1: Subgroups

The isomorphism and correspondence theorems for groups should be familiar to the reader. The first isomorphism theorem (that if $f : G \to H$ is a group morphism then $G/\operatorname{Ker} f \simeq \operatorname{Im} f$) is a fundamental result from which follow further isomorphisms : if $A \leq G$ (i.e. A is a subgroup of G), if $N \triangleleft G$ (i.e. N is a normal subgroup of G), and if $K \triangleleft G$ with $K \leq N$, then

$$A/(A \cap N) \simeq NA/N \qquad \text{and} \qquad G/N \simeq (G/K)/(N/K).$$

The correspondence theorem relates the subgroups of G/N to the subgroups of G that contain N.

Elements a, b of G are said to be conjugate if $a = g^{-1}bg$ for some $g \in G$. Conjugacy is an equivalence relation on G and the corresponding classes are called conjugacy classes. The subset of G consisting of those elements that belong to singleton conjugacy classes forms a normal subgroup $Z(G)$ called the centre of G. For $H \leq G$ the subset

$$\mathcal{N}_G(H) = \{g \in G \mid (\forall h \in H)\ g^{-1}hg \in H\}$$

is called the normaliser of H in G. It is the largest subgroup of G in which H is normal. The derived group of G is the subgroup G' generated by all the commutators $[a, b] = a^{-1}b^{-1}ab$ in G, and is the smallest normal subgroup of G with abelian quotient group.

Examples are most commonly constructed with groups of matrices (subgroups of the group $\mathrm{GL}(n, F)$ of invertible $n \times n$ matrices with entries in a field F), groups of permutations (subgroups of the symmetric groups S_n), groups given by generators and relations, and direct (cartesian) products of given groups.

An example of a presentation is

$$G = \langle\, a, b \mid a^2 = b^3 = 1,\ a^{-1}ba = b^{-1} \,\rangle.$$

Since $|\langle b\rangle| = 3$ and $\langle b\rangle \lhd G$ with $G/\langle b\rangle \simeq C_2$ (the cyclic group of order 2), we see that $|G| = 6$. The generators a and b can be taken to correspond to the permutations $(1\,2)$ and $(1\,2\,3)$ which generate S_3, or to the matrices

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

which generate $\mathrm{SL}(2, \mathbb{Z}_2)$, the group of 2×2 matrices of determinant 1 with entries in the field $\mathbb{Z}_2$. Thus we have that $G \simeq S_3 \simeq \mathrm{SL}(2, \mathbb{Z}_2)$.

1.1 Let G be a group, let H be a subgroup of G and let K be a subgroup of H. Prove that

$$|G : K| = |G : H|\,|H : K|.$$

Deduce that the intersection of a finite number of subgroups of finite index is a subgroup of finite index. Is the intersection of an infinite number of subgroups of finite index necessarily also of finite index?

1.2 Let G be a group and let H be a subgroup of G. Prove that the only left coset of H in G that is a subgroup of G is H itself. Prove that the assignment

$$\varphi : xH \mapsto Hx^{-1}$$

describes a mapping from the set of left cosets of H in G to the set of right cosets of H. Show also that φ is a bijection. Does the prescription

$$\psi : xH \mapsto Hx$$

describe a mapping from the set of left cosets of H to the set of right cosets of H? If so, is ψ a bijection?

1.3 Find a group G with subgroups H and K such that HK is not a subgroup.

1.4 Consider the subgroup $H = \langle(1\ 2)\rangle$ of S_3. Show how the left cosets of H partition S_3. Show also how the right cosets of H partition S_3. Deduce that H is not a normal subgroup of S_3.

1.5 Let G be a group and let H be a subgroup of G. If $g \in G$ is such that $|\langle g\rangle| = n$ and $g^m \in H$ where m and n are coprime, show that $g \in H$.

1.6 Let G be a group. Prove that

(i) If H is a subgroup of G then $HH = H$.

(ii) If X is a finite subset of G with $XX = X$ then X is a subgroup of G.

Show that (ii) fails for infinite subsets X.

1.7 Let G be a group and let H and K be subgroups of G. For a given $x \in G$ define the double coset HxK by

$$HxK = \{hxk \mid h \in H, k \in K\}.$$

If yK is a left coset of K, show that either $HxK \cap yK = \emptyset$ or $yK \subseteq HxK$. Hence show that for all $x, y \in G$ either $HxK \cap HyK = \emptyset$ or $HxK = HyK$.

