KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Coimbatore – 641 021

SYLLABUS

19MMP101 **ALGEBRA** **4H – 4C**

Instruction Hours / week: L: 4 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

This course enables the students to learn

- To provide deep knowledge about various algebraic structures
- Learn the elementary concepts and basic ideas involved in homomorphism and isomorphism.
- Develop the ability to form and evaluate group theory and its actions.

Course Outcomes (COs)

After successful completion of this course the students will be able to

1. Recognize some advances of the theory of groups.
2. Use sylow's theorems in the study of finite groups.
3. Formulate some special types of rings and their properties.
4. Recognize the interplay between fields and vector spaces.
5. Apply the algebraic methods for solving problems.

UNIT I

A counting principle - Normal subgroups and quotient groups – Homomorphisms– Automorphisms -Cayley's theorem - Permutation groups.

UNIT II

Another counting principle - Sylow's theorems - Direct product - Finite abelian groups.

UNIT III

Euclidean rings - A particular Euclidean ring - Polynomial rings – Polynomials over the rational field - Polynomial rings over commutative rings.

UNIT IV

Extension fields - Roots of polynomials - More about roots - Finite fields.

UNIT V

The elements of Galois theory - Solvability by radicals - Galois group over the rational.

SUGGESTED READINGS

1. Herstein.I. N.,(2006). Topics in Algebra, Second edition, Wiley and sons Pvt. Ltd, Singapore.
2. Artin. M., (2015).Algebra, Pearson Prentice-Hall of India, New Delhi.
3. Fraleigh. J. B., (2013). A First Course in Abstract Algebra, Seventh edition, Pearson Education Ltd, New Delhi.
4. Kenneth Hoffman., Ray Kunze., (2015). Linear Algebra, Second edition, Prentice Hall of India Pvt Ltd, New Delhi.
5. Vashista.A.R., (2014). Modern Algebra, KrishnaPrakashan Media Pvt Ltd, Meerut.

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021

LECTURE PLAN
DEPARTMENT OF MATHEMATICS

STAFF NAME: P. VICTOR

SUBJECT NAME: ALGEBRA SUB.CODE:19MMP101

SEMESTER: I CLASS: I M.Sc. Mathematics

S. No	Lecture Duration Period	Topics to be Covered	Support Material/Page No
		UNIT-I	
1	1	A Counting principle-Definitions and theorems	S1:Ch:2.Pg.No:44-46
2	1	Definition and theorem on normal subgroups and quotient groups	S1:Ch:2.Pg.No:49-54
3	1	Continuation of theorems of normal subgroups and quotient groups	S1:Ch:2.Pg.No:49-54
4	1	Homomorphism-Definitions and theorems	S1:Ch:2.Pg.No:54-64
5	1	Continuation of theorems of homomorphism	S1:Ch:2.Pg.No:54-64
6	1	Automorphism-Definitions and theorems	S1:Ch:2.Pg.No:66-70
7	1	Continuation of theorems of automorphisms	S1:Ch:2.Pg.No:66-70
8	1	Cayley's theorem	S1:Ch:2.Pg.No:71-74
9	1	Permutation groups-Definitions and theorems	S1:Ch:2.Pg.No:75-80
10	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit 1=10		
		UNIT-II	
1	1	Another counting principle-Lemma and Theorems	S1: Ch:2.Pg.No:83-88
2	1	Definition and theorems for Conjugacy Relation	S1: Ch:2.Pg.No:83-88
3	1	Cauchy's theorem	S1: Ch:2.Pg.No:88-89
4	1	Sylow's theorem	S3: Ch:7.Pg.No:321-326
5	1	Second proof of Sylow's theorem.	S3: Ch:7.Pg.No:321-326

6	1	Third proof of Sylow's theorem	S3: Ch:7.Pg.No:321-326
7	1	Corollary for Sylow's theorem.	S3: Ch:7.Pg.No:327-332
8	1	Definition and theorems for direct product	S1: Ch:2.Pg.No:104-107
9	1	Finite abelian group-Theorems	S1: Ch:2.Pg.No:109-114
10	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit II=10		
UNIT-III			
1	1	Basic definitions and examples	S3:Ch.4.Pg.No:168-174
2	1	Theorem based on properties of ring	S3:Ch.4.Pg.No:168-174
3	1	Ideal and quotient ring-Definitions and theorems	S5:Ch.4.Pg.No:360-319
4	1	The field of quotient of an integral domain theorems	S5:Ch.4.Pg.No:321-322
5	1	Euclidean ring-Definitions and theorems	S1:Ch.2.Pg.No:143-149
6	1	Theorems on particular Euclidean ring	S1:Ch.2.Pg.No:150-154
7	1	Polynomials over the rational field	S4:Ch.4.Pg.No:127-132
8	1	Polynomial ring over commutative rings	S4:Ch.4.Pg.No:132-140
9	1	Recapitulation and discussion of possible questions	
	Total No of Hours Planned For Unit III=09		
UNIT-IV			
1	1	Field and extension field-Definitions and theorems	S2:Ch.13.Pg.No:492-496
2	1	Continuation of theorems on extension field	S2:Ch.13.Pg.No:492-496
3	1	Some examples for extension field	S1:Ch.5.Pg.No:212-214
4	1	Roots of polynomial-Definition and theorems	S1:Ch.5.Pg.No:219-226
5	1	Lemma and theorems on roots	S1:Ch.5.Pg.No:232-236
6	1	Continuation of theorems on roots	S1:Ch.5.Pg.No:232-236
7	1	Finite fields-Definition and theorems	S1:Ch.7.Pg.No:356-360
8	1	Continuation of theorems on finite fields	S1:Ch.7.Pg.No:356-360
9	1	Recapitulation and discussion of possible questions	

	Total No of Hours Planned For Unit IV=09		
UNIT-V			
1	1	The elements of Galois theory-Definition and lemma	S2:Ch.14.Pg.No:537-543
2	1	Theorems on elements on Galois theory	S2:Ch.14.Pg.No:537-543
3	1	Continuation of theorems on Galois theory	S2:Ch.14.Pg.No:537-543
4	1	Theorems on solvability by radicals	S1:Ch.5.Pg.No:250-256
5	1	Continuation of theorems on solvability by radicals	S1:Ch.5.Pg.No:250-256
6	1	Theorems on Galois group over the rational	S1:Ch.5.Pg.No:256-260
7	1	Recapitulation and discussion of possible Questions	
8	1	Discussion on previous year ESE question papers	
9	1	Discussion on previous year ESE question papers	
10	1	Discussion on previous year ESE question papers	
	Total No of Hours Planned for Unit V=10		
Total Planned Hours			**48**

SUGGESTED READINGS

1. Herstein. I. N. (2006). Topics in Algebra, Second edition, Wiley and sons Pvt. Ltd, Singapore.
2. Artin. M. (2015). Algebra, Pearson Prentice-Hall of India, New Delhi.
3. Fraleigh. J. B., (2013). A First Course in Abstract Algebra, Seventh edition, Pearson Education Ltd, New Delhi.
4. Kenneth Hoffman., Ray Kunze., (2015). Linear Algebra, Second edition, Prentice Hall of India Pvt Ltd, New Delhi.
5. Vashista. A.R., (2014). Modern Algebra, Krishna Prakashan Media Pvt Ltd, Meerut.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

CLASS: I M.Sc. MATHEMATICS **COURSENAME: ALGEBRA**

COURSE CODE: 19MMP101 **BATCH-2019-2021**

UNIT-1

A COUNTING PRINCPLE

A counting principle - Normal subgroups and quotient groups – Homomorphisms – Automorphisms - Cayley's theorem - Permutation groups.

since p is a prime number, we must have that $p \mid a$, so that $a \equiv 0 \bmod p$; hence $0 \equiv a^p \equiv a \bmod p$ here also. Thus

COROLLARY 4 (FERMAT) *If p is a prime number and a is any integer, then $a^p \equiv a \bmod p$.*

COROLLARY 5 *If G is a finite group whose order is a prime number p, then G is a cyclic group.*

Proof. First we claim that G has no nontrivial subgroups H; for $o(H)$ must divide $o(G) = p$ leaving only two possibilities, namely, $o(H) = 1$ or $o(H) = p$. The first of these implies $H = (e)$, whereas the second implies that $H = G$. Suppose now that $a \neq e \in G$, and let $H = (a)$. H is a subgroup of G, $H \neq (e)$ since $a \neq e \in H$. Thus $H = G$. This says that G is cyclic and that every element in G is a power of a.

This section is of great importance in all that comes later, not only for its results but also because the spirit of the proofs occurring here are genuinely group-theoretic. The student can expect to encounter other arguments having a similar flavor. It would be wise to assimilate the material and approach thoroughly, now, rather than a few theorems later when it will be too late.

2.5 A Counting Principle

As we have defined earlier, if H is a subgroup of G and $a \in G$, then Ha consists of all elements in G of the form ha where $h \in H$. Let us generalize this notion. If H, K are two subgroups of G, let

$$HK = \{x \in G \mid x = hk, h \in H, k \in K\}.$$

Let's pause and look at an example; in S_3 let $H = \{e, \phi\}$, $K = \{e, \phi\psi\}$. Since $\phi^2 = (\phi\psi)^2 = e$, both H and K are subgroups. What can we say about HK? Just using the definition of HK we can see that HK consists of the elements $e, \phi, \phi\psi, \phi^2\psi = \psi$. Since HK consists of four elements and 4 is not a divisor of 6, the order of S_3 by Lagrange's theorem HK could not be a subgroup of S_3. (Of course, we could verify this directly but it does not hurt to keep recalling Lagrange's theorem.) We might try to find out why HK is not a subgroup. Note that $KH = \{e, \phi, \phi\psi, \phi\psi\phi = \psi^{-1}\} \neq HK$. This is precisely why HK fails to be a subgroup, as we see in the next lemma.

LEMMA 2.5.1 *HK is a subgroup of G if and only if $HK = KH$.*

Proof. Suppose, first, that $HK = KH$; that is, if $h \in H$ and $k \in K$, then $hk = k_1h_1$ for some $k_1 \in K$, $h_1 \in H$ (it need not be that $k_1 = k$ or

$h_1 = h$!). To prove that HK is a subgroup we must verify that it is closed and every element in HK has its inverse in HK. Let's show the closure first; so suppose $x = hk \in HK$ and $y = h'k' \in HK$. Then $xy = hkh'k'$, but since $kh' \in KH = HK$, $kh' = h_2k_2$ with $h_2 \in H$, $k_2 \in K$. Hence $xy = h(h_2k_2)k' = (hh_2)(k_2k') \in HK$, and HK is closed. Also $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, so $x^{-1} \in HK$. Thus HK is a subgroup of G.

On the other hand, if HK is a subgroup of G, then for any $h \in H$, $k \in K$, $h^{-1}k^{-1} \in HK$ and so $kh = (h^{-1}k^{-1})^{-1} \in HK$. Thus $KH \subset HK$. Now if x is any element of HK, $x^{-1} = hk \in HK$ and so $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$, so $HK \subset KH$. Thus $HK = KH$.

An interesting special case is the situation when G is an abelian group for in that case trivially $HK = KH$. Thus as a consequence we have the

COROLLARY *If H, K are subgroups of the abelian group G, then HK is a subgroup of G.*

If H, K are subgroups of a group G, we have seen that the subset HK need not be a subgroup of G. Yet it is a perfect meaningful question to ask: How many distinct elements are there in the subset HK? If we denote this number by $o(HK)$, we prove

THEOREM 2.5.1 *If H and K are finite subgroups of G of orders $o(H)$ and $o(K)$, respectively, then*

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$

Proof. Although there is no need to pay special attention to the particular case in which $H \cap K = (e)$, looking at this case, which is devoid of some of the complexity of the general situation, is quite revealing. Here we should seek to show that $o(HK) = o(H)o(K)$. One should ask oneself: How could this fail to happen? The answer clearly must be that if we list all the elements hk, $h \in H$, $k \in K$ there should be some collapsing; that is, some element in the list must appear at least twice. Equivalently, for some $h \neq h_1 \in H$, $hk = h_1k_1$. But then $h_1^{-1}h = k_1k^{-1}$; now since $h_1 \in H$, h_1^{-1} must also be in H, thus $h_1^{-1}h \in H$. Similarly, $k_1k^{-1} \in K$. Since $h_1^{-1}h = k_1k^{-1}$, $h_1^{-1}h \in H \cap K = (e)$, so $h_1^{-1}h = e$, whence $h = h_1$, a contradiction. We have proved that no collapsing can occur, and so, here, $o(HK)$ is indeed $o(H)o(K)$.

With this experience behind us we are ready to attack the general case. As above we must ask: How often does a given element hk appear as a product in the list of HK? We assert it must appear $o(H \cap K)$ times! To see this we first remark that if $h_1 \in H \cap K$, then

$$hk = (hh_1)(h_1^{-1}k), \tag{1}$$

where $hh_1 \in H$, since $h \in H$, $h_1 \in H \cap K \subset H$ and $h_1^{-1}k \in K$ since $h_1^{-1} \in H \cap K \subset K$ and $k \in K$. Thus hk is duplicated in the product at least $o(H \cap K)$ times. However, if $hk = h'k'$, then $h^{-1}h' = k(k')^{-1} = u$, and $u \in H \cap K$, and so $h' = hu$, $k' = u^{-1}k$; thus all duplications were accounted for in (1). Consequently hk appears in the list of HK exactly $o(H \cap K)$ times. Thus the number of distinct elements in HK is the total number in the listing of HK, that is, $o(H)o(K)$ divided by the number of times a given element appears, namely, $o(H \cap K)$. This proves the theorem.

Suppose H, K are subgroups of the finite group G and $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$. Since $HK \subset G$, $o(HK) \leq o(G)$. However,

$$o(G) \geq o(HK) = \frac{o(H)o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)},$$

thus $o(H \cap K) > 1$. Therefore, $H \cap K \neq (e)$. We have proved the

COROLLARY *If H and K are subgroups of G and $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$, then $H \cap K \neq (e)$.*

We apply this corollary to a very special group. Suppose G is a finite group of order pq where p and q are prime numbers with $p > q$. We claim that G can have at most one subgroup of order p. For suppose H, K are subgroups of order p. By the corollary, $H \cap K \neq (e)$, and being a subgroup of H, which having prime order has no nontrivial subgroups, we must conclude that $H \cap K = H$, and so $H \subset H \cap K \subset K$. Similarly $K \subset H$, whence $H = K$, proving that there is at most one subgroup of order p. Later on we shall see that there is at least one subgroup of order p, which, combined with the above, will tell us there is exactly one subgroup of order p in G. From this we shall be able to determine completely the structure of G.

Problems

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

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 $o(aHa^{-1})$?
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.
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 $H = \{\sigma \in G \mid x_1\sigma = x_1\}$.
7. Write out all the left cosets of H in G for H and G as in parts (a), (b), (c) of Problem 6.
8. Is every right coset of H in G a left coset of H in G in the groups of Problem 6?
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 $g \in G$.
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.
11. In Problem 10, what is $H_n \cap H_m$?
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?
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.
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.
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?
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) $N(H) \supset H$.
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 $C(H)$?

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 $a \in G$.

*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}.

*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?

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 $\tau_{ab}\tau_{cd}$.

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.

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 $ana^{-1} \in N$.

*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.

*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.

**26. If an abelian group has subgroups of orders m and n, respectively, then show it has a subgroup whose order is the least common multiple of m and n. (Don't be discouraged if you don't get this problem with what you know about group theory up to this stage. I don't know anybody, including myself, who has done it subject to the restriction of using material developed so far in the text. But it is fun to try. I've had more correspondence about this problem than about any other point in the whole book.)

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

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

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.
30. Show that U_9 is a cyclic group. What are all its generators?
31. Show that U_{17} is a cyclic group. What are all its generators?
32. Show that U_{18} is a cyclic group.
33. Show that U_{20} is not a cyclic group.
34. Show that both U_{25} and U_{27} are cyclic groups.
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.)
36. If $a \in G$ and $a^m = e$, prove that $o(a) \mid m$.
37. If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for some $a, b \in G$, find $o(b)$.
*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.
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.)
40. If G is a finite group, show that the number of elements in the double coset AxB is
$$\frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$
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 $g \in G$.

2.6 Normal Subgroups and Quotient Groups

Let G be the group S_3 and let H be the subgroup $\{e, \phi\}$. Since the index of H in G is 3, there are three right cosets of H in G and three left cosets of H in G. We list them:

Right Cosets	Left Cosets
$H = \{e, \phi\}$	$H = \{e, \phi\}$
$H\psi = \{\psi, \phi\psi\}$	$\psi H = \{\psi, \psi\phi = \phi\psi^2\}$
$H\psi^2 = \{\psi^2, \phi\psi^2\}$	$\psi^2 H = \{\psi^2, \psi^2\phi = \phi\psi\}$

A quick inspection yields the interesting fact that the right coset $H\psi$ is not a left coset. Thus, at least for this subgroup, the notions of left and right coset need not coincide.

In $G = S_3$ let us consider the subgroup $N = \{e, \psi, \psi^2\}$. Since the index of N in G is 2 there are two left cosets and two right cosets of N in G. We list these:

Right Cosets	Left Cosets
$N = \{e, \psi, \psi^2\}$	$N = \{e, \psi, \psi^2\}$
$N\phi = \{\phi, \psi\phi, \psi^2\phi\}$	$\phi N = \{\phi, \phi\psi, \phi\psi^2\}$
	$= \{\phi, \psi^2\phi, \psi\phi\}$

A quick inspection here reveals that every left coset of N in G is a right coset in G and conversely. Thus we see that for some subgroups the notion of left coset coincides with that of right coset, whereas for some subgroups these concepts differ.

It is a tribute to the genius of Galois that he recognized that those subgroups for which the left and right cosets coincide are distinguished ones. Very often in mathematics the crucial problem is to recognize and to discover what are the relevant concepts; once this is accomplished the job may be more than half done.

We shall define this special class of subgroups in a slightly different way, which we shall then show to be equivalent to the remarks in the above paragraph.

DEFINITION A subgroup N of G is said to be a *normal subgroup* of G if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Equivalently, if by gNg^{-1} we mean the set of all gng^{-1}, $n \in N$, then N is a normal subgroup of G if and only if $gNg^{-1} \subset N$ for every $g \in G$.

LEMMA 2.6.1 *N is a normal subgroup of G if and only if $gNg^{-1} = N$ for every $g \in G$.*

Proof. If $gNg^{-1} = N$ for every $g \in G$, certainly $gNg^{-1} \subset N$, so N is normal in G.

Suppose that N is normal in G. Thus if $g \in G$, $gNg^{-1} \subset N$ and $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subset N$. Now, since $g^{-1}Ng \subset N$, $N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N$, whence $N = gNg^{-1}$.

In order to avoid a point of confusion here let us stress that Lemma 2.6.1 *does not* say that for every $n \in N$ and every $g \in G$, $gng^{-1} = n$. No! This can be false. Take, for instance, the group G to be S_3 and N to be the sub-

group $\{e, \psi, \psi^2\}$. If we compute $\phi N\phi^{-1}$ we obtain $\{e, \phi\psi\phi^{-1}, \phi\psi^2\phi^{-1}\} = \{e, \psi^2, \psi\}$, yet $\phi\psi\phi^{-1} \neq \psi$. All we require is that the *set* of elements gNg^{-1} be the same as the *set* of elements N.

We now can return to the question of the equality of left cosets and right cosets.

LEMMA 2.6.2 *The subgroup N of G is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.*

Proof. If N is a normal subgroup of G, then for every $g \in G$, $gNg^{-1} = N$, whence $(gNg^{-1})g = Ng$; equivalently $gN = Ng$, and so the left coset gN is the right coset Ng.

Suppose, conversely, that every left coset of N in G is a right coset of N in G. Thus, for $g \in G$, gN, being a left coset, must be a right coset. What right coset can it be?

Since $g = ge \in gN$, whatever right coset gN turns out to be, it must contain the element g; however, g is in the right coset Ng, and two distinct right cosets have no element in common. (Remember the proof of Lagrange's theorem?) So this right coset is unique. Thus $gN = Ng$ follows. In other words, $gNg^{-1} = Ngg^{-1} = N$, and so N is a normal subgroup of G.

We have already defined what is meant by HK whenever H, K are subgroups of G. We can easily extend this definition to arbitrary subsets, and we do so by defining, for two subsets, A and B, of G, $AB = \{x \in G \mid x = ab, a \in A, b \in B\}$. As a special case, what can we say when $A = B = H$, a subgroup of G? $HH = \{h_1h_2 \mid h_1, h_2 \in H\} \subset H$ since H is closed under multiplication. But $HH \supset He = H$ since $e \in H$. Thus $HH = H$.

Suppose that N is a normal subgroup of G, and that $a, b \in G$. Consider $(Na)(Nb)$; since N is normal in G, $aN = Na$, and so

$$NaNb = N(aN)b = N(Na)b = NNab = Nab.$$

What a world of possibilities this little formula opens! But before we get carried away, for emphasis and future reference we record this as

LEMMA 2.6.3 *A subgroup N of G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.*

Proof. If N is normal in G we have just proved the result. The proof of the other half is one of the problems at the end of this section.

Suppose that N is a normal subgroup of G. The formula $NaNb = Nab$, for $a, b \in G$ is highly suggestive; the product of right cosets is a right coset. Can we use this product to make the collection of right cosets into a group? Indeed we can! This type of construction, often occurring in mathematics and usually called forming a *quotient structure*, is of the utmost importance.

Let G/N denote the collection of right cosets of N in G (that is, the elements of G/N are certain subsets of G) and we use the product of subsets of G to yield for us a product in G/N.

For this product we claim

1. $X, Y \in G/N$ implies $XY \in G/N$; for $X = Na$, $Y = Nb$ for some $a, b \in G$, and $XY = NaNb = Nab \in G/N$.
2. $X, Y, Z \in G/N$, then $X = Na$, $Y = Nb$, $Z = Nc$ with $a, b, c \in G$, and so $(XY)Z = (NaNb)Nc = N(ab)Nc = N(ab)c = Na(bc)$ (since G is associative) $= Na(Nbc) = Na(NbNc) = X(YZ)$. Thus the product in G/N satisfies the associative law.
3. Consider the element $N = Ne \in G/N$. If $X \in G/N$, $X = Na$, $a \in G$, so $XN = NaNe = Nae = Na = X$, and similarly $NX = X$. Consequently, Ne is an identity element for G/N.
4. Suppose $X = Na \in G/N$ (where $a \in G$); thus $Na^{-1} \in G/N$, and $NaNa^{-1} = Naa^{-1} = Ne$. Similarly $Na^{-1}Na = Ne$. Hence Na^{-1} is the inverse of Na in G/N.

But a system which satisfies 1, 2, 3, 4 is exactly what we called a group. That is,

THEOREM 2.6.1 *If G is a group, N a normal subgroup of G, then G/N is also a group. It is called the quotient group or factor group of G by N.*

If, in addition, G is a finite group, what is the order of G/N? Since G/N has as its elements the right cosets of N in G, and since there are precisely $i_G(N) = o(G)/o(N)$ such cosets, we can say

LEMMA 2.6.4 *If G is a finite group and N is a normal subgroup of G, then $o(G/N) = o(G)/o(N)$.*

We close this section with an example.

Let G be the group of integers under addition and let N be the set of all multiplies of 3. Since the operation in G is addition we shall write the cosets of N in G as $N + a$ rather than as Na. Consider the three cosets N, $N + 1$, $N + 2$. We claim that these are all the cosets of N in G. For, given $a \in G$, $a = 3b + c$ where $b \in G$ and $c = 0$, 1, or 2 (c is the remainder of a on division by 3). Thus $N + a = N + 3b + c = (N + 3b) + c = N + c$ since $3b \in N$. Thus every coset is, as we stated, one of N, $N + 1$, or $N + 2$, and $G/N = \{N, N + 1, N + 2\}$. How do we add elements in G/N? Our formula $NaNb = Nab$ translates into: $(N + 1) + (N + 2) = N + 3 = N$ since $3 \in N$; $(N + 2) + (N + 2) = N + 4 = N + 1$ and so on. Without being specific one feels that G/N is closely related to the integers mod 3 under addition. Clearly what we did for 3 we could emulate

for any integer n, in which case the factor group should suggest a relation to the integers mod n under addition. This type of relation will be clarified in the next section.

Problems

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.
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.
3. If N is a normal subgroup of G and H is any subgroup of G, prove that NH is a subgroup of G.
4. Show that the intersection of two normal subgroups of G is a normal subgroup of G.
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.
6. Show that every subgroup of an abelian group is normal.
*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.
8. Give an example of a group G, subgroup H, and an element $a \in G$ such that $aHa^{-1} \subset H$ but $aHa^{-1} \neq H$.
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.
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 $N(H) = G$.
11. If N and M are normal subgroups of G, prove that NM is also a normal subgroup of G.
*12. Suppose that N and M are two normal subgroups of G and that $N \cap M = (e)$. Show that for any $n \in N$, $m \in M$, $nm = mn$.
13. If a cyclic subgroup T of G is normal in G, then show that every subgroup of T 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.
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 $o(a)$.

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.

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

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

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

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

(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.

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.

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 $a, b \in G$.

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 $S = \{x \in G \mid x^{p^m} = e \text{ for some } m \text{ depending on } x\}$. 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 $\bar{x} = \bar{e}$.

#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.

2.7 Homomorphisms

The ideas and results in this section are closely interwoven with those of the preceding one. If there is one central idea which is common to all aspects of modern algebra it is the notion of homomorphism. By this one means

a mapping from one algebraic system to a like algebraic system which preserves structure. We make this precise, for groups, in the next definition.

DEFINITION A mapping ϕ from a group G into a group $\bar{G}$ is said to be a *homomorphism* if for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Notice that on the left side of this relation, namely, in the term $\phi(ab)$, the product ab is computed in G using the product of elements of G, whereas on the right side of this relation, namely, in the term $\phi(a)\phi(b)$, the product is that of elements in $\bar{G}$.

Example 2.7.0 $\phi(x) = e$ all $x \in G$. This is trivially a homomorphism. Likewise $\phi(x) = x$ for every $x \in G$ is a homomorphism.

Example 2.7.1 Let G be the group of all real numbers under addition (i.e., ab for $a, b \in G$ is really the real number $a + b$) and let $\bar{G}$ be the group of nonzero real numbers with the product being ordinary multiplication of real numbers. Define $\phi: G \to \bar{G}$ by $\phi(a) = 2^a$. In order to verify that this mapping is a homomorphism we must check to see whether $\phi(ab) = \phi(a)\phi(b)$, remembering that by the product on the left side we mean the operation in G (namely, addition), that is, we must check if $2^{a+b} = 2^a 2^b$, which indeed is true. Since 2^a is always positive, the image of ϕ is not all of $\bar{G}$, so ϕ is a homomorphism of G into $\bar{G}$, but not onto $\bar{G}$.

Example 2.7.2 Let $G = S_3 = \{e, \phi, \psi, \psi^2, \phi\psi, \phi\psi^2\}$ and $\bar{G} = \{e, \phi\}$. Define the mapping $f: G \to \bar{G}$ by $f(\phi^i\psi^j) = \phi^i$. Thus $f(e) = e, f(\phi) = \phi, f(\psi) = e, f(\psi^2) = e, f(\phi\psi) = \phi, f(\phi\psi^2) = \phi$. The reader should verify that f so defined is a homomorphism.

Example 2.7.3 Let G be the group of integers under addition and let $\bar{G} = G$. For the integer $x \in G$ define ϕ by $\phi(x) = 2x$. That ϕ is a homomorphism then follows from $\phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y)$.

Example 2.7.4 Let G be the group of nonzero real numbers under multiplication, $\bar{G} = \{1, -1\}$, where $1.1 = 1$, $(-1)(-1) = 1$, $1(-1) = (-1)1 = -1$. Define $\phi: G \to \bar{G}$ by $\phi(x) = 1$ if x is positive, $\phi(x) = -1$ if x is negative. The fact that ϕ is a homomorphism is equivalent to the statements: positive times positive is positive, positive times negative is negative, negative times negative is positive.

Example 2.7.5 Let G be the group of integers under addition, let $\bar{G}_n$ be the group of integers under addition modulo n. Define ϕ by $\phi(x) =$ remainder of x on division by n. One can easily verify this is a homomorphism.

Example 2.7.6 Let G be the group of positive real numbers under multiplication and let $\bar{G}$ be the group of all real numbers under addition. Define $\phi: G \to G$ by $\phi(x) = \log_{10} x$. Thus

$$\phi(xy) = \log_{10}(xy) = \log_{10}(x) + \log_{10}(y) = \phi(x)\phi(y)$$

since the operation, on the right side, in $\bar{G}$ is in fact addition. Thus ϕ is a homomorphism of G into $\bar{G}$. In fact, not only is ϕ a homomorphism but, in addition, it is one-to-one and onto.

#Example 2.7.7 Let G be the group of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $ad - bc \neq 0$, under matrix multiplication. Let $\bar{G}$ be the group of all nonzero real numbers under multiplication. Define $\phi: G \to \bar{G}$ by $\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.

We leave it to the reader to check that ϕ is a homomorphism of G onto $\bar{G}$.

The result of the following lemma yields, for us, an infinite class of examples of homomorphisms. When we prove Theorem 2.7.1 it will turn out that in some sense this provides us with the most general example of a homomorphism.

LEMMA 2.7.1 *Suppose G is a group, N a normal subgroup of G; define the mapping ϕ from G to G/N by $\phi(x) = Nx$ for all $x \in G$. Then ϕ is a homomorphism of G onto G/N.*

Proof. In actuality, there is nothing to prove, for we already have proved this fact several times. But for the sake of emphasis we repeat it.

That ϕ is onto is trivial, for every element $X \in G/N$ is of the form $X = Ny$, $y \in G$, so $X = \phi(y)$. To verify the multiplicative property required in order that ϕ be a homomorphism, one just notes that if $x, y \in G$,

$$\phi(xy) = Nxy = NxNy = \phi(x)\phi(y).$$

In Lemma 2.7.1 and in the examples preceding it, a fact which comes through is that a homomorphism need not be one-to-one; but there is a certain uniformity in this process of deviating from one-to-oneness. This will become apparent in a few lines.

DEFINITION If ϕ is a homomorphism of G into $\bar{G}$, the *kernel of* ϕ, K_ϕ, is defined by $K_\phi = \{x \in G \mid \phi(x) = \bar{e}, \bar{e} = \text{identity element of } \bar{G}\}$.

Before investigating any properties of K_ϕ it is advisable to establish that, as a set, K_ϕ is not empty. This is furnished us by the first part of

LEMMA 2.7.2 *If ϕ is a homomorphism of G into $\bar{G}$, then*

1. $\phi(e) = \bar{e}$, *the unit element of* $\bar{G}$.
2. $\phi(x^{-1}) = \phi(x)^{-1}$ *for all* $x \in G$.

Proof. To prove (1) we merely calculate $\phi(x)\bar{e} = \phi(x) = \phi(xe) = \phi(x)\phi(e)$, so by the cancellation property in $\bar{G}$ we have that $\phi(e) = \bar{e}$.

To establish (2) one notes that $\bar{e} = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$, so by the very definition of $\phi(x)^{-1}$ in $\bar{G}$ we obtain the result that $\phi(x^{-1}) = \phi(x)^{-1}$.

The argument used in the proof of Lemma 2.7.2 should remind any reader who has been exposed to a development of logarithms of the argument used in proving the familiar results that $\log 1 = 0$ and $\log (1/x) = -\log x$; this is no coincidence, for the mapping $\phi: x \to \log x$ is a homomorphism of the group of positive real numbers under multiplication into the group of real numbers under addition, as we have seen in Example 2.7.6.

Lemma 2.7.2 shows that e is in the kernel of any homomorphism, so any such kernel is not empty. But we can say even more.

LEMMA 2.7.3 *If ϕ is a homomorphism of G into $\bar{G}$ with kernel K, then K is a normal subgroup of G.*

Proof. First we must check whether K is a subgroup of G. To see this one must show that K is closed under multiplication and has inverses in it for every element belonging to K.

If $x, y \in K$, then $\phi(x) = \bar{e}$, $\phi(y) = \bar{e}$, where $\bar{e}$ is the identity element of $\bar{G}$, and so $\phi(xy) = \phi(x)\phi(y) = \bar{e}\bar{e} = \bar{e}$, whence $xy \in K$. Also, if $x \in K$, $\phi(x) = \bar{e}$, so, by Lemma 2.7.2, $\phi(x^{-1}) = \phi(x)^{-1} = \bar{e}^{-1} = \bar{e}$; thus $x^{-1} \in K$. K is, accordingly, a subgroup of G.

To prove the normality of K one must establish that for any $g \in G$, $k \in K$, $gkg^{-1} \in K$; in other words, one must prove that $\phi(gkg^{-1}) = \bar{e}$ whenever $\phi(k) = \bar{e}$. But $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\bar{e}\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = \bar{e}$. This completes the proof of Lemma 2.7.3.

Let ϕ now be a homomorphism of the group G *onto* the group $\bar{G}$, and suppose that K is the kernel of ϕ. If $\bar{g} \in \bar{G}$, we say an element $x \in G$ is an *inverse image* of $\bar{g}$ under ϕ if $\phi(x) = \bar{g}$. What are all the inverse images of $\bar{g}$? For $\bar{g} = \bar{e}$ we have the answer, namely (by its very definition) K. What about elements $\bar{g} \neq \bar{e}$? Well, suppose $x \in G$ is one inverse image of $\bar{g}$; can we write down others? Clearly yes, for if $k \in K$, and if $y = kx$, then $\phi(y) = \phi(kx) = \phi(k)\phi(x) = \bar{e}\bar{g} = \bar{g}$. Thus all the elements Kx are in the inverse image of $\bar{g}$ whenever x is. Can there be others? Let us suppose that $\phi(z) = \bar{g} = \phi(x)$. Ignoring the middle term we are left with $\phi(z) = \phi(x)$, and so $\phi(z)\phi(x)^{-1} = \bar{e}$. But $\phi(x)^{-1} = \phi(x^{-1})$, whence

$\bar{e} = \phi(z)\phi(x)^{-1} = \phi(z)\phi(x^{-1}) = \phi(zx^{-1})$, in consequence of which $zx^{-1} \in K$; thus $z \in Kx$. In other words, we have shown that Kx accounts for exactly all the inverse images of $\bar{g}$ whenever x is a single such inverse image. We record this as

LEMMA 2.7.4 *If ϕ is a homomorphism of G onto $\bar{G}$ with kernel K, then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ in G is given by Kx, where x is any particular inverse image of $\bar{g}$ in G.*

A special case immediately presents itself, namely, the situation when $K = (e)$. But here, by Lemma 2.7.4, any $\bar{g} \in \bar{G}$ has exactly one inverse image. That is, ϕ is a one-to-one mapping. The converse is trivially true, namely, if ϕ is a one-to-one homomorphism of G into (not even onto) G, its kernel must consist exactly of e.

DEFINITION A homomorphism ϕ from G into $\bar{G}$ is said to be an *isomorphism* if ϕ is one-to-one.

DEFINITION Two groups G, G^* are said to be *isomorphic* if there is an isomorphism of G *onto* G^*. In this case we write $G \approx G^*$.

We leave to the reader to verify the following three facts:

1. $G \approx G$.
2. $G \approx G^*$ implies $G^* \approx G$.
3. $G \approx G^*$, $G^* \approx G^{**}$ implies $G \approx G^{**}$.

When two groups are isomorphic, then, in some sense, they are equal. They differ in that their elements are labeled differently. The isomorphism gives us the key to the labeling, and with it, knowing a given computation in one group, we can carry out the analogous computation in the other. The isomorphism is like a dictionary which enables one to translate a sentence in one language into a sentence, of the same meaning, in another language. (Unfortunately no such perfect dictionary exists, for in languages words do not have single meanings, and nuances do not come through in a literal translation.) But merely to say that a given sentence in one language can be expressed in another is of little consequence; one needs the dictionary to carry out the translation. Similarly it might be of little consequence to know that two groups are isomorphic; the object of interest might very well be the isomorphism itself. So, whenever we prove two groups to be isomorphic, we shall endeavor to exhibit the precise mapping which yields this isomorphism.

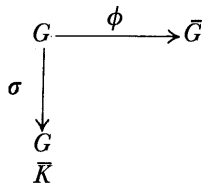
Returning to Lemma 2.7.4 for a moment, we see in it a means of characterizing in terms of the kernel when a homomorphism is actually an isomorphism.

COROLLARY *A homomorphism ϕ of G into $\bar{G}$ with kernel K_ϕ is an isomorphism of G into $\bar{G}$ if and only if $K_\phi = (e)$.*

This corollary provides us with a standard technique for proving two groups to be isomorphic. First we find a homomorphism of one onto the other, and then prove the kernel of this homomorphism consists only of the identity element. This method will be illustrated for us in the proof of the very important

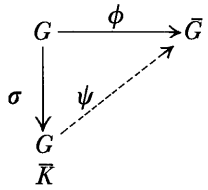
THEOREM 2.7.1 *Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. Then $G/K \approx \bar{G}$.*

Proof. Consider the diagram

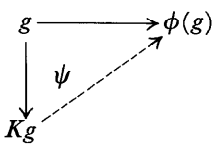


where $\sigma(g) = Kg$.

We should like to complete this to



It seems clear that, in order to construct the mapping ψ from G/K to $\bar{G}$, we should use G as an intermediary, and also that this construction should be relatively uncomplicated. What is more natural than to complete the diagram using



With this preamble we formally define the mapping ψ from G/K to $\bar{G}$ by: if $X \in G/K$, $X = Kg$, then $\psi(X) = \phi(g)$. A problem immediately arises: is this mapping well defined? If $X \in G/K$, it can be written as Kg in several ways (for instance, $Kg = Kkg$, $k \in K$); but if $X = Kg = Kg'$, $g, g' \in G$, then on one hand $\psi(X) = \phi(g)$, and on the other, $\psi(X) = \phi(g')$. For the mapping ψ to make sense it had better be true that $\phi(g) = \phi(g')$. So, suppose $Kg = Kg'$; then $g = kg'$, where $k \in K$, hence $\phi(g) = \phi(kg') = \phi(k)\phi(g') = \bar{e}\phi(g') = \phi(g')$ since $k \in K$, the kernel of ϕ.

We next determine that ψ is onto. For, if $\bar{x} \in \bar{G}$, $\bar{x} = \phi(g)$, $g \in G$ (since ϕ is onto) so $\bar{x} = \phi(g) = \psi(Kg)$.

If $X, Y \in G/K$, $X = Kg$, $Y = Kf$, $g,f \in G$, then $XY = KgKf = Kgf$, so that $\psi(XY) = \psi(Kgf) = \phi(gf) = \phi(g)\phi(f)$ since ϕ is a homomorphism of G onto $\bar{G}$. But $\psi(X) = \psi(Kg) = \phi(g)$, $\psi(Y) = \psi(Kf) = \phi(f)$, so we see that $\psi(XY) = \psi(X)\psi(Y)$, and ψ is a homomorphism of G/K onto $\bar{G}$.

To prove that ψ is an isomorphism of G/K onto $\bar{G}$ all that remains is to demonstrate that the kernel of ψ is the unit element of G/K. Since the unit element of G/K is $K = Ke$, we must show that if $\psi(Kg) = \bar{e}$, then $Kg = Ke = K$. This is now easy, for $\bar{e} = \psi(Kg) = \phi(g)$, so that $\phi(g) = \bar{e}$, whence g is in the kernel of ϕ, namely K. But then $Kg = K$ since K is a subgroup of G. All the pieces have been put together. We have exhibited a one-to-one homomorphism of G/K onto $\bar{G}$. Thus $G/K \approx \bar{G}$, and Theorem 2.7.1 is established.

Theorem 2.7.1 is important, for it tells us precisely what groups can be expected to arise as homomorphic images of a given group. These must be expressible in the form G/K, where K is normal in G. But, by Lemma 2.7.1, for any normal subgroup N of G, G/N is a homomorphic image of G. Thus there is a one-to-one correspondence between homomorphic images of G and normal subgroups of G. If one were to seek all homomorphic images of G one could do it by never leaving G as follows: find all normal subgroups N of G and construct all groups G/N. The set of groups so constructed yields all homomorphic images of G (up to isomorphisms).

A group is said to be *simple* if it has no nontrivial homomorphic images, that is, if it has no nontrivial normal subgroups. A famous, long-standing conjecture was that a non-abelian simple group of finite order has an even number of elements. This important result has been proved by the two American mathematicians, Walter Feit and John Thompson.

We have stated that the concept of a homomorphism is a very important one. To strengthen this statement we shall now show how the methods and results of this section can be used to prove nontrivial facts about groups. When we construct the group G/N, where N is normal in G, if we should happen to know the structure of G/N we would know that of G "up to N." True, we blot out a certain amount of information about G, but often

enough is left so that from facts about G/N we can ascertain certain ones about G. When we photograph a certain scene we transfer a three-dimensional object to a two-dimensional representation of it. Yet, looking at the picture we can derive a great deal of information about the scene photographed.

In the two applications of the ideas developed so far, which are given below, the proofs given are not the best possible. In fact, a little later in this chapter these results will be proved in a more general situation in an easier manner. We use the presentation here because it does illustrate effectively many group-theoretic concepts.

APPLICATION 1 (CAUCHY'S THEOREM FOR ABELIAN GROUPS) *Suppose G is a finite abelian group and $p \mid o(G)$, where p is a prime number. Then there is an element $a \neq e \in G$ such that $a^p = e$.*

Proof. We proceed by induction over $o(G)$. In other words, we assume that the theorem is true for all abelian groups having fewer elements than G. From this we wish to prove that the result holds for G. To start the induction we note that the theorem is vacuously true for groups having a single element.

If G has no subgroups $H \neq (e)$, G, by the result of a problem earlier in the chapter, G must be cyclic of prime order. This prime must be p, and G certainly has $p - 1$ elements $a \neq e$ satisfying $a^p = a^{o(G)} = e$.

So suppose G has a subgroup $N \neq (e)$, G. If $p \mid o(N)$, by our induction hypothesis, since $o(N) < o(G)$ and N is abelian, there is an element $b \in N$, $b \neq e$, satisfying $b^p = e$; since $b \in N \subset G$ we would have exhibited an element of the type required. So we may assume that $p \nmid o(N)$. Since G is abelian, N is a normal subgroup of G, so G/N is a group. Moreover, $o(G/N) = o(G)/o(N)$, and since $p \nmid o(N)$,

$$p \left| \frac{o(G)}{o(N)} < o(G). \right.$$

Also, since G is abelian, G/N is abelian. Thus by our induction hypothesis there is an element $X \in G/N$ satisfying $X^p = e_1$, the unit element of G/N, $X \neq e_1$. By the very form of the elements of G/N, $X = Nb$, $b \in G$, so that $X^p = (Nb)^p = Nb^p$. Since $e_1 = Ne$, $X^p = e_1$, $X \neq e_1$ translates into $Nb^p = N$, $Nb \neq N$. Thus $b^p \in N$, $b \notin N$. Using one of the corollaries to Lagrange's theorem, $(b^p)^{o(N)} = e$. That is, $b^{o(N)p} = e$. Let $c = b^{o(N)}$. Certainly $c^p = e$. In order to show that c is an element that satisfies the conclusion of the theorem we must finally show that $c \neq e$. However, if $c = e$, $b^{o(N)} = e$, and so $(Nb)^{o(N)} = N$. Combining this with $(Nb)^p = N$, $p \nmid o(N)$, p a prime number, we find that $Nb = N$, and so $b \in N$, a contradiction. Thus $c \neq e$, $c^p = e$, and we have completed the induction. This proves the result.

APPLICATION 2 (SYLOW'S THEOREM FOR ABELIAN GROUPS) *If G is an abelian group of order $o(G)$, and if p is a prime number, such that $p^\alpha \mid o(G)$, $p^{\alpha+1} \nmid o(G)$, then G has a subgroup of order p^α.*

Proof. If $\alpha = 0$, the subgroup (e) satisfies the conclusion of the result. So suppose $\alpha \neq 0$. Then $p \mid o(G)$. By Application 1, there is an element $a \neq e \in G$ satisfying $a^p = e$. Let $S = \{x \in G \mid x^{p^n} = e \text{ some integer } n\}$. Since $a \in S$, $a \neq e$, it follows that $S \neq (e)$. We now assert that S is a subgroup of G. Since G is finite we must only verify that S is closed. If $x, y \in S$, $x^{p^n} = e$, $y^{p^m} = e$, so that $(xy)^{p^{n+m}} = x^{p^{n+m}} y^{p^{n+m}} = e$ (we have used that G is abelian), proving that $xy \in S$.

We next claim that $o(S) = p^\beta$ with β an integer $0 < \beta \leq \alpha$. For, if some prime $q \mid o(S)$, $q \neq p$, by the result of Application 1 there is an element $c \in S$, $c \neq e$, satisfying $c^q = e$. However, $c^{p^n} = e$ for some n since $c \in S$. Since p^n, q are relatively prime, we can find integers λ, μ such that $\lambda q + \mu p^n = 1$, so that $c = c^1 = c^{\lambda q + \mu p^n} = (c^q)^\lambda (c^{p^n})^\mu = e$, contradicting $c \neq e$. By Lagrange's theorem $o(S) \mid o(G)$, so that $\beta \leq \alpha$. Suppose that $\beta < \alpha$; consider the abelian group G/S. Since $\beta < \alpha$ and $o(G/S) = o(G)/o(S)$, $p \mid o(G/S)$, there is an element Sx, $(x \in G)$ in G/S satisfying $Sx \neq S$, $(Sx)^{p^n} = S$ for some integer $n > 0$. But $S = (Sx)^{p^n} = Sx^{p^n}$, and so $x^{p^n} \in S$; consequently $e = (x^{p^n})^{o(S)} = (x^{p^n})^{p^\beta} = x^{p^{n+\beta}}$. Therefore, x satisfies the exact requirements needed to put it in S; in other words, $x \in S$. Consequently $Sx = S$ contradicting $Sx \neq S$. Thus $\beta < \alpha$ is impossible and we are left with the only alternative, namely, that $\beta = \alpha$. S is the required subgroup of order p^α.

We strengthen the application slightly. Suppose T is another subgroup of G of order p^α, $T \neq S$. Since G is abelian $ST = TS$, so that ST is a subgroup of G. By Theorem 2.5.1

$$o(ST) = \frac{o(S)o(T)}{o(S \cap T)} = \frac{p^\alpha p^\alpha}{o(S \cap T)}$$

and since $S \neq T$, $o(S \cap T) < p^\alpha$, leaving us with $o(ST) = p^\gamma$, $\gamma > \alpha$. Since ST is a subgroup of G, $o(ST) \mid o(G)$; thus $p^\gamma \mid o(G)$ violating the fact that α is the largest power of p which divides $o(G)$. Thus no such subgroup T exists, and S is the unique subgroup of order p^α. We have proved the

COROLLARY *If G is abelian of order $o(G)$ and $p^\alpha \mid o(G)$, $p^{\alpha+1} \nmid o(G)$, there is a unique subgroup of G of order p^α.*

If we look at $G = S_3$, which is non-abelian, $o(G) = 2.3$, we see that G has 3 distinct subgroups of order 2, namely, $\{e, \phi\}$, $\{e, \phi\psi\}$, $\{e, \phi\psi^2\}$, so that the corollary asserting the uniqueness does not carry over to non-abelian groups. But Sylow's theorem holds for all finite groups.

We leave the application and return to the general development. Suppose ϕ is a homomorphism of G onto $\bar{G}$ with kernel K, and suppose that $\bar{H}$ is a subgroup of $\bar{G}$. Let $H = \{x \in G \mid \phi(x) \in \bar{H}\}$. We assert that H is a subgroup of G and that $H \supset K$. That $H \supset K$ is trivial, for if $x \in K$, $\phi(x) = \bar{e}$ is in $\bar{H}$, so that $K \subset H$ follows. Suppose now that $x, y \in H$; hence $\phi(x) \in \bar{H}$, $\phi(y) \in \bar{H}$ from which we deduce that $\phi(xy) = \phi(x)\phi(y) \in \bar{H}$. Therefore, $xy \in H$ and H is closed under the product in G. Furthermore, if $x \in H$, $\phi(x) \in \bar{H}$ and so $\phi(x^{-1}) = \phi(x)^{-1} \in \bar{H}$ from which it follows that $x^{-1} \in H$. All in all, our assertion has been established. What can we say in addition in case $\bar{H}$ is normal in $\bar{G}$? Let $g \subset G$, $h \subset H$; then $\phi(h) \subset \bar{H}$, whence $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} \in \bar{H}$, since $\bar{H}$ is normal in G. Otherwise stated, $ghg^{-1} \in H$, from which it follows that H is normal in G. One other point should be noted, namely, that the homomorphism ϕ from G onto $\bar{G}$, when just considered on elements of H, induces a homomorphism of H onto $\bar{H}$, with kernel exactly K, since $K \subset H$; by Theorem 2.7.1 we have that $\bar{H} \approx H/K$.

Suppose, conversely, that L is a subgroup of G and $K \subset L$. Let $\bar{L} = \{\bar{x} \in \bar{G} \mid \bar{x} = \phi(l), l \in L\}$. The reader should verify that $\bar{L}$ is a subgroup of $\bar{G}$. Can we explicitly describe the subgroup $T = \{y \in G \mid \phi(y) \in \bar{L}\}$? Clearly $L \subset T$. Is there any element $t \in T$ which is not in L? So, suppose $t \in T$; thus $\phi(t) \in \bar{L}$, so by the very definition of $\bar{L}$, $\phi(t) = \phi(l)$ for some $l \in L$. Thus $\phi(tl^{-1}) = \phi(t)\phi(l)^{-1} = \bar{e}$, whence $tl^{-1} \in K \subset L$, thus t is in $Ll = L$. Equivalently we have proved that $T \subset L$, which, combined with $L \subset T$, yields that $L = T$.

