \lambda_k$ be all distinct characteristic

roots of A. $U_{\lambda_i}=\{v\in F^{(n)} \mid vA=\lambda_i v\}$. By Gram-Schmidt orthogonalization process, we can find an orthonormal basis $(b_{11}^{\lambda_1}, b_{12}^{\lambda_1}, \cdots\cdots b_{1n}^{\lambda_1}), \cdots\cdots (b_{i_1 1}^{\lambda_{i_1}}, b_{i_1 2}^{\lambda_{i_1}}, \cdots b_{i_1 n}^{\lambda_{i_1}})$ of U_{λ_i}. For $(c_1, c_2, \cdots\cdots, c_n)\in U_{\lambda_i}$, and $(d_1, d_2, \cdots\cdots d_n)\in U_{\lambda_j}$, $\lambda_i\neq\lambda_j$

$$\begin{pmatrix} c_1 & c_2 & \cdots\cdots & c_n \\ 0 & 0 & \cdots\cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots\cdots & 0 \end{pmatrix} (A-\lambda_i)=0,$$

$$\begin{pmatrix} d_1 & d_2 & \cdots\cdots & d_n \\ 0 & 0 & \cdots\cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots\cdots & 0 \end{pmatrix} (A-\lambda_j)=0.$$

By (322.33), $\begin{pmatrix} c_1 & c_2 & \cdots\cdots & c_n \\ 0 & 0 & \cdots\cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots\cdots & 0 \end{pmatrix}$.

$$\begin{pmatrix} d_1 & d_2 & \cdots\cdots & d_n \\ 0 & 0 & \cdots\cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots\cdots & 0 \end{pmatrix}^* =0.$$

$\sum_{i=1}^{n} c_i\bar{d}_i=0$.

Since $V=U_{\lambda_1}\oplus U_{\lambda_2}\oplus\cdots\cdots\oplus U_{\lambda_k}$, arrange the veetors we have found, let

$$D=\begin{pmatrix} b_{11} & b_{12} & \cdots\cdots & b_{1n} \\ b_{21} & b_{22} & \cdots\cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots\cdots & b_{nn} \end{pmatrix}$$

DAD^{-1} is diagonal and $DD^*=1$.

35. Let $V_n=\{A\in F_n \mid AA^*=1\}$. Prove that V is a group under matrix multiplication.

322.35 $A,B\in V_n$. $(AB)(AB)^*=(AB)(B^*A^*)=A(BB^*)A^*$ $=AA^*=1$. $AB\in V_n$. $AA^*=1$. $(A^{-1})(A^{-1})^*=(A^{-1})(A^*)^{-1}=(A^*A)^{-1}=1$. $A^{-1}\in V_n$.

V_n is a group under matrix multiplication.

36. If A commutes with AA^*-A^*A prove that $AA^*\equiv A^*A$.

322.36
$$\begin{aligned}
&tr((AA^*-A^*A)(AA^*-A^*A)^*)\\
&=tr((AA^*-A^*A)((AA^*)^*-(A^*A)^*))\\
&=tr((AA^*-A^*A)(AA^*-A^*A))\\
&=tr(A(AA^*-A^*A)A^*-(AA^*-A^*A)A^*A)\\
&=tr((AAA^*A^*)-(AA^*AA^*)-(AA^*A^*A)\\
&\quad+(A^*AA^*A))\\
&=tr(AAA^*A^*)-tr(AA^*AA^*)-tr(AA^*A^*A)+tr(A^*AA^*A)\\
&=tr(AA^*A^*A)-tr(A^*AA^*A)-tr(AA^*A^*A)+tr(A^*AA^*A)\\
&=0.
\end{aligned}$$

By (322.29), $AA^*-A^*A=0$. $AA^*=A^*A$.

6.9. Determinants.

1. If F is the field of complex numbers, evaluate the following determinants:

(a) $\begin{vmatrix} 1 & i \\ 2-i & 3 \end{vmatrix}$. (b) $\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$. (c) $\begin{vmatrix} 5 & 6 & 8 & -1 \\ 4 & 3 & 0 & 0 \\ 10 & 12 & 16 & -2 \\ 1 & 2 & 3 & 4 \end{vmatrix}$.

334.1 (a) $\begin{vmatrix} 1 & i \\ 2-i & 3 \end{vmatrix} = 3-i(2-i) = 3-2i-1 = 2-2i$.

(b) $\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \\ 6 & 6 & 6 \end{vmatrix} = 0$.

(c) $\begin{vmatrix} 5 & 6 & 8 & -1 \\ 4 & 3 & 0 & 0 \\ 10 & 12 & 16 & -2 \\ 1 & 2 & 3 & 4 \end{vmatrix} = 0$.

2. For what characteristics of F are the following determinants 0:

(a) $\begin{vmatrix} 1 & 2 & 3 & 0 \\ 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 2 & 4 & 5 & 6 \end{vmatrix}$? (b) $\begin{vmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \\ 5 & 3 & 4 \end{vmatrix}$?

334.2 (a) $\begin{vmatrix} 1 & 2 & 3 & 0 \\ 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 2 & 4 & 5 & 6 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 & 0 \\ 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ -4 & -2 & -1 & 0 \end{vmatrix}$

$= -\begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ -4 & -2 & -1 \end{vmatrix} = -\begin{vmatrix} 1 & 2 & 3 \\ 2 & 0 & -2 \\ -3 & 0 & 2 \end{vmatrix}$

$= 2\begin{vmatrix} 2 & -2 \\ -3 & 2 \end{vmatrix} = 2(4-6) = -4$.

If the characteristic of F is 2, then the deteminant of (a) is 0.

(b) $\begin{vmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \\ 5 & 3 & 4 \end{vmatrix} = 3\cdot5\cdot4+4\cdot3\cdot5+4\cdot3\cdot5-5\cdot5\cdot5-3\cdot3\cdot3-4\cdot4\cdot4 = 180-216 = -36 = -2^2\cdot3^2$.

If the characteristic of F is 2 or 3, then the determinant of (b) is 0.

3. If A is a matrix with integer entries such that A^{-1} is also a matrix with integer entries, what can the values of det A possibly be?

334.3 $\det A \det A^{-1} = \det A A^{-1} = \det 1 = 1$.

$\det A$ and $\det A$ are integers. Hence $\det A = 1$ or -1.

4. Prove that if you add the multiple of one row to another you do not change the value of the determinant.

334.4 $d(v_1, v_2, \cdots\cdots, v_i+\lambda v_j, v_{i+1}, \cdots\cdots, v_j, \cdots\cdots, v_n)$

$= d(v_1, v_2, \cdots\cdots, v_i, \cdots\cdots, v_n) + \det(v_1, v_2, \cdots \cdots, \lambda v_j, \cdots\cdots, v_j, \cdots\cdots, v_n)$

$= d(v_1, \cdots\cdots, v_n) + 0$

$= d(v_1, \cdots\cdots, v_n)$.

*5. Given the matrix $A = (\alpha_{ij})$ let A_{ij} be the matrix obtained from A by removing the ith row and jth column. Let $M_{ij} = (-1)^{i+j} \det A_{ij}$. M_{ij} is called the *cofactor* of α_{ij}. Prove that $\det A = \alpha_{i1}M_{i1} + \cdots + \alpha_{in}M_{in}$.

334.5 Let $A=(a_{ij})$. $\tau_1 = (n\ n-1\ n-2\ \cdots\cdots\ i)$.

$\tau_2 = (n\ n-1\ n-2\ \cdots\cdots\ j)$. $M_{ij} = (b_{rs})$.

$a_{rs} = b_{\tau_1(r)\tau_2(s)}$.

For $\sigma \in S_n$ and $\sigma(i) = j$, consider the term

$(-1)^\sigma a_{1\sigma(1)} a_{2\sigma(2)} \cdots\cdots a_{ij} a_{i+1\sigma(i+1)} \cdots a_{n\sigma(n)}$

$= a_{ij}(-1)^\sigma b_{\tau_1(1)\tau_2(\sigma(1))} b_{\tau_1(2)\tau_2(\sigma(2))} \cdots\cdots$

$b_{\tau_1(i-1)\tau_2(\sigma(i-1))} b_{\tau_1(i+1)\tau_2(\sigma(i+1))} \cdots\cdots$

$b_{\tau_1(n)\tau_2(\sigma(n))}$.

$=a_{ij}(-1)^{\sigma} b_1\tau_2(\sigma(1))\, b_2\tau_2(\sigma(2)) \cdots\cdots b_{i-1}\tau_2(\sigma(i-1))$
$b_1\tau_2(\sigma(i+1)) \cdots\cdots b_{n-1}\tau_2(\sigma(n))$.
$=a_{ij}(-1)^{\sigma} b_1\tau_2(\sigma\tau_1^{-1}(1))\, b_2(\tau_2\sigma\tau_1^{-1}(2)) \cdots\cdots$
$b_{i-1}(\tau_2\sigma\tau_1^{-1}(i-1))\, b_1\tau_2(\sigma\tau_1^{-1}(i)) \cdots\cdots b_{n-1}\tau_2$
$(\sigma\tau_1^{-1}(n-1))$.
$=a_{ij}(-1)^{\sigma} b_1\tau(1) b_2\tau(2) \cdots\cdots b_{(n-1)}\tau(n-1)$ (where $\tau=\tau_2\sigma\tau_1^{-1}$)
$=(-1)^{i+j}(a_{ij}(-1)^{\tau} b_1\tau(1) b_2\tau(2) \cdots\cdots b_{(n-1)}\tau(n-1)$
$\sigma \longrightarrow \tau_2\sigma\tau_1^{-1}=\tau$
is 1—1 and onto. Hence
$\sum_{\sigma\in S_n} (-1)^{\sigma} a_{1\sigma(1)} \cdots\cdots a_{n\sigma(n)} = a_{i1}M_{i1}+a_{i2}M_{i2}$
$+ \cdots\cdots +a_{in}M_{in}$.
Note that $\tau=\tau_2\sigma\tau_1^{-1}$, $(-1)^{\tau}=(-1)^{n-j+1}(-1)^{\sigma}$
$(-1)^{n-i+1}=(-1)^{i+j}(-1)^{\sigma}$.

6. (a) If A and B are square submatrices, prove that

$$\det\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = (\det A)(\det B).$$

(b) Generalize part (a) to

$$\det\begin{pmatrix} A_1 & & * \\ & A_2 & \\ 0 & & \ddots \\ & & & A_n \end{pmatrix},$$

where each A_i is a square submatrix.

335.6 (a) Let $A=(a_{ij}), B=(b_{ij}), C=(c_{ij})$.
$\begin{pmatrix} A & C \\ O & B \end{pmatrix} = (x_{ij})$.

$$x_{ij} = \begin{cases} a_{ij} & 1\le i\le m,\ 1\le j\le m. \\ 0 & m+1\le i\le m+n,\ 1\le j\le m. \\ c_{i\,j-m} & 1\le i\le m,\ m+1\le j\le m+n \\ b_{i-m\ j-m} & m+1\le i\le m+n,\ m+1\le j\le m+n. \end{cases}$$

$$\det\begin{pmatrix} A & C \\ O & B \end{pmatrix} = \sum_{\sigma\in S_{m+n}} (-1)^{\sigma} x_{1\sigma(1)}x_{2\sigma(2)} \cdots\cdots$$
$x_{m\sigma(m)}x_{m+1\,\sigma(m+1)} \cdots\cdots x_{m+n\,\sigma(m+n)}$

If $\sigma(i)=j$, for some $m+1\le i\le m+n$ and $1\le j\le m$, then the term $(-1)^{\sigma}x_{1\sigma(1)} \cdots\cdots$ $x_{m\sigma(m)}x_{m+1\,\sigma(m+1)} \cdots\cdots x_{m+n\,\sigma(m+n)}=0$.
Hence consider $1\le\sigma(i)\le m$ if $1\le i\le m$ and $m+1\le\sigma(i)\le m+n$ if $m+1\le i\le m+n$.
For a fixed $\sigma\in S_m$, consider those τ in S_{m+n} which equal σ when restricted to $\{1, \cdots\cdots, m\}$.

$$\det\begin{pmatrix} A & C \\ O & B \end{pmatrix} = \Big(\sum_{\sigma\in S_m} (-1)^{\sigma} x_{1\sigma(1)} \cdots\cdots$$
$x_{m\sigma(m)}\Big)\Big(\sum_{\tau\in S_n} (-1)^{\tau} b_{1\tau(1)} \cdots\cdots b_{n\tau(n)}\Big)$
$=(\det A)\cdot(\det B)$.

