GROUP THEORY

J.S. Milne

August 29, 2003*

Abstract

These notes, which are a revision of those handed out during a course taught to first-year graduate students, give a concise introduction to the theory of groups.

Please send comments and corrections to me at math@jmilne.org.

v2.01 (August 21, 1996). First version on the web; 57 pages.

v2.11. (August 29, 2003). Fixed many minor errors; numbering unchanged; 85 pages.

Contents

Notations.

We use the standard (Bourbaki) notations:

$$\begin{aligned}
\mathbb{N} &= \{0, 1, 2, \ldots\},\\
\mathbb{Z} &= \text{ring of integers},\\
\mathbb{R} &= \text{field of real numbers},\\
\mathbb{C} &= \text{field of complex numbers},\\
\mathbb{F}_p &= \mathbb{Z}/p\mathbb{Z} = \text{field with } p \text{ elements, } p \text{ a prime number.}
\end{aligned}$$

Given an equivalence relation, $[*]$ denotes the equivalence class containing $*$.

Throughout the notes, p is a prime number, i.e., $p = 2, 3, 5, 7, 11, \ldots$.

Let I and A be sets. A family of elements of A indexed by I, denoted $(a_i)_{i\in I}$, is a function $i \mapsto a_i \colon I \to A$.

Rings are required to have an identity element 1, and homomorphisms of rings are required to take 1 to 1.

$X \subset Y$ X is a subset of Y (not necessarily proper).
$X \overset{\text{df}}{=} Y$ X is defined to be Y, or equals Y by definition.
$X \approx Y$ X is isomorphic to Y.
$X \cong Y$ X and Y are canonically isomorphic (or there is a given or unique isomorphism).

References.

Artin, M., Algebra, Prentice Hall, 1991.
Dummit, D., and Foote, R.M., Abstract Algebra, Prentice Hall, 1991.
Rotman, J.J., An Introduction to the Theory of Groups, Third Edition, Springer, 1995.

Also,

FT: Milne, J.S., Fields and Galois Theory, available at www.jmilne.org/math/

Prerequisites

An undergraduate "abstract algebra" course.

Acknowledgements

I thank the following for providing corrections and comments for earlier versions of these notes: Demetres Christofides, Martin Klazar, Mark Meckes, Robert Thompson.

1 Basic Definitions

Definitions

DEFINITION 1.1. A ***group*** is a nonempty set G together with a law of composition $(a,b)\mapsto a*b : G\times G\to G$ satisfying the following axioms:

(a) (associative law) for all $a,b,c\in G$,

$$(a*b)*c=a*(b*c);$$

(b) (existence of an identity element) there exists an element $e\in G$ such that

$$a*e=a=e*a$$

for all $a\in G$;

(c) (existence of inverses) for each $a\in G$, there exists an $a'\in G$ such that

$$a*a'=e=a'*a.$$

When (a) and (b) hold, but not necessarily (c), we call $(G,*)$ a ***semigroup***.[1]

We usually abbreviate $(G,*)$ to G, and we usually write $a*b$ and e respectively as ab and 1, or as $a+b$ and 0.

Two groups G and G' are ***isomorphic*** if there exists a one-to-one correspondence $a\leftrightarrow a'$, $G\leftrightarrow G'$, such that $(ab)'=a'b'$ for all $a,b\in G$.

REMARK 1.2. In the following, $a,b,\ldots$ are elements of a group G.

(a) If $aa=a$, then $a=e$ (multiply by a' and apply the axioms). Thus e is the unique element of G with the property that $ee=e$.

(b) If $ba=e$ and $ac=e$, then

$$b=be=b(ac)=(ba)c=ec=c.$$

Hence the element a' in (1.1c) is uniquely determined by a. We call it the ***inverse*** of a, and denote it a^{-1} (or the ***negative*** of a, and denote it $-a$).

(c) Note that (1.1a) implies that the product of any ordered triple a_1, a_2, a_3 of elements of G is unambiguously defined: whether we form a_1a_2 first and then $(a_1a_2)a_3$, or a_2a_3 first and then $a_1(a_2a_3)$, the result is the same. In fact, (1.1a) implies that the product of any ordered n-tuple a_1, a_2,..., a_n of elements of G is unambiguously defined. We prove this by induction on n. In one multiplication, we might end up with

$$(a_1\cdots a_i)(a_{i+1}\cdots a_n) \tag{1}$$

as the final product, whereas in another we might end up with

$$(a_1\cdots a_j)(a_{j+1}\cdots a_n). \tag{2}$$

[1] Some authors use the following definitions: when (a) holds, but not necessarily (b) or (c), $(G,*)$ is ***semigroup***; when (a) and (b) hold, but not necessarily (c), $(G,*)$ is ***monoid***.

Note that the expression within each pair of parentheses is well defined because of the induction hypotheses. Thus, if $i = j$, (1) equals (2). If $i \neq j$, we may suppose $i < j$. Then

$$(a_1 \cdots a_i)(a_{i+1} \cdots a_n) = (a_1 \cdots a_i)\left((a_{i+1} \cdots a_j)(a_{j+1} \cdots a_n)\right)$$
$$(a_1 \cdots a_j)(a_{j+1} \cdots a_n) = \left((a_1 \cdots a_i)(a_{i+1} \cdots a_j)\right)(a_{j+1} \cdots a_n)$$

and the expressions on the right are equal because of (1.1a).

(d) The inverse of $a_1 a_2 \cdots a_n$ is $a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$, i.e., the inverse of a product is the product of the inverses in the reverse order.

(e) Axiom (1.1c) implies that the cancellation laws hold in groups:

$$ab = ac \Rightarrow b = c, \qquad ba = ca \Rightarrow b = c$$

(multiply on left or right by a^{-1}). Conversely, if G *is finite*, then the cancellation laws imply Axiom (c): the map $x \mapsto ax\colon G \to G$ is injective, and hence (by counting) bijective; in particular, 1 is in the image, and so a has a right inverse; similarly, it has a left inverse, and the argument in (b) above shows that the two inverses must then be equal.

The ***order*** of a group is the number of elements in the group. A finite group whose order is a power of a prime p is called a p***-group***.

For an element a of a group G, define

$$a^n = \begin{cases} aa \cdots a & n > 0 \quad (n \text{ copies of } a) \\ 1 & n = 0 \\ a^{-1}a^{-1} \cdots a^{-1} & n < 0 \quad (|n| \text{ copies of } a^{-1}) \end{cases}$$

The usual rules hold:

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}. \tag{3}$$

It follows from (3) that the set

$$\{n \in \mathbb{Z} \mid a^n = 1\}$$

is an ideal in $\mathbb{Z}$. Therefore,[2] this set equals (m) for some $m \geq 0$. When $m = 0$, a is said to have ***infinite order***, and $a^n \neq 1$ unless $n = 0$. Otherwise, a is said to have ***finite order*** m**,** and m is the smallest integer > 0 such that $a^m = 1$; in this case, $a^n = 1 \iff m|n$; moreover $a^{-1} = a^{m-1}$.

EXAMPLE 1.3. (a) For $m \geq 1$, let $C_m = \mathbb{Z}/m\mathbb{Z}$, and for $m = \infty$, let $C_m = \mathbb{Z}$ (regarded as groups under addition).

(b) Probably the most important groups are matrix groups. For example, let R be a commutative ring. If A is an $n \times n$ matrix with coefficients in R whose determinant is a unit[3] in R, then the cofactor formula for the inverse of a matrix (Dummit and Foote 1991, 11.4, Theorem 27) shows that A^{-1} also has coefficients[4] in R. In more detail, if A' is the transpose of the matrix of cofactors of A, then $A \cdot A' = \det A \cdot I$, and so $(\det A)^{-1} A'$ is

[2] We are using that $\mathbb{Z}$ is a principal ideal domain.

[3] An element of a ring is ***unit*** if it has an inverse.

[4] Alternatively, the Cayley-Hamilton theorem provides us with an equation

$$A^n + a_{n-1}A^{n-1} + \cdots \pm (\det A) \cdot I = 0.$$

the inverse of A. It follows that the set $\mathrm{GL}_n(R)$ of such matrices is a group. For example $\mathrm{GL}_n(\mathbb{Z})$ is the group of all $n \times n$ matrices with integer coefficients and determinant ± 1. When R is finite, for example, a finite field, then $\mathrm{GL}_n(R)$ is a finite group. Note that $\mathrm{GL}_1(R)$ is just the group of units in R — we denote it $R^\times$.

(c) If G and H are groups, then we can construct a new group $G \times H$, called the ***(direct) product*** of G and H. As a set, it is the cartesian product of G and H, and multiplication is defined by:

$$(g,h)(g',h') = (gg',hh').$$

(d) A group is ***commutative*** (or ***abelian***) if

$$ab = ba, \quad \text{all } a,b \in G.$$

In a commutative group, the product of any finite (not necessarily ordered) set S of elements is defined.

Recall[5] the classification of finite abelian groups. Every finite abelian group is a product of cyclic groups. If $\gcd(m,n) = 1$, then $C_m \times C_n$ contains an element of order mn, and so $C_m \times C_n \approx C_{mn}$, and isomorphisms of this type give the only ambiguities in the decomposition of a group into a product of cyclic groups.

From this one finds that every finite abelian group is isomorphic to exactly one group of the following form:

$$C_{n_1} \times \cdots \times C_{n_r}, \quad n_1|n_2, \ldots, n_{r-1}|n_r.$$

The order of this group is $n_1 \cdots n_r$.

For example, each abelian group of order 90 is isomorphic to exactly one of C_{90} or $C_3 \times C_{30}$ (note that n_r must be a factor of 90 divisible by all the prime factors of 90).

(e) ***Permutation groups.*** Let S be a set and let G be the set $\mathrm{Sym}(S)$ of bijections $\alpha\colon S \to S$. Then G becomes a group with the composition law $\alpha\beta = \alpha \circ \beta$. For example, the ***permutation group on*** n ***letters*** is $S_n = \mathrm{Sym}(\{1,...,n\})$, which has order $n!$. The symbol $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 4 & 3 & 1 & 6 \end{pmatrix}$ denotes the permutation sending $1 \mapsto 2$, $2 \mapsto 5$, $3 \mapsto 7$, etc..

Subgroups

PROPOSITION 1.4. *Let G be a group and let S be a nonempty subset of G such that*

(a) $a, b \in S \Rightarrow ab \in S$;

(b) $a \in S \Rightarrow a^{-1} \in S$.

Then the law of composition on G makes S into a group.

Therefore,

$$A \cdot (A^{n-1} + a_{n-1}A^{n-2} + \cdots) = \mp(\det A) \cdot I,$$

and

$$A \cdot \left((A^{n-1} + a_{n-1}A^{n-2} + \cdots) \cdot (\mp \det A)^{-1}\right) = I.$$

[5] This was taught in an earlier course.

PROOF. Condition (a) implies that the law of composition on G does define a law of composition $S \times S \to S$ on S, which is automatically associative. By assumption S contains at least one element a, its inverse a^{-1}, and the product $1 = aa^{-1}$. Finally (b) shows that inverses exist in S. □

A subset S as in the proposition is called a ***subgroup*** of G.

If S is finite, then condition (a) implies (b): let $a \in S$; then $\{a, a^2, \ldots\} \subset S$, and so a has finite order, say $a^n = 1$; now $a^{-1} = a^{n-1} \in S$. The example $(\mathbb{N}, +) \subset (\mathbb{Z}, +)$ shows that (a) does not imply (b) when S is infinite.

PROPOSITION 1.5. *An intersection of subgroups of G is a subgroup of G.*

PROOF. It is nonempty because it contains 1, and conditions (a) and (b) of (1.4) are obvious. □

REMARK 1.6. It is generally true that an intersection of subobjects of an algebraic object is a subobject. For example, an intersection of subrings is a subring, an intersection of submodules is a submodule, and so on.

PROPOSITION 1.7. *For any subset X of a group G, there is a smallest subgroup of G containing X. It consists of all finite products (repetitions allowed) of elements of X and their inverses.*

PROOF. The intersection S of all subgroups of G containing X is again a subgroup containing X, and it is evidently the smallest such group. Clearly S contains with X, all finite products of elements of X and their inverses. But the set of such products satisfies (a) and (b) of (1.4) and hence is a subgroup containing X. It therefore equals S. □

We write $\langle X \rangle$ for the subgroup S in the proposition, and call it the ***subgroup generated by*** X. For example, $\langle \emptyset \rangle = \{1\}$. If every element of G has finite order, for example, if G is finite, then the set of all finite products of elements of X is already a group (recall that if $a^m = 1$, then $a^{-1} = a^{m-1}$) and so equals $\langle X \rangle$.

We say that X ***generates*** G if $G = \langle X \rangle$, i.e., if every element of G can be written as a finite product of elements from X and their inverses. Note that the order of an element a of a group is the order of the subgroup $\langle a \rangle$ it generates.

EXAMPLE 1.8. (a) A group is ***cyclic*** if it is generated by one element, i.e., if $G = \langle \sigma \rangle$ for some $\sigma \in G$. If σ has finite order n, then

$$G = \{1, \sigma, \sigma^2, ..., \sigma^{n-1}\} \approx C_n, \quad \sigma^i \leftrightarrow i \mod n,$$

and G can be thought of as the group of rotational symmetries (about the centre) of a regular polygon with n-sides. If σ has infinite order, then

$$G = \{\ldots, \sigma^{-i}, \ldots, \sigma^{-1}, 1, \sigma, \ldots, \sigma^i, \ldots\} \approx C_\infty, \quad \sigma^i \leftrightarrow i.$$

In future, we shall (loosely) use C_m to denote any cyclic group of order m (not necessarily $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}$).

(b) ***Dihedral group***, D_n.[6] This is the group of symmetries of a regular polygon with n-sides. Number the vertices $1, \ldots, n$ in the counterclockwise direction. Let σ be the rotation through $2\pi/n$ (so $i \mapsto i+1 \mod n$), and let τ be the rotation (=reflection) about the axis of symmetry through 1 and the centre of the polygon (so $i \mapsto n+2-i \mod n$). Then

$$\sigma^n = 1; \quad \tau^2 = 1; \quad \tau\sigma\tau^{-1} = \sigma^{-1} \quad (\text{or } \tau\sigma = \sigma^{n-1}\tau).$$

The group has order $2n$; in fact

$$D_n = \{1, \sigma, ..., \sigma^{n-1}, \tau, ..., \sigma^{n-1}\tau\}.$$

(c) ***Quaternion group*** Q: Let $a = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then

$$a^4 = 1, \quad a^2 = b^2, \quad bab^{-1} = a^{-1}.$$

The subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by a and b is

$$Q = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

The group Q can also be described as the subset $\{\pm 1, \pm i, \pm j, \pm k\}$ of the quaternion algebra.

(d) Recall that S_n is the permutation group on $\{1, 2, ..., n\}$. The ***alternating group*** A_n is the subgroup of even permutations (see §4 below). It has order $\frac{n!}{2}$.

Groups of small order

Every group of order < 16 is isomorphic to exactly one on the following list:

1: C_1. 2: C_2. 3: C_3.

4: C_4, $C_2 \times C_2$ (Viergruppe; Klein 4-group).

5: C_5.

6: C_6, $S_3 = D_3$ (S_3 is the first noncommutative group).

7: C_7.

8: C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$, Q, D_4.

9: C_9, $C_3 \times C_3$.

10: C_{10}, D_5.

11: C_{11}.

12: C_{12}, $C_2 \times C_6$, $C_2 \times S_3$, A_4, $C_3 \rtimes C_4$ (see 3.13 below).

13: C_{13}.

14: C_{14}, D_7.

15: C_{15}.

16: (14 groups)

General rules: For each prime p, there is only one group (up to isomorphism), namely C_p (see 1.17 below), and only two groups of order p^2, namely, $C_p \times C_p$ and C_{p^2} (see 4.17).

[6] Some authors denote this group D_{2n}.

For the classification of the groups of order 6, see 4.21; for order 8, see 5.15; for order 12, see 5.14; for orders 10, 14, and 15, see 5.12.

Roughly speaking, the more high powers of primes divide n, the more groups of order n you expect. In fact, if $f(n)$ is the number of isomorphism classes of groups of order n, then

$$f(n) \leq n^{(\frac{2}{27}+o(1))e(n)^2}$$

where $e(n)$ is the largest exponent of a prime dividing n and $o(1) \to 0$ as $e(n) \to \infty$ (see Pyber, Ann. of Math., 137 (1993) 203–220).

By 2001, a complete irredundant list of groups of order ≤ 2000 had been found — up to isomorphism, there are 49,910,529,484 (Besche, Hans Ulrich; Eick, Bettina; O'Brien, E. A. The groups of order at most 2000. Electron. Res. Announc. Amer. Math. Soc. 7 (2001), 1–4 (electronic)).

Multiplication tables

A law of composition on a finite set can be described by its multiplication table:

	1	a	b	c	$\ldots$
1	1	a	b	c	$\ldots$
a	a	a^2	ab	ac	$\ldots$
b	b	ba	b^2	bc	$\ldots$
c	c	ca	cb	c^2	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Note that, if the law of composition defines a group, then, because of the cancellation laws, each row (and each column) is a permutation of the elements of the group.

This suggests an algorithm for finding all groups of a given finite order n, namely, list all possible multiplication tables and check the axioms. Except for very small n, this is not practical! The table has n^2 positions, and if we allow each position to hold any of the n elements, that gives a total of n^{n^2} possible tables. Note how few groups there are. The $8^{64} = 6277\,101\,735\,386\,680\,763\,835\,789\,423\,207\,666\,416\,102\,355\,444\,464\,034\,512\,896$ possible multiplication tables for a set with 8 elements give only 5 isomorphism classes of groups.

Homomorphisms

DEFINITION 1.9. A ***homomorphism*** from a group G to a second G' is a map $\alpha\colon G \to G'$ such that $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in G$.

Note that an isomorphism is simply a bijective homomorphism.

REMARK 1.10. Let α be a homomorphism. Then

$$\alpha(a^m) = \alpha(a^{m-1} \cdot a) = \alpha(a^{m-1}) \cdot \alpha(a),$$

and so, by induction, $\alpha(a^m) = \alpha(a)^m$, $m \geq 1$. Moreover $\alpha(1) = \alpha(1 \times 1) = \alpha(1)\alpha(1)$, and so $\alpha(1) = 1$ (apply 1.2a). Also

$$aa^{-1} = 1 = a^{-1}a \Rightarrow \alpha(a)\alpha(a^{-1}) = 1 = \alpha(a^{-1})\alpha(a),$$

and so $\alpha(a^{-1}) = \alpha(a)^{-1}$. From this it follows that

$$\alpha(a^m) = \alpha(a)^m \qquad \text{all } m \in \mathbb{Z}.$$

We saw above that each row of the multiplication table of a group is a permutation of the elements of the group. As Cayley pointed out, this allows one to realize the group as a group of permutations.

THEOREM 1.11 (CAYLEY). *There is a canonical injective homomorphism*

$$\alpha \colon G \to \mathrm{Sym}(G).$$

PROOF. For $a \in G$, define $a_L \colon G \to G$ to be the map $x \mapsto ax$ (left multiplication by a). For $x \in G$,

$$(a_L \circ b_L)(x) = a_L(b_L(x)) = a_L(bx) = abx = (ab)_L(x),$$

and so $(ab)_L = a_L \circ b_L$. As $1_L = \mathrm{id}$, this implies that

$$a_L \circ (a^{-1})_L = \mathrm{id} = (a^{-1})_L \circ a_L,$$

and so a_L is a bijection, i.e., $a_L \in \mathrm{Sym}(G)$. Hence $a \mapsto a_L$ is a homomorphism $G \to \mathrm{Sym}(G)$, and it is injective because of the cancellation law. □

COROLLARY 1.12. *A finite group of order n can be identified with a subgroup of S_n.*

PROOF. Number the elements of the group $a_1, \ldots, a_n$. □

Unfortunately, when G has large order n, S_n is too large to be manageable. We shall see later (4.20) that G can often be embedded in a permutation group of much smaller order than $n!$.

Cosets

Let H be a subgroup of G. A ***left coset*** of H in G is a set of the form

$$aH = \{ah \mid h \in H\},$$

some fixed $a \in G$; a ***right coset*** is a set of the form

$$Ha = \{ha \mid h \in H\},$$

some fixed $a \in G$.

EXAMPLE 1.13. Let $G = \mathbb{R}^2$, regarded as a group under addition, and let H be a subspace of dimension 1 (line through the origin). Then the cosets (left or right) of H are the lines parallel to H.

PROPOSITION 1.14. *(a) If C is a left coset of H, and $a \in C$, then $C = aH$.*

(b) Two left cosets are either disjoint or equal.

(c) $aH = bH$ if and only if $a^{-1}b \in H$.

(d) Any two left cosets have the same number of elements (possibly infinite).

PROOF. (a) Because C is a left coset, $C = bH$ some $b \in G$, and because $a \in C$, $a = bh$ for some $h \in H$. Now $b = ah^{-1} \in aH$, and for any other element c of C, $c = bh' = ah^{-1}h' \in aH$. Thus, $C \subset aH$. Conversely, if $c \in aH$, then $c = ah' = bhh' \in bH$.

(b) If C and C' are not disjoint, then there is an element $a \in C \cap C'$, and $C = aH$ and $C' = aH$.

(c) We have $aH = bH \iff b \in aH \iff b = ah$, for some $h \in H$, i.e., $\iff a^{-1}b \in H$.

(d) The map $(ba^{-1})_L : ah \mapsto bh$ is a bijection $aH \to bH$. □

In particular, the left cosets of H in G partition G, and the condition "a and b lie in the same left coset" is an equivalence relation on G.

The ***index*** $(G : H)$ of H in G is defined to be the number of left cosets of H in G. In particular, $(G : 1)$ is the order of G.

Each left coset of H has $(H\colon 1)$ elements and G is a disjoint union of the left cosets. When G is finite, we can conclude:

THEOREM 1.15 (LAGRANGE). *If G is finite, then*

$$(G : 1) = (G : H)(H : 1).$$

In particular, the order of H divides the order of G.

COROLLARY 1.16. *The order of every element of a finite group divides the order of the group.*

PROOF. Apply Lagrange's theorem to $H = \langle g \rangle$, recalling that $(H : 1) = \text{order}(g)$. □

EXAMPLE 1.17. If G has order p, a prime, then every element of G has order 1 or p. But only e has order 1, and so G is generated by any element $g \neq e$. In particular, G is cyclic, $G \approx C_p$. Hence, up to isomorphism, there is only one group of order $1,000,000,007$; in fact there are only two groups of order $1,000,000,014,000,000,049$.

REMARK 1.18. (a) There is a one-to-one correspondence between the set of left cosets and the set of right cosets, viz, $aH \leftrightarrow Ha^{-1}$. Hence $(G : H)$ is also the number of right cosets of H in G. But, in general, a left coset will ***not*** be a right coset (see 1.22 below).

(b) Lagrange's theorem has a partial converse: if a prime p divides $m = (G : 1)$, then G has an element of order p; if p^n divides m, then G has a subgroup of order p^n (Sylow's theorem 5.2). However, note that $C_2 \times C_2$ has order 4, but has no element of order 4, and A_4 has order 12, but it has no subgroup of order 6 (see Exercise 31).

More generally, we have the following result.

PROPOSITION 1.19. *Let G be a finite group. If $G \supset H \supset K$ with H and K subgroups of G, then*

$$(G : K) = (G : H)(H : K).$$

PROOF. Write $G = \bigcup g_i H$ (disjoint union), and $H = \bigcup h_j K$ (disjoint union). On multiplying the second equality by g_i, we find that $g_i H = \bigcup_j g_i h_j K$ (disjoint union), and so $G = \bigcup g_i h_j K$ (disjoint union). □

Normal subgroups

When S and T are two subsets of a group G, we let

$$ST = \{st \mid s \in S, \quad t \in T\}.$$

A subgroup N of G is ***normal***, written $N \lhd G$, if $gNg^{-1} = N$ for all $g \in G$. An intersection of normal subgroups of a group is normal (cf. 1.6).

REMARK 1.20. To show N normal, it suffices to check that $gNg^{-1} \subset N$ for all g, because

$$gNg^{-1} \subset N \Rightarrow g^{-1}gNg^{-1}g \subset g^{-1}Ng \text{ (multiply left and right with } g^{-1} \text{ and } g);$$

hence $N \subset g^{-1}Ng$ for all g, and, on rewriting this with g^{-1} for g, we find that $N \subset gNg^{-1}$ for all g.

The next example shows however that there can exist an N and a g such that $gNg^{-1} \subset N$, $gNg^{-1} \neq N$ (famous exercise in Herstein, Topics in Algebra, 2nd Edition, Wiley, 1975, 2.6, Exercise 8).

EXAMPLE 1.21. Let $G = \mathrm{GL}_2(\mathbb{Q})$, and let $H = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \mid n \in \mathbb{Z}\}$. Then H is a subgroup of G; in fact it is isomorphic to $\mathbb{Z}$. Let $g = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then

$$g\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}g^{-1} = \begin{pmatrix} 5 & 5n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 5^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5n \\ 0 & 1 \end{pmatrix}.$$

Hence $gHg^{-1} \subset H$, but $gHg^{-1} \neq H$.

PROPOSITION 1.22. *A subgroup N of G is normal if and only if each left coset of N in G is also a right coset, in which case, $gN = Ng$ for all $g \in G$.*

PROOF. $\Rightarrow$: Multiply the equality $gNg^{-1} = N$ on the right by g.

