Semester – IV

		L	T	P	C
17MMU403	**GROUP THEORY II**	**6**	**2**	**0**	**6**

Scope: On successful completion of course the learners gain about the groups,Fundamental Theorem and its properties.

Objectives: To enable the students to learn and gain knowledge about group homomorphism, isomorphism, automorphismand its related properties.

UNIT I

Group homomorphisms, properties of homomorphisms, Cayley's theorem, properties of isomorphisms, First, Second and Third isomorphism theorems.

UNIT II

Automorphism, inner automorphism, automorphism groups, automorphism groups of finite and infinite cyclic groups, applications of factor groups to automorphism groups, Characteristic subgroups, Commutator subgroup and its properties.

UNIT III

Properties of external direct products, the group of units modulo n as an external direct product, internal direct products, Fundamental Theorem of finite abelian groups.

UNIT IV

Group actions, stabilizers and kernels, permutation representation associated with a given groupaction, Applications of group actions: Generalized Cayley's theorem, Index theorem.

UNIT V

Groups acting on themselves by conjugation, class equation and consequences, conjugacy in Sn, *p*-groups, Sylow's theorems and consequences, Cauchy's theorem, Simplicity of An for $n \geq 5$, non-simplicity tests.

SUGGESTED READINGS

TEXT BOOK

1. Fraleigh.J.B., (2004). A First Course in Abstract Algebra , Seventh edition , Pearson Education Ltd, Singapore.

REFERENCES

1. David S. Dummit and Richard M. Foote,(2004).,Abstract Algebra,. ThirdEdition., John Wiley and Sons(Asia) Pvt. Ltd., Singapore.

2. Herstein.I.N.,(2010). Topics in Algebra ,Second Edition, Willey and sons Pvt Ltd, Singapore.

3. Joseph A. Gallian., (2001).Contemporary Abstract Algebra, FourthEdition.,Narosa Publishing House, New Delhi.

4. Artin.M., (2008).Algebra, Prentice-Hall of India, New Delhi.

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: Dr. K. KALIDASS
SUBJECT NAME: GROUP THEORY II SUB.CODE: 17MMU403
SEMESTER: IV CLASS: II B.SC MATHEMATICS

S. No	Lecture Duration Period	Topics to be Covered	Support Material/Page Nos
		UNIT-I	
1	1	Introduction to group homomorphism/ Tutorial – I	T1: Ch 3, 125-126
2	1	Restriction of homomorphism to a subgroups	T1: Ch 3, 126-127
3	1	Tutorial – II	
4	1	Properties of homomorphism	T1: Ch 3, 128-130
5	1	Continuation of properties of homomorphism	T1: Ch 3, 131-135
6	1	Cayley's theorem	R2: Ch 2, 60-61
7	1	Properties of isomorphism	R3: Ch 6, 133-134
8	1	First isomorphism theorem	R3: Ch 10, 214
9	1	Tutorial – III	
10	1	Examples for First isomorphism theorem	R3: Ch 10, 215-216
11	1	Tutorial-III	
12	1	Second isomorphism theorem	R3: Ch 10, 222
13	1	Third isomorphism theorem	R3: Ch 10, 222
14	1	Recapitulation and discussion of possible questions	
Total No of Hours Planned For Unit 1=14			
		UNIT-II	
1	1	Introduction to automorphism	R3: Ch 6, 134-135

2	1	Theorems on automorphism	R3: Ch 6, 135
3	1	Tutorial-I	
4	1	Inner automorphism	R3: Ch 6, 136
5	1	Tutorial-II	
6	1	Theorem on inner automorphism	R3: Ch 6, 137
7	1	Continuation of theorem on inner automorphism	R3: Ch 6, 138
8	1	Theorems on automorphism groups of finite and infinite cyclic groups	R3: Ch 11, 226-229
9	1	Continuation of theorems on automorphism groups of finite and infinite cyclic groups	R3: Ch 6, 229-233
10	1	Applications of factor groups	T1: Ch 3, 135-136
11	1	Tutorial – III	
12	1	Characteristics subgroup	T1: Ch 3, 137-140
13		Tutorial – IV	
14	1	Commutator subgroup	T1: Ch 3, 150
15	1	Properties of commutator subgroup	T1: Ch 3, 151-152
16	1	Recapitulation and discussion of possible questions	
Total No of Hours Planned For Unit II=16			
		UNIT-III	
1	1	Introduction to direct product	R3: Ch 8, 162
2	1	Theorems on direct problem	R3: Ch 8, 162-163
3	1	Tutorial-I	
4	1	Continuation of theorem on direct product	R3: Ch 8, 163
5	1	Tutorial-II	
6	1	Continuation of theorem on direct product	R3: Ch 8, 163
7	1	Properties of external direct product	R3: Ch 8, 163-164
8	1	Continuation of properties of external direct product	R3: Ch 8, 164-166
9	1	The group of units modulo n as an external direct product	R3: Ch 8, 166
10	1	Continuation of the group of units modulo n as an external direct product	R3: Ch 8, 167-168
11	1	Tutorial III	
12	1	Internal direct product	R3: Ch 9, 195
13	1	Tutorial IV	
14	1	Examples of internal directproduct	R3: Ch 9, 197

15	1	Fundamental theorem of finite abelian group	R3: Ch 11,226
16	1	Recapitulation and discussion of possible questions	
Total No of Hours Planned For Unit III – 16			
		UNIT-IV	
1	1	Introduction to Group action	T1: Ch 3, 168-170
2	1	Theorems on group action	T1: Ch 3, 168-170
3	1	Tutorial – I	
4	1	Theorems on stabilizer	R1: Ch 4, 112-114
5	1	Tutorial II	
6	1	Continuation of theorems on stabilizer	R1: Ch 4, 115
7	1	Theorems on kernels	R1: Ch 4, 116-117
8	1	Theorems on permutation representations	R1: Ch 4, 117
9	1	Continuation of permutation representations	R1: Ch 4, 117
10	1	Generalized Cayley's theorem	R1: Ch 4, 118
11	1	Tutorial-III	
12		Index theorem	R1: Ch 4, 119-120
13	1	Tutorial IV	
14	1	Problems on index theorem	R1: Ch 4, 121
15	1	Recapitulation and discussion of possible questions	
Total No of Hours Planned For Unit IV=15			
		UNIT-V	
1	1	Groups acting on themselves by conjugacy	R1: Ch 4, 122
2	1	Class equation	R4: Ch 6, 198
3	1	Conjugacy in S_n	R1: Ch 4, 142
4	1	Tutorial I	
5	1	p-groups	R1: Ch 4, 143-144
6	1	Tutorial – II	
7	1	Probability that two elements commute	R1: Ch 4, 144
8	1	Sylow's first theorem	R1: Ch 4, 145-146
9	1	Cauchy's Theorem	
10	1	Sylow's second theorem	R1: Ch 4, 146
11	1	Sylow's third theorem	R1: Ch 4, 147-148

12	1	Tutorial-III	
13	1	Applications of Sylow theorem	R1: Ch 4, 148
14	1	Tutorial IV	
15	1	Simplicity of A_n	R1: Ch 4, 149-152
16	1	Recapitulation and discussion of possible questions	
17	1	Discussion of previous ESE question papers.	
18	1	Discussion of previous ESE question papers.	
19	1	Discussion of previous ESE question papers.	
Total No of Hours Planned for unit V -19			
Total planned hours – **80**			

TEXT BOOK

1. Fraleigh.J.B., (2004). A First Course in Abstract Algebra , Seventh edition , Pearson Education Ltd, Singapore.

REFERENCES

1. David S. Dummit and Richard M. Foote, (2004)., Abstract Algebra,. Third Edition., John Wiley and Sons (Asia) Pvt. Ltd., Singapore.

2. Herstein.I.N.,(2010). Topics in Algebra ,Second Edition, Willey and sons Pvt Ltd, Singapore.

3. Joseph A. Gallian., (2001). Contemporary Abstract Algebra, Fourth Edition., Narosa Publishing House, New Delhi.

4. Artin.M., (2008). Algebra, Prentice - Hall of India, New Delhi.

Definition Group Homomorphism
A *homomorphism* ϕ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Definition Kernel of a Homomorphism
The *kernel* of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by Ker ϕ.

■ **EXAMPLE 1** Any isomorphism is a homomorphism that is also onto and one-to-one. The kernel of an isomorphism is the trivial subgroup. ■

■ **EXAMPLE 2** Let $\mathbf{R}^*$ be the group of nonzero real numbers under multiplication. Then the determinant mapping $A \to \det A$ is a homomorphism from $GL(2, \mathbf{R})$ to $\mathbf{R}^*$. The kernel of the determinant mapping is $SL(2, \mathbf{R})$. ■

■ **EXAMPLE 3** The mapping ϕ from $\mathbf{R}^*$ to $\mathbf{R}^*$, defined by $\phi(x) = |x|$, is a homomorphism with Ker $\phi = \{1, -1\}$. ■

■ **EXAMPLE 4** Let $\mathbf{R}[x]$ denote the group of all polynomials with real coefficients under addition. For any f in $\mathbf{R}[x]$, let f' denote the derivative of f. Then the mapping $f \to f'$ is a homomorphism from $\mathbf{R}[x]$ to itself. The kernel of the derivative mapping is the set of all constant polynomials. ■

■ **EXAMPLE 5** The mapping ϕ from Z to Z_n, defined by $\phi(m) = m \bmod n$, is a homomorphism (see Exercise 11 in Chapter 0). The kernel of this mapping is $\langle n \rangle$. ■

■ **EXAMPLE 6** The mapping $\phi(x) = x^2$ from $\mathbf{R}^*$, the nonzero real numbers under multiplication, to itself is a homomorphism, since $\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b)$ for all a and b in R^*. (See Exercise 5.) The kernel is $\{1, -1\}$. ■

■ **EXAMPLE 7** The mapping $\phi(x) = x^2$ from $\mathbf{R}$, the real numbers under addition, to itself is not a homomorphism, since $\phi(a + b) = (a + b)^2 = a^2 + 2ab + b^2$, whereas $\phi(a) + \phi(b) = a^2 + b^2$. ■

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G. Then

1. *ϕ carries the identity of G to the identity of $\overline{G}$.*
2. *$\phi(g^n) = (\phi(g))^n$ for all n in Z.*
3. *If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.*
4. *Ker ϕ is a subgroup of G.*
5. *$\phi(a) = \phi(b)$ if and only if $a\text{Ker } \phi = b\text{Ker } \phi$.*
6. *If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\text{Ker } \phi$.*

PROOF The proofs of properties 1 and 2 are identical to the proofs of properties 1 and 2 of isomorphisms in Theorem 6.2. To prove property 3, notice that properties 1 and 2 together with $g^n = e$ imply that $e = \phi(e) = \phi(g^n) = (\phi(g))^n$. So, by Corollary 2 to Theorem 4.1, we have $|\phi(g)|$ divides n.