(b) $\det\begin{pmatrix} A_1 & & * \\ & A_2 & \\ 0 & & A_n \end{pmatrix} = \det\begin{pmatrix} A_1 & & * \\ & A_2 & \\ 0 & & A_{n-1} \end{pmatrix}$
$(\det A_n) = ((\det A_1)(\det A_2) \cdots\cdots (\det A_{n-1}))(\det A_n)$ (by induction) $= (\det A_1)(\det A_2)$
$\cdots\cdots (\det A_n)$.

7. If $C(f)$ is the companion matrix of the polynomial $f(x)$, prove that the secular equation of $C(f)$ is $f(x)$.

335.7 Let $p(x)$ be the secular equation of $C(f)$. By Theorem 6.9.5., $C(f)$ satisfies $p(x)$. By (312.4), $f(x)$ is the minimal polynomial for $C(f)$. $f(x) \mid p(x)$. Since $\deg f(x)=n=\deg p(x)$ and $p(x)$ and $f(x)$ are monic, $f(x)=p(x)$. The secular equation of $C(f)$ is $p(x)=f(x)$.

8. Using Problems 6 and 7, prove that the secular equation of A is its characteristic polynomial. (See Section 6.7; this proves the remark made earlier that the roots of $p_T(x)$ occur with multiplicities equal to their multiplicities as characteristic roots of T.)

335.8 Let $q_1(x), \cdots\cdots q_n(x)$ be the elementery divisors of T. By definition, the characteristic polyno-

mial of T is $q_1(x) \cdot q_2(x) \cdots\cdots q_n(x)$.

By the Corollary to Theorem 6.7.1., T is similar to

$$\begin{pmatrix} C(q_1) & & \\ & C(q_2) & \\ & & C(q_n) \end{pmatrix}.$$

By Corollary 2 to Theorem 6.9.1 and (335.6.(b)), the secular equation of T is $q_1(x) \cdots\cdots q_n(x)$. Hence the secular equation of T is its characteristic polynomial.

9. Using Problem 8, give an alternative proof of the Cayley-Hamilton theorem.

335.9 By the Remark on page 309 and (335.8), every A in F_n satisfies its secular equation.

10. If F is the field of rational numbers, compute the secular equation, characteristic roots, and their multiplicities, of

(a) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. (b) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 7 \end{pmatrix}$. (c) $\begin{pmatrix} 4 & 1 & 1 & 1 \\ 1 & 4 & 1 & 1 \\ 1 & 1 & 4 & 1 \\ 1 & 1 & 1 & 4 \end{pmatrix}$.

335.10 (a) $$\det\left(x - \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\right) = x^4 - 1.$$

The characteristic roots of (a) are $1, -1$.

(b) $$\det\left(x - \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 7 \end{pmatrix}\right) = x^3 - 10x^2 + 6x.$$

The characteristic root of (b) is 0.

(c) $$\det\left(x - \begin{pmatrix} 4 & 1 & 1 & 1 \\ 1 & 4 & 1 & 1 \\ 1 & 1 & 4 & 1 \\ 1 & 1 & 1 & 4 \end{pmatrix}\right) = (x-7)(x-3)^3.$$

The characteristic root (c) is 7, 3, 3, 3.

11. For each matrix in Problem 10 verify by direct matrix computation that it satisfies its secular equation.

335.11 (a) $$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}^4 = 1.$$

(b) $$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 7 \end{pmatrix}^2 = \begin{pmatrix} 14 & 18 & 32 \\ 18 & 24 & 42 \\ 32 & 42 & 74 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 7 \end{pmatrix}^3 = \begin{pmatrix} 146 & 192 & 338 \\ 192 & 252 & 444 \\ 338 & 444 & 782 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 7 \end{pmatrix}^3 - 10 \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 7 \end{pmatrix}^2 + 6 \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 7 \end{pmatrix} = 0.$$

(C) $$\begin{pmatrix} 4 & 1 & 1 & 1 \\ 1 & 4 & 1 & 1 \\ 1 & 1 & 4 & 1 \\ 1 & 1 & 1 & 4 \end{pmatrix}$$ satisfies its secular equation.

*12. If the rank of A is r, prove that there is a square $r \times r$ submatrix of A of determinant different from 0, and if $r < n$, that there is no $(r+1) \times (r+1)$ submatrix of A with this property.

335.12 See

Jacobson, N. Lectures in Abstract Algebra. (Vol2) page 22 ~ 24.

*13. Let f be a function on n variables from $F^{(n)}$ to F such that

(a) $f(v_1, \ldots, v_n) = 0$ for $v_i = v_j \in F^{(n)}$ for $i \neq j$.

(b) $f(v_1, \ldots, \alpha v_i, \ldots, v_n) = \alpha f(v_1, \ldots, v_n)$ for each i, and $\alpha \in F$.

(c) $f(v_1, \ldots, v_i + u_i, v_{i+1}, \ldots, v_n) = f(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n) + f(v_1, \ldots, v_{i-1}, u_i, v_{i+1}, \ldots, v_n)$.

(d) $f(e_1, \ldots, e_n) = 1$, where $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots, e_n = (0, 0, \ldots, 0, 1)$.
Prove that $f(v_1, \ldots, v_n) = \det A$ for any $A \in F_n$, where v_1 is the first row of A, v_2 the second, etc.

335.13 If f satisfies (a), (b), (c), then Lemma 6.9.5, Lemma 6.9.4 hold.

Clearly, det satisfies (a), (b), (c) and (d).

D=(det−f) satisfies (a), (b) and (c).

$(\det - f)(e_1, e_2, \cdots\cdots, e_n) = \det(e_1, e_2, \cdots\cdots, e_n) - f(e_1, e_2, \cdots\cdots, e_n) = 0.$

$$(\det - f)\left(\sum_{j_1=1}^{n} a_{1j_1} e_{j_1}, \sum_{j_2=1}^{n} a_{2j_2} e_{j_2}, \cdots\cdots, \sum_{j_n=1}^{n} a_{nj_n} e_{j_n}\right)$$

$$= \sum_{j_1, j_2, \cdots, j_n=1} a_{1j_1} a_{2j_2} \cdots\cdots a_{nj_n} (\det - f)(e_{j_1}, e_{j_2}, \cdots\cdots, e_{j_n})$$

If some index of $D(e_{j_1}, \cdots\cdots, e_{j_n})$ are equal, then $D(e_{j_1}, \cdots\cdots, e_{j_n}) = 0$ since D satisfies (a), (b) and (c).

If all the index of $D(e_{j_1}, \cdots\cdots, e_{j_n})$ are distinct, then

$|D(e_{j_1}, e_{j_2}, \cdots\cdots e_{j_n})| = |D(e_1, \cdots\cdots, e_n)| = 0$. Hence $D(v_1, \cdots\cdots v_n) = 0$ for all $v_1, \cdots\cdots v_n$ in $F^{(n)}$.

D=0. det−f=0. det=f.

14. Use Problem 13 tc prove that $\det A' = \det A$.

335.14 Define $f(A) = \det A'$. f satisfies the conditions of (335.13). Hence $\det A' = f(A) = \det A$.

15. (a) Prove that *AB* and *BA* have the same secular (characteristic) equation.
(b) Give an example where *AB* and *BA* do *not* have the same minimal polynomial.

336.15 (a) we suggest the reader see

Jacbson, N, Lectures in Abstract Algebra. page 104 ~ 106. or the following :

Find an extension field K of F such that K has infinite elements. In fact, we want an extension field K of F which has elements more than 2n, suppose A,B are n×n matrices. $A, B \in K_n$.

If A is invertible, then $\det(xI - AB) = \det(A^{-1}(xI - AB)A) = \det(xI - BA)$.

For a fixed a in ,

$f(x) = \det(aI - (xI + A)B) - \det(aI - B(xI + A))$

is a polynomial of degree at most n. f(x) has at most n roots in K if it is not zero.

$\det(xI + A)$ bas at most n roots in K. For α in K, α is not a root of $\det(xI + A)$, we have that $\alpha I + A$ is invertible. Hence $f(\alpha) = 0$. f(x) bas at least n+1 roots in K. Therefore f(x)=0.

In particular, $f(0) = \det(aI - AB) - \det(aI - BA) = 0$. $\det(aI - AB) - \det(aI - BA) = 0$ for all a in K.

$g(x) = \det(xI - AB) - \det(xI - BA)$

has more than 2n roots. g(x)=0.

$\det(xI - AB) = \det(xI - BA)$.

This poves that AB and BA have the same secular equation.

(Note that we have not proved the fact that we can find an extension field K of F which has elements more than a given positive integer (2n). Try to prove this!)

(b)

Let $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

$AB = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $BA = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

The minimal polynomial for AB is x^2 but the minimal polynomial for BA is x.

16. If A is triangular prove by a direct computation that A satisfies its secular equation.

336.16 See (290.4).

17. Use Cramer's rule to compute the solutions, in the real field, of the systems

(a) $x + y + z = 1$,
$2x + 3y + 4z = 1$,
$x - y - z = 0$.

(b) $x + y + z + w = 1$,
$x + 2y + 3z + 4w = 0$,
$x + y + 4z + 5w = 1$,
$x + y + 5z + 6w = 0$.

336.17 (a) $x = \frac{1}{2}$, $y = 2$, $z = -\frac{3}{2}$.

(b) $x = 4$, $y = -2$, $z = -4$, $w = 3$.

18. (a) Let $GL(n, F)$ be the set of all elements in F_n whose determinant is different from 0. Prove $GL(n, F)$ is a group under matrix multiplication.

(b) Let $D(n, F) = \{A \in GL(n, F) \mid \det A = 1\}$. Prove that $D(n, F)$ is a normal subgroup of $GL(n, F)$.

(c) Prove that $GL(n, F)/D(n, F)$ is isomorphic to the group of nonzero elements of F under multiplication.

336.18 (a) $A \in GL(n,F)$. $\det A \neq 0$. $A^{-1} \in F_n$.
$\det A^{-1} \neq 0$. $A^{-1} \in GL(n,F)$. $\det B \neq 0$.
$\det AB = \det A \det B \neq 0$. $AB \in GL(n,F)$.
$C \in GL(n,F)$. $(AB)C = A(BC)$. $\det I = 1$,
$I \in GL(n,F)$. $AI = IA = A$.
$GL(n,F)$ is a group under matrix mutiplication.

(b) $A \in D(n,F)$, $B \in D(n,F)$, $\det A = \det B = 1$.
$\det AB = \det A \det B = 1$.
$\det A^{-1} = \frac{1}{\det A} = 1$. $AB, A^{-1} \in D(n,F)$. $D(n,F)$ is a subgroup of $G(n,F)$. $C \in G(n,F)$,
$\det(CAC^{-1}) = \det A = 1$, $CAC^{-1} \in D(n,F)$.
$D(n,F)$ is a normal subgroup of $G(n,F)$.

(c) $\det : G(n,F) \longrightarrow F$ is a group homormorphism.

Since $\det \begin{pmatrix} \lambda & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = \lambda$ for all λ in F,

$\det$ is an onto mapping. The kernel of $\det$ is $D(n,F)$. Hence $GL(n,F)/D(n,F)$ is isomorphic to the group of nonzero elements of F under mutiplication.

19. If K be an extension field of F, let $E(n, K, F) = \{A \in GL(n, K) \mid \det A \in F\}$.

(a) Prove that $E(n, K, F)$ is a normal subgroup of $GL(n, K)$.

*(b) Determine $GL(n, K)/E(n, K, F)$.

336.19 Define $T : G(n,K) \longrightarrow (K\setminus(0)) / (F\setminus(0))$, where $K\setminus(0)$ is the group of nonzero elements of K under multiplication and $F\setminus(0)$ is the group of nonzero elements of F under multiplications, as $T(A) = \det A + (F\setminus(0))$.
T is cleary a homomorphism of $G(n,K)$ onto $(K\setminus(0)) / (F\setminus(0)))$. The kernel is evidently $E(n,K,F)$. Hence $GL(n,K) / E(n,K,F) \approx (K\setminus(0)) / (F\setminus(0))$. $E(n,K,F)$ is a nomal subgroup of $GL(n,K)$.