$\Leftarrow$: If gN is a right coset, then it must be the right coset Ng — see (1.14a). Hence $gN = Ng$, and so $gNg^{-1} = N$. This holds for all g. □

REMARK 1.23. In other words, in order for N to be normal, we must have that for all $g \in G$ and $n \in N$, there exists an $n' \in N$ such that $gn = n'g$ (equivalently, for all $g \in G$ and $n \in N$, there exists an n' such that $ng = gn'$.) Thus, an element of G can be moved past an element of N at the cost of replacing the element of N by a different element of N.

EXAMPLE 1.24. (a) Every subgroup of index two is normal. Indeed, let $g \in G$, $g \notin H$. Then $G = H \cup gH$ (disjoint union). Hence gH is the complement of H in G. The same argument shows that Hg is the complement of H in G. Hence $gH = Hg$.

(b) Consider the dihedral group $D_n = \{1, \sigma, \ldots, \sigma^{n-1}, \tau, \ldots, \sigma^{n-1}\tau\}$. Then $C_n = \{1, \sigma, \ldots, \sigma^{n-1}\}$ has index 2, and hence is normal. For $n \geq 3$ the subgroup $\{1, \tau\}$ is not normal because $\sigma\tau\sigma^{-1} = \tau\sigma^{n-2} \notin \{1, \tau\}$.

(c) Every subgroup of a commutative group is normal (obviously), but the converse is false: the quaternion group Q is not commutative, but every subgroup is normal (see Exercise 1).

A group G is said to be ***simple*** if it has no normal subgroups other than G and $\{1\}$. Such a group can have still lots of nonnormal subgroups — in fact, the Sylow theorems (§5) imply that every group has nontrivial subgroups unless it is cyclic of prime order.

PROPOSITION 1.25. *If H and N are subgroups of G and N is normal, then*

$$HN \overset{\text{df}}{=} \{hn \mid h \in H, \quad n \in N\}$$

is a subgroup of G. If H is also normal, then HN is a normal subgroup of G.

PROOF. The set HN is nonempty, and

$$(hn)(h'n') \overset{1.22}{=} hh'n''n' \in HN,$$

and so it is closed under multiplication. Since

$$(hn)^{-1} = n^{-1}h^{-1} \overset{1.22}{=} h^{-1}n' \in HN$$

it is also closed under the formation of inverses. If both H and N are normal, then

$$gHNg^{-1} = gHg^{-1} \cdot gNg^{-1} = HN$$

for all $g \in G$. □

Quotients

The ***kernel*** of a homomorphism $\alpha\colon G \to G'$ is

$$\mathrm{Ker}(\alpha) = \{g \in G | \ \alpha(g) = 1\}.$$

If α is injective, then $\mathrm{Ker}(\alpha) = \{1\}$. Conversely, if $\mathrm{Ker}(\alpha) = 1$ then α is injective, because

$$\alpha(g) = \alpha(g') \Rightarrow \alpha(g^{-1}g') = 1 \Rightarrow g^{-1}g' = 1 \Rightarrow g = g'.$$

PROPOSITION 1.26. *The kernel of a homomorphism is a normal subgroup.*

PROOF. It is obviously a subgroup, and if $a \in \mathrm{Ker}(\alpha)$, so that $\alpha(a) = 1$, and $g \in G$, then

$$\alpha(gag^{-1}) = \alpha(g)\alpha(a)\alpha(g)^{-1} = \alpha(g)\alpha(g)^{-1} = 1.$$

Hence $gag^{-1} \in \mathrm{Ker}\,\alpha$. □

PROPOSITION 1.27. *Every normal subgroup occurs as the kernel of a homomorphism. More precisely, if N is a normal subgroup of G, then there is a natural group structure on the set of cosets of N in G (this is if and only if).*

PROOF. Write the cosets as left cosets, and define $(aN)(bN) = (ab)N$. We have to check (a) that this is well-defined, and (b) that it gives a group structure on the set of cosets. It will then be obvious that the map $g \mapsto gN$ is a homomorphism with kernel N.

Check (a). Suppose $aN = a'N$ and $bN = b'N$; we have to show that $abN = a'b'N$. But we are given that $a = a'n$ and $b = b'n'$, some $n, n' \in N$. Hence

$$ab = a'nb'n' \overset{1.23}{=} a'b'n''n' \in a'b'N.$$

Therefore abN and $a'b'N$ have a common element, and so must be equal.

Checking (b) is straightforward: the set is nonempty; the associative law holds; the coset N is an identity element; $a^{-1}N$ is an inverse of aN. □

When N is a normal subgroup, we write G/N for the set of left (= right) cosets of N in G, regarded as a group. It is called the[7] ***quotient*** of G by N. The map $a \mapsto aN\colon G \to G/N$ is a surjective homomorphism with kernel N. It has the following universal property: for any homomorphism $\alpha\colon G \to G'$ of groups such that $\alpha(N) = 1$, there exists a unique homomorphism $G/N \to G'$ such that the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, "a\mapsto aN"] \arrow[dr, "\alpha"] & G/N \arrow[d, dashed] \\
 & G'.
\end{tikzcd}$$

EXAMPLE 1.28. (a) Consider the subgroup $m\mathbb{Z}$ of $\mathbb{Z}$. The quotient group $\mathbb{Z}/m\mathbb{Z}$ is a cyclic group of order m.

(b) Let L be a line through the origin in $\mathbb{R}^2$. Then $\mathbb{R}^2/L$ is isomorphic to $\mathbb{R}$ (because it is a one-dimensional vector space over $\mathbb{R}$).

(c) The quotient $D_n/\langle\sigma\rangle \approx \{1, \tau\}$ (cyclic group of order 2).

Exercises 1–4

Exercises marked with an asterisk were required to be handed in.

1*. Show that the quaternion group has only one element of order 2, and that it commutes with all elements of Q. Deduce that Q is not isomorphic to D_4, and that every subgroup of Q is normal.

2*. Consider the elements

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

in $\mathrm{GL}_2(\mathbb{Z})$. Show that $a^4 = 1$ and $b^3 = 1$, but that ab has infinite order, and hence that the group $\langle a, b\rangle$ is infinite.

3*. Show that every finite group of even order contains an element of order 2.

4*. Let N be a normal subgroup of G of index n. Show that if $g \in G$, then $g^n \in N$. Give an example to show that this may be false when N is not normal.

[7] Some authors say “factor” instead of “quotient”, but this can be confused with “direct factor”.

2 Free Groups and Presentations

It is frequently useful to describe a group by giving a set of generators for the group and a set of relations for the generators from which every other relation in the group can be deduced. For example, D_n can be described as the group with generators σ, τ and relations

$$\sigma^n = 1, \quad \tau^2 = 1, \quad \tau\sigma\tau\sigma = 1.$$

In this section, we make precise what this means. First we need to define the free group on a set X of generators — this is a group generated by X and with no relations except for those implied by the group axioms. Because inverses cause problems, we first do this for semigroups.

Free semigroups

Recall that (for us) a semigroup is a set G with an associative law of composition having an identity element 1. A homomorphism $\alpha\colon S \to S'$ of semigroups is a map such that $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in S$ and $\alpha(1) = 1$. Then α preserves all finite products.

Let $X = \{a, b, c, \ldots\}$ be a (possibly infinite) set of symbols. A ***word*** is a finite sequence of symbols in which repetition is allowed. For example,

$$aa, \quad aabac, \quad b$$

are distinct words. Two words can be multiplied by juxtaposition, for example,

$$aaaa * aabac = aaaaaabac.$$

This defines on the set W of all words an associative law of composition. The empty sequence is allowed, and we denote it by 1. (In the unfortunate case that the symbol 1 is already an element of X, we denote it by a different symbol.) Then 1 serves as an identity element. Write SX for the set of words together with this law of composition. Then SX is a semigroup, called the ***free semigroup*** on X.

When we identify an element a of X with the word a, X becomes a subset of SX and generates it (i.e., there is no proper subsemigroup of SX containing X). Moreover, the map $X \to SX$ has the following universal property: for any map (of sets) $\alpha\colon X \to S$ from X to a semigroup S, there exists a unique homomorphism $SX \to S$ making the following diagram commute:

$$\begin{tikzcd}
X \arrow[r] \arrow[dr, "\alpha"'] & SX \arrow[d, dashed] \\
& S.
\end{tikzcd}$$

In fact, the unique extension of α takes the values:

$$\alpha(1) = 1_S, \quad \alpha(dba\cdots) = \alpha(d)\alpha(b)\alpha(a)\cdots.$$

Free groups

We want to construct a group FX containing X and having the same universal property as SX with “semigroup” replaced by “group”. Define X' to be the set consisting of the symbols in X and also one additional symbol, denoted a^{-1}, for each $a \in X$; thus

$$X' = \{a, a^{-1}, b, b^{-1}, \ldots\}.$$

Let W' be the set of words using symbols from X'. This becomes a semigroup under juxtaposition, but it is not a group because we can’t cancel out the obvious terms in words of the following form:

$$\cdots xx^{-1} \cdots \text{ or } \cdots x^{-1}x \cdots$$

A word is said to be ***reduced*** if it contains no pairs of the form xx^{-1} or $x^{-1}x$. Starting with a word w, we can perform a finite sequence of cancellations to arrive at a reduced word (possibly empty), which will be called the ***reduced form*** of w. There may be many different ways of performing the cancellations, for example,

$$ca\underline{bb^{-1}}a^{-1}c^{-1}ca \mapsto c\underline{aa^{-1}}c^{-1}ca \mapsto \underline{cc^{-1}}ca \mapsto ca :$$

$$cabb^{-1}a^{-1}\underline{c^{-1}c}a \mapsto cabb^{-1}\underline{a^{-1}a} \mapsto ca\underline{bb^{-1}} \mapsto ca.$$

We have underlined the pair we are cancelling. Note that the middle a^{-1} is cancelled with different a’s, and that different terms survive in the two cases. Nevertheless we ended up with the same answer, and the next result says that this always happens.

PROPOSITION 2.1. *There is only one reduced form of a word.*

PROOF. We use induction on the length of the word w. If w is reduced, there is nothing to prove. Otherwise a pair of the form xx^{-1} or $x^{-1}x$ occurs — assume the first, since the argument is the same in both cases.

Observe that any two reduced forms of w obtained by a sequence of cancellations in which xx^{-1} is cancelled first are equal, because the induction hypothesis can be applied to the (shorter) word obtained by cancelling xx^{-1}.

Next observe that any two reduced forms of w obtained by a sequence of cancellations in which xx^{-1} is cancelled at some point are equal, because the result of such a sequence of cancellations will not be affected if xx^{-1} is cancelled first.

Finally, consider a reduced form w_0 obtained by a sequence in which no cancellation cancels xx^{-1} directly. Since xx^{-1} does not remain in w_0, at least one of x or x^{-1} must be cancelled at some point. If the pair itself is not cancelled, then the first cancellation involving the pair must look like

$$\cdots \cancel{x}^{-1}\,\underline{\cancel{x}x^{-1}} \cdots \text{ or } \cdots \underline{x\ \cancel{x}^{-1}}\ \cancel{x} \cdots$$

where our original pair is underlined. But the word obtained after this cancellation is the same as if our original pair were cancelled, and so we may cancel the original pair instead. Thus we are back in the case just proved. □

We say two words w, w' are ***equivalent***, denoted $w \sim w'$, if they have the same reduced form. This is an equivalence relation (obviously).

PROPOSITION 2.2. *Products of equivalent words are equivalent, i.e.,*

$$w \sim w', \quad v \sim v' \Rightarrow wv \sim w'v'.$$

PROOF. Let w_0 and v_0 be the reduced forms of w and of v. To obtain the reduced form of wv, we can first cancel as much as possible in w and v separately, to obtain w_0v_0 and then continue cancelling. Thus the reduced form of wv is the reduced form of w_0v_0. A similar statement holds for $w'v'$, but (by assumption) the reduced forms of w and v equal the reduced forms of w' and v', and so we obtain the same result in the two cases. □

Let FX be the set of equivalence classes of words. The proposition shows that the law of composition on W' defines a law of composition on FX, which obviously makes it into a semigroup. It also has inverses, because

$$ab \cdots gh \cdot h^{-1}g^{-1} \cdots b^{-1}a^{-1} \sim 1.$$

Thus FX is a group, called the ***free group*** on X. To summarize: the elements of FX are represented by words in X'; two words represent the same element of FX if and only if they have the same reduced forms; multiplication is defined by juxtaposition; the empty word represents 1; inverses are obtained in the obvious way. Alternatively, each element of FX is represented by a unique reduced word; multiplication is defined by juxtaposition and passage to the reduced form.

When we identify $a \in X$ with the equivalence class of the (reduced) word a, then X becomes identified with a subset of FX — clearly it generates FX. The next proposition is a precise statement of the fact that there are no relations among the elements of X when regarded as elements of FX except those imposed by the group axioms.

PROPOSITION 2.3. *For any map (of sets) $X \to G$ from X to a group G, there exists a unique homomorphism $FX \to G$ making the following diagram commute:*

$$\begin{tikzcd} X \arrow[r] \arrow[dr] & FX \arrow[d, dashed] \\ & G. \end{tikzcd}$$

PROOF. Consider a map $\alpha\colon X \to G$. We extend it to a map of sets $X' \to G$ by setting $\alpha(a^{-1}) = \alpha(a)^{-1}$. Because G is, in particular, a semigroup, α extends to a homomorphism of semigroups $SX' \to G$. This map will send equivalent words to the same element of G, and so will factor through $FX = SX'/{\sim}$. The resulting map $FX \to G$ is a group homomorphism. It is unique because we know it on a set of generators for FX. □

REMARK 2.4. The universal property of the map $\iota\colon X \to FX$, $x \mapsto x$, characterizes it: if $\iota'\colon X \to F'$ is a second map with the same universal property, then there is a unique isomorphism $\alpha\colon FX \to F'$ such that $\alpha(\iota x) = \iota' x$ for all $x \in X$.

COROLLARY 2.5. *Every group is a quotient of a free group.*

PROOF. Choose a set X of generators for G (e.g., $X = G$), and let F be the free group generated by X. According to (2.3), the inclusion $X \hookrightarrow G$ extends to a homomorphism $F \to G$, and the image, being a subgroup containing X, must equal G. □

The free group on the set $X = \{a\}$ is simply the infinite cyclic group C_∞ generated by a, but the free group on a set consisting of two elements is already very complicated.

I now discuss, without proof, some important results on free groups.

THEOREM 2.6 (NIELSEN-SCHREIER). [8] *Subgroups of free groups are free.*

The best proof uses topology, and in particular covering spaces—see Serre, Trees, Springer, 1980, or Rotman 1995, Theorem 11.44.

Two free groups FX and FY are isomorphic if and only if X and Y have the same number of elements[9]. Thus we can define the ***rank*** of a free group G to be the number of elements in (i.e., cardinality of) a free generating set, i.e., subset $X \subset G$ such that the homomorphism $FX \to G$ given by (2.3) is an isomorphism. Let H be a finitely generated subgroup of a free group F. Then there is an algorithm for constructing from any finite set of generators for H a free finite set of generators. If F has rank n and $(F : H) = i < \infty$, then H is free of rank

$$ni - i + 1.$$

In particular, H may have rank greater than that of F. For proofs, see Rotman 1995, Chapter 11, or Hall, M., The Theory of Groups, MacMillan, 1959, Chapter 7.

Generators and relations

As we noted in §1, an intersection of normal subgroups is again a normal subgroup. Therefore, just as for subgroups, we can define the ***normal subgroup generated by a set*** S in a group G to be the intersection of the normal subgroups containing S. Its description in terms of S is a little complicated. Call a subset S of a group G ***normal*** if $gSg^{-1} \subset S$ for all $g \in G$. Then it is easy to show:

(a) if S is normal, then the subgroup $\langle S \rangle$ generated[10] by it is normal;

(b) for $S \subset G$, $\bigcup_{g\in G} gSg^{-1}$ is normal, and it is the smallest normal set containing S.

From these observations, it follows that:

LEMMA 2.7. *The normal subgroup generated by* $S \subset G$ *is* $\langle \bigcup_{g\in G} gSg^{-1} \rangle$.

Consider a set X and a set R of words made up of symbols in X'. Each element of R represents an element of the free group FX, and the quotient G of FX by the normal subgroup generated by these elements is said to have X as ***generators*** and R as ***relations***. One also says that (X, R) is a ***presentation*** for G, $G = \langle X | R \rangle$, and that R is a set of ***defining relations*** for G.

EXAMPLE 2.8. (a) The dihedral group D_n has generators σ, τ and defining relations

$$\sigma^n, \tau^2, \tau\sigma\tau\sigma.$$

(See 2.10 below for a proof.)

[8] Nielsen (1921) proved this for finitely generated subgroups, and in fact gave an algorithm for deciding whether a word lies in the subgroup; Schreier (1927) proved the general case.

[9] By which I mean that there is a bijection from one to the other.

[10] The map "conjugation by g", $x \mapsto gxg^{-1}$, is a homomorphism $G \to G$. If $x \in G$ can be written $x = a_1 \cdots a_m$ with each a_i or its inverse in S, then so also can $gxg^{-1} = (ga_1g^{-1}) \cdots (ga_mg^{-1})$.

(b) The ***generalized quaternion group*** Q_n, $n \geq 3$, has generators a, b and relations[11] $a^{2^{n-1}} = 1$, $a^{2^{n-2}} = b^2$, $bab^{-1} = a^{-1}$. For $n = 3$ this is the group Q of (1.8c). In general, it has order 2^n (for more on it, see Exercise 8).

(c) Two elements a and b in a group commute if and only if their ***commutator*** $[a, b] =_{\text{df}} aba^{-1}b^{-1}$ is 1. The ***free abelian group*** on generators $a_1, \ldots, a_n$ has generators $a_1, a_2, \ldots, a_n$ and relations

$$[a_i, a_j], \qquad i \neq j.$$

For the remaining examples, see Massey, W., Algebraic Topology: An Introduction, Harbrace, 1967, which contains a good account of the interplay between group theory and topology. For example, for many types of topological spaces, there is an algorithm for obtaining a presentation for the fundamental group.

(d) The fundamental group of the open disk with one point removed is the free group on σ where σ is any loop around the point (ibid. II 5.1).

(e) The fundamental group of the sphere with r points removed has generators $\sigma_1, ..., \sigma_r$ (σ_i is a loop around the i^{th} point) and a single relation

$$\sigma_1 \cdots \sigma_r = 1.$$

(f) The fundamental group of a compact Riemann surface of genus g has $2g$ generators $u_1, v_1, ..., u_g, v_g$ and a single relation

$$u_1 v_1 u_1^{-1} v_1^{-1} \cdots u_g v_g u_g^{-1} v_g^{-1} = 1$$

(ibid. IV Exercise 5.7).

Proposition 2.9. *Let G be the group defined by the presentation (X, R). For any group H and map (of sets) $X \to H$ sending each element of R to 1 (in an obvious sense), there exists a unique homomorphism $G \to H$ making the following diagram commute:*

$$\begin{tikzcd} X \arrow[r] \arrow[dr] & G \arrow[d, dashed] \\ & H. \end{tikzcd}$$

Proof. Let α be a map $X \to H$. From the universal property of free groups (2.3), we know that α extends to a homomorphism $FX \to H$, which we again denote α. Let ιR be the image of R in FX. By assumption $\iota R \subset \operatorname{Ker}(\alpha)$, and therefore the normal subgroup N generated by ιR is contained in $\operatorname{Ker}(\alpha)$. Hence (see p14), α factors through $FX/N = G$. This proves the existence, and the uniqueness follows from the fact that we know the map on a set of generators for X. □

Example 2.10. Let $G = \langle a, b | a^n, b^2, baba \rangle$. We prove that G is isomorphic to D_n. Because the elements $\sigma, \tau \in D_n$ satisfy these relations, the map

$$\{a, b\} \to D_n, \quad a \mapsto \sigma, \quad b \mapsto \tau$$

[11] Strictly speaking, I should say the relations $a^{2^{n-1}}$, $a^{2^{n-2}}b^{-2}$, $bab^{-1}a$.

extends uniquely to a homomorphism $G \to D_n$. This homomorphism is surjective because σ and τ generate D_n. The relations $a^n = 1, \quad b^2 = 1, \quad ba = a^{n-1}b$ imply that each element of G is represented by one of the following elements, $1, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b$, and so $(G : 1) \leq 2n = (D_n : 1)$. Therefore the homomorphism is bijective (and these symbols represent distinct elements of G).

Finitely presented groups

A group is said to be ***finitely presented*** if it admits a presentation (X, R) with both X and R finite.

EXAMPLE 2.11. Consider a finite group G. Let $X = G$, and let R be the set of words

$$\{abc^{-1} \mid ab = c \text{ in } G\}.$$

I claim that (X, R) is a presentation of G, and so G is finitely presented. Let $G' = \langle X | R \rangle$. The map $FX \to G$, $a \mapsto a$, sends each element of R to 1, and therefore defines a homomorphism $G' \to G$, which is obviously surjective. But clearly every element of G' is represented by an element of X, and so the homomorphism is also injective.

Although it is easy to define a group by a finite presentation, calculating the properties of the group can be very difficult — note that we are defining the group, which may be quite small, as the quotient of a huge free group by a huge subgroup. I list some negative results.

The word problem

Let G be the group defined by a finite presentation (X, R). The word problem for G asks whether there is an algorithm (decision procedure) for deciding whether a word on X' represents 1 in G. Unfortunately, the answer is negative: Novikov and Boone showed that there exist finitely presented groups G for which there is no such algorithm. Of course, there do exist other groups for which there is an algorithm.

The same ideas lead to the following result: there does not exist an algorithm that will determine for an arbitrary finite presentation whether or not the corresponding group is trivial, finite, abelian, solvable, nilpotent, simple, torsion, torsion-free, free, or has a solvable word problem.

See Rotman 1995, Chapter 12, for proofs of these statements.

The Burnside problem

A group is said to have ***exponent*** m if $g^m = 1$ for all $g \in G$. It is easy to write down examples of infinite groups generated by a finite number of elements of finite order (see Exercise 2), but does there exist an infinite finitely-generated group with a finite exponent? (Burnside problem). In 1970, Adjan, Novikov, and Britton showed the answer is yes: there do exist infinite finitely-generated groups of finite exponent.

Todd-Coxeter algorithm

There are some quite innocuous looking finite presentations that are known to define quite small groups, but for which this is very difficult to prove. The standard approach to these questions is to use the Todd-Coxeter algorithm (see §4 below).

In the remainder of this course, including the exercises, we'll develop various methods for recognizing groups from their presentations.

Maple

What follows is an annotated transcript of a Maple session:

```
maple    [This starts Maple on a Sun, PC, ....]

with(group);    [This loads the group package, and lists
some of the available commands.]

G:=grelgroup({a,b},{[a,a,a,a],[b,b],[b,a,b,a]});
[This defines G to be the group with generators a,b and
relations aaaa, bb, and baba; use 1/a for the inverse of a.]

grouporder(G);
[This attempts to find the order of the group G.]

H:=subgrel({x=[a,a],y=[b]},G);
[This defines H to be the subgroup of G with
generators x=aa and y=b]

pres(H);    [This computes a presentation of H]

quit  [This exits Maple.]
To get help on a command, type ?command
```

Exercises 5–12

5*. Prove that the group with generators $a_1, \dots, a_n$ and relations $[a_i, a_j] = 1$, $i \neq j$, is the free *abelian* group on $a_1, \dots, a_n$. [Hint: Use universal properties.]

6. Let a and b be elements of an arbitrary free group F. Prove:

(a) If $a^n = b^n$ with $n > 1$, then $a = b$.
(b) If $a^m b^n = b^n a^m$ with $mn \neq 0$, then $ab = ba$.
(c) If the equation $x^n = a$ has a solution x for every n, then $a = 1$.

7*. Let F_n denote the free group on n generators. Prove:

(a) If $n < m$, then F_n is isomorphic to both a subgroup and a quotient group of F_m.
(b) Prove that $F_1 \times F_1$ is not a free group.
(c) Prove that the centre $Z(F_n) = 1$ provided $n > 1$.

8. Prove that Q_n (see 2.8b) has a unique subgroup of order 2, which is $Z(Q_n)$. Prove that $Q_n/Z(Q_n)$ is isomorphic to $D_{2^{n-1}}$.

9. (a) Let $G = \langle a, b | a^2, b^2, (ab)^4 \rangle$. Prove that G is isomorphic to the dihedral group D_4.
(b) Prove that $G = \langle a, b | a^2, abab \rangle$ is an infinite group. (This is usually known as the infinite dihedral group.)

10. Let $G = \langle a, b, c | a^3, b^3, c^4, acac^{-1}, aba^{-1}bc^{-1}b^{-1} \rangle$. Prove that G is the trivial group $\{1\}$. [Hint: Expand $(aba^{-1})^3 = (bcb^{-1})^3$.]

11*. Let F be the free group on the set $\{x, y\}$ and let $G = C_2$, with generator $a \neq 1$. Let α be the homomorphism $F \to G$ such that $\alpha(x) = a = \alpha(y)$. Find a minimal generating set for the kernel of α. Is the kernel a free group?

12. Let $G = \langle s, t | t^{-1}s^3t = s^5 \rangle$. Prove that the element

$$g = s^{-1}t^{-1}s^{-1}tst^{-1}st$$

is in the kernel of every map from G to a finite group.

> Coxeter came to Cambridge and gave a lecture [in which he stated a] problem for which he gave proofs for selected examples, and he asked for a unified proof. I left the lecture room thinking. As I was walking through Cambridge, suddenly the idea hit me, but it hit me while I was in the middle of the road. When the idea hit me I stopped and a large truck ran into me.... So I pretended that Coxeter had calculated the difficulty of this problem so precisely that he knew that I would get the solution just in the middle of the road.... Ever since, I've called that theorem "the murder weapon". One consequence of it is that in a group if $a^2 = b^3 = c^5 = (abc)^{-1}$, then $c^{610} = 1$.
>
> John Conway, Mathematical Intelligencer 23 (2001), no. 2, pp8–9.