By property 1 we know that Ker ϕ is not empty. So, to prove property 4, we assume that $a, b \in$ Ker ϕ and show that $ab^{-1} \in$ Ker ϕ. Since $\phi(a) = e$ and $\phi(b) = e$, we have $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = ee^{-1} = e$. So, $ab^{-1} \in$ Ker ϕ.

To prove property 5, first assume that $\phi(a) = \phi(b)$. Then $e = (\phi(b))^{-1}\phi(a) = \phi(b^{-1})\phi(a) = \phi(b^{-1}a)$, so that $b^{-1}a \in$ Ker ϕ. It now follows from property 5 of the lemma in Chapter 7 that $b\text{Ker } \phi = a\text{Ker } \phi$. Reversing this argument completes the proof.

To prove property 6, we must show that $\phi^{-1}(g') \subseteq g\text{Ker}\ \phi$ and that $g\text{Ker}\ \phi \subseteq \phi^{-1}(g')$. For the first inclusion, let $x \in \phi^{-1}(g')$, so that $\phi(x) = g'$. Then $\phi(g) = \phi(x)$ and by property 5 we have $g\text{Ker}\ \phi = x\text{Ker}\ \phi$ and therefore $x \in g\text{Ker}\ \phi$. This completes the proof that $\phi^{-1}(g') \subseteq g\text{Ker}\ \phi$. To prove that $g\text{Ker}\ \phi \subseteq \phi^{-1}(g')$, suppose that $k \in \text{Ker}\ \phi$. Then $\phi(gk) = \phi(g)\phi(k) = g'e = g'$. Thus, by definition, $gk \in \phi^{-1}(g')$. ∎

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let H be a subgroup of G. Then

1. *$\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.*
2. *If H is cyclic, then $\phi(H)$ is cyclic.*
3. *If H is Abelian, then $\phi(H)$ is Abelian.*
4. *If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.*
5. *If $|\text{Ker}\ \phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$.*
6. *If $|H| = n$, then $|\phi(H)|$ divides n.*
7. *If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a subgroup of G.*
8. *If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a normal subgroup of G.*
9. *If ϕ is onto and $\text{Ker}\ \phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.*

PROOF First note that the proofs of properties 1, 2, and 3 are identical to the proofs of properties 4, 3, and 2, respectively, of Theorem 6.3, since those proofs use only the fact that an isomorphism is an operation-preserving mapping.

To prove property 4, let $\phi(h) \in \phi(H)$ and $\phi(g) \in \phi(G)$. Then $\phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1}) \in \phi(H)$, since H is normal in G.

Property 5 follows directly from property 6 of Theorem 10.1 and the fact that all cosets of Ker $\phi = \phi^{-1}(e)$ have the same number of elements.

To prove property 6, let ϕ_H denote the restriction of ϕ to the elements of H. Then ϕ_H is a homomorphism from H onto $\phi(H)$. Suppose $|\text{Ker } \phi_H| = t$. Then, by property 5, ϕ_H is a t-to-1 mapping. So, $|\phi(H)|t = |H|$.

To prove property 7, we use the One-Step Subgroup Test. Clearly, $e \in \phi^{-1}(\overline{K})$, so that $\phi^{-1}(\overline{K})$ is not empty. Let $k_1, k_2 \in \phi^{-1}(\overline{K})$. Then, by the definition of $\phi^{-1}(\overline{K})$, we know that $\phi(k_1), \phi(k_2) \in \overline{K}$. Thus, $\phi(k_2)^{-1} \in \overline{K}$ as well and $\phi(k_1k_2^{-1}) = \phi(k_1)\phi(k_2)^{-1} \in \overline{K}$. So, by definition of $\phi^{-1}(\overline{K})$, we have $k_1k_2^{-1} \in \phi^{-1}(\overline{K})$.

To prove property 8, we use the normality test given in Theorem 9.1. Note that every element in $x\phi^{-1}(\overline{K})x^{-1}$ has the form xkx^{-1}, where $\phi(k) \in \overline{K}$. Thus, since $\overline{K}$ is normal in $\overline{G}$, $\phi(xkx^{-1}) = \phi(x)\phi(k)(\phi(x))^{-1} \in \overline{K}$, and, therefore, $xkx^{-1} \in \phi^{-1}(\overline{K})$.

Finally, property 9 follows directly from property 5. ∎

Corollary Kernels Are Normal

Let ϕ be a group homomorphism from G to $\overline{G}$. Then Ker ϕ is a normal subgroup of G.

EXAMPLE 8 Consider the mapping ϕ from $\mathbf{C}^*$ to $\mathbf{C}^*$ given by $\phi(x) = x^4$. Since $(xy)^4 = x^4y^4$, ϕ is a homomorphism. Clearly, Ker $\phi = \{x \mid x^4 = 1\} = \{1, -1, i, -i\}$. So, by property 5 of Theorem 10.2, we know that ϕ is a 4-to-1 mapping. Now let's find all elements that map to, say, 2. Certainly, $\phi(\sqrt[4]{2}) = 2$. Then, by property 6 of Theorem 10.1, the set of all elements that map to 2 is $\sqrt[4]{2}\,\text{Ker } \phi = \{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}\,i, -\sqrt[4]{2}\,i\}$.

■ **EXAMPLE 9** Define $\phi: Z_{12} \to Z_{12}$ by $\phi(x) = 3x$. To verify that ϕ is a homomorphism, we observe that in Z_{12}, $3(a + b) = 3a + 3b$ (since the group operation is addition modulo 12). Direct calculations show that Ker $\phi = \{0, 4, 8\}$. Thus, we know from property 5 of Theorem 10.2 that ϕ is a 3-to-1 mapping. Since $\phi(2) = 6$, we have by property 6 of Theorem 10.1 that $\phi^{-1}(6) = 2 + \text{Ker } \phi = \{2, 6, 10\}$. Notice also that $\langle 2 \rangle$ is cyclic and $\phi(\langle 2 \rangle) = \{0, 6\}$ is cyclic. Moreover, $|2| = 6$ and $|\phi(2)| = |6| = 2$, so $|\phi(2)|$ divides $|2|$ in agreement with property 3 of Theorem 10.1. Letting $K = \{0, 6\}$, we see that the subgroup $\phi^{-1}(K) = \{0, 2, 4, 6, 8, 10\}$. This verifies property 7 of Theorem 10.2 in this particular case. ■

■ **EXAMPLE 10** We determine all homomorphisms from Z_{12} to Z_{30}. By property 2 of Theorem 10.1, such a homomorphism is completely specified by the image of 1. That is, if 1 maps to a, then x maps to xa. Lagrange's Theorem and property 3 of Theorem 10.1 require that $|a|$ divide both 12 and 30. So, $|a| = 1$, 2, 3, or 6. Thus, $a = 0$, 15, 10, 20, 5, or 25. This gives us a list of candidates for the homomorphisms. That each of these six possibilities yields an operation-preserving, well-defined function can now be verified by direct calculations. [Note that gcd(12, 30) = 6. This is not a coincidence!] ■

■ **EXAMPLE 11** The mapping from S_n to Z_2 that takes an even permutation to 0 and an odd permutation to 1 is a homomorphism. Figure 10.2 illustrates the telescoping nature of the mapping. ■