1.8 Let n be a prime power and let C_n be a cyclic group of order n. If H and K are subgroups of C_n, prove that either H is a subgroup of K or K is a subgroup of H. Suppose, conversely, that C_n is a cyclic group of order n with the property that, for any two subgroups H and K of C_n, either H is a subgroup of K or K is a subgroup of H. Is n necessarily a prime power?

1.9 Let G be a group. Given a subgroup H of G, define

$$H_G = \bigcap_{g \in G} g^{-1}Hg.$$

Prove that H_G is a normal subgroup of G and that if K is a subgroup of H that is normal in G then K is a normal subgroup of H_G.

Now let $G = \mathrm{GL}(2, \mathbb{Q})$ and let H be the subgroup of non-singular diagonal matrices. Determine H_G. In this case, to what well-known group is H_G isomorphic?

1.10 Let H be the subset of $\mathrm{Mat}_{2\times 2}(\mathbb{C})$ that consists of the elements

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}.$$

Prove that H is a non-abelian group under matrix multiplication (called the *quaternion group*). Find all the elements of order 2 in H. Find also all the subgroups of H. Which of the subgroups are normal? Does H have a quotient group that is isomorphic to the cyclic group of order 4?

1.11 The *dihedral group* D_{2n} is the subgroup of $\mathrm{GL}(2,\mathbb{C})$ that is generated by the matrices

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}$$

where $\alpha = e^{2\pi i/n}$.

Prove that $|D_{2n}| = 2n$ and that D_{2n} contains a cyclic subgroup of index 2.

Let G be the subgroup of $\mathrm{GL}(2,\mathbb{Z}_n)$ given by

$$G = \left\{ \begin{bmatrix} \epsilon & k \\ 0 & 1 \end{bmatrix} \mid \epsilon = \pm 1, k \in \mathbb{Z}_n \right\}.$$

Prove that G is isomorphic to D_{2n}. Show also that, for every positive integer n, D_{2n} is a quotient group of the subgroup D_∞ of $\mathrm{GL}(2,\mathbb{Z})$ given by

$$D_\infty = \left\{ \begin{bmatrix} \epsilon & k \\ 0 & 1 \end{bmatrix} \mid \epsilon = \pm 1, k \in \mathbb{Z} \right\}.$$

1.12 Let $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+$ denote respectively the additive groups of rational, real, complex numbers; and let $\mathbb{Q}^\bullet, \mathbb{R}^\bullet, \mathbb{C}^\bullet$ be the corresponding multiplicative groups. If $U = \{z \in \mathbb{C} \mid |z| = 1\}$ and $\mathbb{Q}^\bullet_{>0}, \mathbb{R}^\bullet_{>0}$ are the multiplicative subgroups of positive rationals and reals, prove that

(i) $\mathbb{C}^+/\mathbb{R}^+ \simeq \mathbb{R}^+$;
(ii) $\mathbb{C}^\bullet/\mathbb{R}^\bullet_{>0} \simeq U$;
(iii) $\mathbb{C}^\bullet/U \simeq \mathbb{R}^\bullet_{>0} \simeq \mathbb{R}^\bullet/C_2$;
(iv) $\mathbb{R}^\bullet/\mathbb{R}^\bullet_{>0} \simeq C_2 \simeq \mathbb{Q}^\bullet/\mathbb{Q}^\bullet_{>0}$;
(v) $\mathbb{Q}^\bullet/C_2 \simeq \mathbb{Q}^\bullet_{>0}$.

1.13 Let p be a fixed prime. Denote by $\mathbb{Z}_{p^\infty}$ the p^nth roots of unity for all positive integers n. Then $\mathbb{Z}_{p^\infty}$ is a subgroup of the group of non-zero complex numbers under multiplication.

Prove that every proper subgroup of $\mathbb{Z}_{p^\infty}$ is a finite cyclic group; and that every non-trivial quotient group of $\mathbb{Z}_{p^\infty}$ is isomorphic to $\mathbb{Z}_{p^\infty}$.

Prove that $\mathbb{Z}_{p^\infty}$ and $\mathbb{Q}^+$ satisfy the property that every finite subset generates a cyclic group.