3 Isomorphism Theorems. Extensions.

Theorems concerning homomorphisms

The next three theorems (or special cases of them) are often called the ***first, second, and third isomorphism theorems*** respectively.

Factorization of homomorphisms

Recall that the image of a map $\alpha\colon S \to T$ is $\alpha(S) = \{\alpha(s) \mid s \in S\}$.

THEOREM 3.1 (FUNDAMENTAL THEOREM OF GROUP HOMOMORPHISMS). *For any homomorphism $\alpha\colon G \to G'$ of groups, the kernel N of α is a normal subgroup of G, the image I of α is a subgroup of G', and α factors in a natural way into the composite of a surjection, an isomorphism, and an injection:*

$$\begin{tikzcd}
G \arrow[r, "\alpha"] \arrow[d, "\text{onto}"] & G' \\
G/N \arrow[r, "\cong"] & I \arrow[u, "\text{inj.}"']
\end{tikzcd}$$

PROOF. We have already seen (1.26) that the kernel is a normal subgroup of G. If $b = \alpha(a)$ and $b' = \alpha(a')$, then $bb' = \alpha(aa')$ and $b^{-1} = \alpha(a^{-1})$, and so $I =_{\text{df}} \alpha(G)$ is a subgroup of G'. For $n \in N$, $\alpha(gn) = \alpha(g)\alpha(n) = \alpha(g)$, and so α is constant on each left coset gN of N in G. It therefore defines a map

$$\overline{\alpha} : G/N \to I, \quad \overline{\alpha}(gN) = \alpha(g).$$

Then $\overline{\alpha}$ is a homomorphism because

$$\overline{\alpha}((gN)\cdot(g'N)) = \overline{\alpha}(gg'N) = \alpha(gg') = \alpha(g)\alpha(g'),$$

and it is certainly surjective. If $\overline{\alpha}(gN) = 1$, then $g \in \operatorname{Ker}(\alpha) = N$, and so $\overline{\alpha}$ has trivial kernel. This implies that it is injective (p. 13). □

The isomorphism theorem

THEOREM 3.2 (ISOMORPHISM THEOREM). *Let H be a subgroup of G and N a normal subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and the map*

$$h(H \cap N) \mapsto hN : H/H \cap N \to HN/N$$

is an isomorphism.

PROOF. We have already seen (1.25) that HN is a subgroup. Consider the map

$$H \to G/N, \quad h \mapsto hN.$$

This is a homomorphism, and its kernel is $H \cap N$, which is therefore normal in H. According to Theorem 3.1, it induces an isomorphism $H/H \cap N \to I$ where I is its image. But I is the set of cosets of the form hN with $h \in H$, i.e., $I = HN/N$. □

The correspondence theorem

The next theorem shows that if $\overline{G}$ is a quotient group of G, then the lattice of subgroups in $\overline{G}$ captures the structure of the lattice of subgroups of G lying over the kernel of $G \to \overline{G}$.

THEOREM 3.3 (CORRESPONDENCE THEOREM). *Let $\alpha\colon G \twoheadrightarrow \overline{G}$ be a surjective homomorphism, and let $N = \mathrm{Ker}(\alpha)$. Then there is a one-to-one correspondence*

$$\{\textit{subgroups of } G \textit{ containing } N\} \overset{1:1}{\leftrightarrow} \{\textit{subgroups of } \overline{G}\}$$

under which a subgroup H of G containing N corresponds to $\overline{H} = \alpha(H)$ and a subgroup $\overline{H}$ of $\overline{G}$ corresponds to $H = \alpha^{-1}(\overline{H})$. Moreover, if $H \leftrightarrow \overline{H}$ and $H' \leftrightarrow \overline{H}'$, then

(a) $\overline{H} \subset \overline{H}' \iff H \subset H'$, *in which case* $(\overline{H}' : \overline{H}) = (H' : H)$;

(b) $\overline{H}$ *is normal in* $\overline{G}$ *if and only if* H *is normal in* G, *in which case,* α *induces an isomorphism*

$$G/H \xrightarrow{\cong} \overline{G}/\overline{H}.$$

PROOF. For any subgroup $\overline{H}$ of $\overline{G}$, $\alpha^{-1}(\overline{H})$ is a subgroup of G containing N, and for any subgroup H of G, $\alpha(H)$ is a subgroup of $\overline{G}$. One verifies easily that $\alpha^{-1}\alpha(H) = H$ if and only if $H \supset N$, and that $\alpha\alpha^{-1}(\overline{H}) = \overline{H}$. Therefore, the two operations give the required bijection. The remaining statements are easily verified. □

COROLLARY 3.4. *Let N be a normal subgroup of G; then there is a one-to-one correspondence between the set of subgroups of G containing N and the set of subgroups of G/N, $H \leftrightarrow H/N$. Moreover H is normal in G if and only if H/N is normal in G/N, in which case the homomorphism $g \mapsto gN : G \to G/N$ induces an isomorphism*

$$G/H \xrightarrow{\cong} (G/N)/(H/N).$$

PROOF. Special case of the theorem in which α is taken to be $g \mapsto gN\colon G \to G/N$. □

Direct products

The next two propositions give criteria for a group to be a direct product of two subgroups.

PROPOSITION 3.5. *Consider subgroups H_1 and H_2 of a group G. The map*

$$(h_1, h_2) \mapsto h_1h_2\colon H_1 \times H_2 \to G$$

is an isomorphism of groups if and only if

(a) $G = H_1H_2$,

(b) $H_1 \cap H_2 = \{1\}$, *and*

(c) *every element of H_1 commutes with every element of H_2.*

PROOF. The conditions are obviously necessary (if $g \in H_1 \cap H_2$, then $(g, g^{-1}) \mapsto 1$, and so $(g, g^{-1}) = (1, 1)$). Conversely, (c) implies that the map $(h_1, h_2) \mapsto h_1h_2$ is a homomorphism, and (b) implies that it is injective:

$$h_1h_2 = 1 \Rightarrow h_1 = h_2^{-1} \in H_1 \cap H_2 = \{1\}.$$

Finally, (a) implies that it is surjective. □

PROPOSITION 3.6. *Consider subgroups H_1 and H_2 of a group G. The map*

$$(h_1, h_2) \mapsto h_1 h_2 \colon H_1 \times H_2 \to G$$

is an isomorphism of groups if and only if
(a) $H_1 H_2 = G$,
(b) $H_1 \cap H_2 = \{1\}$, *and*
(c) H_1 *and* H_2 *are both normal in* G.

PROOF. Again, the conditions are obviously necessary. In order to show that they are sufficient, we check that they imply the conditions of the previous proposition. For this we only have to show that each element h_1 of H_1 commutes with each element h_2 of H_2. But the commutator $[h_1, h_2] = h_1 h_2 h_1^{-1} h_2^{-1} = (h_1 h_2 h_1^{-1}) \cdot h_2^{-1}$ is in H_2 because H_2 is normal, and it's in H_1 because H_1 is normal, and so (b) implies that it is 1. Hence $h_1 h_2 = h_2 h_1$. □

PROPOSITION 3.7. *Consider subgroups $H_1, H_2, \ldots, H_k$ of a group G. The map*

$$(h_1, h_2, \ldots, h_k) \mapsto h_1 h_2 \cdots h_k : H_1 \times H_2 \times \cdots \times H_k \to G$$

is an isomorphism of groups if (and only if)
(a) $G = H_1 H_2 \cdots H_k$,
(b) *for each* j, $H_j \cap (H_1 \cdots H_{j-1} H_{j+1} \cdots H_k) = \{1\}$, *and*
(c) *each of* $H_1, H_2, \ldots, H_k$ *is normal in* G,

PROOF. For $k = 2$, this is becomes the preceding proposition. We proceed by induction on k. The conditions (a,b,c) hold for the subgroups $H_1, \ldots, H_{k-1}$ of $H_1 \cdots H_{k-1}$, and so we may assume that

$$(h_1, h_2, \ldots, h_{k-1}) \mapsto h_1 h_2 \cdots h_{k-1} : H_1 \times H_2 \times \cdots \times H_{k-1} \to H_1 H_2 \cdots H_{k-1}$$

is an isomorphism. An induction argument using (1.25) shows that $H_1 \cdots H_{k-1}$ is normal in G, and so the pair $H_1 \cdots H_{k-1}$, H_k satisfies the hypotheses of (3.6). Hence

$$(h, h_k) \mapsto h h_k : (H_1 \cdots H_{k-1}) \times H_k \to G$$

is an isomorphism. These isomorphisms can be combined to give the required isomorphism:

$$H_1 \times \cdots \times H_{k-1} \times H_k \xrightarrow{(h_1, \ldots, h_k) \mapsto (h_1 \cdots h_{k-1}, h_k)} H_1 \cdots H_{k-1} \times H_k \xrightarrow{(h, h_k) \mapsto h h_k} G. \quad \square$$

REMARK 3.8. When

$$(h_1, h_2, ..., h_k) \mapsto h_1 h_2 \cdots h_k \colon H_1 \times H_2 \times \cdots \times H_k \to G$$

is an isomorphism we say that G is the ***direct product*** of its subgroups H_i. In more down-to-earth terms, this means: each element g of G can be written uniquely in the form $g = h_1 h_2 \cdots h_k$, $h_i \in H_i$; if $g = h_1 h_2 \cdots h_k$ and $g' = h_1' h_2' \cdots h_k'$, then

$$g g' = (h_1 h_1')(h_2 h_2') \cdots (h_k h_k').$$

Automorphisms of groups

Let G be a group. An isomorphism $G \to G$ is called an ***automorphism*** of G. The set $\mathrm{Aut}(G)$ of such automorphisms becomes a group under composition: the composite of two automorphisms is again an automorphism; composition of maps is always associative; the identity map $g \mapsto g$ is an identity element; an automorphism is a bijection, and therefore has an inverse, which is again an automorphism.

For $g \in G$, the map i_g "conjugation by g",

$$x \mapsto gxg^{-1} : G \to G$$

is an automorphism: it is a homomorphism because

$$g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}), \quad \text{i.e.,} \quad i_g(xy) = i_g(x)i_g(y),$$

and it is bijective because $i_{g^{-1}}$ is an inverse. An automorphism of this form is called an ***inner automorphism***, and the remaining automorphisms are said to be ***outer***.

Note that

$$(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1}, \text{ i.e., } i_{gh}(x) = (i_g \circ i_h)(x),$$

and so the map $g \mapsto i_g \colon G \to \mathrm{Aut}(G)$ is a homomorphism. Its image is written $\mathrm{Inn}(G)$. Its kernel is the ***centre*** of G,

$$Z(G) = \{g \in G \mid gx = xg \text{ all } x \in G\},$$

and so we obtain from (3.1) an isomorphism

$$G/Z(G) \to \mathrm{Inn}(G).$$

In fact, $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$: for $g \in G$ and $\alpha \in \mathrm{Aut}(G)$,

$$(\alpha \circ i_g \circ \alpha^{-1})(x) = \alpha(g \cdot \alpha^{-1}(x) \cdot g^{-1}) = \alpha(g) \cdot x \cdot \alpha(g)^{-1} = i_{\alpha(g)}(x).$$

A group G is said to be ***complete*** if the map $g \mapsto i_g \colon G \to \mathrm{Aut}(G)$ is an isomorphism. Note that this is equivalent to the condition:

(a) the centre $Z(G)$ of G is trivial, and

(b) every automorphism of G is inner.

EXAMPLE 3.9. (a) For $n \neq 2, 6$, S_n is complete. The group S_2 is commutative and hence fails (a); $\mathrm{Aut}(S_6)/\mathrm{Inn}(S_6) \approx C_2$, and hence S_6 fails (b). See Rotman 1995, Theorems 7.5, 7.10.

(b) Let $G = \mathbb{F}_p^n$. The automorphisms of G as an abelian group are just the automorphisms of G as a vector space over $\mathbb{F}_p$; thus $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$. Because G is commutative, all nontrivial automorphisms of G are outer.

(c) As a particular case of (b), we see that

$$\mathrm{Aut}(C_2 \times C_2) = \mathrm{GL}_2(\mathbb{F}_2).$$

But $\mathrm{GL}_2(\mathbb{F}_2) \approx S_3$ (see Exercise 16), and so the nonisomorphic groups $C_2 \times C_2$ and S_3 have isomorphic automorphism groups.

(d) Let G be a cyclic group of order n, say $G = \langle g \rangle$. An automorphism α of G must send g to another generator of G. Let m be an integer ≥ 1. The smallest multiple of m divisible by n is $m \cdot \frac{n}{\gcd(m,n)}$. Therefore, g^m has order $\frac{n}{\gcd(m,n)}$, and so the generators of G are the elements g^m with $\gcd(m,n) = 1$. Thus $\alpha(g) = g^m$ for some m relatively prime to n, and in fact the map $\alpha \mapsto m$ defines an isomorphism

$$\mathrm{Aut}(C_n) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

where

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\text{units in the ring } \mathbb{Z}/n\mathbb{Z}\} = \{m + n\mathbb{Z} \mid \gcd(m,n) = 1\}.$$

This isomorphism is independent of the choice of a generator g for G; in fact, if $\alpha(g) = g^m$, then for any other element $g' = g^i$ of G,

$$\alpha(g') = \alpha(g^i) = \alpha(g)^i = g^{mi} = (g^i)^m = (g')^m.$$

(e) Since the centre of the quaternion group Q is $\langle a^2 \rangle$, we have that

$$\mathrm{Inn}(Q) \cong Q/\langle a^2 \rangle \approx C_2 \times C_2.$$

In fact, $\mathrm{Aut}(Q) \approx S_4$. See Exercise 17.

(f) If G is a simple noncommutative group, then $\mathrm{Aut}(G)$ is complete. See Rotman 1995, Theorem 7.14.

REMARK 3.10. It will be useful to have a description of $(\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(C_n)$. If $n = p_1^{r_1} \cdots p_s^{r_s}$ is the factorization of n into powers of distinct primes, then the Chinese Remainder Theorem (Dummit and Foote 1991, 7.6, Theorem 17) gives us an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}, \quad m \mod n \mapsto (m \mod p_1^{r_1}, \ldots, m \mod p_s^{r_s}),$$

which induces an isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \approx (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times.$$

Hence we need only consider the case $n = p^r$, p prime.

Suppose first that p is odd. The set $\{0, 1, \ldots, p^r - 1\}$ is a complete set of representatives for $\mathbb{Z}/p^r\mathbb{Z}$, and $\frac{1}{p}$ of these elements are divisible by p. Hence $(\mathbb{Z}/p^r\mathbb{Z})^\times$ has order $p^r - \frac{p^r}{p} = p^{r-1}(p-1)$. Because $p-1$ and p^r are relatively prime, we know from (1.3d) that $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is isomorphic to the direct product of a group A of order $p-1$ and a group B of order p^{r-1}. The map

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times,$$

induces an isomorphism $A \to \mathbb{F}_p^\times$, and $\mathbb{F}_p^\times$, being a finite subgroup of the multiplicative group of a field, is cyclic (FT, Exercise 3). Thus $(\mathbb{Z}/p^r\mathbb{Z})^\times \supset A = \langle \zeta \rangle$ for some element ζ of order $p-1$. Using the binomial theorem, one finds that $1+p$ has order p^{r-1} in $(\mathbb{Z}/p^r\mathbb{Z})^\times$, and therefore generates B. Thus $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic, with generator $\zeta\cdot(1+p)$, and every element can be written uniquely in the form

$$\zeta^i\cdot(1+p)^j,\quad 0\le i<p-1,\quad 0\le j<p^{r-1}.$$

On the other hand,

$$(\mathbb{Z}/8\mathbb{Z})^\times=\{\bar{1},\bar{3},\bar{5},\bar{7}\}=\langle\bar{3},\bar{5}\rangle\approx C_2\times C_2$$

is not cyclic. The situation can be summarized by:

$$(\mathbb{Z}/p^r\mathbb{Z})^\times\approx\begin{cases}C_{(p-1)p^{r-1}} & p\text{ odd,}\\ C_2 & p^r=2^2\\ C_2\times\ C_{2^{r-2}} & p=2,r>2.\end{cases}$$

See Dummit and Foote 1991, 9.5, Corollary 20 for more details.

DEFINITION 3.11. A ***characteristic subgroup*** of a group G is a subgroup H such that $\alpha(H)=H$ for all automorphisms α of G.

The same argument as in (1.20) shows that it suffices to check that $\alpha(H)\subset H$ for all $\alpha\in\mathrm{Aut}(G)$.

Contrast: a subgroup H of G is normal if it is stable under all inner automorphisms of G; it is characteristic if it stable under all automorphisms. In particular, a characteristic subgroup is normal.

REMARK 3.12. (a) Consider a group G and a normal subgroup H. An inner automorphism of G restricts to an automorphism of H, which may be outer (for an example, see 3.16f). Thus a normal subgroup of H need not be a normal subgroup of G. However, a characteristic subgroup of H will be a normal subgroup of G. Also a characteristic subgroup of a characteristic subgroup is a characteristic subgroup.

(b) The centre $Z(G)$ of G is a characteristic subgroup, because

$$zg=gz\text{ all }g\in G\Rightarrow\alpha(z)\alpha(g)=\alpha(g)\alpha(z)\text{ all }g\in G,$$

and as g runs over G, $\alpha(g)$ also runs over G. Expect subgroups with a general group-theoretic definition to be characteristic.

(c) If H is the only subgroup of G of order m, then it must be characteristic, because $\alpha(H)$ is again a subgroup of G of order m.

(d) Every subgroup of a commutative group is normal but not necessarily characteristic. For example, a subspace of dimension 1 in $G=\mathbb{F}_p^2$ will not be stable under $\mathrm{GL}_2(\mathbb{F}_p)$ and hence is not a characteristic subgroup.

Semidirect products

Let N be a normal subgroup of G. Each element g of G defines an automorphism of N, $n\mapsto gng^{-1}$, and so we have a homomorphism

$$\theta:G\to\mathrm{Aut}(N).$$

If there exists a subgroup Q of G such that $G \to G/N$ maps Q isomorphically onto G/N, then I claim that we can reconstruct G from the triple $(N, Q, \theta|Q)$. Indeed, any $g \in G$ can be written in a unique fashion

$$g = nq, \quad n \in N, \quad q \in Q$$

— q is the unique element of Q representing g in G/N, and $n = gq^{-1}$. Thus, we have a one-to-one correspondence (of sets)

$$G \overset{1-1}{\leftrightarrow} N \times Q.$$

If $g = nq$ and $g' = n'q'$, then

$$gg' = nqn'q' = n(qn'q^{-1})qq' = n \cdot \theta(q)(n') \cdot qq'.$$

DEFINITION 3.13. A group G is said to be a ***semidirect product*** of the subgroups N and Q, written $N \rtimes Q$, if N is normal and $G \to G/N$ induces an isomorphism $Q \xrightarrow{\approx} G/N$. Equivalent condition: N and Q are subgroups of G such that

$$\text{(i) } N \lhd G;\ \text{(ii) } NQ = G;\ \text{(iii) } N \cap Q = \{1\}.$$

Note that Q need *not* be a normal subgroup of G.

EXAMPLE 3.14. (a) In D_n, let $C_n = \langle\sigma\rangle$ and $C_2 = \langle\tau\rangle$; then

$$D_n = \langle\sigma\rangle \rtimes \langle\tau\rangle = C_n \rtimes C_2.$$

(b) The alternating subgroup A_n is a normal subgroup of S_n (because it has index 2), and $Q = \{(12)\} \xrightarrow{\approx} S_n/A_n$. Therefore $S_n = A_n \rtimes C_2$.

(c) The quaternion group can not be written as a semidirect product in any nontrivial fashion (see Exercise 14).

(d) A cyclic group of order p^2, p prime, is not a semidirect product.

(e) Let $G = \mathrm{GL}_n(k)$, the group of invertible $n \times n$ matrices with coefficients in the field k. Let B be the subgroup of upper triangular matrices in G, T the subgroup of diagonal matrices in G, and U subgroup of upper triangular matrices with all their diagonal coefficients equal to 1. Thus, when $n = 2$,

$$B = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}, \quad T = \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}, \quad U = \left\{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\right\}.$$

Then, U is a normal subgroup of B, $UT = B$, and $U \cap T = \{1\}$. Therefore,

$$B = U \rtimes T.$$

Note that, when $n \geq 2$, the action of T on U is not trivial, and so B is not the direct product of T and U.

We have seen that, from a semidirect product $G = N \rtimes Q$, we obtain a triple

$$(N, Q, \theta\colon Q \to \mathrm{Aut}(N)).$$

We now prove that every triple (N, Q, θ) consisting of two groups N and Q and a homomorphism $\theta\colon Q \to \mathrm{Aut}(N)$ arises from a semidirect product. As a set, let $G = N \times Q$, and define

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq').$$

PROPOSITION 3.15. *The above composition law makes G into a group, in fact, the semidirect product of N and Q.*

PROOF. Write ${}^{q}n$ for $\theta(q)(n)$, so that the composition law becomes

$$(n, q)(n', q') = (n \cdot {}^{q}n', qq').$$

Then

$$((n, q), (n', q'))(n'', q'') = (n \cdot {}^{q}n' \cdot {}^{qq'}n'', qq'q'') = (n, q)((n', q')(n'', q''))$$

and so the associative law holds. Because $\theta(1) = 1$ and $\theta(q)(1) = 1$,

$$(1, 1)(n, q) = (n, q) = (n, q)(1, 1),$$

and so $(1, 1)$ is an identity element. Next

$$(n, q)({}^{q^{-1}}n, q^{-1}) = (1, 1) = ({}^{q^{-1}}n, q^{-1})(n, q),$$

and so $({}^{q^{-1}}n, q^{-1})$ is an inverse for (n, q). Thus G is a group, and it easy to check that it satisfies the conditions (i,ii,iii) of (3.13). □

Write $G = N \rtimes_{\theta} Q$ for the above group.

EXAMPLE 3.16. (a) Let θ be the (unique) nontrivial homomorphism

$$C_4 \to \mathrm{Aut}(C_3) \cong C_2,$$

namely, that which sends a generator of C_4 to the map $a \mapsto a^2$. Then $G =_{df} C_3 \rtimes_{\theta} C_4$ is a noncommutative group of order 12, not isomorphic to A_4. If we denote the generators of C_3 and C_4 by a and b, then a and b generate G, and have the defining relations

$$a^3 = 1, \quad b^4 = 1, \quad bab^{-1} = a^2.$$

(b) The bijection

$$(n, q) \mapsto (n, q)\colon N \times Q \to N \rtimes_{\theta} Q$$

is an isomorphism of groups if and only if θ is the trivial homomorphism $Q \to \mathrm{Aut}(N)$, i.e., $\theta(q)(n) = n$ for all $q \in Q$, $b \in N$.

(c) Both S_3 and C_6 are semidirect products of C_3 by C_2 — they correspond to the two homomorphisms $C_2 \to C_2 \cong \mathrm{Aut}(C_3)$.

(d) Let $N=\langle a,b\rangle$ be the product of two cyclic groups $\langle a\rangle$ and $\langle b\rangle$ of order p, and let $Q=\langle c\rangle$ be a cyclic group of order p. Define $\theta\colon Q\to\operatorname{Aut}(N)$ to be the homomorphism such that

$$\theta(c^i)(a)=ab^i,\quad \theta(c^i)(b)=b.$$

[If we regard N as the additive group $N=\mathbb{F}_p^2$ with a and b the standard basis elements, then $\theta(c^i)$ is the automorphism of N defined by the matrix $\begin{pmatrix}1&0\\ i&1\end{pmatrix}$.] The group $G=_{df}N\rtimes_\theta Q$ is a group of order p^3, with generators a,b,c and defining relations

$$a^p=b^p=c^p=1,\quad ab=cac^{-1},\quad [b,a]=1=[b,c].$$

Because $b\neq 1$, the group is not commutative. When p is odd, all elements except 1 have order p. When $p=2$, $G\approx D_4$. Note that this shows that a group can have quite different representations as a semidirect product:

$$D_4\overset{3.14a}{\approx}C_4\rtimes C_2\approx(C_2\times C_2)\rtimes C_2.$$

(e) Let $N=\langle a\rangle$ be cyclic of order p^2, and let $Q=\langle b\rangle$ be cyclic of order p, where p is an odd prime. Then $\operatorname{Aut}N\approx C_{p-1}\times C_p$ (see 3.10), and the generator of C_p is α where $\alpha(a)=a^{1+p}$ (hence $\alpha^2(a)=a^{1+2p},\ldots$). Define $Q\to\operatorname{Aut}N$ by $b\mapsto\alpha$. The group $G=_{df}N\rtimes_\theta Q$ has generators a,b and defining relations

$$a^{p^2}=1,\quad b^p=1,\quad bab^{-1}=a^{1+p}.$$

It is a nonabelian group of order p^3, and possesses an element of order p^2.

For an odd prime p, the groups constructed in (d) and (e) are the only nonabelian groups of order p^3 (see Exercise 21).

(f) Let α be an automorphism, possibly outer, of a group N. We can realize N as a normal subgroup of a group G in such a way that α becomes the restriction to N of an inner automorphism of G. To see this, let $\theta\colon C_\infty\to\operatorname{Aut}(N)$ be the homomorphism sending a generator a of C_∞ to $\alpha\in\operatorname{Aut}(N)$, and let $G=N\rtimes_\theta C_\infty$. Then the element $g=(1,a)$ of G has the property that $g(n,1)g^{-1}=(\alpha(n),1)$ for all $n\in N$.