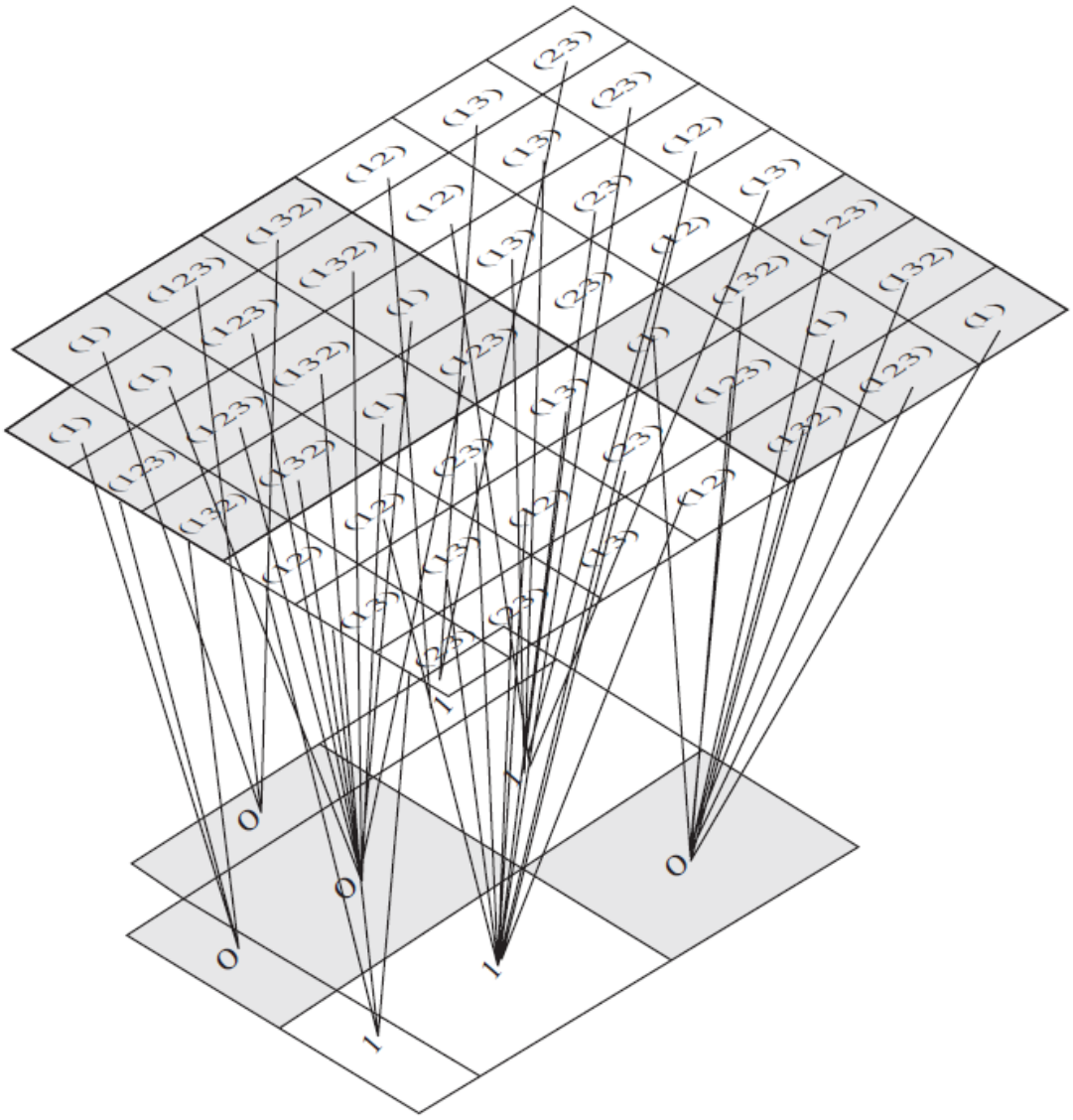


Figure 10.2 Homomorphism from S_3 to Z_2.

The First Isomorphism Theorem

Let ϕ be a group homomorphism from G to $\overline{G}$. Then the mapping from $G/Ker\ \phi$ to $\phi(G)$, given by $gKer\ \phi \to \phi(g)$, is an isomorphism. In symbols, $G/Ker\ \phi \approx \phi(G)$.

PROOF Let us use ψ to denote the correspondence $g\text{Ker}\,\phi \to \phi(g)$. That ψ is well defined (that is, the correspondence is independent of the particular coset representative chosen) and one-to-one follows directly from property 5 of Theorem 10.1. To show that ψ is operation-preserving, observe that $\psi(x\text{Ker}\,\phi\ y\text{Ker}\,\phi) = \psi(xy\text{Ker}\,\phi) = \phi(xy) = \phi(x)\,\phi(y) = \psi(x\text{Ker}\,\phi)\psi(y\text{Ker}\,\phi)$. ∎

Corollary

If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $|\overline{G}|$.

Normal Subgroups Are Kernels

Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping $g \to gN$ from G to G/N.

PROOF Define $\gamma: G \to G/N$ by $\gamma(g) = gN$. (This mapping is called the *natural homomorphism* from G to G/N.) Then, $\gamma(xy) = (xy)N = xNyN = \gamma(x)\gamma(y)$. Moreover, $g \in \text{Ker}\ \gamma$ if and only if $gN = \gamma(g) = N$, which is true if and only if $g \in N$ (see property 2 of the lemma in Chapter 7). ∎

(Second Isomorphism Theorem) If K is a subgroup of G and N is a normal subgroup of G, prove that $K/(K \cap N)$ is isomorphic to KN/N.

(Third Isomorphism Theorem) If M and N are normal subgroups of G and $N \leq M$, prove that $(G/N)/(M/N) \approx G/M$.

Definition Automorphism
An isomorphism from a group G onto itself is called an *automorphism* of G.

Definition Inner Automorphism Induced by *a*
Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is called the *inner automorphism of G induced by a*.

Aut(G) and Inn(G) Are Groups

The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

EXAMPLE

To determine $\text{Inn}(D_4)$, we first observe that the complete list of inner automorphisms is ϕ_{R_0}, $\phi_{R_{90}}$, $\phi_{R_{180}}$, $\phi_{R_{270}}$, ϕ_H, ϕ_V, ϕ_D, and $\phi_{D'}$. Our job is to determine the repetitions in this list. Since $R_{180} \in Z(D_4)$, we have $\phi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = x$, so that $\phi_{R_{180}} = \phi_{R_0}$. Also, $\phi_{R_{270}}(x) = R_{270}xR_{270}^{-1} = R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1} = \phi_{R_{90}}(x)$. Similarly, since $H = R_{180}V$ and $D' = R_{180}D$, we have $\phi_H = \phi_V$ and $\phi_D = \phi_{D'}$.

EXAMPLE

To compute $\text{Aut}(Z_{10})$, we try to discover enough information about an element α of $\text{Aut}(Z_{10})$ to determine how α must be defined. Because Z_{10} is so simple, this is not difficult to do. To begin with, observe that once we know $\alpha(1)$, we know $\alpha(k)$ for any k, because

$$\alpha(k) = \underbrace{\alpha(1 + 1 + \cdots + 1)}_{k \text{ terms}}$$
$$= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{k \text{ terms}} = k\alpha(1).$$

So, we need only determine the choices for $\alpha(1)$ that make α an automorphism of Z_{10}. Since property 5 of Theorem 6.2 tells us that $|\alpha(1)| = 10$, there are four candidates for $\alpha(1)$:

$$\alpha(1) = 1; \qquad \alpha(1) = 3; \qquad \alpha(1) = 7; \qquad \alpha(1) = 9.$$

To distinguish among the four possibilities, we refine our notation by denoting the mapping that sends 1 to 1 by α_1, 1 to 3 by α_3, 1 to 7 by α_7, and 1 to 9 by α_9. So the only possibilities for $\text{Aut}(Z_{10})$ are α_1, α_3, α_7, and α_9. But are all these automorphisms? Clearly, α_1 is the identity. Let us check α_3. Since $x \bmod 10 = y \bmod 10$ implies $3x \bmod 10 = 3y \bmod 10$, α_3 is well defined. Moreover, because $\alpha_3(1) = 3$ is a generator of Z_{10}, it follows that α_3 is onto (and, by Exercise 10 in Chapter 5, it is also one-to-one). Finally, since $\alpha_3(a + b) = 3(a + b) = 3a + 3b = \alpha_3(a) + \alpha_3(b)$, we see that α_3 is operation-preserving as well. Thus, $\alpha_3 \in \text{Aut}(Z_{10})$. The same argument shows that α_7 and α_9 are also automorphisms.

This gives us the elements of $\text{Aut}(Z_{10})$ but not the structure. For instance, what is $\alpha_3\alpha_3$? Well, $(\alpha_3\alpha_3)(1) = \alpha_3(3) = 3 \cdot 3 = 9 = \alpha_9(1)$, so $\alpha_3\alpha_3 = \alpha_9$. Similar calculations show that ${\alpha_3}^3 = \alpha_7$ and ${\alpha_3}^4 = \alpha_1$, so that $|\alpha_3| = 4$. Thus, $\text{Aut}(Z_{10})$ is cyclic. Actually, the following Cayley tables reveal that $\text{Aut}(Z_{10})$ is isomorphic to $U(10)$.

$U(10)$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\text{Aut}(Z_{10})$	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

$\mathrm{Aut}(Z_n) \approx U(n)$

For every positive integer n, $Aut(Z_n)$ is isomorphic to $U(n)$.

PROOF As in Example 13, any automorphism α is determined by the value of $\alpha(1)$, and $\alpha(1) \in U(n)$. Now consider the correspondence from $\mathrm{Aut}(Z_n)$ to $U(n)$ given by $T: \alpha \to \alpha(1)$. The fact that $\alpha(k) = k\alpha(1)$ (see Example 13) implies that T is a one-to-one mapping. For if α and β belong to $\mathrm{Aut}(Z_n)$ and $\alpha(1) = \beta(1)$, then $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$ for all k in Z_n, and therefore $\alpha = \beta$.

To prove that T is onto, let $r \in U(n)$ and consider the mapping α from Z_n to Z_n defined by $\alpha(s) = sr \pmod n$ for all s in Z_n. We leave it as an exercise to verify that α is an automorphism of Z_n (see Exercise 17). Then, since $T(\alpha) = \alpha(1) = r$, T is onto $U(n)$.

Finally, we establish the fact that T is operation-preserving. Let α, $\beta \in \mathrm{Aut}(Z_n)$. We then have

$$\begin{aligned} T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1)) &= \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1)\text{ terms}}) \\ &= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1)\text{ terms}} = \alpha(1)\beta(1) \\ &= T(\alpha)T(\beta). \end{aligned}$$

This completes the proof. ∎

Fundamental Theorem of Finite Abelian Groups

Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Since a cyclic group of order n is isomorphic to Z_n, Theorem 11.1 shows that every finite Abelian group G is isomorphic to a group of the form

$$Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \cdots \oplus Z_{p_k^{n_k}},$$

where the p_i's are not necessarily distinct primes and the prime-powers $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ are uniquely determined by G. Writing a group in this form is called *determining the isomorphism class of G.*

Greedy Algorithm for an Abelian Group of Order p^n

1. Compute the orders of the elements of the group G.
2. Select an element a_1 of maximum order and define $G_1 = \langle a_1 \rangle$. Set $i = 1$.
3. If $|G| = |G_i|$, stop. Otherwise, replace i by $i + 1$.
4. Select an element a_i of maximum order p^k such that $p^k \leq |G|/|G_{i-1}|$ and none of $a_i, a_i^p, a_i^{p^2}, \ldots, a_i^{p^{k-1}}$ is in G_{i-1}, and define $G_i = G_{i-1} \times \langle a_i \rangle$.
5. Return to step 3.

■ EXAMPLE

Let $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51,$ $53, 57, 64\}$ under multiplication modulo 65. Since G has order 16, we know it is isomorphic to one of

$$Z_{16},$$
$$Z_8 \oplus Z_2,$$
$$Z_4 \oplus Z_4,$$
$$Z_4 \oplus Z_2 \oplus Z_2,$$
$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2.$$

To decide which one, we dirty our hands to calculate the orders of the elements of G.

Element	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
Order	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

From the table of orders, we can instantly rule out all but $Z_4 \oplus Z_4$ and $Z_4 \oplus Z_2 \oplus Z_2$ as possibilities. Finally, we observe that since this latter group has a subgroup isomorphic to $Z_2 \oplus Z_2 \oplus Z_2$, it has more than three elements of order 2, and therefore we must have $G \approx Z_4 \oplus Z_4$.