*20. If F is the field of rational numbers, prove that when N is a normal subgroup of $D(2, F)$ then either $N = D(2, F)$ or N consists only of scalar matrices.

336.20 Let Z be the set of all scalar matrices. Let N be a normal subgroup of $D(2,F)$ and contains an element A not in Z.
The characteristic polyomial for A is $x^2 - \alpha x + 1$.
By Lemma 6.7.1, A is similar to $\begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix}$.

Hence $\begin{pmatrix} 0 & 1 \\ -1 & \alpha \end{pmatrix} \in N$.

Let $T=\begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \in D(2,F)$.

$TAT^{-1}A^{-1}=\begin{pmatrix} 4 & 0 \\ \frac{3}{4}\alpha & \frac{1}{4} \end{pmatrix} \in N$.

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 4 & 0 \\ \frac{3}{4}\alpha & \frac{1}{4} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{4} & 0 \\ -\frac{3}{4}\alpha & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ \frac{15}{16} & 1 \end{pmatrix} \in N .$$

Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in D(2,F)$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$

$$= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} .$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \frac{15}{16} & 1 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} =$$

$$\begin{pmatrix} a+\frac{15}{16}b & b \\ c+\frac{15}{16}d & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \begin{pmatrix} ad+\frac{15}{16}bd-bc & -ab-\frac{15}{16}b^2+ab \\ cd+\frac{15}{16}d^2-dc & -bc-\frac{15}{16}bd+ad \end{pmatrix}$$

$$= \begin{pmatrix} 1+\frac{15}{16}bd & -\frac{15}{16}b^2 \\ \frac{15}{16}d^2 & 1-\frac{15}{16}bd \end{pmatrix} \in N .$$

$u>0$, $\begin{pmatrix} \sqrt{\frac{15}{16u}} & 0 \\ 0 & \sqrt{\frac{16}{15}u} \end{pmatrix} \in D(2,F)$ implies

$\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \in N$.

$\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}^{-1}=\begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix} \in N$. Hence $\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \in N$ for all u in F.

$\lambda<0$, $\begin{pmatrix} 0 & -\sqrt{-\frac{16\lambda}{15}} \\ \sqrt{-\frac{15}{16\lambda}} & 0 \end{pmatrix} \in D(2,F)$ implies

$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \in N$, $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^{-1}=\begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \in N$.

Hence $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \in N$ for all λ in F.

For $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in D(2,F)$ with $a_{21} \neq 0$, we have $\begin{pmatrix} 1 & a_{21}^{-1}(a_{11}-1) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a_{21} & 1 \end{pmatrix}$

$$\begin{pmatrix} 1 & a_{21}^{-1}(a_{22}-1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21}^{-1}(a_{11}-1) \\ a_{21} & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & a_{21}^{-1}(a_{22}-1) \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{11}a_{21}^{-1}(a_{22}-1)+a_{21}^{-1}(a_{11}-1) \\ a_{21} & a_{22} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{21}^{-1}(a_{11}a_{22}-a_{11}+a_{11}-1) \\ a_{21} & a_{22} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{21}^{-1}(a_{11}a_{22}-(a_{11}a_{22}-a_{21}a_{12}) \\ a_{21} & a_{22} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in N .$$

For $\begin{pmatrix} a_{11} & a_{21} \\ 0 & a_{22} \end{pmatrix} \in D(2,F)$, we have $a_{11} \neq 0$ and

$$\begin{pmatrix} a_{11} & a_{21} \\ 0 & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} \\ a_{11} & a_{21}+a_{22} \end{pmatrix} \in N .$$

Therefore $D(2,F)=N$. This completes the proof.
(Note : c.f. (118.33.(b)))

6.10. Hermitian, Unitary, and Normal Transformations

1. Determine which of the following matrices are unitary, Hermitian, normal.

(a) $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. (b) $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. (c) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

(d) $\begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix}$. (e) $\begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$.

2. For those matrices in Problem 1 which are normal, find their characteristic roots and bring them to diagonal form by a unitary matrix.

349.1 (a)
349.2 $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ is not normal since

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^* = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^*$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 2 & 3 \end{pmatrix} .$$

(b) $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ is unitary.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

(c) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ is unitary and Hermitian.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

(d) $\begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix}$ is not normal since

$$\begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix} \begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix}^* = \begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2+i \\ 2+i & -i \end{pmatrix} = \begin{pmatrix} 6 & 1-i \\ 1+i & 6 \end{pmatrix}$$

$$\neq \begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix}^* \begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix} = \begin{pmatrix} 1 & 2+i \\ 2+i & -i \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix} = \begin{pmatrix} 6 & 1+i \\ 1-i & 6 \end{pmatrix}.$$

(e) $\begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ is normal.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{-i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} & 0 \\ 0 & 0 & \frac{1-i}{\sqrt{2}} \end{pmatrix}$$

3. If T is unitary, just using the definition $(vT, uT) = (v, u)$, prove that T is nonsingular.

349.3 If $vT=0$ for some v in V, then $0=(vT, vT)=(v, v)$. $v=0$. T is nonsigular.

4. If Q is a real orthogonal matrix, prove that $\det Q = \pm 1$.

349.4 $QQ^*=1$, $Q^*=Q'$. $\det Q=\det Q'$. $1=\det 1=\det(QQ^*)=\det Q \det Q'.(\det Q)^2=1$. $\det Q=\pm 1$.

5. If Q is a real symmetric matrix satisfying $Q^k = 1$ for $k \geq 1$, prove that $Q^2 = 1$.

349.5 Q is Hermitian. The characteristic roots of Q are real. By Corollary 2 to Theorem 6.10.4., there is a unitary matrix U such that UQU^{-1} is diagonal.

$$UQU^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

$$(UQU^{-1})^k = UQ^kU^{-1} = UU^{-1} = 1$$

$$= \begin{pmatrix} \lambda_1^k & & 0 \\ & \ddots & \\ 0 & & \lambda_n^k \end{pmatrix}$$

$\lambda_1^k = 1$ for $i=1, 2, \cdots\cdots, n$.

λ_1 is a real number. $\lambda_k = \pm 1$.

$$(UQU^{-1})^2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=UQ^2U^{-1}.$$

$\therefore Q^2=1$.

6. Complete the proof of Lemma 6.10.4 by showing that $(S+T)^*=S^*+T^*$ and $(\lambda T)^*=\bar{\lambda}T^*$.

349.6 If u,v are in V, then $(u,v(S+T)^*)=(u(S+T),v)=(uS+uT,v)=(uS,v)+(uT,v)=(u,vS^*)+(u,vT^*)=(u,vS^*+vT^*)=(u,v(S^*+T^*))$, in consequence of which $v(S+T)^*=v(S^*+T^*)$ and $(S+T)^*=S^*+T^*$.

Similarly, for $\lambda\in F$, $(u,v(\lambda T)^*)=(u(\lambda T),v)=(\lambda(uT),v)=(uT,\bar{\lambda}v)=(u,(\bar{\lambda}v)T^*)=(u,v(\bar{\lambda}T^*))$, in consequence of which $v((\lambda T)^*)=v(\bar{\lambda}T^*)$ and $(\lambda T)^*=\bar{\lambda}T^*$.

7. Prove the properties of $*$ in Lemma 6.10.4 by making use of the explicit form of $w=vT^*$ given in the proof of Lemma 6.10.3.

349.7 $vT^*=\sum_{i=1}^{n}\overline{(u_iT,v)}u_i$, where $\{u_1,\cdots\cdots,u_n\}$ is an orthonormal basis.

$$(1)\ v(T^*)^*=\sum_{i=1}^{n}\overline{(u_iT^*,v)}\,u_i$$
$$=\sum_{i=1}^{n}\overline{\Big(\sum_{j=1}^{n}\overline{(u_jT,u_i)}u_j,v\Big)}u_i$$
$$=\sum_{i=1}^{n}\sum_{j=1}^{n}(u_jT,u_i)\overline{(u_j,v)}u_i$$
$$=\sum_{j=1}^{n}(v,u_j)\Big(\sum_{i=1}^{n}(u_jT,u_i)u_i\Big)$$
$$=\sum_{j=1}^{n}(v,u_j)(u_jT)$$
$$=\Big(\sum_{j=1}^{n}(v,u_j)\,u_j\Big)T$$
$$=vT,$$

for all v in V, $(T^*)^*=T$.

$$(2)\ v(S+T)^*=\sum_{i=1}^{n}\overline{(u_i(S+T),v)}u_i$$
$$=\sum_{i=1}^{n}\overline{(u_iS+u_iT,v)}u_i$$
$$=\sum_{i=1}^{n}\overline{(u_iS,v)}u_i+\sum_{i=1}^{n}\overline{(u_iT,v)}u_i$$
$$=vS^*+vT^*$$
$$=v(S^*+T^*),$$

for all v in V. $(S+T)^*=S^*+T^*$.

$$(3)\ v(\lambda S)^*=\sum_{i=1}^{n}\overline{(u_i(\lambda S),v)}u_i$$
$$=\sum_{i=1}^{n}\overline{(\lambda u_iS,v)}u_i$$
$$=\sum_{i=1}^{n}\bar{\lambda}\,\overline{(u_iS,v)}u_i$$
$$=\bar{\lambda}\sum_{i=1}^{n}\overline{(u_iS,v)}u_i$$
$$=\bar{\lambda}(vS^*)$$
$$=v(\bar{\lambda}S^*),$$

for all v in V. $\lambda S^*=\bar{\lambda}S^*$.

$$(4)\ v(ST)^*=\sum_{i=1}^{n}\overline{(u_i(ST),v)}u_i$$
$$=\sum_{i=1}^{n}\overline{((u_iS)T,v)}u_i$$
$$=\sum_{i=1}^{n}\overline{\Big(\sum_{j=1}^{n}(u_iS,u_j)u_jT,v\Big)}u_i$$
$$=\sum_{i=1}^{n}\sum_{j=1}^{n}\overline{(u_iS,u_j)}\,\overline{(u_jT,v)}u_i$$
$$=\sum_{j=1}^{n}\Big(\sum_{i=1}^{n}\overline{(u_iS,u_j)}u_i\Big)\overline{(u_jT,v)}$$
$$=\sum_{j=1}^{n}(u_jS^*)\overline{(u_jT,v)}$$
$$=\sum_{j=1}^{n}\overline{(u_jT,v)}(u_jS^*)$$

$$=\Big(\sum_{j=1}^{n}(\overline{u_jT,v})u_j\Big)S^*$$
$$=(vT^*)S^*$$
$$=v(T^*S^*),$$
for all v in V. $(ST)^*=T^*S^*$.

8. If T is skew-Hermitian, prove that all of its characteristic roots are pure imaginaries.

349.8 Let λ be a characteristic root of T and $vT=\lambda v$, $v\neq 0$. $\lambda(v,v)=(\lambda v,v)=(vT,v)=(v,vT^*)=(v,v(-T))=(v,-vT)=(v,-\lambda v)=-\overline{\lambda}(v,v)$, $(v,v)\neq 0$. $\lambda=-\overline{\lambda}$. λ is a pure imaginary.

9. If T is a real, skew-symmetric $n \times n$ matrix, prove that if n is odd, then $\det T = 0$.

349.9 $\det T=\det T'=\det(-T)=\det(-1)\det T=(-1)^n \det T$ $=-\det T$. $\det T=0$.

10. By a direct matrix calculation, prove that a real, 2×2 symmetric matrix can be brought to diagonal form by an orthogonal one.

349.10 Let $A=\begin{pmatrix}\alpha & \beta\\ \beta & \gamma\end{pmatrix}$. The characteristic roots of A are $\frac{\alpha+\gamma+\sqrt{(\alpha-\gamma)^2+4\beta^2}}{2}$ and $\frac{\alpha+\gamma-\sqrt{(\alpha-\gamma)^2+4\beta^2}}{2}$. Suppose $(\alpha-\gamma)^2+4\beta^2\neq 0$.