Thus we have set up a one-to-one correspondence between the set of all subgroups of $\bar{G}$ and the set of all subgroups of G which contain K. Moreover, in this correspondence, a normal subgroup of G corresponds to a normal subgroup of $\bar{G}$.

We summarize these few paragraphs in

LEMMA 2.7.5 *Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. For $\bar{H}$ a subgroup of $\bar{G}$ let H be defined by $H = \{x \in G \mid \phi(x) \in \bar{H}\}$. Then H is a subgroup of G and $H \supset K$; if $\bar{H}$ is normal in $\bar{G}$, then H is normal in G. Moreover, this association sets up a one-to-one mapping from the set of all subgroups of $\bar{G}$ onto the set of all subgroups of G which contain K.*

We wish to prove one more general theorem about the relation of two groups which are homomorphic.

THEOREM 2.7.2. *Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K, and let $\bar{N}$ be a normal subgroup of $\bar{G}$, $N = \{x \in G \mid \phi(x) \in \bar{N}\}$. Then $G/N \approx \bar{G}/\bar{N}$. Equivalently, $G/N \approx (G/K)/(N/K)$.*

Proof. As we already know, there is a homomorphism θ of $\bar{G}$ onto $\bar{G}/\bar{N}$ defined by $\theta(\bar{g}) = \bar{N}\bar{g}$. We define the mapping $\psi: G \to \bar{G}/\bar{N}$ by $\psi(g) = \bar{N}\phi(g)$ for all $g \in G$. To begin with, ψ is onto, for if $\bar{g} \in \bar{G}$, $\bar{g} = \phi(g)$ for some $g \in G$, since ϕ is onto, so the typical element $\bar{N}\bar{g}$ in $\bar{G}/\bar{N}$ can be represented as $\bar{N}\phi(g) = \psi(g)$.

If $a, b \in G$, $\psi(ab) = \bar{N}\phi(ab)$ by the definition of the mapping ψ. However, since ϕ is a homomorphism, $\phi(ab) = \phi(a)\phi(b)$. Thus $\psi(ab) = \bar{N}\phi(a)\phi(b) = \bar{N}\phi(a)\bar{N}\phi(b) = \psi(a)\psi(b)$. So far we have shown that ψ is a homomorphism of G onto $\bar{G}/\bar{N}$. What is the kernel, T, of ψ? Firstly, if $n \in N$, $\phi(n) \in \bar{N}$, so that $\psi(n) = \bar{N}\phi(n) = \bar{N}$, the identity element of $\bar{G}/\bar{N}$, proving that $N \subset T$. On the other hand, if $t \in T$, $\psi(t) =$ identity element of $\bar{G}/\bar{N} = \bar{N}$; but $\psi(t) = \bar{N}\phi(t)$. Comparing these two evaluations of $\psi(t)$, we arrive at $\bar{N} = \bar{N}\phi(t)$, which forces $\phi(t) \in \bar{N}$; but this places t in N by definition of N. That is, $T \subset N$. The kernel of ψ has been proved to be equal to N. But then ψ is a homomorphism of G onto $\bar{G}/\bar{N}$ with kernel N. By Theorem 2.7.1 $G/N \approx \bar{G}/\bar{N}$, which is the first part of the theorem. The last statement in the theorem is immediate from the observation (following as a consequence of Theorem 2.7.1) that $\bar{G} \approx G/K$, $\bar{N} \approx N/K$, $\bar{G}/\bar{N} \approx (G/K)/(N/K)$.

Problems

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 $x \in G$.
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.
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.)
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.

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.

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

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 nonzero real numbers under multiplication.

8. Let G be the dihedral group defined as the set of all formal symbols $x^i y^j$, $i = 0, 1$, $j = 0, 1, \ldots, n-1$, 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.

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

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

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

12. If G is abelian and if N is any subgroup of G, prove that $G/\bar{N}$ is abelian.

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

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

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.

#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 $\bar{G}$.

*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.

#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.

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

#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 $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

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.

2.8 Automorphisms

In the preceding section the concept of an isomorphism of one group into another was defined and examined. The special case in which the isomorphism maps a given group into itself should obviously be of some importance. We use the word "into" advisedly, for groups G do exist which have isomorphisms mapping G into, and not onto, itself. The easiest such example is the following: Let G be the group of integers under addition and define $\phi: G \to G$ by $\phi: x \to 2x$ for every $x \in G$. Since $\phi: x + y \to 2(x + y) = 2x + 2y$, ϕ is a homomorphism. Also if the image of x and y under ϕ are equal, then $2x = 2y$ whence $x = y$. ϕ is thus an isomorphism. Yet ϕ is not onto, for the image of any integer under ϕ is an even integer, so, for instance, 1 does not appear an image under ϕ of any element of G. Of greatest interest to us will be the isomorphisms of a group *onto* itself.

DEFINITION By an *automorphism* of a group G we shall mean an isomorphism of G onto itself.

As we mentioned in Chapter 1, whenever we talk about mappings of a set into itself we shall write the mappings on the right side, thus if $T: S \to S$, $x \in S$, then xT is the image of x under T.

Let I be the mapping of G which sends every element onto itself, that is, $xI = x$ for all $x \in G$. Trivially I is an automorphism of G. Let $\mathscr{A}(G)$ denote the set of all automorphisms of G; being a subset of $A(G)$, the set of one-to-one mappings of G onto itself, for elements of $\mathscr{A}(G)$ we can use the product of $A(G)$, namely, composition of mappings. This product then satisfies the associative law in $A(G)$, and so, *a fortiori*, in $\mathscr{A}(G)$. Also I, the unit element of $A(G)$, is in $\mathscr{A}(G)$, so $\mathscr{A}(G)$ is not empty.

An obvious fact that we should try to establish is that $\mathscr{A}(G)$ is a subgroup of $A(G)$, and so, in its own rights, $\mathscr{A}(G)$ should be a group. If T_1, T_2 are in $\mathscr{A}(G)$ we already know that $T_1T_2 \in A(G)$. We want it to be in the smaller set $\mathscr{A}(G)$. We proceed to verify this. For all $x, y \in G$,

$$(xy)T_1 = (xT_1)(yT_1),$$
$$(xy)T_2 = (xT_2)(yT_2),$$

therefore

$$(xy)T_1T_2 = ((xy)T_1)T_2 = ((xT_1)(yT_1))T_2$$
$$= ((xT_1)T_2)((yT_1)T_2) = (xT_1T_2)(yT_1T_2).$$

That is, $T_1T_2 \in \mathscr{A}(G)$. There is only one other fact that needs verifying in order that $\mathscr{A}(G)$ be a subgroup of $A(G)$, namely, that if $T \in \mathscr{A}(G)$, then $T^{-1} \in \mathscr{A}(G)$. If $x, y \in G$, then

$$((xT^{-1})(yT^{-1}))T = ((xT^{-1})T)((yT^{-1})T) = (xI)(yI) = xy,$$

thus

$$(xT^{-1})(yT^{-1}) = (xy)T^{-1},$$

placing T^{-1} in $\mathscr{A}(G)$. Summarizing these remarks, we have proved

LEMMA 2.8.1 *If G is a group, then $\mathscr{A}(G)$, the set of automorphisms of G, is also a group.*

Of course, as yet, we have no way of knowing that $\mathscr{A}(G)$, in general, has elements other than I. If G is a group having only two elements, the reader should convince himself that $\mathscr{A}(G)$ consists only of I. For groups G with more than two elements, $\mathscr{A}(G)$ always has more than one element.

What we should like is a richer sample of automorphisms than the ones we have (namely, I). If the group G is abelian and there is some element $x_0 \in G$ satisfying $x_0 \neq x_0^{-1}$, we can write down an explicit automorphism, the mapping T defined by $xT = x^{-1}$ for all $x \in G$. For any group G, T is onto; for any abelian G, $(xy)T = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = (xT)(yT)$. Also $x_0T = x_0^{-1} \neq x_0$, so $T \neq I$.

However, the class of abelian groups is a little limited, and we should like to have some automorphisms of non-abelian groups. Strangely enough the task of finding automorphisms for such groups is easier than for abelian groups.

Let G be a group; for $g \in G$ define $T_g: G \to G$ by $xT_g = g^{-1}xg$ for all $x \in G$. We claim that T_g is an automorphism of G. First, T_g is onto, for given $y \in G$, let $x = gyg^{-1}$. Then $xT_g = g^{-1}(x)g = g^{-1}(gyg^{-1})g = y$, so T_g is onto. Now consider, for $x, y \in G$, $(xy)T_g = g^{-1}(xy)g = g^{-1}(xgg^{-1}y)g = (g^{-1}xg)(g^{-1}yg) = (xT_g)(yT_g)$. Consequently T_g is a homomorphism of G onto itself. We further assert that T_g is one-to-one, for if $xT_g = yT_g$, then $g^{-1}xg = g^{-1}yg$, so by the cancellation laws in G, $x = y$. T_g is called the *inner automorphism* corresponding to g. If G is non-abelian, there is a pair $a, b \in G$ such that $ab \neq ba$; but then $bT_a = a^{-1}ba \neq b$, so that $T_a \neq I$. Thus for a non-abelian group G there always exist nontrivial automorphisms.

Let $\mathscr{I}(G) = \{T_g \in \mathscr{A}(G) \mid g \in G\}$. The computation of T_{gh}, for $g, h \in G$, might be of some interest. So, suppose $x \in G$; by definition,

$$xT_{gh} = (gh)^{-1}x(gh) = h^{-1}g^{-1}xgh = (g^{-1}xg)T_h = (xT_g)T_h = xT_gT_h.$$

Looking at the start and finish of this chain of equalities we find that $T_{gh} = T_gT_h$. This little remark is both interesting and suggestive. It is of interest because it immediately yields that $\mathscr{I}(G)$ is a subgroup of $\mathscr{A}(G)$. (Verify!) $\mathscr{I}(G)$ is usually called *the group of inner automorphisms of* G. It is suggestive, for if we consider the mapping $\psi: G \to \mathscr{A}(G)$ defined by $\psi(g) = T_g$ for every $g \in G$, then $\psi(gh) = T_{gh} = T_gT_h = \psi(g)\psi(h)$. That is, ψ is a homomorphism of G into $\mathscr{A}(G)$ whose image is $\mathscr{I}(G)$. What is the kernel of ψ? Suppose we call it K, and suppose $g_0 \in K$. Then $\psi(g_0) = I$, or, equivalently, $T_{g_0} = I$. But this says that for any $x \in G$, $xT_{g_0} = x$; however, $xT_{g_0} = g_0^{-1}xg_0$, and so $x = g_0^{-1}xg_0$ for all $x \in G$. Thus $g_0x = g_0g_0^{-1}xg_0 = xg_0$; g_0 must commute with all elements of G. But the center of G, Z, was defined to be precisely all elements in G which commute with every element of G. (See Problem 15, Section 2.5.) Thus $K \subset Z$. However, if $z \in Z$, then $xT_z = z^{-1}xz = z^{-1}(zx)$ (since $zx = xz$) $= x$, whence $T_z = I$ and so $z \in K$. Therefore, $Z \subset K$. Having proved both $K \subset Z$ and $Z \subset K$ we have that $Z = K$. Summarizing, ψ is a homomorphism of G into $\mathscr{A}(G)$ with image $\mathscr{I}(G)$ and kernel Z. By Theorem 2.7.1 $\mathscr{I}(G) \approx G/Z$. In order to emphasize this general result we record it as

LEMMA 2.8.2 *$\mathscr{I}(G) \approx G/Z$, where $\mathscr{I}(G)$ is the group of inner automorphisms of G, and Z is the center of G.*

Suppose that ϕ is an automorphisms of a group G, and suppose that $a \in G$ has order n (that is, $a^n = e$ *but for no lower positive power*). Then $\phi(a)^n = \phi(a^n) = \phi(e) = e$, hence $\phi(a)^n = e$. If $\phi(a)^m = e$ for some $0 < m < n$, then $\phi(a^m) = \phi(a)^m = e$, which implies, since ϕ is one-to-one, that $a^m = e$, a contradiction. Thus

LEMMA 2.8.3 *Let G be a group and ϕ an automorphism of G. If $a \in G$ is of order $o(a) > 0$, then $o(\phi(a)) = o(a)$.*

Automorphisms of groups can be used as a means of constructing new groups from the original group. Before explaining this abstractly, we consider a particular example.

Let G be a cyclic group of order 7, that is, G consists of all a^i, where we assume $a^7 = e$. The mapping $\phi: a^i \to a^{2i}$, as can be checked trivially, is an automorphism of G of order 3, that is, $\phi^3 = I$. Let x be a symbol which we formally subject to the following conditions: $x^3 = e$, $x^{-1}a^i x = \phi(a^i) = a^{2i}$, and consider all formal symbols $x^i a^j$, where $i = 0, 1, 2$ and $j = 0, 1, 2, \ldots, 6$. We declare that $x^i a^j = x^k a^l$ if and only if $i \equiv k \bmod 3$ and $j \equiv l \bmod 7$. We multiply these symbols using the rules $x^3 = a^7 = e$, $x^{-1}ax = a^2$. For instance, $(xa)(xa^2) = x(ax)a^2 = x(xa^2)a^2 = x^2a^4$. The reader can verify that one obtains, in this way, a non-abelian group of order 21.

Generally, if G is a group, T an automorphism of order r of G which is not an inner automorphism, pick a symbol x and consider all elements $x^i g$, $i = 0, \pm 1, \pm 2, \ldots$, $g \in G$ subject to $x^i g = x^{i'} g'$ if and only if $i \equiv i' \bmod r$, $g = g'$ and $x^{-1} g^i x = gT^i$ for all i. This way we obtain a larger group $\{G, T\}$; G is normal in $\{G, T\}$ and $\{G, T\}/G \approx$ group generated by T = cyclic group of order r.

We close the section by determining $\mathscr{A}(G)$ for all cyclic groups.

Example 2.8.1 Let G be a finite cyclic group of order r, $G = (a)$, $a^r = e$. Suppose T is an automorphism of G. If aT is known, since $a^i T = (aT)^i$, $a^i T$ is determined, so gT is determined for all $g \in G = (a)$. Thus we need consider only possible images of a under T. Since $aT \in G$, and since every element in G is a power of a, $aT = a^t$ for some integer $0 < t < r$. However, since T is an automorphism, aT must have the same order as a (Lemma 2.8.3), and this condition, we claim, forces t to be relatively prime to r. For if $d \mid t$, $d \mid r$, then $(aT)^{r/d} = a^{t(r/d)} = a^{r(t/d)} = (a^r)^{t/d} = e$; thus aT has order a divisor of r/d, which, combined with the fact that aT has order r, leads us to $d = 1$. Conversely, for any $0 < s < r$ and relatively prime to r, the mapping $S: a^i \to a^{si}$ is an automorphism of G. Thus $\mathscr{A}(G)$ is in one-to-one correspondence with the group U_r of integers less than r and relatively prime to r under multiplication modulo r. We claim not only is there such a one-to-one correspondence, but there is one which furthermore is an isomorphism. Let us label the elements of $\mathscr{A}(G)$ as T_i where $T_i: a \to a^i$, $0 < i < r$ and relatively prime to r; $T_i T_j: a \to a^i \to (a^i)^j = a^{ij}$, thus $T_i T_j = T_{ij}$. The mapping $i \to T_i$ exhibits the isomorphism of U_r onto $\mathscr{A}(G)$. Here then, $\mathscr{A}(G) \approx U_r$.

Example 2.8.2 G is an infinite cyclic group. That is, G consists of all a^i, $i = 0, \pm 1, \pm 2, \ldots$, where we assume that $a^i = e$ if and only if $i = 0$. Suppose that T is an automorphism of G. As in Example 2.8.1, $aT = a^t$.

The question now becomes, What values of t are possible? Since T is an automorphism of G, it maps G onto itself, so that $a = gT$ for some $g \in G$. Thus $a = a^iT = (aT)^i$ for some integer i. Since $aT = a^t$, we must have that $a = a^{ti}$, so that $a^{ti-1} = e$. Hence $ti - 1 = 0$; that is, $ti = 1$. Clearly, since t and i are integers, this must force $t = \pm 1$, and each of these gives rise to an automorphism, $t = 1$ yielding the identity automorphism I, $t = -1$ giving rise to the automorphism $T: g \to g^{-1}$ for every g in the cyclic group G. Thus here, $\mathscr{A}(G) \approx$ cyclic group of order 2.

Problems

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, $T: x \to x^{-1}$.
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.
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.
4. For $G = S_3$ prove that $G \approx \mathscr{I}(G)$.
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).
6. Let G be a group of order 4, $G = \{e, a, b, ab\}$, $a^2 = b^2 = e$, $ab = ba$. Determine $\mathscr{A}(G)$.
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.
8. For any group G, prove that the commutator subgroup G' is a characteristic subgroup of G. (See Problem 5, Section 2.7).
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.
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 $x \in G$.
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.

*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.

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?

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

*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.

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

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

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 $N(aT) = (N(a))T$.

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.

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.

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.

2.9 Cayley's Theorem

When groups first arose in mathematics they usually came from some specific source and in some very concrete form. Very often it was in the form of a set of transformations of some particular mathematical object. In fact, most finite groups appeared as groups of permutations, that is, as subgroups of S_n. ($S_n = A(S)$ when S is a finite set with n elements.) The English mathematician Cayley first noted that every group could be realized as a subgroup of $A(S)$ for some S. Our concern, in this section, will be with a presentation of Cayley's theorem and some related results.

THEOREM 2.9.1 (CAYLEY) *Every group is isomorphic to a subgroup of $A(S)$ for some appropriate S.*

Proof. Let G be a group. For the set S we will use the elements of G; that is, put $S = G$. If $g \in G$, define $\tau_g : S(= G) \to S(= G)$ by $x\tau_g = xg$

for every $x \in G$. If $y \in G$, then $y = (yg^{-1})g = (yg^{-1})\tau_g$, so that τ_g maps S onto itself. Moreover, τ_g is one-to-one, for if $x, y \in S$ and $x\tau_g = y\tau_g$, then $xg = yg$, which, by the cancellation property of groups, implies that $x = y$. We have proved that for every $g \in G$, $\tau_g \in A(S)$.

If $g, h \in G$, consider τ_{gh}. For any $x \in S = G$, $x\tau_{gh} = x(gh) = (xg)h = (x\tau_g)\tau_h = x\tau_g\tau_h$. Note that we used the associative law in a very essential way here. From $x\tau_{gh} = x\tau_g\tau_h$ we deduce that $\tau_{gh} = \tau_g\tau_h$. Therefore, if $\psi: G \to A(S)$ is defined by $\psi(g) = \tau_g$, the relation $\tau_{gh} = \tau_g\tau_h$ tells us that ψ is a homomorphism. What is the kernel K of ψ? If $g_0 \in K$, then $\psi(g_0) = \tau_{g_0}$ is the identity map on S, so that for $x \in G$, and, in particular, for $e \in G$, $e\tau_{g_0} = e$. But $e\tau_{g_0} = eg_0 = g_0$. Thus comparing these two expressions for $e\tau_{g_0}$ we conclude that $g_0 = e$, whence $K = (e)$. Thus by the corollary to Lemma 2.7.4 ψ is an isomorphism of G into $A(S)$, proving the theorem.

The theorem enables us to exhibit any abstract group as a more concrete object, namely, as a group of mappings. However, it has its shortcomings; for if G is a finite group of order $o(G)$, then, using $S = G$, as in our proof, $A(S)$ has $o(G)!$ elements. Our group G of order $o(G)$ is somewhat lost in the group $A(S)$ which, with its $o(G)!$ elements, is huge in comparison to G. We ask: Can we find a more economical S, one for which $A(S)$ is smaller? This we now attempt to accomplish.

Let G be a group, H a subgroup of G. Let S be the set whose elements are the right cosets of H in G. That is, $S = \{Hg \mid g \in G\}$. S need not be a group itself, in fact, it would be a group only if H were a normal subgroup of G. However, we can make our group G act on S in the following natural way: for $g \in G$ let $t_g: S \to S$ be defined by $(Hx)t_g = Hxg$. Emulating the proof of Theorem 2.9.1 we can easily prove

1. $t_g \in A(S)$ for every $g \in G$.
2. $t_{gh} = t_g t_h$.

Thus the mapping $\theta: G \to A(S)$ defined by $\theta(g) = t_g$ is a homomorphism of G into $A(S)$. Can one always say that θ is an isomorphism? Suppose that K is the kernel of θ. If $g_0 \in K$, then $\theta(g_0) = t_{g_0}$ is the identity map on S, so that for every $X \in S$, $Xt_{g_0} = X$. Since every element of S is a right coset of H in G, we must have that $Hat_{g_0} = Ha$ for every $a \in G$, and using the definition of t_{g_0}, namely, $Hat_{g_0} = Hag_0$, we arrive at the identity $Hag_0 = Ha$ for every $a \in G$. On the other hand, if $b \in G$ is such that $Hxb = Hx$ for every $x \in G$, retracing our argument we could show that $b \in K$. Thus $K = \{b \in G \mid Hxb = Hx \text{ all } x \in G\}$. We claim that from this characterization of K, K must be the largest normal subgroup of G which is contained in H. We first explain the use of the word largest; by this we mean that if N is a normal subgroup of G which is contained in H, then N must be contained in K. We wish to show this is the case. That K is a normal subgroup

of G follows from the fact that it is the kernel of a homomorphism of G. Now we assert that $K \subset H$, for if $b \in K$, $Hab = Ha$ for every $a \in G$, so, in particular, $Hb = Heb = He = H$, whence $b \in H$. Finally, if N is a normal subgroup of G which is contained in H, if $n \in N$, $a \in G$, then $ana^{-1} \in N \subset H$, so that $Hana^{-1} = H$; thus $Han = Ha$ for all $a \in G$. Therefore, $n \in K$ by our characterization of K.

We have proved

THEOREM 2.9.2 *If G is a group, H a subgroup of G, and S is the set of all right cosets of H in G, then there is a homomorphism θ of G into $A(S)$ and the kernel of θ is the largest normal subgroup of G which is contained in H.*

The case $H = (e)$ just yields Cayley's theorem (Theorem 2.9.1). If H should happen to have no normal subgroup of G other than (e) in it, then θ must be an isomorphism of G into $A(S)$. In this case we would have cut down the size of the S used in proving Theorem 2.9.1. This is interesting mostly for finite groups. For we shall use this observation both as a means of proving certain finite groups have nontrivial normal subgroups, and also as a means of representing certain finite groups as permutation groups on small sets.

We examine these remarks a little more closely. Suppose that G has a subgroup H whose index $i(H)$ (that is, the number of right cosets of H in G) satisfies $i(H)! < o(G)$. Let S be the set of all right cosets of H in G. The mapping, θ, of Theorem 2.9.2 cannot be an isomorphism, for if it were, $\theta(G)$ would have $o(G)$ elements and yet would be a subgroup of $A(S)$ which has $i(H)! < o(G)$ elements. Therefore the kernel of θ must be larger than (e); this kernel being the largest normal subgroup of G which is contained in H, we can conclude that H contains a nontrivial normal subgroup of G.

However, the argument used above has implications even when $i(H)!$ is not less than $o(G)$. If $o(G)$ does not divide $i(H)!$ then by invoking Lagrange's theorem we know that $A(S)$ can have no subgroup of order $o(G)$, hence no subgroup isomorphic to G. However, $A(S)$ does contain $\theta(G)$, whence $\theta(G)$ cannot be isomorphic to G; that is, θ cannot be an isomorphism. But then, as above, H must contain a nontrivial normal subgroup of G.

We summarize this as

LEMMA 2.9.1 *If G is a finite group, and $H \neq G$ is a subgroup of G such that $o(G) \nmid i(H)!$ then H must contain a nontrivial normal subgroup of G. In particular, G cannot be simple.*

APPLICATIONS

1. Let G be a group of order 36. Suppose that G has a subgroup H of order 9 (we shall see later that this is always the case). Then $i(H) = 4$,

$4! = 24 < 36 = o(G)$ so that in H there must be a normal subgroup $N \neq (e)$, of G, of order a divisor of 9, that is, of order 3 or 9.

2. Let G be a group of order 99 and suppose that H is a subgroup of G of order 11 (we shall also see, later, that this must be true). Then $i(H) = 9$, and since $99 \nmid 9!$ there is a nontrivial normal subgroup $N \neq (e)$ of G in H. Since H is of order 11, which is a prime, its only subgroup other than (e) is itself, implying that $N = H$. That is, H itself is a normal subgroup of G.

3. Let G be a non-abelian group of order 6. By Problem 11, Section 2.3, there is an $a \neq e \in G$ satisfying $a^2 = e$. Thus the subgroup $H = \{e, a\}$ is of order 2, and $i(H) = 3$. Suppose, for the moment, that we know that H is not normal in G. Since H has only itself and (e) as subgroups, H has no nontrivial normal subgroups of G in it. Thus G is isomorphic to a subgroup T of order 6 in $A(S)$, where S is the set of right cosets of H in G. Since $o(A(S)) = i(H)! = 3! = 6$, $T = S$. In other words, $G \approx A(S) = S_3$. We would have proved that any non-abelian group of order 6 is isomorphic to S_3. All that remains is to show that H is not normal in G. Since it might be of some interest we go through a detailed proof of this. If $H = \{e, a\}$ were normal in G, then for every $g \in G$, since $gag^{-1} \in H$ and $gag^{-1} \neq e$, we would have that $gag^{-1} = a$, or, equivalently, that $ga = ag$ for every $g \in G$. Let $b \in G$, $b \notin H$, and consider $N(b) = \{x \in G \mid xb = bx\}$. By an earlier problem, $N(b)$ is a subgroup of G, and $N(b) \supset H$; $N(b) \neq H$ since $b \in N(b)$, $b \notin H$. Since H is a subgroup of $N(b)$, $o(H) \mid o(N(b)) \mid 6$. The only even number n, $2 < n \leq 6$ which divides 6 is 6. So $o(N(b)) = 6$; whence b commutes with all elements of G. Thus every element of G commutes with every other element of G, making G into an abelian group, contrary to assumption. Thus H could not have been normal in G. This proof is somewhat long-winded, but it illustrates some of the ideas already developed.

Problems

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 $\lambda_{gh} = \lambda_h\lambda_g$.
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 $x(\tau_h\lambda_g)$.)
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 $h \in G$.
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.

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.

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

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

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.

*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.

2.10 Permutation Groups

We have seen that every group can be represented isomorphically as a subgroup of $A(S)$ for some set S, and, in particular, a finite group G can be represented as a subgroup of S_n, for some n, where S_n is the symmetric group of degree n. This clearly shows that the groups S_n themselves merit closer examination.

Suppose that S is a finite set having n elements $x_1, x_2, \ldots, x_n$. If $\phi \in A(S) = S_n$, then ϕ is a one-to-one mapping of S onto itself, and we could write ϕ out by showing what it does to every element, e.g., $\phi: x_1 \to x_2$, $x_2 \to x_4$, $x_4 \to x_3$, $x_3 \to x_1$. But this is very cumbersome. One short cut might be to write ϕ out as

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_{i_1} & x_{i_2} & x_{i_3} & \cdots & x_{i_n} \end{pmatrix},$$

where x_{i_k} is the image of x_i under ϕ. Returning to our example just above, ϕ might be represented by

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_4 & x_1 & x_3 \end{pmatrix}.$$

While this notation is a little handier there still is waste in it, for there seems to be no purpose served by the symbol x. We could equally well represent the permutation as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

Our specific example would read

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

Given two permutations θ, ψ in S_n, using this symbolic representation of θ and ψ, what would the representation of $\theta\psi$ be? To compute it we could start and see what $\theta\psi$ does to x_1 (henceforth written as 1). θ takes 1 into i_1, while ψ takes i_1 into k, say, then $\theta\psi$ takes 1 into k. Then repeat this procedure for 2, 3, . . . , n. For instance, if θ is the permutation represented by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

and ψ by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix},$$

then $i_1 = 3$ and ψ takes 3 into 2, so $k = 2$ and $\theta\psi$ takes 1 into 2. Similarly $\theta\psi$:2 $\to$ 1, 3 $\to$ 3, 4 $\to$ 4. That is, the representation for $\theta\psi$ is

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

If we write

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

and

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix},$$

then

$$\theta\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

This is the way we shall multiply the symbols of the form

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}.$$

Let S be a set and $\theta \in A(S)$. Given two elements $a, b \in S$ we define $a \equiv {}_\theta b$ if and only if $b = a\theta^i$ for some integer i (i can be positive, negative, or 0). We claim this defines an equivalence relation on S. For

1. $a \equiv {}_\theta a$ since $a = a\theta^0 = ae$.
2. If $a \equiv {}_\theta b$, then $b = a\theta^i$, so that $a = b\theta^{-i}$, whence $b \equiv {}_\theta a$.
3. If $a \equiv {}_\theta b$, $b \equiv {}_\theta c$, then $b = a\theta^i$, $c = b\theta^j = (a\theta^i)\theta^j = a\theta^{i+j}$, which implies that $a \equiv {}_\theta c$.

This equivalence relation by Theorem 1.1.1 induces a decomposition of S into disjoint subsets, namely, the equivalence classes. We call the equivalence class of an element $s \in S$ the *orbit* of s under θ; thus the orbit of s under θ consists of all the elements $s\theta^i$, $i = 0, \pm 1, \pm 2, \ldots$.

In particular, if S is a finite set and $s \in S$, there is a smallest positive integer $l = l(s)$ depending on s such that $s\theta^l = s$. The orbit of s under θ then consists of the elements $s, s\theta, s\theta^2, \ldots, s\theta^{l-1}$. By a *cycle* of θ we mean the *ordered* set $(s, s\theta, s\theta^2, \ldots, s\theta^{l-1})$. If we know all the cycles of θ we clearly know θ since we would know the image of any element under θ. Before proceeding we illustrate these ideas with an example. Let

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix},$$

where S consists of the elements $1, 2, \ldots, 6$ (remember 1 stands for x_1, 2 for x_2, etc.). Starting with 1, then the orbit of 1 consists of $1 = 1\theta^0$, $1\theta^1 = 2$, $1\theta^2 = 2\theta = 1$, so the orbit of 1 is the set of elements 1 and 2. This tells us the orbit of 2 is the same set. The orbit of 3 consists just of 3; that of 4 consists of the elements 4, $4\theta = 5$, $4\theta^2 = 5\theta = 6$, $4\theta^3 = 6\theta = 4$. The cycles of θ are (1, 2), (3), (4, 5, 6).

We digress for a moment, leaving our particular θ. Suppose that by the cycle $(i_1, i_2, \ldots, i_r)$ we mean the permutation ψ which sends i_1 into i_2, i_2 into $i_3 \cdots i_{r-1}$ into i_r and i_r into i_1, and leaves all other elements of S fixed. Thus, for instance, if S consists of the elements $1, 2, \ldots, 9$, then the symbol (1, 3, 4, 2, 6) means the permutation

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

We multiply cycles by multiplying the permutations they represent. Thus again, if S has 9 elements,

$$(1\ 2\ 3)(5\ 6\ 4\ 1\ 8)$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 3 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$$

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

Let us return to the ideas of the paragraph preceding the last one, and ask: Given the permutation

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix},$$

what are the cycles of θ? We first find the orbit of 1; namely, $1, 1\theta = 2$, $1\theta^2 = 2\theta = 3$, $1\theta^3 = 3\theta = 8$, $1\theta^4 = 8\theta = 5$, $1\theta^5 = 5\theta = 6$, $1\theta^6 = 6\theta = 4$, $1\theta^7 = 4\theta = 1$. That is, the orbit of 1 is the set $\{1, 2, 3, 8, 5, 6, 4\}$. The orbits of 7 and 9 can be found to be $\{7\}$, $\{9\}$, respectively. The cycles of θ thus are (7), (9), $(1, 1\theta, 1\theta^2, \ldots, 1\theta^6) = (1, 2, 3, 8, 5, 6, 4)$. The reader should now verify that if he takes the product (as defined in the last paragraph) of (1, 2, 3, 8, 5, 6, 4), (7), (9) he will obtain θ. That is, at least in this case, θ is the product of its cycles.

But this is no accident for it is now trivial to prove

LEMMA 2.10.1 *Every permutation is the product of its cycles.*

Proof. Let θ be the permutation. Then its cycles are of the form $(s, s\theta, \ldots, s\theta^{l-1})$. By the multiplication of cycles, as defined above, and since the cycles of θ are disjoint, the image of $s' \in S$ under θ, which is $s'\theta$, is the same as the image of s' under the product, ψ, of all the distinct cycles of θ. So θ, ψ have the same effect on every element of S, hence $\theta = \psi$, which is what we sought to prove.

If the remarks above are still not transparent at this point, the reader should take a given permutation, find its cycles, take their product, and verify the lemma. In doing so the lemma itself will become obvious.

Lemma 2.10.1 is usually stated in the form *every permutation can be uniquely expressed as a product of disjoint cycles.*

Consider the m-cycle $(1, 2, \ldots, m)$. A simple computation shows that $(1, 2, \ldots, m) = (1, 2)(1, 3)\cdots(1, m)$. More generally the m-cycle $(a_1, a_2, \ldots, a_m) = (a_1, a_2)(a_1, a_3)\cdots(a_1, a_m)$. This decomposition is not unique; by this we mean that an m-cycle can be written as a product of 2-cycles in more than one way. For instance, $(1, 2, 3) = (1, 2)(1, 3) = (3, 1)(3, 2)$. Now, since every permutation is a product of disjoint cycles and every cycle is a product of 2-cycles, we have proved

LEMMA 2.10.2 *Every permutation is a product of 2-cycles.*

We shall refer to 2-cycles as *transpositions.*

DEFINITION A permutation $\theta \in S_n$ is said to be an *even permutation* if it can be represented as a product of an even number of transpositions.

The definition given just insists that θ have one representation as a product of an even number of transpositions. Perhaps it has other representations as a product of an odd number of transpositions. We first want to show that this cannot happen. Frankly, we are not happy with the proof we give of this fact for it introduces a polynomial which seems extraneous to the matter at hand.

Consider the polynomial in n-variables

$$p(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j).$$

If $\theta \in S_n$ let θ act on the polynomial $p(x_1, \ldots, x_n)$ by

$$\theta{:}p(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j) \to \prod_{i<j} (x_{\theta(i)} - x_{\theta(j)}).$$

It is clear that $\theta{:}p(x_1, \ldots, x_n) \to \pm p(x_1, \ldots, x_n)$. For instance, in S_5, $\theta = (134)(25)$ takes

$$p(x_1, \ldots, x_5) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3) \times (x_2 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)$$

into

$$(x_3 - x_5)(x_3 - x_4)(x_3 - x_1)(x_3 - x_2)(x_5 - x_4)(x_5 - x_1) \times (x_5 - x_2)(x_4 - x_1)(x_4 - x_2)(x_1 - x_2),$$

which can easily be verified to be $-p(x_1, \ldots, x_5)$.

If, in particular, θ is a transposition, $\theta{:}p(x_1, \ldots, x_n) \to -p(x_1, \ldots, x_n)$. (Verify!) Thus if a permutation Π can be represented as a product of an even number of transpositions in one representation, Π must leave $p(x_1, \ldots, x_n)$ fixed, so that any representation of Π as a product of transposition must be such that it leaves $p(x_1, \ldots, x_n)$ fixed; that is, in any representation it is a product of an even number of transpositions. This establishes that the definition given for an even permutation is a significant one. We call a permutation *odd* if it is not an even permutation.

The following facts are now clear:

1. The product of two even permutations is an even permutation.
2. The product of an even permutation and an odd one is odd (likewise for the product of an odd and even permutation).
3. The product of two odd permutations is an even permutation.

The rule for combining even and odd permutations is like that of combining even and odd numbers under addition. This is not a coincidence since this latter rule is used in establishing 1, 2, and 3.

Let A_n be the subset of S_n consisting of all even permutations. Since the product of two even permutations is even, A_n must be a subgroup of S_n. We claim it is normal in S_n. Perhaps the best way of seeing this is as follows:

let W be the group of real numbers 1 and -1 under multiplication. Define $\psi: S_n \to W$ by $\psi(s) = 1$ if s is an even permutation, $\psi(s) = -1$ if s is an odd permutation. By the rules 1, 2, 3 above ψ is a homomorphism onto W. The kernel of ψ is precisely A_n; being the kernel of a homomorphism A_n is a normal subgroup of S_n. By Theorem 2.7.1 $S_n/A_n \approx W$, so, since

$$2 = o(W) = o\left(\frac{S_n}{A_n}\right) = \frac{o(S_n)}{o(A_n)},$$

we see that $o(A_n) = \frac{1}{2}n!$. A_n is called the *alternating group* of degree n. We summarize our remarks in

LEMMA 2.10.3 *S_n has as a normal subgroup of index 2 the alternating group, A_n, consisting of all even permutations.*

At the end of the next section we shall return to S_n again.

Problems

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) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$.
2. Write the permutations in Problem 1 as the product of disjoint cycles.
3. Express as the product of disjoint cycles:
   (a) $(1, 2, 3)(4, 5)(1, 6, 7, 8, 9)(1, 5)$.
   (b) $(1, 2)(1, 2, 3)(1, 2)$.
4. Prove that $(1, 2, \ldots, n)^{-1} = (n, n-1, n-2, \ldots, 2, 1)$.
5. Find the cycle structure of all the powers of $(1, 2, \ldots, 8)$.
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?
7. Compute $a^{-1}ba$, where
   (1) $a = (1, 3, 5)(1, 2)$, $b = (1, 5, 7, 9)$.
   (2) $a = (5, 7, 9)$, $b = (1, 2, 3)$.
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 $a^{-1}(1, 2)a = (3, 4)(1, 5)$.
9. Determine for what m 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) $(1, 2)(1, 3)(1, 4)(2, 5)$.

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.)

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

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

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

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

16. Find all the normal subgroups in S_4.

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

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.

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.

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.)

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.)

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

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 $g \in G$.)

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: ALGEBRA **Subject Code: 19MMP101**
Class : I - M.Sc. Mathematics **Semester : I**

Unit I

Part A (20x1=20 Marks)
(Question Nos. 1 to 20 Online Examinations)
Possible Questions

SL.NO	Questions	Opt1	Opt2	Opt3	Opt4	Answer
1	If G is a group, then every a∈G has a -------- inverse in G	zero	two	unique	three	unique
2	For all a,b∈G $(a.b)^{-1}$ = ------	ab	$b.a^{-1}$	$(a.b)^{-1}$	$b^{-1}.a^{-1}$	$b^{-1}.a^{-1}$
3	The number of elements in a finite group is called ---------- of the group	order	Non-abelian	infinite	abeliean	order
4	If G is a group, then the identity element of G is ---------	zero	two	unique	three	unique
5	A nonempty subset H of a group G is said to be ---------- of G H itself forms a group	coset	subset	normal-subgroup	subgroup	subgroup
6	If G is a finite group and H is a subgroup of G then -------- divisor of o(G)	o(G)	o(S)	o(H)	o(A)	o(H)
7	If H is a subgroup of G,a∈G then aH is called----------	coset	left- coset	right- coset	ideal	left- coset
8	If H is a subgroup of G,a∈G then Ha is called----------	coset	left- coset	right- coset	ideal	right- coset
9	If G is a finite group and H is a subgroup of G then -------- divisor of o(G)	o(G)	o(S)	o(H)	o(A)	o(H)
10	An isomorphic mapping Φ of a group G onto itself is called automorphism If Φ is _____	one-to-one	onto	into	one to one & onto	onto
11	An isomorphic mapping of a group G onto itself is called ----------	automorphism	isomorphism	homomorphism	monomorphism	automorphism
12	A homomorphism F from G into Ğ is said to be --------- ifF is one-to-one	automorphism	isomorphism	homomorphism	monomorphism	isomorphism
13	A homomorphism Φ from G into Ğ is said to be isomorphism if Φ is	one-to-one	onto	into	one to one & onto	one-to-one
14	If G is a group, N normal subgroup of G then G/N is called -------	quotient group	ring	subgroup	c)normal-subgroup	quotient group
15	A subgroup N of a group G is said to be normal subgroup of G H if--------	gng^{-1}∈G	gng^{-1}∈N	gn∈N	ng^{-1}∈N	gng^{-1}∈N
16	A subgroup N of a group G is said to be ---------- --- of G H if gng^{-1}∈N	coset	subset	normal-subgroup	subgroup	normal-subgroup
17	If G is a finite group and a∈G the --------- of 'a' is least positive integer m such that $a^m = e$	coset	subset	order	infinite order	order
18	If G is a finite group and a∈G the order of a is least positive integer m such that a^m=-----	1	e	0	p	e
19	N(a) is a ---------- of G	coset	subset	normal-subgroup	subgroup	normal-subgroup
20	Conjugacy is ---------- on G	reflexive	symmetric	transitive	equivalence relation	equivalence relation
21	If o(G) =p^2 where p is a prime number, then G is --------	Non-abelian	abeliean	unity	inverse	abeliean
22	If p is a prime number, and p/o(G) then G has an element of --------	order 1	order p	order e	order 0	order p
23	If p is a prime number, and p^{α}/o(G) then G has a subgroup of --------	order p^{α}	order p	order 0	order e	order p^{α}
24	Let Φ be a homomorphism of G onto G with kernal K. Then ----------	G\K ~G	G\K =G	G\K =1	G\K =K	G\K ~G

25	By an automorphism of a group G we shall mean an ---------- of G onto itself	automorphism	isomorphism	homomorphism	monomorphism	isomorphism
26	The sub group N of G is a normal sub group of G if and only if every--------- of N in G is a right coset of N in G	coset	left- coset	right- coset	ideal	left- coset
27	The sub group N of G is a normal sub group of G if and only if every left coset of N in G is a ---- - of N in G	coset	left- coset	right- coset	ideal	right- coset
28	If N and M are sub groups of G then ------ is also a normal sub group	MN	NM	N/M	M/N	N/M
29	The center of a group is always a normal sub group	normal-subgroup	subgroup	group	Abelian group	normal-subgroup
30	If G is a group then A(G) the set of automorphism of G is a ----------	normal-subgroup	subgroup	group	Abelian group	group
31	Every group is ----------to a sub group of A(S) for some appropriate S	automorphism	isomorphism	homomorphism	monomorphism	isomorphism
32	Every permutation is the product of its ------	cycles	2-cycles	group	subgroup	cycles
33	Every permutation is the --------- of its cycles	sum	division	product	difference	product
34	Every ---------- is the product of its cycles	normal-subgroup	subgroup	group	permutation	permutation
35	The number of group homomorphism from Z_m to Z_n is ---------	m	n	lcm(m,n)	gcd(m,n)	gcd(m,n)
36	The number of generators of a finite cyclic group of order n is ----------	n	n^2	phi(n)	0	phi(n)
37	Order of a quotient group G\K is-------	O(G)	O(K)	O(GK)	O(G)/(O(K)	O(G)/O(K)
38	Any subgroup of index 2 is always ------	normal-subgroup	abeliean	cyclic	identity	normal-subgroup
39	Order of an element divides order of --------	subgroup	identity	group	inverse	group
40	Order of permutation is -------- of lenths of disjoint cycles	gcd	lcm	sum	multiplication	lcm

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

CLASS: I M.Sc. MATHEMATICS **COURSENAME: ALGEBRA**

COURSE CODE: 19MMP101 **BATCH-2019-2021**

UNIT-2

ANOTHER COUNTING PRINCPLE

Another counting principle - Sylow's theorems - Direct product - Finite abelian groups.

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 $a, b \in S_3$.
25. Find the second permutation representation of the group G defined in Problem 21.
26. Find the second permutation representation of the dihedral group of order $2n$.

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

2.11 Another Counting Principle

Mathematics is rich in technique and arguments. In this great variety one of the most basic tools is counting. Yet, strangely enough, it is one of the most difficult. Of course, by counting we do not mean the creation of tables of logarithms or addition tables; rather, we mean the process of precisely accounting for all possibilities in highly complex situations. This can sometimes be done by a brute force case-by-case exhaustion, but such a routine is invariably dull and violates a mathematician's sense of aesthetics. One prefers the light, deft, delicate touch to the hammer blow. But the most serious objection to case-by-case division is that it works far too rarely. Thus in various phases of mathematics we find neat counting devices which tell us exactly how many elements, in some fairly broad context, satisfy certain conditions. A great favorite with mathematicians is the process of counting up a given situation in two different ways; the comparison of the

two counts is then used as a means of drawing conclusions. Generally speaking, one introduces an equivalence relation on a finite set, measures the size of the equivalence classes under this relation, and then equates the number of elements in the set to the sum of the orders of these equivalence classes. This kind of an approach will be illustrated in this section. We shall introduce a relation, prove it is an equivalence relation, and then find a neat algebraic description for the size of each equivalence class. From this simple description there will flow a stream of beautiful and powerful results about finite groups.

DEFINITION If $a, b \in G$, then b is said to be a *conjugate* of a in G if there exists an element $c \in G$ such that $b = c^{-1}ac$.

We shall write, for this, $a \sim b$ and shall refer to this relation as *conjugacy*.

LEMMA 2.11.1 *Conjugacy is an equivalence relation on G.*

Proof. As usual, in order to establish this, we must prove that

1. $a \sim a$;
2. $a \sim b$ implies that $b \sim a$;
3. $a \sim b$, $b \sim c$ implies that $a \sim c$

for all a, b, c in G.

We prove each of these in turn.

1. Since $a = e^{-1}ae$, $a \sim a$, with $c = e$ serving as the c in the definition of conjugacy.
2. If $a \sim b$, then $b = x^{-1}ax$ for some $x \in G$, hence, $a = (x^{-1})^{-1}b(x^{-1})$, and since $y = x^{-1} \in G$ and $a = y^{-1}by$, $b \sim a$ follows.
3. Suppose that $a \sim b$ and $b \sim c$ where $a, b, c \in G$. Then $b = x^{-1}ax$, $c = y^{-1}by$ for some $x, y \in G$. Substituting for b in the expression for c we obtain $c = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$; since $xy \in G$, $a \sim c$ is a consequence.

For $a \in G$ let $C(a) = \{x \in G \mid a \sim x\}$. $C(a)$, the equivalence class of a in G under our relation, is usually called the *conjugate class* of a in G; it consists of the set of all distinct elements of the form $y^{-1}ay$ as y ranges over G.

Our attention now narrows to the case in which G is a finite group. Suppose that $C(a)$ has c_a elements. We seek an alternative description of c_a. Before doing so, note that $o(G) = \sum c_a$ where the sum runs over a set of $a \in G$ using one a from each conjugate class. This remark is, of course, merely a restatement of the fact that our equivalence relation—conjugacy—

induces a decomposition of G into disjoint equivalence classes—the conjugate classes. Of paramount interest now is an evaluation of c_a.

In order to carry this out we recall a concept introduced in Problem 13, Section 2.5. Since this concept is important—far too important to leave to the off-chance that the student solved the particular problem—we go over what may very well be familiar ground to many of the readers.

DEFINITION If $a \in G$, then $N(a)$, the *normalizer of a in G*, is the set $N(a) = \{x \in G \mid xa = ax\}$.

$N(a)$ consists of precisely those elements in G which commute with a.

LEMMA 2.11.2 *$N(a)$ is a subgroup of G.*

Proof. In this result the order of G, whether it be finite or infinite, is of no relevance, and so we put no restrictions on the order of G.

Suppose that $x, y \in N(a)$. Thus $xa = ax$ and $ya = ay$. Therefore, $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, in consequence of which $xy \in N(a)$. From $ax = xa$ it follows that $x^{-1}a = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = ax^{-1}$, so that x^{-1} is also in $N(a)$. But then $N(a)$ has been demonstrated to be a subgroup of G.

We are now in a position to enunciate our counting principle.

THEOREM 2.11.1 *If G is a finite group, then $c_a = o(G)/o(N(a))$; in other words, the number of elements conjugate to a in G is the index of the normalizer of a in G.*

Proof. To begin with, the conjugate class of a in G, $C(a)$, consists exactly of all the elements $x^{-1}ax$ as x ranges over G. c_a measures the number of distinct $x^{-1}ax$'s. Our method of proof will be to show that two elements in the same right coset of $N(a)$ in G yield the same conjugate of a whereas two elements in different right cosets of $N(a)$ in G give rise to different conjugates of a. In this way we shall have a one-to-one correspondence between conjugates of a and right cosets of $N(a)$.

Suppose that $x, y \in G$ are in the same right coset of $N(a)$ in G. Thus $y = nx$, where $n \in N(a)$, and so $na = an$. Therefore, since $y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$, $y^{-1}ay = x^{-1}n^{-1}anx = x^{-1}n^{-1}nax = x^{-1}ax$, whence x and y result in the same conjugate of a.

If, on the other hand, x and y are in different right cosets of $N(a)$ in G we claim that $x^{-1}ax \neq y^{-1}ay$. Were this not the case, from $x^{-1}ax = y^{-1}ay$ we would deduce that $yx^{-1}a = ayx^{-1}$; this in turn would imply that $yx^{-1} \in N(a)$. However, this declares x and y to be in the same right coset of $N(a)$ in G, contradicting the fact that they are in different cosets. The proof is now complete.

COROLLARY

$$o(G) = \sum \frac{o(G)}{o(N(a))}$$

where this sum runs over one element a in each conjugate class.

Proof. Since $o(G) = \sum c_a$, using the theorem the corollary becomes immediate.

The equation in this corollary is usually referred to as the *class equation* of G.