The semidirect product $N\rtimes_\theta Q$ is determined by the triple

$$(N,Q,\theta\colon Q\to\operatorname{Aut}(N)).$$

It will be useful to have criteria for when two triples (N,Q,θ) and (N,Q,θ') determine isomorphic groups.

LEMMA 3.17. *If θ and θ' are conjugate, i.e., there exists an $\alpha\in\operatorname{Aut}(N)$ such that $\theta'(q)=\alpha\circ\theta(q)\circ\alpha^{-1}$ for all $q\in Q$, then*

$$N\rtimes_\theta Q\approx N\rtimes_{\theta'}Q.$$

PROOF. Consider the map

$$\gamma: N\rtimes_\theta Q\to N\rtimes_{\theta'}Q,\quad (n,q)\mapsto(\alpha(n),q).$$

Then

$$\begin{aligned}\gamma(n,q)\cdot\gamma(n',q') &= (\alpha(n),q)\cdot(\alpha(n'),q') \\ &= (\alpha(n)\cdot\theta'(q)(\alpha(n')),qq') \\ &= (\alpha(n)\cdot(\alpha\circ\theta(q)\circ\alpha^{-1})(\alpha(n')),qq') \\ &= (\alpha(n)\cdot\alpha(\theta(q)(n')),qq'),\end{aligned}$$

and

$$\begin{aligned}\gamma((n,q)\cdot(n',q')) &= \gamma(n\cdot\theta(q)(n'),qq') \\ &= (\alpha(n)\cdot\alpha\left(\theta(q)(n')\right),qq').\end{aligned}$$

Therefore γ is a homomorphism, with inverse $(n,q)\mapsto(\alpha^{-1}(n),q)$, and so is an isomorphism. □

LEMMA 3.18. *If $\theta=\theta'\circ\alpha$ with $\alpha\in\mathrm{Aut}(Q)$, then*

$$N\rtimes_{\theta}Q\approx N\rtimes_{\theta'}Q.$$

PROOF. The map $(n,q)\mapsto(n,\alpha(q))$ is an isomorphism $N\rtimes_{\theta}Q\to N\rtimes_{\theta'}Q$. □

LEMMA 3.19. *If Q is cyclic and the subgroup $\theta(Q)$ of $\mathrm{Aut}(N)$ is conjugate to $\theta'(Q)$, then*

$$N\rtimes_{\theta}Q\approx N\rtimes_{\theta'}Q.$$

PROOF. Let a generate Q. Then there exists an i and an $\alpha\in\mathrm{Aut}(N)$ such that

$$\theta'(a^{i})=\alpha\cdot\theta(a)\cdot\alpha^{-1}.$$

The map $(n,q)\mapsto(\alpha(n),q^{i})$ is an isomorphism $N\rtimes_{\theta}Q\to N\rtimes_{\theta'}Q$. □

Extensions of groups

A sequence of groups and homomorphisms

$$1\to N\xrightarrow{\iota}G\xrightarrow{\pi}Q\to 1$$

is ***exact*** if ι is injective, π is surjective, and $\mathrm{Ker}(\pi)=\mathrm{Im}(\iota)$. Thus $\iota(N)$ is a normal subgroup of G (isomorphic by ι to N) and $G/\iota(N)\xrightarrow{\approx}Q$. We often identify N with the subgroup $\iota(N)$ of G and Q with the quotient G/N.

An exact sequence as above is also referred to as an ***extension of*** Q ***by*** N. An extension is ***central*** if $\iota(N)\subset Z(G)$. For example,

$$1\to N\to N\rtimes_{\theta}Q\to Q\to 1$$

is an extension of N by Q, which is central if (and only if) θ is the trivial homomorphism.

Two extensions of Q by N are said to be ***isomorphic*** if there is a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, equal] & G \arrow[r] \arrow[d, "\approx"] & Q \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & N \arrow[r] & G' \arrow[r] & Q \arrow[r] & 1.
\end{tikzcd}$$

An extension

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1$$

is said to be ***split*** if it isomorphic to a semidirect product. Equivalent conditions:

(a) there exists a subgroup $Q' \subset G$ such that π induces an isomorphism $Q' \to Q$; or

(b) there exists a homomorphism $s\colon Q \to G$ such that $\pi \circ s = \mathrm{id}$.

In general, an extension will not split. For example (cf. 3.14c,d), the extensions

$$1 \to N \to Q \to Q/N \to 1$$

(N any subgroup of order 4 in the quaternion group Q) and

$$1 \to C_p \to C_{p^2} \to C_p \to 1$$

do not split. We list two criteria for an extension to split.

PROPOSITION 3.20 (SCHUR-ZASSENHAUS LEMMA). *An extension of finite groups of relatively prime order is split.*

PROOF. Rotman 1995, 7.41. □

PROPOSITION 3.21. *Let N be a normal subgroup of a group G. If N is complete, then G is the direct product of N with the centralizer of N in G,*

$$C_G(N) \overset{\text{df}}{=} \{g \in G \mid gn = ng \text{ all } n \in N\}.$$

PROOF. Let $Q = C_G(N)$. We shall check that N and Q satisfy the conditions of Proposition 3.6.

Observe first that, for any $g \in G$, $n \mapsto gng^{-1}\colon N \to N$ is an automorphism of N, and (because N is complete), it must be the inner automorphism defined by an element $\gamma = \gamma(g)$ of N; thus

$$gng^{-1} = \gamma n \gamma^{-1} \quad \text{all } n \in N.$$

This equation shows that $\gamma^{-1}g \in Q$, and hence $g = \gamma(\gamma^{-1}g) \in NQ$. Since g was arbitrary, we have shown that $G = NQ$.

Next note that every element of $N \cap Q$ is in the centre of N, which (by the completeness assumption) is trivial; hence $N \cap Q = 1$.

Finally, for any element $g = nq \in G$,

$$gQg^{-1} = n(qQq^{-1})n^{-1} = nQn^{-1} = Q$$

(recall that every element of N commutes with every element of Q). Therefore Q is normal in G. □

An extension

$$1 \to N \to G \to Q \to 1$$

gives rise to a homomorphism $\theta' \colon G \to \mathrm{Aut}(N)$, namely,

$$\theta'(g)(n) = gng^{-1}.$$

Let $\tilde{q} \in G$ map to q in Q; then the image of $\theta'(\tilde{q})$ in $\mathrm{Aut}(N)/\mathrm{Inn}(N)$ depends only on q; therefore we get a homomorphism

$$\theta : Q \to \mathrm{Out}(N) \overset{\text{df}}{=} \mathrm{Aut}(N)/\mathrm{Inn}(N).$$

This map θ depends only on the isomorphism class of the extension, and we write $\mathrm{Ext}^1(G,N)_\theta$ for the set of isomorphism classes of extensions with a given θ. These sets have been extensively studied.

The Hölder program.

Recall that a group G is simple if it contains no normal subgroup except 1 and G. In other words, a group is simple if it can't be realized as an extension of smaller groups. Every finite group can be obtained by taking repeated extensions of simple groups. Thus the simple finite groups can be regarded as the basic building blocks for all finite groups.

The problem of classifying all simple groups falls into two parts:

A. Classify all finite simple groups;

B. Classify all extensions of finite groups.

Part A has been solved: there is a complete list of finite simple groups. They are the cyclic groups of prime order, the alternating groups A_n for $n \geq 5$ (see the next section), certain infinite families of matrix groups, and the 26 "sporadic groups". As an example of a matrix group, consider

$$\mathrm{SL}_n(\mathbb{F}_q) =_{df} \{m \times m \text{ matrices } A \text{ with entries in } \mathbb{F}_q \text{ such that } \det A = 1\}.$$

Here $q = p^n$, p prime, and $\mathbb{F}_q$ is "the" field with q elements (see FT, Proposition 4.15). This group may not be simple, because the scalar matrices $\begin{pmatrix} \zeta & 0 & \cdots & 0 \\ 0 & \zeta & & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & \zeta \end{pmatrix}$, $\zeta^m = 1$, are in the centre. But these are the only matrices in centre, and the groups

$$\mathrm{PSL}_m(\mathbb{F}_q) \overset{\text{df}}{=} \mathrm{SL}_n(\mathbb{F}_q)/\{\text{centre}\}$$

are simple when $m \geq 3$ (Rotman 1995, 8.23) and when $m = 2$ and $q > 3$ (ibid. 8.13). For the case $m = 3$ and $q = 2$, see Exercise 24 (note that $\mathrm{PSL}_3(\mathbb{F}_2) \cong \mathrm{GL}_3(\mathbb{F}_2)$).

There are many results on Part B, and at least one expert has told me he considers it solved, but I'm sceptical.

For an historical introduction to the classification of finite simple groups, see Solomon, Ronald, A brief history of the classification of the finite simple groups, Bulletin AMS, 38 (2001), pp. 315–352. He notes (p347) regarding (B): "... the classification of all finite groups is completely infeasible. Nevertheless experience shows that most of the finite groups which occur in "nature" ... are "close" either to simple groups or to groups such as dihedral groups, Heisenberg groups, etc., which arise naturally in the study of simple groups."

Exercises 13–19

13. Let $D_n = \langle a, b | a^n, b^2, abab \rangle$ be the n^{th} dihedral group. If n is odd, prove that $D_{2n} \approx \langle a^n \rangle \times \langle a^2, b \rangle$, and hence that $D_{2n} \approx C_2 \times D_n$.

14*. Let G be the quaternion group (1.8c). Prove that G can't be written as a semidirect product in any nontrivial fashion.

15*. Let G be a group of order mn where m and n have no common factor. If G contains exactly one subgroup M of order m and exactly one subgroup N of order n, prove that G is the direct product of M and N.

16*. Prove that $\mathrm{GL}_2(\mathbb{F}_2) \approx S_3$.

17. Let G be the quaternion group (1.8c). Prove that $\mathrm{Aut}(G) \approx S_4$.

18*. Let G be the set of all matrices in $\mathrm{GL}_3(\mathbb{R})$ of the form $\left(\begin{smallmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & d \end{smallmatrix}\right)$, $ad \neq 0$. Check that G is a subgroup of $\mathrm{GL}_3(\mathbb{R})$, and prove that it is a semidirect product of $\mathbb{R}^2$ (additive group) by $\mathbb{R}^\times \times \mathbb{R}^\times$. Is it a direct product of these two groups?

19. Find the automorphism groups of C_∞ and S_3.

4 Groups Acting on Sets

General definitions and results

DEFINITION 4.1. Let X be a set and let G be a group. A ***left action*** of G on X is a mapping $(g,x) \mapsto gx\colon G \times X \to X$ such that

(a) $1x = x$, for all $x \in X$;

(b) $(g_1g_2)x = g_1(g_2x)$, all g_1, $g_2 \in G$, $x \in X$.

A set together with a (left) action of G is called a (left) G***-set***.

The axioms imply that, for each $g \in G$, left translation by g,

$$g_L\colon X \to X, \quad x \mapsto gx,$$

has $(g^{-1})_L$ as an inverse, and therefore g_L is a bijection, i.e., $g_L \in \mathrm{Sym}(X)$. Axiom (b) now says that

$$g \mapsto g_L\colon G \to \mathrm{Sym}(X)$$

is a homomorphism. Thus, from a left action of G on X, we obtain a homomorphism $G \to \mathrm{Sym}(X)$, and, conversely, every such homomorphism defines an action of G on X.

EXAMPLE 4.2. (a) The symmetric group S_n acts on $\{1, 2, ..., n\}$. Every subgroup H of S_n acts on $\{1, 2, \ldots, n\}$.

(b) Every subgroup H of a group G acts on G by left translation,

$$H \times G \to G, \quad (h,x) \mapsto hx.$$

(c) Let H be a subgroup of G. If C is a left coset of H in G, then so also is gC for any $g \in G$. In this way, we get an action of G on the set of left cosets:

$$G \times G/H \to G/H, \quad (g,C) \mapsto gC.$$

(d) Every group G acts on itself by conjugation:

$$G \times G \to G, \quad (g,x) \mapsto {}^{g}x =_{df} gxg^{-1}.$$

For any normal subgroup N, G acts on N and G/N by conjugation.

(e) For any group G, $\mathrm{Aut}(G)$ acts on G.

A ***right action*** $X \times G \to G$ is defined similarly. To turn a right action into a left action, set $g * x = xg^{-1}$. For example, there is a natural right action of G on the set of right cosets of a subgroup H in G, namely, $(C,g) \mapsto Cg$, which can be turned into a left action $(g,C) \mapsto Cg^{-1}$.

A ***morphism*** of G-sets (better G***-map***; G***-equivariant map***) is a map $\varphi\colon X \to Y$ such that

$$\varphi(gx) = g\varphi(x), \quad \text{all } g \in G, \quad x \in X.$$

An ***isomorphism*** of G-sets is a bijective G-map; its inverse is then also a G-map.

Orbits

Let G act on X. A subset $S \subset X$ is said to be ***stable*** under the action of G if

$$g \in G, \quad x \in S \Rightarrow gx \in S.$$

The action of G on X then induces an action of G on S.

Write $x \sim_G y$ if $y = gx$, some $g \in G$. This relation is reflexive because $x = 1x$, symmetric because

$$y = gx \Rightarrow x = g^{-1}y$$

(multiply by g^{-1} on the left and use the axioms), and transitive because

$$y = gx, \quad z = g'y \Rightarrow z = g'(gx) = (g'g)x.$$

It is therefore an equivalence relation. The equivalence classes are called G-***orbits***. Thus the G-orbits partition X. Write $G\backslash X$ for the set of orbits.

By definition, the G-orbit containing x_0 is

$$Gx_0 = \{gx_0 \mid g \in G\}.$$

It is the smallest G-stable subset of X containing x_0.

EXAMPLE 4.3. (a) Suppose G acts on X, and let $\alpha \in G$ be an element of order n. Then the orbits of $\langle\alpha\rangle$ are the sets of the form

$$\{x_0, \alpha x_0, \dots, \alpha^{n-1}x_0\}.$$

(These elements need not be distinct, and so the set may contain fewer than n elements.)

(b) The orbits for a subgroup H of G acting on G by left multiplication are the right cosets of H in G. We write $H\backslash G$ for the set of right cosets. Similarly, the orbits for H acting by right multiplication are the left cosets, and we write G/H for the set of left cosets. Note that the group law on G will *not* induce a group law on G/H unless H is normal.

(c) For a group G acting on itself by conjugation, the orbits are called ***conjugacy classes:*** for $x \in G$, the conjugacy class of x is the set

$$\{gxg^{-1} \mid g \in G\}$$

of conjugates of x. The conjugacy class of x_0 consists only of x_0 if and only if x_0 is in the centre of G. In linear algebra the conjugacy classes in $G = \mathrm{GL}_n(k)$ are called similarity classes, and the theory of (rational) Jordan canonical forms provides a set of representatives for the conjugacy classes: two matrices are similar (conjugate) if and only if they have essentially the same Jordan canonical form.

Note that a subset of X is stable if and only if it is a union of orbits. For example, a subgroup H of G is normal if and only if it is a union of conjugacy classes.

The group G is said to act ***transitively*** on X if there is only one orbit, i.e., for any two elements x and y of X, there exists a $g \in G$ such that $gx = y$.

For example, S_n acts transitively on $\{1, 2, ...n\}$. For any subgroup H of a group G, G acts transitively on G/H. But G (almost) never acts transitively on G (or G/N or N) by conjugation.

The group G acts ***doubly transitively*** on X if for any two pairs (x, x'), (y, y') of elements of X with $x \neq x'$ and $y \neq y'$, there exists a (single) $g \in G$ such that $gx = y$ and $gx' = y'$. Define k-***fold transitivity***, $k \geq 3$, similarly.

Stabilizers

The ***stabilizer*** (or ***isotropy group***) of an element $x \in X$ is

$$\mathrm{Stab}(x) = \{g \in G \mid gx = x\}.$$

It is a subgroup, but it need not be a normal subgroup. In fact:

LEMMA 4.4. *If* $y = gx$, *then* $\mathrm{Stab}(y) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}$.

PROOF. Certainly, if $g'x = x$, then

$$(gg'g^{-1})y = gg'x = gx = y.$$

Hence $\mathrm{Stab}(y) \supset g \cdot \mathrm{Stab}(x) \cdot g^{-1}$. Conversely, if $g'y = y$, then

$$(g^{-1}g'g)x = g^{-1}g'(y) = g^{-1}y = x,$$

and so $g^{-1}g'g \in \mathrm{Stab}(x)$, i.e., $g' \in g \cdot \mathrm{Stab}(x) \cdot g^{-1}$. □

Clearly

$$\bigcap_{x \in X} \mathrm{Stab}(x) = \mathrm{Ker}(G \to \mathrm{Sym}(X)),$$

which is a normal subgroup of G. If $\bigcap \mathrm{Stab}(x) = \{1\}$, i.e., $G \hookrightarrow \mathrm{Sym}(X)$, then G is said to act ***effectively*** (or ***faithfully***). It acts ***freely*** if $\mathrm{Stab}(x) = 1$ for all $x \in X$, i.e., if $gx = x \Rightarrow g = 1$.

EXAMPLE 4.5. (a) Let G act on G by conjugation. Then

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

This group is called the ***centralizer*** $C_G(x)$ of x in G. It consists of all elements of G that commute with, i.e., centralize, x. The intersection

$$\bigcap_{x \in X} C_G(x) = \{g \in G \mid gx = xg \quad \forall x \in G\}$$

is a normal subgroup of G, called the ***centre*** $Z(G)$ of G. It consists of the elements of G that commute with every element of G.

(b) Let G act on G/H by left multiplication. Then $\mathrm{Stab}(H) = H$, and the stabilizer of gH is gHg^{-1}.

For a subset S of X, we define the ***stabilizer*** of S to be

$$\mathrm{Stab}(S) = \{g \in G \mid gS = S\}.$$

The same argument as in the proof of (4.4) shows that

$$\mathrm{Stab}(gS) = g \cdot \mathrm{Stab}(S) \cdot g^{-1}.$$

EXAMPLE 4.6. Let G act on G by conjugation, and let H be a subgroup of G. The stabilizer of H is called the ***normalizer*** $N_G(H)$ of H in G:

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Clearly $N_G(H)$ is the largest subgroup of G containing H as a normal subgroup.

ASIDE. In Example 1.21, the element $g \notin N_G(H)$ even though $gHg^{-1} \subset H$.

Transitive actions

PROPOSITION 4.7. *Suppose G acts transitively on X, and let $x_0 \in X$; then*

$$gH \mapsto gx_0 : G/\operatorname{Stab}(x_0) \to X$$

is an isomorphism of G-sets.

PROOF. It is well-defined because if $h, h' \in \operatorname{Stab}(x_0)$, then $ghx_0 = gx_0 = gh'x_0$ for any $g \in G$. It is injective because

$$gx_0 = g'x_0 \Rightarrow g^{-1}g'x_0 = x_0 \Rightarrow g, g' \text{ lie in the same left coset of } \operatorname{Stab}(x_0).$$

It is surjective because G acts transitively. Finally, it is obviously G-equivariant. □

The isomorphism is *not canonical*: it depends on the choice of $x_0 \in X$. Thus to give a transitive action of G on a set X is ***not*** the same as to give a subgroup of G.

COROLLARY 4.8. *Let G act on X, and let $O = Gx_0$ be the orbit containing x_0. Then the number of elements in O is*

$$\#O = (G : \operatorname{Stab}(x_0)).$$

For example, the number of conjugates gHg^{-1} of a subgroup H of G is $(G\colon N_G(H))$.

PROOF. The action of G on O is transitive, and so $g \mapsto gx_0$ defines a bijection $G/\operatorname{Stab}(x_0) \to Gx_0$. □

This equation is frequently useful for computing $\#O$.

PROPOSITION 4.9. *If G acts transitively on X, then, for any $x_0 \in X$,*

$$\operatorname{Ker}(G \to \operatorname{Sym}(X))$$

is the largest normal subgroup contained in $\operatorname{Stab}(x_0)$.

PROOF. Let $x_0 \in X$. Then

$$\operatorname{Ker}(G \to \operatorname{Sym}(X)) = \bigcap_{x \in X} \operatorname{Stab}(x) = \bigcap_{g \in G} \operatorname{Stab}(gx_0) \overset{4.4}{=} \bigcap g \cdot \operatorname{Stab}(x_0) \cdot g^{-1}.$$

Hence, the proposition is a consequence of the following lemma. □

LEMMA 4.10. *For any subgroup H of a group G, $\bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup contained in H.*

PROOF. Note that $N_0 =_{df} \bigcap_{g \in G} gHg^{-1}$, being an intersection of subgroups, is itself a subgroup. It is normal because

$$g_1 N_0 g_1^{-1} = \bigcap_{g \in G} (g_1 g) N_0 (g_1 g)^{-1} = N_0$$

— for the second equality, we used that, as g runs over the elements of G, so also does $g_1 g$. Thus N_0 is a normal subgroup of G contained in $1H1^{-1} = H$. If N is a second such group, then

$$N = gNg^{-1} \subset gHg^{-1}$$

for all $g \in G$, and so

$$N \subset \bigcap_{g \in G} gHg^{-1} = N_0. \qquad \square$$

The class equation

When X is finite, it is a disjoint union of a finite number of orbits:

$$X = \bigcup_{i=1}^{m} O_i \qquad \text{(disjoint union).}$$

Hence:

PROPOSITION 4.11. *The number of elements in X is*

$$\#X = \sum_{i=1}^{m} \#O_i = \sum_{i=1}^{m} (G : \mathrm{Stab}(x_i)), \quad x_i \textit{ in } O_i.$$

When G acts on itself by conjugation, this formula becomes:

PROPOSITION 4.12 (CLASS EQUATION).

$$(G : 1) = \sum (G : C_G(x))$$

(x runs over a set of representatives for the conjugacy classes), or

$$(G : 1) = (Z(G) : 1) + \sum (G : C_G(y))$$

(y runs over set of representatives for the conjugacy classes containing more than one element).

THEOREM 4.13 (CAUCHY). *If the prime p divides $(G : 1)$, then G contains an element of order p.*

PROOF. We use induction on $(G : 1)$. If for some y not in the centre of G, p does not divide $(G : C_G(y))$, then $p|C_G(y)$ and we can apply induction to find an element of order p in $C_G(y)$. Thus we may suppose that p divides all of the terms $(G : C_G(y))$ in the class equation (second form), and so also divides $Z(G)$. But $Z(G)$ is commutative, and it follows from the structure theorem[12] of such groups that $Z(G)$ will contain an element of order p. □

[12] Here is a direct proof that the theorem holds for an abelian group Z. We use induction on the order of Z. It suffices to show that Z contains an element whose order is divisible by p, for then some power of the element will have order exactly p. Let $g \neq 1$ be an element of Z. Either p divides the order of g, or (by induction) there is an element of h of Z whose order in $Z/\langle g \rangle$ is divisible by p. In the second case, the order of h itself must be divisible by p.

COROLLARY 4.14. *Any group of order $2p$, p an odd prime, is cyclic or dihedral.*

PROOF. From Cauchy's theorem, we know that such a G contains elements τ and σ of orders 2 and p respectively. Let $H = \langle\sigma\rangle$. Then H is of index 2, and so is normal. Obviously $\tau \notin H$, and so $G = H \cup H\tau$:

$$G = \{1, \sigma, \ldots, \sigma^{p-1}, \tau, \sigma\tau, \ldots, \sigma^{p-1}\tau\}.$$

As H is normal, $\tau\sigma\tau^{-1} = \sigma^i$, some i. Because $\tau^2 = 1$, $\sigma = \tau^2\sigma\tau^{-2} = \tau(\tau\sigma\tau^{-1})\tau^{-1} = \sigma^{i^2}$, and so $i^2 \equiv 1 \bmod p$. The only elements of $\mathbb{F}_p$ with square 1 are ± 1, and so $i \equiv 1$ or -1 mod p. In the first case, the group is commutative (any group generated by a set of commuting elements is obviously commutative); in the second $\tau\sigma\tau^{-1} = \sigma^{-1}$ and we have the dihedral group (2.10). □

p-groups

THEOREM 4.15. *A finite p-group $\neq 1$ has centre $\neq \{1\}$.*

PROOF. By assumption, $(G : 1)$ is a power of p, and it follows that $(G : C_G(y))$ is power of p ($\neq p^0$) for all y in the class equation (second form). Since p divides every term in the class equation except (perhaps) $(Z(G) : 1)$, it must divide $(Z(G) : 1)$ also. □

COROLLARY 4.16. *A group of order p^m has normal subgroups of order p^n for all $n \leq m$.*

PROOF. We use induction on m. The centre of G contains an element g of order p, and so $N = \langle g\rangle$ is a normal subgroup of G of order p. Now the induction hypothesis allows us to assume the result for G/N, and the correspondence theorem (3.3) then gives it to us for G. □

PROPOSITION 4.17. *A group of order p^2 is commutative, and hence is isomorphic to $C_p \times C_p$ or C_{p^2}.*

PROOF. We know that the centre Z is nontrivial, and that G/Z therefore has order 1 or p. In either case it is cyclic, and the next result implies that G is commutative. □

LEMMA 4.18. *Suppose G contains a subgroup H in its centre (hence H is normal) such that G/H is cyclic. Then G is commutative.*

PROOF. Let $a \in G$ be such that aH generates G/H, so that $G/H = \{(aH)^i \mid i \in \mathbb{Z}\}$. Since $(aH)^i = a^iH$, we see that every element of G can be written $g = a^ih$ with $h \in H$, $i \in \mathbb{Z}$. Now

$$\begin{aligned} a^ih \cdot a^{i'}h' &= a^ia^{i'}hh' && \text{because } H \subset Z(G) \\ &= a^{i'}a^ih'h \\ &= a^{i'}h' \cdot a^ih. \end{aligned}$$

□

REMARK 4.19. The above proof shows that if $H \subset Z(G)$ and G contains a set of representatives for G/H whose elements commute, then G is commutative.