Expressing G as an internal direct product is even easier. Pick an element of maximum order, say the element 8. Then $\langle 8 \rangle$ is a factor in the product. Next, choose a second element, say a, so that a has order 4 and a and a^2 are not in $\langle 8 \rangle = \{1, 8, 64, 57\}$. Since 12 has this property, we have $G = \langle 8 \rangle \times \langle 12 \rangle$. ∎

∎ EXAMPLE

Let $G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$ under multiplication modulo 135. Since G has order 24, it is isomorphic to one of

$$Z_8 \oplus Z_3 \approx Z_{24},$$
$$Z_4 \oplus Z_2 \oplus Z_3 \approx Z_{12} \oplus Z_2,$$
$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \approx Z_6 \oplus Z_2 \oplus Z_2.$$

Consider the element 8. Direct calculations show that $8^6 = 109$ and $8^{12} = 1$. (Be sure to mod as you go. For example, $8^3 \bmod 135 = 512 \bmod 135 = 107$, so compute 8^4 as $8 \cdot 107$ rather than $8 \cdot 512$.) But now we know G. Why? Clearly, $|8| = 12$ rules out the third group in the list. At the same time, $|109| = 2 = |134|$ (remember, $134 = -1 \bmod 135$) implies that G is not Z_{24} (see Theorem 4.4). Thus, $G \approx Z_{12} \oplus Z_2$, and $G = \langle 8 \rangle \times \langle 134 \rangle$. ∎

Existence of Subgroups of Abelian Groups

If m divides the order of a finite Abelian group G, then G has a subgroup of order m.

Lemma 1

Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.

PROOF It is an easy exercise to prove that H and K are subgroups of G (see Exercise 29 in Chapter 3). Because G is Abelian, to prove that $G = H \times K$ we need only prove that $G = HK$ and $H \cap K = \{e\}$. Since we have $\gcd(m, p^n) = 1$, there are integers s and t such that $1 = sm + tp^n$. For any x in G, we have $x = x^1 = x^{sm+tp^n} = x^{sm}x^{tp^n}$ and, by Corollary 4 of Lagrange's Theorem (Theorem 7.1), $x^{sm} \in H$ and $x^{tp^n} \in K$. Thus, $G = HK$. Now suppose that some $x \in H \cap K$. Then $x^{p^n} = e = x^m$ and, by Corollary 2 to Theorem 4.1, $|x|$ divides both p^n and m. Since p does not divide m, we have $|x| = 1$ and, therefore, $x = e$.

To prove the second assertion of the lemma, note that $p^n m = |HK| = |H||K|/|H \cap K| = |H||K|$ (see Exercise 7 in the Supplementary Exercises for Chapters 5–8). It follows from Theorem 9.5 and Corollary 2 to Theorem 4.1 that p does not divide $|K|$ and therefore $|H| = p^n$. ∎

Lemma 2

Let G be an Abelian group of prime-power order and let a be an element of maximal order in G. Then G can be written in the form $\langle a \rangle \times K$.

PROOF We denote $|G|$ by p^n and induct on n. If $n = 1$, then $G = \langle a \rangle \times \langle e \rangle$. Now assume that the statement is true for all Abelian groups of order p^k, where $k < n$. Among all the elements of G, choose a of maximal order p^m. Then $x^{p^m} = e$ for all x in G. We may assume that $G \neq \langle a \rangle$, for otherwise there is nothing to prove. Now, among all the elements of G, choose b of smallest order such that $b \notin \langle a \rangle$. We claim that $\langle a \rangle \cap \langle b \rangle = \{e\}$. Since $|b^p| = |b|/p$, we know that $b^p \in \langle a \rangle$ by the manner in which b was chosen. Say $b^p = a^i$. Notice that $e = b^{p^m} = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}$, so $|a^i| \leq p^{m-1}$. Thus, a^i is not a generator of $\langle a \rangle$ and, therefore, by Corollary 3 to Theorem 4.2, $\gcd(p^m, i) \neq 1$. This proves that p divides i, so that we can write $i = pj$. Then $b^p = a^i = a^{pj}$. Consider the element $c = a^{-j}b$. Certainly, c is not in $\langle a \rangle$, for if it were, b would be, too. Also, $c^p = a^{-jp}b^p = a^{-i}b^p = b^{-p}b^p = e$. Thus, we have found an element c of order p such that $c \notin \langle a \rangle$. Since b was chosen to have smallest order such that $b \notin \langle a \rangle$, we conclude that b also has order p. It now follows that $\langle a \rangle \cap \langle b \rangle = \{e\}$ because any nonidentity element of the intersection would generate $\langle b \rangle$ and thus contradict $b \notin \langle a \rangle$.

Now consider the factor group $\overline{G} = G/\langle b \rangle$. To simplify the notation, we let $\overline{x}$ denote the coset $x\langle b \rangle$ in $\overline{G}$. If $|\overline{a}| < |a| = p^m$, then $\overline{a}^{p^{m-1}} = \overline{e}$. This means that $(a\langle b \rangle)^{p^{m-1}} = a^{p^{m-1}}\langle b \rangle = \langle b \rangle$, so that $a^{p^{m-1}} \in \langle a \rangle \cap \langle b \rangle = \{e\}$, contradicting the fact that $|a| = p^m$. Thus, $|\overline{a}| = |a| = p^m$, and therefore $\overline{a}$ is an element of maximal order in $\overline{G}$. By induction, we know that $\overline{G}$ can be written in the form $\langle \overline{a} \rangle \times \overline{K}$ for some subgroup $\overline{K}$ of $\overline{G}$. Let K be the pullback of $\overline{K}$ under the natural homomorphism from G to $\overline{G}$ (that is, $K = \{x \in G \mid \overline{x} \in \overline{K}\}$). We claim that $\langle a \rangle \cap K = \{e\}$. For if $x \in \langle a \rangle \cap K$, then $\overline{x} \in \langle \overline{a} \rangle \cap \overline{K} = \{\overline{e}\} = \langle b \rangle$ and $x \in \langle a \rangle \cap \langle b \rangle = \{e\}$. It now follows from an order argument (see Exercise 33) that $G = \langle a \rangle K$, and therefore $G = \langle a \rangle \times K$. ∎

Lemma 3

A finite Abelian group of prime-power order is an internal direct product of cyclic groups.

Lemma 4

Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the H's and K's are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

PROOF We proceed by induction on $|G|$. Clearly, the case where $|G| = p$ is true. Now suppose that the statement is true for all Abelian groups of order less than $|G|$. For any Abelian group L, the set $L^p = \{x^p \mid x \in L\}$ is a subgroup of L (see Exercise 15 in the Supplementary Exercises for Chapters 1–4) and, by Theorem 9.5, is a proper subgroup if p divides $|L|$. It follows that $G^p = {H_1}^p \times {H_2}^p \times \cdots \times {H_{m'}}^p$, and $G^p = {K_1}^p \times {K_2}^p \times \cdots \times {K_{n'}}^p$, where m' is the largest integer i such that $|H_i| > p$, and n' is the largest integer j such that $|K_j| > p$. (This ensures that our two direct products for G^p do not have trivial factors.) Since $|G^p| < |G|$, we have, by induction, $m' = n'$ and $|{H_i}^p| = |{K_i}^p|$ for $i = 1, \ldots, m'$. Since $|H_i| = p|{H_i}^p|$, this proves that $|H_i| = |K_i|$ for all $i = 1, \ldots, m'$. All that remains to be proved is that the number of H_i of order p equals the number of K_i of order p; that is, we must prove that $m - m' = n - n'$ (since $n' = m'$). This follows directly from the facts that $|H_1||H_2| \cdots |H_{m'}|p^{m-m'} = |G| = |K_1||K_2| \cdots |K_{n'}|p^{n-n'}$, $|H_i| = |K_i|$, and $m' = n'$. ∎

Factor Groups

Factor Groups from Homomorphisms

Theorem

Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a **factor group**, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.

Example

Consider the factor group $\mathbb{Z}/5\mathbb{Z}$ with the cosets shown above. We can add $(2 + 5\mathbb{Z}) + (4 + 5\mathbb{Z})$ by choosing 2 and 4, finding $2 + 4 = 6$, and noticing that 6 is in the coset $1 + 5\mathbb{Z}$. We could equally well add these two cosets by choosing 27 in $2 + 5\mathbb{Z}$ and -16 in $4 + 5\mathbb{Z}$; the sum $27 + (-16) = 11$ is also in the coset $1 + 5\mathbb{Z}$. ▲

The factor groups $\mathbb{Z}/n\mathbb{Z}$ in the preceding example are classics. Recall that we refer to the cosets of $n\mathbb{Z}$ as *residue classes modulo* n. Two integers in the same coset are *congruent modulo* n. This terminology is carried over to other factor groups. A factor group G/H is often called the **factor group of** G **modulo** H. Elements in the same coset of H are often said to be **congruent modulo** H. By abuse of notation, we may sometimes write $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ and think of $\mathbb{Z}_n$ as the additive group of residue classes of $\mathbb{Z}$ modulo $\langle n \rangle$, or abusing notation further, modulo n.

Factor Groups from Normal Subgroups

Theorem

Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Proof

Suppose first that $(aH)(bH) = (ab)H$ does give a well-defined binary operation on left cosets. Let $a \in G$. We want to show that aH and Ha are the same set. We use the standard technique of showing that each is a subset of the other.

Let $x \in aH$. Choosing representatives $x \in aH$ and $a^{-1} \in a^{-1}H$, we have $(xH)(a^{-1}H) = (xa^{-1})H$. On the other hand, choosing representatives $a \in aH$ and $a^{-1} \in a^{-1}H$, we see that $(aH)(a^{-1}H) = eH = H$. Using our assumption that left coset multiplication by representatives is well defined, we must have $xa^{-1} = h \in H$. Then $x = ha$, so $x \in Ha$ and $aH \subseteq Ha$. We leave the symmetric proof that $Ha \subseteq aH$ to Exercise 25.