Before going on to the applications of these results let us examine these concepts in some specific group. There is no point in looking at abelian groups because there two elements are conjugate if and only if they are equal (that is, $c_a = 1$ for every a). So we turn to our familiar friend, the group S_3. Its elements are e, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2). We enumerate the conjugate classes:

$$C(e) = \{e\}$$

$$\begin{aligned} C(1,2) &= \{(1,2), (1,3)^{-1}(1,2)(1,3), (2,3)^{-1}(1,2)(2,3), \\ &\qquad (1,2,3)^{-1}(1,2)(1,2,3), (1,3,2)^{-1}(1,2)(1,3,2)\} \\ &= \{(1,2), (1,3), (2,3)\} \quad \text{(Verify!)} \end{aligned}$$

$$C(1,2,3) = \{(1,2,3), (1,3,2)\} \quad \text{(after another verification)}.$$

The student should verify that $N((1, 2)) = \{e, (1, 2)\}$ and $N((1, 2, 3)) = \{e, (1, 2, 3), (1, 3, 2)\}$, so that $c_{(1,2)} = \frac{6}{2} = 3$, $c_{(1,2,3)} = \frac{6}{3} = 2$.

Applications of Theorem 2.11.1

Theorem 2.11.1 lends itself to immediate and powerful application. We need no artificial constructs to illustrate its use, for the results below which reveal the strength of the theorem are themselves theorems of stature and importance.

Let us recall that the center $Z(G)$ of a group G is the set of all $a \in G$ such that $ax = xa$ for all $x \in G$. Note the

SUBLEMMA *$a \in Z$ if and only if $N(a) = G$. If G is finite, $a \in Z$ if and only if $o(N(a)) = o(G)$.*

Proof. If $a \in Z$, $xa = ax$ for all $x \in G$, whence $N(a) = G$. If, conversely, $N(a) = G$, $xa = ax$ for all $x \in G$, so that $a \in Z$. If G is finite, $o(N(a)) = o(G)$ is equivalent to $N(a) = G$.

APPLICATION 1

THEOREM 2.11.2 *If $o(G) = p^n$ where p is a prime number, then $Z(G) \neq (e)$.*

Proof. If $a \in G$, since $N(a)$ is a subgroup of G, $o(N(a))$, being a divisor of $o(G) = p^n$, must be of the form $o(N(a)) = p^{n_a}$; $a \in Z(G)$ if and only if $n_a = n$. Write out the class equation for this G, letting $z = o(Z(G))$. We get $p^n = o(G) = \sum(p^n/p^{n_a})$; however, since there are exactly z elements such that $n_a = n$, we find that

$$p^n = z + \sum_{n_a < n} \frac{p^n}{p^{n_a}}.$$

Now look at this! p is a divisor of the left-hand side; since $n_a < n$ for each term in the $\sum$ of the right side,

$$p \left| \frac{p^n}{p^{n_a}} = p^{n-n_a} \right.$$

so that p is a divisor of each term of this sum, hence a divisor of this sum. Therefore,

$$p \left| \left(p^n - \sum_{n_a < n} \frac{p^n}{p^{n_a}} \right) = z. \right.$$

Since $e \in Z(G)$, $z \neq 0$; thus z is a positive integer divisible by the prime p. Therefore, $z > 1$! But then there must be an element, besides e, in $Z(G)$! This is the contention of the theorem.

Rephrasing, the theorem states that a group of prime-power order must always have a nontrivial center.

We can now simply prove, as a corollary for this, a result given in an earlier problem.

COROLLARY *If $o(G) = p^2$ where p is a prime number, then G is abelian.*

Proof. Our aim is to show that $Z(G) = G$. At any rate, we already know that $Z(G) \neq (e)$ is a subgroup of G so that $o(Z(G)) = p$ or p^2. If $o(Z(G)) = p^2$, then $Z(G) = G$ and we are done. Suppose that $o(Z(G)) = p$; let $a \in G$, $a \notin Z(G)$. Thus $N(a)$ is a subgroup of G, $Z(G) \subset N(a)$, $a \in N(a)$, so that $o(N(a)) > p$, yet by Lagrange's theorem $o(N(a)) \mid o(G) = p^2$. The only way out is for $o(N(a)) = p^2$, implying that $a \in Z(G)$, a contradiction. Thus $o(Z(G)) = p$ is not an actual possibility.

APPLICATION 2 We now use Theorem 2.11.1 to prove an important theorem due to Cauchy. The reader may remember that this theorem was already proved for abelian groups as an application of the results developed in the section on homomorphisms. In fact, we shall make use of this special

case in the proof below. But, to be frank, we shall prove, in the very next section, a much stronger result, due to Sylow, which has Cauchy's theorem as an immediate corollary, in a manner which completely avoids Theorem 2.11.1. To continue our candor, were Cauchy's theorem itself our ultimate and only goal, we could prove it, using the barest essentials of group theory, in a few lines. [The reader should look up the charming, one-paragraph proof of Cauchy's theorem found by McKay and published in the *American Mathematical Monthly*, Vol. 66 (1959), page 119.] Yet, despite all these counter-arguments we present Cauchy's theorem here as a striking illustration of Theorem 2.11.1.

THEOREM 2.11.3 (CAUCHY) *If p is a prime number and $p \mid o(G)$, then G has an element of order p.*

Proof. We seek an element $a \neq e \in G$ satisfying $a^p = e$. To prove its existence we proceed by induction on $o(G)$; that is, we assume the theorem to be true for all groups T such that $o(T) < o(G)$. We need not worry about starting the induction for the result is vacuously true for groups of order 1.

If for any subgroup W of G, $W \neq G$, were it to happen that $p \mid o(W)$, then by our induction hypothesis there would exist an element of order p in W, and thus there would be such an element in G. Thus we may assume that p is not a divisor of the order of any proper subgroup of G. In particular, if $a \notin Z(G)$, since $N(a) \neq G$, $p \nmid o(N(a))$. Let us write down the class equation:

$$o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}.$$

Since $p \mid o(G)$, $p \nmid o(N(a))$ we have that

$$p \left| \frac{o(G)}{o(N(a))}, \right.$$

and so

$$p \left| \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}; \right.$$

since we also have that $p \mid o(G)$, we conclude that

$$p \left| \left(o(G) - \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))} \right) = o(Z(G)). \right.$$

$Z(G)$ is thus a subgroup of G whose order is divisible by p. But, after all, we have assumed that p is not a divisor of the order of any proper subgroup of G, so that $Z(G)$ cannot be a proper subgroup of G. We are forced to

accept the only possibility left us, namely, that $Z(G) = G$. But then G is abelian; now we invoke the result already established for abelian groups to complete the induction. This proves the theorem.

We conclude this section with a consideration of the conjugacy relation in a specific class of groups, namely, the symmetric groups S_n.

Given the integer n we say the sequence of positive integers $n_1, n_2, \ldots, n_r$, $n_1 \leq n_2 \leq \cdots \leq n_r$ constitute a *partition* of n if $n = n_1 + n_2 + \cdots + n_r$. Let $p(n)$ denote the number of partitions of n. Let us determine $p(n)$ for small values of n:

$$p(1) = 1 \text{ since } 1 = 1 \text{ is the only partition of } 1,$$

$$p(2) = 2 \text{ since } 2 = 2 \text{ and } 2 = 1 + 1,$$

$$p(3) = 3 \text{ since } 3 = 3,\ 3 = 1 + 2,\ 3 = 1 + 1 + 1,$$

$$p(4) = 5 \text{ since } 4 = 4,\ 4 = 1 + 3,\ 4 = 1 + 1 + 2,$$
$$4 = 1 + 1 + 1 + 1,\ 4 = 2 + 2.$$

Some others are $p(5) = 7$, $p(6) = 11$, $p(61) = 1{,}121{,}505$. There is a large mathematical literature on $p(n)$.

Every time we break a given permutation in S_n into a product of disjoint cycles we obtain a partition of n; for if the cycles appearing have lengths $n_1, n_2, \ldots, n_r$, respectively, $n_1 \leq n_2 \leq \cdots \leq n_r$, then $n = n_1 + n_2 + \cdots + n_r$. We shall say a permutation $\sigma \in S_n$ has the cycle decomposition $\{n_1, n_2, \ldots, n_r\}$ if it can be written as the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$, $n_1 \leq n_2 \leq \cdots \leq n_r$. Thus in S_9

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

has cycle decomposition $\{1, 1, 2, 2, 3\}$; note that $1 + 1 + 2 + 2 + 3 = 9$. We now aim to prove that two permutations in S_n are conjugate if and only if they have the same cycle decomposition. Once this is proved, then S_n will have exactly $p(n)$ conjugate classes.

To reach our goal we exhibit a very simple rule for computing the conjugate of a given permutation. Suppose that $\sigma \in S_n$ and that σ sends $i \to j$. How do we find $\theta^{-1}\sigma\theta$ where $\theta \in S_n$? Suppose that θ sends $i \to s$ and $j \to t$; then $\theta^{-1}\sigma\theta$ sends $s \to t$. *In other words, to compute* $\theta^{-1}\sigma\theta$ *replace every symbol in* σ *by its image under* θ. For example, to determine $\theta^{-1}\sigma\theta$ where $\theta = (1, 2, 3)(4, 7)$ and $\sigma = (5, 6, 7)(3, 4, 2)$, then, since θ:$5 \to 5$, $6 \to 6$, $7 \to 4$, $3 \to 1$, $4 \to 7$, $2 \to 3$, $\theta^{-1}\sigma\theta$ is obtained from σ by replacing in σ, 5 by 5, 6 by 6, 7 by 4, 3 by 1, 4 by 7, and 2 by 3, so that $\theta^{-1}\sigma\theta = (5, 6, 4)(1, 7, 3)$.

With this algorithm for computing conjugates it becomes clear that two permutations having the same cycle decomposition are conjugate. For if

$\sigma = (a_1, a_2, \ldots, a_{n_1})(b_1, b_2, \ldots, b_{n_2}) \cdots (x_1, x_2, \ldots, x_{n_r})$ and $\tau = (\alpha_1, \alpha_2, \ldots, \alpha_{n_1})(\beta_1, \beta_2, \ldots, \beta_{n_2}) \cdots (\chi_1, \chi_2, \ldots, \chi_{n_r})$, then $\tau = \theta^{-1}\sigma\theta$, where one could use as θ the permutation

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n_1} & b_1 & \cdots & b_{n_2} & \cdots & x_1 & \cdots & x_{n_r} \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n_1} & \beta_1 & \cdots & \beta_{n_2} & \cdots & \chi_1 & \cdots & \chi_{n_r} \end{pmatrix}.$$

Thus, for instance, $(1, 2)(3, 4, 5)(6, 7, 8)$ and $(7, 5)(1, 3, 6)(2, 4, 8)$ can be exhibited as conjugates by using the conjugating permutation

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

That two conjugates have the same cycle decomposition is now trivial for, by our rule, to compute a conjugate, replace every element in a given cycle by its image under the conjugating permutation.

We restate the result proved in the previous discussion as

LEMMA 2.11.3 *The number of conjugate classes in S_n is $p(n)$, the number of partitions of n.*

Since we have such an explicit description of the conjugate classes in S_n we can find all the elements commuting with a given permutation. We illustrate this with a very special and simple case.

Given the permutation $(1, 2)$ in S_n, what elements commute with it? Certainly any permutation leaving both 1 and 2 fixed does. There are $(n - 2)!$ such. Also $(1, 2)$ commutes with itself. This way we get $2(n - 2)!$ elements in the group generated by $(1, 2)$ and the $(n - 2)!$ permutations leaving 1 and 2 fixed. Are there others? There are $n(n - 1)/2$ transpositions and these are precisely all the conjugates of $(1, 2)$. Thus the conjugate class of $(1, 2)$ has in it $n(n - 1)/2$ elements. If the order of the normalizer of $(1, 2)$ is r, then, by our counting principle,

$$\frac{n(n-1)}{2} = \frac{o(S_n)}{r} = \frac{n!}{r}.$$

Thus $r = 2(n - 2)!$. That is, the order of the normalizer of $(1, 2)$ is $2(n - 2)!$. But we exhibited $2(n - 2)!$ elements which commute with $(1, 2)$; thus the general element σ commuting with $(1, 2)$ is $\sigma = (1, 2)^i\tau$, where $i = 0$ or 1, τ is a permutation leaving both 1 and 2 fixed.

As another application consider the permutation $(1, 2, 3, \ldots, n) \in S_n$. We claim this element commutes only with its powers. Certainly it does commute with all its powers, and this gives rise to n elements. Now, any n-cycle is conjugate to $(1, 2, \ldots, n)$ and there are $(n - 1)!$ distinct n-cycles in S_n. Thus if u denotes the order of the normalizer of $(1, 2, \ldots, n)$

in S_n, since $o(S_n)/u$ = number of conjugates of $(1, 2, \ldots, n)$ in S_n = $(n-1)!$,

$$u = \frac{n!}{(n-1)!} = n.$$

So the order of the normalizer of $(1, 2, \ldots, n)$ in S_n is n. The powers of $(1, 2, \ldots, n)$ having given us n such elements, there is no room left for others and we have proved our contention.

Problems

1. List all the conjugate classes in S_3, find the c_a's, and verify the class equation.
2. List all the conjugate classes in S_4, find the c_a's and verify the class equation.
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.
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.
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.
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.
7. If p is a prime number, show that in S_p there are $(p-1)! + 1$ elements x satisfying $x^p = e$.
8. If in a finite group G an element a has exactly two conjugates, prove that G has a normal subgroup $N \neq (e), G$.
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.
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.

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 $0 \leq \alpha \leq n$.

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.

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 $x^{-1}Hx = H$.

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.

*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.

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

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

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

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

2.12 Sylow's Theorem

Lagrange's theorem tells us that the order of a subgroup of a finite group is a divisor of the order of that group. The converse, however, is false. There are very few theorems which assert the existence of subgroups of prescribed order in arbitrary finite groups. The most basic, and widely used, is a classic theorem due to the Norwegian mathematician Sylow.

We present here three proofs of this result of Sylow. The first is a very elegant and elementary argument due to Wielandt. It appeared in the journal *Archiv der Matematik*, Vol. 10 (1959), pages 401–402. The basic elements in Wielandt's proof are number-theoretic and combinatorial. It has the advantage, aside from its elegance and simplicity, of producing the subgroup we are seeking. The second proof is based on an exploitation of induction in an interplay with the class equation. It is one of the standard classical proofs, and is a nice illustration of combining many of the ideals developed so far in the text to derive this very important cornerstone due to Sylow. The third proof is of a completely different philosophy. The basic idea there is to show that if a larger group than the one we are considering satisfies the conclusion of Sylow's theorem, then our group also must.

This forces us to prove Sylow's theorem for a special family of groups—the symmetric groups. By invoking Cayley's theorem (Theorem 2.9.1) we are then able to deduce Sylow's theorem for all finite groups. Apart from this strange approach—to prove something for a given group, first prove it for a much larger one—this third proof has its own advantages. Exploiting the ideas used, we easily derive the so-called second and third parts of Sylow's theorem.

One might wonder: why give three proofs of the same result when, clearly, one suffices? The answer is simple. Sylow's theorem is *that* important that it merits this multifront approach. Add to this the completely diverse nature of the three proofs and the nice application each gives of different things that we have learned, the justification for the whole affair becomes persuasive (at least to the author). Be that as it may, we state Sylow's theorem and get on with Wielandt's proof.

THEOREM 2.12.1 (SYLOW) *If p is a prime number and $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.*

Before entering the first proof of the theorem we digress slightly to a brief number-theoretic and combinatorial discussion.

The number of ways of picking a subset of k elements from a set of n elements can easily be shown to be

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

If $n = p^\alpha m$ where p is a prime number, and if $p^r \mid m$ but $p^{r+1} \nmid m$, consider

$$\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!}$$

$$= \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha m - i)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha(p^\alpha - 1)\cdots(p^\alpha - i)\cdots(p^\alpha - p^\alpha + 1)}.$$

The question is, What power of p divides $\binom{p^\alpha m}{p^\alpha}$? Looking at this number, written out as we have written it out, one can see that except for the term m in the numerator, the power of p dividing $(p^\alpha m - i)$ is the same as that dividing $p^\alpha - i$, so all powers of p cancel out except the power which divides m. Thus

$$p^r \mid \binom{p^\alpha m}{p^\alpha} \quad \text{but} \quad p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}.$$

First Proof of the Theorem. Let $\mathscr{M}$ be the set of all subsets of G which have p^α elements. Thus $\mathscr{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements. Given $M_1, M_2 \in \mathscr{M}$ (M is a subset of G having p^α elements, and likewise so is M_2) define $M_1 \sim M_2$ if there exists an element $g \in G$ such that $M_1 = M_2 g$. It is immediate to verify that this defines an equivalence relation on $\mathscr{M}$. We claim that there is at least one equivalence class of elements in $\mathscr{M}$ such that the number of elements in this class is not a multiple of p^{r+1}, for if p^{r+1} is a divisor of the size of each equivalence class, then p^{r+1} would be a divisor of the number of elements in $\mathscr{M}$. Since $\mathscr{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements and $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$, this cannot be the case. Let $\{M_1, \ldots, M_n\}$ be such an equivalence class in $\mathscr{M}$ where $p^{r+1} \nmid n$. By our very definition of equivalence in $\mathscr{M}$, if $g \in G$, for each $i = 1, \ldots, n$, $M_i g = M_j$ for some j, $1 \leq j \leq n$. We let $H = \{g \in G \mid M_1 g = M_1\}$. Clearly H is a subgroup of G, for if $a, b \in H$, then $M_1 a = M_1$, $M_1 b = M_1$ whence $M_1 ab = (M_1 a)b = M_1 b = M_1$. We shall be vitally concerned with $o(H)$. We claim that $no(H) = o(G)$; we leave the proof to the reader, but suggest the argument used in the counting principle in Section 2.11. Now $no(H) = o(G) = p^\alpha m$; since $p^{r+1} \nmid n$ and $p^{\alpha+r} \mid p^\alpha m = no(H)$, it must follow that $p^\alpha \mid o(H)$, and so $o(H) \geq p^\alpha$. However, if $m_1 \in M_1$, then for all $h \in H$, $m_1 h \in M_1$. Thus M_1 has at least $o(H)$ distinct elements. However, M_1 was a subset of G containing p^α elements. Thus $p^\alpha \geq o(H)$. Combined with $o(H) \geq p^\alpha$ we have that $o(H) = p^\alpha$. *But then we have exhibited a subgroup of G having exactly p^α elements, namely H.* This proves the theorem; it actually has done more—it has constructed the required subgroup before our very eyes!

What is usually known as Sylow's theorem is a special case of Theorem 2.12.1, namely that

COROLLARY *If $p^m \mid o(G)$, $p^{m+1} \nmid o(G)$, then G has a subgroup of order p^m.*

A subgroup of G of order p^m, where $p^m \mid o(G)$ but $p^{m+1} \nmid o(G)$, is called a *p-Sylow subgroup of G*. The corollary above asserts that a finite group has p-Sylow subgroups for every prime p dividing its order. Of course the conjugate of a p-Sylow subgroup is a p-Sylow subgroup. In a short while we shall see how any two p-Sylow subgroups of G—for the same prime p—are related. We shall also get some information on how many p-Sylow subgroups there are in G for a given prime p. Before passing to this, we want to give two other proofs of Sylow's theorem.

We begin with a remark. As we observed just prior to the corollary, the corollary is a special case of the theorem. However, we claim that the

theorem is easily derivable from the corollary. That is, if we know that G possesses a subgroup of order p^m, where $p^m \mid o(G)$ but $p^{m+1} \nmid o(G)$, then we know that G has a subgroup of order p^α for any α such that $p^\alpha \mid o(G)$. This follows from the result of Problem 11, Section 2.11. This result states that any group of order p^m, p a prime, has subgroups of order p^α for any $0 \leq \alpha \leq m$. Thus to prove Theorem 2.12.1—as we shall proceed to do, again, in two more ways—it is enough for us to prove the existence of p-Sylow subgroups of G, for every prime p dividing the order of G.

Second Proof of Sylow's Theorem. We prove, by induction on the order of the group G, that for every prime p dividing the order of G, G has a p-Sylow subgroup.

If the order of the group is 2, the only relevant prime is 2 and the group certainly has a subgroup of order 2, namely itself.

So we suppose the result to be correct for all groups of order less than $o(G)$. From this we want to show that the result is valid for G. Suppose, then, that $p^m \mid o(G)$, $p^{m+1} \nmid o(G)$, where p is a prime, $m \geq 1$. If $p^m \mid o(H)$ for any subgroup H of G, where $H \neq G$, then by the induction hypothesis, H would have a subgroup T of order p^m. However, since T is a subgroup of H, and H is a subgroup of G, T too is a subgroup of G. But then T would be the sought-after subgroup of order p^m.

We therefore may assume that $p^m \nmid o(H)$ for *any* subgroup H of G, where $H \neq G$. We restrict our attention to a limited set of such subgroups. Recall that if $a \in G$ then $N(a) = \{x \in G \mid xa = ax\}$ is a subgroup of G; moreover, if $a \notin Z$, the center of G, then $N(a) \neq G$. Recall, too, that the class equation of G states that

$$o(G) = \sum \frac{o(G)}{o(N(a))},$$

where this sum runs over one element a from each conjugate class. We separate this sum into two pieces: those a which lie in Z, and those which don't. This gives

$$o(G) = z + \sum_{a \notin Z} \frac{o(G)}{o(N(a))},$$

where $z = o(Z)$. Now invoke the reduction we have made, namely, that $p^m \nmid o(H)$ for any subgroup $H \neq G$ of G, to those subgroups $N(a)$ for $a \notin Z$. Since in this case, $p^m \mid o(G)$ and $p^m \nmid o(N(a))$, we must have that

$$p \left| \frac{o(G)}{o(N(a))} \right.$$

Restating this result,

$$p \left| \frac{o(G)}{o(N(a))} \right.$$

for every $a \in G$ where $a \notin Z$. Look at the class equation with this information in hand. Since $p^m \mid o(G)$, we have that $p \mid o(G)$; also

$$p \Big| \sum_{a \notin Z} \frac{o(G)}{o(N(a))}.$$

Thus the class equation gives us that $p \mid z$. Since $p \mid z = o(Z)$, by Cauchy's theorem (Theorem 2.11.3), Z has an element $b \neq e$ of order p. Let $B = (b)$, the subgroup of G generated by b. B is of order p; moreover, *since* $b \in Z$, B *must be normal* in G. Hence we can form the quotient group $\bar{G} = G/B$. We look at $\bar{G}$. First of all, its order is $o(G)/o(B) = o(G)/p$, hence is certainly less than $o(G)$. Secondly, we have $p^{m-1} \mid o(\bar{G})$, but $p^m \nmid o(\bar{G})$. Thus, by the induction hypothesis, $\bar{G}$ has a subgroup $\bar{P}$ of order p^{m-1}. Let $P = \{x \in G \mid xB \in \bar{P}\}$; by Lemma 2.7.5, P is a subgroup of G. Moreover, $\bar{P} \approx P/B$ (Prove!); thus

$$p^{m-1} = o(\bar{P}) = \frac{o(P)}{o(B)} = \frac{o(P)}{p}.$$

This results in $o(P) = p^m$. Therefore P is the required p-Sylow subgroup of G. This completes the induction and so proves the theorem.

With this we have finished the second proof of Sylow's theorem. Note that this second proof can easily be adapted to prove that if $p^\alpha \mid o(G)$, then G has a subgroup of order p^α directly, without first passing to the existence of a p-Sylow subgroup. (This is Problem 1 of the problems at the end of this section.)

We now proceed to the third proof of Sylow's theorem.

Third Proof of Sylow's Theorem. Before going into the details of the proof proper, we outline its basic strategy. We will first show that the symmetric groups S_{p^r}, p a prime, all have p-Sylow subgroups. The next step will be to show that if G is contained in M and M has a p-Sylow subgroup, then G has a p-Sylow subgroup. Finally we will show, via Cayley's theorem, that we can use S_{p^k}, for large enough k, as our M. With this we will have all the pieces, and the theorem will drop out.

In carrying out this program in detail, we will have to know how large a p-Sylow subgroup of S_{p^r} should be. This will necessitate knowing what power of p divides $(p^r)!$. This will be easy. To produce the p-Sylow subgroup of S_{p^r} will be harder. To carry out another vital step in this rough sketch, it will be necessary to introduce a new equivalence relation in groups, and the corresponding equivalence classes known as *double cosets*. This will have several payoffs, not only in pushing through the proof of Sylow's theorem, but also in getting us the second and third parts of the full Sylow theorem.

So we get down to our first task, that of finding what power of a prime p exactly divides $(p^k)!$. Actually, it is quite easy to do this for $n!$ for any integer n (see Problem 2). But, for our purposes, it will be clearer and will suffice to do it only for $(p^k)!$.

Let $n(k)$ be defined by $p^{n(k)} \mid (p^k)!$ but $p^{n(k)+1} \nmid (p^k)!$.

LEMMA 2.12.1 $n(k) = 1 + p + \cdots + p^{k-1}$.

Proof. If $k = 1$ then, since $p! = 1 \cdot 2 \cdots (p-1) \cdot p$, it is clear that $p \mid p!$ but $p^2 \nmid p!$. Hence $n(1) = 1$, as it should be.

What terms in the expansion of $(p^k)!$ can contribute to powers of p dividing $(p^k)!$? Clearly, only the multiples of p; that is, $p, 2p, \ldots, p^{k-1}p$. In other words $n(k)$ must be the power of p which divides $p(2p)(3p)\cdots(p^{k-1}p) = p^{p^{k-1}}(p^{k-1})!$. But then $n(k) = p^{k-1} + n(k-1)$. Similarly, $n(k-1) = n(k-2) + p^{k-2}$, and so on. Write these out as

$$\begin{aligned} n(k) - n(k-1) &= p^{k-1}, \\ n(k-1) - n(k-2) &= p^{k-2}, \\ &\vdots \\ n(2) - n(1) &= p, \\ n(1) &= 1. \end{aligned}$$

Adding these up, with the cross-cancellation that we get, we obtain $n(k) = 1 + p + p^2 + \cdots + p^{k-1}$. This is what was claimed in the lemma, so we are done.

We are now ready to show that S_{p^k} has a p-Sylow subgroup; that is, we shall show (in fact, produce) a subgroup of order $p^{n(k)}$ in S_{p^k}.

LEMMA 2.12.2 *S_{p^k} has a p-Sylow subgroup.*

Proof. We go by induction on k. If $k = 1$, then the element $(1\ 2\ \ldots\ p)$, in S_p is of order p, so generated a subgroup of order p. Since $n(1) = 1$, the result certainly checks out for $k = 1$.

Suppose that the result is correct for $k-1$; we want to show that it then must follow for k. Divide the integers $1, 2, \ldots, p^k$ into p clumps, each with p^{k-1} elements as follows:

$$\{1, 2, \ldots, p^{k-1}\}, \{p^{k-1}+1, p^{k-1}+2, \ldots, 2p^{k-1}\}, \ldots, \{(p-1)p^{k-1}+1, \ldots, p^k\}.$$

The permutation σ defined by $\sigma = (1, p^{k-1}+1, 2p^{k-1}+1, \ldots, (p-1)p^{k-1}+1) \cdots (j, p^{k-1}+j, 2p^{k-1}+j, \ldots, (p-1)p^{k-1}+1+j) \cdots (p^{k-1}, 2p^{k-1}, \ldots, (p-1)p^{k-1}, p^k)$ has the following properties:

1. $\sigma^p = e$.

2. If τ is a permutation that leaves all i fixed for $i > p^{k-1}$ (hence, affects only $1, 2, \ldots, p^{k-1}$), then $\sigma^{-1}\tau\sigma$ moves only elements in $\{p^{k-1} + 1, p^{k-1} + 2, \ldots, 2p^{k-1}\}$, and more generally, $\sigma^{-j}\tau\sigma^j$ moves only elements in $\{jp^{k-1} + 1, jp^{k-1} + 2, \ldots, (j + 1)p^{k-1}\}$.

Consider $A = \{\tau \in S_{p^k} \mid \tau(i) = i \text{ if } i > p^{k-1}\}$. A is a subgroup of S_{p^k} and elements in A can carry out any permutation on $1, 2, \ldots, p^{k-1}$. From this it follows easily that $A \approx S_{p^{k-1}}$. By induction, A has a subgroup P_1 of order $p^{n(k-1)}$.

Let $T = P_1(\sigma^{-1}P_1\sigma)(\sigma^{-2}P_1\sigma^2)\cdots(\sigma^{-(p-1)}P_1\sigma^{p-1}) = P_1P_2\cdots P_{n-1}$, where $P_i = \sigma^{-i}P_1\sigma^i$. Each P_i is isomorphic to P_1 so has order $p^{n(k-1)}$. Also elements in distinct P_i's influence nonoverlapping sets of integers, *hence commute.* Thus T is a subgroup of S_{p^k}. What is its order? Since $P_i \cap P_j = (e)$ if $0 \leq i \neq j \leq p - 1$, we see that $o(T) = o(P_1)^p = p^{pn(k-1)}$. We are not quite there yet. T is not the p-Sylow subgroup we seek!

Since $\sigma^p = e$ and $\sigma^{-i}P_1\sigma^i = P_i$ we have $\sigma^{-1}T\sigma = T$. Let $P = \{\sigma^j t \mid t \in T, 0 \leq j \leq p - 1\}$. Since $\sigma \notin T$ and $\sigma^{-1}T\sigma = T$ we have two things: firstly, T is a subgroup of S_{p^k} and, furthermore, $o(P) = p \cdot o(T) = p \cdot p^{n(k-1)p} = p^{n(k-1)p+1}$. Now we are finally there! P is the sought-after p-Sylow subgroup of S_{p^k}.

Why? Well, what is its order? It is $p^{n(k-1)p+1}$. But $n(k - 1) = 1 + p + \cdots + p^{k-2}$, hence $pn(k - 1) + 1 = 1 + p + \cdots + p^{k-1} = n(k)$. Since now $o(P) = p^{n(k)}$, P is indeed a p-Sylow subgroup of S_{p^k}.

Note something about the proof. Not only does it prove the lemma, it actually allows us to construct the p-Sylow subgroup inductively. We follow the procedure of the proof to construct a 2-Sylow subgroup in S_4.

Divide $1, 2, 3, 4$ into $\{1, 2\}$ and $\{3, 4\}$. Let $P_1 = ((1\,2))$ and $\sigma = (1\,3)(2\,4)$. Then $P_2 = \sigma^{-1}P_1\sigma = (3\,4)$. Our 2-Sylow subgroup is then the group generated by $(1\,3)(2\,4)$ and

$$T = P_1P_2 = \{(1\,2), (3\,4), (1\,2)(3\,4), e\}.$$

In order to carry out the program of the third proof that we outlined, we now introduce a new equivalence relation in groups (see Problem 39, Section 2.5).

DEFINITION Let G be a group, A, B subgroups of G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$.

We leave to the reader the verification—it is easy—of

LEMMA 2.12.3 *The relation defined above is an equivalence relation on G. The equivalence class of $x \in G$ is the set $AxB = \{axb \mid a \in A, b \in B\}$.*

We call the set AxB a *double coset* of A, B in G.

If A, B are finite subgroups of G, how many elements are there in the double coset AxB? To begin with, the mapping $T:AxB \to AxBx^{-1}$ given by $(axb)T = axbx^{-1}$ is one-to-one and onto (verify). Thus $o(AxB) = o(AxBx^{-1})$. Since xBx^{-1} is a subgroup of G, of order $o(B)$, by Theorem 2.5.1,

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

We summarize this in

LEMMA 2.12.4 *If A, B are finite subgroups of G then*

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

We now come to the gut step in this third proof of Sylow's theorem.

LEMMA 2.12.5 *Let G be a finite group and suppose that G is a subgroup of the finite group M. Suppose further that M has a p-Sylow subgroup Q. Then G has a p-Sylow subgroup P. In fact, $P = G \cap xQx^{-1}$ for some $x \in M$.*

Proof. Before starting the details of the proof, we translate the hypotheses somewhat. Suppose that $p^m \mid o(M)$, $p^{m+1} \nmid o(M)$, Q is a subgroup of M of order p^m. Let $o(G) = p^n t$ where $p \nmid t$. We want to produce a subgroup P in G of order p^n.

Consider the double coset decomposition of M given by G and Q; $M = \bigcup GxQ$. By Lemma 2.12.4,

$$o(GxQ) = \frac{o(G)o(Q)}{o(G \cap xQx^{-1})} = \frac{p^n t p^m}{o(G \cap xQx^{-1})}.$$

Since $G \cap xQx^{-1}$ is a subgroup of xQx^{-1}, its order is p^{m_x}. We claim that $m_x = n$ for some $x \in M$. If not, then

$$o(GxQ) = \frac{p^n t p^m}{p^{m_x}} = t p^{m+n-m_x},$$

so is divisible by p^{m+1}. Now, since $M = \bigcup GxQ$, and this is disjoint union, $o(M) = \sum o(GxQ)$, the sum running over one element from each double coset. But $p^{m+1} \mid o(GxQ)$; hence $p^{m+1} \mid o(M)$. This contradicts $p^{m+1} \nmid o(M)$. Thus $m_x = n$ for some $x \in M$. But then $o(G \cap xQx^{-1}) = p^n$. Since $G \cap xQx^{-1} = P$ is a subgroup of G and has order p^n, the lemma is proved.

We now can easily prove Sylow's theorem. By Cayley's theorem (Theorem 2.9.1) we can isomorphically embed our finite group G in S_n, the symmetric group of degree n. Pick k so that $n < p^k$; then we can isomorphically embed S_n in S_{p^k} (by acting on $1, 2, \ldots, n$ only in the set

$1, 2, \ldots, n, \ldots, p^k$), hence G is isomorphically embedded in S_{p^k}. By Lemma 2.12.2, S_{p^k} has a p-Sylow subgroup. Hence, by Lemma 2.12.5, G must have a p-Sylow subgroup. This finishes the third proof of Sylow's theorem.

This third proof has given us quite a bit more. From it we have the machinery to get the other parts of Sylow's theorem.

THEOREM 2.12.2 (SECOND PART OF SYLOW'S THEOREM) *If G is a finite group, p a prime and $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$, then any two subgroups of G of order p^n are conjugate.*

Proof. Let A, B be subgroups of G, each of order p^n. We want to show that $A = gBg^{-1}$ for some $g \in G$.

Decompose G into double cosets of A and B; $G = \bigcup AxB$. Now, by Lemma 2.12.4,

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

If $A \neq xBx^{-1}$ for every $x \in G$ then $o(A \cap xBx^{-1}) = p^m$ where $m < n$. Thus

$$o(AxB) = \frac{o(A)o(B)}{p^m} = \frac{p^{2n}}{p^m} = p^{2n-m}$$

and $2n - m \geq n + 1$. Since $p^{n+1} \mid o(AxB)$ for every x and since $o(G) = \sum o(AxB)$, we would get the contradiction $p^{n+1} \mid o(G)$. Thus $A = gBg^{-1}$ for some $g \in G$. This is the assertion of the theorem.

Knowing that for a given prime p all p-Sylow subgroups of G are conjugate allows us to count up precisely how many such p-Sylow subgroups there are in G. The argument is exactly as that given in proving Theorem 2.11.1. In some earlier problems (see, in particular, Problem 16, Section 2.5) we discussed the normalizer $N(H)$, of a subgroup, defined by $N(H) = \{x \in G \mid xHx^{-1} = H\}$. Then, as in the proof of Theorem 2.11.1, we have that *the number of distinct conjugates, xHx^{-1}, of H in G is the index of $N(H)$ in G.* Since all p-Sylow subgroups are conjugate we have

LEMMA 2.12.6 *The number of p-Sylow subgroups in G equals $o(G)/o(N(P))$, where P is any p-Sylow subgroup of G. In particular, this number is a divisor of $o(G)$.*

However, much more can be said about the number of p-Sylow subgroups there are, for a given prime p, in G. We go into this now. The technique will involve double cosets again.

THEOREM 2.12.3 (THIRD PART OF SYLOW'S THEOREM) *The number of p-Sylow subgroups in G, for a given prime, is of the form $1 + kp$.*

Proof. Let P be a p-Sylow subgroup of G. We decompose G into double cosets of P and P. Thus $G = \bigcup PxP$. We now ask: How many elements are there in PxP? By Lemma 2.12.4 we know the answer:

$$o(PxP) = \frac{o(P)^2}{o(P \cap xPx^{-1})}.$$

Thus, if $P \cap xPx^{-1} \neq P$ then $p^{n+1} \mid o(PxP)$, where $p^n = o(P)$. Paraphrasing this: if $x \notin N(P)$ then $p^{n+1} \mid o(PxP)$. Also, if $x \in N(P)$, then $PxP = P(Px) = P^2x = Px$, so $o(PxP) = p^n$ in this case.

Now

$$o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP),$$

where each sum runs over one element from each double coset. However, if $x \in N(P)$, since $PxP = Px$, the first sum is merely $\sum_{x \in N(P)} o(Px)$ over the *distinct cosets* of P in $N(P)$. Thus this first sum is just $o(N(P))$. What about the second sum? We saw that each of its constituent terms is divisible by p^{n+1}, hence

$$p^{n+1} \Bigg| \sum_{x \notin N(P)} o(PxP).$$

We can thus write this second sum as

$$\sum_{x \notin N(P)} o(PxP) = p^{n+1}u.$$

Therefore $o(G) = o(N(P)) + p^{n+1}u$, so

$$\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}u}{o(N(P))}.$$

Now $o(N(P)) \mid o(G)$ since $N(P)$ is a subgroup of G, hence $p^{n+1}u/o(N(P))$ is an integer. Also, since $p^{n+1} \nmid o(G)$, p^{n+1} can't divide $o(N(P))$. But then $p^{n+1}u/o(N(P))$ *must be divisible by* p, so we can write $p^{n+1}u/o(N(P))$ as kp, where k is an integer. Feeding this information back into our equation above, we have

$$\frac{o(G)}{o(N(P))} = 1 + kp.$$

Recalling that $o(G)/o(N(P))$ is the number of p-Sylow subgroups in G, we have the theorem.

In Problems 20–24 in the Supplementary Problems at the end of this chapter, there is outlined another approach to proving the second and third parts of Sylow's theorem.

We close this section by demonstrating how the various parts of Sylow's theorem can be used to gain a great deal of information about finite groups.

Let G be a group of order $11^2 \cdot 13^2$. We want to determine how many 11-Sylow subgroups and how many 13-Sylow subgroups there are in G. The number of 11-Sylow subgroups, by Theorem 2.12.13, is of the form $1 + 11k$. By Lemma 2.12.5, this must divide $11^2 \cdot 13^2$; being prime to 11, it must divide 13^2. Can 13^2 have a factor of the form $1 + 11k$? Clearly no, other than 1 itself. Thus $1 + 11k = 1$, and so there must be only one 11-Sylow subgroup in G. Since all 11-Sylow subgroups are conjugate (Theorem 2.12.2) we conclude that the 11-Sylow subgroup is *normal* in G.

What about the 13-Sylow subgroups? Their number is of the form $1 + 13k$ and must divide $11^2 \cdot 13^2$, hence must divide 11^2. Here, too, we conclude that there can be only one 13-Sylow subgroup in G, and it must be normal.

We now know that G has a normal subgroup A of order 11^2 and a normal subgroup B of order 13^2. By the corollary to Theorem 2.11.2, any group of order p^2 is abelian; hence A and B are both abelian. Since $A \cap B = (e)$, we easily get $AB = G$. Finally, if $a \in A$, $b \in B$, then $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in A$ since A is normal, and $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in B$ since B is normal. Thus $aba^{-1}b^{-1} \in A \cap B = (e)$. This gives us $aba^{-1}b^{-1} = e$, and so $ab = ba$ for $a \in A$, $b \in B$. This, together with $AB = G$, A, B abelian, allows us to conclude that G *is abelian.* Hence any group of order $11^2 \cdot 13^2$ must be abelian.

We give one other illustration of the use of the various parts of Sylow's theorem. Let G be a group of order 72; $o(G) = 2^3 3^2$. How many 3-Sylow subgroups can there be in G? If this number is t, then, according to Theorem 2.12.3, $t = 1 + 3k$. According to Lemma 2.12.5, $t \mid 72$, and since t is prime to 3, we must have $t \mid 8$. The only factors of 8 of the form $1 + 3k$ are 1 and 4; hence $t = 1$ or $t = 4$ are the only possibilities. In other words G has either one 3-Sylow subgroup or 4 such.

If G has only one 3-Sylow subgroup, since all 3-Sylow subgroups are conjugate, this 3-Sylow subgroup must be normal in G. In this case G would certainly contain a nontrivial normal subgroup. On the other hand if the number of 3-Sylow subgroups of G is 4, by Lemma 2.12.5 the index of N in G is 4, where N is the normalizer of a 3-Sylow subgroup. But $72 \nmid 4! = (i(N))!$. By Lemma 2.9.1 N must contain a nontrivial normal subgroup of G (of order at least 3). Thus here again we can conclude that G contains a nontrivial normal subgroup. The upshot of the discussion is that any group of order 72 must have a nontrivial normal subgroup, hence cannot be simple.

Problems

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.

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

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

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.
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.
5. If p is a prime number, give explicit generators for 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 $3^2 \cdot 5^2$.
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?
8. If G is a group of order 231, prove that the 11-Sylow subgroup is 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.
10. If G is of order 108 show that G has a normal subgroup of order 3^k, where $k \geq 2$.
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.

*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.
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 subgroup or a q-Sylow subgroup of G must be normal in G.

15. Let G be a finite group in which $(ab)^p = a^p b^p$ 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.

**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 $PN = G$.

*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 $N(N(P)) = N(P)$.

*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 $a = yby^{-1}$.

**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.

#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.

21. Find the possible number of 11-Sylow subgroups, 7-Sylow subgroups, and 5-Sylow subgroups in a group of order $5^2 \cdot 7 \cdot 11$.

22. If G is S_3 and $A = ((1\ 2))$ in G, find all the double cosets AxA of A in G.

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.

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 $K = (b^3)$.

2.13 Direct Products

On several occasions in this chapter we have had a need for constructing a new group from some groups we already had on hand. For instance, towards the end of Section 2.8, we built up a new group using a given group and one of its automorphisms. A special case of this type of construction has been seen earlier in the recurring example of the dihedral group.

However, no attempt had been made for some systematic device for

constructing new groups from old. We shall do so now. The method represents the most simple-minded, straightforward way of combining groups to get other groups.

We first do it for two groups—not that two is sacrosanct. However, with this experience behind us, we shall be able to handle the case of any finite number easily and with dispatch. Not that any finite number is sacrosanct either; we could equally well carry out the discussion in the wider setting of any number of groups. However, we shall have no need for so general a situation here, so we settle for the case of any finite number of groups as our ultimate goal.

Let A and B be any two groups and consider the Cartesian product (which we discussed in Chapter 1) $G = A \times B$ of A and B. G consists of all ordered pairs (a, b), where $a \in A$ and $b \in B$. Can we use the operations in A and B to endow G with a product in such a way that G is a group? Why not try the obvious? Multiply componentwise. That is, let us define, for (a_1, b_1) and (a_2, b_2) in G, their product via $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$. Here, the product a_1a_2 in the first component is the product of the elements a_1 and a_2 as calculated in the group A. The product b_1b_2 in the second component is that of b_1 and b_2 as elements in the group B.

With this definition we at least have a product defined in G. Is G a group relative to this product? The answer is yes, and is easy to verify. We do so now.

First we do the associative law. Let (a_1, b_1), (a_2, b_2), and (a_3, b_3) be three elements of G. Then $((a_1, b_1)(a_2, b_2))(a_3, b_3) = (a_1a_2, b_1b_2)(a_3, b_3) = ((a_1a_2)a_3, (b_1b_2)b_3)$, while $(a_1, b_1)((a_2, b_2)(a_3, b_3)) = (a_1, b_1)(a_2a_3, b_2b_3) = (a_1(a_2a_3), b_1(b_2b_3))$. The associativity of the product in A and in B then show us that our product in G is indeed associative.

Now to the unit element. What would be more natural than to try (e, f), where e is the unit element of A and f that of B, as the proposed unit element for G? We have $(a, b)(e, f) = (ae, bf) = (a, b)$ and $(e, f)(a, b) = (ea, fb) = (a, b)$. Thus (e, f) acts as a unit element in G.

Finally, we need the inverse in G for any element of G. Here, too, why not try the obvious? Let $(a, b) \in G$; try (a^{-1}, b^{-1}) as its inverse. Now $(a, b)(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e, f)$ and $(a^{-1}, b^{-1})(a, b) = (a^{-1}a, b^{-1}b) = (e, f)$, so that (a^{-1}, b^{-1}) does serve as the inverse for (a, b).

With this we have verified that $G = A \times B$ is a group. We call it the *external direct product* of A and B.

Since $G = A \times B$ has been built up from A and B in such a trivial manner, we would expect that the structure of A and B would reflect heavily in that of G. This is indeed the case. Knowing A and B completely gives us complete information, structurally, about $A \times B$.

The construction of $G = A \times B$ has been from the outside, external. Now we want to turn the affair around and try to carry it out internally in G.

Consider $\bar{A} = \{(a,f) \in G \mid a \in A\} \subset G = A \times B$, where f is the unit element of B. What would one expect of $\bar{A}$? Answer: $\bar{A}$ is a subgroup of G and is isomorphic to A. To effect this isomorphism, define $\phi: A \to \bar{A}$ by $\phi(a) = (a,f)$ for $a \in A$. It is trivial that ϕ is an isomorphism of A onto $\bar{A}$. It is equally trivial that $\bar{A}$ is a subgroup of G. Furthermore, $\bar{A}$ is normal in G. For if $(a,f) \in \bar{A}$ and $(a_1, b_1) \in G$, then $(a_1, b_1)(a,f)(a_1, b_1)^{-1} = (a_1, b_1)(a,f)(a_1^{-1}, b_1^{-1}) = (a_1 a a_1^{-1}, b_1 f b^{1-1}) = (a_1 a a_1^{-1}, f) \in \bar{A}$. So we have an isomorphic copy, $\bar{A}$, of A in G which is a normal subgroup of G.

What we did for A we can also do for B. If $\bar{B} = \{(e, b) \in G \mid b \in B\}$, then $\bar{B}$ is isomorphic to B and is a normal subgroup of G.

We claim a little more, namely $G = \bar{A}\bar{B}$ and every $g \in G$ has a unique decomposition in the form $g = \bar{a}\bar{b}$ with $\bar{a} \in \bar{A}$ and $\bar{b} \in \bar{B}$. For, $g = (a, b) = (a,f)(e, b)$ and, since $(a,f) \in \bar{A}$ and $(e, b) \in \bar{B}$, we do have $g = \bar{a}\bar{b}$ with $\bar{a} = (a,f)$ and $\bar{b} = (e, b)$. Why is this unique? If $(a, b) = \bar{x}\bar{y}$, where $\bar{x} \in \bar{A}$ and $\bar{y} \in \bar{B}$, then $\bar{x} = (x,f)$, $x \in A$ and $\bar{y} = (e,y)$, $y \in B$; thus $(a, b) = \bar{x}\bar{y} = (x,f)(e,y) = (x,y)$. This gives $x = a$ and $y = b$, and so $\bar{x} = \bar{a}$ and $\bar{y} = \bar{b}$.

Thus we have realized G as an internal product $\bar{A}\bar{B}$ of two normal subgroups, $\bar{A}$ isomorphic to A, $\bar{B}$ to B in such a way that every element $g \in G$ has a unique representation in the form $g = \bar{a}\bar{b}$, with $\bar{a} \in \bar{A}$ and $\bar{b} \in \bar{B}$.

We leave the discussion of the product of two groups and go to the case of n groups, $n > 1$ any integer.

Let $G_1, G_2, \ldots, G_n$ be any n groups. Let $G = G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$ be the set of all ordered n-tuples, that is, the Cartesian product of $G_1, G_2, \ldots, G_n$. We define a product in G via $(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n')$, that is, via componentwise multiplication. The product in the ith component is carried in the group G_i. Then G is a group in which $(e_1, e_2, \ldots, e_n)$ is the unit element, where each e_i is the unit element of G_i, and where $(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$. We call this group G the *external direct product* of $G_1, G_2, \ldots, G_n$.

In $G = G_1 \times G_2 \times \cdots \times G_n$ let $\bar{G}_i = \{(e_1, e_2, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n) \mid g_i \in G_i\}$. Then $\bar{G}_i$ is a normal subgroup of G and is isomorphic to G_i. Moreover, $G = \bar{G}_1 \bar{G}_2 \cdots \bar{G}_n$ and every $g \in G$ has a unique decomposition $g = \bar{g}_1 \bar{g}_2 \cdots \bar{g}_n$, where $\bar{g}_1 \in \bar{G}_1, \ldots, \bar{g}_n \in \bar{G}_n$. We leave the verification of these facts to the reader.

Here, too, as in the case $A \times B$, we have realized the group G *internally* as the product of normal subgroups $\bar{G}_1, \ldots, \bar{G}_n$ in such a way that every element is uniquely representable as a product of elements $\bar{g}_1 \cdots \bar{g}_n$, where each $\bar{g}_i \in \bar{G}_i$. With this motivation we make the

DEFINITION Let G be a group and $N_1, N_2, \ldots, N_n$ *normal* subgroups of G such that

1. $G = N_1 N_2 \cdots N_n$.
2. Given $g \in G$ then $g = m_1 m_2 \cdots m_n$, $m_i \in N_i$ in a unique way.

We then say that G is the *internal direct product* of $N_1, N_2, \ldots, N_n$.