1.14 Show that if no element of a 2–group G has order 4 then G is abelian.

Show that the dihedral and quaternion groups of order 8 are the only non-abelian groups of order 8. Show further that these two groups are not isomorphic.

1.15 According to Lagrange's theorem, what are the possible orders of subgroups of S_4? For each kind of cycle structure in S_4, write down an element with that cycle structure, and determine the total number of such elements. State the order of the elements of each type.

What are the orders of the elements of S_4, and how many are there of each order? How many subgroups of order 2 does S_4 have, and how many of order 3? Find all the cyclic subgroups of S_4 that are of order 4. Find all the non-cyclic subgroups of order 4.

Find all the subgroups of order 6, and all of order 8. Find also a subgroup of order 12.

Find an abelian normal subgroup V of S_4. Is S_4/V isomorphic to some subgroup of S_4?

Does A_4 have a subgroup of order 6?

1.16 Consider the subgroup of S_8 that is generated by $\{a, b\}$ where

$$a = (1234)\,(5678) \quad \text{and} \quad b = (1537)\,(2846).$$

Determine the order of this subgroup and show that it is isomorphic to the quaternion group. Is it isomorphic to any of the subgroups of order 8 in S_4?

1.17 Suppose that p is a permutation which, when decomposed into a product of disjoint cycles, has all these cycles of the same length. Prove that p is a power of some cycle ϑ.

Prove conversely that if $\vartheta = (1\,2 \cdots m)$ then ϑ^s decomposes into a product of h.c.f.(m, s) disjoint cycles of length $m/\text{h.c.f.}(m, s)$.

1.18 Let $\mathrm{SL}(2, p)$ be the group of 2×2 matrices of determinant 1 with entries in the field $\mathbb{Z}_p$ (where p is a prime). Show that $\mathrm{SL}(2, p)$ contains $p^2(p-1)$ elements of the form

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where $a \neq 0$. Show also that $\mathrm{SL}(2, p)$ contains $p(p-1)$ elements of the form

$$\begin{bmatrix} 0 & b \\ c & d \end{bmatrix}.$$

Deduce that $|\mathrm{SL}(2, p)| = p(p-1)(p+1)$.

If Z denotes the centre of $\mathrm{SL}(2, p)$ define

$$\mathrm{PSL}(2, p) = \mathrm{SL}(2, p)/Z.$$

Show that $|\mathrm{PSL}(2,p)| = \frac{1}{2}p(p-1)(p+1)$ if $p \neq 2$.

More generally, consider the group $\mathrm{SL}(n,p)$ of $n \times n$ matrices of determinant 1 with entries in the field $\mathbb{Z}_p$. Using the fact that the rows of a non-singular matrix are linearly independent, prove that

$$|\mathrm{SL}(n,p)| = \frac{1}{p-1}\prod_{i=0}^{n-1}(p^n - p^i).$$

1.19 Let F be a field in which $1+1 \neq 0$ and consider the group $\mathrm{SL}(2,F)$ of 2×2 matrices of determinant 1 with entries in F. Prove that if $A \in \mathrm{SL}(2,F)$ then $A^2 = -I_2$ if and only if $\mathrm{tr}(A) = 0$ (where $\mathrm{tr}(A)$ is the *trace* of A, namely the sum of its diagonal elements).

Let $\mathrm{PSL}(2,F)$ be the group $\mathrm{SL}(2,F)/Z(\mathrm{SL}(2,F))$ and denote by $\overline{A}$ the image of $A \in \mathrm{SL}(2,F)$ under the natural morphism $\natural : \mathrm{SL}(2,F) \to \mathrm{PSL}(2,F)$. Show that $\overline{A}$ is of order 2 if and only if $\mathrm{tr}(A) = 0$.

1.20 Show that $C_2 \times C_2$ is a non-cyclic group of order 4. Prove that if G is a non-cyclic group of order 4 then $G \simeq C_2 \times C_2$.

1.21 If p, q are primes show that the number of proper non-trivial subgroups of $C_p \times C_q$ is greater than or equal to 2, and that equality holds if and only if $p \neq q$.

1.22 If G, H are simple groups show that $G \times H$ has exactly two proper non-trivial normal subgroups unless $|G| = |H|$ and is a prime.