We turn now to the converse: If H is a normal subgroup, then left coset multiplication by representatives is well-defined. Due to our hypothesis, we can simply say *cosets,* omitting *left* and *right*. Suppose we wish to compute $(aH)(bH)$. Choosing $a \in aH$ and $b \in bH$, we obtain the coset $(ab)H$. Choosing different representatives $ah_1 \in aH$ and $bh_2 \in bH$, we obtain the coset ah_1bh_2H. We must show that these are the same cosets. Now $h_1b \in Hb = bH$, so $h_1b = bh_3$ for some $h_3 \in H$. Thus

$$(ah_1)(bh_2) = a(h_1b)h_2 = a(bh_3)h_2 = (ab)(h_3h_2)$$

and $(ab)(h_3h_2) \in (ab)H$. Therefore, ah_1bh_2 is in $(ab)H$. ◆

Corollary

Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$. ▲

Proof

Computing, $(aH)[(bH)(cH)] = (aH)[(bc)H] = [a(bc)]H$, and similarly, we have $[(aH)(bH)](cH) = [(ab)c]H$, so associativity in G/H follows from associativity in G. Because $(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH)$, we see that $eH = H$ is the identity element in G/H. Finally, $(a^{-1}H)(aH) = (a^{-1}a)H = eH = (aa^{-1})H = (aH)(a^{-1}H)$ shows that $a^{-1}H = (aH)^{-1}$. ◆

Example

Since $\mathbb{Z}$ is an abelian group, $n\mathbb{Z}$ is a normal subgroup. Corollary 14.5 allows us to construct the factor group $\mathbb{Z}/n\mathbb{Z}$ with no reference to a homomorphism. As we observed in Example 14.2, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. ▲

Example

Consider the abelian group $\mathbb{R}$ under addition, and let $c \in \mathbb{R}^+$. The cyclic subgroup $\langle c \rangle$ of $\mathbb{R}$ contains as elements

$$\cdots -3c, -2c, -c, 0, c, 2c, 3c, \cdots.$$

Every coset of $\langle c \rangle$ contains just one element x such that $0 \leq x < c$. If we choose these elements as representatives of the cosets when computing in $\mathbb{R}/\langle c \rangle$, we find that we are computing their sum modulo c as discussed for the computation in $\mathbb{R}_c$ in Section 1. For example, if $c = 5.37$, then the sum of the cosets $4.65 + \langle 5.37 \rangle$ and $3.42 + \langle 5.37 \rangle$ is the coset $8.07 + \langle 5.37 \rangle$, which contains $8.07 - 5.37 = 2.7$, which is $4.65 +_{5.37} 3.42$. Working with these coset elements x where $0 \leq x < c$, we thus see that the group $\mathbb{R}_c$ of Example 4.2 is isomorphic to $\mathbb{R}/\langle c \rangle$ under an isomorphism ψ where $\psi(x) = x + \langle c \rangle$ for all $x \in \mathbb{R}_c$. Of course, $\mathbb{R}/\langle c \rangle$ is then also isomorphic to the circle group U of complex numbers of magnitude 1 under multiplication. ▲

The Center and Commutator Subgroups

Example

The center of a group G always contains the identity element e. It may be that $Z(G) = \{e\}$, in which case we say that **the center of G is trivial**. For example, examination of Table 8.8 for the group S_3 shows us that $Z(S_3) = \{\rho_0\}$, so the center of S_3 is trivial. (This is a special case of Exercise 38, which shows that the center of every nonabelian group of order pq for primes p and q is trivial.) Consequently, the center of $S_3 \times \mathbb{Z}_5$ must be $\{\rho_0\} \times \mathbb{Z}_5$, which is isomorphic to $\mathbb{Z}_5$. ▲

Theorem

Let G be a group. The set of all commutators $aba^{-1}b^{-1}$ for $a, b \in G$ generates a subgroup C (the **commutator subgroup**) of G. This subgroup C is a normal subgroup of G. Furthermore, if N is a normal subgroup of G, then G/N is abelian if and only if $C \leq N$.

Proof

The commutators certainly generate a subgroup C; we must show that it is normal in G. Note that the inverse $(aba^{-1}b^{-1})^{-1}$ of a commutator is again a commutator, namely, $bab^{-1}a^{-1}$. Also $e = eee^{-1}e^{-1}$ is a commutator. Theorem 7.6 then shows that C consists precisely of all finite products of commutators. For $x \in C$, we must show that $g^{-1}xg \in C$ for all $g \in G$, or that if x is a product of commutators, so is $g^{-1}xg$ for all $g \in G$. By inserting $e = gg^{-1}$ between each product of commutators occurring in x, we see that it is sufficient to show for each commutator $cdc^{-1}d^{-1}$ that $g^{-1}(cdc^{-1}d^{-1})g$ is in C. But

$$\begin{aligned} g^{-1}(cdc^{-1}d^{-1})g &= (g^{-1}cdc^{-1})(e)(d^{-1}g) \\ &= (g^{-1}cdc^{-1})(gd^{-1}dg^{-1})(d^{-1}g) \\ &= [(g^{-1}c)d(g^{-1}c)^{-1}d^{-1}][dg^{-1}d^{-1}g], \end{aligned}$$

which is in C. Thus C is normal in G.

The rest of the theorem is obvious if we have acquired the proper feeling for factor groups. One doesn't visualize in this way, but writing out that G/C is abelian follows from

$$\begin{aligned} (aC)(bC) &= abC = ab(b^{-1}a^{-1}ba)C \\ &= (abb^{-1}a^{-1})baC = baC = (bC)(aC). \end{aligned}$$

Furthermore, if N is a normal subgroup of G and G/N is abelian, then $(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$; that is, $aba^{-1}b^{-1}N = N$, so $aba^{-1}b^{-1} \in N$, and $C \leq N$. Finally, if $C \leq N$, then

$$\begin{aligned} (aN)(bN) &= abN = ab(b^{-1}a^{-1}ba)N \\ &= (abb^{-1}a^{-1})baN = baN = (bN)(aN). \end{aligned}$$

◆

Definition External Direct Product

Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.

EXAMPLE

$$U(8) \oplus U(10) = \{(1, 1), (1, 3), (1, 7), (1, 9), (3, 1), (3, 3), (3, 7), (3, 9), (5, 1), (5, 3), (5, 7), (5, 9), (7, 1),(7, 3), (7, 7), (7, 9)\}.$$

The product $(3, 7)(7, 9) = (5, 3)$, since the first components are combined by multiplication modulo 8, whereas the second components are combined by multiplication modulo 10. ∎

EXAMPLE

$$Z_2 \oplus Z_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

Clearly, this is an Abelian group of order 6. Is this group related to another Abelian group of order 6 that we know, namely, Z_6? Consider the subgroup of $Z_2 \oplus Z_3$ generated by $(1, 1)$. Since the operation in each component is addition, we have $(1, 1) = (1, 1)$, $2(1, 1) = (0, 2)$, $3(1, 1) = (1, 0)$, $4(1, 1) = (0, 1)$, $5(1, 1) = (1, 2)$, and $6(1, 1) = (0, 0)$. Hence $Z_2 \oplus Z_3$ is cyclic. It follows that $Z_2 \oplus Z_3$ is isomorphic to Z_6. ∎

EXAMPLE

Classification of Groups of Order 4

A group of order 4 is isomorphic to Z_4 or $Z_2 \oplus Z_2$. To verify this, let $G = \{e, a, b, ab\}$. If G is not cyclic, then it follows from Lagrange's Theorem that $|a| = |b| = |ab| = 2$. Then the mapping $e \to (0, 0)$, $a \to (1, 0)$, $b \to (0, 1)$, and $ab \to (1, 1)$ is an isomorphism from G onto $Z_2 \oplus Z_2$. ∎

Properties of External Direct Products

∎ Theorem

The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|).$$

PROOF Denote the identity of G_i by e_i. Let $s = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$ and $t = |(g_1, g_2, \ldots, g_n)|$. Because s is a multiple of each $|g_i|$ implies that $(g_1, g_2, \ldots, g_n)^s = (g_1^s, g_2^s, \ldots, g_n^s) = (e_1, e_2, \ldots, e_n)$, we know that $t \leq s$. On the other hand, from $(g_1^t, g_2^t, \ldots, g_n^t) = (g_1, g_2, \ldots, g_n)^t = (e_1, e_2, \ldots, e_n)$ we see that t is a common multiple of $|g_1|, |g_2|, \ldots, |g_n|$. Thus, $s \leq t$. ∎

∎ EXAMPLE

We determine the number of elements of order 5 in

$Z_{25} \oplus Z_5$. By Theorem 8.1, we may count the number of elements (a, b) in $Z_{25} \oplus Z_5$ with the property that $5 = |(a, b)| = \text{lcm}(|a|, |b|)$. Clearly this requires that either $|a| = 5$ and $|b| = 1$ or 5, or $|b| = 5$ and $|a| = 1$ or 5. We consider two mutually exclusive cases.

Case 1 $|a| = 5$ and $|b| = 1$ or 5. Here there are four choices for a (namely, 5, 10, 15, and 20) and five choices for b. This gives 20 elements of order 5.

Case 2 $|a| = 1$ and $|b| = 5$. This time there is one choice for a and four choices for b, so we obtain four more elements of order 5.

Thus, $Z_{25} \oplus Z_5$ has 24 elements of order 5. ∎

∎ EXAMPLE

We determine the number of cyclic subgroups of order 10 in $Z_{100} \oplus Z_{25}$. We begin by counting the number of elements (a, b) of order 10.

Case 1 $|a| = 10$ and $|b| = 1$ or 5. Since Z_{100} has a unique cyclic subgroup of order 10 and any cyclic group of order 10 has four generators (Theorem 4.4), there are four choices for a. Similarly, there are five choices for b. This gives 20 possibilities for (a, b).

Case 2 $|a| = 2$ and $|b| = 5$. Since any finite cyclic group of even order has a unique subgroup of order 2 (Theorem 4.4), there is only one choice for a. Obviously, there are four choices for b. So, this case yields four more possibilities for (a, b).