Before proceeding let's look at an example of a group G which is the internal direct product of some of its subgroups. Let G be a finite *abelian* group of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and each $\alpha_i > 0$. If $P_1, \ldots, P_k$ are the p_1-Sylow subgroup, $\ldots$, p_k-Sylow subgroup respectively of G, then G is the internal direct product of $P_1, P_2, \ldots, P_k$ (see Problem 5).

We continue with the general discussion. Suppose that G is the internal direct product of the normal subgroups $N_1, \ldots, N_n$. The $N_1, \ldots, N_n$ are groups in their own right—forget that they are normal subgroups of G for the moment. Thus we can form the group $T = N_1 \times N_2 \times \cdots \times N_n$, the external direct product of $N_1, \ldots, N_n$. One feels that G and T should be related. Our aim, in fact, is to show that G is isomorphic to T. If we could establish this then we could abolish the prefix external and internal in the phrases external direct product, internal direct product—after all these would be the same group up to isomorphism—and just talk about the direct product.

We start with

LEMMA 2.13.1 *Suppose that G is the internal direct product of $N_1, \ldots, N_n$. Then for $i \neq j$, $N_i \cap N_j = (e)$, and if $a \in N_i$, $b \in N_j$ then $ab = ba$.*

Proof. Suppose that $x \in N_i \cap N_j$. Then we can write x as

$$x = e_1 \cdots e_{i-1} x e_{i+1} \cdots e_j \cdots e_n,$$

where $e_t = e$, viewing x as an element in N_i. Similarly, we can write x as

$$x = e_1 \cdots e_i \cdots e_{j-1} x e_{j+1} \cdots e_n,$$

where $e_t = e$, viewing x as an element of N_j. But every element—and so, in particular x—has a unique representation in the form $m_1 m_2 \cdots m_n$, where $m_i \in N_1, \ldots, m_n \in N_n$. Since the two decompositions in this form for x must coincide, the entry from N_i in each must be equal. In our first decomposition this entry is x, in the other it is e; hence $x = e$. Thus $N_i \cap N_j = (e)$ for $i \neq j$.

Suppose $a \in N_i$, $b \in N_j$, and $i \neq j$. Then $aba^{-1} \in N_j$ since N_j is normal; thus $aba^{-1}b^{-1} \in N_j$. Similarly, since $a^{-1} \in N_i$, $ba^{-1}b^{-1} \in N_i$, whence $aba^{-1}b^{-1} \in N_i$. But then $aba^{-1}b^{-1} \in N_i \cap N_j = (e)$. Thus $aba^{-1}b^{-1} = e$; this gives the desired result $ab = ba$.

One should point out that if $K_1, \ldots, K_n$ are normal subgroups of G such that $G = K_1 K_2 \cdots K_n$ and $K_i \cap K_j = (e)$ for $i \neq j$ it *need not be*

true that G is the internal direct product of $K_1, \ldots, K_n$. A more stringent condition is needed (see Problems 8 and 9).

We now can prove the desired isomorphism between the external and internal direct products that was stated earlier.

THEOREM 2.13.1 *Let G be a group and suppose that G is the internal direct product of $N_1, \ldots, N_n$. Let $T = N_1 \times N_2 \times \cdots \times N_n$. Then G and T are isomorphic.*

Proof. Define the mapping $\psi: T \to G$ by

$$\psi((b_1, b_2, \ldots, b_n)) = b_1 b_2 \cdots b_n,$$

where each $b_i \in N_i$, $i = 1, \ldots, n$. We claim that ψ is an isomorphism of T onto G.

To begin with, ψ is certainly onto; for, since G is the internal direct product of $N_1, \ldots, N_n$, if $x \in G$ then $x = a_1 a_2 \cdots a_n$ for some $a_1 \in N_1, \ldots, a_n \in N_n$. But then $\psi((a_1, a_2, \ldots, a_n)) = a_1 a_2 \cdots a_n = x$. The mapping ψ is one-to-one by the *uniqueness* of the representation of every element as a product of elements from $N_1, \ldots, N_n$. For, if $\psi((a_1, \ldots, a_n)) = \psi((c_1, \ldots, c_n))$, where $a_i \in N_i$, $c_i \in N_i$, for $i = 1, 2, \ldots, n$, then, by the definition of ψ, $a_1 a_2 \cdots a_n = c_1 c_2 \cdots c_n$. The uniqueness in the definition of internal direct product forces $a_1 = c_1$, $a_2 = c_2, \ldots, a_n = c_n$. Thus ψ is one-to-one.

All that remains is to show that ψ is a homomorphism of T onto G. If $X = (a_1, \ldots, a_n)$, $Y = (b_1, \ldots, b_n)$ are elements of T then

$$\begin{aligned} \psi(XY) &= \psi((a_1, \ldots, a_n)(b_1, \ldots, b_n)) \\ &= \psi(a_1 b_1, a_2 b_2, \ldots, a_n b_n) \\ &= a_1 b_1 a_2 b_2 \cdots a_n b_n. \end{aligned}$$

However, by Lemma 2.13.1, $a_i b_j = b_j a_i$ if $i \neq j$. This tells us that $a_1 b_1 a_2 b_2 \cdots a_n b_n = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_n$. Thus $\psi(XY) = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_n$. But we can recognize $a_1 a_2 \cdots a_n$ as $\psi((a_1, a_2, \ldots, a_n)) = \psi(X)$ and $b_1 b_2 \cdots b_n$ as $\psi(Y)$. We therefore have $\psi(XY) = \psi(X)\psi(Y)$. In short, we have shown that ψ is an isomorphism of T onto G. This proves the theorem.

Note one particular thing that the theorem proves. If a group G is isomorphic to an external direct product of certain groups G_i, then G *is*, in fact, the internal direct product of groups $\bar{G}_i$ isomorphic to the G_i. We simply say that G is the direct product of the $\bar{G}_i$ (or G_i).

In the next section we shall see that every finite abelian group is a direct product of cyclic groups. Once we have this, we have the structure of all finite abelian groups pretty well under our control.

One should point out that the analog of the direct product of groups exists in the study of almost all algebraic structures. We shall see this later

for vector-spaces, rings, and modules. Theorems that describe such an algebraic object in terms of direct products of more describable algebraic objects of the same kind (for example, the case of abelian groups above) are important theorems in general. Through such theorems we can reduce the study of a fairly complex algebraic situation to a much simpler one.

Problems

1. If A and B are groups, prove that $A \times B$ 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?
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.
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.
5. Let G be a finite abelian group. Prove that 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.
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 $x \equiv v \bmod n$.
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 $N_1, \ldots, N_n$.
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 $i = 1, \ldots, n$.
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 $V_1 \times V_2 \times \cdots \times V_n$.

*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 $o(G)$?

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.

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.
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.
*15. Let $G = A \times A$ where A is cyclic of order p, p a prime. How many automorphisms does G have?
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.
17. If $G = K_1 \times K_2 \times \cdots \times K_n$ and $g \in G$, describe

$$N(g) = \{x \in G \mid xg = gx\}.$$

18. If G is a finite group and $N_1, \ldots, N_n$ are normal subgroups of G such that $G = N_1 N_2 \cdots N_n$ and $o(G) = o(N_1)o(N_2) \cdots o(N_n)$, prove that G is the direct product of $N_1, N_2, \ldots, N_n$.

2.14 Finite Abelian Groups

We close this chapter with a discussion (and description) of the structure of an arbitrary finite abelian group. The result which we shall obtain is a famous classical theorem, often referred to as the Fundamental Theorem on Finite Abelian Groups. It is a highly satisfying result because of its decisiveness. Rarely do we come out with so compact, succinct, and crisp a result. In it the structure of a finite abelian group is completely revealed, and by means of it we have a ready tool for attacking any structural problem about finite abelian groups. It even has some arithmetic consequences. For instance, one of its by-products is a precise count of how many non-isomorphic abelian groups there are of a given order.

In all fairness one should add that this description of finite abelian groups is not as general as we can go and still get so sharp a theorem. As you shall see in Section 4.5, we completely describe all abelian groups generated by a finite set of elements—a situation which not only covers the finite abelian group case, but much more.

We now state this very fundamental result.

THEOREM 2.14.1 *Every finite abelian group is the direct product of cyclic groups.*

Proof. Our first step is to reduce the problem to a slightly easier one. We have already indicated in the preceding section (see Problem 5 there) that any finite abelian group G is the direct product of its Sylow subgroups. If we knew that each such Sylow subgroup was a direct product of cyclic groups we could put the results together for these Sylow subgroups to

realize G as a direct product of cyclic groups. Thus it suffices to prove the theorem for abelian groups of order p^n where p is a prime.

So suppose that G is an abelian group of order p^n. Our objective is to find elements $a_1, \ldots, a_k$ in G such that every element $x \in G$ can be written in a unique fashion as $x = a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_k^{\alpha_k}$. Note that if this were true and $a_1, \ldots, a_k$ were of order $p^{n_1}, \ldots, p^{n_k}$, where $n_1 \geq n_2 \geq \cdots \geq n_k$, then the maximal order of any element in G would be p^{n_1} (Prove!). This gives us a cue of how to go about finding the elements $a_1, \ldots, a_k$ that we seek.

The procedure suggested by this is: let a_1 be an element of maximal order in G. How shall we pick a_2? Well, if $A_1 = (a_1)$ the subgroup generated by a_1, then a_2 maps into an element of highest order in G/A_1. If we can successfully exploit this to find an appropriate a_2, and if $A_2 = (a_2)$, then a_3 would map into an element of maximal order in G/A_1A_2, and so on. With this as guide we can now get down to the brass tacks of the proof.

Let a_1 be an element in G of highest possible order, p^{n_1}, and let $A_1 = (a_1)$. Pick b_2 in G such that $\bar{b}_2$, the image of b_2 in $\bar{G} = G/A_1$, has maximal order p^{n_2}. Since the order of $\bar{b}_2$ divides that of b_2, and since the order of a_1 is maximal, we must have that $n_1 \geq n_2$. In order to get a direct product of A_1 with (b_2) we would need $A_1 \cap (b_2) = (e)$; this might not be true for the initial choice of b_2, so we may have to adapt the element b_2. Suppose that $A_1 \cap (b_2) \neq (e)$; then, since ${b_2}^{p^{n_2}} \in A_1$ and is the first power of b_2 to fall in A_1 (by our mechanism of choosing b_2) we have that ${b_2}^{p^{n_2}} = {a_1}^i$. Therefore $({a_1}^i)^{p^{n_1-n_2}} = ({b_2}^{p^{n_2}})^{p^{n_1-n_2}} = {b_2}^{p^{n_1}} = e$, whence ${a_1}^{ip^{n_1-n_2}} = e$. Since a_1 is of order p^{n_1} we must have that $p^{n_1} \mid ip^{n_1-n_2}$, and so $p^{n_2} \mid i$. Thus, recalling what i is, we have ${b_2}^{p^{n_2}} = {a_1}^i = {a_1}^{jp^{n_2}}$. This tells us that if $a_2 = {a_1}^{-j} b_2$ then ${a_2}^{p^{n_2}} = e$. The element a_2 is indeed the element we seek. Let $A_2 = (a_2)$. We claim that $A_1 \cap A_2 = (e)$. For, suppose that ${a_2}^t \in A_1$; since $a_2 = {a_1}^{-j} b_2$, we get $({a_1}^{-j} b_2)^t \in A_1$ and so ${b_2}^t \in A_1$. By choice of b_2, this last relation forces $p^{n_2} \mid t$, and since ${a_2}^{p^{n_2}} = e$ we must have that ${a_2}^t = e$. In short $A_1 \cap A_2 = (e)$.

We continue one more step in the program we have outlined. Let $b_3 \in G$ map into an element of maximal order in $G/(A_1A_2)$. If the order of the image of b_3 in $G/(A_1A_2)$ is p^{n_3}, we claim that $n_3 \leq n_2 \leq n_1$. Why? By the choice of n_2, ${b_3}^{p^{n_2}} \in A_1$ so is certainly in A_1A_2. Thus $n_3 \leq n_2$. Since ${b_3}^{p^{n_3}} \in A_1A_2$, ${b_3}^{p^{n_3}} = {a_1}^{i_1} {a_2}^{i_2}$. We claim that $p^{n_3} \mid i_1$ and $p^{n_3} \mid i_2$. For, ${b_3}^{p^{n_2}} \in A_1$ hence $({a_1}^{i_1} {a_2}^{i_2})^{p^{n_2-n_3}} = ({b_3}^{p^{n_3}})^{p^{n_2-n_3}} \equiv {b_3}^{p^{n_2}} \in A_1$. This tells us that ${a_2}^{i_2 p^{n_2-n_3}} \in A_1$ and so $p^{n_2} \mid i_2 p^{n_2-n_3}$, which is to say, $p^{n_3} \mid i_2$. Also ${b_3}^{p^{n_1}} = e$, hence $({a_1}^{i_1} {a_2}^{i_2})^{p^{n_1-n_3}} = {b_3}^{p^{n_1}} = e$; this says that ${a_1}^{i_1 p^{n_1-n_3}} \in A_2 \cap A_1 = (e)$, that is, ${a_1}^{i_1 p^{n_1-n_3}} = e$. This yields that $p^{n_3} \mid i_1$. Let $i_1 = j_1 p^{n_3}$, $i_2 = j_2 p^{n_3}$; thus ${b_3}^{p^{n_3}} = {a_1}^{j_1 p^{n_3}} {a_2}^{j_2 p^{n_3}}$. Let $a_3 = {a_1}^{-j_1} {a_2}^{-j_2} b_3$, $A_3 = (a_3)$; note that ${a_3}^{p^{n_3}} = e$. We claim that $A_3 \cap (A_1A_2) = (e)$. For if ${a_3}^t \in A_1A_2$ then $({a_1}^{-j_1} {a_2}^{-j_2} b_3)^t \in A_1A_2$, giving us ${b_3}^t \in A_1A_2$. But then $p^{n_3} \mid t$, whence, since ${a_3}^{p^{n_3}} = e$, we have ${a_3}^t = e$. In other words, $A_3 \cap (A_1A_2) = (e)$.

Continuing this way we get cyclic subgroups $A_1 = (a_1)$, $A_2 = (a_2), \ldots, A_k = (a_k)$ of order $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$, respectively, with $n_1 \geq n_2 \geq \cdots \geq n_k$ such that $G = A_1A_2 \cdots A_k$ and such that, for each i, $A_i \cap (A_1A_2 \cdots A_{i-1}) = (e)$. This tells us that every $x \in G$ has a unique representation as $x = a_1'a_2' \cdots a_k'$ where $a_1' \in A_1, \ldots, a_k' \in A_k$. In other words, G is the direct product of the cyclic subgroups $A_1, A_2, \ldots, A_k$. The theorem is now proved.

DEFINITION If G is an abelian group of order p^n, p a prime, and $G = A_1 \times A_2 \times \cdots \times A_k$ where each A_i is cyclic of order p^{n_i} with $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, then the integers $n_1, n_2, \ldots, n_k$ are called the *invariants* of G.

Just because we called the integers above the invariants of G does not mean that they *are* really *the* invariants of G. That is, it is possible that we can assign different sets of invariants to G. We shall soon show that the invariants of G are indeed unique and completely describe G.

Note one other thing about the invariants of G. If $G = A_1 \times \cdots \times A_k$, where A_i is cyclic of order p^{n_i}, $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, then $o(G) = o(A_1)o(A_2) \cdots o(A_k)$, hence $p^n = p^{n_1}p^{n_2} \cdots p^{n_k} = p^{n_1+n_2+\cdots+n_k}$, whence $n = n_1 + n_2 + \cdots + n_k$. In other words, $n_1, n_2, \ldots, n_k$ give us a *partition* of n. We have already run into this concept earlier in studying the conjugate classes in the symmetric group.

Before discussing the uniqueness of the invariants of G, one thing should be made absolutely clear: the elements $a_1, \ldots, a_k$ and the subgroups $A_1, \ldots, A_k$ which they generate, which arose above to give the decomposition of G into a direct product of cyclic groups, are *not* unique. Let's see this in a very simple example. Let $G = \{e, a, b, ab\}$ be an abelian group of order 4 where $a^2 = b^2 = e$, $ab = ba$. Then $G = A \times B$ where $A = (a)$, $B = (b)$ are cyclic groups of order 2. But we have another decomposition of G as a direct product, namely, $G = C \times B$ where $C = (ab)$ and $B = (b)$. So, even in this group of very small order, we can get distinct decompositions of the group as the direct product of cyclic groups. Our claim—which we now want to substantiate—is that while these cyclic subgroups are not unique, their *orders are*

DEFINITION If G is an abelian group and s is any integer, then $G(s) = \{x \in G \mid x^s = e\}$.

Because G is abelian it is evident that $G(s)$ is a subgroup of G. We now prove

LEMMA 2.14.1 *If G and G' are isomorphic abelian groups, then for every integer s, $G(s)$, and $G'(s)$ are isomorphic.*

Proof. Let ϕ be an isomorphism of G onto G'. We claim that ϕ maps $G(s)$ isomorphically onto $G'(s)$. First we show that $\phi(G(s)) \subset G'(s)$. For, if $x \in G(s)$ then $x^s = e$, hence $\phi(x^s) = \phi(e) = e'$. But $\phi(x^s) = \phi(x)^s$; hence $\phi(x)^s = e'$ and so $\phi(x)$ is in $G'(s)$. Thus $\phi(G(s)) \subset G'(s)$.

On the other hand, if $u' \in G'(s)$ then $(u')^s = e'$. But, since ϕ is onto, $u' = \phi(y)$ for some $y \in G$. Therefore $e' = (u')^s = \phi(y)^s = \phi(y^s)$. Because ϕ is one-to-one, we have $y^s = e$ and so $y \in G(s)$. Thus ϕ maps $G(s)$ *onto* $G'(s)$.

Therefore since ϕ is one-to-one, onto, and a homomorphism from $G(s)$ to $G'(s)$, we have that $G(s)$ and $G'(s)$ are isomorphic.

We continue with

LEMMA 2.14.2 *Let G be an abelian group of order p^n, p a prime. Suppose that $G = A_1 \times A_2 \times \cdots \times A_k$, where each $A_i = (a_i)$ is cyclic of order p^{n_i}, and $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. If m is an integer such that $n_t > m \geq n_{t+1}$ then $G(p^m) = B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$ where B_i is cyclic of order p^m, generated by $a_i^{p^{n_i - m}}$, for $i \leq t$. The order of $G(p^m)$ is p^u, where*

$$u = mt + \sum_{i=t+1}^{k} n_i.$$

Proof. First of all, we claim that $A_{t+1}, \ldots, A_k$ are all in $G(p^m)$. For, since $m \geq n_{t+1} \geq \cdots \geq n_k > 0$, if $j \geq t + 1$, $a_j^{p^m} = (a_j^{p^{n_j}})^{p^{m-n_j}} = e$. Hence A_j, for $j \geq t + 1$ lies in $G(p^m)$.

Secondly, if $i \leq t$ then $n_i > m$ and $(a_i^{p^{n_i - m}})^{p^m} = a_i^{p^{n_i}} = e$, whence each such $a_i^{p^{n_i - m}}$ is in $G(p^m)$ and so the subgroup it generates, B_i, is also in $G(p^m)$.

Since $B_1, \ldots, B_t, A_{t+1}, \ldots, A_k$ are all in $G(p^m)$, their product (which is direct, since the product $A_1 A_2 \cdots A_k$ is direct) is in $G(p^m)$. Hence $G(p^m) \supset B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$.

On the other hand, if $x = a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_k^{\lambda_k}$ is in $G(p^m)$, since it then satisfies $x^{p^m} = e$, we set $e = x^{p^m} = a_1^{\lambda_1 p^m} \cdots a_k^{\lambda_k p^m}$. However, the product of the subgroups $A_1, \ldots, A_k$ is direct, so we get

$$a_1^{\lambda_1 p^m} = e, \ldots, a_k^{\lambda_k p^m} = e.$$

Thus the order of a_i, that is, p^{n_i} must divide $\lambda_i p^m$ for $i = 1, 2, \ldots, k$. If $i \geq t + 1$ this is automatically true whatever be the choice of $\lambda_{t+1}, \ldots, \lambda_k$ since $m \geq n_{t+1} \geq \cdots \geq n_k$, hence $p^{n_i} \mid p^m$, $i \geq t + 1$. However, for $i \leq t$, we get from $p^{n_i} \mid \lambda_i p^m$ that $p^{n_i - m} \mid \lambda_i$. Therefore $\lambda_i = v_i p^{n_i - m}$ for some integer v_i. Putting all this information into the values of the λ_i's in the expression for x as $x = a_1^{\lambda_1} \cdots a_k^{\lambda_k}$ we see that

$$x = a_1^{v_1 p^{n_1 - m}} \cdots a_t^{v_t p^{n_t - m}} a_{t+1}^{\lambda_{t+1}} \cdots a_k^{\lambda_k}.$$

This says that $x \in B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$.

Now since each B_i is of order p^m and since $o(A_i) = p^{n_i}$ and since $G = B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$,

$$o(G) = o(B_1)o(B_2)\cdots o(B_t)o(A_{t+1})\cdots o(A_k) = \underbrace{p^m p^m \cdots p^m}_{t\text{-times}} p^{n_{t+1}} \cdots p^{n_k}.$$

Thus, if we write $o(G) = p^u$, then

$$u = mt + \sum_{i=t+1}^{k} n_i.$$

The lemma is proved.

COROLLARY *If G is as in Lemma 2.14.2, then $o(G(p)) = p^k$.*

Proof. Apply the lemma to the case $m = 1$. Then $t = k$, hence $u = 1k = k$ and so $o(G) = p^k$.

We now have all the pieces required to prove the uniqueness of the invariants of an abelian group of order p^n.

THEOREM 2.14.2 *Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.*

In other words, if G and G' are abelian groups of order p^n and $G = A_1 \times \cdots \times A_k$, where each A_i is a cyclic group of order p^{n_i}, $n_1 \geq \cdots \geq n_k > 0$, and $G' = B_1' \times \cdots \times B_s'$, where each B_i' is a cyclic group of order p^{h_i}, $h_1 \geq \cdots \geq h_s > 0$, then G and G' are isomorphic if and only if $k = s$ and for each i, $n_i = h_i$.

Proof. One way is very easy, namely, if G and G' have the same invariants then they are isomorphic. For then $G = A_1 \times \cdots \times A_k$ where $A_i = (a_i)$ is cyclic of order p^{n_i}, and $G' = B_1' \times \cdots \times B_k'$ where $B_i' = (b_i')$ is cyclic of order p^{n_i}. Map G onto G' by the map $\phi(a_1^{\alpha_1} \cdots a_k^{\alpha_k}) = (b_1')^{\alpha_1} \cdots (b_k')^{\alpha_k}$. We leave it to the reader to verify that this defines an isomorphism of G onto G'.

Now for the other direction. Suppose that $G = A_1 \times \cdots \times A_k$, $G' = B_1' \times \cdots \times B_s'$, A_i, B_i' as described above, cyclic of orders p^{n_i}, p^{h_i}, respectively, where $n_1 \geq \cdots \geq n_k > 0$ and $h_1 \geq \cdots \geq h_s > 0$. We want to show that if G and G' are isomorphic then $k = s$ and each $n_i = h_i$.

If G and G' are isomorphic then, by Lemma 2.14.1, $G(p^m)$ and $G'(p^m)$ must be isomorphic for any integer $m \geq 0$, hence must have the same order. Let's see what this gives us in the special case $m = 1$; that is, what information can we garner from $o(G(p)) = o(G'(p))$. According to the corollary to Lemma 2.14.2, $o(G(p)) = p^k$ and $o(G'(p)) = p^s$. Hence $p^k = p^s$ and so $k = s$. At least we now know that the *number* of invariants for G and G' is the same.

If $n_i \neq h_i$ for some i, let t be the first i such that $n_t \neq h_t$; we may suppose that $n_t > h_t$. Let $m = h_t$. Consider the subgroups, $H = \{x^{p^m} \mid x \in G\}$ and $H' = \{(x')^{p^m} \mid x' \in G\}$, of G and G', respectively. Since G and G' are isomorphic, it follows easily that H and H' are isomorphic. We now examine the invariants of H and H'.

Because $G = A_1 \times \cdots \times A_k$, where $A_i = (a_i)$ is of order p^{n_i}, we get that

$$H = C_1 \times \cdots \times C_t \times \cdots \times C_r,$$

where $C_i = (a_i^{p^m})$ is of order $p^{n_i - m}$, and where r is such that $n_r > m = h_t \geq n_{r-1}$. Thus the invariants of H are $n_1 - m$, $n_2 - m, \ldots, n_r - m$ and the number of invariants of H is $r \geq t$.

Because $G' = B_1' \times \cdots \times B_k'$, where $B_i = (b_i')$ is cyclic of order p^{h_i}, we get that $H' = D_1' \times \cdots \times D_{t-1}'$, where $D_i' = ((b_i')^{p^m})$ is cyclic of order $p^{h_i - m}$. Thus the invariants of H' are $h_1 - m, \ldots, h_{t-1} - m$ and so the number of invariants of H' is $t - 1$.

But H and H' are isomorphic; as we saw above this forces them to have the same number of invariants. But we saw that assuming that $n_i \neq h_i$ for some i led to a discrepancy in the number of their invariants. In consequence each $n_i = h_i$, and the theorem is proved.

An immediate consequence of this last theorem is that an abelian group of order p^n can be decomposed in only one way—*as far as the orders of the cyclic subgroups is concerned*—as a direct product of cyclic subgroups. Hence the invariants are indeed *the* invariants of G and completely determine G.

If $n_1 \geq \cdots \geq n_k > 0$, $n = n_1 + \cdots + n_k$, is any partition of n, then we can easily construct an abelian group of order p^n whose invariants are $n_1 \geq \cdots \geq n_k > 0$. To do this, let A_i be a cyclic group of order p^{n_i} and let $G = A_1 \times \cdots \times A_k$ be the external direct product of $A_1, \ldots, A_k$. Then, by the very definition, the invariants of G are $n_1 \geq \cdots \geq n_k > 0$. Finally, two different partitions of n give rise to nonisomorphic abelian groups of order p^n. This, too, comes from Theorem 2.14.2. Hence we have

THEOREM 2.14.3 *The number of nonisomorphic abelian groups of order p^n, p a prime, equals the number of partitions of n.*

Note that the answer given in Theorem 2.14.3 does *not* depend on the prime p; it only depends on the exponent n. Hence, for instance, the number of nonisomorphic abelian groups of order 2^4 equals that of orders 3^4, or 5^4, etc. Since there are five partitions of 4, namely: $4 = 4$, $3 + 1$, $2 + 2$, $2 + 1 + 1$, $1 + 1 + 1 + 1$, then there are five nonisomorphic abelian groups of order p^4 for any prime p.

Since any finite abelian group is a direct product of its Sylow subgroups, and two abelian groups are isomorphic if and only if their corresponding Sylow subgroups are isomorphic, we have the

COROLLARY *The number of nonisomorphic abelian groups of order* $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, *where the* p_i *are distinct primes and where each* $\alpha_i > 0$, *is* $p(\alpha_1)p(\alpha_2) \cdots p(\alpha_r)$, *where* $p(u)$ *denotes the number of partitions of* u.

Problems

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}.
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 $G = A_1A_2 \cdots A_k$.
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.
4. Describe all finite abelian groups of order
   (a) 2^6. (b) 11^6. (c) 7^5. (d) $2^4 \cdot 3^4$.
5. Show how to get all abelian groups of order $2^3 \cdot 3^4 \cdot 5$.
6. If G is an abelian group of order p^n with invariants $n_1 \geq \cdots \geq n_k > 0$ and $H \neq (e)$ is a subgroup of G, show that if $h_1 \geq \cdots \geq h_s > 0$ are the invariants of H, then $k \geq s$ and for each i, $h_i \leq n_i$ 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 $g \in G$.
7. Show that $\hat{G}$ is an abelian group under the operation defined.
8. If $\phi \in \hat{G}$ and G is finite, show that $\phi(g)$ is a root of unity for every $g \in G$.
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.
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 $\phi(g_1) \neq \phi(g_2)$.
11. If G is a finite abelian group prove that $o(G) = o(\hat{G})$ and G is isomorphic to $\hat{G}$.
12. If $\phi \neq 1 \in \hat{G}$ where G is an abelian group, show that $\sum_{g \in G} \phi(g) = 0$.

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 $(p-1)! \equiv -1 (p)$.
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 $p^2 \mid a$.
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 $a^{(p-1)/2} \equiv +1 (p)$.
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.
5. Prove that the nonzero integers mod p under multiplication form a cyclic group if p is a prime.
6. Give an example of a non-abelian group in which $(xy)^3 = x^3 y^3$ 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.
8. Same as Problem 7, but do not assume the group to be abelian.
9. Find all automorphisms of S_3 and S_4, the symmetric groups of degree 3 and 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.
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.
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.

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 $k \geq 1$.

14. Prove that a solvable group always has an abelian normal subgroup $M \neq (e)$.
    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.

16. Show that any subgroup and homomorphic image of a nilpotent group must be nilpotent.

17. Show that every homomorphic image, different from (e), of a nilpotent group has a nontrivial center.

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 $N(H) = \{x \in G \mid xHx^{-1} = H\}$.

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.

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.

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 $N(N(P)) = N(P)$.

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.)

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.)
24. Combine Problems 22 and 23 to give another proof of all parts of Sylow's 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.
26. Using the result of Problem 25, prove that any group of order less than 60 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.
28. Prove that (1 2 3) 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.
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.
31. Show that a group cannot 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.

#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 $LF(2, p) = G/C$.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: ALGEBRA **Subject Code: 19MMP101**
Class : I - M.Sc. Mathematics **Semester : I**

Unit II

Part A (20x1=20 Marks)
(Question Nos. 1 to 20 Online Examinations)
Possible Questions

SL.NO	Questions	Opt1	Opt2	Opt3	Opt4	Answer
1	If o(G)=p2 where p is a prime number then is ----------	non-Abelian	subgroup	group	Abelian	Abelian
2	If ---------- where p is a prime number then is abelian	o(G)=p2	o(G)=p	o(G)=1	o(G)=n	o(G)=p2
3	Let G be a -------- then the identity element is unique	normal-subgroup	subgroup	group	permutation	group
4	The product of even permutation is an -------- permutation	even	even & odd	odd	prime	even
5	The product of two odd permutation is an ---------- permutation	even	even & odd	odd	prime	even
6	Conjugacy is an ---------- relation on G	reflexive	symmetric	transitive	equivalence	equivalence
7	If G is a group of order231then the --------- is in the center of G	sylow subgroup	subgroup	11sylow subgroup	normal subgroup	11sylow subgroup
8	If G is a group of order231then the 11- sylow subgroup is in the ---------- of G	sylow subgroup	subgroup	normal subgroup	center	center
9	If o(G)=pq ,p and q are distinct primes p<q then p/(q-1) there exists a unique -------- group of order pq	non abelian	abelian	cyclic	non cyclic	non abelian
10	If o(G)= --------,p and q are distinct primes p<q then p/(q-1) there exists a unique non abelian group of order pq	p	q	pq	p/q	pq
11	If o(G)=pq ,p and q are distinct primes p<q then --------- there exists a unique non abelian group of order pq	p/(q-1)	p-1/q-1	p/q	pq	p/(q-1)
12	S_{pk} has -------subgroup	sylow	k-sylow	p-sylow	11sylow subgroup	p-sylow
13	Every finite ----------group is the direct product of cyclic groups	abeliean	Non-abeliean	cyclic	permutation	abeliean
14	If b = c^-1ac then b and a is ------- elements	inverse	co prime	conjugate	equal	conjugate
15	The conjugacy class of a is denoted as -------	c(a)	a^2	c_a	c^a	c_a
16	a in Z(G), then N(a)-------- G	equal	greater than	less than	not equal	equal
17	If p is a prime number and p\O(G), then G has an element of order p is --------therorem	Cayley's	Cauchy's	fundamental	Fermat's	Cauchy's
18	If O(G) =p^3 , the G is ---------	normal	abelian	cyclic	identity	Abelian
19	The number of conjugate classes in S_n is-----	n	c(n)	p(n)	0	p(n)
20	The number of conjugate classes in S_3 is-------	3	0	1	4	3
21	If A and B are two groups then A x B is isomorphic to-------	A	B	B x A	{e}	B x A
22	The number of non-isomorphic abelian groups of order p^n is ---------	n	1	0	p(n)	p(n)
23	The number p-sylow subgroups of G is ------	1	kp	1+kp	0	1+kp
24	Two abelian groups of order p^n are isomorphic iff they have same --------	invariants	subgroups	elements	identity	invariants
25	If G is direct product of its sylow subgroups then G is-------	abeliean	normal	nilpotent	idempotent	nilpotent

26	|A|=m, |B|=n, then A, B are cyclic iff----------	m=n	m >n	gcd(m,n)=1	m=0	gcd(m,n)=1
27	Z(G) = G iff G is -------	normal	cyclic	nilpotent	solvable	cyclic
28	Every cyclic group is ---------	abeliean	{0}	infinite	solvable	Abelian
29	Subgroup of a abelian group is ---------	abeliean	normal	cyclic	solvable	normal
30	If p \O(G), then G has a ---------	element of order p	subgroup of order p	idempotent	both a and b	both a and b

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

CLASS: I M.Sc. MATHEMATICS **COURSENAME: ALGEBRA**

COURSE CODE: 19MMP101 **BATCH-2019-2021**

UNIT-III

RING THEORY

Euclidean rings - A particular Euclidean ring - Polynomial rings – Polynomials over the rational field - Polynomial rings over commutative rings.

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 $[r_1, s_1] + [r_2, s_2] = [r_1s_2 + r_2s_1, s_1s_2]$ and $[r_1, s_1][r_2, s_2] = [r_1r_2, s_1s_2]$.

(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.

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 $a = b$.

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 $a = b$.

3.7 Euclidean Rings

The class of rings we propose to study now is motivated by several existing examples—the ring of integers, the Gaussian integers (Section 3.8), and polynomial rings (Section 3.9). The definition of this class is designed to incorporate in it certain outstanding characteristics of the three concrete examples listed above.

DEFINITION An integral domain R is said to be a *Euclidean ring* if for every $a \neq 0$ in R there is defined a nonnegative integer $d(a)$ such that

1. For all $a, b \in R$, both nonzero, $d(a) \leq d(ab)$.
2. For any $a, b \in R$, both nonzero, there exist $t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

We do not assign a value to $d(0)$. The integers serve as an example of a Euclidean ring, where $d(a) =$ absolute value of a acts as the required function. In the next section we shall see that the Gaussian integers also form a Euclidean ring. Out of that observation, and the results developed in this part, we shall prove a classic theorem in number theory due to

Fermat, namely, that every prime number of the form $4n + 1$ can be written as the sum of two squares.

We begin with

THEOREM 3.7.1 *Let R be a Euclidean ring and let A be an ideal of R. Then there exists an element $a_0 \in A$ such that A consists exactly of all a_0x as x ranges over R.*

Proof. If A just consists of the element 0, put $a_0 = 0$ and the conclusion of the theorem holds.

Thus we may assume that $A \neq (0)$; hence there is an $a \neq 0$ in A. Pick an $a_0 \in A$ such that $d(a_0)$ is minimal. (Since d takes on nonnegative integer values this is always possible.)

Suppose that $a \in A$. By the properties of Euclidean rings there exist $t, r \in R$ such that $a = ta_0 + r$ where $r = 0$ or $d(r) < d(a_0)$. Since $a_0 \in A$ and A is an ideal of R, ta_0 is in A. Combined with $a \in A$ this results in $a - ta_0 \in A$; but $r = a - ta_0$, whence $r \in A$. If $r \neq 0$ then $d(r) < d(a_0)$, giving us an element r in A whose d-value is smaller than that of a_0, in contradiction to our choice of a_0 as the element in A of minimal d-value. Consequently $r = 0$ and $a = ta_0$, which proves the theorem.

We introduce the notation $(a) = \{xa \mid x \in R\}$ to represent the ideal of all multiples of a.

DEFINITION An integral domain R with unit element is a *principal ideal ring* if every ideal A in R is of the form $A = (a)$ for some $a \in R$.

Once we establish that a Euclidean ring has a unit element, in virtue of Theorem 3.7.1, we shall know that a Euclidean ring is a principal ideal ring. The converse, however, is false; there are principal ideal rings which are not Euclidean rings. [See the paper by T. Motzkin, *Bulletin of the American Mathematical Society*, Vol. 55 (1949), pages 1142–1146, entitled "The Euclidean algorithm."]

COROLLARY TO THEOREM 3.7.1 *A Euclidean ring possesses a unit element.*

Proof. Let R be a Euclidean ring; then R is certainly an ideal of R, so that by Theorem 3.7.1 we may conclude that $R = (u_0)$ for some $u_0 \in R$. Thus every element in R is a multiple of u_0. Therefore, in particular, $u_0 = u_0c$ for some $c \in R$. If $a \in R$ then $a = xu_0$ for some $x \in R$, hence $ac = (xu_0)c = x(u_0c) = xu_0 = a$. Thus c is seen to be the required unit element.

DEFINITION If $a \neq 0$ and b are in a commutative ring R then a is said to *divide* b if there exists a $c \in R$ such that $b = ac$. We shall use the symbol

$a \mid b$ to represent the fact that a divides b and $a \nmid b$ to mean that a does not divide b.

The proof of the next remark is so simple and straightforward that we omit it.

REMARK 1. *If* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$.
2. *If* $a \mid b$ *and* $a \mid c$ *then* $a \mid (b \pm c)$.
3. *If* $a \mid b$ *then* $a \mid bx$ *for all* $x \in R$.

DEFINITION If $a, b \in R$ then $d \in R$ is said to be a *greatest common divisor* of a and b if

1. $d \mid a$ and $d \mid b$.
2. Whenever $c \mid a$ and $c \mid b$ then $c \mid d$.

We shall use the notation $d = (a, b)$ to denote that d is a greatest common divisor of a and b.

LEMMA 3.7.1 *Let R be a Euclidean ring. Then any two elements a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.*

Proof. Let A be the set of all elements $ra + sb$ where r, s range over R. We claim that A is an ideal of R. For suppose that $x, y \in A$; therefore $x = r_1a + s_1b$, $y = r_2a + s_2b$, and so $x \pm y = (r_1 \pm r_2)a + (s_1 \pm s_2)b \in A$. Similarly, for any $u \in R$, $ux = u(r_1a + s_1b) = (ur_1)a + (us_1)b \in A$.

Since A is an ideal of R, by Theorem 3.7.1 there exists an element $d \in A$ such that every element in A is a mutiple of d. By dint of the fact that $d \in A$ and that every element of A is of the form $ra + sb$, $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$. Now by the corollary to Theorem 3.7.1, R has a unit element 1; thus $a = 1a + 0b \in A$, $b = 0a + 1b \in A$. Being in A, they are both multiples of d, whence $d \mid a$ and $d \mid b$.

Suppose, finally, that $c \mid a$ and $c \mid b$; then $c \mid \lambda a$ and $c \mid \mu b$ so that c certainly divides $\lambda a + \mu b = d$. Therefore d has all the requisite conditions for a greatest common divisor and the lemma is proved.

DEFINITION Let R be a commutative ring with unit element. An element $a \in R$ is a *unit* in R if there exists an element $b \in R$ such that $ab = 1$.

Do not confuse a unit with a unit element! A unit in a ring is an element whose inverse is also in the ring.

LEMMA 3.7.2 *Let R be an integral domain with unit element and suppose that for $a, b \in R$ both $a \mid b$ and $b \mid a$ are true. Then $a = ub$, where u is a unit in R.*

Proof. Since $a \mid b$, $b = xa$ for some $x \in R$; since $b \mid a$, $a = yb$ for some $y \in R$. Thus $b = x(yb) = (xy)b$; but these are elements of an integral domain, so that we can cancel the b and obtain $xy = 1$; y is thus a unit in R and $a = yb$, proving the lemma.

DEFINITION Let R be a commutative ring with unit element. Two elements a and b in R are said to be *associates* if $b = ua$ for some unit u in R.

The relation of being associates is an equivalence relation. (Problem 1 at the end of this section.) Note that in a Euclidean ring any two greatest common divisors of two given elements are associates (Problem 2).

Up to this point we have, as yet, not made use of condition 1 in the definition of a Euclidean ring, namely that $d(a) \leq d(ab)$ for $b \neq 0$. We now make use of it in the proof of

LEMMA 3.7.3 *Let R be a Euclidean ring and $a, b \in R$. If $b \neq 0$ is not a unit in R, then $d(a) < d(ab)$.*

Proof. Consider the ideal $A = (a) = \{xa \mid x \in R\}$ of R. By condition 1 for a Euclidean ring, $d(a) \leq d(xa)$ for $x \neq 0$ in R. Thus the d-value of a is the minimum for the d-value of any element in A. Now $ab \in A$; if $d(ab) = d(a)$, by the proof used in establishing Theorem 3.7.1, since the d-value of ab is minimal in regard to A, every element in A is a multiple of ab. In particular, since $a \in A$, a must be a multiple of ab; whence $a = abx$ for some $x \in R$. Since all this is taking place in an integral domain we obtain $bx = 1$. In this way b is a unit in R, in contradiction to the fact that it was not a unit. The net result of this is that $d(a) < d(ab)$.

DEFINITION In the Euclidean ring R a nonunit π is said to be a *prime element* of R if whenever $\pi = ab$, where a, b are in R, then one of a or b is a unit in R.

A prime element is thus an element in R which cannot be factored in R in a nontrivial way.

LEMMA 3.7.4 *Let R be a Euclidean ring. Then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.*

Proof. The proof is by induction on $d(a)$.

If $d(a) = d(1)$ then a is a unit in R (Problem 3), and so in this case, the assertion of the lemma is correct.

We assume that the lemma is true for all elements x in R such that $d(x) < d(a)$. On the basis of this assumption we aim to prove it for a. This would complete the induction and prove the lemma.

If a is a prime element of R there is nothing to prove. So suppose that $a = bc$ where neither b nor c is a unit in R. By Lemma 3.7.3, $d(b) < d(bc) = d(a)$ and $d(c) < d(bc) = d(a)$. Thus by our induction hypothesis b and c can be written as a product of a finite number of prime elements of R; $b = \pi_1\pi_2 \cdots \pi_n$, $c = \pi_1'\pi_2' \cdots \pi_m'$ where the π's and π''s are prime elements of R. Consequently $a = bc = \pi_1\pi_2 \cdots \pi_n\pi_1'\pi_2' \cdots \pi_m'$ and in this way a has been factored as a product of a finite number of prime elements. This completes the proof.

DEFINITION In the Euclidean ring R, a and b in R are said to be *relatively prime* if their greatest common divisor is a unit of R.

Since any associate of a greatest common divisor is a greatest common divisor, and since 1 is an associate of any unit, if a and b are relatively prime we may assume that $(a, b) = 1$.

LEMMA 3.7.5 *Let R be a Euclidean ring. Suppose that for $a, b, c \in R$, $a \mid bc$ but $(a, b) = 1$. Then $a \mid c$.*

Proof. As we have seen in Lemma 3.7.1, the greatest common divisor of a and b can be realized in the form $\lambda a + \mu b$. Thus by our assumptions, $\lambda a + \mu b = 1$. Multiplying this relation by c we obtain $\lambda ac + \mu bc = c$. Now $a \mid \lambda ac$, always, and $a \mid \mu bc$ since $a \mid bc$ by assumption; therefore $a \mid (\lambda ac + \mu bc) = c$. This is, of course, the assertion of the lemma.

We wish to show that prime elements in a Euclidean ring play the same role that prime numbers play in the integers. If π in R is a prime element of R and $a \in R$, then either $\pi \mid a$ or $(\pi, a) = 1$, for, in particular, (π, a) is a divisor of π so it must be π or 1 (or any unit). If $(\pi, a) = 1$, one-half our assertion is true; if $(\pi, a) = \pi$, since $(\pi, a) \mid a$ we get $\pi \mid a$, and the other half of our assertion is true.

LEMMA 3.7.6 *If π is a prime element in the Euclidean ring R and $\pi \mid ab$ where $a, b \in R$ then π divides at least one of a or b.*

Proof. Suppose that π does not divide a; then $(\pi, a) = 1$. Applying Lemma 3.7.5 we are led to $\pi \mid b$.

COROLLARY *If π is a prime element in the Euclidean ring R and $\pi \mid a_1a_2 \cdots a_n$ then π divides at least one $a_1, a_2, \ldots, a_n$.*

We carry the analogy between prime elements and prime numbers further and prove

THEOREM 3.7.2 (UNIQUE FACTORIZATION THEOREM) *Let R be a Euclidean ring and $a \neq 0$ a nonunit in R. Suppose that $a = \pi_1\pi_2 \cdots \pi_n = \pi'_1\pi'_2 \cdots \pi'_m$ where the π_i and π'_j are prime elements of R. Then $n = m$ and each π_i, $1 \leq i \leq n$ is an associate of some π'_j, $1 \leq j \leq m$ and conversely each π'_k is an associate of some π_q.*

Proof. Look at the relation $a = \pi_1\pi_2 \cdots \pi_n = \pi'_1\pi'_2 \cdots \pi'_m$. But $\pi_1 \mid \pi_1\pi_2 \cdots \pi_n$, hence $\pi_1 \mid \pi'_1\pi'_2 \cdots \pi'_m$. By Lemma 3.7.6, π_1 must divide some π'_i; since π_1 and π'_i are both prime elements of R and $\pi_1 \mid \pi'_i$ they must be associates and $\pi'_i = u_1\pi_1$, where u_1 is a unit in R. Thus $\pi_1\pi_2 \cdots \pi_n = \pi'_1\pi'_2 \cdots \pi'_m = u_1\pi_1\pi'_2 \cdots \pi'_{i-1}\pi'_{i+1} \cdots \pi'_m$; cancel off π_1 and we are left with $\pi_2 \cdots \pi_n = u_1\pi'_2 \cdots \pi'_{i-1}\pi'_{i+1} \cdots \pi'_m$. Repeat the argument on this relation with π_2. After n steps, the left side becomes 1, the right side a product of a certain number of π' (the excess of m over n). This would force $n \leq m$ since the π' are not units. Similarly, $m \leq n$, so that $n = m$. In the process we have also showed that every π_i has some π'_i as an associate and conversely.

Combining Lemma 3.7.4 and Theorem 3.7.2 we have that *every nonzero element in a Euclidean ring R can be uniquely written (up to associates) as a product of prime elements or is a unit in R.*

We finish the section by determining all the maximal ideals in a Euclidean ring.

In Theorem 3.7.1 we proved that any ideal A in the Euclidean ring R is of the form $A = (a_0)$ where $(a_0) = \{xa_0 \mid x \in R\}$. We now ask: What conditions imposed on a_0 insure that A is a maximal ideal of R? For this question we have a simple, precise answer, namely

LEMMA 3.7.7 *The ideal $A = (a_0)$ is a maximal ideal of the Euclidean ring R if and only if a_0 is a prime element of R.*

Proof. We first prove that if a_0 is not a prime element, then $A = (a_0)$ is not a maximal ideal. For, suppose that $a_0 = bc$ where $b, c \in R$ and neither b nor c is a unit. Let $B = (b)$; then certainly $a_0 \in B$ so that $A \subset B$. We claim that $A \neq B$ and that $B \neq R$.

If $B = R$ then $1 \in B$ so that $1 = xb$ for some $x \in R$, forcing b to be a unit in R, which it is not. On the other hand, if $A = B$ then $b \in B = A$ whence $b = xa_0$ for some $x \in R$. Combined with $a_0 = bc$ this results in $a_0 = xca_0$, in consequence of which $xc = 1$. But this forces c to be a unit in R, again contradicting our assumption. Therefore B is neither A nor R and since $A \subset B$, A cannot be a maximal ideal of R.

Conversely, suppose that a_0 is a prime element of R and that U is an ideal of R such that $A = (a_0) \subset U \subset R$. By Theorem 3.7.1, $U = (u_0)$. Since $a_0 \in A \subset U = (u_0)$, $a_0 = xu_0$ for some $x \in R$. But a_0 is a prime element of R, from which it follows that either x or u_0 is a unit in R. If u_0

is a unit in R then $U = R$ (see Problem 5). If, on the other hand, x is a unit in R, then $x^{-1} \in R$ and the relation $a_0 = xu_0$ becomes $u_0 = x^{-1}a_0 \in A$ since A is an ideal of R. This implies that $U \subset A$; together with $A \subset U$ we conclude that $U = A$. Therefore there is no ideal of R which fits strictly between A and R. This means that A is a maximal ideal of R.

Problems

1. In a commutative ring with unit element prove that the relation a is an associate of b is an equivalence relation.
2. In a Euclidean ring prove that any two greatest common divisors of a and b are associates.
3. Prove that a necessary and sufficient condition that the element a in the Euclidean ring be a unit is that $d(a) = d(1)$.
4. Prove that in a Euclidean ring (a, b) can be found as follows:

$$\begin{aligned} b &= q_0 a + r_1, && \text{where} \quad d(r_1) < d(a) \\ a &= q_1 r_1 + r_2, && \text{where} \quad d(r_2) < d(r_1) \\ r_1 &= q_2 r_2 + r_3, && \text{where} \quad d(r_3) < d(r_2) \\ &\vdots && \qquad\qquad \vdots \\ r_{n-1} &= q_n r_n \end{aligned}$$

and $r_n = (a, b)$.

5. Prove that if an ideal U of a ring R contains a unit of R, then $U = R$.
6. Prove that the units in a commutative ring with a unit element form an abelian group.
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 $[a, b] = ab/(a, b)$.