Let $a=\sqrt{\frac{2}{(\alpha-\gamma)^2+4\beta^2+(-\alpha+\gamma)\sqrt{(\alpha-\gamma)^2+4\beta^2}}}$,

$b=\sqrt{\frac{2}{(\alpha-\gamma)^2+4\beta^2-(-\alpha+\gamma)\sqrt{(\alpha-\gamma)^2+4\beta^2}}}$,

$$U=\begin{pmatrix} a\beta & \frac{-\alpha+\gamma+\sqrt{(\alpha-\gamma)^2+4\beta^2}}{2}a\\ b\beta & \frac{-\alpha+\gamma-\sqrt{(\alpha-\gamma)^2+4\beta^2}}{2}b\end{pmatrix}$$

$$UAU^{-1}=\begin{pmatrix}\frac{\alpha+\gamma+\sqrt{(\alpha-\gamma)^2+4\beta^2}}{2} & 0\\ 0 & \frac{\alpha+\gamma-\sqrt{(\alpha-\gamma)^2+4\beta^2}}{2}\end{pmatrix}.$$

If $(\alpha-\gamma)^2+4\beta^2=0$, then $\beta=0$ and $\alpha=\gamma$.

$A=\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix}$.

11. Complete the proof outlined for the matrix-equivalent part of Theorem 6.10.4.

349.11 By Theorem 6.10.1. and Theorm 6.3.2., we get the matrix-equivalent part of Theorem 6.10.4.

12. Prove that a normal transformation is unitary if and only if the characteristic roots are all of absolute value 1.

349.12 Suppose T is unitary. Let λ be a characteristic root of T and $vT=\lambda v, v\neq 0$.
$(v,v)=(vTT^*,v)=(vT,vT)=(\lambda v,\lambda v)=\lambda\overline{\lambda}(v,v)$.
Since $(v,v)\neq 0$, $\lambda\overline{\lambda}=|\lambda|^2=1$.
The characteristic roots of T are all of absolute value 1.
Conversely, suppose T is normal and the characteristic roots of T are all of absolute value 1.
We argue using matrices. By Theorem 6.10.4., there is a unitary matrix U such that $UTU^{-1}=UTU^*=D$, where D is a diagonal matrix with absolute value 1 entries on the diagonal.
Thus $DD^*=1$. $D^*=(UTU^*)^*=UT^*U^*$.
$1=DD^*=(UTU^{-1})(UT^*U^*)=UTT^*U^*=UTT^*U^{-1}$, $TT^*=U^{-1}U=1$. T is unitary.

13. If $N_1,\ldots,N_k$ is a finite number of commuting normal transformations, prove that there exists a unitary transformation T such that all of TN_iT^{-1} are diagonal.

349.13 We argue using matrices.

Use indiuction on dim V. dimV=1, we are done.

(i) Suppose $U_{\lambda_i}(N_i)=\{ v\in V \mid vN_i=\lambda_i v \}=V$, where λ_i is a characteristic root of N_i, $i=1, 2, \cdots\cdots, k$. Then $N_i=\lambda_i$.
In this case, we are also done.

(ii) Suppose there is an N_i such that $U_\lambda(N_i)\neq V$ for a characteristic root λ of N_i.
$V=U_{\lambda_1}(N_i)\oplus U_{\lambda_2}(N_i)\oplus\cdots\cdots\oplus U_{\lambda_r}(N_i)$, where $\lambda_1, \cdots\cdots, \lambda_r$ are all characteristic roots of N_i.
Every $U_\lambda(N_i)$ is invariant under each N_j for $\lambda=\lambda_1, \cdots\cdots, \lambda_r$. N_j induces a linear tranformation on $N_\lambda(N_i)$ which is clarly normal. dim $U_\lambda(N_i)<$ dim V. By induction hypothesis, there is an orthonormal basis of $U_\lambda(N_i)$ such that N_j is diagonal in this basis. Combining these bases, we have an orthonormal basis of V. In this basis, all N_j are diagonal. By Theroem 6.10.1 and Theorem 6.3.2, there exists a unitary matrix T such that all TN_jT^{-1} are diagonal.

14. If N is normal, prove that $N^* = p(N)$ for some polynomial $p(x)$.

350.14 We argue using matrices. Let $a_1, a_2, \cdots\cdots, a_k$ be the distinct characteristic roots of N.
Consider the system of linear equations

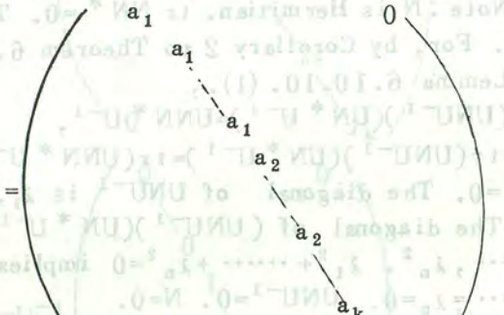
$$a_1^{k-1}x_{k-1}+a_1^{k-2}x_{k-2}+\cdots\cdots+a_1^{0}x_0=\bar{a}_1$$
$$a_2^{k-1}x_{k-1}+a_2^{k-2}x_{k-2}+\cdots\cdots+a_2^{0}x_0=\bar{a}_2$$
$$\cdots\cdots\cdots$$
$$\cdots\cdots\cdots$$
$$a_k^{k-1}x_{k-1}+a_k^{k-2}x_{k-2}+\cdots\cdots+a_k^{0}x_0=\bar{a_k}.$$

The determinant of the system is

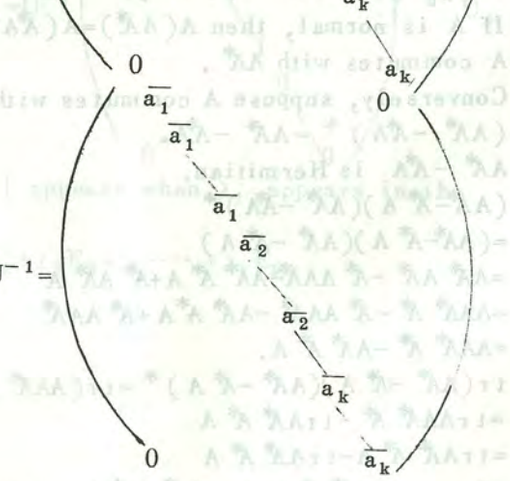
$$\begin{vmatrix} a_1^{k-1} & a_1^{k-2} & \cdots\cdots & a_1^{0} \\ a_2^{k-1} & a_2^{k-2} & \cdots\cdots & a_2^{0} \\ \cdots\cdots & & & \\ \cdots\cdots & & & \\ a_k^{k-1} & a_k^{k-2} & \cdots\cdots & a_k^{0} \end{vmatrix} = \prod_{i<j}(a_i-a_j)\neq 0 .$$

By Cramer's Rule, we know that there is a solution $x_0=\alpha_0$, $x_1=\alpha_1$, $\cdots\cdots$, $x_{k-1}=\alpha_{k-1}$ for the given system of linear equation. That is,
$\alpha_{k-1}a_i^{k-1}+\alpha_{k-2}a_i^{k-2}+\cdots\cdots+\alpha_0=\bar{a}_i$,
for $i=1, 2, \cdots\cdots, k$.
Since N is normal, there is a unitary matrix U such that

$UNU^{-1}=$



$UN^*U^{-1}=$



Hence $UN^*U^{-1}=\alpha_{k-1}(UNU^{-1})^{k-1}+\alpha_{k-2}(UNU^{-1})^{k-2}+\cdots\cdots+\alpha_1(UNU^{-1})+\alpha_0=U(\alpha_{k-1}N^{k-1}+\alpha_{k-2}N^{k-2}+\cdots\cdots+\alpha_1N+\alpha_0)U^{-1}$.

$N^*=\alpha_{k-1}N^{k-1}+\alpha_{k-2}N^{k-2}+\cdots\cdots+\alpha_1N+\alpha_0$.

Let $p(x)=\alpha_{k-1}x^{k-1}+\alpha_{k-2}x^{k-2}+\cdots\cdots\alpha_1x+\alpha_0$.

$N^*=p(N)$.

15. If N is normal and if $AN = 0$, prove that $AN^* = 0$.

350.15 For v in V, $v(AN)=0$. $(vA)N=0$. By Lemma 6.10.7., $(vA)N^*=0$. $v(AN^*)=0$. $AN^*=0$.

16. Prove that A is normal if and only if A commutes with AA^*.

350.16 Note : N is Hermitian. $trNN^*=0$. Then $N=0$. For, by Corollary 2 to Theorem 6.10.4 and Lemma 6.10.10. (1).,

$(UNU^{-1})(UN^*U^{-1})=UNN^*U^{-1}$,

$tr(UNU^{-1})(UN^*U^{-1})=tr(UNN^*U^{-1})=trNN^*=0$. The diagonal of UNU^{-1} is $\lambda_1,\cdots\cdots,\lambda_n$. The diagonal of $(UNU^{-1})(UN^*U^{-1})$ is $\lambda_1^2,\cdots\cdots,\lambda_n^2$. $\lambda_1^2+\cdots\cdots+\lambda_n^2=0$ implies $\lambda_1=\lambda_2=\cdots\cdots=\lambda_n=0$. $UNU^{-1}=0$. $N=0$.

If A is normal, then $A(AA^*)=A(A^*A)=(AA^*)A$.

A commutes with AA^*.

Conversely, suppose A commutes with AA^*.

$(AA^*-A^*A)^*=AA^*-A^*A$.

AA^*-A^*A is Hermitian.

$(AA^*-A^*A)(AA^*-A^*A)^*$

$=(AA^*-A^*A)(AA^*-A^*A)$

$=AA^*AA^*-A^*AAA^*-AA^*A^*A+A^*AA^*A$

$=AAA^*A^*-A^*AAA^*-AA^*A^*A+A^*AAA^*$

$=AAA^*A^*-AA^*A^*A$.

$tr(AA^*-A^*A)(AA^*-A^*A)^*=tr(AAA^*A^*-AA^*A^*A)$

$=trAAA^*A^*-trAA^*A^*A$

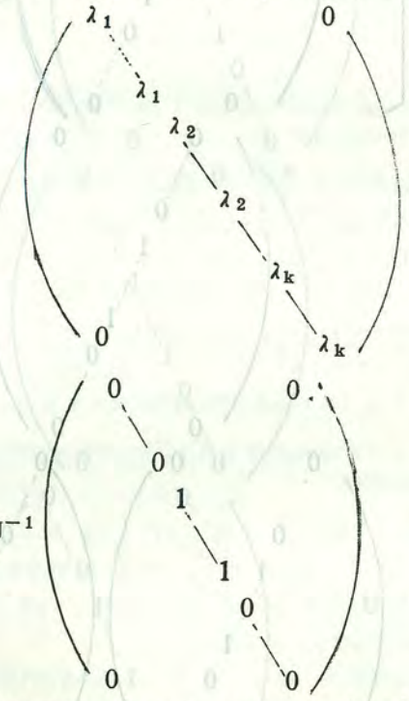
$=trAA^*A^*A-trAA^*A^*A$

$=0$. $AA^*-A^*A=0$. $AA^*=A^*A$. A is normal.

17. If N is normal prove that $N=\sum\lambda_iE_i$ where $E_i^2=E_i$, $E_i^*=E_i$, and the λ_i's are the characteristic roots of N. (This is called the *spectral resolution* of N.)