It is now not difficult to show that any noncommutative group of order p^3 is isomorphic to exactly one of the groups constructed in (3.16d,e) (Exercise 21). Thus, up to isomorphism, there are exactly two noncommutative groups of order p^3.

Action on the left cosets

The action of G on the set of left cosets G/H of H in G is a very useful tool in the study of groups. We illustrate this with some examples.

Let $X = G/H$. Recall that, for any $g \in G$,

$$\operatorname{Stab}(gH) = g \operatorname{Stab}(H) g^{-1} = gHg^{-1}$$

and the kernel of

$$G \to \operatorname{Sym}(X)$$

is the largest normal subgroup $\bigcap_{g \in G} gHg^{-1}$ of G contained in H.

REMARK 4.20. (a) Let H be a subgroup of G not containing a normal subgroup of G other than 1. Then $G \to \operatorname{Sym}(G/H)$ is injective, and we have realized G as a subgroup of a symmetric group of order much smaller than $(G : 1)!$. For example, if G is simple, then the Sylow theorems imply that G has many proper subgroups $H \neq 1$ (unless G is cyclic), but (by definition) it has no such normal subgroup.

(b) If $(G : 1)$ does not divide $(G : H)!$, then

$$G \to \operatorname{Sym}(G/H)$$

can't be injective (Lagrange's theorem, 1.15), and we can conclude that H contains a normal subgroup $\neq 1$ of G. For example, if G has order 99, then it will have a subgroup N of order 11 (Cauchy's theorem, 4.13), and the subgroup must be normal. In fact, $G = N \times Q$.

EXAMPLE 4.21. Corollary 4.14 shows that every group G of order 6 is either cyclic or dihedral. Here we present a slightly different argument. According to Cauchy's theorem (4.13), G must contain an element σ of order 3 and an element τ of order 2. Moreover $N =_{\text{df}} \langle \sigma \rangle$ must be normal because 6 doesn't divide $2!$ (or simply because it has index 2). Let $H = \langle \tau \rangle$.

Either (a) H is normal in G, or (b) H is not normal in G. In the first case, $\sigma\tau\sigma^{-1} = \tau$, i.e., $\sigma\tau = \tau\sigma$, and so (4.18) shows that G is commutative, $G \approx C_2 \times C_3$. In the second case, $G \to \operatorname{Sym}(G/H)$ is injective, hence surjective, and so $G \approx S_3$.

Permutation groups

Consider $\operatorname{Sym}(X)$ where X has n elements. Since (up to isomorphism) a symmetry group $\operatorname{Sym}(X)$ depends only on the number of elements in X, we may take $X = \{1, 2, \ldots, n\}$, and so work with[13] S_n. Consider a permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \ldots & \alpha(n) \end{pmatrix}.$$

Then α is said to be ***even*** or ***odd*** according as the number of pairs (i, j) with $i < j$ and $\alpha(i) > \alpha(j)$ is even or odd. The ***signature***, $\operatorname{sign}(\alpha)$**,** of α is $+1$ or -1 according as α is even or odd.

[13] We, of course, define multiplication in S_n to be composition; other authors (see, for example, Artin 1991) write things backwards.

ASIDE: To compute the signature of α, connect (by a line) each element i in the top row to the element i in the bottom row, and count the number of times the lines cross: α is even or odd according as this number is even or odd. For example,

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

is even (6 intersections).

For any polynomial $F(X_1, ..., X_n)$ and permutation α of $\{1, \ldots, n\}$, define

$$(\alpha F)(X_1, ..., X_n) = F(X_{\alpha(1)}, ..., X_{\alpha(n)}),$$

i.e., αF is obtained from F by replacing each X_i with $X_{\alpha(i)}$. Note that

$$(\alpha\beta F)(X_1, ..., X_n) = F(X_{\alpha\beta(1)}, \ldots) = F(X_{\alpha(\beta(1))}, \ldots) = (\alpha(\beta F))(X_1, ..., X_n).$$

Let $G(X_1, ..., X_n) = \prod_{i<j}(X_j - X_i)$. Then

$$(\alpha G)(X_1, ..., X_n) = \prod_{i<j}(X_{\alpha(j)} - X_{\alpha(i)}).$$

Hence $\alpha G = \text{sign}(\alpha) \cdot G$. Since this holds for all α, $(\alpha\beta)G = \text{sign}(\alpha\beta)G$, but

$$(\alpha\beta)G = \alpha(\beta G) = \alpha(\text{sign}(\beta)G) = \text{sign}\,\beta(\alpha G) = \text{sign}(\alpha)\,\text{sign}(\beta)G.$$

Hence

$$\text{sign}(\alpha\beta) = (\text{sign}\,\alpha)\,(\text{sign}\,\beta)\,,$$

and we have shown that "sign" is a homomorphism $S_n \rightarrow \{\pm 1\}$. When $n \geq 2$, it is surjective, and so its kernel is a normal subgroup of S_n of order $\frac{n!}{2}$, called the ***alternating group*** A_n.

A ***cycle*** is a permutation of the following form

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1, \quad \text{remaining } i\text{'s fixed.}$$

The i_j are required to be distinct. We denote this cycle by $(i_1 i_2 ... i_r)$, and call r its ***length*** — note that r is also its order. A cycle of length 2 is called a ***transposition.*** A cycle (i) of length 1 is the identity map. The ***support of the cycle*** $(i_1 \ldots i_r)$ is the set $\{i_1, \ldots, i_r\}$, and cycles are said to be ***disjoint*** if their supports are disjoint. Note that disjoint cycles commute. If

$$\alpha = (i_1 ... i_r)(j_1 ... j_s) \cdots (l_1 ... l_u) \qquad \text{(disjoint cycles)},$$

then

$$\alpha^m = (i_1 ... i_r)^m (j_1 ... j_s)^m \cdots (l_1 ... l_u)^m \qquad \text{(disjoint cycles)},$$

and it follows that α has order lcm$(r, s, ..., u)$.

PROPOSITION 4.22. *Every permutation can be written (in essentially one way) as a product of disjoint cycles.*

PROOF. Let $\alpha \in S_n$, and let $O \subset \{1, 2, \ldots, n\}$ be an orbit for $\langle\alpha\rangle$. If $\#O = r$, then for any $i \in O$,

$$O = \{i, \alpha(i), \ldots, \alpha^{r-1}(i)\}.$$

Therefore α and the cycle $(i\,\alpha(i)\ \ldots\ \alpha^{r-1}(i))$ have the same action on any element of O. Let

$$\{1, 2, \ldots, n\} = \bigcup_{j=1}^{m} O_j$$

be a the decomposition of $\{1, \ldots, n\}$ into a disjoint union of orbits for $\langle\alpha\rangle$, and let γ_j be the cycle associated (as above) with O_j. Then

$$\alpha = \gamma_1 \cdots \gamma_m$$

is a decomposition of α into a product of disjoint cycles. For the uniqueness, note that a decomposition $\alpha = \gamma_1 \cdots \gamma_m$ into a product of disjoint cycles must correspond to a decomposition of $\{1, ..., n\}$ into orbits (ignoring cycles of length 1 and orbits with only one element). We can drop cycles of length one, change the order of the cycles, and change how we write each cycle (by choosing different initial elements), but that's all because the orbits are intrinsically attached to α. □

For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 4 & 2 & 1 & 3 & 6 & 8 \end{pmatrix} = (15)(27634)(8).$$

It has order $\mathrm{lcm}(2, 5) = 10$.

COROLLARY 4.23. *Each permutation α can be written as a product of transpositions; the number of transpositions in such a product is even or odd according as α is even or odd.*

PROOF. The cycle

$$(i_1 i_2 ... i_r) = (i_1 i_2) \cdots (i_{r-2} i_{r-1})(i_{r-1} i_r),$$

and so the first statement follows from the proposition. Because sign is a homomorphism, and the signature of a transposition is -1, $\mathrm{sign}(\alpha) = (-1)^{\#\text{transpositions}}$. □

Note that the formula in the proof shows that the signature of a cycle of length r is $(-1)^{r-1}$, that is, an r-cycle is even or odd according as r is odd or even.

It is possible to define a permutation to be even or odd according as it is a product of an even or odd number of transpositions, but then one has to go through an argument as above to show that this is a well-defined notion.

The corollary says that S_n is generated by transpositions. For A_n there is the following result.

COROLLARY 4.24. *The alternating group A_n is generated by cycles of length three.*

PROOF. Any $\alpha \in A_n$ is the product of an even number of transpositions, $\alpha = t_1 t_1' \cdots t_m t_m'$, but the product of two transpositions can always be written as a product of 3-cycles:

$$(ij)(kl) = \begin{cases} (ij)(jl) = (ijl) & \text{case } j = k, \\ (ij)(jk)(jk)(kl) = (ijk)(jkl) & \text{case } i, j, k, l \text{ distinct}, \\ 1 & \text{case } (ij) = (kl). \end{cases}$$

□

Recall that two elements a and b of a group G are said to be conjugate $a \sim b$ if there exists an element $g \in G$ such that $b = gag^{-1}$, and that conjugacy is an equivalence relation. For any group G, it is useful to determine the conjugacy classes in G.

EXAMPLE 4.25. In S_n, the conjugate of a cycle is given by:

$$g(i_1 \ldots i_k)g^{-1} = (g(i_1) \ldots g(i_k)).$$

Hence $g(i_1 \ldots i_r)(j_1 \ldots j_s) \ldots (l_1 \ldots l_u)g^{-1} = (g(i_1) \ldots g(i_r))(g(j_1) \ldots g(j_s)) \ldots (g(l_1)...g(l_u))$ (even if the cycles are not disjoint). In other words, to obtain $g\alpha g^{-1}$, replace each element in a cycle of α be its image under g.

We shall now determine the conjugacy classes in S_n. By a ***partition*** of n, we mean a sequence of integers $n_1, \ldots, n_k$ such that $1 \leq n_i \leq n_{i+1} \leq n$ (all i) and

$$n_1 + n_2 + \cdots + n_k = n.$$

Thus there are $1,\ 2,\ 3,\ 5,\ 7,\ 11, \ldots$ partitions of $1,\ 2,\ 3,\ 4,\ 5,\ 6, \ldots$ respectively (and $1, 121, 505$ partitions of 61). Note that a partition

$$\{1, 2, ..., n\} = O_1 \cup ... \cup O_k \qquad \text{(disjoint union)}$$

of $\{1, 2, \ldots, n\}$ determines a partition of n,

$$n = n_1 + n_2 + ... + n_k, \quad n_i = \# O_i.$$

Since the orbits of an element α of S_n form a partition of $\{1, \ldots, n\}$, we can attach to each such α a partition of n. For example, if

$$\alpha = (i_1 \ldots i_{n_1}) \cdots (l_1 \ldots l_{n_k}), \quad \text{(disjoint cycles)} \quad 1 < n_i \leq n_{i+1},$$

then the partition of n attached to α is

$$1, 1, \ldots, 1, n_1, \ldots, n_k \qquad (n - \textstyle\sum n_i \text{ ones}).$$

PROPOSITION 4.26. *Two elements α and β of S_n are conjugate if and only if they define the same partitions of n.*

PROOF. $\Longrightarrow$: We saw in (4.25) that conjugating an element preserves the type of its disjoint cycle decomposition.

$\Longleftarrow$: Since α and β define the same partitions of n, their decompositions into products of disjoint cycles have the same type:

$$\alpha = (i_1 \dots i_r)(j_1 \dots j_s) \dots (l_1 \dots l_u),$$

$$\beta = (i'_1 \dots i'_r)(j'_1 \dots j'_s) \dots (l'_1 \dots l'_u).$$

If we define g to be

$$\begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_s & \cdots & l_1 & \cdots & l_u \\ i'_1 & \cdots & i'_r & j'_1 & \cdots & j'_s & \cdots & l'_1 & \cdots & l'_u \end{pmatrix},$$

then

$$g\alpha g^{-1} = \beta. \qquad \square$$

EXAMPLE 4.27. $(ijk) = \binom{1234\dots}{ijk4\dots}(123)\binom{1234\dots}{ijk4\dots}^{-1}$.

REMARK 4.28. For $1 < k \leq n$, there are $\frac{n(n-1)\cdots(n-k+1)}{k}$ distinct k-cycles in S_n. The $\frac{1}{k}$ is needed so that we don't count

$$(i_1 i_2 \dots i_k) = (i_k i_1 \dots i_{k-1}) = \dots$$

k times. Similarly, it is possible to compute the number of elements in any conjugacy class in S_n, but a little care is needed when the partition of n has several terms equal. For example, the number of permutations in S_4 of type $(ab)(cd)$ is

$$\frac{1}{2}\left(\frac{4\times 3}{2} \times \frac{2\times 1}{2}\right) = 3.$$

The $\frac{1}{2}$ is needed so that we don't count $(ab)(cd) = (cd)(ab)$ twice. For S_4 we have the following table:

Partition	Element	No. in Conj. Class	Parity
$1+1+1+1$	1	1	even
$1+1+2$	(ab)	6	odd
$1+3$	(abc)	8	even
$2+2$	$(ab)(cd)$	3	even
4	$(abcd)$	6	odd

Note that A_4 contains exactly 3 elements of order 2, namely those of type $2+2$, and that together with 1 they form a subgroup V. This group is a union of conjugacy classes, and is therefore a normal subgroup of S_4.

THEOREM 4.29 (GALOIS). *The group A_n is simple if $n \geq 5$*

REMARK 4.30. For $n = 2$, A_n is trivial, and for $n = 3$, A_n is cyclic of order 3, and hence simple; for $n = 4$ it is nonabelian and nonsimple (it contains the normal, even characteristic, subgroup V — see above).

LEMMA 4.31. *Let N be a normal subgroup of A_n ($n \geq 5$); if N contains a cycle of length three, then it contains all cycles of length three, and so equals A_n (by 4.24).*

PROOF. Let γ be the cycle of length three in N, and let α be a second cycle of length three in A_n. We know from (4.26) that $\alpha = g\gamma g^{-1}$ for some $g \in S_n$. If $g \in A_n$, then this shows that α is also in N. If not, because $n \geq 5$, there exists a transposition $t \in S_n$ disjoint from α. Then $tg \in A_n$ and

$$\alpha = t\alpha t^{-1} = tg\gamma g^{-1}t^{-1},$$

and so again $\alpha \in N$. □

The next lemma completes the proof of the Theorem.

LEMMA 4.32. *Every normal subgroup N of A_n, $n \geq 5$, $N \neq 1$, contains a cycle of length 3.*

PROOF. Let $\alpha \in N$, $\alpha \neq 1$. If α is not a 3-cycle, we shall construct another element $\alpha' \in N$, $\alpha' \neq 1$, which fixes more elements of $\{1, 2, \ldots, n\}$ than does α. If α' is not a 3-cycle, then we can apply the same construction. After a finite number of steps, we arrive at a 3-cycle.

Suppose α is not a 3-cycle. When we express it as a product of disjoint cycles, either it contains a cycle of length ≥ 3 or else it is a product of transpositions, say

(i) $\alpha = (i_1 i_2 i_3 ...) \cdots$ or
(ii) $\alpha = (i_1 i_2)(i_3 i_4) \cdots$.

In the first case, α moves two numbers, say i_4, i_5, other than i_1, i_2, i_3, because $\alpha \neq (i_1 i_2 i_3)$, $(i_1 \ldots i_4)$. Let $\gamma = (i_3 i_4 i_5)$. Then $\alpha_1 =_{df} \gamma\alpha\gamma^{-1} = (i_1 i_2 i_4 \ldots) \cdots \in N$, and is distinct from α (because it acts differently on i_2). Thus $\alpha' =_{df} \alpha_1 \alpha^{-1} \neq 1$, but $\alpha' = \gamma\alpha\gamma^{-1}\alpha^{-1}$ fixes i_2 and all elements other than $i_1, ..., i_5$ fixed by α — it therefore fixes more elements than α.

In the second case, form γ, α_1, α' as in the first case with i_4 as in (ii) and i_5 any element distinct from i_1, i_2, i_3, i_4. Then $\alpha_1 = (i_1 i_2)(i_4 i_5) \cdots$ is distinct from α because it acts differently on i_4. Thus $\alpha' = \alpha_1 \alpha^{-1} \neq 1$, but α' fixes i_1 and i_2, and all elements $\neq i_1, ..., i_5$ not fixed by α — it therefore fixes at least one more element than α. □

COROLLARY 4.33. *For $n \geq 5$, the only normal subgroups of S_n are 1, A_n, and S_n.*

PROOF. If N is normal in S_n, then $N \cap A_n$ is normal in A_n. Therefore either $N \cap A_n = A_n$ or $N \cap A_n = \{1\}$. In the first case, $N \supset A_n$, which has index 2 in S_n, and so $N = A_n$ or S_n. In the second case, the map $x \mapsto xA_n \colon N \to S_n/A_n$ is injective, and so N has order 1 or 2, but it can't have order 2 because no conjugacy class in S_n (other than $\{1\}$) consists of a single element. □

REMARK 4.34. A group G is said to be ***solvable*** if there exist subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset G_3 \supset \cdots \supset G_r = \{1\}$$

such that each G_i is normal in G_{i-1} and each quotient G_{i-1}/G_i is commutative. Thus A_n (also S_n) is not solvable if $n \geq 5$.

Let $f(X) \in \mathbb{Q}[X]$ be of degree n. In FT, §3, we attach to f a subgroup of the group of permutations of the roots of f, $G_f \subset S_n$, and we show that the roots of f can be obtained from the coefficients of f by extracting radicals if and only if G_f is solvable (ibid. 5.23). For every n, there exist (lots of) polynomials f of degree n with $G_f = S_n$.

The Todd-Coxeter algorithm.

Let G be a group described by a finite presentation, and let H be a subgroup described by a generating set. Then the Todd-Coxeter algorithm[14] is a strategy for writing down the set of left cosets of H in G together with the action of G on the set. I illustrate it with an example (from Artin 1991, 6.9, which provides more details, but note that he composes permutations backwards).

Let $G = \langle a, b, c | a^3, b^2, c^2, cba \rangle$ and let H be the subgroup generated by c (strictly speaking, H is the subgroup generated by the element of G represented by the reduced word c). The operation of G on the set of cosets is described by the action of the generators, which must satisfy the following rules:

(i) Each generator (a, b, c in our example) acts as a permutation.

(ii) The relations (a^3, b^2, c^2, cba in our example) act trivially.

(iii) The generators of H (c in our example) fix the coset $1H$.

(iv) The operation on the cosets is transitive.

The strategy is to introduce cosets, denoted $1, 2, \ldots$ with $1 = 1H$, as necessary.

Rule (iii) tells us simply that $c1 = c$. We now apply the first two rules. Since we don't know what $a1$ is, let's denote it 2: $a1 = 2$. Similarly, let $a2 = 3$. Now $a3 = a^3 1$, which according to (ii) must be 1. Thus, we have introduced three (potential) cosets 1, 2, 3, permuted by a as follows:

$$1 \overset{a}{\mapsto} 2 \overset{a}{\mapsto} 3 \overset{a}{\mapsto} 1.$$

What is $b1$? We don't know, and so it is prudent to introduce another coset $4 = b1$. Now $b4 = 1$, and so we have

$$1 \overset{b}{\mapsto} 4 \overset{b}{\mapsto} 1.$$

We still have the relation cba. We know $a1 = 2$, but we don't know what $b2$ is, and so set $b2 = 5$. By (iii) $c1 = 1$, and by (ii) applied to cba we have $c5 = 1$. Therefore, according to (i) we must have $5 = 1$; we drop 5, and so now $b2 = 1$. Since $b4 = 1$ we must have $4 = 2$, and so we can drop 4 also. What we know can be summarized by the table:

	a		a		a		b		b		c		c		a		b		c	
1		2		3		**1**		2		**1**		1		**1**		2		1		**1**
2		3		1		**2**		1		**2**				**2**		3				**2**
3		1		2		**3**				**3**				**3**		1		2		**3**

[14] To solve a problem, an algorithm must always terminate in a finite time with the correct answer to the problem. The Todd-Coxeter algorithm does not solve the problem of determining whether a finite presentation defines a finite group (in fact, there is no such algorithm). It does, however, solve the problem of determining the order of a finite group from a finite presentation of the group (use the algorithm with H the trivial subgroup 1.)

The bottom right corner, which is forced by (ii), tells us that $c2 = 3$. Hence also $c3 = 2$, and this then determines the rest of the table:

	a	a	a	b	b	c	c	a	b	c
1	2	3	**1**	2	**1**	1	**1**	2	1	**1**
2	3	1	**2**	1	**2**	3	**2**	3	3	**2**
3	1	2	**3**	3	**3**	2	**3**	1	2	**3**

We find that we have three cosets on which a, b, c act as

$$a = (123) \quad b = (12) \quad c = (23).$$

More precisely, we have written down a map $G \to S_3$ that is consistent with the above rules. A theorem (Artin 1991, 9.10) now says that this does in fact describe the action of G on G/H. Since the three elements (123), (12), and (23) generate S_3, this shows that the action of G on G/H induces an isomorphism $G \to S_3$, and that H is a subgroup of order 2.

In (Artin 1991, 6.9) it is explained how to make this procedure into an algorithm which, when it succeeds in producing a consistent table, will in fact produce the correct table.

This algorithm is implemented in Maple, except that it computes the action the ***right*** cosets. Here is a transcript:

```
  >with(group); [loads the group theory package.]
  >G:=grelgroup({a,b,c},{[a,a,a],[b,b],[c,c],[a,b,c]}); [defines
G to have generators a,b,c and relations aaa, bb, cc, abc]
  >H:=subgrel({x=[c]},G); [defines H to be the subgroup generated
by c]
  >permrep(H);
  permgroup(3, a=[[1,2,3],b=[1,2],c=[2,3]])
  [computes the action of G on the set of right cosets of H in
G].
```

Primitive actions.

Let G be a group acting on a set X, and let π be a partition of X. We say that π is ***stabilized*** by G if

$$A \in \pi \Rightarrow gA \in \pi.$$

EXAMPLE 4.35. (a) The subgroup $G = \langle(1234)\rangle$ of S_4 stabilizes the partition $\{\{1,3\},\{2,4\}\}$ of $\{1,2,3,4\}$.

(b) Identify $X = \{1,2,3,4\}$ with the set of vertices of the square on which D_4 acts in the usual way, namely, with $\sigma = (1234)$, $\tau = (2,4)$. Then D_4 stabilizes the partition $\{\{1,3\},\{2,4\}\}$.

(c) Let X be the set of partitions of $\{1,2,3,4\}$ into two sets, each with two elements. Then S_4 acts on X, and $\mathrm{Ker}(S_4 \to \mathrm{Sym}(X))$ is the subgroup V defined in (4.28).

The group G always stabilizes the trivial partitions of X, namely, the set of all one-element subsets of X, and $\{X\}$. When it stabilizes only those partitions, we say that the action is ***primitive***; otherwise it is ***imprimitive***. A subgroup of $\mathrm{Sym}(X)$ (e.g., of S_n) is said to be ***primitive*** if it acts primitively on X. Obviously, S_n itself is primitive, but Example 4.35b shows that D_4, regarded as a subgroup of S_4 in the obvious way, is not primitive.

EXAMPLE 4.36. A doubly transitive action is primitive: if it stabilized

$$\{\{x,x',...\},\{y,...\}...\},$$

then there would be no element sending (x,x') to (x,y).

REMARK 4.37. The G-orbits form a partition of X that is stabilized by G. If the action is primitive, then the partition into orbits must be one of the trivial ones. Hence

$$\text{action primitive} \Rightarrow \text{action transitive or trivial } (gx = x \text{ all } g,x).$$

For the remainder of this section, G ***is a finite group acting transitively on a set*** X ***with at least two elements***.

PROPOSITION 4.38. *The group G acts imprimitively if and only if there is an*

$$A \subset X, \quad A \neq X, \quad \#A \geq 2,$$

such that, for each $g \in G$, either $gA = A$ or $gA \cap A = \emptyset$.

PROOF. $\Longrightarrow$: The partition π stabilized by G contains such an A.

$\Longleftarrow$: From such an A, we can form a partition $\{A, g_1A, g_2A, ...\}$ of X, which is stabilized by G. □

A subset A of X such that, for each $g \in G$, $gA = A$ or $gA \cap A = \emptyset$ is called ***block***.

PROPOSITION 4.39. *Let A be a block in X with $\#A \geq 2$, $A \neq X$. For any $x \in A$,*

$$\mathrm{Stab}(x) \subsetneqq \mathrm{Stab}(A) \subsetneqq G.$$

PROOF. We have $\mathrm{Stab}(A) \supset \mathrm{Stab}(x)$ because

$$gx = x \Rightarrow gA \cap A \neq \emptyset \Rightarrow gA = A.$$

Let $y \in A$, $y \neq x$. Because G acts transitively on X, there is a $g \in G$ such that $gx = y$. Then $g \in \mathrm{Stab}(A)$, but $g \notin \mathrm{Stab}(x)$.

Let $y \notin A$. There is a $g \in G$ such that $gx = y$, and then $g \notin \mathrm{Stab}(A)$. □

THEOREM 4.40. *The group G acts primitively on X if and only if, for one (hence all) x in X, $\mathrm{Stab}(x)$ is a maximal subgroup of G.*

PROOF. If G does not act primitively on X, then (see 4.38) there is a block $A \subsetneqq X$ with at least two elements, and so (4.39) shows that $\mathrm{Stab}(x)$ will not be maximal for any $x \in A$.