3.8 A Particular Euclidean Ring

An abstraction in mathematics gains in substance and importance when, particularized to a specific example, it sheds new light on this example. We are about to particularize the notion of a Euclidean ring to a concrete ring, the ring of Gaussian integers. Applying the general results obtained about Euclidean rings to the Gaussian integers we shall obtain a highly nontrivial theorem about prime numbers due to Fermat.

Let $J[i]$ denote the set of all complex numbers of the form $a + bi$ where a and b are integers. Under the usual addition and multiplication of complex numbers $J[i]$ forms an integral domain called the domain of *Gaussian integers*.

Our first objective is to exhibit $J[i]$ as a Euclidean ring. In order to do this we must first introduce a function $d(x)$ defined for every nonzero element in $J[i]$ which satisfies

1. $d(x)$ is a nonnegative integer for every $x \neq 0 \in J[i]$.
2. $d(x) \leq d(xy)$ for every $y \neq 0$ in $J[i]$.
3. Given $u, v \in J[i]$ there exist $t, r \in J[i]$ such that $v = tu + r$ where $r = 0$ or $d(r) < d(u)$.

Our candidate for this function d is the following: if $x = a + bi \in J[i]$, then $d(x) = a^2 + b^2$. The $d(x)$ so defined certainly satisfies property 1; in fact, if $x \neq 0 \in J[i]$ then $d(x) \geq 1$. As is well known, for any two complex numbers (not necessarily in $J[i]$) x, y, $d(xy) = d(x)d(y)$; thus if x and y are in addition in $J[i]$ and $y \neq 0$, then since $d(y) \geq 1$, $d(x) = d(x)1 \leq d(x)d(y) = d(xy)$, showing that condition 2 is satisfied. All our effort now will be to show that condition 3 also holds for this function d in $J[i]$. This is done in the proof of

THEOREM 3.8.1 *$J[i]$ is a Euclidean ring.*

Proof. As was remarked in the discussion above, to prove Theorem 3.8.1 we merely must show that, given $x, y \in J[i]$ there exists $t, r \in J[i]$ such that $y = tx + r$ where $r = 0$ or $d(r) < d(x)$.

We first establish this for a very special case, namely, where y is arbitrary in $J[i]$ but where x is an (ordinary) positive integer n. Suppose that $y = a + bi$; by the division algorithm for the ring of integers we can find integers u, v such that $a = un + u_1$ and $b = vn + v_1$ where u_1 and v_1 are integers satisfying $|u_1| \leq \frac{1}{2}n$ and $|v_1| \leq \frac{1}{2}n$. Let $t = u + vi$ and $r = u_1 + v_1 i$; then $y = a + bi = un + u_1 + (vn + v_1)i = (u + vi)n + u_1 + v_1 i = tn + r$. Since $d(r) = d(u_1 + v_1 i) = {u_1}^2 + {v_1}^2 \leq n^2/4 + n^2/4 < n^2 = d(n)$, we see that in this special case we have shown that $y = tn + r$ with $r = 0$ or $d(r) < d(n)$.

We now go to the general case; let $x \neq 0$ and y be arbitrary elements in $J[i]$. Thus $x\bar{x}$ is a positive integer n where $\bar{x}$ is the complex conjugate of x. Applying the result of the paragraph above to the elements $y\bar{x}$ and n we see that there are elements $t, r \in J[i]$ such that $y\bar{x} = tn + r$ with $r = 0$ or $d(r) < d(n)$. Putting into this relation $n = x\bar{x}$ we obtain $d(y\bar{x} - tx\bar{x}) < d(n) = d(x\bar{x})$; applying to this the fact that $d(y\bar{x} - tx\bar{x}) = d(y - tx)d(\bar{x})$ and $d(x\bar{x}) = d(x)d(\bar{x})$ we obtain that $d(y - tx)d(\bar{x}) < d(x)d(\bar{x})$. Since $x \neq 0$, $d(\bar{x})$ is a positive integer, so this inequality simplifies to $d(y - tx) < d(x)$. We represent $y = tx + r_0$, where $r_0 = y - tx$; thus t and r_0 are in

$J[i]$ and as we saw above, $r_0 = 0$ or $d(r_0) = d(y - tx) < d(x)$. This proves the theorem.

Since $J[i]$ has been proved to be a Euclidean ring, we are free to use the results established about this class of rings in the previous section to the Euclidean ring we have at hand, $J[i]$.

LEMMA 3.8.1 *Let p be a prime integer and suppose that for some integer c relatively prime to p we can find integers x and y such that $x^2 + y^2 = cp$. Then p can be written as the sum of squares of two integers, that is, there exist integers a and b such that $p = a^2 + b^2$.*

Proof. The ring of integers is a subring of J[i]. Suppose that the integer p is also a prime element of $J[i]$. Since $cp = x^2 + y^2 = (x + yi)(x - yi)$, by Lemma 3.7.6, $p \mid (x + yi)$ or $p \mid (x - yi)$ in $J[i]$. But if $p \mid (x + yi)$ then $x + yi = p(u + vi)$ which would say that $x = pu$ and $y = pv$ so that p also would divide $x - yi$. But then $p^2 \mid (x + yi)(x - yi) = cp$ from which we would conclude that $p \mid c$ contrary to assumption. Similarly if $p \mid (x - yi)$. Thus p is *not* a prime element in $J[i]$! In consequence of this,

$$p = (a + bi)(g + di)$$

where $a + bi$ and $g + di$ are in $J[i]$ and where neither $a + bi$ nor $g + di$ is a unit in $J[i]$. But this means that neither $a^2 + b^2 = 1$ nor $g^2 + d^2 = 1$. (See Problem 2.) From $p = (a + bi)(g + di)$ it follows easily that $p = (a - bi)(g - di)$. Thus

$$p^2 = (a + bi)(g + di)(a - bi)\ (g - di) = (a^2 + b^2)(g^2 + d^2).$$

Therefore $(a^2 + b^2) \mid p^2$ so $a^2 + b^2 = 1$, p or p^2; $a^2 + b^2 \neq 1$ since $a + bi$ is not a unit, in $J[i]$; $a^2 + b^2 \neq p^2$, otherwise $g^2 + d^2 = 1$, contrary to the fact that $g + di$ is not a unit in $J[i]$. Thus the only feasibility left is that $a^2 + b^2 = p$ and the lemma is thereby established.

The odd prime numbers divide into two classes, those which have a remainder of 1 on division by 4 and those which have a remainder of 3 on division by 4. We aim to show that every prime number of the first kind can be written as the sum of two squares, whereas no prime in the second class can be so represented.

LEMMA 3.8.2 *If p is a prime number of the form $4n + 1$, then we can solve the congruence $x^2 \equiv -1 \bmod p$.*

Proof. Let $x = 1 \cdot 2 \cdot 3 \cdots (p - 1)/2$. Since $p - 1 = 4n$, in this product for x there are an even number of terms, in consequence of which

$$x = (-1)(-2)(-3) \cdots \left(-\left(\frac{p-1}{2}\right)\right).$$

But $p - k \equiv -k \bmod p$, so that

$$x^2 \equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)(-1)(-2)\cdots\left(-\left(\frac{p-1}{2}\right)\right)$$

$$\equiv 1 \cdot 2 \cdots \frac{p-1}{2}\frac{p+1}{2}\cdots(p-1)$$

$$\equiv (p-1)! = -1 \bmod p.$$

We are using here Wilson's theorem, proved earlier, namely that if p is a prime number $(p-1)! \equiv -1(p)$.

To illustrate this result, if $p = 13$,

$$x = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720 = 5 \bmod 13 \text{ and } 5^2 = -1 \bmod 13.$$

THEOREM 3.8.2 (FERMAT) *If p is a prime number of the form $4n + 1$, then $p = a^2 + b^2$ for some integers a, b.*

Proof. By Lemma 3.8.2 there exists an x such that $x^2 \equiv -1 \bmod p$. The x can be chosen so that $0 \leq x \leq p - 1$ since we only need to use the remainder of x on division by p. We can restrict the size of x even further, namely to satisfy $|x| \leq p/2$. For if $x > p/2$, then $y = p - x$ satisfies $y^2 \equiv -1 \bmod p$ but $|y| \leq p/2$. Thus we may assume that we have an integer x such that $|x| \leq p/2$ and $x^2 + 1$ is a multiple of p, say cp. Now $cp = x^2 + 1 \leq p^2/4 + 1 < p^2$, hence $c < p$ and so $p \nmid c$. Invoking Lemma 3.8.1 we obtain that $p = a^2 + b^2$ for some integers a and b, proving the theorem.

Problems

1. Find all the units in $J[i]$.
2. If $a + bi$ is not a unit of $J[i]$ prove that $a^2 + b^2 > 1$.
3. Find the greatest common divisor in $J[i]$ of
   (a) $3 + 4i$ and $4 - 3i$. (b) $11 + 7i$ and $18 - i$.
4. Prove that if p is a prime number of the form $4n + 3$, then there is no x such that $x^2 \equiv -1 \bmod p$.
5. Prove that no prime of the form $4n + 3$ can be written as $a^2 + b^2$ where a and b are integers.
6. Prove that there is an infinite number of primes of the form $4n + 3$.

*7. Prove there exists an infinite number of primes of the form $4n + 1$.

*8. Determine all the prime elements in $J[i]$.

*9. Determine all positive integers which can be written as a sum of two squares (of integers).

3.9 Polynomial Rings

Very early in our mathematical education—in fact in junior high school or early in high school itself—we are introduced to polynomials. For a seemingly endless amount of time we are drilled, to the point of utter boredom, in factoring them, multiplying them, dividing them, simplifying them. Facility in factoring a quadratic becomes confused with genuine mathematical talent.

Later, at the beginning college level, polynomials make their appearance in a somewhat different setting. Now they are functions, taking on values, and we become concerned with their continuity, their derivatives, their integrals, their maxima and minima.

We too shall be interested in polynomials but from neither of the above viewpoints. To us polynomials will simply be elements of a certain ring and we shall be concerned with algebraic properties of this ring. Our primary interest in them will be that they give us a Euclidean ring whose properties will be decisive in discussing fields and extensions of fields.

Let F be a field. By the *ring of polynomials* in the indeterminate, x, written as $F[x]$, we mean the set of all symbols $a_0 + a_1x + \cdots + a_nx^n$, where n can be any nonnegative integer and where the coefficients $a_1, a_2, \ldots, a_n$ are all in F. In order to make a ring out of $F[x]$ we must be able to recognize when two elements in it are equal, we must be able to add and multiply elements of $F[x]$ so that the axioms defining a ring hold true for $F[x]$. This will be our initial goal.

We could avoid the phrase "the set of all symbols" used above by introducing an appropriate apparatus of sequences but it seems more desirable to follow a path which is somewhat familiar to most readers.

DEFINITION If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$ are in $F[x]$, then $p(x) = q(x)$ if and only if for every integer $i \geq 0$, $a_i = b_i$.

Thus two polynomials are declared to be equal if and only if their corresponding coefficients are equal.

DEFINITION If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$ are both in $F[x]$, then $p(x) + q(x) = c_0 + c_1x + \cdots + c_tx^t$ where for each i, $c_i = a_i + b_i$.

In other words, add two polynomials by adding their coefficients and collecting terms. To add $1 + x$ and $3 - 2x + x^2$ we consider $1 + x$ as $1 + x + 0x^2$ and add, according to the recipe given in the definition, to obtain as their sum $4 - x + x^2$.

The most complicated item, and the only one left for us to define for $F[x]$, is the multiplication.

DEFINITION If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$, then $p(x)q(x) = c_0 + c_1x + \cdots + c_kx^k$ where $c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \cdots + a_0b_t$.

This definition says nothing more than: multiply the two polynomials by multiplying out the symbols formally, use the relation $x^\alpha x^\beta = x^{\alpha+\beta}$, and collect terms. Let us illustrate the definition with an example:

$$p(x) = 1 + x - x^2, \qquad q(x) = 2 + x^2 + x^3.$$

Here $a_0 = 1$, $a_1 = 1$, $a_2 = -1$, $a_3 = a_4 = \cdots = 0$, and $b_0 = 2$, $b_1 = 0$, $b_2 = 1$, $b_3 = 1$, $b_4 = b_5 = \cdots = 0$. Thus

$$c_0 = a_0b_0 = 1.2 = 2,$$

$$c_1 = a_1b_0 + a_0b_1 = 1.2 + 1.0 = 2,$$

$$c_2 = a_2b_0 + a_1b_1 + a_0b_2 = (-1)(2) + 1.0 + 1.1 = -1,$$

$$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = (0)(2) + (-1)(0) + 1.1 + 1.1 = 2,$$

$$\begin{aligned} c_4 &= a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 \\ &= (0)(2) + (0)(0) + (-1)(1) + (1)(1) + 1(0) = 0, \end{aligned}$$

$$\begin{aligned} c_5 &= a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 \\ &= (0)(2) + (0)(0) + (0)(1) + (-1)(1) + (1)(0) + (0)(0) = -1, \end{aligned}$$

$$\begin{aligned} c_6 &= a_6b_0 + a_5b_1 + a_4b_2 + a_3b_3 + a_2b_4 + a_1b_5 + a_0b_6 \\ &= (0)(2) + (0)(0) + (0)(1) + (0)(1) + (-1)(0) + (1)(0) + (1)(0) = 0, \end{aligned}$$

$$c_7 = c_8 = \cdots = 0.$$

Therefore according to our definition,

$$(1 + x - x^2)(2 + x^2 + x^3) = c_0 + c_1x + \cdots = 2 + 2x - x^2 + 2x^3 - x^5.$$

If you multiply these together high-school style you will see that you get the same answer. Our definition of product is the one the reader has always known.

Without further ado we assert that $F[x]$ is a ring with these operations, its multiplication is commutative, and it has a unit element. We leave the verification of the ring axioms to the reader.

DEFINITION If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$ then the *degree* of $f(x)$, written as $\deg f(x)$, is n.

That is, the degree of $f(x)$ is the largest integer i for which the ith coefficient of $f(x)$ is not 0. We do not define the degree of the zero polynomial. We say a polynomial is a *constant* if its degree is 0. The degree

function defined on the nonzero elements of $F[x]$ will provide us with the function $d(x)$ needed in order that $F[x]$ be a Euclidean ring.

LEMMA 3.9.1 *If $f(x)$, $g(x)$ are two nonzero elements of $F[x]$, then*

$$\deg (f(x)g(x)) = \deg f(x) + \deg g(x).$$

Proof. Suppose that $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ and that $a_m \neq 0$ and $b_n \neq 0$. Therefore $\deg f(x) = m$ and $\deg g(x) = n$. By definition, $f(x)g(x) = c_0 + c_1x + \cdots + c_kx^k$ where $c_t = a_tb_0 + a_{t-1}b_1 + \cdots + a_1b_{t-1} + a_0b_t$. We claim that $c_{m+n} = a_mb_n \neq 0$ and $c_i = 0$ for $i > m + n$. That $c_{m+n} = a_mb_n$ can be seen at a glance by its definition. What about c_i for $i > m + n$? c_i is the sum of terms of the form a_jb_{i-j}; since $i = j + (i - j) > m + n$ then either $j > m$ or $(i - j) > n$. But then one of a_j or b_{i-j} is 0, so that $a_jb_{i-j} = 0$; since c_i is the sum of a bunch of zeros it itself is 0, and our claim has been established. Thus the highest nonzero coefficient of $f(x)g(x)$ is c_{m+n}, whence $\deg f(x)g(x) = m + n = \deg f(x) + \deg g(x)$.

COROLLARY *If $f(x)$, $g(x)$ are nonzero elements in $F[x]$ then* $\deg f(x) \leq \deg f(x)g(x)$.

Proof. Since $\deg f(x)g(x) = \deg f(x) + \deg g(x)$, and since $\deg g(x) \geq 0$, this result is immediate from the lemma.

COROLLARY *$F[x]$ is an integral domain.*

We leave the proof of this corollary to the reader.

Since $F[x]$ is an integral domain, in light of Theorem 3.6.1 we can construct for it its field of quotients. This field merely consists of all quotients of polynomials and is called the field of *rational functions* in x over F.

The function $\deg f(x)$ defined for all $f(x) \neq 0$ in $F[x]$ satisfies

1. $\deg f(x)$ is a nonnegative integer.
2. $\deg f(x) \leq \deg f(x)g(x)$ for all $g(x) \neq 0$ in $F[x]$.

In order for $F[x]$ to be a Euclidean ring with the degree function acting as the d-function of a Euclidean ring we still need that given $f(x)$, $g(x) \in F[x]$, there exist $t(x)$, $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. This is provided us by

LEMMA 3.9.2 (THE DIVISION ALGORITHM) *Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, then there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.*

Proof. The proof is actually nothing more than the "long-division" process we all used in school to divide one polynomial by another.

If the degree of $f(x)$ is smaller than that of $g(x)$ there is nothing to prove, for merely put $t(x) = 0$, $r(x) = f(x)$, and we certainly have that $f(x) = 0g(x) + f(x)$ where $\deg f(x) < \deg g(x)$ or $f(x) = 0$.

So we may assume that $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ where $a_m \neq 0$, $b_n \neq 0$ and $m \geq n$.

Let $f_1(x) = f(x) - (a_m/b_n)x^{m-n}g(x)$; thus $\deg f_1(x) \leq m - 1$, so by induction on the degree of $f(x)$ we may assume that $f_1(x) = t_1(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. But then $f(x) - (a_m/b_n)x^{m-n}g(x) = t_1(x)g(x) + r(x)$, from which, by transposing, we arrive at $f(x) = ((a_m/b_n)x^{m-n} + t_1(x))g(x) + r(x)$. If we put $t(x) = (a_m/b_n)x^{m-n} + t_1(x)$ we do indeed have that $f(x) = t(x)g(x) + r(x)$ where $t(x)$, $r(x) \in F[x]$ and where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. This proves the lemma.

This last lemma fills the gap needed to exhibit $F[x]$ as a Euclidean ring and we now have the right to say

THEOREM 3.9.1 *$F[x]$ is a Euclidean ring.*

All the results of Section 3.7 now carry over and we list these, for our particular case, as the following lemmas. It could be very instructive for the reader to try to prove these directly, adapting the arguments used in Section 3.7 for our particular ring $F[x]$ and its Euclidean function, the degree.

LEMMA 3.9.3 *$F[x]$ is a principal ideal ring.*

LEMMA 3.9.4 *Given two polynomials $f(x)$, $g(x)$ in $F[x]$ they have a greatest common divisor $d(x)$ which can be realized as $d(x) = \lambda(x)f(x) + \mu(x)g(x)$.*

What corresponds to a prime element?

DEFINITION A polynomial $p(x)$ in $F[x]$ is said to be *irreducible* over F if whenever $p(x) = a(x)b(x)$ with $a(x)$, $b(x) \in F[x]$, then one of $a(x)$ or $b(x)$ has degree 0 (i.e., is a constant).

Irreducibility depends on the field; for instance the polynomial $x^2 + 1$ is irreducible over the real field but not over the complex field, for there $x^2 + 1 = (x + i)(x - i)$ where $i^2 = -1$.

LEMMA 3.9.5 *Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.*

LEMMA 3.9.6 *The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F.*

In Chapter 5 we shall return to take a much closer look at this field $F[x]/(p(x))$, but for now we should like to compute an example.

Let F be the field of rational numbers and consider the polynomial $p(x) = x^3 - 2$ in $F[x]$. As is easily verified, it is irreducible over F, whence $F[x]/(x^3 - 2)$ is a field. What do its elements look like? Let $A = (x^3 - 2)$, the ideal in $F[x]$ generated by $x^3 - 2$.

Any element in $F[x]/(x^3 - 2)$ is a coset of the form $f(x) + A$ of the ideal A with $f(x)$ in $F[x]$. Now, given any polynomial $f(x) \in F[x]$, by the division algorithm, $f(x) = t(x)(x^3 - 2) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg (x^3 - 2) = 3$. Thus $r(x) = a_0 + a_1x + a_2x^2$ where a_0, a_1, a_2 are in F; consequently $f(x) + A = a_0 + a_1x + a_2x^2 + t(x)(x^3 - 2) + A = a_0 + a_1x + a_2x^2 + A$ since $t(x)(x^3 - 2)$ is in A, hence by the addition and multiplication in $F[x]/(x^3 - 2)$, $f(x) + A = (a_0 + A) + a_1(x + A) + a_2(x + A)^2$. If we put $t = x + A$, then every element in $F[x]/(x^3 - 2)$ is of the form $a_0 + a_1t + a_2t^2$ with a_0, a_1, a_2 in F. What about t? Since $t^3 - 2 = (x + A)^3 - 2 = x^3 - 2 + A = A = 0$ (since A is the zero element of $F[x]/(x^3 - 2)$) we see that $t^3 = 2$.

Also, if $a_0 + a_1t + a_2t^2 = b_0 + b_1t + b_2t^2$, then $(a_0 - b_0) + (a_1 - b_1)t + (a_2 - b_2)t^2 = 0$, whence $(a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2$ is in $A = (x^3 - 2)$. How can this be, since every element in A has degree at least 3? Only if $a_0 - b_0 + (a_1 - b_1)x + (a_2 - b_2)x^2 = 0$, that is, only if $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2$. Thus every element in $F[x]/(x^3 - 2)$ has a *unique* representation as $a_0 + a_1t + a_2t^2$ where $a_0, a_1, a_2 \in F$. By Lemma 3.9.6, $F[x]/(x^3 - 2)$ is a field. It would be instructive to see this directly; all that it entails is proving that if $a_0 + a_1t + a_2t^2 \neq 0$ then it has an inverse of the form $\alpha + \beta t + \gamma t^2$. Hence we must solve for α, β, γ in the relation $(a_0 + a_1t + a_2t^2)(\alpha + \beta t + \gamma t^2) = 1$, where not all of a_0 a_1, a_2 are 0. Multiplying the relation out and using $t^3 = 2$ we obtain $(a_0\alpha + 2a_2\beta + 2a_1\gamma) + (a_1\alpha + a_0\beta + 2a_2\gamma)t + (a_2\alpha + a_1\beta + a_0\gamma)t^2 = 1$; thus

$$a_0\alpha + 2a_2\beta + 2a_1\gamma = 1,$$

$$a_1\alpha + a_0\beta + 2a_2\gamma = 0,$$

$$a_2\alpha + a_1\beta + a_0\gamma = 0.$$

We can try to solve these three equations in the three unknowns α, β, γ. When we do so we find that a solution exists if and only if

$$a_0^3 + 2a_1^3 + 4a_2^3 - 6a_0a_1a_2 \neq 0.$$

Therefore the problem of proving directly that $F[x]/(x^3 - 2)$ is a field boils down to proving that the only solution in *rational* numbers of

$$a_0^3 + 2a_1^3 + 4a_2^3 = 6a_0a_1a_2 \tag{1}$$

is the solution $a_0 = a_1 = a_2 = 0$. We now proceed to show this. If a solution exists in rationals, by clearing of denominators we can show that a solution exists where a_0, a_1, a_2 are integers. Thus we may assume that a_0, a_1, a_2 are integers satisfying (1). We now assert that we may assume that a_0, a_1, a_2 have no common divisor other than 1, for if $a_0 = b_0 d$, $a_1 = b_1 d$, and $a_2 = b_2 d$, where d is their greatest common divisor, then substituting in (1) we obtain $d^3(b_0^3 + 2b_1^3 + 4b_2^3) = d^3(6b_0b_1b_2)$, and so $b_0^3 + 2b_1^3 + 4b_2^3 = 6b_0b_1b_2$. The problem has thus been reduced to proving that (1) has no solutions in integers which are relatively prime. But then (1) implies that a_0^3 is even, so that a_0 is even; substituting $a_0 = 2\alpha_0$ in (1) gives us $4\alpha_0^3 + a_1^3 + 2a_2^3 = 6\alpha_0 a_1 a_2$. Thus a_1^3, and so, a_1 is even; $a_1 = 2\alpha_1$. Substituting in (1) we obtain $2\alpha_0^3 + 4\alpha_1^3 + a_2^3 = 6\alpha_0\alpha_1 a_2$. Thus a_2^3, and so a_2, is even! But then a_0, a_1, a_2 have 2 as a common factor! This contradicts that they are relatively prime, and we have proved that the equation $a_0^3 + 2a_1^3 + 4a_2^3 = 6a_0a_1a_2$ has no rational solution other than $a_0 = a_1 = a_2 = 0$. Therefore we can solve for α, β, γ and $F[x]/(x^3 - 2)$ is seen, directly, to be a field.

Problems

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 $x^6 + x^3 + x + 1$.
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.
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 $K[x]$.
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.
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.

*6. Define the *derivative* $f'(x)$ of the polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

as

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}.$$

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.

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.

3.10 Polynomials over the Rational Field

We specialize the general discussion to that of polynomials whose coefficients are rational numbers. Most of the time the coefficients will actually be integers. For such polynomials we shall be concerned with their irreducibility.

DEFINITION The polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where the $a_0, a_1, a_2, \ldots, a_n$ are integers is said to be *primitive* if the greatest common divisor of $a_0, a_1, \ldots, a_n$ is 1.

LEMMA 3.10.1 *If $f(x)$ and $g(x)$ are primitive polynomials, then $f(x)g(x)$ is a primitive polynomial.*

Proof. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$. Suppose that the lemma was false; then all the coefficients of $f(x)g(x)$ would be divisible by some integer larger than 1, hence by some prime number p. Since $f(x)$ is primitive, p does not divide some coefficient a_i. Let a_j be the first coefficient of $f(x)$ which p does not divide. Similarly let b_k be the first coefficient of $g(x)$ which p does not divide. In $f(x)g(x)$ the coefficient of x^{j+k}, c_{j+k}, is

$$c_{j+k} = a_jb_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0) + (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0b_{j+k}). \quad (1)$$

Now by our choice of b_k, $p \mid b_{k-1}, b_{k-2}, \ldots$ so that $p \mid (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0)$. Similarly, by our choice of a_j, $p \mid a_{j-1}, a_{j-2}, \ldots$ so that $p \mid (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0b_{k+j})$. By assumption, $p \mid c_{j+k}$. Thus by (1), $p \mid a_jb_k$, which is nonsense since $p \nmid a_j$ and $p \nmid b_k$. This proves the lemma.

DEFINITION The *content* of the polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where the a's are integers, is the greatest common divisor of the integers $a_0, a_1, \ldots, a_n$.

Clearly, given any polynomial $p(x)$ with integer coefficients it can be written as $p(x) = dq(x)$ where d is the content of $p(x)$ and where $q(x)$ is a primitive polynomial.

THEOREM 3.10.1 (GAUSS' LEMMA) *If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.*

Proof. Suppose that $f(x) = u(x)v(x)$ where $u(x)$ and $v(x)$ have rational coefficients. By clearing of denominators and taking out common factors we can then write $f(x) = (a/b)\lambda(x)\mu(x)$ where a and b are integers and where both $\lambda(x)$ and $\mu(x)$ have integer coefficients and are primitive. Thus $bf(x) = a\lambda(x)\mu(x)$. The content of the left-hand side is b, since $f(x)$ is primitive; since both $\lambda(x)$ and $\mu(x)$ are primitive, by Lemma 3.10.1 $\lambda(x)\mu(x)$ is primitive, so that the content of the right-hand side is a. Therefore $a = b$, $(a/b) = 1$, and $f(x) = \lambda(x)\mu(x)$ where $\lambda(x)$ and $\mu(x)$ have integer coefficients. This is the assertion of the theorem.

DEFINITION A polynomial is said to be *integer monic* if all its coefficients are integers and its highest coefficient is 1.

Thus an integer monic polynomial is merely one of the form $x^n + a_1x^{n-1} + \cdots + a_n$ where the a's are integers. Clearly an integer monic polynomial is primitive.

COROLLARY *If an integer monic polynomial factors as the product of two non-constant polynomials having rational coefficients then it factors as the product of two integer monic polynomials.*

We leave the proof of the corollary as an exercise for the reader.

The question of deciding whether a given polynomial is irreducible or not can be a difficult and laborious one. Few criteria exist which declare that a given polynomial is or is not irreducible. One of these few is the following result:

THEOREM 3.10.2 (THE EISENSTEIN CRITERION) *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial with integer coefficients. Suppose that for some prime number p, $p \nmid a_n$, $p \mid a_1, p \mid a_2, \ldots, p \mid a_0$, $p^2 \nmid a_0$. Then $f(x)$ is irreducible over the rationals.*

Proof. Without loss of generality we may assume that $f(x)$ is primitive, for taking out the greatest common factor of its coefficients does not disturb the hypotheses, since $p \nmid a_n$. If $f(x)$ factors as a product of two rational polynomials, by Gauss' lemma it factors as the product of two polynomials having integer coefficients. Thus if we assume that $f(x)$ is reducible, then

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s),$$

where the b's and c's are integers and where $r > 0$ and $s > 0$. Reading off

the coefficients we first get $a_0 = b_0c_0$. Since $p \mid a_0$, p must divide one of b_0 or c_0. Since $p^2 \nmid a_0$, p cannot divide both b_0 and c_0. Suppose that $p \mid b_0$, $p \nmid c_0$. Not all the coefficients $b_0, \ldots, b_r$ can be divisible by p; otherwise all the coefficients of $f(x)$ would be divisible by p, which is manifestly false since $p \nmid a_n$. Let b_k be the first b not divisible by p, $k \leq r < n$. Thus $p \mid b_{k-1}$ and the earlier b's. But $a_k = b_kc_0 + b_{k-1}c_1 + b_{k-2}c_2 + \cdots + b_0c_k$, and $p \mid a_k, p \mid b_{k-1}, b_{k-2}, \ldots, b_0$, so that $p \mid b_kc_0$. However, $p \nmid c_0, p \nmid b_k$, which conflicts with $p \mid b_kc_0$. This contradiction proves that we could not have factored $f(x)$ and so $f(x)$ is indeed irreducible.

Problems

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.
2. If p is a prime number, prove that the polynomial $x^n - p$ 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.)
4. If m and n are relatively prime integers and if

$$\left(x - \frac{m}{n}\right) \mid (a_0 + a_1x + \cdots + a_rx^r),$$

where the a's are integers, prove that $m \mid a_0$ and $n \mid a_r$.

5. If a is rational and $x - a$ divides an integer monic polynomial, prove that a must be an integer.

3.11 Polynomial Rings over Commutative Rings

In defining the polynomial ring in one variable over a field F, no essential use was made of the fact that F was a field; all that was used was that F was a commutative ring. The field nature of F only made itself felt in proving that $F[x]$ was a Euclidean ring.

Thus we can imitate what we did with fields for more general rings. While some properties may be lost, such as "Euclideanism," we shall see that enough remain to lead us to interesting results. The subject could have been developed in this generality from the outset, and we could have obtained the particular results about $F[x]$ by specializing the ring to be a field. However, we felt that it would be healthier to go from the concrete to the abstract rather than from the abstract to the concrete. The price we

pay for this is repetition, but even that serves a purpose, namely, that of consolidating the ideas. Because of the experience gained in treating polynomials over fields, we can afford to be a little sketchier in the proofs here.

Let R be a commutative ring with unit element. By *the polynomial ring in x over R*, $R[x]$, we shall mean the set of formal symbols $a_0 + a_1x + \cdots + a_mx^m$, where $a_0, a_1, \ldots, a_m$ are in R, and where equality, addition, and multiplication are defined exactly as they were in Section 3.9. As in that section, $R[x]$ is a commutative ring with unit element.

We now define the *ring of polynomials in the n-variables* $x_1, \ldots, x_n$ over R, $R[x_1, \ldots, x_n]$, as follows: Let $R_1 = R[x_1]$, $R_2 = R_1[x_2]$, the polynomial ring in x_2 over $R_1, \ldots, R_n = R_{n-1}[x_n]$. R_n is called the ring of polynomials in $x_1, \ldots, x_n$ over R. Its elements are of the form $\sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, where equality and addition are defined coefficientwise and where multiplication is defined by use of the distributive law and the rule of exponents $(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n})(x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}) = x_1^{i_1+j_1} x_2^{i_2+j_2} \cdots x_n^{i_n+j_n}$. Of particular importance is the case in which $R = F$ is a field; here we obtain the ring of polynomials in n-variables over a field.

Of interest to us will be the influence of the structure of R on that of $R[x_1, \ldots, x_n]$. The first result in this direction is

LEMMA 3.11.1 *If R is an integral domain, then so is $R[x]$.*

Proof. For $0 \neq f(x) = a_0 + a_1x + \cdots + a_mx^m$, where $a_m \neq 0$, in $R[x]$, we define the *degree* of $f(x)$ to be m; thus $\deg f(x)$ is the index of the highest nonzero coefficient of $f(x)$. If R is an integral domain we leave it as an exercise to prove that $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$. But then, for $f(x) \neq 0$, $g(x) \neq 0$, it is impossible to have $f(x)g(x) = 0$. That is, $R[x]$ is an integral domain.

Making successive use of the lemma immediately yields the

COROLLARY *If R is an integral domain, then so is $R[x_1, \ldots, x_n]$.*

In particular, when F is a field, $F[x_1, \ldots, x_n]$ must be an integral domain. As such, we can construct its field of quotients; *we call this the field of rational functions in $x_1, \ldots, x_n$ over F* and denote it by $F(x_1, \ldots, x_n)$. This field plays a vital role in algebraic geometry. For us it shall be of utmost importance in our discussion, in Chapter 5, of Galois theory.

However, we want deeper interrelations between the structures of R and of $R[x_1, \ldots, x_n]$ than that expressed in Lemma 3.11.1. Our development now turns in that direction.

Exactly in the same way as we did for Euclidean rings, we can speak about divisibility, units, etc., in arbitrary integral domains, R, with unit element. Two elements a, b in R are said to be *associates* if $a = ub$ where u

is a unit in R. An element a which is not a unit in R will be called *irreducible* (or a *prime element*) if, whenever $a = bc$ with b, c both in R, then one of b or c must be a unit in R. An irreducible element is thus an element which cannot be factored in a "nontrivial" way.

DEFINITION An integral domain, R, with unit element is a *unique factorization domain* if

a. Any nonzero element in R is either a unit or can be written as the product of a finite number of irreducible elements of R.
b. The decomposition in part (a) is unique up to the order and associates of the irreducible elements.

Theorem 3.7.2 asserts that a Euclidean ring is a unique factorization domain. The converse, however, is false; for example, the ring $F[x_1, x_2]$, where F is a field, is not even a principal ideal ring (hence is certainly not Euclidean), but as we shall soon see it is a unique factorization domain.

In general commutative rings we may speak about the greatest common divisors of elements; the main difficulty is that these, in general, might not exist. However, in unique factorization domains their existence is assured. This fact is not difficult to prove and we leave it as an exercise; equally easy are the other parts of

LEMMA 3.11.2 *If R is a unique factorization 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 $a \mid c$.*

COROLLARY *If $a \in R$ is an irreducible element and $a \mid bc$, then $a \mid b$ or $a \mid c$.*

We now wish to transfer the appropriate version of the Gauss lemma (Theorem 3.10.1), which we proved for polynomials with integer coefficients, to the ring $R[x]$, where R is a unique factorization domain.

Given the polynomial $f(x) = a_0 + a_1x + \cdots + a_mx^m$ in $R[x]$, then the *content of* $f(x)$ is defined to be the greatest common divisor of $a_0, a_1, \ldots, a_m$. It is unique within units of R. We shall denote the content of $f(x)$ by $c(f)$. A polynomial in $R[x]$ is said to be *primitive* if its content is 1 (that is, is a unit in R). Given any polynomial $f(x) \in R[x]$, we can write $f(x) = af_1(x)$ where $a = c(f)$ and where $f_1(x) \in R[x]$ is primitive. (Prove!) Except for multiplication by units of R this decomposition of $f(x)$, as an element of R by a primitive polynomial in $R[x]$, is unique. (Prove!)

The proof of Lemma 3.10.1 goes over completely to our present situation; the only change that must be made in the proof is to replace the prime number p by an irreducible element of R. Thus we have

LEMMA 3.11.3 *If R is a unique factorization domain, then the product of two primitive polynomials in $R[x]$ is again a primitive polynomial in $R[x]$.*

Given $f(x)$, $g(x)$ in $R[x]$ we can write $f(x) = af_1(x)$, $g(x) = bg_1(x)$, where $a = c(f)$, $b = c(g)$ and where $f_1(x)$ and $g_1(x)$ are primitive. Thus $f(x)g(x) = abf_1(x)g_1(x)$. By Lemma 3.11.3, $f_1(x)g_1(x)$ is primitive. Hence the content of $f(x)g(x)$ is ab, that is, it is $c(f)c(g)$. We have proved the

COROLLARY *If R is a unique factorization domain and if $f(x)$, $g(x)$ are in $R[x]$, then $c(fg) = c(f)c(g)$ (up to units).*

By a simple induction, the corollary extends to the product of a finite number of polynomials to read $c(f_1f_2 \cdots f_k) = c(f_1)c(f_2) \cdots c(f_k)$.

Let R be a unique factorization domain. Being an integral domain, by Theorem 3.6.1, it has a field of quotients F. We can consider $R[x]$ to be a subring of $F[x]$. Given any polynomial $f(x) \in F[x]$, then $f(x) = (f_0(x)/a)$, where $f_0(x) \in R[x]$ and where $a \in R$. (Prove!) It is natural to ask for the relation, in terms of reducibility and irreducibility, of a polynomial in $R[x]$ considered as a polynomial in the larger ring $F[x]$

LEMMA 3.11.4 *If $f(x)$ in $R[x]$ is both primitive and irreducible as an element of $R[x]$, then it is irreducible as an element of $F[x]$. Conversely, if the primitive element $f(x)$ in $R[x]$ is irreducible as an element of $F[x]$, it is also irreducible as an element of $R[x]$.*

Proof. Suppose that the primitive element $f(x)$ in $R[x]$ is irreducible in $R[x]$ but is reducible in $F[x]$. Thus $f(x) = g(x)h(x)$, where $g(x)$, $h(x)$ are in $F[x]$ and are of positive degree. Now $g(x) = (g_0(x)/a)$, $h(x) = (h_0(x)/b)$, where $a, b \in R$ and where $g_0(x), h_0(x) \in R[x]$. Also $g_0(x) = \alpha g_1(x)$, $h_0(x) = \beta h_1(x)$, where $\alpha = c(g_0)$, $\beta = c(h_0)$, and $g_1(x)$, $h_1(x)$ are primitive in $R[x]$. Thus $f(x) = (\alpha\beta/ab)g_1(x)h_1(x)$, whence $abf(x) = \alpha\beta g_1(x)h_1(x)$. By Lemma 3.11.3, $g_1(x)h_1(x)$ is primitive, whence the content of the right-hand side is $\alpha\beta$. Since $f(x)$ is primitive, the content of the left-hand side is ab; but then $ab = \alpha\beta$; the implication of this is that $f(x) = g_1(x)h_1(x)$, and we have obtained a nontrivial factorization of $f(x)$ in $R[x]$, contrary to hypothesis. (Note: this factorization is nontrivial since each of $g_1(x)$, $h_1(x)$ are of the same degree as $g(x)$, $h(x)$, so cannot be units in $R[x]$ (see Problem 4).) We leave the converse half of the lemma as an exercise.

LEMMA 3.11.5 *If R is a unique factorization domain and if $p(x)$ is a primitive polynomial in $R[x]$, then it can be factored in a unique way as the product of irreducible elements in $R[x]$.*

Proof. When we consider $p(x)$ as an element in $F[x]$, by Lemma 3.9.5, we can factor it as $p(x) = p_1(x) \cdots p_k(x)$, where $p_1(x), p_2(x), \ldots, p_k(x)$ are

irreducible polynomials in $F[x]$. Each $p_i(x) = (f_i(x)/a_i)$, where $f_i(x) \in R[x]$ and $a_i \in R$; moreover, $f_i(x) = c_i q_i(x)$, where $c_i = c(f_i)$ and where $q_i(x)$ is primitive in $R[x]$. Thus each $p_i(x) = (c_i q_i(x)/a_i)$, where $a_i, c_i \in R$ and where $q_i(x) \in R[x]$ is primitive. Since $p_i(x)$ is irreducible in $F[x]$, $q_i(x)$ must also be irreducible in $F[x]$, hence by Lemma 3.11.4 *it is irreducible in* $R[x]$.

Now

$$p(x) = p_1(x) \cdots p_k(x) = \frac{c_1 c_2 \cdots c_k}{a_1 a_2 \cdots a_k} q_1(x) \cdots q_k(x),$$

whence $a_1 a_2 \cdots a_k p(x) = c_1 c_2 \cdots c_k q_1(x) \cdots q_k(x)$. Using the primitivity of $p(x)$ and of $q_1(x) \cdots q_k(x)$, we can read off the content of the left-hand side as $a_1 a_2 \cdots a_k$ and that of the right-hand side as $c_1 c_2 \cdots c_k$. Thus $a_1 a_2 \cdots a_k = c_1 c_2 \cdots c_k$, hence $p(x) = q_1(x) \cdots q_k(x)$. We have factored $p(x)$, in $R[x]$, as a product of irreducible elements.

Can we factor it in another way? If $p(x) = r_1(x) \cdots r_k(x)$, where the $r_i(x)$ are irreducible in $R[x]$, by the primitivity of $p(x)$, each $r_i(x)$ must be primitive, *hence irreducible in* $F[x]$ by Lemma 3.11.4. But by Lemma 3.9.5 we know unique factorization in $F[x]$; the net result of this is that the $r_i(x)$ and the $q_i(x)$ are equal (up to associates) in some order, hence $p(x)$ has a unique factorization as a product of irreducibles in $R[x]$.

We now have all the necessary information to prove the principal theorem of this section.

THEOREM 3.11.1 *If R is a unique factorization domain, then so is $R[x]$.*

Proof. Let $f(x)$ be an arbitrary element in $R[x]$. We can write $f(x)$ in a unique way as $f(x) = cf_1(x)$ where $c = c(f)$ is in R and where $f_1(x)$, in $R[x]$, is primitive. By Lemma 3.11.5 we can decompose $f_1(x)$ in a unique way as the product of irreducible elements of $R[x]$. What about c? Suppose that $c = a_1(x)a_2(x) \cdots a_m(x)$ in $R[x]$; then $0 = \deg c = \deg(a_1(x)) + \deg(a_2(x)) + \cdots + \deg(a_m(x))$. Therefore, each $a_i(x)$ must be of degree 0, that is, it must be an element of R. In other words, the only factorizations of c as an element of $R[x]$ are those it had as an element of R. In particular, an irreducible element in R is still irreducible in $R[x]$. Since R is a unique factorization domain, c has a unique factorization as a product of irreducible elements of R, hence of $R[x]$.

Putting together the unique factorization of $f(x)$ in the form $cf_1(x)$ where $f_1(x)$ is primitive and where $c \in R$ with the unique factorizability of c and of $f_1(x)$ we have proved the theorem.

Given R as a unique factorization domain, then $R_1 = R[x_1]$ is also a unique factorization domain. Thus $R_2 = R_1[x_2] = R[x_1, x_2]$ is also a unique factorization domain. Continuing in this pattern we obtain

COROLLARY 1 *If R is a unique factorization domain then so is $R[x_1, \ldots, x_n]$.*

A special case of Corollary 1 but of independent interest and importance is

COROLLARY 2 *If F is a field then $F[x_1, \ldots, x_n]$ is a unique factorization domain.*

Problems

1. Prove that $R[x]$ is a commutative ring with unit element whenever R is.
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 $(1, 2, \ldots, n)$.
3. If R is an integral domain, prove that for $f(x)$, $g(x)$ in $R[x]$, $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.
4. If R is an integral domain with unit element, prove that any unit in $R[x]$ must already be 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 $ba_0 = ba_1 = \cdots = ba_m = 0$.

*6. Do Problem 5 dropping the assumption that R has no nonzero nilpotent elements.

*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.

8. Prove that when F is a field, $F[x_1, x_2]$ is not a principal ideal ring.
9. Prove, completely, Lemma 3.11.2 and its corollary.
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).
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 $a \in R$.
12. Prove the converse part of Lemma 3.11.4.
13. Prove Corollary 2 to Theorem 3.11.1.
14. Prove that a principal ideal ring is a unique factorization domain.
15. If J is the ring of integers, prove that $J[x_1, \ldots, x_n]$ is a unique factorization domain.

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.
2. Let R be a commutative ring with unit element; prove that every maximal ideal of R is a prime ideal.
3. Give an example of a ring in which some prime ideal is not a maximal ideal.
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.
5. If F is a field, prove that $F[x]$ is isomorphic to $F[t]$.
6. Find all the automorphisms σ of $F[x]$ with the property that $\sigma(f) = f$ for every $f \in F$.
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 $\bar{x} = 0$.
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.
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.
10. If A and B are ideals in a ring R such that $A \cap B = (0)$, prove that for every $a \in A$, $b \in B$, $ab = 0$.
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.
12. If R is a division ring, prove that $Z(R)$ 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.
14. Construct a field having 625 elements.
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.

16. Prove that the polynomial $f(x) = 1 + x + x^3 + x^4$ is not irreducible over any field F.
17. Prove that the polynomial $f(x) = x^4 + 2x + 2$ 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 $a^{p^n} = a$.
19. Prove that any nonzero ideal in the Gaussian integers $J[i]$ must contain some positive integer.
20. Prove that if R is a ring in which $a^4 = a$ for every $a \in R$ then R must be 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
    $$U_a = \{x \in R \mid \phi(ax) = \phi(x)\phi(a)\}.)$$
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.
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.
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.
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.
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.
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 $a^2 = a$.
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.

Supplementary Reading

ZARISKI, OSCAR, and SAMUEL, PIERRE, *Commutative Algebra*, Vol. 1. Princeton, New Jersey: D. Van Nostrand Company, Inc., 1958.

MCCOY, N. H., *Rings and Ideals*, Carus Monograph No. 8. La Salle, Illinois: Open Court Publishing Company, 1948.

Topic for Class Discussion

MOTZKIN, T., "The Euclidean algorithm," *Bulletin of the American Mathematical Society*, Vol. 55 (1949), pages 1142–1146.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: ALGEBRA **Subject Code: 19MMP101**
Class : I - M.Sc. Mathematics **Semester : I**

Unit III

Part A (20x1=20 Marks)
Possible Questions

Questions	Opt1	Opt2	Opt3	Opt4	Answer
Another name of division ring is----------	Field	integral domain	skew Field	group	Field
Every ---------- is a field	integral domain	finite integral domain	infinite integral domain	ring	finite integral domain
An element a of a ring R is said to be idempotent if -------	a=1	$a^2=1$	$a^2=a$	$a^2=0$	$a^2=a$
An element a of a ring R is said to be ---------- if $a^2=a$	idempotent	nilpotent	identity	none	idempotent
An element a of a ring R is said to be ---------- if $a^2=0$	idempotent	nilpotent	identity	none	nilpotent
A commutative ring is an ---------- if it has no zero divisors	Division ring	field	integral domain	Eucledian ring	integral domain
A ring is said to be ---------- if its nonzero elements form a group under multiplication	Division ring	field	integral domain	Eucledian ring	Division ring
A ring is said to be division ring if its nonzero elements form a ---------- under multiplication	Division ring	group	integral domain	Eucledian ring	group
A commutative ring is an integral domain if it has ----------	Division ring	field	no zero divisiors	zero divisiors	no zero divisiors
A finite integral domain is a ----------	Division ring	field	integral domain	Eucledian ring	field
A ---------- is a field.	Division ring	finite integral domain	integral domain	ring	finite integral domain
A homomorphism of R into R' is said to be an ---------- if it is a one-to one mapping	isomorphism	automorphism	homomorphism	monomorphism	isomorphism
A homomorphism of R into R' is said to be an isomrphism if it is a ----------mapping	one-one	onto	into	into & onto	one-one
A homomorphism of R into R' is said to be an isomrphism if and only if I(Φ)= -------	one	zero	two	three	zero
A ---------- ring is an integral domain if it has no zero divisors	Division ring	field	commutative ring	Eucledian ring	commutative ring
A---------- possesses a unit element	Division ring	field	integral domain	Eucledian ring	Eucledian ring
A non-empty set I is called ---------- if it is both left and right ideal K	one-sided ideal	two-sided ideal	field	integral domain	two-sided ideal
A non-empty set I is called two sided ideal if it is ----------	left ideal	right ideal	field	both left and right ideal	both left and right ideal
The polynomial is said to be --------- if the G.C.D is one	primitive	field	integral domain	Eucledian ring	primitive
The polynomial is said to be primitive if the G.C.D is ----------	two	one	zero	four	one
A polynomial is said to be integer monic if all its coefficients are ----------	integers	rational	real	complex	integers
A polynomial is said to be ---------- if all its coefficients are integers	integer monic	rational monic	real monic	complex monic	integer monic
J(i) is a ----------	integral domain	Euclidean ring	Field	skew field	Euclidean ring
.---------- is a Eucledian ring.	F(i)	J(i)	M(i)	A(i)	J(i)

If a∈R is an ---------- and a/bc, then a/b or a/c	zero divisor	primitive	irreducible	integers	irreducible
The--------- is a commutative ring with unit element	(R, +,.)	(Z, *,.)	(R, *,.)	(R, +,*)	(R, +,.)
(R, +,.) is a ---------- with unit element	field	commutative ring	Eucledian ring	ring	commutative ring
The ---------- is an Integral domain.	skew Field	Field	ring	group	Field
Field is an ----------	integer monic	Eucledian ring	integers	integral domain	integral domain
The smallest such positive integer n is called -------- if no positive integer then r is said to be a characteristic zero or infinite.	Euclidean ring R	the characteristics of a ring R	infinite integral domain	Division ring R	the characteristics of a ring R
The smallest such positive integer n is called the characteristics of a ring R if no -------- integer then r is said to be a characteristic zero or infinite.	positive	real	rational	complex	positive
The smallest such positive integer n is called the characteristics of a ring R if no positive integer then r is said to be a ----------	characteristic zero or infinite	characteristic one	characteristic finite	characteristic ring	characteristic zero or infinite
A ---------- has no proper ideals	field	group	ideal	ring	field
A field has no ----------	right ideal	proper ideals	one-sided ideal	two-sided ideal	proper ideals
An ---------- generated by a single element of itself it called a principle ideal	group	ideal	Field	ring	ideal
An ideal generated by a --------- element of itself it called a principle ideal	two-sided ideal	one-sided ideal	double	single	single
An ideal generated by a single element of itself it called a --------	integral domain	principle ideal	ideal	Eucledian ring	principle ideal
An ---------- possess a unit element.	integer monic	Division ring	Euclidean ring	integral domain	Euclidean ring
An Euclidean ring possess a ------- element.	field	unit	double	no	unit
An --------- is said to be of characteristics zero if the relation Ma = 0, where a ≠0 is in D and where m is an integer can hold only if m=0	skew Field	Integral domain D	Division ring R	the characteristics of a ring R	Integral domain D
A ---------- of R into R' is said to be an isomorphism if it is one- one mapping.	homomorphism	isomorphism	automorphism	monomorphism	homomorphism
A homomorphism of R into R' is said to be an ---------- if it is one- one mapping.	isomorphism	identity	integral domain	Eucledian ring	isomorphism
A homomorphism of R into R' is said to be an isomorphism if it is --------- mapping.	onto	one- one	into	into & onto	one- one
We cannot define the ---------- of the zero polynomial.	sum	degree	order	power	degree
A---------- is a constant if it degree is zero.	monomial	trinomial	polynomial	binomial	polynomial

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

CLASS: I M.Sc. MATHEMATICS **COURSENAME: ALGEBRA**

COURSE CODE: 19MMP101 **BATCH-2019-2021**

UNIT-IV

EXTENSION FIELDS

Extension fields - Roots of polynomials - More about roots - Finite fields.