1.23 Is the cartesian product of two periodic groups also periodic? Is the cartesian product of two torsion-free groups also torsion-free?

1.24 Let G be a group and let A, B be normal subgroups of G such that $G = AB$. If $A \cap B = N$ prove that

$$G/N \simeq A/N \times B/N.$$

Show that this result fails if $G = AB$ where the subgroup A is normal but the subgroup B is not.

1.25 Let $f : G \to H$ be a group morphism. Suppose that A is a normal subgroup of G and that the restriction of f to A is an isomorphism onto H. Prove that

$$G \simeq A \times \mathrm{Ker}\, f.$$

Is this result true without the condition that A be normal?

Deduce that (using the notation defined in question 1.12)

(i) $\mathbb{C}^+ \simeq \mathbb{R}^+ \times \mathbb{R}^+$;

(ii) $\mathbb{Q}^\bullet \simeq \mathbb{Q}^\bullet_{>0} \times C_2$;
(iii) $\mathbb{R}^\bullet \simeq \mathbb{R}^\bullet_{>0} \times C_2$;
(iv) $\mathbb{C}^\bullet \simeq \mathbb{R}^\bullet_{>0} \times U$.

1.26 Find all the subgroups of $C_2 \times C_2$. Draw the subgroup Hasse diagram.
Prove that if G is a group whose subgroup Hasse diagram is identical to that of $C_2 \times C_2$ then $G \simeq C_2 \times C_2$.

1.27 Find all the subgroups of $C_2 \times C_2 \times C_2$ and draw the subgroup Hasse diagram.

1.28 Consider the set of integers n with $1 \leq n \leq 21$ and n coprime to 21. Show that this set forms an abelian group under multiplication modulo 21, and that this group is isomorphic to $C_2 \times C_6$. Is this group cyclic?
Is the set

$$\{n \in \mathbb{Z} \mid 1 \leq n \leq 12,\ n \text{ coprime to } 12\}$$

a cyclic group under multiplication modulo 12?

1.29 Determine which of the following groups are decomposable into a cartesian product of two non-trivial subgroups :

$$S_4, \quad S_5, \quad A_4, \quad A_5, \quad \mathbb{R}^\bullet, \quad C_6, \quad C_8, \quad \mathbb{C}^+, \quad \mathbb{Z}_{p^\infty}.$$

1.30 Let G be an abelian group and let H be a subgroup of G. Suppose that, given $h \in H$ and $n \in \mathbb{N}$, the equation $x^n = h$ has a solution in G if and only if it has a solution in H. Show that given xH there exists $y \in xH$ with y of the same order in G as xH has in G/H. Deduce that if G/H is cyclic then there is a subgroup K of G with $G \simeq H \times K$.

1.31 Let G be an abelian group. If $x, y \in G$ have orders m, n respectively, show that xy has order at most mn. Show also that if $z \in G$ has order mn where m and n are coprime then $z = xy$ where $x, y \in G$ satisfy $x^m = y^n = 1$. Deduce that x and y have orders m, n respectively.
Extend this result to the case where z has order $m_1 m_2 \cdots m_k$ where $m_1, \ldots, m_k$ are pairwise coprime.
Hence prove that if G is a finite abelian group of order

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, \ldots, p_k$ are distinct primes then

$$G = H_1 \times H_2 \times \cdots \times H_k$$

where $H_i = \{x \in G \mid x^{p_i^{\alpha_i}} = 1\}$ for $i = 1, \ldots, k$. Show also that if r divides $|G|$ then G has a subgroup of order r.

1.32 Let H be a subgroup of a group G. Prove that the intersection of all the conjugates of H is a normal subgroup of G.

If $x \in G$ is it possible that

$$A = \{g^{-1}xg \mid g \in G\}$$

is a subgroup of G? Can A be a normal subgroup? Can A be a subgroup that is not normal?

1.33 Are all subgroups of order 2 conjugate in S_4? What about all subgroups of order 3?

Are the elements $(1\,2\,3)$ and $(2\,3\,4)$ conjugate in A_4?

1.34 Show that a subgroup H of a group G is normal if and only if it is a union of conjugacy classes.

Exhibit an element from each conjugacy class of S_4 and state how many elements there are in each class. Deduce that the only possible orders for non-trivial proper normal subgroups of S_4 are 4 and 12. Show also that normal subgroups of orders 4 and 12 do exist in S_4.