Conversely, suppose that there exists an x in X and a subgroup H such that

$$\mathrm{Stab}(x) \subsetneqq H \subsetneqq G.$$

Then I claim that $A = Hx$ is a block $\neq X$ with at least two elements.

Because $H \neq \mathrm{Stab}(x)$, $Hx \neq \{x\}$, and so $\{x\} \subsetneqq A \subsetneqq X$.

If $g \in H$, then $gA = A$. If $g \notin H$, then gA is disjoint from A: for suppose $ghx = h'x$ some $h' \in H$; then $h'^{-1}gh \in \mathrm{Stab}(x) \subset H$, say $h'^{-1}gh = h''$, and $g = h'h''h^{-1} \in H$. □

Exercises 20–33

20*. (a) Show that a finite group can't be equal to the union of the conjugates of a proper subgroup.
(b) Give an example of a proper subset S of a finite group G such that $G = \bigcup_{g \in G} gSg^{-1}$.

21*. Prove that any noncommutative group of order p^3, p an odd prime, is isomorphic to one of the two groups constructed in (3.16d).

22*. Let p be the smallest prime dividing $(G:1)$ (assumed finite). Show that any subgroup of G of index p is normal.

23*. Show that a group of order $2m$, m odd, contains a subgroup of index 2. (Hint: Use Cayley's theorem 1.11)

24. Let $G = \mathrm{GL}_3(\mathbb{F}_2)$.

(a) Show that $(G:1) = 168$.

(b) Let X be the set of lines through the origin in $\mathbb{F}_2^3$; show that X has 7 elements, and that there is a natural injective homomorphism $G \hookrightarrow \mathrm{Sym}(X) = S_7$.

(c) Use Jordan canonical forms to show that G has six conjugacy classes, with 1, 21, 42, 56, 24, and 24 elements respectively. [Note that if M is a free $\mathbb{F}_2[\alpha]$-module of rank one, then $\mathrm{End}_{\mathbb{F}_2[\alpha]}(M) = \mathbb{F}_2[\alpha]$.]

(d) Deduce that G is simple.

25. Let G be a group. If $\mathrm{Aut}(G)$ is cyclic, prove that G is commutative; if further, G is finite, prove that G is cyclic.

26. Show that S_n is generated by $(1\,2), (1\,3), \ldots, (1\,n)$; also by $(1\,2), (2\,3), \ldots, (n-1\,n)$.

27*. Let K be a conjugacy class of a finite group G contained in a normal subgroup H of G. Prove that K is a union of k conjugacy classes of equal size in H, where $k = (G : H \cdot C_G(x))$ for any $x \in K$.

28*. (a) Let $\sigma \in A_n$. From Ex. 27 we know that the conjugacy class of σ in S_n either remains a single conjugacy class in A_n or breaks up as a union of two classes of equal size. Show that the second case occurs $\iff$ σ does not commute with an odd permutation $\iff$ the partition of n defined by σ consists of distinct odd integers.
(b) For each conjugacy class K in A_7, give a member of K, and determine $\#K$.

29*. Let G be the group with generators a, b and relations $a^4 = 1 = b^2$, $aba = bab$.

(a) (4 pts) Use the Todd-Coxeter algorithm (with $H = 1$) to find the image of G under the homomorphism $G \to S_n$, $n = (G:1)$, given by Cayley's Theorem 1.11. [No need to include every step; just an outline will do.]

(b) (1 pt) Use Maple to check your answer.

30*. Show that if the action of G on X is primitive and effective, then the action of any normal subgroup $H \neq 1$ of G is transitive.

31. (a) Check that A_4 has 8 elements of order 3, and 3 elements of order 2. Hence it has no element of order 6.
(b) Prove that A_4 has no subgroup of order 6 (cf. 1.18b). (Use 4.21.)

(c) Prove that A_4 is the only subgroup of S_4 of order 12.

32. Let G be a group with a subgroup of index r. Prove:

(a) If G is simple, then $(G:1)$ divides $r!$.

(b) If $r = 2, 3,$ or 4, then G can't be simple.

(c) There exists a nonabelian simple group with a subgroup of index 5.

33. Prove that S_n is isomorphic to a subgroup of A_{n+2}.

5 The Sylow Theorems; Applications

In this section, all groups are finite.

Let G be a group and let p be a prime dividing $(G\colon 1)$. A subgroup of G is called a ***Sylow*** p***-subgroup of*** G if its order is the highest power of p dividing $(G:1)$. The Sylow theorems state that there exist Sylow p-subgroups for all primes p dividing $(G\colon 1)$, that the Sylow p-subgroups for a fixed p are conjugate, and that every p-subgroup of G is contained in such a subgroup; moreover, the theorems restrict the possible number of Sylow p-subgroups in G.

The Sylow theorems

In the proofs, we frequently use that if O is an orbit for a group H acting on a set X, and $x_0 \in O$, then the map $H \to X$, $g \mapsto hx_0$ induces a bijection

$$H/\operatorname{Stab}(x_0) \to O;$$

see (4.7). Therefore

$$(H : \operatorname{Stab}(x_0)) = \# O.$$

In particular, when H is a p-group, $\# O$ is a power of p: either O consists of a single element, or $\# O$ is divisible by p. Since X is a disjoint union of the orbits, we can conclude:

LEMMA 5.1. *Let H be a p-group acting on a finite set X, and let X^H be the set of points fixed by H; then*

$$\# X \equiv \# X^H \quad (\textit{mod}\, p).$$

When the lemma is applied to a p-group H acting on itself by conjugation, we find that

$$(Z(H):1) \equiv (H:1) \mod p$$

and so $p|(Z(H)\colon 1)$ (cf. the proof of 4.15).

THEOREM 5.2 (SYLOW I). *Let G be a finite group, and let p be prime. If $p^r|(G:1)$, then G has a subgroup of order p^r.*

PROOF. According to (4.16), it suffices to prove this with p^r the highest power of p dividing $(G:1)$, and so from now on we assume that $(G:1) = p^r m$ with m not divisible by p. Let

$$X = \{\text{sub}\textbf{\textit{sets}} \text{ of } G \text{ with } p^r \text{ elements}\},$$

with the action of G defined by

$$G \times X \to X, \quad (g, A) \mapsto gA \overset{\text{df}}{=} \{ga \mid a \in A\}.$$

Let $A \in X$, and let

$$H = \operatorname{Stab}(A) \overset{\text{df}}{=} \{g \in G \mid gA = A\}.$$

For any $a_0 \in A$, $h \mapsto ha_0\colon H \to A$ is injective (cancellation law), and so $(H:1) \leq \#A = p^r$. In the equation

$$(G:1) = (G:H)(H:1)$$

we know that $(G:1) = p^r m$, $(H:1) \leq p^r$, and that $(G:H)$ is the number of elements in the orbit of A. If we can find an A such that p doesn't divide the number of elements in its orbit, then we can conclude that (for such an A), $H = \operatorname{Stab} A$ has order p^r.

The number of elements in X is

$$\#X = \left(\begin{array}{c} p^r m \\ p^r \end{array}\right) = \frac{(p^r m)(p^r m-1)\cdots(p^r m-i)\cdots(p^r m-p^r+1)}{p^r(p^r-1)\cdots(p^r-i)\cdots(p^r-p^r+1)}.$$

Note that, because $i < p^r$, the power of p dividing $p^r m - i$ is the power of p dividing i. The same is true for $p^r - i$. Therefore the corresponding terms on top and bottom are divisible by the same powers of p, and so p does not divide $\#X$. Because the orbits form a partition of X,

$$\#X = \sum \#O_i, \quad O_i \text{ the distinct orbits},$$

and so at least one of the $\#O_i$ is not divisible by p. □

EXAMPLE 5.3. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field with p elements, and let $G = \mathrm{GL}_n(\mathbb{F}_p)$. The $n \times n$ matrices in G are precisely those whose columns form a basis for $\mathbb{F}_p^n$. Thus, the first column can be any nonzero vector in $\mathbb{F}_p^n$, of which there are $p^n - 1$; the second column can be any vector not in the span of the first vector, of which there are $p^n - p$; and so on. Therefore, the order of G is

$$(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1}),$$

and so the power of p dividing $(G:1)$ is $p^{1+2+\cdots+(n-1)}$. Consider the matrices of the form

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ 0 & 0 & \cdots & * \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

They form a subgroup U of order $p^{n-1}p^{n-2}\cdots p$, which is therefore a Sylow p-subgroup G.

REMARK 5.4. The theorem gives another proof of Cauchy's theorem (4.13). If a prime p divides $(G\colon 1)$, then H will have a subgroup H of order p, and any $g \in H$, $g \neq 1$, is an element of G of order p.

REMARK 5.5. The proof of Theorem 5.2 can be modified to show directly that for each power p^r of p dividing $(G:1)$ there is a subgroup H of G of order p^r. One again writes $(G:1) = p^r m$ and considers the set X of all subsets of order p^r. In this case, the highest power p^{r_0} of p dividing $\#X$ is the highest power of p dividing m, and it follows that there is an orbit in X whose order is not divisible by p^{r_0+1}. For an A in such an orbit, the same counting argument shows that $\operatorname{Stab}(A)$ has p^r elements. We recommend that the reader write out the details.

THEOREM 5.6 (SYLOW II). *Let G be a finite group, and let $(G:1) = p^r m$ with m not divisible by p.*

(a) Any two Sylow p-subgroups are conjugate.

(b) Let s_p be the number of Sylow p-subgroups in G; then $s_p \equiv 1 \bmod p$ and $s_p|m$.

(c) Any p-subgroup of G is contained in a Sylow p-subgroup.

Let H be a subgroup of G. Recall (4.6, 4.8) that the normalizer of H in G is

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\},$$

and that the number of conjugates of H in G is $(G : N_G(H))$.

LEMMA 5.7. *Let P be a Sylow p-subgroup of G, and let H be a p-subgroup. If H normalizes P, i.e., if $H \subset N_G(P)$, then $H \subset P$. In particular, no Sylow p-subgroup of G other than P normalizes P.*

PROOF. Because H and P are subgroups of $N_G(P)$ with P normal in $N_G(P)$, HP is a subgroup, and $H/H \cap P \cong HP/P$ (apply 3.2). Therefore $(HP : P)$ is a power of p (here is where we use that H is a p-group), but

$$(HP:1) = (HP:P)(P:1),$$

and $(P:1)$ is the largest power of p dividing $(G:1)$, hence also the largest power of p dividing $(HP:1)$. Thus $(HP:P) = p^0 = 1$, and $H \subset P$. □

PROOF OF SYLOW II. (a) Let X be the set of Sylow p-subgroups in G, and let G act on X by conjugation:

$$(g, P) \mapsto gPg^{-1} \colon G \times X \to X.$$

Let O be one of the G-orbits: we have to show O is all of X.

Let $P \in O$, and consider the action by conjugation of P on O. This single G-orbit may break up into several P-orbits, one of which will be $\{P\}$. In fact this is the only one-point orbit because

$$\{Q\} \text{ is a } P\text{-orbit} \iff P \text{ normalizes } Q,$$

which we know (5.7) happens only for $Q = P$. Hence the number of elements in every P-orbit other than $\{P\}$ is divisible by p, and we have that $\#O \equiv 1$ mod p.

Suppose there exists a $P \notin O$. We again let P act on O, but this time the argument shows that there are no one-point orbits, and so the number of elements in every P-orbit is divisible by p. This implies that $\#O$ is divisible by p, which contradicts what we proved in the last paragraph. There can be no such P, and so O is all of X.

(b) Since s_p is now the number of elements in O, we have also shown that $s_p \equiv 1$ (mod p).

Let P be a Sylow p-subgroup of G. According to (a), s_p is the number of conjugates of P, which equals

$$(G : N_G(P)) = \frac{(G:1)}{(N_G(P):1)} = \frac{(G:1)}{(N_G(P):P)\cdot(P:1)} = \frac{m}{(N_G(P):P)}.$$

This is a factor of m.

(c) Let H be a p-subgroup of G, and let H act on the set X of Sylow p-subgroups by conjugation. Because $\#X = s_p$ is not divisible by p, X^H must be nonempty (Lemma 5.1), i.e., at least one H-orbit consists of a single Sylow p-subgroup. But then H normalizes P and Lemma 5.7 implies that $H \subset P$. □

COROLLARY 5.8. *A Sylow p-subgroup is normal if and only if it is the only Sylow p-subgroup.*

PROOF. Let P be a Sylow p-subgroup of G. If P is normal, then (a) of Sylow II implies that it is the only Sylow p-subgroup. The converse statement follows from (3.12c) (which shows, in fact, that P is even characteristic). □

COROLLARY 5.9. *Suppose that a group G has only one Sylow p-subgroup for each $p|(G:1)$. Then G is a direct product of its Sylow p-subgroups.*

PROOF. Let $P_1, \ldots, P_r$ be the Sylow subgroups of G, and let $(P_i : 1) = p_i^{r_i}$. The p_i are distinct primes. Because P_1 and P_2 are normal, P_1P_2 is a normal subgroup of G. As $P_1 \cap P_2 = 1$, (3.6) implies that

$$(a, b) \mapsto ab\colon P_1 \times P_2 \to P_1P_2$$

is an isomorphism. In particular, P_1P_2 has order $p_1^{r_1}p_2^{r_2}$. Now $P_1P_2 \cap P_3 = 1$, and so

$$P_1 \times P_2 \times P_3 \cong P_1P_2P_3,$$

which has order $p_1^{r_1}p_2^{r_2}p_3^{r_3}$. Continue in this manner. (Alternatively, apply Exercise 15.) □

EXAMPLE 5.10. There is a geometric description of the Sylow subgroups of $G = \mathrm{GL}_n(\mathbb{F}_p)$. Let $V = \mathbb{F}_p^n$, regarded as a vector space of dimension n over $\mathbb{F}_p$. A ***full flag*** F in V is a sequence of subspaces

$$V = V_n \supset V_{n-1} \supset \cdots \supset V_i \supset \cdots \supset V_1 \supset \{0\}$$

with $\dim V_i = i$. Given such a flag F, let $U(F)$ be the set of linear maps $\alpha\colon V \to V$ such that

(a) $\alpha(V_i) \subset V_i$ for all i, and

(b) the endomorphism of V_i/V_{i-1} induced by α is the identity map.

I claim that $U(F)$ is a Sylow p-subgroup of G. Indeed, we can construct a basis $\{e_1, \ldots, e_n\}$ for V such $\{e_1\}$ is basis for V_1, $\{e_1, e_2\}$ is a basis for V_2, and so on. Relative to this basis, the matrices of the elements of $U(F)$ are exactly the elements of the group U of (5.3).

Let $\alpha \in \mathrm{GL}_n(\mathbb{F})$. Then $\alpha F =_{df} \{\alpha V_n, \alpha V_{n-1}, \ldots\}$ is again a full flag, and $U(\alpha F) = \alpha \cdot U(F) \cdot \alpha^{-1}$. From (a) of Sylow II, we see that the Sylow p-subgroups of G are precisely the groups of the form $U(F)$ for some full flag F. (In fact, conversely, these ideas can be used to prove the Sylow theorems — see Exercise 70 for Sylow I.)

Applications

We apply what we have learnt to obtain information about groups of various orders.

EXAMPLE 5.11 (GROUPS OF ORDER 99). Let G have order 99. The Sylow theorems imply that G has at least one subgroup H of order 11, and in fact $s_{11}\left|\frac{99}{11}\right.$ and $s_{11}\equiv 1$ mod 11. It follows that $s_{11}=1$, and H is normal. Similarly, $s_9|11$ and $s_9\equiv 1 \mod 3$, and so the Sylow 3-subgroup is also normal. Hence G is isomorphic to the direct product of its Sylow subgroups (5.9), which are both commutative (4.17), and so G commutative.

Here is an alternative proof. Verify as before that the Sylow 11-subgroup N of G is normal. The Sylow 3-subgroup Q maps bijectively onto G/N, and so $G=N\rtimes Q$. It remains to determine the action by conjugation of Q on N. But $\mathrm{Aut}(N)$ is cyclic of order 10 (see 3.10), and so the only homomorphism $Q\to\mathrm{Aut}(N)$ is the trivial one (the homomorphism that maps everything to 1). It follows that G is the direct product of N and Q.

EXAMPLE 5.12 (GROUPS OF ORDER pq, p,q PRIMES, $p<q$). Let G be such a group, and let P and Q be Sylow p and q subgroups. Then $(G:Q)=p$, which is the smallest prime dividing $(G:1)$, and so (see Exercise 22) Q is normal. Because P maps bijectively onto G/Q, we have that

$$G=Q\rtimes P,$$

and it remains to determine the action of P on Q by conjugation.

The group $\mathrm{Aut}(Q)$ is cyclic of order $q-1$ (see 3.10), and so, unless $p|q-1$, $G=Q\times P$.

If $p|q-1$, then $\mathrm{Aut}(Q)$ (being cyclic) has a unique subgroup P' of order p. In fact P' consists of the maps

$$x\mapsto x^i,\quad \{i\in\mathbb{Z}/q\mathbb{Z}\mid i^p=1\}.$$

Let a and b be generators for P and Q respectively, and suppose that the action of a on Q by conjugation is $x\mapsto x^{i_0}$, $i_0\neq 1$ (in $\mathbb{Z}/q\mathbb{Z}$). Then G has generators a,b and relations a^p, b^q, $aba^{-1}=b^{i_0}$. Choosing a different i_0 amounts to choosing a different generator a for P, and so gives an isomorphic group G.

In summary: if $p\nmid q-1$, then the only group of order pq is the cyclic group C_{pq}; if $p|q-1$, then there is also a nonabelian group given by the above generators and relations.

EXAMPLE 5.13 (GROUPS OF ORDER 30). Let G be a group of order 30. Then

$$s_3=1,4,7,10,\ldots \text{ and divides } 10;$$
$$s_5=1,6,11,\ldots \text{ and divides } 6.$$

Hence $s_3=1$ or 10, and $s_5=1$ or 6. In fact, at least one is 1, for otherwise there would be 20 elements of order 3 and 24 elements of order 5, which is impossible. Therefore, a Sylow 3-subgroup P or a Sylow 5-subgroup Q is normal, and so $H=PQ$ is a subgroup of G. Because 3 doesn't divide $5-1=4$, (5.12) shows that H is commutative, $H\approx C_3\times C_5$. Hence

$$G=(C_3\times C_5)\rtimes_\theta C_2,$$

and it remains to determine the possible homomorphisms $\theta\colon C_2 \to \mathrm{Aut}(C_3 \times C_5)$. But such a homomorphism θ is determined by the image of the nonidentity element of C_2, which must be an element of order 2. Let a, b, c generate C_3, C_5, C_2. Then

$$\mathrm{Aut}(C_3 \times C_5) = \mathrm{Aut}(C_3) \times \mathrm{Aut}(C_5),$$

and the only elements of $\mathrm{Aut}\, C_3$ and $\mathrm{Aut}\, C_5$ of order 2 are $a \mapsto a^{-1}$ and $b \mapsto b^{-1}$. Thus there are exactly 4 homomorphisms θ, and $\theta(c)$ is one of the following elements:

$$\left\{\begin{array}{c} a \mapsto a \\ b \mapsto b \end{array}\right. \quad \left\{\begin{array}{c} a \mapsto a \\ b \mapsto b^{-1} \end{array}\right. \quad \left\{\begin{array}{c} a \mapsto a^{-1} \\ b \mapsto b \end{array}\right. \quad \left\{\begin{array}{c} a \mapsto a^{-1} \\ b \mapsto b^{-1} \end{array}\right. .$$

The groups corresponding to these homomorphisms have centres of order 30, 3 (generated by a), 5 (generated by b), and 1 respectively, and hence are nonisomorphic. We have shown that (up to isomorphism) there are exactly 4 groups of order 30. For example, the third on our list has generators a, b, c and relations

$$a^3, \quad b^5, \quad c^2, \quad ab = ba, \quad cac^{-1} = a^{-1}, \quad cbc^{-1} = b.$$

EXAMPLE 5.14 (GROUPS OF ORDER 12). Let G be a group of order 12, and let P be its Sylow 3-subgroup. If P is not normal, then P doesn't contain a nontrivial normal subgroup of G, and so the map (4.2, action on the left cosets)

$$\varphi : G \to \mathrm{Sym}(G/P) \approx S_4$$

is injective, and its image is a subgroup of S_4 of order 12. From Sylow II we see that G has exactly 4 Sylow 3-subgroups, and hence it has exactly 8 elements of order 3. But all elements of S_4 of order 3 are in A_4 (see the table in 4.28), and so $\varphi(G)$ intersects A_4 in a subgroup with at least 8 elements. By Lagrange's theorem $\varphi(G) = A_4$, and so $G \approx A_4$.

Now assume that P is normal. Then $G = P \rtimes Q$ where Q is the Sylow 4-subgroup. If Q is cyclic of order 4, then there is a unique nontrivial map $Q(= C_4) \to \mathrm{Aut}(P)(= C_2)$, and hence we obtain a single noncommutative group $C_3 \rtimes C_4$. If $Q = C_2 \times C_2$, there are exactly 3 nontrivial homomorphism $\theta\colon Q \to \mathrm{Aut}(P)$, but the three groups resulting are all isomorphic to $S_3 \times C_2$ with $C_2 = \mathrm{Ker}\,\theta$. (The homomorphisms differ by an automorphism of Q, and so we can also apply Lemma 3.18.)

In total, there are 3 noncommutative groups of order 12 and 2 commutative groups.

EXAMPLE 5.15 (GROUPS OF ORDER p^3). Let G be a group of order p^3, with p an odd prime, and assume G is not commutative. We know from (4.16) that G has a normal subgroup N of order p^2.

If every element of G has order p (except 1), then $N \approx C_p \times C_p$ and there is a subgroup Q of G of order p such that $Q \cap N = \{1\}$. Hence

$$G = N \rtimes_\theta Q$$

for some homomorphism $\theta\colon Q \to N$. The order of $\mathrm{Aut}(N) \approx \mathrm{GL}_2(\mathbb{F}_p)$ is $(p^2-1)(p^2-p)$ (see 5.3), and so its Sylow p-subgroups have order p. By the Sylow theorems, they are conjugate, and so Lemma 3.19 shows that there is exactly one nonabelian group in this case.

Suppose G has elements of order p^2, and let N be the subgroup generated by such an element a. Because $(G:N) = p$ is the smallest (in fact only) prime dividing $(G:1)$, N is normal in G (Exercise 22). We next show that G contains an element of order p not in N.

We know $Z(G) \neq 1$, and, because G isn't commutative, that $G/Z(G)$ is not cyclic (4.18). Therefore $(Z(G):1) = p$ and $G/Z(G) \approx C_p \times C_p$. In particular, we see that for all $x \in G$, $x^p \in Z(G)$. Because $G/Z(G)$ is commutative, the commutator of any pair of elements of G lies in $Z(G)$, and an easy induction argument shows that

$$(xy)^n = x^n y^n [y,x]^{\frac{n(n-1)}{2}}, \quad n \geq 1.$$

Therefore $(xy)^p = x^p y^p$, and so $x \mapsto x^p \colon G \to G$ is a homomorphism. Its image is contained in $Z(G)$, and so its kernel has order at least p^2. Since N contains only $p-1$ elements of order p, we see that there exists an element b of order p outside N. Hence $G = \langle a \rangle \rtimes \langle b \rangle \approx C_{p^2} \rtimes C_p$, and it remains to observe (3.19) that the nontrivial homomorphisms $C_p \to \mathrm{Aut}(C_{p^2}) \approx C_p \times C_{p-1}$ give isomorphic groups.

Thus, up to isomorphism, the only noncommutative groups of order p^3 are those constructed in (3.16e).

EXAMPLE 5.16 (GROUPS OF ORDER $2p^n$, $4p^n$, AND $8p^n$, p ODD). Let G be a group of order $2^m p^n$, $1 \leq m \leq 3$, p an odd prime, $1 \leq n$. We shall show that G is not simple. Let P be a Sylow p-subgroup and let $N = N_G(P)$, so that $s_p = (G:N)$.

From Sylow II, we know that $s_p | 2^m$, $s_p = 1, p+1, 2p+1, \ldots$. If $s_p = 1$, P is normal. If not, there are two cases to consider:

(i) $s_p = 4$ and $p = 3$, or

(ii) $s_p = 8$ and $p = 7$.

In the first case, the action by conjugation of G on the set of Sylow 3-subgroups[15] defines a homomorphism $G \to S_4$, which, if G is simple, must be injective. Therefore $(G:1)|4!$, and so $n = 1$; we have $(G:1) = 2^m 3$. Now the Sylow 2-subgroup has index 3, and so we have a homomorphism $G \to S_3$. Its kernel is a nontrivial normal subgroup of G.

In the second case, the same argument shows that $(G:1)|8!$, and so $n = 1$ again. Thus $(G:1) = 56$ and $s_7 = 8$. Therefore G has 48 elements of order 7, and so there can be only one Sylow 2-subgroup, which must therefore be normal.

Note that groups of order pq^r, p, q primes, $p < q$ are not simple, because Exercise 22 shows that the Sylow q-subgroup is normal. An examination of cases now reveals that A_5 is the smallest noncyclic simple group.

EXAMPLE 5.17. Let G be a simple group of order 60. We shall show that G is isomorphic to A_5.

Note that, because G is simple, $s_2 = 3, 5$, or 15. If P is a Sylow 2-subgroup and $N = N_G(P)$, then $s_2 = (G:N)$.