5

Fields

In our discussion of rings we have already singled out a special class which we called fields. A field, let us recall, is a commutative ring with unit element in which every nonzero element has a multiplicative inverse. Put another way, a field is a commutative ring in which we can divide by any nonzero element.

Fields play a central role in algebra. For one thing, results about them find important applications in the theory of numbers. For another, their theory encompasses the subject matter of the theory of equations which treats questions about the roots of polynomials.

In our development we shall touch only lightly on the field of algebraic numbers. Instead, our greatest emphasis will be on aspects of field theory which impinge on the theory of equations. Although we shall not treat the material in its fullest or most general form, we shall go far enough to introduce some of the beautiful ideas, due to the brilliant French mathematician Evariste Galois, which have served as a guiding inspiration for algebra as it is today.

5.1 Extension Fields

In this section we shall be concerned with the relation of one field to another. Let F be a field; a field K is said to be an *extension* of F if K contains F. Equivalently, K is an extension of F if F is a subfield of K. *Throughout this chapter F will denote a given field and K an extension of F.*

As was pointed out earlier, in the chapter on vector spaces, if K is

an extension of F, then, under the ordinary field operations in K, K is a vector space over F. As a vector space we may talk about linear dependence, dimension, bases, etc., in K relative to F.

DEFINITION The *degree* of K over F is the dimension of K as a vector space over F.

We shall always denote the degree of K over F by $[K:F]$. Of particular interest to us is the case in which $[K:F]$ is finite, that is, when K is finite-dimensional as a vector space over F. This situation is described by saying that K is a *finite extension* of F.

We start off with a relatively simple but, at the same time, highly effective result about finite extensions, namely,

THEOREM 5.1.1 *If L is a finite extension of K and if K is a finite extension of F, then L is a finite extension of F. Moreover, $[L:F] = [L:K][K:F]$.*

Proof. The strategy we employ in the proof is to write down explicitly a basis of L over F. In this way not only do we show that L is a finite extension of F, but we actually prove the sharper result and the one which is really the heart of the theorem, namely that $[L:F] = [L:K][K:F]$.

Suppose, then, that $[L:K] = m$ and that $[K:F] = n$. Let $v_1, \ldots, v_m$ be a basis of L over K and let $w_1, \ldots, w_n$ be a basis of K over F. What could possibly be nicer or more natural than to have the elements $v_i w_j$, where $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, serve as a basis of L over F? Whatever else, they do at least provide us with the right number of elements. We now proceed to show that they do in fact form a basis of L over F. What do we need to establish this? First we must show that every element in L is a linear combination of them with coefficients in F, and then we must demonstrate that these mn elements are linearly independent over F.

Let t be any element in L. Since every element in L is a linear combination of $v_1, \ldots, v_m$ with coefficients in K, in particular, t must be of this form. Thus $t = k_1 v_1 + \cdots + k_m v_m$, where the elements $k_1, \ldots, k_m$ are all in K. However, every element in K is a linear combination of $w_1, \ldots, w_n$ with coefficients in F. Thus $k_1 = f_{11} w_1 + \cdots + f_{1n} w_n, \ldots, k_i = f_{i1} w_1 + \cdots + f_{in} w_n, \ldots, k_m = f_{m1} w_1 + \cdots + f_{mn} w_n$, where every f_{ij} is in F.

Substituting these expressions for $k_1, \ldots, k_m$ into $t = k_1 v_1 + \cdots + k_m v_m$, we obtain $t = (f_{11} w_1 + \cdots + f_{1n} w_n) v_1 + \cdots + (f_{m1} w_1 + \cdots + f_{mn} w_n) v_m$ Multiplying this out, using the distributive and associative laws, we finally arrive at $t = f_{11} v_1 w_1 + \cdots + f_{1n} v_1 w_n + \cdots + f_{ij} v_i w_j + \cdots + f_{mn} v_m w_n$. Since the f_{ij} are in F, we have realized t as a linear combination over F of the elements $v_i w_j$. Therefore, the elements $v_i w_j$ do indeed span all of L over F, and so they fulfill the first requisite property of a basis.

We still must show that the elements $v_i w_j$ are linearly independent over F. Suppose that $f_{11}v_1w_1 + \cdots + f_{1n}v_1w_n + \cdots + f_{ij}v_iw_j + \cdots + f_{mn}v_mw_n = 0$, where the f_{ij} are in F. Our objective is to prove that each $f_{ij} = 0$. Regrouping the above expression yields $(f_{11}w_1 + \cdots + f_{1n}w_n)v_1 + \cdots + (f_{i1}w_1 + \cdots + f_{in}w_n)v_i + \cdots + (f_{m1}w_1 + \cdots + f_{mn}w_n)v_m = 0$.

Since the w_i are in K, and since $K \supset F$, all the elements $k_i = f_{i1}w_1 + \cdots + f_{in}w_n$ are in K. Now $k_1v_1 + \cdots + k_mv_m = 0$ with $k_1, \ldots, k_m \in K$. But, by assumption, $v_1, \ldots, v_m$ form a basis of L over K, so, in particular they must be linearly independent over K. The net result of this is that $k_1 = k_2 = \cdots = k_m = 0$. Using the explicit values of the k_i, we get

$$f_{i1}w_1 + \cdots + f_{in}w_n = 0 \qquad \text{for} \quad i = 1, 2, \ldots, m.$$

But now we invoke the fact that the w_i are linearly independent over F; this yields that each $f_{ij} = 0$. In other words, we have proved that the v_iw_j are linearly independent over F. In this way they satisfy the other requisite property for a basis.

We have now succeeded in proving that the mn elements v_iw_j form a basis of L over F. Thus $[L:F] = mn$; since $m = [L:K]$ and $n = [K:F]$ we have obtained the desired result $[L:F] = [L:K][K:F]$.

Suppose that L, K, F are three fields in the relation $L \supset K \supset F$ and, suppose further that $[L:F]$ is finite. Clearly, any elements in L linearly independent over K are, all the more so, linearly independent over F. Thus the assumption that $[L:F]$ is finite forces the conclusion that $[L:K]$ is finite. Also, since K is a subspace of L, $[K:F]$ is finite. By the theorem, $[L:F] = [L:K][K:F]$, whence $[K:F] \mid [L:F]$. We have proved the

COROLLARY *If L is a finite extension of F and K is a subfield of L which contains F, then $[K:F] \mid [L:F]$.*

Thus, for instance, if $[L:F]$ is a prime number, then there can be no fields properly between F and L. A little later, in Section 5.4, when we discuss the construction of certain geometric figures by straightedge and compass, this corollary will be of great significance.

DEFINITION An element $a \in K$ is said to be *algebraic over F* if there exist elements $\alpha_0, \alpha_1, \ldots, \alpha_n$ in F, not all 0, such that $\alpha_0 a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$.

If the polynomial $q(x) \in F[x]$, the ring of polynomials in x over F, and if $q(x) = \beta_0 x^m + \beta_1 x^{m-1} + \cdots + \beta_m$, then for any element $b \in K$, by $q(b)$ we shall mean the element $\beta_0 b^m + \beta_1 b^{m-1} + \cdots + \beta_m$ in K. In the expression commonly used, $q(b)$ is the *value* of the polynomial $q(x)$ obtained by substituting b for x. The element b is said to *satisfy* $q(x)$ if $q(b) = 0$.

In these terms, $a \in K$ is algebraic over F if there is a nonzero polynomial $p(x) \in F[x]$ which a satisfies, that is, for which $p(a) = 0$.

Let K be an extension of F and let a be in K. Let $\mathscr{M}$ be the collection of all subfields of K which contain both F and a. $\mathscr{M}$ is not empty, for K itself is an element of $\mathscr{M}$. Now, as is easily proved, the intersection of any number of subfields of K is again a subfield of K. Thus the intersection of all those subfields of K which are members of $\mathscr{M}$ is a subfield of K. We denote this subfield by $F(a)$. What are its properties? Certainly it contains both F and a, since this is true for every subfield of K which is a member of $\mathscr{M}$. Moreover, by the very definition of intersection, every subfield of K in $\mathscr{M}$ contains $F(a)$, yet $F(a)$ itself is in $\mathscr{M}$. *Thus $F(a)$ is the smallest subfield of K containing both F and a.* We call $F(a)$ the subfield obtained by *adjoining* a to F.

Our description of $F(a)$, so far, has been purely an external one. We now give an alternative and more constructive description of $F(a)$. Consider all these elements in K which can be expressed in the form $\beta_0 + \beta_1 a + \cdots + \beta_s a^s$; here the β's can range freely over F and s can be any nonnegative integer. As elements in K, one such element can be divided by another, provided the latter is not 0. Let U be the set of all such quotients. We leave it as an exercise to prove that U is a subfield of K.

On one hand, U certainly contains F and a, whence $U \supset F(a)$. On the other hand, any subfield of K which contains both F and a, by virtue of closure under addition and multiplication, must contain all the elements $\beta_0 + \beta_1 a + \cdots + \beta_s a^s$ where each $\beta_i \in F$. Thus $F(a)$ must contain all these elements; being a subfield of K, $F(a)$ must also contain all quotients of such elements. Therefore, $F(a) \supset U$. The two relations $U \subset F(a)$, $U \supset F(a)$ of course imply that $U = F(a)$. In this way we have obtained an internal construction of $F(a)$, namely as U.

We now intertwine the property that $a \in K$ is algebraic over F with macroscopic properties of the field $F(a)$ itself. This is

THEOREM 5.1.2 *The element $a \in K$ is algebraic over F if and only if $F(a)$ is a finite extension of F.*

Proof. As is so very common with so many such "if and only if" propositions, one-half of the proof will be quite straightforward and easy, whereas the other half will be deeper and more complicated.

Suppose that $F(a)$ is a finite extension of F and that $[F(a):F] = m$. Consider the elements $1, a, a^2, \ldots, a^m$; they are all in $F(a)$ and are $m+1$ in number. By Lemma 4.2.4, these elements are linearly dependent over F. Therefore, there are elements $\alpha_0, \alpha_1, \ldots, \alpha_m$ in F, not all 0, such that $\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_m a^m = 0$. Hence a is algebraic over F and satisfies the nonzero polynomial $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$ in $F[x]$ of degree at most $m = [F(a):F]$. This proves the "if" part of the theorem.

Now to the "only if" part. Suppose that a in K is algebraic over F. By

assumption, a satisfies some nonzero polynomial in $F[x]$; let $p(x)$ be a polynomial in $F[x]$ of smallest positive degree such that $p(a) = 0$. We claim that $p(x)$ is irreducible over F. For, suppose that $p(x) = f(x)g(x)$, where $f(x)$, $g(x) \in F[x]$; then $0 = p(a) = f(a)g(a)$ (see Problem 1) and, since $f(a)$ and $g(a)$ are elements of the field K, the fact that their product is 0 forces $f(a) = 0$ or $g(a) = 0$. Since $p(x)$ is of lowest positive degree with $p(a) = 0$, we must conclude that one of $\deg f(x) \geq \deg p(x)$ or $\deg g(x) \geq \deg p(x)$ must hold. But this proves the irreducibility of $p(x)$.

We define the mapping ψ from $F[x]$ into $F(a)$ as follows. For any $h(x) \in F[x]$, $h(x)\psi = h(a)$. We leave it to the reader to verify that ψ is a ring homomorphism of the ring $F[x]$ into the field $F(a)$ (see Problem 1). What is V, the kernel of ψ? By the very definition of ψ, $V = \{h(x) \in F[x] \mid h(a) = 0\}$. Also, $p(x)$ is an element of lowest degree in the ideal V of $F[x]$. By the results of Section 3.9, every element in V is a multiple of $p(x)$, and since $p(x)$ is irreducible, by Lemma 3.9.6, V is a maximal ideal of $F[x]$. By Theorem 3.5.1, $F[x]/V$ is a field. Now by the general homomorphism theorem for rings (Theorem 3.4.1), $F[x]/V$ is isomorphic to the image of $F[x]$ under ψ. Summarizing, we have shown that the image of $F[x]$ under ψ is a subfield of $F(a)$. This image contains $x\psi = a$ and, for every $\alpha \in F$, $\alpha\psi = \alpha$. Thus the image of $F[x]$ under ψ is a subfield of $F[a]$ which contains both F and a; by the very definition of $F(a)$ we are forced to conclude that the image of $F[x]$ under ψ is *all* of $F(a)$. Put more succinctly, $F[x]/V$ is isomorphic to $F(a)$.

Now, $V = (p(x))$, the ideal generated by $p(x)$; from this we claim that the dimension of $F[x]/V$, as a vector space over F, is precisely equal to $\deg p(x)$ (see Problem 2). In view of the isomorphism between $F[x]/V$ and $F(a)$ we obtain the fact that $[F(a):F] = \deg p(x)$. Therefore, $[F(a):F]$ is certainly finite; this is the contention of the "only if" part of the theorem. Note that we have actually proved more, namely that $[F(a):F]$ is equal to the degree of the polynomial of least degree satisfied by a over F.

The proof we have just given has been somewhat long-winded, but deliberately so. The route followed contains important ideas and ties in results and concepts developed earlier with the current exposition. No part of mathematics is an island unto itself.

We now redo the "only if" part, working more on the inside of $F(a)$. This reworking is, in fact, really identical with the proof already given; the constituent pieces are merely somewhat differently garbed.

Again let $p(x)$ be a polynomial over F of lowest positive degree satisfied by a. Such a polynomial is called a *minimal polynomial* for a over F. We may assume that its coefficient of the highest power of x is 1, that is, it is monic; in that case we can speak of *the* minimal polynomial for a over F for any two minimal, monic polynomials for a over F are equal. (Prove!)

Suppose that $p(x)$ is of degree n; thus $p(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$ where the α_i are in F. By assumption, $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$, whence $a^n = -\alpha_1 a^{n-1} - \alpha_2 a^{n-2} - \cdots - \alpha_n$. What about a^{n+1}? From the above, $a^{n+1} = -\alpha_1 a^n - \alpha_2 a^{n-1} - \cdots - \alpha_n a$; if we substitute the expression for a^n into the right-hand side of this relation, we realize a^{n+1} as a linear combination of the elements $1, a, \ldots, a^{n-1}$ over F. Continuing this way, we get that a^{n+k}, for $k \geq 0$, is a linear combination over F of $1, a, a^2, \ldots, a^{n-1}$.

Now consider $T = \{\beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1} \mid \beta_0, \beta_1, \ldots, \beta_{n-1} \in F\}$. Clearly, T is closed under addition; in view of the remarks made in the paragraph above, it is also closed under multiplication. Whatever further it may be, T has at least been shown to be a ring. Moreover, T contains both F and a. We now wish to show that T is more than just a ring, that it is, in fact, a field.

Let $0 \neq u = \beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1}$ be in T and let $h(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1} \in F[x]$. Since $u \neq 0$, and $u = h(a)$, we have that $h(a) \neq 0$, whence $p(x) \nmid h(x)$. By the irreducibility of $p(x)$, $p(x)$ and $h(x)$ must therefore be relatively prime. Hence we can find polynomials $s(x)$ and $t(x)$ in $F[x]$ such that $p(x)s(x) + h(x)t(x) = 1$. But then $1 = p(a)s(a) + h(a)t(a) = h(a)t(a)$, since $p(a) = 0$; putting into this that $u = h(a)$, we obtain $ut(a) = 1$. The inverse of u is thus $t(a)$; in $t(a)$ all powers of a higher than $n - 1$ can be replaced by linear combinations of $1, a, \ldots, a^{n-1}$ over F, whence $t(a) \in T$. We have shown that every nonzero element of T has its inverse in T; consequently, T is a field. However, $T \subset F(a)$, yet F and a are both contained in T, which results in $T = F(a)$. We have identified $F(a)$ as the set of all expressions $\beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1}$.

Now T is spanned over F by the elements $1, a, \ldots, a^{n-1}$ in consequence of which $[T:F] \leq n$. However, the elements $1, a, a^2, \ldots, a^{n-1}$ are linearly independent over F, for any relation of the form $\gamma_0 + \gamma_1 a + \cdots + \gamma_{n-1} a^{n-1}$, with the elements $\gamma_i \in F$, leads to the conclusion that a satisfies the polynomial $\gamma_0 + \gamma_1 x + \cdots + \gamma_{n-1} x^{n-1}$ over F of degree less than n. This contradiction proves the linear independence of $1, a, \ldots, a^{n-1}$, and so these elements actually form a basis of T over F, whence, in fact, we now know that $[T:F] = n$. Since $T = F(a)$, the result $[F(a):F] = n$ follows.

DEFINITION The element $a \in K$ is said to be *algebraic of degree n* over F if it satisfies a nonzero polynomial over F of degree n but no nonzero polynomial of lower degree.

In the course of proving Theorem 5.1.2 (in each proof we gave), we proved a somewhat sharper result than that stated in that theorem, namely,

THEOREM 5.1.3 *If $a \in K$ is algebraic of degree n over F, then $[F(a):F] = n$.*

This result adapts itself to many uses. We give now, as an immediate consequence thereof, the very interesting

THEOREM 5.1.4 *If a, b in K are algebraic over F then $a \pm b$, ab, and a/b (if $b \neq 0$) are all algebraic over F. In other words, the elements in K which are algebraic over F form a subfield of K.*

Proof. Suppose that a is algebraic of degree m over F while b is algebraic of degree n over F. By Theorem 5.1.3 the subfield $T = F(a)$ of K is of degree m over F. Now b is algebraic of degree n over F, *a fortiori* it is algebraic of degree at most n over T which contains F. Thus the subfield $W = T(b)$ of K, again by Theorem 5.1.3, is of degree at most n over T. But $[W:F] = [W:T][T:F]$ by Theorem 5.1.1; therefore, $[W:F] \leq mn$ and so W is a finite extension of F. However, a and b are both in W, whence all of $a \pm b$, ab, and a/b are in W. By Theorem 5.1.2, since $[W:F]$ is finite, these elements must be algebraic over F, thereby proving the theorem.

Here, too, we have proved somewhat more. Since $[W:F] \leq mn$, every element in W satisfies a polynomial of degree at most mn over F, whence the

COROLLARY *If a and b in K are algebraic over F of degrees m and n, respectively, then $a \pm b$, ab, and a/b (if $b \neq 0$) are algebraic over F of degree at most mn.*

In the proof of the last theorem we made two extensions of the field F. The first we called T; it was merely the field $F(a)$. The second we called W and it was $T(b)$. Thus $W = (F(a))(b)$; it is customary to write it as $F(a, b)$. Similarly, we could speak about $F(b, a)$; it is not too difficult to prove that $F(a, b) = F(b, a)$. Continuing this pattern, we can define $F(a_1, a_2, \ldots, a_n)$ for elements $a_1, \ldots, a_n$ in K.

DEFINITION The extension K of F is called an *algebraic extension* of F if every element in K is algebraic over F.

We prove one more result along the lines of the theorems we have proved so far.

THEOREM 5.1.5 *If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.*

Proof. Let u be any arbitrary element of L; our objective is to show that u satisfies some nontrivial polynomial with coefficients in F. What information do we have at present? We certainly do know that u satisfies some

polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$, where $\sigma_1, \ldots, \sigma_n$ are in K. But K is algebraic over F; therefore, by several uses of Theorem 5.1.3, $M = F(\sigma_1, \ldots, \sigma_n)$ is a finite extension of F. Since u satisfies the polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$ whose coefficients are in M, u is algebraic over M. Invoking Theorem 5.1.2 yields that $M(u)$ is a finite extension of M. However, by Theorem 5.1.1, $[M(u):F] = [M(u):M][M:F]$, whence $M(u)$ is a finite extension of F. But this implies that u is algebraic over F, completing proof of the theorem.

A quick description of Theorem 5.1.5: algebraic over algebraic is algebraic.

The preceding results are of special interest in the particular case in which F is the field of rational numbers and K the field of complex numbers.

DEFINITION A complex number is said to be an *algebraic number* if it is algebraic over the field of rational numbers.

A complex number which is not algebraic is called *transcendental.* At the present stage we have no reason to suppose that there are any transcendental numbers. In the next section we shall prove that the familiar real number e is transcendental. This will, of course, establish the existence of transcendental numbers. In actual fact, they exist in great abundance; in a very well-defined way there are more of them than there are algebraic numbers.

Theorem 5.1.4 applied to algebraic numbers proves the interesting fact that *the algebraic numbers form a field*; that is, the sum, products, and quotients of algebraic numbers are again algebraic numbers.

Theorem 5.1.5 when used in conjunction with the so-called "fundamental theorem of algebra," has the implication that the roots of a polynomial whose coefficients are algebraic numbers are themselves algebraic numbers.

Problems

1. Prove that the mapping $\psi:F[x] \to F(a)$ defined by $h(x)\psi = h(a)$ 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.
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).

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?
5. With the same notation as in Problem 4, show that $\sqrt{2} + \sqrt[3]{5}$ 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 $Q(w) \neq Q(\sqrt{2}, \sqrt[3]{5})$.
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
$$F(a_1, \ldots, a_n) = F(a_{i_1}, a_{i_2}, \ldots, a_{i_n}).$$
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.
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 $m > 0$.

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.
11. If the rational number r is also an algebraic integer, prove that r must be an ordinary 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.
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.
**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.

15. (a) Prove that $\sin 1^\circ$ is an algebraic number.
(b) From part (a) prove that $\sin m^\circ$ is an algebraic number for any integer m.

5.2 The Transcendence of e

In defining algebraic and transcendental numbers we pointed out that it could be shown that transcendental numbers exist. One way of achieving this would be the demonstration that some specific number is transcendental.

In 1851 Liouville gave a criterion that a complex number be algebraic; using this, he was able to write down a large collection of transcendental numbers. For instance, it follows from his work that the number .101001000000100 ... 10 ... is transcendental; here the number of zeros between successive ones goes as $1!, 2!, \ldots \ldots, n!, \ldots$.

This certainly settled the question of existence. However, the question whether some given, familiar numbers were transcendental still persisted. The first success in this direction was by Hermite, who in 1873 gave a proof that e is transcendental. His proof was greatly simplified by Hilbert. The proof that we shall give here is a variation, due to Hurwitz, of Hilbert's proof.

The number π offered greater difficulties. These were finally overcome by Lindemann, who in 1882 produced a proof that π is transcendental. One immediate consequence of this is the fact that it is impossible, by straightedge and compass, to square the circle, for such a construction would lead to an algebraic number θ such that $\theta^2 = \pi$. But if θ is algebraic then so is θ^2, in virtue of which π would be algebraic, in contradiction to Lindemann's result.

In 1934, working independently, Gelfond and Schneider proved that if a and b are algebraic numbers and if b is irrational, then a^b is transcendental. This answered in the affirmative the question raised by Hilbert whether $2^{\sqrt{2}}$ was transcendental.

For those interested in pursuing the subject of transcendental numbers further, we would strongly recommend the charming books by C. L. Siegel, entitled *Transcendental Numbers*, and by I. Niven, *Irrational Numbers*.

To prove that e is irrational is easy; to prove that π is irrational is much more difficult. For a very clever and neat proof of the latter, see the paper by Niven entitled "A simple proof that π is irrational," *Bulletin of the American Mathematical Society*, Vol. 53 (1947), page 509.

Now to the transcendence of e. Aside from its intrinsic interest, its proof offers us a change of pace. Up to this point all our arguments have been of an algebraic nature; now, for a short while, we return to the more familiar

grounds of the calculus. The proof itself will use only elementary calculus; the deepest result needed, therefrom, will be the mean value theorem.

THEOREM 5.2.1 *The number e is transcendental.*

Proof. In the proof we shall use the standard notation $f^{(i)}(x)$ to denote the ith derivative of $f(x)$ with respect to x.

Suppose that $f(x)$ is a polynomial of degree r with real coefficients. Let $F(x) = f(x) + f^{(1)}(x) + f^{(2)}(x) + \cdots + f^{(r)}(x)$. We compute $(d/dx)(e^{-x}F(x))$; using the fact that $f^{(r+1)}(x) = 0$ (since $f(x)$ is of degree r) and the basic property of e, namely that $(d/dx)e^x = e^x$, we obtain $(d/dx)(e^{-x}F(x)) = -e^{-x}f(x)$.

The mean value theorem asserts that if $g(x)$ is a continuously differentiable, single-valued function on the closed interval $[x_1, x_2]$ then

$$\frac{g(x_1) - g(x_2)}{x_1 - x_2} = g^{(1)}(x_1 + \theta(x_2 - x_1)), \qquad \text{where} \quad 0 < \theta < 1.$$

We apply this to our function $e^{-x}F(x)$, which certainly satisfies all the required conditions for the mean value theorem on the closed interval $[x_1, x_2]$ where $x_1 = 0$ and $x_2 = k$, where k is any positive integer. We then obtain that $e^{-k}F(k) - F(0) = -e^{-\theta_k k}f(\theta_k k)k$, where θ_k depends on k and is some real number between 0 and 1. Multiplying this relation through by e^k yields $F(k) - F(0)e^k = -e^{(1-\theta_k)k}f(\theta_k k)k$. We write this out explicitly:

$$\begin{aligned} F(1) - eF(0) &= -e^{(1-\theta_1)}f(\theta_1) = \varepsilon_1, \\ F(2) - e^2F(0) &= -2e^{2(1-\theta_2)}f(2\theta_2) = \varepsilon_2, \\ &\vdots \\ F(n) - e^nF(0) &= -ne^{n(1-\theta_n)}f(n\theta_n) = \varepsilon_n. \end{aligned} \tag{1}$$

Suppose now that e is an algebraic number; then it satisfies some relation of the form

$$c_ne^n + c_{n-1}e^{n-1} + \cdots + c_1e + c_0 = 0, \tag{2}$$

where $c_0, c_1, \ldots, c_n$ are integers and where $c_0 > 0$.

In the relations (1) let us multiply the first equation by c_1, the second by c_2, and so on; adding these up we get $c_1F(1) + c_2F(2) + \cdots + c_nF(n) - F(0)(c_1e + c_2e^2 + \cdots + c_ne^n) = c_1\varepsilon_1 + c_2\varepsilon_2 + \cdots + c_n\varepsilon_n$.

In view of relation (2), $c_1e + c_2e^2 + \cdots + c_ne^n = -c_0$, whence the above equation simplifies to

$$c_0F(0) + c_1F(1) + \cdots + c_nF(n) = c_1\varepsilon_1 + \cdots + c_n\varepsilon_n. \tag{3}$$

All this discussion has held for the $F(x)$ constructed from an arbitrary

polynomial $f(x)$. We now see what all this implies for a very specific polynomial, one first used by Hermite, namely,

$$f(x) = \frac{1}{(p-1)!}x^{p-1}(1-x)^p(2-x)^p\cdots(n-x)^p.$$

Here p can be any prime number chosen so that $p > n$ and $p > c_0$. For this polynomial we shall take a very close look at $F(0), F(1), \ldots, F(n)$ and we shall carry out an estimate on the size of $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$.

When expanded, $f(x)$ is a polynomial of the form

$$\frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{a_0x^p}{(p-1)!} + \frac{a_1x^{p+1}}{(p-1)!} + \cdots,$$

where $a_0, a_1, \ldots,$ are integers.

When $i \geq p$ we claim that $f^{(i)}(x)$ is a polynomial, with coefficients which are integers all of which are multiples of p. (Prove! See Problem 2.) *Thus for any integer j, $f^{(i)}(j)$, for $i \geq p$, is an integer and is a multiple of p.*

Now, from its very definition, $f(x)$ has a root of multiplicity p at $x = 1, 2, \ldots, n$. Thus for $j = 1, 2, \ldots, n$, $f(j) = 0, f^{(1)}(j) = 0, \ldots, f^{(p-1)}(j) = 0$. However, $F(j) = f(j) + f^{(1)}(j) + \cdots + f^{(p-1)}(j) + f^{(p)}(j) + \cdots + f^{(r)}(j)$; by the discussion above, for $j = 1, 2, \ldots, n$, $F(j)$ *is an integer and is a multiple of p.*

What about $F(0)$? Since $f(x)$ has a root of multiplicity $p-1$ at $x = 0$, $f(0) = f^{(1)}(0) = \cdots = f^{(p-2)}(0) = 0$. For $i \geq p$, $f^{(i)}(0)$ is an integer which is a multiple of p. But $f^{(p-1)}(0) = (n!)^p$ and since $p > n$ and is a prime number, $p \nmid (n!)^p$ so that $f^{(p-1)}(0)$ *is an integer not divisible by p.* Since $F(0) = f(0) + f^{(1)}(0) + \cdots + f^{(p-2)}(0) + f^{(p-1)}(0) + f^{(p)}(0) + \cdots + f^{(r)}(0)$, we conclude that $F(0)$ *is an integer not divisible by p.* Because $c_0 > 0$ and $p > c_0$ and because $p \nmid F(0)$ whereas $p \mid F(1), p \mid F(2), \ldots, p \mid F(n)$, we can assert that $c_0F(0) + c_1F(1) + \cdots + c_nF(n)$ *is an integer and is not divisible by p.*

However, by (3), $c_0F(0) + c_1F(1) + \cdots + c_nF(n) = c_1\varepsilon_1 + \cdots + c_n\varepsilon_n$. What can we say about ε_i? Let us recall that

$$\varepsilon_i = \frac{-e^{i(1-\theta_i)}(1-i\theta_i)^p\cdots(n-i\theta_i)^p(i\theta_i)^{p-1}i}{(p-1)!},$$

where $0 < \theta_i < 1$. Thus

$$|\varepsilon_i| \leq e^n\frac{n^p(n!)^p}{(p-1)!}.$$

As $p \to \infty$,

$$\frac{e^nn^p(n!)^p}{(p-1)!} \to 0,$$

(Prove!) whence we can find a prime number larger than both c_0 and n and large enough to force $|c_1\varepsilon_1 + \cdots + c_n\varepsilon_n| < 1$. But $c_1\varepsilon_1 + \cdots + c_n\varepsilon_n = c_0F(0) + \cdots + c_nF(n)$, *so must be an integer*; since it is smaller than 1 in size our only possible conclusion is that $c_1\varepsilon_1 + \cdots + c_n\varepsilon_n = 0$. Consequently, $c_0F(0) + \cdots + c_nF(n) = 0$; this however is sheer nonsense, since we know that $p \nmid (c_0F(0) + \cdots + c_nF(n))$, whereas $p \mid 0$. This contradiction, stemming from the assumption that e is algebraic, proves that e must be transcendental.

Problems

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.

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.

3. If a is any real number, prove that $(a^m/m!) \to 0$ as $m \to \infty$.

4. If $m > 0$ and n are integers, prove that $e^{m/n}$ is transcendental.

5.3 Roots of Polynomials

In Section 5.1 we discussed elements in a given extension K of F which were algebraic over F, that is, elements which satisfied polynomials in $F[x]$. We now turn the problem around; given a polynomial $p(x)$ in $F[x]$ we wish to find a field K which is an extension of F in which $p(x)$ has a root. No longer is the field K available to us; in fact it is our prime objective to construct it. Once it is constructed, we shall examine it more closely and see what consequences we can derive.

DEFINITION If $p(x) \in F[x]$, then an element a lying in some extension field of F is called a *root* of $p(x)$ if $p(a) = 0$.

We begin with the familiar result known as the *Remainder Theorem.*

LEMMA 5.3.1 *If $p(x) \in F[x]$ and if K is an extension of F, then for any element $b \in K$, $p(x) = (x - b)q(x) + p(b)$ where $q(x) \in K[x]$ and where* $\deg q(x) = \deg p(x) - 1$.

Proof. Since $F \subset K$, $F[x]$ is contained in $K[x]$, whence we can consider $p(x)$ to be lying in $K[x]$. By the division algorithm for polynomials in $K[x]$, $p(x) = (x - b)q(x) + r$, where $q(x) \in K[x]$ and where $r = 0$ or $\deg r < \deg (x - b) = 1$. Thus either $r = 0$ or $\deg r = 0$; in either case r must be an element of K. But exactly what element of K is it? Since $p(x) = (x - b)q(x) + r$, $p(b) = (b - b)q(b) + r = r$. Therefore, $p(x) = (x - b)q(x) + p(b)$. That the degree of $q(x)$ is one less than that of $p(x)$ is easy to verify and is left to the reader.

COROLLARY *If $a \in K$ is a root of $p(x) \in F[x]$, where $F \subset K$, then in $K[x]$, $(x - a) \mid p(x)$.*

Proof. From Lemma 5.3.1, in $K[x]$, $p(x) = (x - a)q(x) + p(a) = (x - a)q(x)$ since $p(a) = 0$. Thus $(x - a) \mid p(x)$ in $K[x]$.

DEFINITION The element $a \in K$ is a root of $p(x) \in F[x]$ of *multiplicity* m if $(x - a)^m \mid p(x)$, whereas $(x - a)^{m+1} \nmid p(x)$.

A reasonable question to ask is, How many roots can a polynomial have in a given field? Before answering we must decide how to count a root of multiplicity m. *We shall always count it as m roots.* Even with this convention we can prove

LEMMA 5.3.2 *A polynomial of degree n over a field can have at most n roots in any extension field.*

Proof. We proceed by induction on n, the degree of the polynomial $p(x)$. If $p(x)$ is of degree 1, then it must be of the form $\alpha x + \beta$ where α, β are in a field F and where $\alpha \neq 0$. Any a such that $p(a) = 0$ must then imply that $\alpha a + \beta = 0$, from which we conclude that $a = (-\beta/\alpha)$. That is, $p(x)$ has the unique root $-\beta/\alpha$, whence the conclusion of the lemma certainly holds in this case.

Assuming the result to be true in any field for all polynomials of degree less than n, let us suppose that $p(x)$ is of degree n over F. Let K be any extension of F. If $p(x)$ has no roots in K, then we are certainly done, for the number of roots in K, namely zero, is definitely at most n. So, suppose that $p(x)$ has at least one root $a \in K$ and that a is a root of multiplicity m. Since $(x - a)^m \mid p(x)$, $m \leq n$ follows. Now $p(x) = (x - a)^m q(x)$, where $q(x) \in K[x]$ is of degree $n - m$. From the fact that $(x - a)^{m+1} \nmid p(x)$, we get that $(x - a) \nmid q(x)$, whence, by the corollary to Lemma 5.3.1, a is not a root of $q(x)$. If $b \neq a$ is a root, in K, of $p(x)$, then $0 = p(b) = (b - a)^m q(b)$; however, since $b - a \neq 0$ and since we are in a field, we conclude that $q(b) = 0$. That is, any root of $p(x)$, in K, other than a, must be a root of

$q(x)$. Since $q(x)$ is of degree $n - m < n$, by our induction hypothesis, $q(x)$ has at most $n - m$ roots in K, which, together with the other root a, counted m times, tells us that $p(x)$ has at most $m + (n - m) = n$ roots in K. This completes the induction and proves the lemma.

One should point out that commutativity is essential in Lemma 5.3.2. If we consider the ring of real quaternions, which falls short of being a field only in that it fails to be commutative, then the polynomial $x^2 + 1$ has at least 3 roots, i, j, k (in fact, it has an infinite number of roots). In a somewhat different direction we need, even when the ring is commutative, that it be an integral domain, for if $ab = 0$ with $a \neq 0$ and $b \neq 0$ in the commutative ring R, then the polynomial ax of degree 1 over R has at least two distinct roots $x = 0$ and $x = b$ in R.

The previous two lemmas, while interesting, are of subsidiary interest. We now set ourselves to our prime task, that of providing ourselves with suitable extensions of F in which a given polynomial has roots. Once this is done, we shall be able to analyze such extensions to a reasonable enough degree of accuracy to get results. The most important step in the construction is accomplished for us in the next theorem. The argument used will be very reminiscent of some used in Section 5.1.

THEOREM 5.3.1 *If $p(x)$ is a polynomial in $F[x]$ of degree $n \geq 1$ and is irreducible over F, then there is an extension E of F, such that $[E:F] = n$, in which $p(x)$ has a root.*

Proof. Let $F[x]$ be the ring of polynomials in x over F and let $V = (p(x))$ be the ideal of $F[x]$ generated by $p(x)$. By Lemma 3.9.6, V is a maximal ideal of $F[x]$, whence by Theorem 3.5.1, $E = F[x]/V$ is a field. This E will be shown to satisfy the conclusions of the theorem.

First we want to show that E is an extension of F; however, in fact, it is not! But let $\bar{F}$ be the image of F in E; that is, $\bar{F} = \{\alpha + V \mid \alpha \in F\}$. We assert that $\bar{F}$ is a field isomorphic to F; in fact, if ψ is the mapping from $F[x]$ into $F[x]/V = E$ defined by $f(x)\psi = f(x) + V$, then the restriction of ψ to F induces an isomorphism of F onto $\bar{F}$. (Prove!) Using this isomorphism, we identify F and $\bar{F}$; *in this way we can consider E to be an extension of F.*

We claim that E is a finite extension of F of degree $n = \deg p(x)$, for the elements $1 + V, x + V, (x + V)^2 = x^2 + V, \ldots, (x + V)^i = x^i + V, \ldots, (x + V)^{n-1} = x^{n-1} + V$ form a basis of E over F. (Prove!) For convenience of notation let us denote the element $x\psi = x + V$ in the field E as a. Given $f(x) \in F[x]$, what is $f(x)\psi$? We claim that it is merely $f(a)$, for, since ψ is a homomorphism, if $f(x) = \beta_0 + \beta_1 x + \cdots + \beta_k x^k$, then $f(x)\psi = \beta_0\psi + (\beta_1\psi)(x\psi) + \cdots + (\beta_k\psi)(x\psi)^k$, and using the identification indicated above of $\beta\psi$ with β, we see that $f(x)\psi = f(a)$.

In particular, since $p(x) \in V$, $p(x)\psi = 0$; however, $p(x)\psi = p(a)$. *Thus the element* $a = x\psi$ *in* E *is a root of* $p(x)$. The field E has been shown to satisfy all the properties required in the conclusion of Theorem 5.3.1, and so this theorem is now proved.

An immediate consequence of this theorem is the

COROLLARY *If* $f(x) \in F[x]$, *then there is a finite extension* E *of* F *in which* $f(x)$ *has a root. Moreover,* $[E:F] \leq \deg f(x)$.

Proof. Let $p(x)$ be an irreducible factor of $f(x)$; any root of $p(x)$ is a root of $f(x)$. By the theorem there is an extension E of F with $[E:F] = \deg p(x) \leq \deg f(x)$ in which $p(x)$, and so, $f(x)$ has a root.

Although it is, in actuality, a corollary to the above corollary, the next theorem is of such great importance that we single it out as a theorem.

THEOREM 5.3.2 *Let* $f(x) \in F[x]$ *be of degree* $n \geq 1$. *Then there is an extension* E *of* F *of degree at most* $n!$ *in which* $f(x)$ *has* n *roots (and so, a full complement of roots).*

Proof. In the statement of the theorem, a root of multiplicity m is, of course, counted as m roots.

By the above corollary there is an extension E_0 of F with $[E_0:F] \leq n$ in which $f(x)$ has a root α. Thus in $E_0[x]$, $f(x)$ factors as $f(x) = (x - \alpha)q(x)$, where $q(x)$ is of degree $n - 1$. Using induction (or continuing the above process), there is an extension E of E_0 of degree at most $(n - 1)!$ in which $q(x)$ has $n - 1$ roots. Since any root of $f(x)$ is either α or a root of $q(x)$, we obtain in E all n roots of $f(x)$. Now, $[E:F] = [E:E_0][E_0:F] \leq (n-1)!n = n!$ All the pieces of the theorem are now established.

Theorem 5.3.2 asserts the existence of a finite extension E in which the given polynomial $f(x)$, of degree n, over F has n roots. If $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, $a_0 \neq 0$ and if the n roots in E are $\alpha_1, \ldots, \alpha_n$, making use of the corollary to Lemma 5.3.1, $f(x)$ can be factored over E as $f(x) = a_0(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$. Thus $f(x)$ splits up completely over E as a product of *linear* (first degree) factors. Since a finite extension of F exists with this property, a *finite extension of* F *of minimal degree* exists which also enjoys this property of decomposing $f(x)$ as a product of linear factors. For such a minimal extension, no proper subfield has the property that $f(x)$ factors over it into the product of linear factors. This prompts the

DEFINITION If $f(x) \in F[x]$, a finite extension E of F is said to be a *splitting field* over F for $f(x)$ if over E (that is, in $E[x]$), but not over any proper subfield of E, $f(x)$ can be factored as a product of linear factors.

We reiterate: *Theorem 5.3.2 guarantees for us the existence of splitting fields.* In fact, it says even more, for it assures that given a polynomial of degree n over F there is a splitting field of this polynomial which is an extension of F of degree at most $n!$ over F. We shall see later that this upper bound of $n!$ is actually taken on; that is, given n, we can find a field F and a polynomial of degree n in $F[x]$ such that the splitting field of $f(x)$ over F has degree $n!$.

Equivalent to the definition we gave of a splitting field for $f(x)$ over F is the statement: *E is a splitting field of $f(x)$ over F if E is a minimal extension of F in which $f(x)$ has n roots, where $n = \deg f(x)$.*

An immediate question arises: given two splitting fields E_1 and E_2 of the same polynomial $f(x)$ in $F[x]$, what is their relation to each other? At first glance, we have no right to assume that they are at all related. Our next objective is to show that they are indeed intimately related; in fact, that they are isomorphic by an isomorphism leaving every element of F fixed. It is in this direction that we now turn.

Let F and F' be two fields and let τ be an isomorphism of F onto F'. For convenience let us denote the image of any $\alpha \in F$ under τ by α'; that is, $\alpha\tau = \alpha'$. We shall maintain this notation for the next few pages.

Can we make use of τ to set up an isomorphism between $F[x]$ and $F'[t]$, the respective polynomial rings over F and F'? Why not try the obvious? For an arbitrary polynomial $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n \in F[x]$ we define τ^* by $f(x)\tau^* = (\alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n)\tau^* = \alpha_0' t^n + \alpha_1' t^{n-1} + \cdots + \alpha_n'$.

It is an easy and straightforward matter, which we leave to the reader, to verify.

LEMMA 5.3.3 *τ^* defines an isomorphism of $F[x]$ onto $F'[t]$ with the property that $\alpha\tau^* = \alpha'$ for every $\alpha \in F$.*

If $f(x)$ is in $F[x]$ we shall write $f(x)\tau^*$ as $f'(t)$. Lemma 5.3.3 immediately implies that factorizations of $f(x)$ in $F[x]$ result in like factorizations of $f'(t)$ in $F'[t]$, and vice versa. In particular, $f(x)$ is irreducible in $F[x]$ if and only if $f'(t)$ is irreducible in $F'[t]$.

However, at the moment, we are not particularly interested in polynomial rings, but rather, in extensions of F. Let us recall that in the proof of Theorem 5.1.2 we employed quotient rings of polynomial rings to obtain suitable extensions of F. In consequence it should be natural for us to study the relationship between $F[x]/(f(x))$ and $F'[t]/(f'(t))$, where $(f(x))$ denotes the ideal generated by $f(x)$ in $F[x]$ and $(f'(t))$ that generated by $f'(t)$ in $F'[t]$. The next lemma, which is relevant to this question, is actually part of a more general, purely ring-theoretic result, but we shall content ourselves with it as applied in our very special setting.

LEMMA 5.3.4 *There is an isomorphism* τ^{**} *of* $F[x]/(f(x))$ *onto* $F'[t]/(f'(t))$ *with the property that for every* $\alpha \in F$, $\alpha\tau^{**} = \alpha'$, $(x + (f(x)))\tau^{**} = t + (f'(t))$.

Proof. Before starting with the proof proper, we should make clear what is meant by the last part of the statement of the lemma. As we have already done several times, we can consider F as imbedded in $F[x]/(f(x))$ by identifying the element $\alpha \in F$ with the coset $\alpha + (f(x))$ in $F[x]/(f(x))$. Similarly, we can consider F' to be contained in $F'[t]/(f'(t))$. The isomorphism τ^{**} is then supposed to satisfy $[\alpha + (f(x))]\tau^{**} = \alpha' + (f'(t))$.

We seek an isomorphism τ^{**} of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$. What could be simpler or more natural than to try the τ^{**} defined by $[g(x) + (f(x))]\tau^{**} = g'(t) + (f'(t))$ for every $g(x) \in F[x]$? We leave it as an exercise to fill in the necessary details that the τ^{**} so defined is well defined and is an isomorphism of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$ with the properties needed to fulfill the statement of Lemma 5.3.4.

For our purpose—that of proving the uniqueness of splitting fields—Lemma 5.3.4 provides us with the entering wedge, for we can now prove

THEOREM 5.3.3 *If* $p(x)$ *is irreducible in* $F[x]$ *and if* v *is a root of* $p(x)$, *then* $F(v)$ *is isomorphic to* $F'(w)$ *where* w *is a root of* $p'(t)$; *moreover, this isomorphism* σ *can so be chosen that*

1. $v\sigma = w$.
2. $\alpha\sigma = \alpha'$ *for every* $\alpha \in F$.

Proof. Let v be a root of the irreducible polynomial $p(x)$ lying in some extension K of F. Let $M = \{f(x) \in F[x] \mid f(v) = 0\}$. Trivially M is an ideal of $F[x]$, and $M \neq F[x]$. Since $p(x) \in M$ and is an irreducible polynomial, we have that $M = (p(x))$. As in the proof of Theorem 5.1.2, map $F[x]$ into $F(v) \subset K$ by the mapping ψ defined by $q(x)\psi = q(v)$ for every $q(x) \in F[x]$. We saw earlier (in the proof of Theorem 5.1.2) that ψ maps $F[x]$ onto $F(v)$. The kernel of ψ is precisely M, so must be $(p(x))$. By the fundamental homomorphism theorem for rings there is an isomorphism ψ^* of $F[x]/(p(x))$ onto $F(v)$. Note further that $\alpha\psi^* = \alpha$ for every $\alpha \in F$. Summing up: ψ^* is an isomorphism of $F[x]/(p(x))$ onto $F(v)$ leaving every element of F fixed and with the property that $v = [x + (p(x))]\psi^*$.

Since $p(x)$ is irreducible in $F[x]$, $p'(t)$ is irreducible in $F'[t]$ (by Lemma 5.3.3), and so there is an isomorphism θ^* of $F'[t]/(p'(t))$ onto $F'(w)$ where w is a root of $p'(t)$ such that θ^* leaves every element of F' fixed and such that $[t + (p'(t)]\theta^* = w$.

We now stitch the pieces together to prove Theorem 5.3.3. By Lemma 5.3.4 there is an isomorphism τ^{**} of $F[x]/(p(x))$ onto $F'[t]/(p'(t))$ which coincides with τ on F and which takes $x + (p(x))$ onto $t + (p'(t))$. Con-

sider the mapping $\sigma = (\psi^*)^{-1}\tau^{**}\theta^*$ (motivated by

$$F(v) \xrightarrow{(\psi^*)^{-1}} \frac{F[x]}{(p(x))} \xrightarrow{\tau^{**}} \frac{F'[t]}{(p'(t))} \xrightarrow{\theta^*} F'(w))$$

of $F(v)$ onto $F'(w)$. It is an isomorphism of $F(v)$ onto $F'(w)$ since all the mapping ψ^*, τ^{**}, and θ^* are isomorphisms and onto. Moreover, since $v = [x + (p(x))]\psi^*$, $v\sigma = (v(\psi^*)^{-1})\tau^{**}\theta^* = ([x + (p(x)]\tau^{**})\theta^* = [t + (p'(t))]\theta^* = w$. Also, for $\alpha \in F$, $\alpha\sigma = (\alpha(\psi^*)^{-1})\tau^{**}\theta^* = (\alpha\tau^{**})\theta^* = \alpha'\theta^* = \alpha'$. We have shown that σ is an isomorphism satisfying all the requirements of the isomorphism in the statement of the theorem. Thus Theorem 5.3.3 has been proved.

