Problems on groups

Peter J. Cameron

Associated with *Introduction to Algebra*, OUP 2008

1. The purpose of this exercise is to construct a family of groups known as *free groups*.

Let X be a set, and let $\overline{X} = \{\bar{x} : x \in X\}$ be a set disjoint from X but in one-to-one correspondence with it. A *word* is defined to be an ordered string of symbols from the "alphabet" $X \cup \overline{X}$. A word is *reduced* if it does not contain any consecutive pair of symbols of the form $x\bar{x}$ or $\bar{x}x$, for $x \in X$.

Consider the following process of *cancellation*, which can be applied to any word w. Select any consecutive pair of symbols $\bar{x}x$ or $x\bar{x}$ in w (if such exists) and remove it. Repeat until the word is reduced.

(a)** Given a word, there may be several different ways to apply the cancellation process to it. Show that the same result is obtained no matter how the cancellation is performed.

Hint: One rather indirect way to prove this is as follows. Construct an (infinite) tree $T(X)$ whose edges are directed and labelled with elements of X such that, for any vertex v and any $x \in X$, there is a unique edge with label x leaving v and a unique edge with label x entering v. Choose a fixed starting vertex s in the tree. Then any word describes a path starting from s: symbol x means "leave the current vertex on the outgoing edge labelled x", while $\bar{x}$ means "leave the current vertex along the incoming edge labelled x". Show that the finishing vertex of the path is not changed by cancellation.

(b) Let $F(X)$ denote the set of all reduced words in the alphabet $X \cup \overline{X}$, including the "empty word". Define an operation on $F(X)$ as follows: $w_1 \circ w_2$ is obtained by concatenating the words w_1 and w_2 and then applying cancellation to the result. Prove that $F(X)$ is a group, in which the empty string is the identity and the inverse of x is $\bar{x}$.

(c) Let G be any group and $\theta : X \to G$ an arbitrary function. Show that there is a unique homomorphism $\theta^* : F(X) \to G$ whose restriction to X is θ.

The group $F(X)$ is called the *free group generated by X*.

2. Let G be a group. For subgroups H, K of G, let $[H, K]$ denote the subgroup generated by all commutators $[h, k] = h^{-1}k^{-1}hk$, for $h \in H$ and $k \in K$.

Define the *lower central series*

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots$$

by the rule that $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G]$.

Define the *upper central series*

$$\{1\} = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

by the rule that $Z_0(G) = \{1\}$ and $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$, where $Z(H)$ is the centre of the group H.

(a) Let H and K be normal subgroups of G, with $H \leq K$. Prove that $[K, G] \leq H$ if and only if $K/H \leq Z(G/H)$.

(b) Prove that $G^{(m)} = \{1\}$ if and only if $Z_m(G) = G$.

Remark A group (finite or infinite) satisfying this condition is said to be *nilpotent*: its *nilpotency class* is the smallest value of m for which these equivalent conditions hold.

(c) Prove that a finite group G is nilpotent according to this definition if and only if it satisfies the equivalent conditions of Exercise 7.8 in the book: viz.,

- every proper subgroup of G is properly contained in its normaliser;
- G is the direct product of its Sylow subgroups.

3. Define the *subgroup length* $\ell(G)$ of a finite group G to be the maximum number r for which there is a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_r = \{1\}$$

of G.

(a) Show that, if N is a normal subgroup of G, then $\ell(G) = \ell(N) + \ell(G/N)$.

(b) Deduce that $\ell(G)$ is the sum of the subgroup lengths of the composition factors of G, counted with multiplicities.

(c) Deduce that, if G is soluble, then $\ell(G)$ is equal to the number of prime divisors of $|G|$, counted with multiplicities.

(d) Find a group G which satisfies the conclusion of (c) but is not soluble.

4. Let A be a finite abelian group. The *dual* of A is the set A^* of all homomorphisms from A to the multiplicative group of non-zero complex numbers, with operation defined pointwise (that is, the product of homomorphisms α and β is given by

$$z(\alpha\beta) = (z\alpha)(z\beta).$$

(a) Show that, if A is cyclic of order n generated by a, then A^* is cyclic of order n generated by α, where $a\alpha = \mathrm{e}^{2\pi\mathrm{i},n}$.

(b) Show that $(A \times B)^* \cong A^* \times B^*$.

(c) Deduce that $A^* \cong A$ for any finite abellian group A.