350.17 We argue using matrices. Let $\lambda_1,\cdots\cdots,\lambda_k$ be distinct characteristic roots of N. By Theorem 6.10.4., there is a unitary matrix U snch that

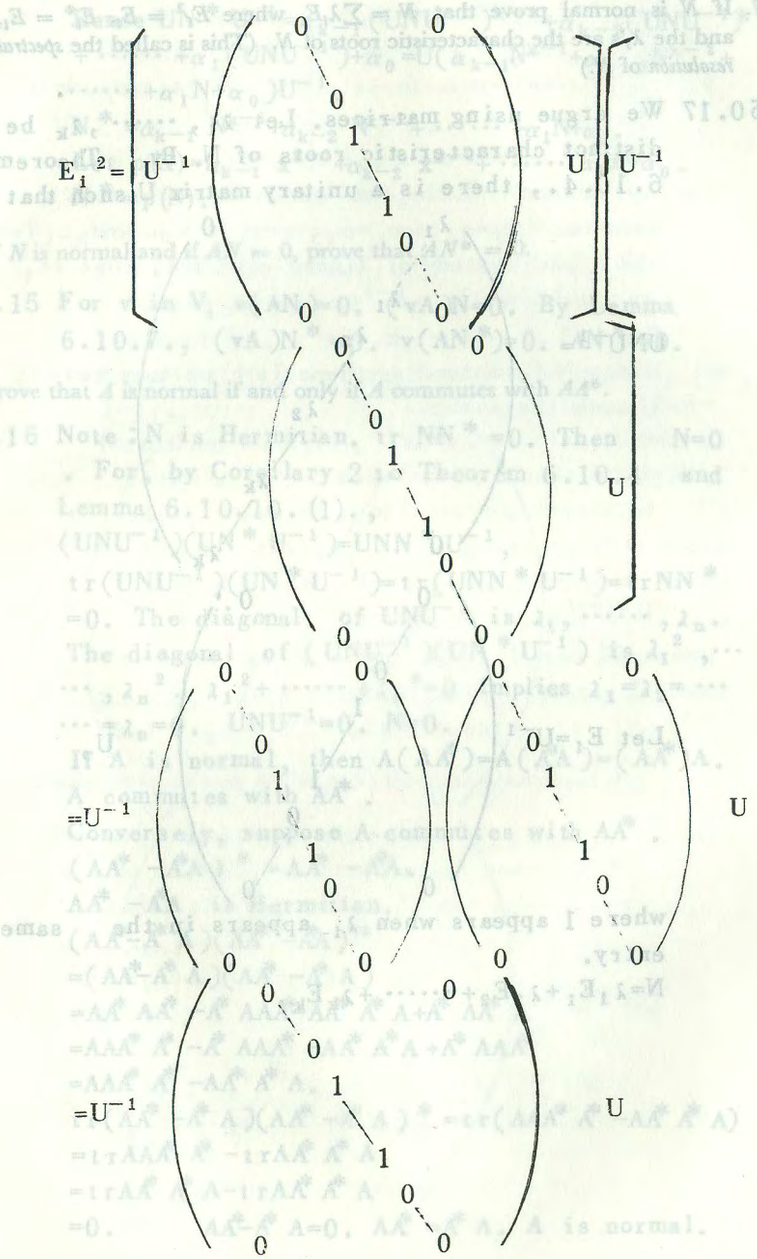
$UNU^{-1}=$

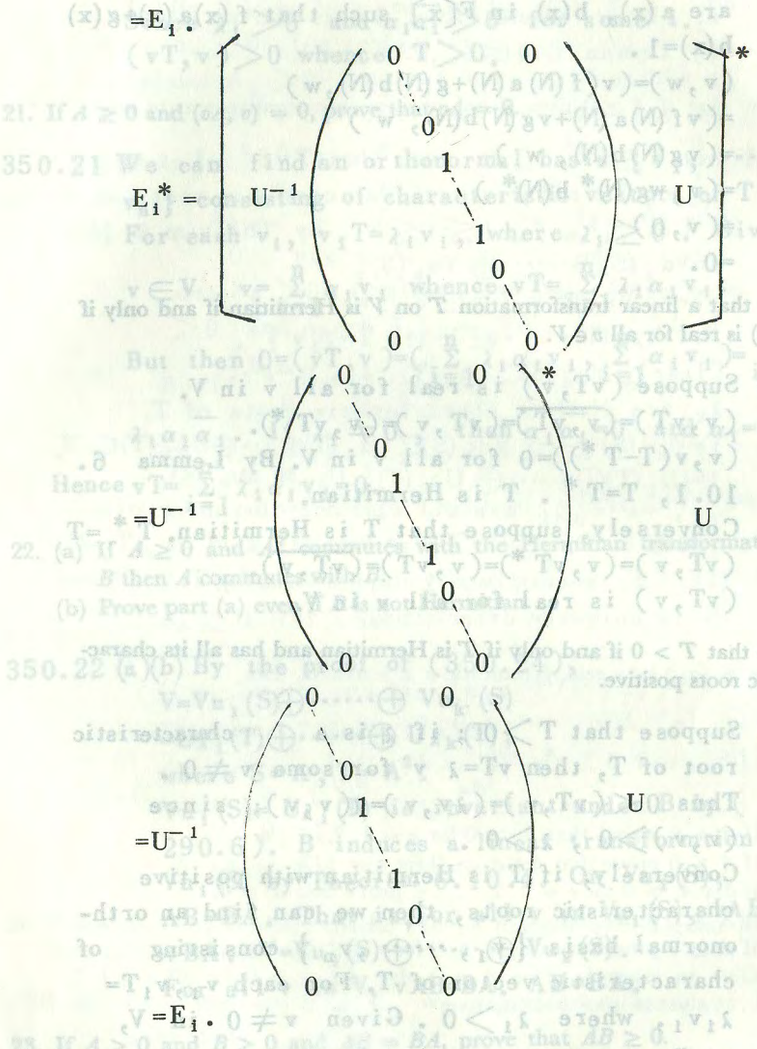


Let $E_1=U^{-1}$ U,

where 1 appears when λ_1 appears in the same entry.

$N=\lambda_1E_1+\lambda_2E_2+\cdots\cdots+\lambda_kE_k$.





18. If N is a normal transformation on V and if $f(x)$ and $g(x)$ are two relatively prime polynomials with real coefficients, prove that if $vf(N) = 0$ and $wg(N) = 0$, for v, w in V, then $(v, w) = 0$.

350.18 Since f(x) and g(x) are relatively prime, there

are $a(x)$, $b(x)$ in $F[x]$ such that $f(x)a(x)+g(x)b(x)=1$.

$(v,w)=(v(f(N)a(N)+g(N)b(N),w)$
$=(vf(N)a(N)+vg(N)b(N),\ w)$
$=(vg(N)b(N),\ w)$
$=(v, wg(N)^* b(N)^*)$
$=(v,0)$
$=0$.

19. Prove that a linear transformation T on V is Hermitian if and only if (vT, v) is real for all $v \in V$.

350.19 Suppose (vT,v) is real for all v in V.
$(v,vT)=\overline{(v,vT)}=(vT,v)=(v,vT^*)$.
$(v,v(T-T^*))=0$ for all v in V. By Lemma 6.10.1, $T=T^*$. T is Hermitian.
Conversely, suppose that T is Hermitian. $T^*=T$
$(vT,v)=(v,vT^*)=(v,vT)=\overline{(vT,v)}$.
(vT,v) is real for all v in V.

20. Prove that $T > 0$ if and only if T is Hermitian and has all its characteristic roots positive.

350.20 Suppose that $T>0$; if λ is a characteristic root of T, then $vT=\lambda v$ for some $v \neq 0$.
Thus $0<(vT,v)=(\lambda v,v)=\lambda(v,v)$; since $(v,v)>0$, $\lambda>0$.
Conversely, if T is Hermitian with positive characteristic roots, then we can find an orthonormal basis $\{v_1, \cdots\cdots, v_n\}$ consisting of characteristic vector of T. For each v_i, $v_iT=\lambda_i v_i$, where $\lambda_i>0$. Given $v \neq 0$ in V,

$v=\sum_{i=1}^{n}\alpha_i v_i$ whence $vT=\sum_{i=1}^{n}\alpha_i v_i$ $T=\sum_{i=1}^{n}\lambda_i\alpha_i v_i$.

But then $(vT,v)=(\sum_{i=1}^{n}\lambda_i\alpha_i v_i, \sum_{i=1}^{n}\alpha_i v_i)=\sum_{i=1}^{n}\lambda_i\alpha_i\overline{\alpha_i}$ by the orthonormality of the v_i's.

Since $\lambda_i>0$ and $\alpha_i\overline{\alpha_i}>0$ for some i.
$(vT,v)>0$ whence $T>0$.

21. If $A \geq 0$ and $(vA, v) = 0$, prove that $vA = 0$.

350.21 We can find an orthonormal basis $\{v_1, \cdots\cdots v_n\}$ consisting of characteristic vectors of T.
For each v_i, $v_iT=\lambda_i v_i$, where $\lambda_i \geq 0$. Given $v \in V$. $v=\sum_{i=1}^{n}\alpha_i v_i$ whence $vT=\sum_{i=1}^{n}\lambda_i\alpha_i v_i$.

But then $0=(vT,v)=(\sum_{i=1}^{n}\lambda_i\alpha_i v_i, \sum_{i=1}^{n}\alpha_i v_i)=\sum_{i=1}^{n}\lambda_i\alpha_i\overline{\alpha_i}$. If $\lambda_i \neq 0$, then $\alpha_i\overline{\alpha_i}=0$ and $\alpha_i=0$.

Hence $vT=\sum_{i=1}^{n}\lambda_i\alpha_i v_i=0$.

22. (a) If $A \geq 0$ and A^2 commutes with the Hermitian transformation B then A commutes with B.
(b) Prove part (a) even if B is not Hermitian.

350.22 (a)(b) By the proof of (350.24),
$V=Vu_1(S)\oplus\cdots\cdots\oplus Vu_k(S)$
$=U\lambda_1(T)\oplus\cdots\cdots\oplus U\lambda_k(T)$,
where $S=A$, $T=A^2$.
$Vu_i(S)=U\lambda_i(T)$ is invariant under B by (290.6). B induces a linear transformtion on $Vu_i(S)$ by Theorem 6.10.4. On $Vu_i(S)$, $AB=BA$. That is, for all v in $Vu_i(S)$, $vAB=vBA$. $V=Vu_1(S)\oplus\cdots\cdots\oplus Vu_k(S)$.
For all v in V, $vAB=BA$. $AB=BA$.

23. If $A \geq 0$ and $B \geq 0$ and $AB = BA$, prove that $AB \geq 0$.

305.23 By (349.13), there is a unitary matrix U such that UAU^{-1} and UBU^{-1} are diagonal.
$UABU^{-1}=(UAU^{-1})(UBU^{-1})$ is diagonal. The characteristic roots of AB are the products of those of A and B. Hence the characteristic roots

of AB are nonnegative. AB is Hermitian.
By Lemma 6.10.12, $AB \geq 0$.

24. Prove that if $A \geq 0$ then A has a *unique* nonnegative square root.

305.24 Let $T \geq 0$, $S \geq 0$ such that $T=S^2$. Let $u_1, \cdots$ $\cdots, u_k$ be all distinct characteristic roots of S . Let $\lambda_i = u_i^2$, $1 \leq i \leq k$. By Theorem 6.10.4., $V = Vu_1(S) \oplus \cdots\cdots \oplus Vu_k(S)$,
where $Vu_i(S) = \{ v \in V \mid vS = u_i v \}$.
Let $U\lambda_i(T) = \{ v \in V \mid vT = \lambda_i v \}$.
Clearly $Vu_i(S) \subset U\lambda_i(T)$. $\lambda_1, \cdots\cdots,$
λ_k are distinct characteristic roots of T.
$V = V_{u_1}(S) \oplus \cdots\cdots Vu_k(S) \subset U\lambda_1(T) \oplus \cdots \oplus U\lambda_k(T) \subset V$.
$U = U\lambda_1(T) \oplus \cdots\cdots \oplus U\lambda_k(T)$. $U\lambda_1(T) = Vu_i(S)$.
$\lambda_1, \cdots\cdots, \lambda_k$ are all distinct characteristic roots of T. $vS = \sqrt{\lambda_i}\, v$ for all v in $Vu_i(T) = U\lambda_i$ (T). S is completely determined by T. Hence S is uniquely determined.

25. Let $A = (\alpha_{ij})$ be a real, symmetric $n \times n$ matrix. Let

$$A_s = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1s} \\ \vdots & & \vdots \\ \alpha_{s1} & \cdots & \alpha_{ss} \end{pmatrix}$$

(a) If $A > 0$, prove that $A_s > 0$ for $s = 1, 2, \ldots, n$.
(b) If $A > 0$ prove that $\det A_s > 0$ for $s = 1, 2, \ldots, n$.
(c) If $\det A_s > 0$ for $s = 1, 2, \ldots, n$, prove that $A > 0$.
(d) If $A \geq 0$ prove that $A_s \geq 0$ for $s = 1, 2, \ldots, n$.
(e) If $A \geq 0$ prove that $\det A_s \geq 0$ for $s = 1, 2, \ldots, n$.
(f) Give an example of an A such that $\det A_s \geq 0$ for all $s = 1, 2, \ldots, n$ yet A is *not* nonnegative.