Thus, $Z_{100} \oplus Z_{25}$ has 24 elements of order 10. Because each cyclic subgroup of order 10 has four elements of order 10 and no two of the cyclic subgroups can have an element of order 10 in common, there must be $24/4 = 6$ cyclic subgroups of order 10. (This method is analogous to determining the number of sheep in a flock by counting legs and dividing by 4.) ∎

∎ EXAMPLE

For each divisor r of m and s of n the group $Z_m \oplus Z_n$

has a subgroup isomorphic to $Z_r \oplus Z_s$ (see Exercise 17). To find a subgroup of say $Z_{30} \oplus Z_{12}$ isomorphic to $Z_6 \oplus Z_4$ we observe that $\langle 5 \rangle$ is a subgroup of Z_{30} of order 6 and $\langle 3 \rangle$ is a subgroup of Z_{12} of order 4, so $\langle 5 \rangle \oplus \langle 3 \rangle$ is the desired subgroup. ∎

Theorem

Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

PROOF Let $|G| = m$ and $|H| = n$, so that $|G \oplus H| = mn$. To prove the first half of the theorem, we assume $G \oplus H$ is cyclic and show that m and n are relatively prime. Suppose that $\gcd(m, n) = d$ and (g, h) is a generator of $G \oplus H$. Since $(g, h)^{mn/d} = ((g^m)^{n/d}, (h^n)^{m/d}) = (e, e)$, we have $mn = |(g, h)| \leq mn/d$. Thus, $d = 1$.

To prove the other half of the theorem, let $G = \langle g \rangle$ and $H = \langle h \rangle$ and suppose $\gcd(m, n) = 1$. Then, $|(g, h)| = \text{lcm}(m, n) = mn = |G \oplus H|$, so that (g, h) is a generator of $G \oplus H$. ∎

Corollary

Criterion for $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ to Be Cyclic

An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.

Corollary

Criterion for $Z_{n_1 n_2 \cdots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$

Let $m = n_1 n_2 \cdots n_k$. Then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

Theorem $U(n)$ as an External Direct Product

Suppose s and t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. In short,

$$U(st) \approx U(s) \oplus U(t).$$

Moreover, $U_s(st)$ is isomorphic to $U(t)$ and $U_t(st)$ is isomorphic to $U(s)$.

PROOF An isomorphism from $U(st)$ to $U(s) \oplus U(t)$ is $x \to (x \bmod s, x \bmod t)$; an isomorphism from $U_s(st)$ to $U(t)$ is $x \to x \bmod t$; an isomorphism from $U_t(st)$ to $U(s)$ is $x \to x \bmod s$. We leave the verification that these mappings are operation-preserving, one-to-one, and onto to the reader. (See Exercises 11, 17, and 19 in Chapter 0; see also [1].) ∎

Corollary

Let $m = n_1 n_2 \cdots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then,

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k).$$

GROUP ACTION ON A SET

The Notion of a Group Action

Definition

Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \to X$ such that ■

1. $ex = x$ for all $x \in X$,
2. $(g_1g_2)(x) = g_1(g_2x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.**

Example

Let X be any set, and let H be a subgroup of the group S_X of all permutations of X. Then X is an H-set, where the action of $\sigma \in H$ on X is its action as an element of S_X, so that $\sigma x = \sigma(x)$ for all $x \in X$. Condition 2 is a consequence of the definition of permutation multiplication as function composition, and Condition 1 is immediate from the definition of the identity permutation as the identity function. Note that, in particular, $\{1, 2, 3, \cdots, n\}$ is an S_n-set. ▲

Theorem

Let X be a G-set. For each $g \in G$, the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X. Also, the map $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

Proof

To show that σ_g is a permutation of X, we must show that it is a one-to-one map of X onto itself. Suppose that $\sigma_g(x_1) = \sigma_g(x_2)$ for $x_1, x_2 \in X$. Then $gx_1 = gx_2$. Consequently, $g^{-1}(gx_1) = g^{-1}(gx_2)$. Using Condition 2 in Definition 16.1, we see that $(g^{-1}g)x_1 = (g^{-1}g)x_2$, so $ex_1 = ex_2$. Condition 1 of the definition then yields $x_1 = x_2$, so σ_g is one to one. The two conditions of the definition show that for $x \in X$, we have $\sigma_g(g^{-1}x) = g(g^{-1})x = (gg^{-1})x = ex = x$, so σ_g maps X onto X. Thus σ_g is indeed a permutation.

To show that $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism, we must show that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. We show the equality of these two permutations in S_X by showing they both carry an $x \in X$ into the same element. Using the two conditions in Definition 16.1 and the rule for function composition, we obtain

$$\phi(g_1g_2)(x) = \sigma_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = g_1\sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x))$$
$$= (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\sigma_{g_1}\sigma_{g_2})(x) = (\phi(g_1)\phi(g_2))(x).$$

Thus ϕ is a homomorphism. The stated property of ϕ follows at once since by our definitions, we have $\phi(g)(x) = \sigma_g(x) = gx$. ◆

Example

Every group G is itself a G-set, where the action on $g_2 \in G$ by $g_1 \in G$ is given by left multiplication. That is, $*(g_1, g_2) = g_1g_2$. If H is a subgroup of G, we can also regard G as an H-set, where $*(h, g) = hg$. ▲

Example

Let H be a subgroup of G. Then G is an H-set under conjugation where $*(h, g) = hgh^{-1}$ for $g \in G$ and $h \in H$. Condition 1 is obvious, and for Condition 2 note that

$$*(h_1h_2, g) = (h_1h_2)g(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1} = *(h_1, *(h_2, g)).$$

We always write this action of H on G by conjugation as hgh^{-1}. The abbreviation hg described before the definition would cause terrible confusion with the group operation of G. ▲

Example

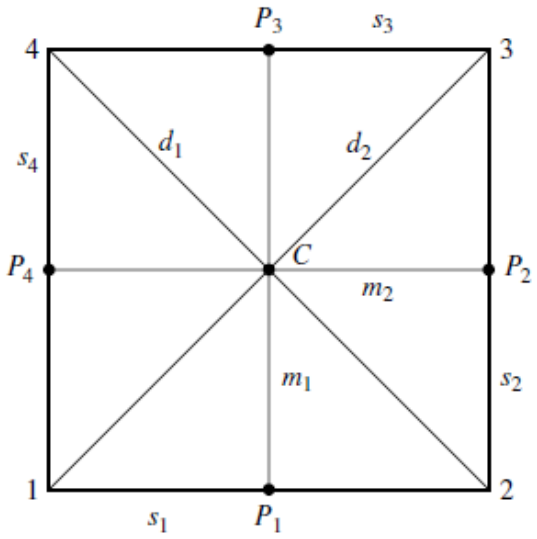
For students who have studied vector spaces with real (or complex) scalars, we mention that the axioms $(rs)\mathbf{v} = r(s\mathbf{v})$ and $1\mathbf{v} = \mathbf{v}$ for scalars r and s and a vector $\mathbf{v}$ show that the set of vectors is an $\mathbb{R}^*$-set (or a $\mathbb{C}^*$-set) for the multiplicative group of nonzero scalars. ▲

Example

Let H be a subgroup of G, and let L_H be the set of all left cosets of H. Then L_H is a G-set, where the action of $g \in G$ on the left coset xH is given by $g(xH) = (gx)H$. Observe that this action is well defined: if $yH = xH$, then $y = xh$ for some $h \in H$, and $g(yH) = (gy)H = (gxh)H = (gx)(hH) = (gx)H = g(xH)$. A series of exercises shows that every G-set is isomorphic to one that may be formed using these left coset G-sets as building blocks. (See Exercises 14 through 17.) ▲

Example

Let G be the group $D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$ of symmetries of the square, described in Example 8.10. In Fig. 16.9 we show the square with vertices 1, 2, 3, 4 as in Fig. 8.11. We also label the sides s_1, s_2, s_3, s_4, the diagonals d_1 and d_2, vertical and horizontal axes m_1 and m_2, the center point C, and midpoints P_i of the sides s_i. Recall that ρ_i corresponds to rotating the square counterclockwise through $\pi i/2$ radians, μ_i



16.9 Figure

	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_0	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_1	2	3	4	1	s_2	s_3	s_4	s_1	m_2	m_1	d_2	d_1	C	P_2	P_3	P_4	P_1
ρ_2	3	4	1	2	s_3	s_4	s_1	s_2	m_1	m_2	d_1	d_2	C	P_3	P_4	P_1	P_2
ρ_3	4	1	2	3	s_4	s_1	s_2	s_3	m_2	m_1	d_2	d_1	C	P_4	P_1	P_2	P_3
μ_1	2	1	4	3	s_1	s_4	s_3	s_2	m_1	m_2	d_2	d_1	C	P_1	P_4	P_3	P_2
μ_2	4	3	2	1	s_3	s_2	s_1	s_4	m_1	m_2	d_2	d_1	C	P_3	P_2	P_1	P_4
δ_1	3	2	1	4	s_2	s_1	s_4	s_3	m_2	m_1	d_1	d_2	C	P_2	P_1	P_4	P_3
δ_2	1	4	3	2	s_4	s_3	s_2	s_1	m_2	m_1	d_1	d_2	C	P_4	P_3	P_2	P_1

corresponds to flipping on the axis m_i, and δ_i to flipping on the diagonal d_i. We let

$$X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}.$$

Then X can be regarded as a D_4-set in a natural way. Table 16.10 describes completely the action of D_4 on X and is given to provide geometric illustrations of ideas to be introduced. We should be sure that we understand how this table is formed before continuing. ▲

Isotropy Subgroups

Let X be a G-set. Let $x \in X$ and $g \in G$. It will be important to know when $gx = x$. We let

$$X_g = \{x \in X \mid gx = x\} \qquad \text{and} \qquad G_x = \{g \in G \mid gx = x\}.$$

Example

For the D_4-set X in Example 16.8, we have

$$X_{\rho_0} = X, \qquad X_{\rho_1} = \{C\}, \qquad X_{\mu_1} = \{s_1, s_3, m_1, m_2, C, P_1, P_3\}$$

Also, with $G = D_4$,

$$G_1 = \{\rho_0, \delta_2\}, \qquad G_{s_3} = \{\rho_0, \mu_1\}, \qquad G_{d_1} = \{\rho_0, \rho_2, \delta_1, \delta_2\}.$$

We leave the computation of the other X_σ and G_x to Exercises 1 and 2. ▲

Theorem

Let X be a G-set. Then G_x is a subgroup of G for each $x \in X$.