The case $s_2 = 3$ is impossible, because the kernel of $G \to \mathrm{Sym}(G/N)$ would be a nontrivial subgroup of G.

[15] Equivalently, the usual map $G \to \mathrm{Sym}(G/N)$.

In the case $s_2 = 5$, we get an inclusion $G \hookrightarrow \mathrm{Sym}(G/N) = S_5$, which realizes G as a subgroup of index 2 in S_5, but we saw in (4.33) that, for $n \geq 5$, A_n is the only subgroup of index 2 in S_n.

In the case $s_2 = 15$, a counting argument (using that $s_5 = 6$) shows that there exist two Sylow 2-subgroups P and Q intersecting in a group of order 2. The normalizer N of $P \cap Q$ contains P and Q, and so has order 12, 20, or 60. In the first case, the above argument show that $G \approx A_5$, and the remaining cases contradict the simplicity of G.

6 Normal Series; Solvable and Nilpotent Groups

Normal Series.

Let G be a group. A ***normal series*** (better ***subnormal series***) in G is a finite chain of subgroups

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_i \triangleright G_{i+1} \triangleright \cdots \triangleright G_n = \{1\}.$$

Thus G_{i+1} is normal in G_i, but not necessarily in G. The series is said to be without repetitions if $G_i \neq G_{i+1}$. Then n is called the ***length*** of the series. The quotient groups G_i/G_{i+1} are called the ***quotient*** (or ***factor) groups*** of the series.

A normal series is said to be a ***composition series*** if it has no repetitions and can't be refined, i.e., if G_{i+1} is a maximal proper normal subgroup in G_i for each i. Thus a normal series is a composition series if and only if each quotient group is simple and $\neq 1$. Obviously, every finite group has a composition series (usually many): choose G_1 to be a maximal proper normal subgroup of G; then choose G_2 to be a maximal proper normal subgroup of G_1, etc.. An infinite group may or may not have a finite composition series.

Note that from a normal series

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_i \triangleright G_{i+1} \triangleright \cdots \triangleright G_n \supset \{1\}$$

we obtain a sequence of exact sequences

$$1 \to G_n \to G_{n-1} \to G_n/G_{n-1} \to 1$$

$$1 \to G_{n-1} \to G_{n-2} \to G_{n-2}/G_{n-1} \to 1$$

$$\cdots$$

$$1 \to G_1 \to G_0 \to G_0/G_1 \to 1.$$

Thus G is built up out of the quotients $G_0/G_1, G_1/G_2, \ldots, G_n$ by forming successive extensions. In particular, since every finite group has a composition series, it can be regarded as being built up out of simple groups. The Jordan-Hölder theorem, which is the main topic of this subsection, says that these simple groups are independent of the composition series (up to order and isomorphism).

Note that if G has a normal series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n \supset \{1\}$, then

$$(G:1) = \prod (G_{i-1} : G_i) = \prod (G_{i-1}/G_i : 1).$$

EXAMPLE 6.1. (a) The symmetric group S_3 has a composition series

$$S_3 \triangleright A_3 \triangleright 1$$

with quotients C_2, C_3.

(b) The symmetric group S_4 has a composition series

$$S_4 \triangleright A_4 \triangleright V \triangleright \langle (13)(24) \rangle \triangleright 1,$$

where $V \approx C_2 \times C_2$ consists of all elements of order 2 in A_4 (see 4.28). The quotients are C_2, C_3, C_2, C_2.

(c) Any full flag in $\mathbb{F}_p^n$, p a prime, is a composition series. Its length is n, and its quotients are $C_p, C_p, \ldots, C_p$.

(d) Consider the cyclic group C_m. For any factorization $m = p_1 \cdots p_r$ of m into a product of primes (not necessarily distinct), there is a composition series

$$\begin{array}{ccccccc} C_m & \rhd & C_{\frac{m}{p_1}} & \rhd & C_{\frac{m}{p_1 p_2}} & \rhd & \cdots \\ \| & & \| & & \| & & \\ \langle\sigma\rangle & & \langle\sigma^{p_1}\rangle & & \langle\sigma^{p_1 p_2}\rangle & & \end{array}$$

The length is r, and the quotients are $C_{p_1}, C_{p_2}, \ldots, C_{p_r}$.

(e) Suppose G is a direct product of simple groups, $G = H_1 \times \cdots \times H_r$. Then G has a composition series

$$G \rhd H_2 \times \cdots \times H_r \rhd H_3 \times \cdots \times H_r \rhd \cdots$$

of length r and with quotients $H_1, H_2, \ldots, H_r$. Note that for any permutation π of $\{1, 2, \ldots r\}$, there is another composition series with quotients $H_{\pi(1)}, H_{\pi(2)}, \ldots, H_{\pi(r)}$.

(f) We saw in (4.33) that for $n \geq 5$, the only normal subgroups of S_n are S_n, A_n, $\{1\}$, and in (4.29) that A_n is simple. Hence $S_n \rhd A_n \rhd \{1\}$ is the ***only*** composition series for S_n.

As we have seen, a finite group may have many composition series. The Jordan-Hölder theorem says that they all have the same length, and the same quotients (up to order and isomorphism). More precisely:

THEOREM 6.2 (JORDAN-HÖLDER). *If*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = \{1\}$$

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_t = \{1\}$$

are two composition series for G*, then* $s = t$ *and there is a permutation* π *of* $\{1, 2, \ldots, s\}$ *such that* $G_i/G_{i+1} \approx H_{\pi(i)}/H_{\pi(i+1)}$. [16]

PROOF. We use induction on the order of G.

Case I: $H_1 = G_1$. In this case, we have two composition series for G_1, to which we can apply the induction hypothesis.

Case II: $H_1 \neq G_1$. Because each of G_1 and H_1 is normal in G, $G_1 H_1$ is a normal subgroup of G, and it properly contains both G_1 and H_1. But they are maximal normal subgroups of G, and so $G_1 H_1 = G$. Therefore

$$G/G_1 = G_1 H_1/G_1 \cong H_1/G_1 \cap H_1 \qquad \text{(see 3.2).}$$

Similarly $G/H_1 \cong G_1/G_1 \cap H_1$. Hence $K_2 =_{df} G_1 \cap H_1$ is a maximal normal subgroup in both G_1 and H_1, and

$$G/G_1 \approx H_1/K_2, \quad G/H_1 \approx G_1/K_2.$$

[16] Jordan showed that corresponding quotients had the same order, and Hölder that they were isomorphic.

Choose a composition series

$$K_2 \rhd K_3 \rhd \cdots \rhd K_u.$$

We have the picture:

$$\begin{tikzcd}
 & G_1 \arrow[r, phantom, "\rhd"] \arrow[dr, dash] & G_2 \arrow[r, phantom, "\rhd"] & \cdots \arrow[r, phantom, "\rhd"] & G_s \\
G \arrow[ur, dash] \arrow[dr, dash] & & K_2 \arrow[r, phantom, "\rhd"] & \cdots \arrow[r, phantom, "\rhd"] & K_u \\
 & H_1 \arrow[r, phantom, "\rhd"] \arrow[ur, dash] & H_2 \arrow[r, phantom, "\rhd"] & \cdots \arrow[r, phantom, "\rhd"] & H_t
\end{tikzcd}.$$

On applying the induction hypothesis to G_1 and H_1 and their composition series in the diagram, we find that

$$\begin{aligned}
\text{Quotients}(G \rhd G_1 \rhd G_2 \rhd \cdots) &= \{G/G_1, G_1/G_2, G_2/G_3, \ldots\} \\
&\sim \{G/G_1, G_1/K_2, K_2/K_3, \ldots\} \\
&\sim \{H_1/K_2, G/H_1, K_2/K_3, \ldots\} \\
&\sim \{G/H_1, H_1/K_2, K_2/K_3, \ldots\} \\
&\sim \{G/H_1, H_1/H_2, H_2/H_3, \ldots\} \\
&= \text{Quotients}(G \rhd H_1 \rhd H_2 \rhd \cdots).
\end{aligned}$$

In passing from the second to the third line, we used the isomorphisms $G/G_1 \approx H_1/K_2$ and $G/H_1 \approx G_1/K_2$. □

Note that the theorem applied to a cyclic group C_m implies that the factorization of an integer into a product of primes is unique.

REMARK 6.3. There are infinite groups having finite composition series (there are even infinite simple groups). For such a group, let $d(G)$ be the minimum length of a composition series. Then the Jordan-Hölder theorem extends to show that all composition series have length $d(G)$ and have isomorphic quotient groups. The same proof works except that you have to use induction on $d(G)$ instead of $(G : 1)$ and verify that K_2 has a finite composition series.

The quotients of a composition series are also called ***composition factors.***

Solvable groups

A normal series whose quotient groups are all commutative is called a ***solvable series***. A group is solvable if it has a solvable series. Alternatively, we can say that a group is solvable if it can be obtained by forming successive extensions of abelian groups. Since a commutative group is simple if and only if it is cyclic of prime order, we see that G is solvable if and only if for one (hence every) composition series the quotients are all cyclic groups of prime order.

Every commutative group is solvable, as is every dihedral group. The results in Section 5 show that every group of order < 60 is solvable. By contrast, a noncommutative simple group, e.g., A_n for $n \geq 5$, will not be solvable.

There is the following result:

THEOREM 6.4 (FEIT-THOMPSON). *Every finite group of odd order is solvable.*

PROOF. The proof occupies an entire issue of the Pacific Journal of Mathematics (Feit, Walter, and Thompson, John G., Solvability of groups of odd order. Pacific J. Math. 13 (1963), 775–1029). □

This theorem played a very important role in the development of group theory, because it shows that every noncommutative finite simple group contains an element of order 2. It was a starting point in the program that eventually led to the classification of all finite simple groups. See the article cited on p34.

EXAMPLE 6.5. Consider the subgroups $B = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$ and $U = \left\{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\right\}$ of $\mathrm{GL}_2(k)$, some field k. Then U is a normal subgroup of B, and $B/U \cong k^\times \times k^\times$, $U \cong (k, +)$. Hence B is solvable.

PROPOSITION 6.6. *(a) Every subgroup and every quotient group of a solvable group is solvable.*

(b) An extension of solvable groups is solvable.

PROOF. (a) Let $G \triangleright G_1 \triangleright \cdots \triangleright G_n$ be a solvable series for G, and let H be a subgroup of G. The homomorphism

$$x \mapsto xG_{i+1} : H \cap G_i \to G_i/G_{i+1}$$

has kernel $(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}$. Therefore, $H \cap G_{i+1}$ is a normal subgroup of $H \cap G_i$ and the quotient $H \cap G_i/H \cap G_{i+1}$ injects into G_i/G_{i+1}, which is commutative. We have shown that

$$H \triangleright H \cap G_1 \triangleright \cdots \triangleright H \cap G_n$$

is a solvable series for H.

Let $\overline{G}$ be a quotient group of G, and let $\overline{G}_i$ be the image of G_i in $\overline{G}$. Then

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = \{1\}$$

is a solvable series for $\overline{G}$.

(b) Let N be a normal subgroup of G, and let $\overline{G} = G/N$. We have to show that if N and $\overline{G}$ are solvable, then so also is G. Let

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = \{1\}$$

$$N \triangleright N_1 \triangleright \cdots \triangleright N_m = \{1\}$$

be a solvable series for $\overline{G}$ and N, and let G_i be the inverse image of $\overline{G}_i$ in G. Then $G_i/G_{i+1} \approx \overline{G}_i/\overline{G}_{i+1}$ (see 3.4), and so

$$G \triangleright G_1 \triangleright \cdots \triangleright G_n (= N) \triangleright N_1 \triangleright \cdots \triangleright N_m$$

is a solvable series for G. □

COROLLARY 6.7. *A finite p-group is solvable.*

PROOF. We use induction on the order the group G. According to (4.15), the centre $Z(G)$ of G is nontrivial, and so the induction hypothesis implies that $G/Z(G)$ is solvable. Because $Z(G)$ is commutative, (b) of the proposition shows that G is solvable. □

Let G be a group. Recall that the commutator of $x, y \in G$ is

$$[x,y] = xyx^{-1}y^{-1} = xy(yx)^{-1}$$

Thus

$$[x,y] = 1 \iff xy = yx,$$

and G is commutative if and only if every commutator equals 1.

EXAMPLE 6.8. For any finite-dimensional vector space V over a field k and any full flag $F = \{V_n, V_{n-1}, \ldots\}$ in V, the group

$$B(F) = \{\alpha \in \mathrm{Aut}(V) \mid \alpha(V_i) \subset V_i \text{ all } i\}$$

is solvable. Indeed, let $U(F)$ be the group defined in Example 5.10. Then $B(F)/U(F)$ is commutative, and, when $k = \mathbb{F}_p$, $U(F)$ is a p-group. This proves that $B(F)$ is solvable when $k = \mathbb{F}_p$, and we leave the general case as an exercise.

For any homomorphism $\varphi\colon G \to H$

$$\varphi([x,y]) = \varphi(xyx^{-1}y^{-1}) = [\varphi(x), \varphi(y)],$$

i.e., φ maps the commutator of x, y to the commutator of $\varphi(x), \varphi(y)$. In particular, we see that if H is commutative, then φ maps all commutators in G to 1.

The group G' generated by the commutators in G is called the ***commutator*** or ***first derived subgroup*** of G.

PROPOSITION 6.9. *The commutator subgroup G' is a characteristic subgroup of G; it is the smallest normal subgroup of G such that G/G' is commutative.*

PROOF. An automorphism α of G maps the generating set for G' into G', and hence maps G' into G'. Since this is true for all automorphisms of G, G' is characteristic (see p28).

Write $g \mapsto \overline{g}$ for the homomorphism $g \mapsto gG'\colon G \to G/G'$. As for any homomorphism, $[g,h] \mapsto [\overline{g}, \overline{h}]$, but, in this case, we know $[g,h] \mapsto 1$. Hence $[\overline{g}, \overline{h}] = 1$ for all $\overline{g}$, $\overline{h} \in G/G'$, which shows that G/G' is commutative.

Let N be a second normal subgroup of G such that G/N is commutative. Then $[g,h] \mapsto 1$ in G/N, and so $[g,h] \in N$. Since these elements generate G', $N \supset G'$. □

For $n \geq 5$, A_n is the smallest normal subgroup of S_n giving a commutative quotient. Hence $(S_n)' = A_n$.

The ***second derived subgroup*** of G is $(G')'$; the ***third*** is $G^{(3)} = (G'')'$; and so on. Since a characteristic subgroup of a characteristic subgroup is characteristic (3.12a), each derived group $G^{(n)}$ is a characteristic subgroup of G. Hence we obtain a normal series

$$G \supset G' \supset G^{(2)} \supset \cdots,$$

which is called the ***derived series***. For example, when $n \geq 5$, the derived series of S_n is

$$S_n \supset A_n \supset A_n \supset A_n \supset \cdots .$$

PROPOSITION 6.10. *A group G is solvable if and only if its k^{th} derived subgroup $G^{(k)} = 1$ for some k.*

PROOF. If $G^{(k)} = 1$, then the derived series is a solvable series for G. Conversely, let

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s = 1$$

be a solvable series for G. Because G/G_1 is commutative, $G_1 \supset G'$. Now $G'G_2$ is a subgroup of G_1, and from

$$G'/G' \cap G_2 \overset{\cong}{\to} G'G_2/G_2 \subset G_1/G_2$$

we see that

$$G_1/G_2 \text{ commutative } \Rightarrow G'/G' \cap G_2 \text{ commutative } \Rightarrow G'' \subset G' \cap G_2 \subset G_2.$$

Continuing in the fashion, we find that $G^{(i)} \subset G_i$ for all i, and hence $G^{(s)} = 1$. □

Thus, a solvable group G has a *canonical* solvable series, namely the derived series, in which all the groups are normal in G. The proof of the proposition shows that the derived series is the shortest solvable series for G. Its length is called the ***solvable length*** of G.

Nilpotent groups

Let G be a group. Recall that we write $Z(G)$ for the centre of G. Let $Z^2(G) \supset Z(G)$ be the subgroup of G corresponding to $Z(G/Z(G))$. Thus

$$g \in Z^2(G) \iff [g,x] \in Z(G) \text{ for all } x \in G.$$

Continuing in this fashion, we get a sequence of subgroups (***ascending central series***)

$$\{1\} \subset Z(G) \subset Z^2(G) \subset \cdots$$

where

$$g \in Z^i(G) \iff [g,x] \in Z^{i-1}(G) \text{ for all } x \in G.$$

If $Z^m(G) = G$ for some m, then G is said to be ***nilpotent***, and the smallest such m is called the ***(nilpotency) class*** of G. For example, all finite p-groups are nilpotent (apply 4.15).

For example, only the group $\{1\}$ has class 0, and the groups of class 1 are exactly the commutative groups. A group G is of class 2 if and only if $G/Z(G)$ is commutative — such a group is said to be ***metabelian***.

EXAMPLE 6.11. (a) A nilpotent group is obviously solvable, but the converse is false. For example, for a field k, let

$$B = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \middle| \, a, b, c \in k, \quad ac \neq 0 \right\}.$$

Then $Z(B) = \{aI \mid a \neq 0\}$, and the centre of $B/Z(B)$ is trivial. Therefore $B/Z(B)$ is not nilpotent, but we saw in (6.5) that it is solvable.

(b) The group $G = \left\{ \left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix} \right) \right\}$ is metabelian: its centre is $\left\{ \left(\begin{smallmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix} \right) \right\}$, and $G/Z(G)$ is commutative.

(c) Any nonabelian group G of order p^3 is metabelian. In fact, $G' = Z(G)$ has order p (see 5.15), and G/G' is commutative (4.17). In particular, the quaternion and dihedral groups of order 8, Q and D_4, are metabelian. The dihedral group D_{2^n} is nilpotent of class n — this can be proved by induction, using that $Z(D_{2^n})$ has order 2, and $D_{2^n}/Z(D_{2^n}) \approx D_{2^{n-1}}$. If n is not a power of 2, then D_n is not nilpotent (use Theorem 6.17 below).

PROPOSITION 6.12. *(a) A subgroup of a nilpotent group is nilpotent.*

(b) A quotient of a nilpotent group is nilpotent.

PROOF. (a) Let H be a subgroup of a nilpotent group G. Clearly, $Z(H) \supset Z(G) \cap H$. Assume (inductively) that $Z^i(H) \supset Z^i(G) \cap H$; then $Z^{i+1}(H) \supset Z^{i+1}(G) \cap H$, because (for $h \in H$)

$$h \in Z^{i+1}(G) \Rightarrow [h, x] \in Z^i(G) \text{ all } x \in G \Rightarrow [h, x] \in Z^i(H) \text{ all } x \in H.$$

(b) Straightforward. □

REMARK 6.13. It is worth noting that if H is a subgroup of G, then $Z(H)$ may be bigger than $Z(G)$. For example

$$H = \left\{ \left(\begin{array}{cc} a & 0 \\ 0 & b \end{array} \right) \middle| \, ab \neq 0 \right\} \subset \mathrm{GL}_2(k).$$

is commutative, i.e., $Z(H) = H$, but the centre of G consists of only of the scalar matrices.

PROPOSITION 6.14. *A group G is nilpotent of class $\leq m$ if and only if*

$$[\ldots[[g_1, g_2], g_3], \ldots, , g_{m+1}] = 1$$

for all $g_1, ..., g_{m+1} \in G$.

PROOF. Recall, $g \in Z^i(G) \iff [g, x] \in Z^{i-1}(G)$ for all $x \in G$.

Assume G is nilpotent of class $\leq m$; then

$$\begin{aligned} G = Z^m(G) &\Rightarrow [g_1, g_2] \in Z^{m-1}(G) \text{ all } g_1, g_2 \in G \\ &\Rightarrow [[g_1, g_2], g_3] \in Z^{m-2}(G) \text{ all } g_1, g_2, g_3 \in G \\ &\cdots\cdots \\ &\Rightarrow [\cdots[[g_1, g_2], g_3], ..., g_m] \in Z(G) \text{ all } g_1, \ldots, g_m \in G \\ &\Rightarrow [\cdots[[g_1, g_2], g_3], \ldots, g_{m+1}] = 1 \text{ all } g_1, \ldots, g_m \in G. \end{aligned}$$

For the converse, let $g_1 \in G$. Then

$$\begin{aligned}[...[[g_1,g_2],g_3],...,g_m],g_{m+1}] =& 1 \text{ for all } g_1,g_2,...,g_{m+1} \in G \\ & \Rightarrow [...[[g_1,g_2],g_3],...,g_m] \in Z(G), \text{ for all } g_1,...,g_m \in G \\ & \Rightarrow [...[[g_1,g_2],g_3],...,g_{m-1}] \in Z^2(G), \text{ for all } g_1,...,g_{m-1} \in G \\ & \cdots\cdots \\ & \Rightarrow g_1 \in Z^m(G) \text{ all } g_1 \in G.\end{aligned}$$

□

An extension of nilpotent groups need not be nilpotent, i.e.,

$$N \text{ and } G/N \text{ nilpotent } \not\Rightarrow G \text{ nilpotent.} \tag{4}$$

For example, the subgroup U of the group B in Examples 6.5 and 6.11 is commutative and B/U is commutative, but B is not nilpotent.

However, the implication (4) holds when N is contained in the centre of G. In fact, we have the following more precise result.

COROLLARY 6.15. *For any subgroup N of the centre of G,*

$$G/N \textit{ nilpotent of class } m \Rightarrow G \textit{ nilpotent of class } \leq m+1.$$

PROOF. Write π for the map $G \to G/N$. Then

$$\pi([...[[g_1,g_2],g_3],...,g_m],g_{m+1}]) = [...[[\pi g_1,\pi g_2],\pi g_3],...,\pi g_m],\pi g_{m+1}] = 1$$

all $g_1,...,g_{m+1} \in G$. Hence $[...[[g_1,g_2],g_3],...,g_m],g_{m+1}] \in N \subset Z(G)$, and so

$$[...[[g_1,g_2],g_3],...,g_{m+1}],g_{m+2}] = 1 \text{ all } g_1,...,g_{m+2} \in G.$$

□

COROLLARY 6.16. *A finite p-group is nilpotent.*

PROOF. We use induction on the order of G. Because $Z(G) \neq 1$, $G/Z(G)$ nilpotent, which implies that G is nilpotent. □

Recall that an extension

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1$$

is central if $\iota(N) \subset Z(G)$. Then:

> the nilpotent groups are those that can be obtained from commutative groups by successive central extensions.

Contrast:

> the solvable groups are those that can be obtained from commutative groups by successive extensions (not necessarily central).

THEOREM 6.17. *A finite group is nilpotent if and only if it is equal to a direct product of its Sylow subgroups.*

PROOF. A direct product of nilpotent groups is (obviously) nilpotent, and so the "if" direction follows from the preceding corollary. For the converse, let G be a finite nilpotent group. According to (5.9) it suffices to prove that all Sylow subgroups are normal. Let P be such a subgroup of G, and let $N = N_G(P)$. The first lemma below shows that $N_G(N) = N$, and the second then implies that $N = G$, i.e., that P is normal in G. □

LEMMA 6.18. *Let P be a Sylow p-subgroup of a finite group G. For any subgroup H of G containing $N_G(P)$, we have $N_G(H) = H$.*

PROOF. Let $g \in N_G(H)$, so that $gHg^{-1} = H$. Then $H \supset gPg^{-1} = P'$, which is a Sylow p-subgroup of H. By Sylow II, $hP'h^{-1} = P$ for some $h \in H$, and so $hgPg^{-1}h^{-1} \subset P$. Hence $hg \in N_G(P) \subset H$, and so $g \in H$. □

LEMMA 6.19. *Let H be proper subgroup of a finite nilpotent group G; then $H \neq N_G(H)$.*

PROOF. The statement is obviously true for commutative groups, and so we can assume G to be noncommutative. We use induction on the order of G. Because G is nilpotent, $Z(G) \neq 1$. Certainly the elements of $Z(G)$ normalize H, and so if $Z(G) \not\subseteq H$, we have $H \subsetneqq Z(G) \cdot H \subset N_G(H)$. Thus we may suppose $Z(G) \subset H$. Then the normalizer of H in G corresponds under (3.3) to the normalizer of $H/Z(G)$ in $G/Z(G)$, and we can apply the induction hypothesis. □

REMARK 6.20. For a finite abelian group G we recover the fact that G is a direct product of its p-primary subgroups.

PROPOSITION 6.21 (FRATTINI'S ARGUMENT). *Let H be a normal subgroup of a finite group G, and let P be a Sylow p-subgroup of H. Then $G = H \cdot N_G(P)$.*

PROOF. Let $g \in G$. Then $gPg^{-1} \subset gHg^{-1} = H$, and both gPg^{-1} and P are Sylow p-subgroups of H. According to Sylow II, there is an $h \in H$ such that $gPg^{-1} = hPh^{-1}$, and it follows that $h^{-1}g \in N_G(P)$ and so $g \in H \cdot N_G(P)$. □

THEOREM 6.22. *A finite group is nilpotent if and only if every maximal proper subgroup is normal.*

PROOF. We saw in Lemma 6.19 that for any proper subgroup H of a nilpotent group G, $H \subsetneqq N_G(H)$. Hence,

$$H \text{ maximal} \Rightarrow N_G(H) = G,$$

i.e., H is normal in G.