A special case, but itself of interest, is the

COROLLARY *If $p(x) \in F[x]$ is irreducible and if a, b are two roots of $p(x)$, then $F(a)$ is isomorphic to $F(b)$ by an isomorphism which takes a onto b and which leaves every element of F fixed.*

We now come to the theorem which is, as we indicated earlier, the foundation stone on which the whole Galois theory rests. For us it is the focal point of this whole section.

THEOREM 5.3.4 *Any splitting fields E and E' of the polynomials $f(x) \in F[x]$ and $f'(t) \in F'[t]$, respectively, are isomorphic by an isomorphism ϕ with the property that $\alpha\phi = \alpha'$ for every $\alpha \in F$. (In particular, any two splitting fields of the same polynomial over a given field F are isomorphic by an isomorphism leaving every element of F fixed.)*

Proof. We should like to use an argument by induction; in order to do so, we need an integer-valued indicator of size which we can decrease by some technique or other. We shall use as our indicator the degree of some splitting field over the initial field. It may seem artificial (in fact, it may even be artificial), but we use it because, as we shall soon see, Theorem 5.3.3 provides us with the mechanism for decreasing it.

If $[E:F] = 1$, then $E = F$, whence $f(x)$ splits into a product of linear factors over F itself. By Lemma 5.3.3 $f'(t)$ splits over F' into a product of linear factors, hence $E' = F'$. But then $\phi = \tau$ provides us with an isomorphism of E onto E' coinciding with τ on F.

Assume the result to be true for any field F_0 and any polynomial $f(x) \in F_0[x]$ provided the degree of some splitting field E_0 of $f(x)$ has degree less than n over F_0, that is, $[E_0:F_0] < n$.

Suppose that $[E:F] = n > 1$, where E is a splitting field of $f(x)$ over F. Since $n > 1$, $f(x)$ has an irreducible factor $p(x)$ of degree $r > 1$. Let $p'(t)$ be the corresponding irreducible factor of $f'(t)$. Since E splits $f(x)$, a

full complement of roots of $f(x)$, and so, *a priori*, of roots of $p(x)$, are in E. Thus there is a $v \in E$ such that $p(v) = 0$; by Theorem 5.1.3, $[F(v):F] = r$. Similarly, there is a $w \in E'$ such that $p'(w) = 0$. By Theorem 5.3.4 there is an isomorphism σ of $F(v)$ onto $F'(w)$ with the property that $\alpha\sigma = \alpha'$ for every $\alpha \in F$.

Since $[F(v):F] = r > 1$,

$$[E:F(v)] = \frac{[E:F]}{[F(v):F]} = \frac{n}{r} < n.$$

We claim that E is a splitting field for $f(x)$ considered as a polynomial over $F_0 = F(v)$, for no subfield of E, containing F_0 and hence F, can split $f(x)$, since E is assumed to be a splitting field of $f(x)$ over F. Similarly E' is a splitting field for $f'(t)$ over $F_0' = F'(w)$. By our induction hypothesis there is an isomorphism ϕ of E onto E' such that $a\phi = a\sigma$ for all $a \in F_0$. But for every $\alpha \in F$, $\alpha\sigma = \alpha'$ hence for every $\alpha \in F \subset F_0$, $\alpha\phi = \alpha\sigma = \alpha'$. This completes the induction and proves the theorem.

To see the truth of the "(in particular . . .)" part, let $F = F'$ and let τ be the identity map $\alpha\tau = \alpha$ for every $\alpha \in F$. Suppose that E_1 and E_2 are two splitting fields of $f(x) \in F[x]$. Considering $E_1 = E \supset F$ and $E_2 = E' \supset F' = F$, and applying the theorem just proved, yields that E_1 and E_2 are isomorphic by an isomorphism leaving every element of F fixed.

In view of the fact that any two splitting fields of the same polynomial over F are isomorphic and by an isomorphism leaving every element of F fixed, we are justified in speaking about *the* splitting field, rather than *a* splitting field, for it is essentially unique.

Examples

1. Let F be any field and let $p(x) = x^2 + \alpha x + \beta$, $\alpha, \beta \in F$, be in $F[x]$. If K is any extension of F in which $p(x)$ has a root, a, then the element $b = -\alpha - a$ also in K is also a root of $p(x)$. If $b = a$ it is easy to check that $p(x)$ must then be $p(x) = (x - a)^2$, and so both roots of $p(x)$ are in K. If $b \neq a$ then again both roots of $p(x)$ are in K. Consequently, $p(x)$ can be split by an extension of degree 2 of F. We could also get this result directly by invoking Theorem 5.3.2.

2. Let F be the field of rational numbers and let $f(x) = x^3 - 2$. In the field of complex numbers the three roots of $f(x)$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, where $\omega = (-1 + \sqrt{3}\,i)/2$ and where $\sqrt[3]{2}$ is a real cube root of 2. Now $F(\sqrt[3]{2})$ cannot split $x^3 - 2$, for, as a subfield of the real field, it cannot contain the complex, but not real, number $\omega\sqrt[3]{2}$. Without explicitly determining it, what can we say about E, the splitting field of $x^3 - 2$ over

F? By Theorem 5.3.2, $[E:F] \leq 3! = 6$; by the above remark, since $x^3 - 2$ is irreducible over F and since $[F(\sqrt[3]{2}):F] = 3$, by the corollary to Theorem 5.1.1, $3 = [F(\sqrt[3]{2}):F] \mid [E:F]$. Finally, $[E:F] > [F(\sqrt[3]{2}):F] = 3$. The only way out is $[E:F] = 6$. We could, of course, get this result by making two extensions $F_1 = F(\sqrt[3]{2})$ and $E = F_1(\omega)$ and showing that ω satisfies an irreducible quadratic equation over F_1.

3. Let F be the field of rational numbers and let

$$f(x) = x^4 + x^2 + 1 \in F[x].$$

We claim that $E = F(\omega)$, where $\omega = (-1 + \sqrt{3}\,i)/2$, is a splitting field of $f(x)$. Thus $[E:F] = 2$, far short of the maximum possible $4! = 24$.

Problems

1. In the proof of Lemma 5.3.1, prove that the degree of $q(x)$ is one less than that of $p(x)$.
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.
3. Prove Lemma 5.3.3 in all detail.
4. Show that τ^{**} in Lemma 5.3.4 is well defined and is an isomorphism of $F[x]/(f(x))$ onto $F[t]/(f'(t))$.
5. In Example 3 at the end of this section prove that $F(\omega)$ 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) $x^6 + x^3 + 1$.
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 $p - 1$.

**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.

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.

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.

12. Prove that $F(\sqrt[3]{2})$, where F is the field of rational numbers, has no automorphisms other than the identity automorphism.

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 $p(x)$.

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 $p(x)$.

*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.

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 $sts^{-1} = i$.

5.4 Construction with Straightedge and Compass

We pause in our general development to examine some implications of the results obtained so far in some familiar, geometric situations.

A real number α is said to be a *constructible number* if by the use of straightedge and compass alone we can construct a line segment of length α. We assume that we are given some fundamental unit length. Recall that from high-school geometry we can construct with a straightedge and compass a line perpendicular to and a line parallel to a given line through a given point. From this it is an easy exercise (see Problem 1) to prove that if α and β are constructible numbers then so are $\alpha \pm \beta$, $\alpha\beta$, and when $\beta \neq 0$, α/β. Therefore, the set of constructible numbers form a subfield, W, of the field of real numbers.

In particular, since $1 \in W$, W must contain F_0, the field of rational numbers. We wish to study the relation of W to the rational field.

Since we shall have many occasions to use the phrase "construct by straightedge and compass" (and variants thereof) *the words construct, constructible, construction, will always mean by straightedge and compass.*

If $w \in W$, we can reach w from the rational field by a *finite* number of constructions.

Let F be any subfield of the field of real numbers. Consider all the points (x, y) in the real Euclidean plane both of whose coordinates x and y are in F; we call the set of these points the *plane of* F. Any straight line joining two points in the plane of F has an equation of the form $ax + by + c = 0$ where a, b, c are all in F (see Problem 2). Moreover, any circle having as center a point in the plane of F and having as radius an element of F has an equation of the form $x^2 + y^2 + ax + by + c = 0$, where all of a, b, c are in F (see Problem 3). We call such lines and circles *lines and circles in* F.

Given two lines in F which intersect in the real plane, then their intersection point is a point in the plane of F (see Problem 4). On the other hand, the intersection of a line in F and a circle in F need not yield a point in the plane of F. But, using the fact that the equation of a line in F is of the form $ax + by + c = 0$ and that of a circle in F is of the form $x^2 + y^2 + dx + ey + f = 0$, where a, b, c, d, e, f are all in F, we can show that when a line and circle of F intersect in the real plane, they intersect either in a point in the plane of F or in the plane of $F(\sqrt{\gamma})$ for some positive γ in F (see Problem 5). Finally, the intersection of two circles in F can be realized as that of a line in F and a circle in F, for if these two circles are $x^2 + y^2 + a_1x + b_1y + c_1 = 0$ and $x^2 + y^2 + a_2x + b_2y + c_2 = 0$, then their intersection is the intersection of either of these with the line $(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$, so also yields a point either in the plane of F or of $F(\sqrt{\gamma})$ for some positive γ in F.

Thus lines and circles of F lead us to points either in F or in quadratic extensions of F. If we now are in $F(\sqrt{\gamma_1})$ for some quadratic extension of F, then lines and circles in $F(\sqrt{\gamma_1})$ intersect in points in the plane of $F(\sqrt{\gamma_1}, \sqrt{\gamma_2})$ where γ_2 is a positive number in $F(\sqrt{\gamma_1})$. A point is constructible from F if we can find real numbers $\lambda_1, \ldots, \lambda_n$, such that $\lambda_1^2 \in F$, $\lambda_2^2 \in F(\lambda_1)$, $\lambda_3^2 \in F(\lambda_1, \lambda_2), \ldots, \lambda_n^2 \in F(\lambda_1, \ldots, \lambda_{n-1})$, such that the point is in the plane of $F(\lambda_1, \ldots, \lambda_n)$. Conversely, if $\gamma \in F$ is such that $\sqrt{\gamma}$ is real then we can realize γ as an intersection of lines and circles in F (see Problem 6). Thus a point is constructible from F if and only if we can find a finite number of real numbers $\lambda_1, \ldots, \lambda_n$, such that

1. $[F(\lambda_1):F] = 1$ or 2;
2. $[F(\lambda_1, \ldots, \lambda_i):F(\lambda_1, \ldots, \lambda_{i-1})] = 1$ or 2 for $i = 1, 2, \ldots, n$;

and such that our point lies in the plane of $F(\lambda_1, \ldots, \lambda_n)$.

We have defined a real number α to be constructible if by use of straightedge and compass we can construct a line segment of length α. But this translates, in terms of the discussion above, into: α is constructible if starting from the plane of the rational numbers, F_0, we can imbed α in a field obtained from F_0 by a finite number of quadratic extensions. This is

THEOREM 5.4.1 *The real number α is constructible if and only if we can find a finite number of real numbers $\lambda_1, \ldots, \lambda_n$ such that*

1. $\lambda_1^2 \in F_0$,
2. $\lambda_i^2 \in F_0(\lambda_1, \ldots, \lambda_{i-1})$ *for* $i = 1, 2, \ldots, n$,

such that $\alpha \in F_0(\lambda_1, \ldots, \lambda_n)$.

However, we can compute the degree of $F_0(\lambda_1, \ldots, \lambda_n)$ over F_0, for by Theorem 5.1.1

$$\begin{aligned}[F_0(\lambda_1, \ldots, \lambda_n):F_0] = {} & [F_0(\lambda_1, \ldots, \lambda_n):F_0(\lambda_1, \ldots, \lambda_{n-1})] \cdots \\ & \times [F_0(\lambda_1, \ldots, \lambda_i):F_0(\lambda_1, \ldots, \lambda_{i-1})] \cdots \\ & \times [F_0(\lambda_1):F_0].\end{aligned}$$

Since each term in the product is either 1 or 2, we get that

$$[F_0(\lambda_1, \ldots, \lambda_n):F_0] = 2^r,$$

and thus the

COROLLARY 1 *If α is constructible then α lies in some extension of the rationals of degree a power of* 2.

If α is constructible, by Corollary 1 above, there is a subfield K of the real field such that $\alpha \in K$ and such that $[K:F_0] = 2^r$. However, $F_0(\alpha) \subset K$, whence by the corollary to Theorem 5.1.1 $[F_0(\alpha):F_0] \mid [K:F_0] = 2^r$; thereby $[F_0(\alpha):F_0]$ is also a power of 2. However, if α satisfies an irreducible polynomial of degree k over F_0, we have proved in Theorem 5.1.3 that $[F_0(\alpha):F_0] = k$. Thus we get the important criterion for nonconstructibility

COROLLARY 2 *If the real number α satisfies an irreducible polynomial over the field of rational numbers of degree k, and if k is not a power of* 2, *then α is not constructible.*

This last corollary enables us to settle the ancient problem of trisecting an angle by straightedge and compass, for we prove

THEOREM 5.4.2 *It is impossible, by straightedge and compass alone, to trisect* 60°.

Proof. If we could trisect 60° by straightedge and compass, then the length $\alpha = \cos 20°$ would be constructible. At this point, let us recall the identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Putting $\theta = 20°$ and remembering that $\cos 60° = \frac{1}{2}$, we obtain $4\alpha^3 - 3\alpha = \frac{1}{2}$, whence $8\alpha^3 - 6\alpha - 1 = 0$. Thus α is a root of the polynomial $8x^3 - 6x - 1$ over the rational field.

However, this polynomial is irreducible over the rational field (Problem 7(a)), and since its degree is 3, which certainly is not a power of 2, by Corollary 2 to Theorem 5.4.1, α is not constructible. Thus 60° cannot be trisected by straightedge and compass.

Another ancient problem is that of duplicating the cube, that is, of constructing a cube whose volume is twice that of a given cube. If the original cube is the unit cube, this entails constructing a length α such that $\alpha^3 = 2$. Since the polynomial $x^3 - 2$ is irreducible over the rationals (Problem 7(b)), by Corollary 2 to Theorem 5.4.1, α is not constructible. Thus

THEOREM 5.4.3 *By straightedge and compass it is impossible to duplicate the cube.*

We wish to exhibit yet another geometric figure which cannot be constructed by straightedge and compass, namely, the regular septagon. To carry out such a construction would require the constructibility of $\alpha = 2\cos(2\pi/7)$. However, we claim that α satisfies $x^3 + x^2 - 2x - 1$ (Problem 8) and that this polynomial is irreducible over the field of rational numbers (Problem 7(c)). Thus again using Corollary 2 to Theorem 5.4.1 we obtain

THEOREM 5.4.4 *It is impossible to construct a regular septagon by straightedge and compass.*

Problems

1. Prove that if α, β are constructible, then so are $\alpha \pm \beta$, $\alpha\beta$, and α/β (when $\beta \neq 0$).
2. Prove that a line in F has an equation of the form $ax + by + c = 0$ with a, b, c 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.
4. Prove that two lines in F, which intersect in the real plane, intersect at a point 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.
6. If $\gamma \in F$ is positive, prove that $\sqrt{\gamma}$ is realizable as an intersection of lines and circles in F.

7. Prove that the following polynomials are irreducible over the field of rational numbers.
   (a) $8x^3 - 6x - 1$.
   (b) $x^3 - 2$.
   (c) $x^3 + x^2 - 2x - 1$.
8. Prove that $2 \cos (2\pi/7)$ satisfies $x^3 + x^2 - 2x - 1$. (*Hint:* Use $2 \cos (2\pi/7) = e^{2\pi i/7} + e^{-2\pi i/7}$.)
9. Prove that the regular pentagon is constructible.
10. Prove that the regular hexagon is constructible.
11. Prove that the regular 15-gon is constructible.
12. Prove that it is possible to trisect 72°.
13. Prove that a regular 9-gon is not constructible.

*14. Prove a regular 17-gon is constructible.

5.5 More about Roots

We return to the general exposition. Let F be any field and, as usual, let $F[x]$ be the ring of polynomials in x over F.

DEFINITION If $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_i x^{n-i} + \cdots + \alpha_{n-1}x + \alpha_n$ in $F[x]$, then the *derivative* of $f(x)$, written as $f'(x)$, is the polynomial $f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + \cdots + (n-i)\alpha_i x^{n-i-1} + \cdots + \alpha_{n-1}$ in $F[x]$.

To make this definition or to prove the basic formal properties of the derivatives, as applied to polynomials, does not require the concept of a limit. However, since the field F is arbitrary, we might expect some strange things to happen.

At the end of Section 5.2, we defined what is meant by the characteristic of a field. Let us recall it now. A field F is said to be of characteristic 0 if $ma \neq 0$ for $a \neq 0$ in F and $m > 0$, an integer. If $ma = 0$ for some $m > 0$ and some $a \neq 0 \in F$, then F is said to be of finite characteristic. In this second case, the characteristic of F is defined to be the smallest positive integer p such that $pa = 0$ for all $a \in F$. It turned out that if F is of finite characteristic then its characteristic p is a prime number.

We return to the question of the derivative. Let F be a field of characteristic $p \neq 0$. In this case, the derivative of the polynomial x^p is $px^{p-1} = 0$. Thus the usual result from the calculus that a polynomial whose derivative is 0 must be a constant no longer need hold true. However, if the characteristic of F is 0 and if $f'(x) = 0$ for $f(x) \in F[x]$, it is indeed true that $f(x) = \alpha \in F$ (see Problem 1). Even when the characteristic of F is $p \neq 0$, we can still describe the polynomials with zero derivative; if $f'(x) = 0$, then $f(x)$ is a polynomial in x^p (see Problem 2).

We now prove the analogs of the formal rules of differentiation that we know so well.

LEMMA 5.5.1 *For any $f(x), g(x) \in F[x]$ and any $\alpha \in F$,*

1. $(f(x) + g(x))' = f'(x) + g'(x)$.
2. $(\alpha f(x))' = \alpha f'(x)$.
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Proof. The proofs of parts 1 and 2 are extremely easy and are left as exercises. To prove part 3, note that from parts 1 and 2 it is enough to prove it in the highly special case $f(x) = x^i$ and $g(x) = x^j$ where both i and j are positive. But then $f(x)g(x) = x^{i+j}$, whence $(f(x)g(x))' = (i + j)x^{i+j-1}$; however, $f'(x)g(x) = ix^{i-1}x^j = ix^{i+j-1}$ and $f(x)g'(x) = jx^ix^{j-1} = jx^{i+j-1}$; consequently, $f'(x)g(x) + f(x)g'(x) = (i + j)x^{i+j-1} = (f(x)g(x))'$.

Recall that in elementary calculus the equivalence is shown between the existence of a multiple root of a function and the simultaneous vanishing of the function and its derivative at a given point. Even in our setting, where F is an arbitrary field, such an interrelation exists.

LEMMA 5.5.2 *The polynomial $f(x) \in F[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a nontrivial (that is, of positive degree) common factor.*

Proof. Before proving the lemma proper, a related remark is in order, namely, if $f(x)$ and $g(x)$ in $F[x]$ have a nontrivial common factor in $K[x]$, for K an extension of F, then they have a nontrivial common factor in $F[x]$. For, were they relatively prime as elements in $F[x]$, then we would be able to find two polynomials $a(x)$ and $b(x)$ in $F[x]$ such that $a(x)f(x) + b(x)g(x) = 1$. Since this relation also holds for those elements viewed as elements of $K[x]$, in $K[x]$ they would have to be relatively prime.

Now to the lemma itself. From the remark just made, we may assume, without loss of generality, that the roots of $f(x)$ all lie in F (otherwise extend F to K, the splitting field of $f(x)$). If $f(x)$ has a multiple root α, then $f(x) = (x - \alpha)^m q(x)$, where $m > 1$. However, as is easily computed, $((x - \alpha)^m)' = m(x - \alpha)^{m-1}$ whence, by Lemma 5.5.1, $f'(x) = (x - \alpha)^m q'(x) + m(x - \alpha)^{m-1}q(x) = (x - \alpha)r(x)$, since $m > 1$. But this says that $f(x)$ and $f'(x)$ have the common factor $x - \alpha$, thereby proving the lemma in one direction.

On the other hand, if $f(x)$ has no multiple root then $f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$ where the α_i's are all distinct (we are supposing $f(x)$ to be monic). But then

$$f'(x) = \sum_{i=1}^{n} (x - \alpha_1)\cdots\widehat{(x - \alpha_i)}\cdots(x - \alpha_n)$$

where the $\wedge$ denotes the term is omitted. We claim no root of $f(x)$ is a root of $f'(x)$, for

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0,$$

since the roots are all distinct. However, if $f(x)$ and $f'(x)$ have a nontrivial common factor, they have a common root, namely, any root of this common factor. The net result is that $f(x)$ and $f'(x)$ have no nontrivial common factor, and so the lemma has been proved in the other direction.

COROLLARY 1 *If $f(x) \in F[x]$ is irreducible, then*

1. *If the characteristic of F is 0, $f(x)$ has no multiple roots.*
2. *If the characteristic of F is $p \neq 0$, $f(x)$ has a multiple root only if it is of the form $f(x) = g(x^p)$.*

Proof. Since $f(x)$ is irreducible, its only factors in $F[x]$ are 1 and $f(x)$. If $f(x)$ has a multiple root, then $f(x)$ and $f'(x)$ have a nontrivial common factor by the lemma, hence $f(x) \mid f'(x)$. However, since the degree of $f'(x)$ is less than that of $f(x)$, the only possible way that this can happen is for $f'(x)$ to be 0. In characteristic 0 this implies that $f(x)$ is a constant, which has no roots; in characteristic $p \neq 0$, this forces $f(x) = g(x^p)$.

We shall return in a moment to discuss the implications of Corollary 1 more fully. But first, for later use in Chapter 7 in our treatment of finite fields, we prove the rather special

COROLLARY 2 *If F is a field of characteristic $p \neq 0$, then the polynomial $x^{p^n} - x \in F[x]$, for $n \geq 1$, has distinct roots.*

Proof. The derivative of $x^{p^n} - x$ is $p^n x^{p^n - 1} - 1 = -1$, since F is of characteristic p. Therefore, $x^{p^n} - x$ and its derivative are certainly relatively prime, which, by the lemma, implies that $x^{p^n} - x$ has no multiple roots.

Corollary 1 does not rule out the possibility that in characteristic $p \neq 0$ an irreducible polynomial might have multiple roots. To clinch matters, we exhibit an example where this actually happens. Let F_0 be a field of characteristic 2 and let $F = F_0(x)$ be the field of rational functions in x over F_0. We claim that the polynomial $t^2 - x$ in $F[t]$ is irreducible over F and that its roots are equal. To prove irreducibility we must show that there is no rational function in $F_0(x)$ whose square is x; this is the content of Problem 4. To see that $t^2 - x$ has a multiple root, notice that its derivative (the derivative is with respect to t; for x, being in F, is considered as a constant) is $2t = 0$. Of course, the analogous example works for any prime characteristic.

Now that the possibility has been seen to be an actuality, it points out a sharp difference between the case of characteristic 0 and that of characteristic p. The presence of irreducible polynomials with multiple roots in the latter case leads to many interesting, but at the same time complicating, subtleties. These require a more elaborate and sophisticated treatment which we prefer to avoid at this stage of the game. *Therefore, we make the flat assumption for the rest of this chapter that all fields occurring in the text material proper are fields of characteristic* 0.

DEFINITION The extension K of F is a *simple extension of* F if $K = F(\alpha)$ for some α in K.

In characteristic 0 (or in properly conditioned extensions in characteristic $p \neq 0$; see Problem 14) all finite extensions are realizable as simple extensions. This result is

THEOREM 5.5.1 *If F is of characteristic* 0 *and if a, b, are algebraic over F, then there exists an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.*

Proof. Let $f(x)$ and $g(x)$, of degrees m and n, be the irreducible polynomials over F satisfied by a and b, respectively. Let K be an extension of F in which both $f(x)$ and $g(x)$ split completely. Since the characteristic of F is 0, all the roots of $f(x)$ are distinct, as are all those of $g(x)$. Let the roots of $f(x)$ be $a = a_1, a_2, \ldots, a_m$ and those of $g(x)$, $b = b_1, b_2, \ldots, b_n$.

If $j \neq 1$, then $b_j \neq b_1 = b$, hence the equation $a_i + \lambda b_j = a_1 + \lambda b_1 = a + \lambda b$ has only one solution λ in K, namely,

$$\lambda = \frac{a_i - a}{b - b_j}$$

Since F is of characteristic 0 it has an infinite number of elements, so we can find an element $\gamma \in F$ such that $a_i + \gamma b_j \neq a + \gamma b$ for all i and for all $j \neq 1$. Let $c = a + \gamma b$; our contention is that $F(c) = F(a, b)$. Since $c \in F(a, b)$, we certainly do have that $F(c) \subset F(a, b)$. We will now show that both a and b are in $F(c)$ from which it will follow that $F(a, b) \subset F(c)$.

Now b satisfies the polynomial $g(x)$ over F, hence satisfies $g(x)$ considered as a polynomial over $K = F(c)$. Moreover, if $h(x) = f(c - \gamma x)$ then $h(x) \in K[x]$ and $h(b) = f(c - \gamma b) = f(a) = 0$, since $a = c - \gamma b$. Thus in some extension of K, $h(x)$ and $g(x)$ have $x - b$ as a common factor. We assert that $x - b$ is in fact their greatest common divisor. For, if $b_j \neq b$ is another root of $g(x)$, then $h(b_j) = f(c - \gamma b_j) \neq 0$, since by our choice of γ, $c - \gamma b_j$ for $j \neq 1$ avoids all roots a_i of $f(x)$. Also, since $(x - b)^2 \nmid g(x)$, $(x - b)^2$ cannot divide the greatest common divisor of $h(x)$ and $g(x)$. Thus $x - b$ is the greatest common divisor of $h(x)$ and $g(x)$ over some extension

of K. But then they have a nontrivial greatest common divisor over K, which must be a divisor of $x - b$. Since the degree of $x - b$ is 1, we see that the greatest common divisor of $g(x)$ and $h(x)$ in $K[x]$ is exactly $x - b$. Thus $x - b \in K[x]$, whence $b \in K$; remembering that $K = F(c)$, we obtain that $b \in F(c)$. Since $a = c - \gamma b$, and since $b, c \in F(c)$, $\gamma \in F \subset F(c)$, we get that $a \in F(c)$, whence $F(a, b) \subset F(c)$. The two opposite containing relations combine to yield $F(a, b) = F(c)$.

A simple induction argument extends the result from 2 elements to any finite number, that is, if $\alpha_1, \ldots, \alpha_n$ are algebraic over F, then there is an element $c \in F(\alpha_1, \ldots, \alpha_n)$ such that $F(c) = F(\alpha_1, \ldots, \alpha_n)$. Thus the

COROLLARY *Any finite extension of a field of characteristic* 0 *is a simple extension.*

Problems

1. If F is of characteristic 0 and $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = \alpha \in F$.
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 $g(x) \in F[x]$.
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 $\alpha \in F$.
4. Prove that 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.

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.
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.
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.
*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 $b^p = a$.
10. Using the result of Problem 9, prove that any finite field is perfect.

**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.

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.

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 $a^{p^n} \in F$.

14. If K is a finite, separable extension of F prove that 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.

5.6 The Elements of Galois Theory

Given a polynomial $p(x)$ in $F[x]$, the polynomial ring in x over F, we shall associate with $p(x)$ a group, called the *Galois group* of $p(x)$. There is a very close relationship between the roots of a polynomial and its Galois group; in fact, the Galois group will turn out to be a certain permutation group of the roots of the polynomial. We shall make a study of these ideas in this, and in the next, section.

The means of introducing this group will be through the splitting field of $p(x)$ over F, the Galois group of $p(x)$ being defined as a certain group of automorphisms of this splitting field. This accounts for our concern, in so many of the theorems to come, with the automorphisms of a field. A beautiful duality, expressed in the fundamental theorem of the Galois theory (Theorem 5.6.6), exists between the subgroups of the Galois group and the subfields of the splitting field. From this we shall eventually derive a condition for the solvability by means of radicals of the roots of a polynomial in terms of the algebraic structure of its Galois group. From this will follow the classical result of Abel that the general polynomial of degree 5 is not solvable by radicals. Along the way we shall also derive, as side results, theorems of great interest in their own right. One such will be the fundamental theorem on symmetric functions. Our approach to the subject is founded on the treatment given it by Artin.

Recall that we are assuming that all our fields are of characteristic 0, hence we can (and shall) make free use of Theorem 5.5.1 and its corollary.

By an *automorphism of the field* K we shall mean, as usual, a mapping σ of K onto itself such that $\sigma(a + b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in K$. Two automorphisms σ and τ of K are said to be distinct if $\sigma(a) \neq \tau(a)$ for some element a in K.

We begin the material with

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: ALGEBRA **Subject Code: 19MMP101**
Class : I - M.Sc. Mathematics **Semester : I**

Unit IV

Part A (20x1=20 Marks)
Possible Questions

Question	Opt 1	Opt 2	Opt 3	Opt 4	Answer
A field K is said to be an extension of F if ----------	F⊆K	F=K	K⊆F	F<K	F⊆K
A field K is said to be an ---------- F if F⊆K	zero divisor	primitive	irreducible	extension	extension
The ---------- is the dimension of K as a vector space over F	degree of F over K	degree of K over F	degree of F	none	degree of K over F
The degree of K over F is the ---------- of K as a vector space over F	degree of F over K	dimension	degree of F	none	dimension
If L is a finite extension of K and K is a finite extension of F,then---- --------	L is a finite extension of K	K is a finite extension of K	L is a finite extension of F	K is a finite extension of L	L is a finite extension of F
If---------- and K is a finite extension of F,then L is a finite extension of F	L is a finite extension of K	K is a finite extension of K	L is a finite extension of F	K is a finite extension of L	L is a finite extension of K
If L is a finite extension of K and ---------- ,then L is a finite extension of F	L is a finite extension of K	K is a finite extension of F	L is a finite extension of F	K is a finite extension of L	K is a finite extension of F
If a∈K is algebraic of degree n over F,then ----------	[F(a):F] = n	[F(a):F] =m	[F(a):F] =0	[F(a):F] = a	[F(a):F] = n
If a∈K is ----------,then [F(a):F] = n	algebraic of degree n over F	algebraic of degree n over F	algebraic of degree n over F	algebraic of degree n over F	algebraic of degree n over F
If a and b in K are ----------F then a+b, a-b, ab, a/b are all algebraic over F	algebraic over K	algebraic over F	algebraic of degree F	algebraicof degree K	algebraic over F
The elements in K which are algebraic over F form a ---------of K	field	subfield	root	group	subfield
If α is constructible then α lies in some extension of the rationals of degree ------	power of 2	power of 3	not a power of 3	not a power of 2	power of 2
If the ----------α satisfies an irreducible polynomial over the field of rational numbers of degree k,and if k is not a power of 2 ,then α is not constuctible.	real number	rational number	irrational number	complex number	real number
If the real number α satisfies an irreducible polynomial over the field of rational numbers of degree k,and if k is----------,then α is not constuctible.	power of 2	power of 3	not a power of 3	not a power of 2	not a power of 2
G(K,F) is a ---------- of the group of all automorphisms of K	group	sub group	normal subgroup	none	sub group
If U is an ideal of the ring R then R/U is a ---------- and is a homomorphic image of R	field	group	sub group	ring	ring
If U is an ideal of the ring R then R/U is a ring and is a ---------- image of R	homomorphic	isomorphic	homeomorphic	automorphic	homomorphic
If U is --------- of the ring R then R/U is a ring and is a homomorphic image of R	group	ring	ideal	field	ideal

If R is a commutative ring with a unit element and M is an ---------- of R then M is a maximal ideal of R iff R/M is a field	group	ring	ideal	field	ideal
If R is a commutative ring with a unit element and M is an ideal of R then M is a maximal ideal of R iff R/M is a -------	group	ring	ideal	field	field
If R is a commutative ring with a unit element and M is an ideal of R then M is a ---------- of R iff R/M is a field	maximal ideal	ring	ideal	minimal ideal	maximal ideal
If R is a commutative ring with a unit element and M is an ideal of R then M is a maximal ideal of R iff--------- is a field	R	R/M	R and M	M	R/M
Every -------- can be imbedded in a field	integral domaim	ring	ideal	field	integral domaim
Every integral domaim can be imbedded in a ----------	integral domaim	ring	ideal	field	field
A---------- possesses a unit element	integral domain	ring	ideal	Eucledian ring	Eucledian ring
If --------- U of a ring R contains a unit of R then U=R	Euclidean ring	ring	ideal	field	ideal
If an ideal U of a --------- R contains a unit of R then U=R	Euclidean ring	ring	field	ideal	ring
If an ideal U of a ring R contains a unit of R then--------	U=R	U<R	U>R	U≤R	U=R
A --------- said to be generating set of V if L(S) = V.	set S	ring	ideal U	Euclidean ring	set S
A set S said to be ---------- of V if L(S) = V.	maximal ideal	ideal	generating set	field	generating set
A set S said to be generating set of V if ---------.	L(S) = V	L(S) = 0	L(V) =S	L(S) = 1	L(S) = V
Any ---------- F is a finite extension of F.	ring	field	ideal	group	field
Any field F is a ----------of F.	primitive	irreducible	extension	finite extension	finite extension
An element a ∈k is said to be ---------- over F if it is not algebraic over F	generating set	transcendental	extension	finite extension	transcendental
An element a ∈k is said to be transcendental over F if it is ----------	not algebraic over F	algebraic over F	finite extension of L	not a finite extension of L	not algebraic over F
A ---------- K is said to be an extension F if F⊆K	field	ring	ideal	group	field
A ---------- is said to be an algebraic number if it is algebraic over field of rational number.	real number	rational number	irrational number	complex number	complex number
A complex number is said to be an ---------- if it is algebraic over field of rational number.	rational number	irrational number	algebraic number	real number	algebraic number
A complex number is said to be an algebraic number if it is ---------- over field of rational number.	real	algebraic	integers	rational	algebraic
A complex number is said to be an algebraic number if it is algebraic over ----- of rational number.	field	ring	ideal	group	field
A complex number is said to be an algebraic number if it is algebraic over field of ----------.	real number	irrational number	rational number	algebraic number	rational number
An ---------- of a fields F is said to be simple extension if k = F(a) for some a∈k	Euclidean ring R	transcendental k	extension k	finite extension k	extension k

An extension k of a fields F is said to be ---------- if k = F(a) for some a∈k	Euclidean ring	transcendental	extension	simple extension	simple extension
An extension k of a fields F is said to be simple extension if ---------- for some a∈k	k = F(0)	k = F(a)	k = F(1)	k = F(a *1)	k = F(a)
A ---------- is called Prefect if all its Finite extension of F is separable.	field	ring	ideal	group	field
A field F is called ----------if all its Finite extension of F is separable.	algebraic	Prefect	prime	normal	Prefect
A field F is called Prefect if all its---------- of F is separable.	primitive	irreducible	extension	finite extension	finite extension
A field F is called Prefect if all its Finite extension of F is ----------	irreducible	transcendental	separable	inseparable	separable

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

CLASS: I M.Sc. MATHEMATICS **COURSENAME: ALGEBRA**

COURSE CODE: 19MMP101 **BATCH-2019-2021**

UNIT-V

GALOIS THEORY

The elements of Galois theory - Solvability by radicals - Galois group over the rational.

**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.

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.

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 $a^{p^n} \in F$.

14. If K is a finite, separable extension of F prove that 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.

5.6 The Elements of Galois Theory

Given a polynomial $p(x)$ in $F[x]$, the polynomial ring in x over F, we shall associate with $p(x)$ a group, called the *Galois group* of $p(x)$. There is a very close relationship between the roots of a polynomial and its Galois group; in fact, the Galois group will turn out to be a certain permutation group of the roots of the polynomial. We shall make a study of these ideas in this, and in the next, section.

The means of introducing this group will be through the splitting field of $p(x)$ over F, the Galois group of $p(x)$ being defined as a certain group of automorphisms of this splitting field. This accounts for our concern, in so many of the theorems to come, with the automorphisms of a field. A beautiful duality, expressed in the fundamental theorem of the Galois theory (Theorem 5.6.6), exists between the subgroups of the Galois group and the subfields of the splitting field. From this we shall eventually derive a condition for the solvability by means of radicals of the roots of a polynomial in terms of the algebraic structure of its Galois group. From this will follow the classical result of Abel that the general polynomial of degree 5 is not solvable by radicals. Along the way we shall also derive, as side results, theorems of great interest in their own right. One such will be the fundamental theorem on symmetric functions. Our approach to the subject is founded on the treatment given it by Artin.

Recall that we are assuming that all our fields are of characteristic 0, hence we can (and shall) make free use of Theorem 5.5.1 and its corollary.

By an *automorphism of the field* K we shall mean, as usual, a mapping σ of K onto itself such that $\sigma(a + b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in K$. Two automorphisms σ and τ of K are said to be distinct if $\sigma(a) \neq \tau(a)$ for some element a in K.

We begin the material with

THEOREM 5.6.1 *If K is a field and if $\sigma_1, \ldots, \sigma_n$ are distinct automorphisms of K, then it is impossible to find elements $a_1, \ldots, a_n$, not all 0, in K such that $a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma_n(u) = 0$ for all $u \in K$.*

Proof. Suppose we could find a set of elements $a_1, \ldots, a_n$ in K, not all 0, such that $a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) = 0$ for all $u \in K$. Then we could find such a relation having as few nonzero terms as possible; on renumbering we can assume that this minimal relation is

$$a_1\sigma_1(u) + \cdots + a_m\sigma_m(u) = 0 \tag{1}$$

where $a_1, \ldots, a_m$ are all different from 0.

If m were equal to 1 then $a_1\sigma_1(u) = 0$ for all $u \in K$, leading to $a_1 = 0$, contrary to assumption. Thus we may assume that $m > 1$. Since the automorphisms are distinct there is an element $c \in K$ such that $\sigma_1(c) \neq \sigma_m(c)$. Since $cu \in K$ for all $u \in K$, relation (1) must also hold for cu, that is, $a_1\sigma_1(cu) + a_2\sigma_2(cu) + \cdots + a_m\sigma_m(cu) = 0$ for all $u \in K$. Using the hypothesis that the σ's are automorphisms of K, this relation becomes

$$a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_2(c)\sigma_2(u) + \cdots + a_m\sigma_m(c)\sigma_m(u) = 0. \tag{2}$$

Multiplying relation (1) by $\sigma_1(c)$ and subtracting the result from (2) yields

$$a_2(\sigma_2(c) - \sigma_1(c))\sigma_2(u) + \cdots + a_m(\sigma_m(c) - \sigma_1(c))\sigma_m(u) = 0. \tag{3}$$

If we put $b_i = a_i(\sigma_i(c) - \sigma_1(c))$ for $i = 2, \ldots, m$, then the b_i are in K, $b_m = a_m(\sigma_m(c) - \sigma_1(c)) \neq 0$, since $a_m \neq 0$, and $\sigma_m(c) - \sigma_1(c) \neq 0$ yet $b_2\sigma_2(u) + \cdots + b_m\sigma_m(u) = 0$ for all $u \in K$. This produces a shorter relation, contrary to the choice made; thus the theorem is proved.

DEFINITION If G is a group of automorphisms of K, then the *fixed field* of G is the set of all elements $a \in K$ such that $\sigma(a) = a$ for all $\sigma \in G$.

Note that this definition makes perfectly good sense even if G is not a group but is merely a set of automorphisms of K. However, the fixed field of a set of automorphisms and that of the group of automorphisms generated by this set (in the group of all automorphisms of K) are equal (Problem 1), hence we lose nothing by defining the concept just for groups of automorphisms. Besides, we shall only be interested in the fixed fields of groups of automorphisms.

Having called the set, in the definition above, the fixed *field* of G, it would be nice if this terminology were accurate. That it is we see in

LEMMA 5.6.1 *The fixed field of G is a subfield of K.*

Proof. Let a, b be in the fixed field of G. Thus for all $\sigma \in G$, $\sigma(a) = a$ and $\sigma(b) = b$. But then $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b$ and $\sigma(ab) = \sigma(a)\sigma(b) = ab$; hence $a \pm b$ and ab are again in the fixed field of G. If $b \neq 0$, then $\sigma(b^{-1}) = \sigma(b)^{-1} = b^{-1}$, hence b^{-1} also falls in the fixed field of G. Thus we have verified that the fixed field of G is indeed a subfield of K.

We shall be concerned with the automorphisms of a field which behave in a prescribed manner on a given subfield.

DEFINITION Let K be a field and let F be a subfield of K. Then the *group of automorphisms of K relative to F*, written $G(K, F)$, is the set of *all* automorphisms of K leaving every element of F fixed; that is, the automorphism σ of K is in $G(K, F)$ if and only if $\sigma(\alpha) = \alpha$ for every $\alpha \in F$.

It is not surprising, and is quite easy to prove

LEMMA 5.6.2 *$G(K, F)$ is a subgroup of the group of all automorphisms of K.*

We leave the proof of this lemma to the reader. One remark: K contains the field of rational numbers F_0, since K is of characteristic 0, and it is easy to see that the fixed field of any group of automorphisms of K, being a field, must contain F_0. Hence, every rational number is left fixed by every automorphism of K.

We pause to examine a few examples of the concepts just introduced.

Example 5.6.1 Let K be the field of complex numbers and let F be the field of real numbers. We compute $G(K, F)$. If σ is any automorphism of K, since $i^2 = -1$, $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, hence $\sigma(i) = \pm i$. If, in addition, σ leaves every real number fixed, then for any $a + bi$ where a, b are real, $\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a \pm bi$. Each of these possibilities, namely the mapping $\sigma_1(a + bi) = a + bi$ and $\sigma_2(a + bi) = a - bi$ defines an automorphism of K, σ_1 being the identity automorphism and σ_2 complex-conjugation. Thus $G(K, F)$ is a group of order 2.

What is the fixed field of $G(K, F)$? It certainly must contain F, but does it contain more? If $a + bi$ is in the fixed field of $G(K, F)$ then $a + bi = \sigma_2(a + bi) = a - bi$, whence $b = 0$ and $a = a + bi \in F$. In this case we see that the fixed field of $G(K, F)$ is precisely F itself.

Example 5.6.2 Let F_0 be the field of rational numbers and let $K = F_0(\sqrt[3]{2})$ where $\sqrt[3]{2}$ is the real cube root of 2. Every element in K is of the form $\alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2$, where $\alpha_0, \alpha_1, \alpha_2$ are rational numbers. If

σ is an automorphism of K, then $\sigma(\sqrt[3]{2})^3 = \sigma((\sqrt[3]{2})^3) = \sigma(2) = 2$, hence $\sigma(\sqrt[3]{2})$ must also be a cube root of 2 lying in K. However, there is only one real cube root of 2, and since K is a subfield of the real field, we must have that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. But then $\sigma(\alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2) = \alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2$, that is, σ is the identity automorphism of K. We thus see that $G(K, F_0)$ consists only of the identity map, and in this case the *fixed field of* $G(K, F_0)$ *is not* F_0 *but is, in fact, larger, being all of* K.

Example 5.6.3 Let F_0 be the field of rational numbers and let $\omega = e^{2\pi i/5}$; thus $\omega^5 = 1$ and ω satisfies the polynomial $x^4 + x^3 + x^2 + x + 1$ over F_0. By the Eisenstein criterion one can show that $x^4 + x^3 + x^2 + x + 1$ is irreducible over F_0 (see Problem 3). Thus $K = F_0(\omega)$ is of degree 4 over F_0 and every element in K is of the form $\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3$ where all of $\alpha_0, \alpha_1, \alpha_2$, and α_3 are in F_0. Now, for any automorphism σ of K, $\sigma(\omega) \neq 1$, since $\sigma(1) = 1$, and $\sigma(\omega)^5 = \sigma(\omega^5) = \sigma(1) = 1$, whence $\sigma(\omega)$ is also a 5th root of unity. In consequence, $\sigma(\omega)$ can only be one of $\omega, \omega^2, \omega^3$, or ω^4. We claim that each of these possibilities actually occurs, for let us define the four mappings $\sigma_1, \sigma_2, \sigma_3$, and σ_4 by $\sigma_i(\alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3) = \alpha_0 + \alpha_1(\omega^i) + \alpha_2(\omega^i)^2 + \alpha_3(\omega^i)^3$, for $i = 1, 2, 3$, and 4. Each of these defines an automorphism of K (Problem 4). Therefore, since $\sigma \in G(K, F_0)$ is completely determined by $\sigma(\omega)$, $G(K, F_0)$ is a group of order 4, with σ_1 as its unit element. In light of $\sigma_2^2 = \sigma_4$, $\sigma_2^3 = \sigma_3$, $\sigma_2^4 = \sigma_1$, $G(K, F_0)$ is a cyclic group of order 4. One can easily prove that the fixed field of $G(K, F_0)$ is F_0 itself (Problem 5). The subgroup $A = \{\sigma_1, \sigma_4\}$ of $G(K, F_0)$ has as its fixed field the set of all elements $\alpha_0 + \alpha_2(\omega^2 + \omega^3)$, which is an extension of F_0 of degree 2.

The examples, although illustrative, are still too special, for note that in each of them $G(K, F)$ turned out to be a cyclic group. This is highly atypical for, in general, $G(K, F)$ need not even be abelian (see Theorem 5.6.3). However, despite their speciality, they do bring certain important things to light. For one thing they show that we must study the effect of the automorphisms on the roots of polynomials and, for another, they point out that F *need not* be equal to all of the fixed field of $G(K, F)$. The cases in which this does happen are highly desirable ones and are situations with which we shall soon spend much time and effort.

We now compute an important bound on the size of $G(K, F)$.

THEOREM 5.6.2 *If* K *is a finite extension of* F, *then* $G(K, F)$ *is a finite group and its order,* $o(G(K, F))$ *satisfies* $o(G(K, F)) \leq [K:F]$.

Proof. Let $[K:F] = n$ and suppose that $u_1, \ldots, u_n$ is a basis of K over F. Suppose we can find $n + 1$ distinct automorphisms $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$

in $G(K, F)$. By the corollary to Theorem 4.3.3 the system of n homogeneous linear equations in the $n + 1$ unknowns $x_1, \ldots, x_{n+1}$:

$$\begin{aligned}
&\sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \cdots + \sigma_{n+1}(u_1)x_{n+1} = 0 \\
&\vdots \\
&\sigma_1(u_i)x_1 + \sigma_2(u_i)x_2 + \cdots + \sigma_{n+1}(u_i)x_{n+1} = 0 \\
&\vdots \\
&\sigma_1(u_n)x_1 + \sigma_2(u_n)x_2 + \cdots + \sigma_{n+1}(u_n)x_{n+1} = 0
\end{aligned}$$

has a nontrivial solution (not all 0) $x_1 = a_1, \ldots, x_{n+1} = a_{n+1}$ in K. Thus

$$a_1\sigma_1(u_i) + a_2\sigma_2(u_i) + \cdots + a_{n+1}\sigma_{n+1}(u_i) = 0 \qquad (1)$$

for $i = 1, 2, \ldots, n$.

Since every element in F is left fixed by each σ_i and since an arbitrary element t in K is of the form $t = \alpha_1 u_1 + \cdots + \alpha_n u_n$ with $\alpha_1, \ldots, \alpha_n$ in F, then from the system of equations (1) we get $a_1\sigma_1(t) + \cdots + a_{n+1}\sigma_{n+1}(t) = 0$ for all $t \in K$. But this contradicts the result of Theorem 5.6.1. Thus Theorem 5.6.2 has been proved.

Theorem 5.6.2 is of central importance in the Galois theory. However, aside from its key role there, it serves us well in proving a classic result concerned with symmetric rational functions. This result on symmetric functions in its turn will play an important part in the Galois theory.

First a few remarks on the field of rational functions in n-variables over a field F. Let us recall that in Section 3.11 we defined the ring of polynomials in the n-variables $x_1, \ldots, x_n$ over F and from this defined the field of rational functions in $x_1, \ldots, x_n$, $F(x_1, \ldots, x_n)$, over F as the ring of all quotients of such polynomials.

Let S_n be the symmetric group of degree n considered to be acting on the set $[1, 2, \ldots, n]$; for $\sigma \in S_n$ and i an integer with $1 \leq i \leq n$, let $\sigma(i)$ be the image of i under σ. We can make S_n act on $F(x_1, \ldots, x_n)$ in the following natural way: for $\sigma \in S_n$ and $r(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n)$, define the mapping which takes $r(x_1, \ldots, x_n)$ onto $r(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. We shall write this mapping of $F(x_1, \ldots, x_n)$ onto itself also as σ. It is obvious that these mappings define automorphisms of $F(x_1, \ldots, x_n)$. What is the fixed field of $F(x_1, \ldots, x_n)$ with respect to S_n? It consists of all rational functions $r(x_1, \ldots, x_n)$ such that $r(x_1, \ldots, x_n) = r(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for all $\sigma \in S_n$. But these are precisely those elements in $F(x_1, \ldots, x_n)$ which are known as the *symmetric rational functions*. Being the fixed field of S_n they form a subfield of $F(x_1, \ldots, x_n)$, called the field of symmetric rational functions which we shall denote by S. We shall be concerned with three questions:

1. What is $[F(x_1, \ldots, x_n) : S]$?
2. What is $G(F(x_1, \ldots, x_n), S)$?
3. Can we describe S in terms of some particularly easy extension of F?