350.25 (a) For $0 \neq (\alpha_1, \cdots\cdots, \alpha_s) \in F^{(s)}$,
$((\alpha_1, \cdots\cdots, \alpha_s)A_s, (\alpha_1, \cdots\cdots, \alpha_s))$
$= ((\alpha_1, \cdots\cdots \alpha_s, 0, \cdots\cdots, 0)A, (\alpha_1, \cdots\cdots \alpha_s$
$, 0, \cdots\cdots 0)) > 0$.
$A_s > 0$ for $s = 1, 2, \cdots\cdots, n$.

(b) By (350.20) and Lemma 6.9.7., $\det$
$A_s \geq 0$ for $s = 1.2 \cdots n$
(c) $\det A_1 > 0$ implies A_1 is invertible and $A_1 > 0$. By induction, suppose that $A_{s-1} > 0$

$$A_s = \begin{pmatrix} A_{s-1} & a \\ a' & a_{ss} \end{pmatrix} = \begin{pmatrix} I_{s-1} & 0 \\ a'A_{s-1}^{-1} & 1 \end{pmatrix} \begin{pmatrix} A_{s-1} & 0 \\ 0 & a_{ss} - a'A_{s-1}^{-1}a \end{pmatrix} \begin{pmatrix} I_{s-1} & A_{s-1}^{-1}a \\ 0 & 1 \end{pmatrix}.$$

$\det A_s > 0$ implies $(\det A_{s-1})(a_{ss} - a'A_{s-1}^{-1}a) > 0$ and $a_{ss} - a'A_{s-1}^{-1}a > 0$. $A_{s-1} > 0$.

$$B_s = \begin{pmatrix} A_{s-1} & 0 \\ 0 & a_{ss} - a'A_{s-1}^{-1}a \end{pmatrix} > 0 .$$

$$T = \begin{pmatrix} I_{s-1} & 0 \\ a'A_{s-1}^{-1} & 1 \end{pmatrix} .$$ For $0 \neq v \in F^{(s)}$,
$(vA_s, v) = (vTB_sT', v) = ((vT)B_s, vT) > 0$.
$A_s > 0$. Hence $A_n = A > 0$.
(d) By Lemma 6.10.12 and Lemma 6.9.7, $\det$
$A_s \geq 0$ for $s = 1, 2, \cdots\cdots, n$.
(e) For $(\alpha_1, \cdots\cdots, \alpha_s) \in F^{(s)}$,
$((\alpha_1, \cdots\cdots, \alpha_s)A_s, (\alpha_1, \cdots\cdots, \alpha_s))$
$= ((\alpha_1, \cdots\cdots, \alpha_s, 0, 0, \cdots\cdots, 0)A, (\alpha_1, \cdots\cdots$
$, \alpha_s, 0, 0, \cdots\cdots, 0) \geq 0$. $A_s \leq 0$ for, $s = 1, 2 \cdots n$
(f) $A = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$. $\det A_1 = 0$. $\det A_2 = \det A = 0$.
A is clarly not nonnegative.

26. Prove that any complex matrix can be brought to triangular form by a unitary matrix.

350.26 By Theorem 6.4.2, we can find a basis of $F^{(n)}$ such that

$v_1T = \lambda_1 v_1$
$v_2T = \alpha_{21} v_1 + \lambda_2 v_2$
$\vdots$
$v_iT = \alpha_{i1} v_1 + \alpha_{i,2} v_2 + \cdots\cdots + \alpha_{i\ i-1} v_{i-1} + \lambda_i v_i$
$\vdots$

$\vdots$

$v_nT=\alpha_{n1}v_1+\alpha_{n2}v_2+\cdots\cdots+\alpha_{nn-1}v_{n-1}+\lambda_nv_n$.

By Gram-Schmidt orthogonalization process, define

$u_1=v_1$, $w_1=\frac{u_1}{\|u_1\|}$,

$u_{i+1}=-(v_{i+1},w_1)w_1-(v_{i+1},w_2)w_2-\cdots\cdots$
$-(v_{i+1},w_i)w_i+v_{i+1}$.

$w_{i+1}=\frac{u_{i+1}}{\|u_{i+1}\|}$,

for $i=1,2,\cdots\cdots,n-1$. $w_1,\cdots\cdots,w_n$ is an orhonormal bases of $F^{(n)}$.

$u_1T=v_1T=\lambda_1v_1$

$w_1T=(\frac{u_1}{\|u_1\|})T=\frac{\lambda_1}{\|u_1\|}v_1=\lambda_1w_1$.

$u_{i+1}T=-(v_{i+1},w_i)w_1T-\cdots\cdots-(v_{i+1},w_i)w_iT+$
$v_{i+1}T\in Fw_1\oplus Fw_2\oplus\cdots\cdots\oplus Fw_i\oplus Fw_{i+1}$ by induction hypothesis and $v_{i+1}T=(v_{i+1},w_i)w_1T+$
$\cdots\cdots+(v_{i+1},w_1)w_iT+u_{i+1}T$.

$w_{i+1}T\in Fw_1\oplus\cdots\cdots\oplus Fw_{i+1}$.

In this basis, the matrix of T is of triangular form. By Therrem 6.3.2, and Theorem 6.10.1, there is a unitary matrix U in F_n such that UTU^{-1} is triangular.

6.11. Real Quadratic Forms

1. Determine the rank and signature of the following real quadratic forms:
   (a) $x_1^2+2x_1x_2+x_2^2$.
   (b) $x_1^2+x_1x_2+2x_1x_3+2x_2^2+4x_2x_3+2x_3^2$.

354.1 (a) $\begin{pmatrix}1&1\\1&1\end{pmatrix}$.

$$\begin{pmatrix}1&0\\1&-1\end{pmatrix}\begin{pmatrix}1&1\\1&1\end{pmatrix}\begin{pmatrix}1&0\\1&-1\end{pmatrix}'$$
$$=\begin{pmatrix}1&0\\1&-1\end{pmatrix}\begin{pmatrix}1&1\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&-1\end{pmatrix}$$
$$=\begin{pmatrix}1&1\\0&0\end{pmatrix}\begin{pmatrix}1&1\\0&-1\end{pmatrix}$$
$$=\begin{pmatrix}1&0\\0&0\end{pmatrix}.$$

The rank of (a) is 1 and the signature of (a) is 1.

(b) $A=\begin{pmatrix}1&\frac{1}{2}&1\\\frac{1}{2}&2&2\\1&2&2\end{pmatrix}$

$f(x)=\det(xI-A)=x^3-3x^2-\frac{9}{4}x+\frac{11}{2}$.

$f'(x)=3x^2-6x-\frac{9}{4}$.

$f(x)$ has maximal at $x=1-\frac{\sqrt{7}}{2}$ and minimal at $x=1+\frac{\sqrt{7}}{2}$. $f(1-\frac{\sqrt{7}}{2})=\frac{5}{4}+\frac{7\sqrt{7}}{4}$,

$f(1+\frac{\sqrt{7}}{2})=\frac{5}{4}-\frac{7\sqrt{7}}{4}$. $f(x)$ has two positive roots and a negative root. The rank of the quadratic form is 3 and the signature of it is $2-1=1$.

2. If A is a symmetric matrix with complex entries, prove we can find a complex invertible matrix B such that $BAB' = \begin{pmatrix} I_r & \\ & 0_t \end{pmatrix}$ and that r, the rank of A, determines the congruence class of A relative to complex congruence.

354.2 Let A=C+iD, where C and D are real matrices, $A'=C'+iD'=A=C+iD$.
$C=C'$, $D=D'$. C and D are real symmetric matrices.
$((C+iD)(C-iD))^* = (C-iD)^*(C+iD)^* =$
$(C^*+iD^*)(C^*-iD^*)=(C+iD)(C-iD)$.
$(C+iD)(C-iD))$ is a real matrix.
$(C+iD)(C-iD)=(C^2+D^2)+i(DC-CD)$.
$CD=DC$. Modefying the proof of (349.13), we can find a real orthogonal matrix U such that

$$UCU'=UCU^{-1}=\begin{pmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_r & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix},$$

$$UDU'=UDU^{-1}=\begin{pmatrix} b_1 & & & & \\ & b_2 & & & \\ & & \ddots & & \\ & & & b_r & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix},$$

where $a_1, \cdots\cdots a_r, b_1, \cdots\cdots, b_r$ are real numbers and $a_i^2+b_i^2 \neq 0$ for $i=1,2, \cdots\cdots, r$. Let E be the diagonal matrix shown below

$$E=\begin{pmatrix} \frac{1}{\sqrt{a_1+ib_1}} & & & & & \\ & \frac{1}{\sqrt{a_2+ib_2}} & & & & \\ & & \ddots & & & \\ & & & \frac{1}{\sqrt{a_r+ib_r}} & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

$$EUAU'E'=EUCU'E'+iEUDU'E'=\begin{pmatrix} I_r & \\ & O_{n-r} \end{pmatrix}.$$

Let $B=EU$. $BAB'=\begin{pmatrix} I_r & \\ & O_{n-r} \end{pmatrix}$. By Lemma 6.1.3. (3), the rank of A is equal to BAB'. Thus r is the rank of A.
Our task is now to show that two symmetric complex matrices are complex congruent if and only if they have the same rank. Clearly, if two symmetric complex matrices have the same rank, then by what we have proved they are complex congruent. Conversely, suppose
$L=\begin{pmatrix} I_r & \\ & O_{n-r} \end{pmatrix}$ and $M=\begin{pmatrix} I_{r'} & \\ & O_{n-r'} \end{pmatrix}$
are complex congruent. We want to show that $r=r'$. $M=TLT'$, where T is invertible.
The rank of L and M are equal. Hence $r=r'$. This completes the proof.

3. If F is a field of characteristic different from 2, given $A \in F_n$, prove that there exists a $B \in F_n$ such that BAB' is diagonal.

354.3 Note: In the problem we require that B is invertible, otherurise O is a trivial solution for the problem. Further more, A must be symmetric under our assumption that B is invertible. For, $(BAB')=(BAB')'=(BA'B')$, $A=A'$ since BAB' is diagonal and B is invertible.

Proof of the exercise : Use induction on n. Let $A=(\alpha_{ij})=\sum_{i,j=1}^{n}\alpha_{ij}E_{ij}$.

If $\alpha_{11}=0$ for $i=2,3,\cdots\cdots,n$, then, as $A_1=\sum_{i,j=2}^{n}\alpha_{ij}E_{ij}$ is also a symmetric matrix in F_{n-1}, there is an invertible matrix B_1 in F_{n-1} such that B_1AB_1' is diagonal by induction hypothesis.

Hence $\begin{pmatrix}1&0\\0&B_1\end{pmatrix}$ is invertible in F_n and

$$\begin{pmatrix}1&0\\0&B_1\end{pmatrix}\begin{pmatrix}\alpha_{11}&0\\0&A_1\end{pmatrix}\begin{pmatrix}1&0\\0&B_1\end{pmatrix}'=\begin{pmatrix}\alpha_{11}&0\\0&B_1A_1B_1'\end{pmatrix}$$

is diagonal. Therefore, our aim is to find an invertible C_2 in F_n such that the entries of the first column, or equally the first row, of C_2AC_2' are zero except the $(1,1)$-entry.

We first claim that we can reach our end if $\alpha_{11}\neq 0$

For,

$$\begin{aligned}&(I-\alpha_{11}^{-1}\alpha_{k1}E_{k1})A(I-\alpha_{11}^{-1}\alpha_{k1}E_{k1})'\\&=(I-\alpha_{11}^{-1}\alpha_{k1}E_{k1})(\sum_{i,j}\alpha_{ij}E_{ij})(I-\alpha_{11}^{-1}\alpha_{k1}E_{1k})\\&=(\sum_{i,j}\alpha_{ij}E_{ij}-\sum_{j}\alpha_{11}^{-1}\alpha_{k1}\alpha_{1j}E_{kj})(I-\alpha_{11}^{-1}\alpha_{k1}E_{1k})\\&=\sum_{i,j}(\alpha_{ij}E_{ij})-\sum_{j}(\alpha_{11}^{-1}\alpha_{k1}\alpha_{1j}E_{kj})-\sum_{i}(\alpha_{11}^{-1}\alpha_{k1}\alpha_{i1}E_{1k})\\&\quad+\alpha_{11}^{-1}\alpha_{k1}\alpha_{11}\alpha_{11}^{-1}\alpha_{k1}E_{kk}.\end{aligned}$$

For $k\neq 1$, the $(1,i)$-entry of $(I-\alpha_{11}^{-1}\alpha_{k1}E_{k1})$, $A(I-\alpha_{11}^{-1}\alpha_{k1}E_{k1})'$ is α_{1i} except the $(1,k)$-entry is 0.