Proof

Let $x \in X$ and let $g_1, g_2 \in G_x$. Then $g_1x = x$ and $g_2x = x$. Consequently, $(g_1g_2)x = g_1(g_2x) = g_1x = x$, so $g_1g_2 \in G_x$, and G_x is closed under the induced operation of G. Of course $ex = x$, so $e \in G_x$. If $g \in G_x$, then $gx = x$, so $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$, and consequently $g^{-1} \in G_x$. Thus G_x is a subgroup of G. ◆

Definition

Let X be a G-set and let $x \in X$. The subgroup G_x is the **isotropy subgroup of** x. ■

Orbits

For the D_4-set X of Example 16.8 with action table in Table 16.10, the elements in the subset $\{1, 2, 3, 4\}$ are carried into elements of this same subset under action by D_4. Furthermore, each of the elements 1, 2, 3, and 4 is carried into all the other elements of the subset by the various elements of D_4. We proceed to show that every G-set X can be partitioned into subsets of this type.

Theorem

Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

Proof

For each $x \in X$, we have $ex = x$, so $x \sim x$ and $\sim$ is reflexive.

Suppose $x_1 \sim x_2$, so $gx_1 = x_2$ for some $g \in G$. Then $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1$, so $x_2 \sim x_1$, and $\sim$ is symmetric.

Finally, if $x_1 \sim x_2$ and $x_2 \sim x_3$, then $g_1x_1 = x_2$ and $g_2x_2 = x_3$ for some $g_1, g_2 \in G$. Then $(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$, so $x_1 \sim x_3$ and $\sim$ is transitive. ◆

Definition

Let X be a G-set. Each cell in the partition of the equivalence relation described in Theorem 16.14 is an **orbit in** X **under** G. If $x \in X$, the cell containing x is the **orbit of** x. We let this cell be Gx. ■

Theorem

Let X be a G-set and let $x \in X$. Then $|Gx| = (G : G_x)$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.

Proof

We define a one-to-one map ψ from Gx onto the collection of left cosets of G_x in G. Let $x_1 \in Gx$. Then there exists $g_1 \in G$ such that $g_1x = x_1$. We define $\psi(x_1)$ to be the left coset g_1G_x of G_x. We must show that this map ψ is well defined, independent of the choice of $g_1 \in G$ such that $g_1x = x_1$. Suppose also that $g_1'x = x_1$. Then, $g_1x = g_1'x$, so $g_1^{-1}(g_1x) = g_1^{-1}(g_1'x)$, from which we deduce $x = (g_1^{-1}g_1')x$. Therefore $g_1^{-1}g_1' \in G_x$, so $g_1' \in g_1G_x$, and $g_1G_x = g_1'G_x$. Thus the map ψ is well defined.

To show the map ψ is one to one, suppose $x_1, x_2 \in Gx$, and $\psi(x_1) = \psi(x_2)$. Then there exist $g_1, g_2 \in G$ such that $x_1 = g_1x$, $x_2 = g_2x$, and $g_2 \in g_1G_x$. Then $g_2 = g_1g$ for some $g \in G_x$, so $x_2 = g_2x = g_1(gx) = g_1x = x_1$. Thus ψ is one to one.

Finally, we show that each left coset of G_x in G is of the form $\psi(x_1)$ for some $x_1 \in Gx$. Let g_1G_x be a left coset. Then if $g_1x = x_1$, we have $g_1G_x = \psi(x_1)$. Thus ψ maps Gx one to one onto the collection of left cosets so $|Gx| = (G : G_x)$.

If $|G|$ is finite, then the equation $|G| = |G_x|(G : G_x)$ shows that $|Gx| = (G : G_x)$ is a divisor of $|G|$. ◆

Example

Let X be the D_4-set in Example 16.8, with action table given by Table 16.10. With $G = D_4$, we have $G1 = \{1, 2, 3, 4\}$ and $G_1 = \{\rho_0, \delta_2\}$. Since $|G| = 8$, we have $|G1| = (G : G_1) = 4$. ▲

GROUPS ACTING ON THEMSELVES BY CONJUGATION —THE CLASS EQUATION

Definition. Two elements a and b of G are said to be *conjugate in* G if there is some $g \in G$ such that $b = gag^{-1}$ (i.e., if and only if they are in the same orbit of G acting on itself by conjugation). The orbits of G acting on itself by conjugation are called the *conjugacy classes of* G.

Examples

(1) If G is an abelian group then the action of G on itself by conjugation is the trivial action: $g \cdot a = a$, for all $g, a \in G$, and for each $a \in G$ the conjugacy class of a is $\{a\}$.

(2) If $|G| > 1$ then, unlike the action by left multiplication, G does *not* act transitively on itself by conjugation because $\{1\}$ is always a conjugacy class (i.e., an orbit for this action). More generally, the one element subset $\{a\}$ is a conjugacy class if and only if $gag^{-1} = a$ for all $g \in G$ if and only if a is in the center of G.

(3) In S_3 one can compute directly that the conjugacy classes are $\{1\}$, $\{(1\ 2), (1\ 3), (2\ 3)\}$ and $\{(1\ 2\ 3), (1\ 3\ 2)\}$. We shall shortly develop techniques for computing conjugacy classes more easily, particularly in symmetric groups.

Definition. Two subsets S and T of G are said to be *conjugate in* G if there is some $g \in G$ such that $T = gSg^{-1}$ (i.e., if and only if they are in the same orbit of G acting on its subsets by conjugation).

Proposition 6. The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.

Proof: The second assertion of the proposition follows from the observation that $N_G(\{s\}) = C_G(s)$.

Theorem

(The Class Equation) Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Proof: As noted in Example 2 above the element $\{x\}$ is a conjugacy class of size 1 if and only if $x \in Z(G)$, since then $gxg^{-1} = x$ for all $g \in G$. Let $Z(G) = \{1, z_2, ..., z_m\}$, let $\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_r$ be the conjugacy classes of G not contained in the center, and let g_i be a representative of $\mathcal{K}_i$ for each i. Then the full set of conjugacy classes of G is given by

$$\{1\},\ \{z_2\},\ \ldots,\ \{z_m\},\ \mathcal{K}_1,\ \mathcal{K}_2,\ \ldots,\ \mathcal{K}_r.$$

Since these partition G we have

$$|G| = \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} |\mathcal{K}_i|$$

$$= |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|,$$

where $|\mathcal{K}_i|$ is given by Proposition 6. This proves the class equation.

Examples

(1) The class equation gives no information in an abelian group since conjugation is the trivial action and all conjugacy classes have size 1.

(2) In any group G we have $\langle g \rangle \leq C_G(g)$; this observation helps to minimize computations of conjugacy classes. For example, in the quaternion group Q_8 we see that $\langle i \rangle \leq C_{Q_8}(i) \leq Q_8$. Since $i \notin Z(Q_8)$ and $|Q_8 : \langle i \rangle| = 2$, we must have $C_{Q_8}(i) = \langle i \rangle$. Thus i has precisely 2 conjugates in Q_8, namely i and $-i = kik^{-1}$. The other conjugacy classes in Q_8 are determined similarly and are

$$\{1\},\quad \{-1\},\quad \{\pm i\},\quad \{\pm j\},\quad \{\pm k\}.$$

The first two classes form $Z(Q_8)$ and the class equation for this group is

$$|Q_8| = 2 + 2 + 2 + 2.$$

(3) In D_8 we may also use the fact that the three subgroups of index 2 are abelian to quickly see that if $x \notin Z(D_8)$, then $|C_{D_8}(x)| = 4$. The conjugacy classes of D_8 are

$$\{1\},\quad \{r^2\},\quad \{r, r^3\},\quad \{s, sr^2\},\quad \{sr, sr^3\}.$$

The first two classes form $Z(D_8)$ and the class equation for this group is

$$|D_8| = 2 + 2 + 2 + 2.$$

Theorem

If p is a prime and P is a group of prime power order p^α for some $\alpha \geq 1$, then P has a nontrivial center: $Z(P) \neq 1$.

Proof: By the class equation

$$|P| = |Z(P)| + \sum_{i=1}^{r} |P : C_P(g_i)|$$

where $g_1, \ldots, g_r$ are representatives of the distinct non-central conjugacy classes. By definition, $C_P(g_i) \neq P$ for $i = 1, 2, \ldots, r$ so p divides $|P : C_P(g_i)|$. Since p also divides $|P|$ it follows that p divides $|Z(P)|$, hence the center must be nontrivial.

Corollary

If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.

Proof: Since $Z(P) \neq 1$ by the theorem, it follows that $P/Z(P)$ is cyclic. By Exercise 36, Section 3.1, P is abelian. If P has an element of order p^2, then P is cyclic. Assume therefore that every nonidentity element of P has order p. Let x be any nonidentity element of P and let $y \in P - \langle x \rangle$. Since $|\langle x, y \rangle| > |\langle x \rangle| = p$, we must have that $P = \langle x, y \rangle$. Both x and y have order p so $\langle x \rangle \times \langle y \rangle = Z_p \times Z_p$. It now follows directly that the map $(x^a, y^b) \mapsto x^a y^b$ is an isomorphism from $\langle x \rangle \times \langle y \rangle$ onto P. This completes the proof.

Conjugacy in S_n

Proposition

Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1\, a_2\, \ldots\, a_{k_1})\,(b_1\, b_2\, \ldots\, b_{k_2}) \ldots .$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1)\, \tau(a_2)\, \ldots\, \tau(a_{k_1}))\,(\tau(b_1)\, \tau(b_2)\, \ldots\, \tau(b_{k_2})) \ldots ,$$

that is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

Proof: Observe that if $\sigma(i) = j$, then

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(j).$$

Thus, if the ordered pair i, j appears in the cycle decomposition of σ, then the ordered pair $\tau(i), \tau(j)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. This completes the proof.

Example

Let $\sigma = (1\,2)(3\,4\,5)(6\,7\,8\,9)$ and let $\tau = (1\,3\,5\,7)(2\,4\,6\,8)$. Then

$$\tau\sigma\tau^{-1} = (3\,4)(5\,6\,7)(8\,1\,2\,9).$$

Definition.