(d) Let B be a subgroup of A, and define its *annihilator* to be the subgroup $B^\dagger$ of A^* defined by

$$B^\dagger = \{\phi \in A^* : b\phi = 1 \text{ for all } b \in B\}.$$

Show that $B^\dagger$ is a subgroup of A^* and $A^*/B^\dagger \cong B$.

(e) Show that, if ϕ is a non-identity element of A^*, then

$$\sum_{a\in A} a\phi = 0.$$

(f) Let M be the matrix whose rows are indexed by elements of A and columns by elements of A^*, wiith (a,ϕ) entry $a\phi$. Prove that

$$M^\top M = nI,$$

where $n = |A|$, and deduce that $|\det(M)| = n^{n/2}$.

5. Show that the automorphism group of $C_2 \times C_2 \times C_2$ is a simple group of order 168.

6. Let a,b,c,d be elements of a *finite* group which satisfy

$$b^{-1}ab = a^2, c^{-1}bc = b^2, d^{-1}cd = c^2, a^{-1}da = d^2.$$

Prove that $a = b = c = d = 1$. [*Hint:* Let p be the smallest prime divisor of the order of a, assumed greater than 1, Show that the order of b is divisible by a prime divisor of $p-1$.]

7. Let G be the group of 2×2 matrices over $\mathbb{Z}_p$ with determinant 1, where p is an odd prime.

(a) Show that G contains a unique element z of order 2.

(b) For $p = 3$ and $p = 5$, show that $G/\langle z \rangle$ is isomorphic to the alternating group A_4 or A_5 respectively.

(c)* Identify the group $G/\langle z \rangle$ for $p = 7$ with the simple group defined in Question 5.

8. Let G be a finite group. Let $g_1, \ldots, g_r$ be representatives of the conjugacy classes of G (with $g_1 = 1$, and let $m_i = |C_G(g_i)|$ for $i = 1, \ldots, r$.
medskip
(a) Show that
$$\sum_{i=1}^{r} \frac{1}{m_i} = 1,$$
with $m_1 = |G|$.

(b) Show that the displayed equation in (a) has only finitely many solutions in non-negative integers $m_1, \ldots, m_r$ for fixed r.

(c) Deduce that there are only finitely many finite groups with a given number of conjugacy classes.

(d) Find all finite groups with three or four conjugacy classes.

9. Let G be a group, and $g \in G$. The *inner automorphism* ι_g induced by g is the map $x \mapsto g^{-1}xg$ of G.

(a) Prove that ι_g is an automorphism of G.

(b) Prove that the map $\theta : G \to \mathrm{Aut}(G)$ given by $g\theta = \iota_g$ is a homomorphism, whose image is the set $\mathrm{Inn}(G)$ of all inner automorphisms of G and whose kernel is $Z(G)$, the centre of G. Deduce that $\mathrm{Inn}(G) \cong G/Z(G)$.

(c) Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. (The factor group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G.)

10. Prove that every group (finite or infinite) except the trivial group and the cyclic group of order 2 has a non-identity automorphism. [You will need to use the Axiom of Choice to answer this question!]

11. Let P_n denote the Sylow 2-subgroup of the symmetric group of degree 2^n.

(a) Show that P_{n+1} has a subgroup of index 2 isomorphic to $P_n \times P_n$.

(b) Let p_n be the proportion of fixed-point-free elements in P_n, Prove that $p_0 = 0$ and

$$p_{n+1} = \tfrac{1}{2}(1 + p_n^2)$$

for $n \geq 0$.

(c) Deduce that $\lim_{n\to\infty} p_n = 1$.

(d) Prove that, in any subgroup P of S_{2^n} which is a transitive 2-group, there is an intransitive subgroup of index 2, and deduce that more than half of the elements of P are fixed-point-free.

(e)** For every $n > 0$, construct a subgroup of S_{2^n} which is a transitive 2-group in which fewer than two-thirds of the elements are fixed-point-free.

12. A finite group G is said to be *supersoluble* if it has a sequence

$$G = G_0 > G_1 > \cdots > G_r = \{1\}$$

of *normal* subgroups with the property that G_i/G_{i+1} is cyclic for $i = 0, \ldots, r-1$. [Compare this with the property of being soluble: what is the difference?]

(a) Show that the symmetric group A_4 is soluble but not supersoluble.

(b)* Prove that, if G is supersoluble, then the derived group G' is nilpotent.