Let $C_2=(I-\alpha_{11}^{-1}\alpha_{n1}E_{n1})(I-\alpha_{11}^{-1}\alpha_{n-11}E_{n-11})\cdots\cdots\cdots(I-\alpha_{11}^{-1}\alpha_{21}E_{21})$. By a computation as above we know that C_2 is the required matrix in Fn. Hence we have reduced our exercise to find an invertible matrix C_1 in F_n such that the $(1,1)$-entry of C_1AC_1' is not zero.

Suppose one of α_{1i}, $i=1,2,\cdots\cdots,n$ is not zero, say $\alpha_{kk}\neq 0$. Let $C_1=I-E_{11}-E_{kk}+E_{1k}+E_{k1}$. Then, by computing matrix, we know that the $(1,1)$-entry of C_1AC_1' is $\alpha_{kk}\neq 0$. We may suppose that $\alpha_{1i}=0$ for $i=1,2,\cdots\cdots,n$ and $\alpha_{1k}\neq 0$ for some $k=2,3,\cdots\cdots;n$. Let $B=I+E_{1k}$. Then the $(1,1)$-entry of BAB' is $2\alpha_{1k}$. Since F is a field of characteristic different from 2, $2\alpha_{1k}\neq 0$. This completes the proof of the exercise.

4. prove the result of Problem 3 is false if the characteristic of *F* is 2.

354.4 Let $F=\{0,1\}=Z_2$. Let $A=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.

$\{\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix}\}$ is the subset of invertible elements of F_2. All

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

$$\begin{pmatrix}0&1\\1&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&1\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

$$\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

are not diagonal.

5. How many congruence classes are there of $n \times n$ real symmetric matrices.

354.5 There are $(n+1)+(n)+\cdots\cdots+2+1=\dfrac{(n+2)(n+1)}{2}$ congruence classes.

7 Selected Topics

7.1. Finite Fields

1. By Theorem 7.1.2 the nonzero elements of J_p form a cyclic group under multiplication. Any generator of this group is called a *primitive root* of p
   (a) Find primitive roots of: 17, 23, 31.
   (b) How many primitive roots does a prime p have?

360.1 (a) 3,5,6,7,10,11,12,14 are primitive roots of17. 5,7,10,11,14,15,17,19,20,21 are primitive roots of 23.
3,11,12,13,17,21,22,24 are primitive roots of 31.
(b) p has $\varphi(p-1)$ primitive roots,where $\varphi(n)$is the Euler φ-function.

2. Using Theorem 7.1.2 prove that $x^2 \equiv -1 \bmod p$ is solvable if and only if the odd prime p is of the form $4n + 1$.

360.2 By Theorem 7.1.2, p has a primitive root a. o(a) =p-1.
If $x^2 \equiv -1$ is solvable, then a solution x is of order 4. By Thearem 2.4.1, $4 \mid p-1$. Hence p is of the form 4n+1.
Conversely, suppose that p is of the form 4n+1. $o(a)=p-1=4n$. a^n is of order 4 and $(a^n)^2$ is of order 2. Therefore $(a^n)^2 \equiv -1$ since -1 is the unique element of Jp of order 2 in a cyclic group.

3. If a is an integer not divisible by the odd prime p, prove that $x^2 \equiv a \bmod p$ is solvable for some integer x if and only if $a^{(p-1)/2} \equiv 1 \bmod p$. (This is called the *Euler criterion* that a be a quadratic residue mod p.)

360.3 Let y be a primitive root of p.
If $x^2 \equiv a \bmod p$ for some integer x, then $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p$ by (24.14).
Conversely, suppose that $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Since y

is a primitive root of p, $a \equiv y^s$ for some integer s.
$(y^s)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1$.
Since $o(y)=p-1$, $(p-1) \mid \frac{p-1}{2} \cdot s$ by (49.36).
Hence $2 \mid s$. $s = 2s'$ for some integer s'. $a \equiv y^s \equiv (y^{s'})^2 \bmod p$. $x^2 \equiv a \bmod p$ is solvable.

4. Using the result of Problem 3 determine if:
   (a) 3 is a square mod 17.
   (b) 10 is a square mod 13.

360.4 $3^{\frac{17-1}{2}} \equiv 3^8 \equiv 81^2 \equiv 13^2 \equiv -1 \bmod 17$. 3 is not a sguare mod 17.
$10^{\frac{13-1}{2}} \equiv 10^6 \equiv 1000^2 \equiv (-1)^2 \equiv 1 \bmod 13$. By (360.3), 10 is a sguare mod 13.

5. If the field F has p^n elements prove that the automorphisms of F form a cyclic group of order n.

360.5 We first show that there are at most n automorphisms of F. By Theorem 7.1.2, let a be a generator of the multiplicative group of nonzero elements of the finite field F. Let f(x) be the minimal polynomial of a over the prime field Jp of F. f(x) is of degree n. The automorphism σ of F is determined by $\sigma(a)$, $\sigma(i) = i$, for all $i \in Jp$. Hence $\sigma(a)$ is a root of f(x). This proves our assertion In fact, F has n automorphisms σ_i defined as $\sigma_i(x) = x^{p^i}$, for $i = 0, 1, 2, \cdots\cdots, n-1$. Therefore, the automorphisms of F form a cyclic group of order n.

6. If F is a finite field, by the quaternions over F we shall mean the set of all $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in F$ and where addition and multiplication are carried out as in the real quaternions (i.e., $i^2 = j^2 = k^2 = ijk = -1$, etc.). Prove that the quaternions over a finite field *do not* form a division ring.

360.6 By Lemma 7.1.7, there are a, b in F such that $1+a^2+b^2=0$. Therefore, $(1+ai+bj)(1-ai-bj)=1+a^2+b^2=0$, $1+ai+bj \neq 0$, $1-ai-bj \neq 0$. The quaternions over a finite field do not form a division ring.

7.2 Wedderburn's Theorem on Finite Division Rings.

1. If $t > 1$ is an integer and $(t^m - 1)|(t^n - 1)$, prove that $m \mid n$.

367.1 $n=rm+s$ for some integers r and s such that $0 \leq s < m$.
$t^n-1=t^{rm+s}-1=t^s(t^{rm}-1)+(t^s-1)$.
$(t^m-1)|(t^n-1)$ and $(t^m-1)|(t^{rm}-1)$ implies $(t^m-1)|t^s-1$. $t^s-1 < t^m-1$ implies $s=0$ and $n=rm$, $m \mid n$.

2. If D is a division ring, prove that its dimension (as a vector space) over its center cannot be 2.

367.2 Let Z be the center of D. Suppose D is of dimension 2 over Z. Let 1, a be the basis of D over Z. It's clear that $D=Z(a)$ is commutative and $D=Z$. D can not be 2 dimension over Z.

3. Show that any finite subring of a division ring is a division ring.

367.3 Let R be a finite subring of a division ring D. To prove that R is division ring we must show that the nonzoro elements of R form a group under multiplication. In fact we need only show that if $x, y \in R$, $x \neq 0$, $y \neq 0$, then $xy \in R$ and $x^{-1} \in R$ and $xy \neq 0$. $x, y \in R$, $x \neq 0$, $y \neq 0$ implies $xy \in R$ and $xy \neq 0$ since R is a subring and D is a division ring. If $x \in R$ and $x \neq 0$, then $x^m = x^n$ for some m and n and $m \neq n$ since $\{x, x^2, x^3 \cdots\cdots\}$ is a finite set. Let's suppose that $m > n$. Then $x^{m-n}=e$ and $x^{m-n-1}=x^{-1} \in R$. Hence R is a division ring.

4. (a) Let D be a division ring of characteristic $p \neq 0$ and let G be a finite subgroup of the group of nonzero elements of D under multiplication. Prove that G is abelian. (*Hint:* consider the subset $\{x \in D \mid x = \sum \lambda_i g_i,\ \lambda_i \in P,\ g_i \in G\}$.)
(b) In part (a) prove that G is actually cyclic.

368.4 (a) Let $P=J_p$. $R=\{x \in D \mid x=\Sigma \lambda_i g_i$, $\lambda_i \in P, g_i \in G\}$. Clearly, R is a finite subring of D. By (367.3) , R is a finite division ring.
By Theorem7.2.1, R is commutative. In particular, G is abelian.

(b) By Theorem 7.1.2, the nonzero elements of R form a cyclic group. Hence, as a subgroup of a cyclic group, G is cyclic.

*5. (a) If R is a finite ring in which $x^n = x$, for all $x \in R$ where $n > 1$ prove that R is commutative.

(b) If R is a finite ring in which $x^2 = 0$ implies that $x = 0$, prove that R is commutative.

368.5 (a) A ring R is said to be a J-ring if $x^n=x$ for all x in R where $n>1$ (possibly depending on x). If I is an ideal of the J-ring R, then R/I is also a J-ring. A J-ring has no nonzero nilpotent element. For, suppose $x^m=0$ and $x^n=x$. Then $(x^{n-1})^2 = (x^{n-1})(x^{n-1}) = x^n \cdot x^{n-2} = x \cdot x^{n-2} = x^{n-1}$ since $n>1$. x^{n-1} is an idempotent. $(x^{n-1})^k = x^{n-1}$ for all $k=1, 2, \cdots\cdots$. $x = x^n = x \cdot x^{n-1} \Rightarrow x \cdot x^{k(n-1)} = x^{1+k(n-1)}$ for all $k=1,2, \cdots\cdots$. Hence $x = 0$. As we have proved in (136.19), if R has no nonzero nilpotent element, then every idempotent of R lies in Z(R), the center of R. Hence $x^n = x$, $n>1$, implies $x^{n-1} \in Z(R)$. Let R be a finite J-ring.
For $x \in R$ and $x \neq 0$ define M(x) as the maximal ideal of R subject to $x \notin M(x)$. Such an M(x) must exist since R is finite and (0) is an ideal of R with $x \notin (0)$. We prove this exercise by induction on the order of R.

(i) Suppose that there is an element z in R such that M (z) = 0. That is, every nonzero ideal of R contains z.
We first show that every idempotent e of R is the unity of R. $e \in Z(R)$. Let $A = \{ex-x \mid x \in R\}$ and $B = \{ex \mid x \in R\}$. Since $e \in Z(R)$, A and B are ideals of R. $A \cap B = (0)$. $e = ee \in B$ whence $B \neq 0$. If $A \neq 0$, then $z \in A \cap B$ by our assumption. This is a contradiction. Hence $A = 0$ and $ex = x$ for all x in R. e is the unity of R.
R is a division ring. For, $x \in R$, $x \neq 0$ implies $x^n = x$, $n>1$. x^{n-1} is an idempotent in R. x^{n-1} is the unity of R. $n>1$. x is invertible in R. This clearly shows that R is a finite division ring. By Theorem 7.2.1. (Wedderburn's Theorem) or Theorem 7.2.2., R is commutative.

(ii) We may suppose that $M(x) \neq 0$ for all $x \neq 0$ in R. Let
$R \setminus (0) = \{x_1, x_2, \cdots\cdots, x_m\}$ and
$N_i = R / M(x_i)$. N_i is also a J-ring. N_i is commutative by induction hypothesis. Let $N = \prod_{i=1}^{m} N_i$ be the direct sum of $N_1, N_2, \cdots\cdots, N_m$.
Define a mapping σ of R into N as $\sigma(x) = (x+M(x_1), x+M(x_2), \cdots\cdots x+M(x_m))$. σ is clearly a homomorphism of R into the commutative ring N. The kernel of σ is $\bigcap_{i=1}^{m} M(x_i)$.
Evidently, $\bigcap_{i=1}^{m} M(x_i) = 0$. Hence, σ is an isomorphism of R into a commutative ring. By Theorem 3.4.1, R is also commutative. This

completes the proof of (a).