(1) If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$ with $n_1 \leq n_2 \leq \cdots \leq n_r$ (including its 1-cycles) then the integers $n_1, n_2, \ldots, n_r$ are called the *cycle type* of σ.

(2) If $n \in \mathbb{Z}^+$, a *partition* of n is any nondecreasing sequence of positive integers whose sum is n.

Proposition

Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.

Proof: By Proposition 10, conjugate permutations have the same cycle type. Conversely, suppose the permutations σ_1 and σ_2 have the same cycle type. Order the cycles in nondecreasing length, including 1-cycles (if several cycles of σ_1 and σ_2 have the same length then there are several ways of doing this). Ignoring parentheses, each cycle decomposition is a list in which all the integers from 1 to n appear exactly once. Define τ to be the function which maps the i^{th} integer in the list for σ_1 to the i^{th} integer in the list for σ_2. Thus τ is a permutation and since the parentheses which delineate the cycle decompositions appear at the same positions in each list, Proposition 10 ensures that $\tau\sigma_1\tau^{-1} = \sigma_2$, so that σ_1 and σ_2 are conjugate.

Since there is a bijection between the conjugacy classes of S_n and the permissible cycle types and each cycle type for a permutation in S_n is a partition of n, the second assertion of the proposition follows, completing the proof.

Examples

(1) Let $\sigma_1 = (1)(3\,5)(8\,9)(2\,4\,7\,6)$ and let $\sigma_2 = (3)(4\,7)(8\,1)(5\,2\,6\,9)$. Then define τ by $\tau(1) = 3, \tau(3) = 4, \tau(5) = 7, \tau(8) = 8$, etc. Then

$$\tau = (1\,3\,4\,2\,5\,7\,6\,9)(8)$$

and $\tau\sigma_1\tau^{-1} = \sigma_2$.

(2) If in the previous example we had reordered σ_2 as $\sigma_2 = (3)(8\,1)(4\,7)(5\,2\,6\,9)$ by interchanging the two cycles of length 2, then the corresponding τ described above is defined by $\tau(1) = 3, \tau(3) = 8, \tau(5) = 1, \tau(8) = 4$, etc., which gives the permutation

$$\tau = (1\,3\,8\,4\,2\,5)(6\,9\,7)$$

again with $\tau\sigma_1\tau^{-1} = \sigma_2$, which shows that there are many elements conjugating σ_1 into σ_2.

(3) If $n = 5$, the partitions of 5 and corresponding representatives of the conjugacy classes (with 1-cycles not written) are as given in the following table:

Partition of 5	Representative of Conjugacy Class
1, 1, 1, 1, 1	1
1, 1, 1, 2	(1 2)
1, 1, 3	(1 2 3)
1, 4	(1 2 3 4)
5	(1 2 3 4 5)
1, 2, 2	(1 2)(3 4)
2, 3	(1 2)(3 4 5)

Theorem A_5 is a simple group.

Proof: We first work out the conjugacy classes of A_5 and their orders. Proposition 11 does not apply directly since two elements of the same cycle type (which are conjugate in S_5) need *not* be conjugate in A_5. Exercises 19 to 22 analyze the relation of classes in S_n to classes in A_n in detail.

We have already seen that representatives of the cycle types of even permutations can be taken to be

$$1, \quad (1\,2\,3), \quad (1\,2\,3\,4\,5) \quad \text{and} \quad (1\,2)(3\,4).$$

The centralizers of 3-cycles and 5-cycles in S_5 were determined above, and checking which of these elements are contained in A_5 we see that

$$C_{A_5}((1\,2\,3)) = \langle (1\,2\,3) \rangle \quad \text{and} \quad C_{A_5}((1\,2\,3\,4\,5)) = \langle (1\,2\,3\,4\,5) \rangle.$$

These groups have orders 3 and 5 (index 20 and 12), respectively, so there are 20 distinct conjugates of (1 2 3) and 12 distinct conjugates of (1 2 3 4 5) in A_5. Since there are a total of twenty 3-cycles in S_5 (Exercise 16, Section 1.3) and all of these lie in A_5, we see that

all twenty 3-cycles are conjugate in A_5.

There are a total of twenty-four 5-cycles in A_5 but only 12 distinct conjugates of the 5-cycle (1 2 3 4 5). Thus some 5-cycle, σ, is *not* conjugate to (1 2 3 4 5) in A_5 (in fact, (1 3 5 2 4) is not conjugate in A_5 to (1 2 3 4 5) since the method of proof in Proposition 11 shows that any element of S_5 conjugating (1 2 3 4 5) into (1 3 5 2 4) must be an odd permutation). As above we see that σ also has 12 distinct conjugates in A_5, hence

the 5-cycles lie in two conjugacy classes in A_5, each of which has 12 elements.

Since the 3-cycles and 5-cycles account for all the nonidentity elements of odd order, the 15 remaining nonidentity elements of A_5 must have order 2 and therefore have cycle type (2,2). It is easy to see that (1 2)(3 4) commutes with (1 3)(2 4) but does not commute with any element of odd order in A_5. It follows that $|C_{A_5}((12)(34))| = 4$. Thus (1 2)(3 4) has 15 distinct conjugates in A_5, hence

all 15 elements of order 2 in A_5 are conjugate to (1 2)(3 4).

In summary, the conjugacy classes of A_5 have orders 1, 15, 20, 12 and 12.

Now, suppose H were a normal subgroup of A_5. Then as we observed above, H would be the union of conjugacy classes of A_5. Then the order of H would be both a divisor of 60 (the order of A_5) and be the sum of some collection of the integers {1, 12, 12, 15, 20} (the sizes of the conjugacy classes in A_5). A quick check shows the only possibilities are $|H| = 1$ or $|H| = 60$, so that A_5 has no proper, nontrivial normal subgroups.

Reg. No.....

17MMU403

Karpagam Academy of Higher Education
Coimbatore-21
Department of Mathematics
IV Semester- II Internal test
Group theory II

Date: 05.02.2019(FN) Time: 2 hours
Class: II B.Sc Mathematics Max Marks: 50

Answer ALL questions
PART - A ($20 \times 1 = 20$ marks)

1. Inner Automorphism Induced by a, $\phi_a(x) = - - -$
   a. xax^{-1} b. axa^{-1}
   c. both a and b d. neither a nor b

2. $|\text{Aut}(\mathbb{Z}_{10})| = - - -$
   a. 1 b. 2
   c. 3 d. 4

3. $\text{Aut}(\mathbb{Z}_{100})$ is isomorphic to
   a. $U(10)$ b. $U(5)$
   c. $U(100)$ d. $U(2)$

4. Suppose $\phi : G to \overline{G}$ is an isomorphism with G and $\overline{G}$ are group under + and $\cdot$, respectively. Then
   a. $\phi(a+b) = \phi(a) + \phi(b)$ b. $\phi(a \cdot b) = \phi(a) + \phi(b)$
   c. $\phi(a+b) = \phi(a) \cdot \phi(b)$ d. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

5. Any infinite cyclic group is isomorphic to $- - -$
   a. $\mathbb{R}$ b. $\mathbb{C}$
   c. $\mathbb{Z}$ d. $\mathbb{Q}$

6. Number of isomorphism from $\mathbb{Q}$, the group of rational numbers under addition, to $\mathbb{Q}^*$, the group of nonzero rational numbers under multiplication is $- - -$
   a. one to one b. 2 to one
   c. 3 to one d. 4 to one

7. Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then $|a| - - - \phi(a)$
   a. $<$ b. $>$
   c. $=$ d. $\neq$

8. The equation $x^4 = 1$ has $- - -$ solutions in $\mathbb{C}^*$
   a. 0 b. 1
   c. 4 d. 6

9. An $- - -$ from a group G onto itself is called an automorphism of G.
   a. homomorphism b. isomorphism
   c. one to one homomorphism d. all the above

10. The function ϕ from $\mathbb{C}$ to $\mathbb{C}$ given by $\phi(a+bi) = a-bi$ is ——- of the group of complex numbers under addition.
    a. an automorphism b. a homomorphism
    c. an isomorphism d. all the above

11. $U(8)$ is $- - -$ to $U(10)$.
    a. not isomorphic b. isomorphic
    c. both a and b d. neither a nor b

12. Let G be a group. Prove that the mapping $\phi(g) = - - -$ for all g in G is an automorphism if and only if G is Abelian
    a. g b. g^{-1}
    c. both a and b d. neither a nor b

13. $|\text{Aut}(\mathbb{Z})| = ---$
    a. 0 b. 1
    c. 2 d. 3

14. Which of the following is an element of $\text{Aut}(\mathbb{Z}_6)$?
    a. $\phi(x) = x$ b. $\phi(x) = -x$
    c. both a and b d. neither a nor b

15. The identity inner automorphism is a $---$ of a group G.
    a. normal subgroup b. subgroup
    c. both a and b d. neither a nor b

16. If G is an infinite cyclic group, then $\text{Aut}(G)$ is a $---$ group of order 2.
    a. cyclic b. abelian
    c. both a and b d. neither a nor b

17. An element $---$ in a group is a commutator of the group.
    a. aba^{-1} b. $aba^{-1}b^{-1}$
    c. both a and b d. neither a nor b

18. The equation $x^4 = 1$ has $---$ solutions in $\mathbb{R}^*$
    a. 0 b. 1
    c. 4 d. 6

19. If G is $---$, then $\overline{G}$ and have exactly the same number of elements of every order.

    a. infinite b. finite
    c. both a and b d. neither a nor b

20. The number of elements in the left regular representation of $U(12)$ is $---$

    a. 1 b. 2
    c. 3 d. 4

Part B-($3 \times 2 = 6$ marks)

21. Write any two properties of isomorphism

22. Define an automorphism

23. Find an isomorphism from the group of integers under addition to the group of even integers under addition

Part C-($3 \times 8 = 24$ marks)

24. a) State and prove Cayley's theorem

    OR

    b) Show that $U(8)$ is isomorphic to $U(12)$.

25. a) Suppose that $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{20}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$?

    OR

    b) Find $\mathbb{Z}_{10}$

26. a) Find $\mathbb{Z}$

    OR

    b) Let ϕ be an isomorphism from a group G to a group $\overline{G}$ and let a belong to G. Prove that $\phi(C(a)) = C(\phi(a))$.