13. This exercise asks you to prove the following strengthening of Jordan's theorem:

> *Let G be a finite group acting transitively on a set Ω of n elements, where $n > 1$. Then the proportion of fixed-point-free elements in G is at least $1/n$.*

(a) Let $\mathrm{fix}(g)$ be the number of fixed points of g in Ω. Show that $\mathrm{fix}(g)^2$ is the number of fixed points of g in its coordinatewise action on the Cartesian product $\Omega \times \Omega$, and deduce that

$$\frac{1}{|G|} \sum_{g \in G} \mathrm{fix}(g)^2 \geq 2.$$

(b) By evaluating
$$\sum_{g\in G} (\mathrm{fix}(g)-1)(\mathrm{fix}(g)-n),$$
noting that only fixed-point-free elements give a positive contribution to the sum, prove the theorem stated above.

(c)* What can be concluded about a group which attains the bound? Give an example of such a group.

14. The *Frattini subgroup* $\Phi(G)$ of a group G is defined to be the intersection of all the maximal proper subgroups of G.

(a) Prove that $\Phi(G)$ is a normal subgroup of G.

(b) An element $g \in G$ is said to be a *non-generator* of G if, whenever G is generated by $A \cup \{g\}$, for some subset A of G, it actually holds that G is generated by A. Prove that an element $g \in G$ belongs to $\Phi(G)$ if and only if it is a non-generator.

(c) Let G be a finite group. Recall the *Frattini argument* (Exercise 7.10 on p.255 in the book): If H is a normal subgroup of G, and P a Sylow p-subgroup of H, then $G = HN_G(P)$. Deduce that the Sylow subgroups of $\Phi(G)$ are normal in G, and from this, deduce that $\Phi(G)$ is nilpotent.

(d) Now let G be a finite p-group. Prove that $\Phi(G) = 1$ if and only if G is elementary abelian (a direct product of cyclic groups of order p). Hence show that, in general, $G/\Phi(G)$ is elementary abelian, and that if the cosets $\Phi(G)g_1, \ldots, \Phi(G)g_r$ form a basis for $G/\Phi(G)$ (as vector space over $\mathbb{Z}_p$, then $g_1, \ldots, g_r$ generate G.

15. For any group G, define two parameters as follows:

- $d(G)$ is the minimum number of elements in a generating set for G;
- $\mu(G)$ is the maximum number of elements in a minimal generating set for G (where a generating set S is *minimal* if no proper subset of S is a generating set).

(a) Let G be the symmetric group S_n, where $n \geq 3$. Show that $d(G) = 2$ and $\mu(G) \geq n-1$. [*Remark:* In fact it was proved by Julius Whiston that $\mu(G) = n-1$, but the proof is much more complicated.]

(b) Prove that $\mu(G) \leq \ell(G)$, where $\ell(G)$ is the subgroup length of G (see Problem 3 above).

(c) Prove that, if G is a p-group, then $\mu(G) = d(G)$. Is the converse true?

16. (a)** Let A and B be nilpotent normal subgroups of a group G. Prove that AB is a nilpotent normal subgroup.

(b) Deduce that G contains a unique maximal nilpotent normal subgroup. (This subgroup is called the *Fitting subgroup* of G, denoted by $F(G)$.)

(c) Show that, if G is a finite group, then $\Phi(G) \leq F(G)$. Give an example of a group where these two subgroups are not equal.

17. A group G is said to be *finitely generated* if it is generated by a finite set of elements.

(a) Prove that, if G is finitely generated and H is finite, then there are only finitely many homomorphisms from G to H.

(b) Prove that, if G is finitely generated, then the number of subgroups of G of index n is finite, for any natural number n. [*Hint:* A subgroup of index n gives rise to a homomorphism from G to S_n.]

(c) Prove that, if G is generated by d elements, then G has at most $n(n!)^d$ subgroups of index n for any n.

(d) Find a group which is not finitely generated but has only finitely many subgroups of index n for any n.

18. (a) Show that, if H is a proper subgroup of the finite group G, then there is a conjugacy class in G which is disjoint from H.

(b) Show that this is not the case for infinite groups. (You may wish to consider the group $G = \mathrm{GL}(n,F)$, where F is an algebraically closed field, with H the group of upper triangular matrices.)

19. Let G be a permutation group on the set $\{1,\ldots,n\}$ (a subgroup of the symmetric group S_n). Let $p_i(G)$ be the proportion of elements of G which have precisely i fixed points, and let $F_j(G)$ be the number of orbits of G on ordered j-tuples of distinct elements of $\{1,\ldots,n\}$. Define polynomials P and Q of degree n by

- $P(x) = \sum_{i=0}^{n} p_i(G)x^i$,
- $Q(x) = \sum_{j=0}^{n} F_j(G)x^j/j!$.