(b) R has no nonzero nilpotent element. For, suppose $x^n = 0$. Then $x^m = 0$ for a minimal nonnegative integer m. We show that $m = 1$. If m is even and $m = 2k$, the $(x^k)^2 = x^{2k} = x^m = 0$, $x^k = 0$, a contradiction. Hence m is odd, $m-1$ is even. If $m > 1$, then $(x^{\frac{m-1}{2}})^2 = 0$, $x^{\frac{m-1}{2}} = 0$, a contradication. Hence $m = 1$ and $x = x^m = 0$. R has no nonzero nilpotent element. $\{x, x^2, x^3, \cdots\}$ is finite since R is finite. Therefore $x^n = x^m$ for two distinct positive integers m and n. Let's say $n > m$.

$$(x^{n-m+1} - x)^m = \sum_{k=0}^{m} \binom{m}{k} (x^{n-m+1})^k (-x)^{m-k}$$

$$= \sum_{k=0}^{m} \binom{m}{k} (-1)^{m-k} x^{(nk-mk+k)+(m-k)}$$

$$= \sum_{k=0}^{m} \binom{m}{k} (-1)^{m-k} x^m$$

since $x^{nk-mk+m} = x^n \cdot x^{n(k-1)-mk+m}$

$$= x^m \cdot x^{n(k-1)-mk+m}$$

$$= x^{n(k-1)-m(k-1)+m}$$

$$= \cdots\cdots$$

$$= x^m.$$

$$\sum_{k=0}^{m} \binom{m}{k} (-1)^{m-k} x^m = \left(\sum_{k=0}^{m} \binom{m}{k} (-1)^{m-k}\right) x^m$$

$$= (1-1)^m x^m = 0.$$

$(x^{n-m+1} - x)^m = 0$. $x^{n-m+1} - x = 0$. $x^{n-m+1} = x$. R is a finite J-ring. By (368.5. (a)), R is commutative.

*6. Let D be a division ring and suppose tnat $a \in D$ only has a finite number of conjugates (i.e., only a finite number of distinct $x^{-1}ax$).

Prove that a has only one conjugate and must be in the center of D.

368.6 $D \setminus (0)$ is a group under multiplcation. Since $a \in D \setminus (0)$ has only finite number of conjugates, $N(a) \setminus (0)$ has finite index in $D \setminus (0)$. Let $a_1, a_2, \cdots\cdots, a_n$ be coset represtatives of $N(a) \setminus 0$ in $D \setminus (0)$. Then $D = \bigcup_{i=1}^{n} N(a)\, a_i$. $N(a)\, a_i$ is a vector space over $N(a)$, a subdivision ring of D. By the proof of (177.21), $N(a)$ is finite or $N(a)a_i = D$ for some i. If $N(a)$ is finite, then D is finite. By Theorem 7.2.1., D is commutative. a lies in the center of D. If $N(a)a_i = D$, then $N(a) = Da_i^{-1} = D$. Every element of D commutes with a. a must be in the center of D. This completes the proof the exercise.

7. Use the result of Problem 6 to prove that if a polynomial of degree n having coefficients in the center of a division ring has $n + 1$ roots in the division ring then it has an infinite number of roots in that division ring.

368.7 Let $f(x)$ be the given polynomial. Since the center Z of a division ring is a field. By Lemma 5.3.2, $f(x)$ has at least a root x which does not lie in Z. By (368.6), x has infinite number of conjugates in D. Since $f(x) \in Z[x]$, the conjugates of x are also roots of $f(x)$. Hence $f(x)$ has infinite number of roots in D.

*8. Let D be a division ring and K a subdivision ring of D such that $xKx^{-1} \subset K$ for every $x \neq 0$ in D. Prove that either $K \subset Z$, the center of D or $K = D$. (This result is known as the *Brauer-Cartan-Hua theorem.*)

368.8 Suppose that $K \neq D$. Let $a \in K$, $b \in D \setminus K$, $c = b^{-1}ab \in K$ by assumption. $d = (b+1)^{-1}a(b+1) \in K$.

$$\begin{cases} ab = bc \\ ab + a = bd + d. \end{cases}$$

$a = b(c-d) + d$. If $c \neq d$, then $b = (a-d)(c-d)^{-1} \in K$, a contradiction. Hence $c = d$ and $a = d$. $a = c$

$ab=ba$.
This shows that $ab=ba$ for all $b\in D\setminus K$. For $r\in K$. Let $b_0\in D\setminus K$. $b_0r\in D\setminus K$. Hence $b_0ar=ab_0r=b_0ra$ and $ar=ra$. $a\in Z$. $K\subset Z$. This completes the proof.

*9. Let D be a division ring and K a subdivision ring of D. Suppose that the group of nonzero elements of K is a subgroup of finite index in the group (under multiplication) of nonzero elements of D. Prove that either D is finite or $K = D$.

368.9 $D=\bigcup_{i=1}^{n} Ka_i$ for some $a_i\in D$, $i=1,2,\cdots\cdots,n$. D can be viewed as a vector space over the division ring K. By (177.21), K is finite or $Ka_i = D$ for some a_i since Ka_i can be viewed as subspace of D over K. If K is finite, then D is finite since $D=\bigcup_{i=1}^{n} Ka_i$. If $Ka_i=D$, then $K=Da_i^{-1}=D$. This completes the proof.

10. If $\theta \neq 1$ is a root of unity and if q is a positive integer, prove that $|q - \theta| > q - 1$.

368.10 $\theta=\cos\alpha+i\sin\alpha$ with $\cos\alpha\neq 1$.
$|q-\theta|^2=(\cos\alpha-q)^2+\sin^2\alpha=q^2-2q\cos\alpha+1$.
$-2q\cos\alpha>-2q$. $|q-\theta|^2=q^2-2q\cos\alpha+1$
$>q^2-2q+1=(q-1)^2$. $|q-\theta|>q-1$.

7.3. A Theorem of Frobenius

1. If the division ring D is finite-dimensional, as a vector space, over the field F contained in the center of D, prove that D is algebraic over F.

371.1 Suppose D is of dimension n over F. $a\in D$, $1, a, a^2, \cdots\cdots, a^n$ are linearly dependent over F. Hence, there are $\alpha_i\in F$, $i=0,1,\cdots\cdots,n$, not all zero, such that $\alpha_n a^n+\alpha_{n-1}a^{n-1}+\cdots\cdots+a_0=0$. a satisfies a nontrivial polynomial with coefficients in F. By definition, D is algebraic over F.

2. Give an example of a field K algebraic over another field F but not finite-dimensional over F.

371.2 Let F be the field of rational numbers and K be the field of algebraic numbers. Since $\{\sqrt{p}\mid p$ is a positive prime integer$\}$ is an independent set over F, K is not finite dimension over F.

3. If A is a ring algebraic over a field F and A has no zero divisors prove that A is a division ring.

371.3 Let $f(x)$ be a polynomial in $F(x)$ satisfied by $a\in D\setminus(0)$ with minimal degree. $f(0)\neq 0$, otherwise a is a honzero zero divisor. Hence $f(a)=\alpha_n a^n+\alpha_{n-1}a^{n-1}+\cdots\cdots+\alpha_0=0$,
$1=a\left[-\alpha_0^{-1}(\alpha_n a^{n-1}+\alpha_{n-1}a^{n-2}+\cdots\cdots+\alpha_1)\right]$.
a has an inverse element in D. D is a division ring.

7.4. Integral Quaternions and the Four-Square Theorem

1. Prove Lemma 7.4.4.

377.1 Let $x \in H$, $x = m_0\zeta + m_1 i + m_2 j + m_3 k$

$$= \frac{m_0}{2} + \frac{m_0+2m_1}{2} i + \frac{m_0+2m_2}{2} j + \frac{m_0+2m_3}{2} k$$

Then $x^* = \frac{m_0}{2} - \frac{m_0+2m_1}{2} i - \frac{m_0+2m_2}{2} j - \frac{m_0+2m_3}{2} k$

$= m_0\zeta - (m_0+m_1) i - (m_0+m_2) j - (m_0+m_3) k \in H.$

$y = n_0\zeta + n_1 i + n_2 j + n_3 k.$

$x+y \in H$, $-x \in H$. $\zeta^2 = -\zeta + i + j + k$, $\zeta i = -\zeta + i + j \in H$, $\zeta j, \zeta k \in H$, $i\zeta, j\zeta, k\zeta \in H$.

Therefore, H is a ring.

$$N(x) = xx^* = \left(\frac{m_0}{2}\right)^2 + \left(\frac{m_0+2m_1}{2}\right)^2 + \left(\frac{m_0+2m_2}{2}\right)^2 + \left(\frac{m_0+2m_3}{2}\right)^2$$

$= m_0^2 + m_1^2 + m_2^2 + m_3^2 + m_0(m_1+m_2+m_3) \in N$ if $x \neq 0$.

2. Find all the elements a in Q_0 such that a^{-1} is also in Q_0.

377.2 $a = m_0 + m_1 i + m_2 j + m_3 k \in Q_0$, $a^{-1} \in Q_0$,
$N(a), N(a^{-1}) \in N$, $N(a)(N(a^{-1})) = N(1) = 1$, $N(a) = 1$
$N(a) = m_0^2 + m_1^2 + m_2^2 + m_3^2 = 1$. Hence $a = \pm 1, \pm i, \pm j$ or $\pm k$.

3. Prove that there are exactly 24 elements a in H such that a^{-1} is also in H. Determine all of them.

377.3 $a = m_0\zeta + m_1 i + m_2 j + m_3 k \in H$, $a^{-1} \in H$.
$N(a), N(a^{-1}) \in N$ by (377.1). $N(a)N(a^{-1}) = N(1) = 1$, $N(a) = 1$.

$$N(a) = \left(\frac{m_0}{2}\right)^2 + \left(\frac{m_0+2m_1}{2}\right)^2 + \left(\frac{m_0+2m_2}{2}\right)^2 + \left(\frac{m_0+2m_3}{2}\right)^2 = 1$$

$m_0 = 0$ implies $a = \pm i, \pm j$ or $\pm k$.
$m_0 = 2$ implies $m_1 = m_2 = m_3 = -1$ and $a = 1$.

$m_0 = -2$ implies $m_1 = m_2 = m_3 = 1$ and $a = -1$.

$m_0 = \pm 1$ implies $\left(\frac{1+2m}{2}\right)^2 = \left(\frac{1+2m_2}{2}\right)^2 = \left(\frac{1+2m_3}{2}\right)^2 = \frac{1}{4}$.

$m_1 = 0$ or -1, $m_2 = 0$ or -1, $m_3 = 0$ or -1.

Hence $a = \pm\frac{1}{2} \pm \frac{1}{2} i \pm \frac{1}{2} j \pm \frac{1}{2} k$ or $\pm 1, \pm i, \pm j, \pm k$.

4. Give an example of an a and b, $b \neq 0$, in Q_0 such that it is impossible to find c and d in Q_0 satisfying $a = cb + d$ where $N(d) < N(b)$.

377.4 $a = 1+2i+j$, $b = 1+i$. $N(b) = 2$. Suppose that there are $c, d \in Q_0$ such that $a = cb+d$ and $N(d) < N(b)$. Since $N(b) = 2$ and $N(d)$ is a nonnegative integer, $N(d) = 1$ or $N(d) = 0$, $N(d) = 0$ implies $d = 0$, $c = ab^{-1}$
$= (1+2i)(1+i)^{-1} = (1+2i+j)\left[\frac{1}{2}(1-i)\right]$

$$= \frac{1}{2}(3+i+j+k) \notin Q_0.$$

$N(d) = 1$, $d = \pm 1$, $\pm i$, $\pm j$ or $\pm k$.

$$c = ab^{-1} - db^{-1} = \frac{1}{2}(3+i+j+k) - \frac{1}{2} d(1-i) \notin Q_0.$$

5. Prove that if $a \in H$ then there exist integers α, β such that $a^2 + \alpha a + \beta = 0$.

377.5 $a = m_0 + m_1 i + m_2 j + m_3 k$, $2m_0 - a = a^*$.
$N(a) = aa^* = -a^2 + 2m_0 a$, $a^2 - 2m_0 a + N(a) = 0$.
$2m_0$, $N(a)$ are integers.

6. Prove that there is a positive integer which cannot be written as the sum of three squares.

377.6 It's easy to check that 7 can not be written as the sum of three squares.

*7. Exhibit an infinite number of positive integers which cannot be written as the sum of three squares.

377.7 $8n+7$ can not be written as the sum of three squares for n in J.

Consider integers module 8. The square of any integer is 0, 1 or 4 module 8. The sum of three numbers selected from $\{0,1,4\}$ can not be 7 mod 8. Hence $8n+7$ can not be written as the sum of three squares.