We shall answer these three questions simultaneously.

We can explicitly produce in S some particularly simple functions constructed from $x_1, \ldots, x_n$ known as the *elementary symmetric functions* in $x_1, \ldots, x_n$. These are defined as follows:

$$a_1 = x_1 + x_2 + \cdots + x_n = \sum_{i=1}^{n} x_i$$

$$a_2 = \sum_{i<j} x_i x_j$$

$$a_3 = \sum_{i<j<k} x_i x_j x_k$$

$$\vdots$$

$$a_n = x_1 x_2 \cdots x_n.$$

That these are symmetric functions is left as an exercise. For $n = 2$, 3 and 4 we write them out explicitly below.

$n = 2$

$$a_1 = x_1 + x_2.$$

$$a_2 = x_1 x_2.$$

$n = 3$

$$a_1 = x_1 + x_2 + x_3.$$

$$a_2 = x_1 x_2 + x_1 x_3 + x_2 x_3.$$

$$a_3 = x_1 x_2 x_3.$$

$n = 4$

$$a_1 = x_1 + x_2 + x_3 + x_4.$$

$$a_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4.$$

$$a_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4.$$

$$a_4 = x_1 x_2 x_3 x_4.$$

Note that when $n = 2$, x_1 and x_2 are the roots of the polynomial $t^2 - a_1 t + a_2$, that when $n = 3$, x_1, x_2, and x_3 are roots of $t^3 - a_1 t^2 + a_2 t - a_3$ and that when $n = 4$, x_1, x_2, x_3, and x_4 are all roots of $t^4 - a_1 t^3 + a_2 t^2 - a_3 t + a_4$.

Since $a_1, \ldots, a_n$ are all in S, the field $F(a_1, \ldots, a_n)$ obtained by adjoining $a_1, \ldots, a_n$ to F must lie in S. Our objective is now twofold, namely, to prove

1. $[F(x_1, \ldots, x_n) : S] = n!$.
2. $S = F(a_1, \ldots, a_n)$.

Since the group S_n is a group of automorphisms of $F(x_1, \ldots, x_n)$ leaving S fixed, $S_n \subset G(F(x_1, \ldots, x_n), S)$. Thus, by Theorem 5.6.2,

$[F(x_1, \ldots, x_n):S] \geq o(G(F(x_n, \ldots, x_n), S)) \geq o(S_n) = n!$. If we could show that $[F(x_1, \ldots, x_n):F(a_1, \ldots, a_n)] \leq n!$, well then, since $F(a_1, \ldots, a_n)$ is a subfield of S, we would have $n! \geq [F(x_1, \ldots, x_n):F(a_1, \ldots, a_n)] = [F(x_1, \ldots, x_n):S][S:F(a_1, \ldots, a_n)] \geq n!$. But then we would get that $[F(x_1, \ldots, x_n):S] = n!$, $[S:F(a_1, \ldots, a_n)] = 1$ and so $S = F(a_1, \ldots, a_n)$, and, finally, $S_n = G(F(x_1, \ldots, x_n), S)$ (this latter from the second sentence of this paragraph). These are precisely the conclusions we seek.

Thus we merely must prove that $[F(x_1, \ldots, x_n):F(a_1, \ldots, a_n)] \leq n!$. To see how this settles the whole affair, note that the polynomial $p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} \cdots + (-1)^n a_n$, which has coefficients in $F(a_1, \ldots, a_n)$, factors over $F(x_1, \ldots, x_n)$ as $p(t) = (t - x_1)(t - x_2) \cdots (t - x_n)$. (This is in fact the origin of the elementary symmetric functions.) Thus $p(t)$, of degree n over $F(a_1, \ldots, a_n)$, splits as a product of linear factors over $F(x_1, \ldots, x_n)$. It cannot split over a proper subfield of $F(x_1, \ldots, x_n)$ which contains $F(a_1, \ldots, a_n)$ for this subfield would then have to contain both F and each of the roots of $p(t)$, namely, $x_1, x_2, \ldots, x_n$; but then this subfield would be all of $F(x_1, \ldots, x_n)$. *Thus we see that $F(x_1, \ldots, x_n)$ is the splitting field of the polynomial $p(t) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n$ over $F(a_1, \ldots, a_n)$.* Since $p(t)$ is of degree n, by Theorem 5.3.2 we get $[F(x_1, \ldots, x_n):F(a_1, \ldots, a_n)] \leq n!$. Thus all our claims are established. We summarize the whole discussion in the basic and important result

THEOREM 5.6.3 *Let F be a field and let $F(x_1, \ldots, x_n)$ be the field of rational functions in $x_1, \ldots, x_n$ over F. Suppose that S is the field of symmetric rational functions; then*

1. $[F(x_1, \ldots, x_n):S] = n!$.
2. $G(F(x_1, \ldots, x_n), S) = S_n$, *the symmetric group of degree n.*
3. *If $a_1, \ldots, a_n$ are the elementary symmetric functions in $x_1, \ldots, x_n$, then $S = F(a_1, a_2, \ldots, a_n)$.*
4. *$F(x_1, \ldots, x_n)$ is the splitting field over $F(a_1, \ldots, a_n) = S$ of the polynomial $t^n - a_1 t^{n-1} + a_2 t^{n-2} \cdots + (-1)^n a_n$.*

We mentioned earlier that given any integer n it is possible to construct a field and a polynomial of degree n over this field whose splitting field is of maximal possible degree, $n!$, over this field. Theorem 5.6.3 explicitly provides us with such an example for if we put $S = F(a_1, \ldots, a_n)$, the rational function field in n variables $a_1, \ldots, a_n$ and consider the splitting field of the polynomial $t^n - a_1 t^{n-1} + a_2 t^{n-2} \cdots + (-1)^n a_n$ over S then it is of degree $n!$ over S.

Part 3 of Theorem 5.6.3 is a very classical theorem. *It asserts that a symmetric rational function in n variables is a rational function in the elementary symmetric functions of these variables.* This result can even be sharpened to: A symmetric polynomial in n variables is a *polynomial* in their elementary symmetric

functions (see Problem 7). This result is known as the *theorem on symmetric polynomials.*

In the examples we discussed of groups of automorphisms of fields and of fixed fields under such groups, we saw that it might very well happen that F is actually smaller than the whole fixed field of $G(K, F)$. Certainly F is always contained in this field but need not fill it out. Thus to impose the condition on an extension K of F that F be precisely the fixed field of $G(K, F)$ is a genuine limitation on the type of extension of F that we are considering. It is in this kind of extension that we shall be most interested.

DEFINITION K is a *normal extension* of F if K is a finite extension of F such that F is the fixed field of $G(K, F)$.

Another way of saying the same thing: If K is a normal extension of F, then every element in K which is outside F is moved by some element in $G(K, F)$. In the examples discussed, Examples 5.6.1 and 5.6.3 were normal extensions whereas Example 5.6.2 was not.

An immediate consequence of the assumption of normality is that it allows us to calculate with great accuracy the size of the fixed field of any subgroup of $G(K, F)$ and, in particular, to sharpen Theorem 5.6.2 from an inequality to an equality.

THEOREM 5.6.4 *Let K be a normal extension of F and let H be a subgroup of $G(K, F)$; let $K_H = \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ be the fixed field of H. Then*

1. $[K:K_H] = o(H)$.
2. $H = G(K, K_H)$.

(In particular, when $H = G(K, F)$, $[K:F] = o(G(K, F))$.)

Proof. Since very element in H leaves K_H elementwise fixed, certainly $H \subset G(K, K_H)$. By Theorem 5.6.2 we know that $[K:K_H) \geq o(G(K, K_H))$; and since $o(G(K, K_H)) \geq o(H)$ we have the inequalities $[K:K_H] \geq o(G(K, K_H)) \geq o(H)$. If we could show that $[K:K_H] = o(H)$, it would immediately follow that $o(H) = o(G(K, K_H))$ and as a subgroup of $G(K, K_H)$ having order that of $G(K, K_H)$, we would obtain that $H = G(K, K_H)$. So we must merely show that $[K:K_H] = o(H)$ to prove everything.

By Theorem 5.5.1 there exists an $a \in K$ such that $K = K_H(a)$; this a must therefore satisfy an irreducible polynomial over K_H of degree $m = [K:K_H]$ and no nontrivial polynomial of lower degree (Theorem 5.1.3). Let the elements of H be $\sigma_1, \sigma_2, \ldots, \sigma_h$, where σ_1 is the identity of $G(K, F)$

and where $h = o(H)$. Consider the elementary symmetric functions of $a = \sigma_1(a), \sigma_2(a), \ldots, \sigma_h(a)$, namely,

$$\alpha_1 = \sigma_1(a) + \sigma_2(a) + \cdots + \sigma_h(a) = \sum_{i=1}^{h} \sigma_i(a)$$

$$\alpha_2 = \sum_{i<j} \sigma_i(a)\sigma_j(a)$$

$$\vdots$$

$$\alpha_h = \sigma_1(a)\sigma_2(a)\cdots\sigma_h(a).$$

Each α_i is invariant under every $\sigma \in H$. (Prove!) Thus, by the definition of K_H, $\alpha_1, \alpha_2, \ldots, \alpha_h$ are all elements of K_H. However, a (as well as $\sigma_2(a), \ldots, \sigma_h(a)$) is a root of the polynomial $p(x) = (x - \sigma_1(a))(x - \sigma_2(a))\cdots(x - \sigma_h(a)) = x^h - \alpha_1 x^{h-1} + \alpha_2 x^{h-2} + \cdots + (-1)^h\alpha_h$ having coefficients in K_H. By the nature of a, this forces $h \geq m = [K:K_H]$, whence $o(H) \geq [K:K_H]$. Since we already know that $o(H) \leq [K:K_H]$ we obtain $o(H) = [K:K_H]$, the desired conclusion.

When $H = G(K, F)$, *by the normality of* K *over* F, $K_H = F$; consequently for this particular case we read off the result $[K:F] = o(G(K, F))$.

We are rapidly nearing the central theorem of the Galois theory. What we still lack is the relationship between splitting fields and normal extensions. This gap is filled by

THEOREM 5.6.5 *K is a normal extension of F if and only if K is the splitting field of some polynomial over F.*

Proof. In one direction the proof will be highly reminiscent of that of Theorem 5.6.4.

Suppose that K is a normal extension of F; by Theorem 5.5.1, $K = F(a)$. Consider the polynomial $p(x) = (x - \sigma_1(a))(x - \sigma_2(a))\cdots(x - \sigma_n(a))$ over K, where $\sigma_1, \sigma_2, \ldots, \sigma_n$ are all the elements of $G(K, F)$. Expanding $p(x)$ we see that $p(x) = x^n - \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + (-1)^n\alpha_n$ where $\alpha_1, \ldots, \alpha_n$ are the elementary symmetric functions in $a = \sigma_1(a), \sigma_2(a), \ldots, \sigma_n(a)$. But then $\alpha_1, \ldots, \alpha_n$ are each invariant with respect to every $\sigma \in G(K, F)$, whence by the normality of K over F, must all be in F. Therefore, K splits the polynomial $p(x) \in F[x]$ into a product of linear factors. Since a is a root of $p(x)$ and since a generates K over F, a can be in no proper subfield of K which contains F. Thus K is the splitting field of $p(x)$ over F.

Now for the other direction; it is a little more complicated. We separate off one piece of its proof in

LEMMA 5.6.3 *Let K be the splitting field of $f(x)$ in $F[x]$ and let $p(x)$ be an*

irreducible factor of $f(x)$ in $F[x]$. If the roots of $p(x)$ are $\alpha_1, \ldots, \alpha_r$, then for each i there exists an automorphism σ_i in $G(K, F)$ such that $\sigma_i(\alpha_1) = \alpha_i$.

Proof. Since every root of $p(x)$ is a root of $f(x)$, it must lie in K. Let α_1, α_i be any two roots of $p(x)$. By Theorem 5.3.3, there is an isomorphism τ of $F_1 = F(\alpha_1)$ onto $F_1' = F(\alpha_i)$ taking α_1 onto α_i and leaving every element of F fixed. Now K is the splitting field of $f(x)$ considered as a polynomial over F_1; likewise, K is the splitting field of $f(x)$ considered as a polynomial over F_1'. By Theorem 5.3.4 there is an isomorphism σ_i of K onto K (thus an automorphism of K) coinciding with τ on F_1. But then $\sigma_i(\alpha_1) = \tau(\alpha_1) = \alpha_i$ and σ_i leaves every element of F fixed. This is, of course, exactly what Lemma 5.6.3 claims.

We return to the completion of the proof of Theorem 5.6.5. Assume that K is the splitting field of the polynomial $f(x)$ in $F[x]$. We want to show that K is normal over F. We proceed by induction on $[K:F]$, assuming that for any pair of fields K_1, F_1 of degree less than $[K:F]$ that whenever K_1 is the splitting field over F_1 of a polynomial in $F_1[x]$, then K_1 is normal over F_1.

If $f(x) \in F[x]$ splits into linear factors over F, then $K = F$, which is certainly a normal extension of F. So, assume that $f(x)$ has an irreducible factor $p(x) \in F[x]$ of degree $r > 1$. The r *distinct* roots $\alpha_1, \alpha_2, \ldots, \alpha_r$ of $p(x)$ all lie in K and K is the splitting field of $f(x)$ considered as a polynomial over $F(\alpha_1)$. Since

$$[K:F(\alpha_1)] = \frac{[K:F]}{[F(\alpha_1):F]} = \frac{n}{r} < n,$$

by our induction hypothesis K is a normal extension of $F(\alpha_1)$.

Let $\theta \in K$ be left fixed by every automorphism $\sigma \in G(K, F)$; we would like to show that θ is in F. Now, any automorphism in $G(K, F(\alpha_1))$ certainly leaves F fixed, hence leaves θ fixed; by the normality of K over $F(\alpha_1)$, this implies that θ is in $F(\alpha_1)$. Thus

$$\theta = \lambda_0 + \lambda_1\alpha_1 + \lambda_2{\alpha_1}^2 + \cdots + \lambda_{r-1}{\alpha_1}^{r-1} \quad \text{where } \lambda_0, \ldots, \lambda_{r-1} \in F. \tag{1}$$

By Lemma 5.6.3 there is an automorphism σ_i of K, $\sigma_i \in G(K, F)$, such that $\sigma_i(\alpha_1) = \alpha_i$; since this σ_i leaves θ and each λ_j fixed, applying it to (1) we obtain

$$\theta = \lambda_0 + \lambda_1\alpha_i + \lambda_2{\alpha_i}^2 + \cdots + \lambda_{r-1}{\alpha_i}^{r-1} \quad \text{for } i = 1, 2, \ldots, r. \tag{2}$$

Thus the polynomial

$$q(x) = \lambda_{r-1}x^{r-1} + \lambda_{r-2}x^{r-2} + \cdots + \lambda_1 x + (\lambda_0 - \theta)$$

in $K[x]$, of degree at most $r - 1$, has the r distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_r$.

This can only happen if all its coefficients are 0; in particular, $\lambda_0 - \theta = 0$ whence $\theta = \lambda_0$ so is in F. This completes the induction and proves that K is a normal extension of F. Theorem 5.6.5 is now completely proved.

DEFINITION Let $f(x)$ be a polynomial in $F[x]$ and let K be its splitting field over F. The *Galois group* of $f(x)$ is the group $G(K, F)$ of all the automorphisms of K, leaving every element of F fixed.

Note that the Galois group of $f(x)$ can be considered as a group of permutations of its roots, for if α is a root of $f(x)$ and if $\sigma \in G(K, F)$, then $\sigma(\alpha)$ is also a root of $f(x)$.

We now come to the result known as the *fundamental theorem of Galois theory*. It sets up a one-to-one correspondence between the subfields of the splitting field of $f(x)$ and the subgroups of its Galois group. Moreover, it gives a criterion that a subfield of a normal extension itself be a normal extension of F. This fundamental theorem will be used in the next section to derive conditions for the solvability by radicals of the roots of a polynomial.

THEOREM 5.6.6 *Let $f(x)$ be a polynomial in $F[x]$, K its splitting field over F, and $G(K, F)$ its Galois group. For any subfield T of K which contains F let $G(K, T) = \{\sigma \in G(K, F) \mid \sigma(t) = t \text{ for every } t \in T\}$ and for any subgroup H of $G(K, F)$ let $K_H = \{x \in K \mid \sigma(x) = x \text{ for every } \sigma \subset H\}$. Then the association of T with $G(K, T)$ sets up a one-to-one correspondence of the set of subfields of K which contain F onto the set of subgroups of $G(K, F)$ such that*

1. $T = K_{G(K,T)}$.
2. $H = G(K, K_H)$.
3. $[K:T] = o(G(K, T))$, $[T:F] =$ *index of* $G(K, T)$ *in* $G(K, F)$.
4. *T is a normal extension of F if and only if $G(K, T)$ is a normal subgroup of $G(K, F)$.*
5. *When T is a normal extension of F, then $G(T, F)$ is isomorphic to $G(K, F)/G(K, T)$.*

Proof. Since K is the splitting field of $f(x)$ over F it is also the splitting field of $f(x)$ over any subfield T which contains F, therefore, by Theorem 5.6.5, K is a normal extension of T. Thus, by the definition of normality, T is the fixed field of $G(K, T)$, that is, $T = K_{G(K,T)}$, proving part 1.

Since K is a normal extension of F, by Theorem 5.6.4, given a subgroup H of $G(K, F)$, then $H = G(K, K_H)$, which is the assertion of part 2. Moreover, this shows that any subgroup of $G(K, F)$ arises in the form $G(K, T)$, whence the association of T with $G(K, T)$ maps the set of all subfields of K containing F *onto* the set of all subgroups of $G(K, F)$. That it is one-to-one

is clear, for, if $G(K, T_1) = G(K, T_2)$ then, by part 1, $T_1 = K_{G(K,T_1)} = K_{G(K,T_2)} = T_2$.

Since K is normal over T, again using Theorem 5.6.4, $[K:T] = o(G(K, T))$; but then we have $o(G(K, F)) = [K:F] = [K:T][T:F] = o(G(K, T))[T:F]$, whence

$$[T:F] = \frac{o(G(K, F))}{o(G(K, T))} = \text{index of } G(K, T)$$

in $G(K, F)$. This is part 3.

The only parts which remain to be proved are those which pertain to normality. We first make the following observation. T is a normal extension of F if and only if for every $\sigma \in G(K, F)$, $\sigma(T) \subset T$. Why? We know by Theorem 5.5.1 that $T = F(a)$; thus if $\sigma(T) \subset T$, then $\sigma(a) \in T$ for all $\sigma \in G(K, F)$. But, as we saw in the proof of Theorem 5.6.5, this implies that T is the splitting field of

$$p(x) = \prod_{\sigma \in G(K,F)} (x - \sigma(a))$$

which has coefficients in F. As a splitting field, T, by Theorem 5.6.5, is a normal extension of F. Conversely, if T is a normal extension of F, then $T = F(a)$, where the minimal polynomial of a, $p(x)$, over F has all its roots in T (Theorem 5.6.5). However, for any $\sigma \in G(K, F)$, $\sigma(a)$ is also a root of $p(x)$, whence $\sigma(a)$ must be in T. Since T is generated by a over F, we get that $\sigma(T) \subset T$ for every $\sigma \in G(K, F)$.

Thus T is a normal extension of F if and only if for any $\sigma \in G(K, F)$, $\tau \in G(K, T)$ and $t \in T$, $\sigma(t) \in T$ and so $\tau(\sigma(t)) = \sigma(t)$; that is, if and only if $\sigma^{-1}\tau\sigma(t) = t$. But this says that T is normal over F if and only if $\sigma^{-1}G(K, T)\sigma \subset G(K, T)$ for every $\sigma \in G(K, F)$. This last condition being precisely that which defines $G(K, T)$ as a normal subgroup of $G(K, F)$, we see that part 4 is proved.

Finally, if T is normal over F, given $\sigma \in G(K, F)$, since $\sigma(T) \subset T$, σ induces an automorphism σ_* of T defined by $\sigma_*(t) = \sigma(t)$ for every $t \in T$. Because σ_* leaves every element of F fixed, σ_* must be in $G(T, F)$. Also, as is evident, for any $\sigma, \psi \in G(K, F)$, $(\sigma\psi)_* = \sigma_*\psi_*$ whence the mapping of $G(K, F)$ into $G(T, F)$ defined by $\sigma \to \sigma_*$ is a homomorphism of $G(K, F)$ into $G(T, F)$. What is the kernel of this homomorphism? It consists of all elements σ in $G(K, F)$ such that σ_* is the identity map on T. That is, the kernel is the set of all $\sigma \in G(K, F)$ such that $t = \sigma_*(t) = \sigma(t)$; by the very definition, we get that the kernel is exactly $G(K, T)$. The image of $G(K, F)$ in $G(T, F)$, by Theorem 2.7.1 is isomorphic to $G(K, F)/G(K, T)$, whose order is $o(G(K, F))/o(G(K, T)) = [T:F]$ (by part 3) $= o(G(T, F))$ (by Theorem 5.6.4). Thus the image of $G(K, F)$ in $G(T, F)$ is all of $G(T, F)$ and so we have $G(T, F)$ isomorphic to

$G(K, F)/G(K, T)$. This finishes the proof of part 5 and thereby completes the proof of Theorem 5.6.6.

Problems

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.
2. Prove Lemma 5.6.2.
3. Using the Eisenstein criterion, prove that $x^4 + x^3 + x^2 + x + 1$ is irreducible over the field of rational numbers.
4. In Example 5.6.3, prove that each mapping σ_i defined is an automorphism of $F_0(\omega)$.
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.
6. Prove directly that any automorphism of K must leave every rational number fixed.

*7. Prove that a symmetric polynomial in $x_1, \ldots, x_n$ is a polynomial in the elementary symmetric functions in $x_1, \ldots, x_n$.

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) $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$.
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) $\alpha_1^3, \alpha_2^3, \alpha_3^3$.

*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.
11. Prove that the elementary symmetric functions in $x_1, \ldots, x_n$ are indeed symmetric functions in $x_1, \ldots, x_n$.
12. If $p(x) = x^n - 1$ prove that the Galois group of $p(x)$ over the field of rational numbers is abelian.

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 $\phi(n)$ primitive nth roots of unity, prove that any automorphism of $F_0(\omega_1)$ takes ω_1 into some ω_i.
    (d) Prove that $[F_0(\omega_1):F_0] \leq \phi(n)$.

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.)

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.

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.

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.

5.7 Solvability by Radicals

Given the specific polynomial $x^2 + 3x + 4$ over the field of rational numbers F_0, from the quadratic formula for its roots we know that its roots are $(-3 \pm \sqrt{-7})/2$; thus the field $F_0(\sqrt{7}\,i)$ is the splitting field of $x^2 + 3x + 4$ over F_0. Consequently there is an element $\gamma = -7$ in F_0 such that the extension field $F_0(\omega)$ where $\omega^2 = \gamma$ is such that it contains all the roots of $x^2 + 3x + 4$.

From a slightly different point of view, given the *general* quadratic polynomial $p(x) = x^2 + a_1x + a_2$ over F, we can consider it as a *particular* polynomial over the field $F(a_1, a_2)$ of rational functions in the two variables a_1 and a_2 over F; in the extension obtained by adjoining ω to $F(a_1, a_2)$ where $\omega^2 = {a_1}^2 - 4a_2 \in F(a_1, a_2)$, we find all the roots of $p(x)$. There is

a formula which expresses the roots of $p(x)$ in terms of a_1, a_2 and square roots of rational functions of these.

For a cubic equation the situation is very similar; given the general cubic equation $p(x) = x^3 + a_1x^2 + a_2x + a_3$ an explicit formula can be given, involving combinations of square roots and cube roots of rational functions in a_1, a_2, a_3. While somewhat messy, they are explicitly given by *Cardan's formulas:* Let $p = a_2 - ({a_1}^2/3)$ and

$$q = \frac{2{a_1}^3}{27} - \frac{a_1a_2}{3} + a_3$$

and let

$$P = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

and

$$Q = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

(with cube roots chosen properly); then the roots are $P + Q - (a_1/3)$, $\omega P + \omega^2 Q - (a_1/3)$, and $\omega^2 P + \omega Q - (a_1/3)$, where $\omega \neq 1$ is a cube root of 1. The above formulas only serve to illustrate for us that by adjoining a certain square root and then a cube root to $F(a_1, a_2, a_3)$ we reach a field in which $p(x)$ has its roots.

For fourth-degree polynomials, which we shall not give explicitly, by using rational operations and square roots, we can reduce the problem to that of solving a certain cubic, so here too a formula can be given expressing the roots in terms of combinations of radicals (surds) of rational functions of the coefficients.

For polynomials of degree five and higher, no such universal radical formula can be given, for we shall prove that it is impossible to express their roots, in general, in this way.

Given a field F and a polynomial $p(x) \in F[x]$, we say that $p(x)$ *is solvable by radicals over* F if we can find a finite sentence of fields $F_1 = F(\omega_1)$, $F_2 = F_1(\omega_2), \ldots, F_k = F_{k-1}(\omega_k)$ such that ${\omega_1}^{r_1} \in F$, ${\omega_2}^{r_2} \in F_1, \ldots,$ ${\omega_k}^{r_k} \in F_{k-1}$ such that the roots of $p(x)$ all lie in F_k.

If K is the splitting field of $p(x)$ over F, then $p(x)$ is solvable by radicals over F if we can find a sequence of fields as above such that $K \subset F_k$. An important remark, and one we shall use later, in the proof of Theorem 5.7.2, is that if such an F_k can be found, we can, without loss of generality, assume it to be a *normal* extension of F; we leave its proof as a problem (Problem 1).

By the *general polynomial of degree n over* F, $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$, we mean the following: Let $F(a_1, \ldots, a_n)$ be the field of rational functions,

in the n variables $a_1, \ldots, a_n$ over F, and consider the particular polynomial $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$ over the field $F(a_1, \ldots, a_n)$. We say that it is solvable by radicals if it is solvable by radicals over $F(a_1, \ldots, a_n)$. This really expresses the intuitive idea of "finding a formula" for the roots of $p(x)$ involving combinations of mth roots, for various m's, of rational functions in $a_1, a_2, \ldots, a_n$. For $n = 2$, 3, and 4, we pointed out that this can always be done. For $n \geq 5$, Abel proved that this cannot be done. However, this does not exclude the possibility that a given polynomial over F may be solvable by radicals. In fact, we shall give a criterion for this in terms of the Galois group of the polynomial. But first we must develop a few purely group-theoretical results. Some of these occurred as problems at the end of Chapter 2, but we nevertheless do them now officially.

DEFINITION A group G is said to be *solvable* if we can find a finite chain of subgroups $G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k = (e)$, where each N_i is a normal subgroup of N_{i-1} and such that every factor group N_{i-1}/N_i is abelian.

Every abelian group is solvable, for merely take $N_0 = G$ and $N_1 = (e)$ to satisfy the above definition. The symmetric group of degree 3, S_3, is solvable for take $N_1 = \{e, (1, 2, 3), (1, 3, 2)\}$; N_1 is a normal subgroup of S_3 and S_3/N_1 and $N_1/(e)$ are both abelian being of orders 2 and 3, respectively. It can be shown that S_4 is solvable (Problem 3). For $n \geq 5$ we show in Theorem 5.7.1 below that S_n is *not* solvable.

We seek an alternative description for solvability. Given the group G and elements a, b in G, then the *commutator* of a and b is the element $a^{-1}b^{-1}ab$. The *commutator subgroup*, G', of G is the subgroup of G generated by all the commutators in G. (It is *not* necessarily true that the set of commutators itself forms a subgroup of G.) It was an exercise before that G' is a normal subgroup of G. Moreover, the group G/G' is abelian, for, given any two elements in it, aG', bG', with $a, b \in G$, then

$$\begin{aligned}(aG')(bG') &= abG' = ba(a^{-1}b^{-1}ab)G' \\ &= (\text{since } a^{-1}b^{-1}ab \in G')\ baG' = (bG')(aG').\end{aligned}$$

On the other hand, if M is a normal subgroup of G such that G/M is abelian, then $M \supset G'$, for, given $a, b \in G$, then $(aM)(bM) = (bM)(aM)$, from which we deduce $abM = baM$ whence $a^{-1}b^{-1}abM = M$ and so $a^{-1}b^{-1}ab \in M$. Since M contains all commutators, it contains the group these generate, namely G'.

G' is a group in its own right, so we can speak of its commutator subgroup $G^{(2)} = (G')'$. This is the subgroup of G generated by all elements $(a')^{-1}(b')^{-1}a'b'$ where $a', b' \in G'$. It is easy to prove that not only is $G^{(2)}$ a normal subgroup of G' but it is also a normal subgroup of G (Problem 4).

We continue this way and define the higher commutator subgroups $G^{(m)}$ by $G^{(m)} = (G^{(m-1)})'$. Each $G^{(m)}$ is a normal subgroup of G (Problem 4) and $G^{(m-1)}/G^{(m)}$ is an abelian group.

In terms of these higher commutator subgroups of G, we have a very succinct criterion for solvability, namely,

LEMMA 5.7.1 *G is solvable if and only if $G^{(k)} = (e)$ for some integer k.*

Proof. If $G^{(k)} = (e)$ let $N_0 = G$, $N_1 = G'$, $N_2 = G^{(2)}, \ldots, N_k = G^{(k)} = (e)$. We have

$$G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k = (e);$$

each N_i being normal in G is certainly normal in N_{i-1}. Finally,

$$\frac{N_{i-1}}{N_i} = \frac{G^{(i-1)}}{G^{(i)}} = \frac{G^{(i-1)}}{(G^{(i-1)})'}$$

hence is abelian. Thus by the definition of solvability G is a solvable group.

Conversely, if G is a solvable group, there is a chain $G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k = (e)$ where each N_i is normal in N_{i-1} and where N_{i-1}/N_i is abelian. But then the commutator subgroup N'_{i-1} of N_{i-1} must be contained in N_i. Thus $N_1 \supset N'_0 = G'$, $N_2 \supset N'_1 \supset (G')' = G^{(2)}$, $N_3 \supset N'_2 \supset (G^{(2)})' = G^{(3)}, \ldots, N_i \supset G^{(i)}$, $(e) = N_k \supset G^{(k)}$. We therefore obtain that $G^{(k)} = (e)$.

COROLLARY *If G is a solvable group and if $\bar{G}$ is a homomorphic image of G, then $\bar{G}$ is solvable.*

Proof. Since $\bar{G}$ is a homomorphic image of G it is immediate that $(\bar{G})^{(k)}$ is the image of $G^{(k)}$. Since $G^{(k)} = (e)$ for some k, $(\bar{G})^{(k)} = (e)$ for the same k, whence by the lemma $\bar{G}$ is solvable.

The next lemma is the key step in proving that the infinite family of groups S_n, with $n \geq 5$, is not solvable; here S_n is the symmetric group of degree n.

LEMMA 5.7.2 *Let $G = S_n$, where $n \geq 5$; then $G^{(k)}$ for $k = 1, 2, \ldots,$ contains every 3-cycle of S_n.*

Proof. We first remark that for an arbitrary group G, if N is a normal subgroup of G, then N' must also be a normal subgroup of G (Problem 5).

We claim that if N is a normal subgroup of $G = S_n$, where $n \geq 5$, which contains every 3-cycle in S_n, then N' must also contain every 3-cycle. For suppose $a = (1, 2, 3)$, $b = (1, 4, 5)$ are in N (we are using here that $n \geq 5$); then $a^{-1}b^{-1}ab = (3, 2, 1)(5, 4, 1)(1, 2, 3)(1, 4, 5) = (1, 4, 2)$, as a commutator of elements of N must be in N'. Since N' is a normal

subgroup of G, for any $\pi \in S_n$, $\pi^{-1}(1, 4, 2)\pi$ must also be in N'. Choose a π in S_n such that $\pi(1) = i_1$, $\pi(4) = i_2$, and $\pi(2) = i_3$, where i_1, i_2, i_3 are any three distinct integers in the range from 1 to n; then $\pi^{-1}(1, 4, 2)\pi = (i_1, i_2, i_3)$ is in N'. Thus N' contains all 3-cycles.

Letting $N = G$, which is certainly normal in G and contains all 3-cycles, we get that G' contains all 3-cycles; since G' is normal in G, $G^{(2)}$ contains all 3-cycles; since $G^{(2)}$ is normal in G, $G^{(3)}$ contains all 3-cycles. Continuing this way we obtain that $G^{(k)}$ contains all 3-cycles for arbitrary k.

A direct consequence of this lemma is the interesting group-theoretic result.

THEOREM 5.7.1 *S_n is not solvable for $n \geq 5$.*

Proof. If $G = S_n$, by Lemma 5.7.2, $G^{(k)}$ contains all 3-cycles in S_n for every k. Therefore, $G^{(k)} \neq (e)$ for any k, whence by Lemma 5.7.1, G cannot be solvable.

We now interrelate the solvability by radicals of $p(x)$ with the solvability, as a group, of the Galois group of $p(x)$. The very terminology is highly suggestive that such a relation exists. But first we need a result about the Galois group of a certain type of polynomial.

LEMMA 5.7.3 *Suppose that the field F has all nth roots of unity (for some particular n) and suppose that $a \neq 0$ is in F. Let $x^n - a \in F[x]$ and let K be its splitting field over F. Then*

1. *$K = F(u)$ where u is any root of $x^n - a$.*
2. *The Galois group of $x^n - a$ over F is abelian.*

Proof. Since F contains all nth roots of unity, it contains $\xi = e^{2\pi i/n}$; 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 $u, \xi u, \xi^2 u, \ldots, \xi^{n-1}u$ are all the roots of $x^n - a$. That they are roots is clear; that they are distinct follows from: $\xi^i u = \xi^j u$ with $0 \leq i < j < n$, then since $u \neq 0$, and $(\xi^i - \xi^j)u = 0$, we must have $\xi^i = \xi^j$, which is impossible since $\xi^{j-i} = 1$, with $0 < j - i < n$. Since $\xi \in F$, all of $u, \xi u, \ldots, \xi^{n-1}u$ are in $F(u)$, thus $F(u)$ splits $x^n - a$; since no proper subfield of $F(u)$ which contains F also contains u, no proper subfield of $F(u)$ can split $x^n - a$. Thus $F(u)$ is the splitting field of $x^n - a$, and we have proved that $K = F(u)$.

If σ, τ are any two elements in the Galois group of $x^n - a$, that is, if σ, τ are automorphisms of $K = F(u)$ 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 $\sigma\tau(u) = \sigma(\xi^j u) = \xi^j \sigma(u)$ (since $\xi^j \in F$) $= \xi^i \xi^j u = \xi^{i+j}u$; similarly, $\tau\sigma(u) = \xi^{i+j}u$. Therefore, $\sigma\tau$ and $\tau\sigma$ agree on u and on

F hence on all of $K = F(u)$. But then $\sigma\tau = \tau\sigma$, whence the Galois group is abelian.

Note that the lemma says that when F has all nth roots of unity, then adjoining one root of $x^n - a$ to F, where $a \in F$, gives us the whole splitting field of $x^n - a$; thus this must be a normal extension of F.

We assume for the rest of the section that F is a field which contains all nth roots of unity for every integer n. We have

THEOREM 5.7.2 *If $p(x) \in F[x]$ is solvable by radicals over F, then the Galois group over F of $p(x)$ is a solvable group.*

Proof. Let K be the splitting field of $p(x)$ over F; the Galois group of $p(x)$ over F is $G(K, F)$. Since $p(x)$ is solvable by radicals, there exists 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 $\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1, \ldots, \omega_k^{r_k} \in F_{k-1}$ and where $K \subset F_k$. As we pointed out, without loss of generality we may assume that F_k is a normal extension of F. As a normal extension of F, F_k is also a normal extension of any intermediate field, hence F_k is a normal extension of each F_i.

By Lemma 5.7.3 each F_i is a normal extension of F_{i-1} and since F_k is normal over F_{i-1}, by Theorem 5.6.6, $G(F_k, F_i)$ is a normal subgroup in $G(F_k, F_{i-1})$. Consider the chain

$$G(F_k, F) \supset G(F_k, F_1) \supset G(F_k, F_2) \supset \cdots \supset G(F_k, F_{k-1}) \supset (e). \quad (1)$$

As we just remarked, each subgroup in this chain is a normal subgroup in the one preceding it. Since F_i is a normal extension of F_{i-1}, by the fundamental theorem of Galois theory (Theorem 5.6.6) the group of F_i over F_{i-1}, $G(F_i, F_{i-1})$ is isomorphic to $G(F_k, F_{i-1})/G(F_k, F_i)$. However, by Lemma 5.7.3, $G(F_i, F_{i-1})$ is an abelian group. Thus each quotient group $G(F_k, F_{i-1})/G(F_k, F_i)$ of the chain (1) is abelian.

Thus the group $G(F_k, F)$ is solvable! Since $K \subset F_k$ and is a normal extension of F (being a splitting field), by Theorem 5.6.6, $G(F_k, K)$ is a normal subgroup of $G(F_k, F)$ and $G(K, F)$ is isomorphic to $G(F_k, F)/G(F_k, K)$. Thus $G(K, F)$ is a homomorphic image of $G(F_k, F)$, a solvable group; by the corollary to Lemma 5.7.1, $G(K, F)$ itself must then be a solvable group. Since $G(K, F)$ is the Galois group of $p(x)$ over F the theorem has been proved.

We make two remarks without proof.

1. The converse of Theorem 5.7.2 is also true; that is, if the Galois group of $p(x)$ over F is solvable then $p(x)$ is solvable by radicals over F.

2. Theorem 5.7.2 and its converse are true even if F does not contain roots of unity.

Recalling what is meant by the general polynomial of degree n over F, $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$, and what is meant by solvable by radicals, we close with the great, classic theorem of Abel:

THEOREM 5.7.3 *The general polynomial of degree $n \geq 5$ is not solvable by radicals.*

Proof. In Theorem 5.6.3 we saw that if $F(a_1, \ldots, a_n)$ is the field of rational functions in the n variables $a_1, \ldots, a_n$, then the Galois group of the polynomial $p(t) = t^n + a_1t^{n-1} + \cdots + a_n$ over $F(a_1, \ldots, a_n)$ was S_n, the symmetric group of degree n. By Theorem 5.7.1, S_n is not a solvable group when $n \geq 5$, thus by Theorem 5.7.2, $p(t)$ is not solvable by radicals over $F(a_1, \ldots, a_n)$ when $n \geq 5$.

Problems

*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.

2. Prove that a subgroup of a solvable group is solvable.
3. Prove that S_4 is a solvable group.
4. If G is a group, prove that all $G^{(k)}$ are normal subgroups of G.
5. If N is a normal subgroup of G prove that N' must also be 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 $n \geq 5$.

5.8 Galois Groups over the Rationals

In Theorem 5.3.2 we saw that, given a field F and a polynomial $p(x)$, of degree n, in $F[x]$, then the splitting field of $p(x)$ over F has degree at most $n!$ over F. In the preceding section we saw that this upper limit of $n!$ is, indeed, taken on for some choice of F and some polynomial $p(x)$ of degree n over F. In fact, if F_0 is any field and if F is the field of rational functions in the variables $a_1, \ldots, a_n$ over F_0, it was shown that the splitting field, K, of the polynomial $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$ over F has degree exactly $n!$ over F. Moreover, it was shown that the Galois group of K over

F is S_n, the symmetric group of degree n. This turned out to be the basis for the fact that the general polynomial of degree n, with $n \geq 5$, is not solvable by radicals.

However, it would be nice to know that the phenomenon described above can take place with fields which are more familiar to us than the field of rational functions in n variables. What we shall do will show that for any prime number p, at least, we can find polynomials of degree p over the field of rational numbers whose splitting fields have degree $p!$ over the rationals. This way we will have polynomials with rational coefficients whose Galois group over the rationals is S_p. In light of Theorem 5.7.2, we will conclude from this that the roots of these polynomials cannot be expressed in combinations of radicals involving rational numbers. Although in proving Theorem 5.7.2 we used that roots of unity were in the field, and roots of unity do not lie in the rationals, we make use of remark 2 following the proof of Theorem 5.7.2 here, namely that Theorem 5.7.2 remains valid even in the absence of roots of unity.

We shall make use of the fact that polynomials with rational coefficients have all their roots in the complex field.

We now prove

THEOREM 5.8.1 *Let $q(x)$ be an irreducible polynomial of degree p, p a prime, over the field Q of rational numbers. Suppose that $q(x)$ has exactly two nonreal roots in the field of complex numbers. Then the Galois group of $q(x)$ over Q is S_p, the symmetric group of degree p. Thus the splitting field of $q(x)$ over Q has degree $p!$ over Q.*

Proof. Let K be the splitting field of the polynomial $q(x)$ over Q. If α is a root of $q(x)$ in K, then, since $q(x)$ is irreducible over Q, by Theorem 5.1.3, $[Q(\alpha):Q] = p$. Since $K \supset Q(\alpha) \supset Q$ and, according to Theorem 5.1.1, $[K:Q] = [K:Q(\alpha)][Q(\alpha):Q] = [K:Q(\alpha)]p$, we have that $p|[K:Q]$. If G is the Galois group of K over Q, by Theorem 5.6.4, $o(G) = [K:F]$. Thus $p \mid o(G)$. Hence, by Cauchy's theorem (Theorem 2.11.3), G has an element σ of order p.

To this point we have not used our hypothesis that $q(x)$ has exactly two nonreal roots. We use it now. If α_1, α_2 are these nonreal roots, then $\alpha_1 = \bar{\alpha}_2$, $\alpha_2 = \bar{\alpha}_1$ (see Problem 13, Section 5.3), where the bar denotes the complex conjugate. If $\alpha_3, \ldots, \alpha_p$ are the other roots, then, since they are real, $\bar{\alpha}_i = \alpha_i$ for $i \geq 3$. Thus the complex conjugate mapping takes K into itself, is an automorphism τ of K over Q, and interchanges α_1 and α_2, leaving the other roots of $q(x)$ fixed.

Now, the elements of G take roots of $q(x)$ into roots of $q(x)$, so induce permutations of $\alpha_1, \ldots, \alpha_p$. In this way we imbed G in S_p. The automorphism τ described above is the transposition $(1, 2)$ since $\tau(\alpha_1) = \alpha_2$,

$\tau(\alpha_2) = \alpha_1$, and $\tau(\alpha_i) = \alpha_i$ for $i \geq 3$. What about the element $\sigma \in G$, which we mentioned above, which has order p? As an element of S_p, σ has order p. But the only elements of order p in S_p are p-cycles. Thus σ must be a p-cycle.

Therefore G, as a subgroup of S_p, contains a transposition and a p-cycle. It is a relatively easy exercise (see Problem 4) to prove that any transposition and any p-cycle in S_p generate S_p. Thus σ and τ generate S_p. But since they are in G, the group generated by σ and τ must be in G. The net result of this is that $G = S_p$. In other words, the Galois group of $q(x)$ over Q is indeed S_p. This proves the theorem.

The theorem gives us a fairly general criterion to get S_p as a Galois group over Q. Now we must produce polynomials of degree p over the rationals which are irreducible over Q and have exactly two nonreal roots. To produce irreducible polynomials, we use the Eisenstein criterion (Theorem 3.10.2). To get all but two real roots one can play around with the coefficients, but always staying in a context where the Eisenstein criterion is in force.

We do it explicitly for $p = 5$. Let $q(x) = 2x^5 - 10x + 5$. By the Eisenstein criterion, $q(x)$ is irreducible over Q. We graph $y = q(x) = 2x^5 - 10x + 5$. By elementary calculus it has a maximum at $x = -1$ and a minimum at $x = 1$ (see Figure 5.8.1). As the graph clearly indicates,

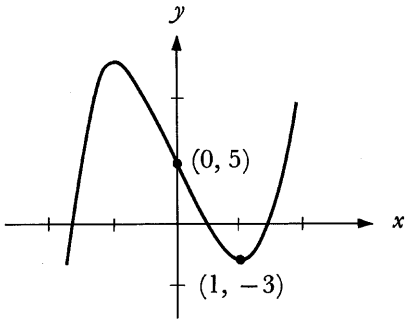


Figure 5.8.1

$y = q(x) = 2x^5 - 10x + 5$ crosses the x-axis exactly three times, so $q(x)$ has exactly three roots which are real. Hence the other two roots must be complex, nonreal numbers. Therefore $q(x)$ satisfies the hypothesis of Theorem 5.8.1, in consequence of which the Galois group of $q(x)$ over Q is S_5. Using Theorem 5.7.2, we know that it is not possible to express the roots of $q(x)$ in a combination of radicals of rational numbers.

Problems

1. In S_5 show that (1 2) and (1 2 3 4 5) generate S_5.
2. In S_5 show that (1 2) and (1 3 2 4 5) generate S_5.
3. If $p > 2$ is a prime, show that (1 2) and (1 2 $\cdots$ $p-1$ p) generate S_p.
4. Prove that any transposition and p-cycle in S_p, p a prime, generate S_p.
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) $p(x) = x^5 + 5x^4 + 10x^3 + 10x^2 - x - 2$.
6. What are the Galois groups over Q of the polynomials in Problem 5?
7. Construct a polynomial of degreee 7 with rational coefficients whose Galois group over Q is S_7.

Supplementary Reading

ARTIN, E., *Galois Theory*, 2nd ed. Notre Dame Mathematical Lectures Number 2. Notre Dame, Ind.: Notre Dame Press, 1966.

KAPLANSKY, IRVING, *Fields and Rings*, 2nd ed. Chicago: University of Chicago Press, 1972.

POLLARD, H., *Theory of Algebraic Numbers*, Carus Monograph, Number 9. New York: John Wiley & Sons, 1950.

VAN DER WAERDEN, B. L., *Modern Algebra*, Vol. 1. New York: Ungar Publishing Company, 1949.

WEISNER, L., *Theory of Equations*. New York: The Macmillan Company, 1938.

SIEGAL, C. L., *Transcendental Numbers*, Annals of Mathematics Studies Number 16. Princeton, N.J.: Princeton University Press, 1949. Milwood, N.Y.: Kraus Reprint Company, 1949.

NIVEN, I., *Irrational Numbers*, Carus Monograph Number 11. New York: John Wiley & Sons, 1956.

Topics for Class Discussion

NIVEN, I., "A simple proof of the irrationality of π," *Bulletin of the American Mathematical Society*, Vol. 53 (1947), page 509.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University Established Under Section 3 of UGC Act 1956)
Pollachi Main Road, Eachanari (Po),
Coimbatore –641 021

Subject: ALGEBRA **Subject Code: 19MMP101**
Class : I - M.Sc. Mathematics **Semester : I**

Unit V

Part A (20x1=20 Marks)
Possible Questions

Question	Opt 1	Opt 2	Opt 3	Opt 4	Answer
If G is a ---------- and if G^{-} is a homomorphic image of G then G^{-} is solvable	solvable group	field	group	simple field	solvable group
If G is a sovlable group and if G^{-} is a---------- image of G then G^{-} is solvable	isomorphism	automorphism	homomorphism	monomorphism	homomorphism
If G is a solvable group and if G^{-} is a homomorphic image of G then G^{-} is ---------	non-separable	separable	reducible	solvable	solvable
Sn is---------- for $n^{3}5$	separable	not solvable	solvable	non-separable	not solvable
Sn is not solvable for ----------	n>5	n≥5	n<5	n<4	$n^{3}5$
The fixed field of G is a -------- of K	subgroup	subfield	integral domain	ring	subfield
G(K,F) is a subgroup of the group all ------- of K	isomorphism	homomorphism	automorphisms	functions	automorphisms
O(G(K,F)) ---------- [K:F]	equal	not equal	less than or equal	greater than or equal	less than or equal
K is a finite extension of F such that F is the fixed field of G(K,F), then K is-----	normal extension	finite extension	splitting field	solvable	normal extension.
The set of all automorphisms of K, G(K,F) is the -------- group.	normal group	abelian group	Galois group	solvable group	Galois group
If p(x) = x^n-1, then the Galois group of p(x) over rational numbers	normal	symmetric	abelian	solvable group	abelian
Let G=S_n, n >= 5; contains	even permutations	3-cycle of S_n	odd permutations	2-cycles	3-cycle of S_n
K is a normal extension of F iff K is ------ of F	splitting field	integral domain	Galois group	solvable	Splitting field
The polynomial p_n(x) is called the ------- polynomial	reducible	irreducible	cyclotomic	monic	cyclotomic
The number of primitive nth roots of unity is-------	n	1	phi(n)	0	phi(n)
The number of primitive 5th roots of unity is--------	5	1	4	0	4
The general polynomial of degree n ------ 5 is not solvable by radicals	equal	>=	<=	not equal	>=
If p(x) in F[x] is solvable by radicals over F, then the Galois group F of p(x) is-------	abelian	normal	solvable	cyclic	solvable
Subgroup of a solvable is --------	solvable	abelian group	cyclic	normal	solvable
G is solvable iff G^(K) is---------	0	e	G	H	e
If G is solvable then G\N is ------	normal	not solvable	solvable	e	solvable
Any group G is solvable if O(G) =------	n	0	p^n	1	p^n
Any group G is solvable if O(G) =------	not solvable	solvable	abelian	cyclic	solvable
The collection of all automorphisms of K is denoted as----------	(K)	G(K)	Aut(K)	Hom(K)	Aut(K)

If both N and G\N are solvable then G is----	abelian	normal	solvable	cyclic	solvable
The dihedral groups are------	solvable	abelian group	normal	cyclic	solvable
The symmetric group S_5 is------	abelian	normal	not solvable	solvable	not solvable