(a)* By using the Orbit-Counting Lemma, show that $Q(x) = P(x+1)$.

(b) Deduce that the proportion of fixed-point-free elements in G is equal to $Q(-1)$.

(c) In the case that $G = S_n$, show that

$$Q(x) = \sum_{j=0}^{n} \frac{x^j}{j!},$$

the Taylor series for e^x truncated to degree n. Deduce that the proportion of fixed-point-free elements in S_n is approximately $1/\mathrm{e}$.

20. How many groups of order 12 are there (up to isomorphism)?

21. A *Steiner triple system* is a pair $(X, \mathscr{B})$, where X is a finite set and $\mathscr{B}$ a collection of 3-element subsets of X (called *triples*), such that any two distinct points of X are contained in a unique triple. Its *order* is the cardinality of X.

Let $(X, \mathscr{B})$ be a Steiner triple system. Take a new element $0 \notin X$, and define a binary operation $+$ on $X \cup \{0\}$ by the rules

- $0 + 0 = 0$;
- $0 + x = x + 0 = x$, $x + x = 0$ for all $x \in X$;
- $x + y = z$ if $\{x, y, z\} \in \mathscr{B}$.

(a) Prove that $(X \cup \{0\}, +)$ satisfies the closure, identity, inverse, and commutative laws.

(b) Prove that $(X \cup \{0\}, +)$ satisfies the associative law if and only if $(X, \mathscr{B})$ has the following property:

> for all distinct $u, \ldots, z \in X$, if $\{u, v, w\}$, $\{u, x, y\}$, $\{v, x, z\}$ are triples, then $\{w, y, z\}$ is a triple.

(c) Deduce that a Steiner triple system satisfying the displayed property in part (b) has order $2^n - 1$ for some natural number n.

(d) Construct such a system for every $n \in \mathbb{N}$.

22. Let G be a group generated by elements $x_1,\ldots,x_r$. Let H be a subgroup of G of index n, and let $g_1,\ldots,g_n$ be right coset representatives for H in G, with $g_1 = 1$. For $i = 1,\ldots,n$ and $j = 1,\ldots,r$, put

$$y_{ij} = g_i x_j g_k^{-1} \text{ where } Hg_i x_j = Hg_k.$$

(a) Show that, if $Hg_i x_j = Hg_k$, then $Hg_k x_j^{-1} = Hg_i$. Deduce that under this hypothesis $y_{ij}^{-1} = g_k x_j^{-1} g_i^{-1}$.

(b) Show that the elements y_{ij}, for $i = 1,\ldots,n$ and $j = 1,\ldots,r$, all belong to H.

(c) Show that the elements in (b) generate H.

(d) Deduce that a subgroup of finite index in a finitely generated group is finitely generated.

(e) By choosing the coset representatives with more care, show that H can be generated by $nr-n+1$ elements.

23. Let $X = \{1,2,3,4,5,6\}$. Following Sylvester, we define a *duad* to be a 2-element subset of X; a *syntheme* to be a partition of X into three duads; and a *synthematic total* (or *total*, for short) to be a partition of the set of duads into synthemes. Let Y be the set of totals.

(a) Show that there are 15 duads; there are 15 synthemes, each containing three duads; there are 6 totals, each containing five synthemes. Show that the symmetric group S_6 acts in a natural way on the sets of duads, synthemes and totals.

(b) Write $Y = \{y_1,\ldots,y_6\}$. Given a permutation $g \in S_6$, let g^* be the permutation in S_6 given by $(y_i)g = y_{ig^*}$ for $i = 1,\ldots,6$, where $(y_i)g$ is the image of y_i under the induced action defined in (a). Prove that the map $\sigma : g \mapsto g^*$ is an automorphism of S_6.

(c) Show that the stabiliser of a total fixes no point in X. Deduce that σ is an outer automorphism of S_6 (see Problem 9).

(d) Show that a syntheme lies in exactly two totals (i.e. a "duad of totals"); a duad lies in three synthemes belonging to disjoint pairs of totals (i.e. a "syntheme of totals"; and that, given an element x of X, the five sets of three synthemes corresponding to the duads containing x cover each pair of totals once (i.e. a "total of totals").

(e) Deduce that σ^2 is an inner automorphism of S_6.

(f)* Prove that the outer automorphism group of S_6 has order 2.

(g)** Prove that, for $n \neq 6$, the outer automorphism group of S_6 is trivial (that is, every automorphism is inner).