1.35 Exhibit an element from each conjugacy class of S_5. How many elements are there in each conjugacy class? What are the orders of the elements of S_5? Find all the non-trivial proper normal subgroups of S_5.

Find the conjugacy classes of A_5 and deduce that it has no proper non-trivial normal subgroups.

1.36 If G is a group and $a \in G$ prove that the number of elements in the conjugacy class of a is the index of $\mathcal{N}_G(a)$ in G. Deduce that in S_n the only elements that commute with a cycle of length n are the powers of that cycle.

Suppose that n is an odd integer, with $n \geq 3$. Prove that there are two conjugacy classes of cycles of length n in A_n. Show also that each of these classes contains $\frac{1}{2}(n-1)!$ elements.

Show that if n is an even integer with $n \geq 4$ then there are two conjugacy classes of cycles of length $n-1$ in S_n, and that each of these classes contains $\frac{1}{2}n\,(n-2)!$ elements.

1.37 If G is a group and $a \in G$ prove that the conjugacy class containing a and that containing a^{-1} have the same number of elements.

Suppose now that $|G|$ is even. Show that there is at least one $a \in G$ with $a \neq 1$ such that a is conjugate to a^{-1}.

1.38 Find the conjugacy classes of the dihedral group D_{2n} when n is odd. What are the classes when n is even?

1.39 Let G be a group and let H and K be conjugate subgroups of G. Prove that $\mathcal{N}_G(H)$ and $\mathcal{N}_G(K)$ are conjugate.

1.40 Let H be a normal subgroup of a group G with $|H| = 2$. Prove that $H \subseteq Z(G)$.

Is it necessarily true that $H \subseteq G'$?

Prove that if G contains exactly one element x of order 2 then $\langle x \rangle \subseteq Z(G)$.

1.41 Suppose that N is a normal subgroup of a group G with the property that $N \cap G' = 1$. Prove that $N \subseteq Z(G)$ and deduce that

$$Z(G/N) = Z(G)/N.$$

CAMBRIDGE

Cambridge University Press
978-0-521-27290-2 - Algebra Through Practice: A Collection of Problems in Algebra with Solutions, Groups
T. S. Blyth and E. F. Robertson
Excerpt
More information

2: Automorphisms and Sylow theory

An isomorphism $f : G \to G$ is called an automorphism on G. The automorphisms on a group G form, under composition of mappings, a group $\operatorname{Aut} G$. Conjugation by a fixed element g of G, namely the mapping $\varphi_g : G \to G$ described by $x \mapsto \varphi_g(x) = g^{-1}xg$, is an automorphism on G. The inner automorphism group $\operatorname{Inn} G = \{\varphi_g \mid g \in G\}$ is a normal subgroup of $\operatorname{Aut} G$, and the quotient group $\operatorname{Aut} G/\operatorname{Inn} G$ is called the outer automorphism group of G. For example, the cyclic group C_n (being abelian) has trivial inner automorphism group, and $\vartheta : C_n \to C_n$ given by $\vartheta(g) = g^{-1}$ is an (outer) automorphism of order 2. A subgroup H of a group G is normal if and only if $\vartheta(H) \subseteq H$ for every $\vartheta \in \operatorname{Inn} G$, and is called characteristic if $\vartheta(H) \subseteq H$ for every $\vartheta \in \operatorname{Aut} G$.

For finite groups, the converse of Lagrange's theorem is false. However, a partial converse is provided by the important theorems of Sylow. A group P is called a p–group if every element has order a power of p for a fixed prime p. In this case, if P is finite, $|P|$ is also a power of p. If G is a group with $|G| = p^n k$ where k is coprime to p then a subgroup of order p^n is called a Sylow p–subgroup. In this situation we have the following results, with which we assume the reader is familiar :

(a) G has a subgroup of order p^m for every $m \le n$;
(b) every p–subgroup of G is contained in a Sylow p–subgroup;
(c) any two Sylow p–subgroups are conjugate in G;
(d) the number of Sylow p–subgroups of G is congruent to 1 modulo p and divides $|G|$.

2.1 Let p be a prime. Use the class equation to show that every finite p–group has a non-trivial centre. Deduce that all groups of order p^2 are abelian.