Conversely, suppose every maximal proper subgroup of G is normal. We shall check the condition of Theorem 6.17. Thus, let P be a Sylow p-subgroup of G. If P is not normal in G, then there exists a maximal proper subgroup H of G containing $N_G(P)$. Being maximal, H is normal, and so Frattini's argument shows that $G = H \cdot N_G(P) = H$ — contradiction. □

Groups with operators

Recall that the set $\mathrm{Aut}(G)$ of automorphisms of a group G is again a group. Let A be a group. A pair (G,φ) consisting of a group G together with a homomorphism $\varphi\colon A\to\mathrm{Aut}(G)$ is called an A-***group***, or G is said to have A as a ***group of operators***.

Let G be an A-group, and write ${}^{\alpha}x$ for $\varphi(\alpha)x$. Then

(a) ${}^{(\alpha\beta)}x={}^{\alpha}({}^{\beta}x)$ (φ is a homomorphism);
(b) ${}^{\alpha}(xy)={}^{\alpha}x\cdot{}^{\alpha}y$ ($\varphi(\alpha)$ is a homomorphism);
(c) ${}^{1}x=x$ (φ is a homomorphism).

Conversely, a map $(\alpha,x)\mapsto{}^{\alpha}x : A\times G\to G$ satisfying (a), (b), (c) arises from a homomorphism $A\to\mathrm{Aut}(G)$. Conditions (a) and (c) show that $x\mapsto{}^{\alpha}x$ is inverse to $x\mapsto{}^{(\alpha^{-1})}x$, and so $x\mapsto{}^{\alpha}x$ is a bijection $G\to G$. Condition (b) then shows that it is an automorphism of G. Finally, (a) shows that the map $\varphi(\alpha)=(x\mapsto{}^{\alpha}x)$ is a homomorphism $A\to\mathrm{Aut}(G)$.

Let G be a group with operators A. A subgroup H of G is ***admissible*** or an A-***invariant subgroup*** if

$$x\in H\Rightarrow{}^{\alpha}x\in H,\text{ all }\alpha\in A.$$

An intersection of admissible groups is admissible. If H is admissible, so also are its normalizer $N_G(H)$ and centralizer $C_G(H)$.

An A-***homomorphism*** (or ***admissible homomorphism***) of A-groups is a homomorphism $\gamma\colon G\to G'$ such that $\gamma({}^{\alpha}g)={}^{\alpha}\gamma(g)$ for all $\alpha\in A$, $g\in G$.

EXAMPLE 6.23. (a) A group G can be regarded as a group with $\{1\}$ as group of operators. In this case all subgroups and homomorphisms are admissible, and so the theory of groups with operators includes the theory of groups without operators.

(b) Consider G with G acting by conjugation, i.e., consider G together with

$$g\mapsto i_g : G\to\mathrm{Aut}(G).$$

In this case, the admissible subgroups are the normal subgroups.

(c) Consider G with $A=\mathrm{Aut}(G)$ as group of operators. In this case, the admissible subgroups are the characteristic subgroups.

Almost everything we have proved in this course for groups also holds for groups with operators. In particular, the Isomorphism Theorems 3.1, 3.2, and 3.3 hold for groups with operators. In each case, the proof is the same as before except that admissibility must be checked.

THEOREM 6.24. *For any admissible homomorphism $\gamma\colon G\to G'$ of A-groups, $N\overset{\text{df}}{=}\mathrm{Ker}(\gamma)$ is an admissible normal subgroup of G, $\gamma(G)$ is an admissible subgroup of G', and γ factors in a natural way into the composite of an admissible surjection, an admissible isomorphism, and an admissible injection:*

$$G\twoheadrightarrow G/N\xrightarrow{\cong}\gamma(G)\hookrightarrow G'.$$

THEOREM 6.25. *Let G be a group with operators A, and let H and N be admissible subgroups with N normal. Then $H\cap N$ is normal admissible subgroup of H, HN is an admissible subgroup of G, and $h(H\cap N)\mapsto hH$ is an admissible isomorphism $H/H\cap N\to HN/N$.*

THEOREM 6.26. *Let $\varphi\colon G \to \overline{G}$ be a surjective admissible homomorphism of A-groups. Under the one-to-one correspondence $H \leftrightarrow \overline{H}$ between the set of subgroups of G containing $\mathrm{Ker}(\varphi)$ and the set of subgroups of $\overline{G}$ (see 3.3), admissible subgroups correspond to admissible subgroups.*

Let $\varphi\colon A \to \mathrm{Aut}(G)$ be a group with A operating. An ***admissible normal series*** is a chain of admissible subgroups of G

$$G \supset G_1 \supset G_2 \supset \cdots \supset G_r$$

with each G_i normal in G_{i-1}. Define similarly an admissible composition series. The quotients of an admissible normal series are A-groups, and the quotients of an admissible composition series are simple A-groups, i.e., they have no normal admissible subgroups apart from the obvious two.

The Jordan-Hölder theorem continues to hold for A-groups. In this case the isomorphisms between the corresponding quotients of two composition series are admissible. The proof is the same as that of the original theorem, because it uses only the isomorphism theorems, which we have noted also hold for A-groups.

EXAMPLE 6.27. (a) Consider G with G acting by conjugation. In this case an admissible normal series is a sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = \{1\},$$

with each G_i normal in G. (This is what *should* be called a normal series.) The action of G on G_i by conjugation passes to the quotient, to give an action of G on G_i/G_{i+1}. The quotients of two admissible normal series are isomorphic as G-groups.

(b) Consider G with $A = \mathrm{Aut}(G)$ as operator group. In this case, an admissible normal series is a sequence

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = \{1\}$$

with each G_i a characteristic subgroup of G.

Krull-Schmidt theorem

A group G is ***indecomposable*** if $G \neq 1$ and G is not isomorphic to a direct product of two nontrivial groups, i.e., if

$$G \approx H \times H' \Rightarrow H = 1 \text{ or } H' = 1.$$

EXAMPLE 6.28. (a) A simple group is indecomposable, but an indecomposable group need not be simple: it may have a normal subgroup. For example, S_3 is indecomposable but has C_3 as a normal subgroup.

(b) A finite commutative group is indecomposable if and only if it is cyclic of prime-power order.

Of course, this is obvious from the classification, but it is not difficult to prove it directly. Let G be cyclic of order p^n, and suppose that $G \approx H \times H'$. Then H and H' must be p-groups, and they can't both be killed by p^m, $m < n$. It follows that one must be cyclic of order p^n, and that the other is trivial. Conversely, suppose that G is commutative and indecomposable. Since every finite commutative group is (obviously) a direct product of p-groups with p running over the primes, G is a p-group. If g is an element of G of highest order, one shows that $\langle g\rangle$ is a direct factor of G, $G \approx \langle g\rangle \times H$, which is a contradiction.

(c) Every finite group can be written as a direct product of indecomposable groups (obviously).

Recall (3.8) that when $G_1, G_2, \ldots, G_r$ are subgroups of G such that the map

$$(g_1, g_2, ..., g_r) \mapsto g_1 g_2 \cdots g_r : G_1 \times G_2 \times \cdots \times G_r \to G$$

is an isomorphism, we say that G is the direct product of its subgroups $G_1, \ldots, G_r$, and we write

$$G = G_1 \times G_2 \times \cdots \times G_r.$$

THEOREM 6.29 (KRULL-SCHMIDT). *Let*

$$G = G_1 \times \cdots \times G_s \quad \textit{and} \quad G = H_1 \times \cdots \times H_t$$

be two decompositions of G into direct products of indecomposable subgroups. Then $s = t$, and there is a re-indexing such that $G_i \approx H_i$. Moreover, given r, we can arrange the numbering so that

$$G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t.$$

PROOF. See Rotman 1995, 6.36. □

EXAMPLE 6.30. Let $G = \mathbb{F}_p \times \mathbb{F}_p$, and think of it as a two-dimensional vector space over $\mathbb{F}_p$. Let

$$G_1 = \langle (1,0)\rangle, \quad G_2 = \langle (0,1)\rangle; \quad H_1 = \langle (1,1)\rangle, \quad H_2 = \langle (1,-1)\rangle.$$

Then $G = G_1 \times G_2$, $G = H_1 \times H_2$, $G = G_1 \times H_2$.

REMARK 6.31. (a) The Krull-Schmidt theorem holds also for an infinite group provided it satisfies both chain conditions on subgroups, i.e., ascending and descending sequences of subgroups of G become stationary.

(b) The Krull-Schmidt theorem also holds for groups with operators. For example, let $\mathrm{Aut}(G)$ operate on G; then the subgroups in the statement of the theorem will all be characteristic.

(c) When applied to a finite abelian group, the theorem shows that the groups C_{m_i} in a decomposition $G = C_{m_1} \times ... \times C_{m_r}$ with each m_i a prime power are uniquely determined up to isomorphism (and ordering).

Further reading

For more on abstract groups, see Rotman 1995.

For an introduction to the theory of algebraic groups, see: Curtis, Morton L., Matrix groups. Second edition. Universitext. Springer-Verlag, New York, 1984.

For the representation theory of groups, see: Serre, Jean-Pierre, Linear Representations of Finite Groups. Graduate Texts in Mathematics: Vol 42, Springer, 1987.

A Solutions to Exercises

These solutions fall somewhere between hints and complete solutions. Students were expected to write out complete solutions.

1. By inspection, the only element of order 2 is $c = a^2 = b^2$. Since gcg^{-1} also has order 2, it must equal c, i.e., $gcg^{-1} = c$ for all $g \in Q$. Thus c commutes with all elements of Q, and $\{1, c\}$ is a normal subgroup of Q. The remaining subgroups have orders 1, 4, or 8, and are automatically normal (see 1.24a).

2. The element $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

3. Consider the subsets $\{g, g^{-1}\}$ of G. Each set has exactly 2 elements unless g has order 1 or 2, in which case it has 1 element. Since G is a disjoint union of these sets, there must be a (nonzero) even number of sets with 1 element, and hence at least one element of order 2.

4. Because the group G/N has order n, $(gN)^n = 1$ for every $g \in G$ (Lagrange's theorem). But $(gN)^n = g^n N$, and so $g^n \in N$. For the second statement, consider $N = \{1, \tau\} \subset D_3$. It has index 3, but the element $\tau\sigma$ has order 2, and so $(\tau\sigma)^3 = \tau\sigma \notin N$.

5. Note first that any group generated by a commuting set of elements must be commutative, and so the group G in the problem is commutative. According to (2.9), any map $\{a_1, \ldots, a_n\} \to A$ with A commutative extends uniquely to homomorphism $G \to A$, and so G has the universal property that characterizes the free abelian group on the generators a_i.

6. (a) If $a \neq b$, then the word $a \cdots ab^{-1} \cdots b^{-1}$ is reduced and $\neq 1$. Therefore, if $a^n b^{-n} = 1$, then $a = b$. (b) is similar. (c) The reduced form of x^n, $x \neq 1$, has length at least n.

7. (a) Universality. (b) $C_\infty \times C_\infty$ is commutative, and the only commutative free groups are 1 and C_∞. (c) Suppose a is a nonempty reduced word in $x_1, \ldots, x_n$, say $a = x_i \cdots$ (or $x_i^{-1} \cdots$). For $j \neq i$, the reduced form of $[x_j, a] =_{df} x_j a x_j^{-1} a^{-1}$ can't be empty, and so a and x_j don't commute.

8. The unique element of order 2 is b^2. The quotient group $Q_n/\langle b^2 \rangle$ has generators a and b, and relations $a^{2^{n-2}} = 1$, $b^2 = 1$, $bab^{-1} = a^{-1}$, which is a presentation for $D_{2^{n-2}}$ (see 2.10).

9. (a) A comparison of the presentation $D_4 = \langle \sigma^4, \tau^2, \tau\sigma\tau\sigma = 1 \rangle$ with that for G suggests putting $\sigma = ab$ and $\tau = a$. Check (using 2.9) that there are homomorphisms:

$$D_4 \to G, \quad \sigma \mapsto ab, \quad \tau \mapsto a, \qquad G \to D_4, \quad a \mapsto \tau, \quad b \mapsto \tau^{-1}\sigma.$$

The composites $D_4 \to G \to D_4$ and $G \to D_4 \to G$ are the both the identity map on generating elements, and therefore (2.9 again) are identity maps. (b) Omit.

10. The hint gives $ab^3a^{-1} = bc^3b^{-1}$. But $b^3 = 1$. So $c^3 = 1$. Since $c^4 = 1$, this forces $c = 1$. From $acac^{-1} = 1$ this gives $a^2 = 1$. But $a^3 = 1$. So $a = 1$. The final relation then gives $b = 1$.

11. The elements x^2, xy, y^2 lie in the kernel, and it is easy to see that $\langle x, y | x^2, xy, y^2 \rangle$ has order (at most) 2, and so they must generate the kernel (at least as a normal group — the problem is unclear). One can prove directly that these elements are free, or else apply the Nielsen-Schreier theorem (2.6). Note that the formula on p. 18 (correctly) predicts that the kernel is free of rank $2 \cdot 2 - 2 + 1 = 3$

12. We have to show that if s and t are elements of a finite group satisfying $t^{-1}s^3t = s^5$, then the given element g is equal to 1. So, $s^n = 1$ for some n. The interesting case is when $(3, n) = 1$. But in this case, $s^{3r} = s$ for some r. Hence $t^{-1}s^{3r}t = (t^{-1}s^3t)^r = s^{5r}$. Now,

$$g = s^{-1}(t^{-1}s^{-1}t)s(t^{-1}st) = s^{-1}s^{-5r}ss^{5r} = 1;$$

done. [In such a question, look for a pattern. I also took a while to see it, but what eventually clicked was that g had two conjugates in it, as did the relation for G. So I tried to relate them.]

13. The key point is that $\langle a\rangle = \langle a^2\rangle \times \langle a^n\rangle$. Apply (3.5) to see that D_{2n} breaks up as a product.

14. Let N be the unique subgroup of order 2 in G. Then G/N has order 4, but there is no subgroup $Q \subset G$ of order 4 with $Q \cap N = 1$ (because every group of order 4 contains a group of order 2), and so $G \neq N \rtimes Q$ for any Q. A similar argument applies to subgroups N of order 4.

15. For any $g \in G$, gMg^{-1} is a subgroup of order m, and therefore equals M. Thus M (similarly N) is normal in G, and MN is a subgroup of G. The order of any element of $M \cap N$ divides $\gcd(m, n) = 1$, and so equals 1. Now (3.6) shows that $M \times N \approx MN$, which therefore has order mn, and so equals G.

16. Show that $\mathrm{GL}_2(\mathbb{F}_2)$ permutes the 3 nonzero vectors in $\mathbb{F}_2^2$ (2-dimensional vector space over $\mathbb{F}_2$).

17. Omit. [If anyone has a neat solution, please send it to me.]

18. The pair

$$N = \left\{\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\right\} \text{ and } Q = \left\{\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & d \end{pmatrix}\right\}$$

satisfies the conditions (i), (ii), (iii) of (3.13). For example, for (i) (Maple says that)

$$\begin{pmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & d \end{pmatrix}\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & -\frac{b}{d}+\frac{1}{d}(b+ab) \\ 0 & 1 & -\frac{c}{d}+\frac{1}{d}(c+ac) \\ 0 & 0 & 1 \end{pmatrix}$$

It is not a direct product of the two groups because it is not commutative.

19. Let g generate C_∞. Then the only other generator is g^{-1}, and the only nontrivial automorphism is $g \mapsto g^{-1}$. Hence $\mathrm{Aut}(C_\infty) = \{\pm 1\}$. The homomorphism $S_3 \to \mathrm{Aut}(S_3)$ is injective because $Z(S_3) = 1$, but S_3 has exactly 3 elements a_1, a_2, a_3 of order 2 and 2 elements b, b^2 of order 3. The elements a_1, b generate S_3, and there are only 6 possibilities for $\alpha(a_1)$, $\alpha(b)$, and so $S_3 \to \mathrm{Aut}(S_3)$ is also onto.

20. Let H be a proper subgroup of G, and let $N = N_G(H)$. The number of conjugates of H is $(G : N) \leq (G : H)$ (see 4.8). Since each conjugate of H has $(H : 1)$ elements and the conjugates overlap (at least) in $\{1\}$, we see that

$$\#\bigcup gHg^{-1} < (G : H)(H : 1) = (G : 1).$$

For the second part, choose S to be a set of representatives for the conjugacy classes.

21. According to 4.16, 4.17, there is a normal subgroup N of order p^2, which is commutative. Now show that G has an element c of order p not in N, and deduce that $G = N \rtimes \langle c \rangle$, etc..

22. Let H be a subgroup of index p, and let N be the kernel of $G \to \mathrm{Sym}(G/H)$ — it is the largest normal subgroup of G contained in H (see 4.20). If $N \neq H$, then $(H : N)$ is divisible by a prime $q \geq p$, and $(G : N)$ is divisible by pq. But pq doesn't divide $p!$ — contradiction.

23. Embed G into S_{2m}, and let $N = A_{2m} \cap G$. Then $G/N \hookrightarrow S_{2m}/A_{2m} = C_2$, and so $(G : N) \leq 2$. Let a be an element of order 2 in G, and let $b_1, \ldots, b_m$ be a set of right coset representatives for $\langle a \rangle$ in G, so that $G = \{b_1, ab_1, \ldots, b_m, ab_m\}$. The image of a in S_{2m} is the product of the m transpositions $(b_1, ab_1), \ldots, (b_m, ab_m)$, and since m is odd, this implies that $a \notin N$.

24. (a) The number of possible first rows is $2^3 - 1$; of second rows $2^3 - 2$; of third rows $2^3 - 2^2$; whence $(G : 1) = 7 \times 6 \times 4 = 168$.
(b) Let $V = \mathbb{F}_2^3$. Then $\#V = 2^3 = 8$. Each line through the origin contains exactly one point $\neq$ origin, and so $\#X = 7$.
(c) We make a list of possible characteristic and minimal polynomials:

	Characteristic poly.	Min'l poly.	Size	Order of element in class
1	$X^3 + X^2 + X + 1$	$X + 1$	1	1
2	$X^3 + X^2 + X + 1$	$(X+1)^2$	21	2
3	$X^3 + X^2 + X + 1$	$(X+1)^3$	42	4
4	$X^3 + 1 = (X+1)(X^2 + X + 1)$	Same	56	3
5	$X^3 + X + 1$ (irreducible)	Same	24	7
6	$X^3 + X^2 + 1$ (irreducible)	Same	24	7

Here size denotes the number of elements in the conjugacy class.
Case 5: Let α be an endomorphism with characteristic polynomial $X^3 + X + 1$. Check from its minimal polynomial that $\alpha^7 = 1$, and so α has order 7. Note that V is a free $\mathbb{F}_2[\alpha]$-module of rank one, and so the centralizer of α in G is $\mathbb{F}_2[\alpha] \cap G = \langle \alpha \rangle$. Thus $\#C_G(\alpha) = 7$, and the number of elements in the conjugacy class of α is $168/7 = 24$.
Case 6: Exactly the same as Case 5.
Case 4: Here $V = V_1 \oplus V_2$ as an $\mathbb{F}_2[\alpha]$-module, and

$$\mathrm{End}_{\mathbb{F}_2[\alpha]}(V) = \mathrm{End}_{\mathbb{F}_2[\alpha]}(V_1) \oplus \mathrm{End}_{\mathbb{F}_2[\alpha]}(V_2).$$

Deduce that $\#C_G(\alpha) = 3$, and so the number of conjugates of α is $\frac{168}{3} = 56$.
Case 3: Here $C_G(\alpha) = \mathbb{F}_2[\alpha] \cap G = \langle \alpha \rangle$, which has order 4.
Case 1: Here α is the identity element.
Case 2: Here $V = V_1 \oplus V_2$ as an $\mathbb{F}_2[\alpha]$-module, where α acts as 1 on V_1 and has minimal polynomial $X^2 + 1$ on V_2. Either analyse, or simply note that this conjugacy class contains all the remaining elements.

(d) Since $168 = 2^3 \times 3 \times 7$, a proper nontrivial subgroup H of G will have order

$$2, 4, 8, 3, 6, 12, 24, 7, 14, 28, 56, 21, 24, \text{ or } 84.$$

If H is normal, it will be a disjoint union of $\{1\}$ and some other conjugacy classes, and so $(N : 1) = 1 + \sum c_i$ with c_i equal to 21, 24, 42, or 56, but this doesn't happen.

25. Since $G/Z(G) \hookrightarrow \mathrm{Aut}(G)$, we see that $G/Z(G)$ is cyclic, and so by (4.18) that G is commutative. If G is finite and not cyclic, it has a factor $C_{p^r} \times C_{p^s}$ etc..

26. Clearly $(ij) = (1j)(1i)(1j)$. Hence any subgroup containing $(12), (13), \ldots$ contains all transpositions, and we know S_n is generated by transpositions.

27. Note that $C_G(x) \cap H = C_H(x)$, and so $H/C_H(x) \approx H \cdot C_G(x)/C_G(x))$. Prove each class has the same number c of elements. Then

$$\#K = (G : C_G(x)) = (G : H \cdot C_G(x))(H \cdot C_G(x) : C_G(x)) = kc.$$

28. (a) The first equivalence follows from the preceding problem. For the second, note that σ commutes with all cycles in its decomposition, and so they must be even (i.e., have odd length); if two cycles have the same odd length k, one can find a product of k transpositions which interchanges them, and commutes with σ; conversely, show that if the partition of n defined by σ consists of distinct integers, then σ commutes only with the group generated by the cycles in its cycle decomposition.

(b) List of conjugacy classes in S_7, their size, parity, and (when the parity is even) whether it splits in A_7.

	Cycle	Size	Parity	Splits in A_7?	$C_7(\sigma)$ contains
1	(1)	1	E	N	
2	(12)	21	O		
3	(123)	70	E	N	(67)
4	(1234)	210	O		
5	(12345)	504	E	N	(67)
6	(123456)	840	O		
7	(1234567)	720	E	Y	720 doesn't divide 2520
8	$(12)(34)$	105	E	N	(67)
9	$(12)(345)$	420	O		
10	$(12)(3456)$	630	E	N	(12)
11	$(12)(3456)$	504	O		
12	$(123)(456)$	280	E	N	$(14)(25)(36)$
13	$(123)(4567)$	420	O		
14	$(12)(34)(56)$	105	O		
15	$(12)(34)(567)$	210	E	N	(12)

29. According to Maple, $n = 6$, $a \mapsto (13)(26)(45)$, $b \mapsto (12)(34)(56)$.

30. Since $\mathrm{Stab}(gx_0) = g\,\mathrm{Stab}(x_0)g^{-1}$, if $H \subset \mathrm{Stab}(x_0)$ then $H \subset \mathrm{Stab}(x)$ for all x, and so $H = 1$, contrary to hypothesis. Now $\mathrm{Stab}(x_0)$ is maximal, and so $H \cdot \mathrm{Stab}(x_0) = G$, which shows that H acts transitively.

B Review Problems

34. Prove that a finite group G having just one maximal subgroup must be a cyclic p-group, p prime.

35. Let a and b be two elements of S_{76}. If a and b both have order 146 and $ab = ba$, what are the possible orders of the product ab?

37. Suppose that the group G is generated by a set X.

(a) Show that if $gxg^{-1} \in X$ for all $x \in X$, $g \in G$, then the commutator subgroup of G is generated by the set of all elements $xyx^{-1}y^{-1}$ for $x, y \in X$.

(b) Show that if $x^2 = 1$ for all $x \in X$, then the subgroup H of G generated by the set of all elements xy for $x, y \in X$ has index 1 or 2.

38. Suppose $p \geq 3$ and $2p - 1$ are both prime numbers (e.g., $p = 3, 7, 19, 31, \ldots$). Prove, or disprove by example, that every group of order $p(2p - 1)$ is commutative.

39. Let H be a subgroup of a group G. Prove or disprove the following:

(a) If G is finite and P is a Sylow p-subgroup, then $H \cap P$ is a Sylow p-subgroup of H.

(b) If G is finite, P is a Sylow p-subgroup, and $H \supset N_G(P)$, then $N_G(H) = H$.

(c) If g is an element of G such that $gHg^{-1} \subset H$, then $g \in N_G(H)$.

40. Prove that there is no simple group of order 616.

41. Let n and k be integers $1 \leq k \leq n$. Let H be the subgroup of S_n generated by the cycle $(a_1 \ldots a_k)$. Find the order of the centralizer of H in S_n. Then find the order of the normalizer of H in S_n. [The ***centralizer*** of H is the set of $g \in G$ such $ghg^{=1} = h$ for all $h \in H$. It is again a subgroup of G.]

42. Prove or disprove the following statement: if H is a subgroup of an infinite group G, then for all $x \in G$, $xHx^{-1} \subset H \implies x^{-1}Hx \subset H$.

43. Let H be a finite normal subgroup of a group G, and let g be an element of G. Suppose that g has order n and that the only element of H that commutes with g is 1. Show that:

(a) the mapping $h \mapsto g^{-1}h^{-1}gh$ is a bijection from H to H;

(b) the coset gH consists of elements of G of order n.

44. Show that if a permutation in a subgroup G of S_n maps x to y, then the normalizers of the stabilizers $\mathrm{Stab}(x)$ and $\mathrm{Stab}(y)$ of x and y have the same order.

45. Prove that if all Sylow subgroups of a finite group G are normal and abelian, then the group is abelian.

46. A group is generated by two elements a and b satisfying the relations: $a^3 = b^2$, $a^m = 1$, $b^n = 1$ where m and n are positive integers. For what values of m and n can G be infinite.

47. Show that the group G generated by elements x and y with defining relations $x^2 = y^3 = (xy)^4 = 1$ is a finite solvable group, and find the order of G and its successive derived subgroups G', G'', G'''.

48. A group G is generated by a normal set X of elements of order 2. Show that the commutator subgroup G' of G is generated by all squares of products xy of pairs of elements of X.

49. Determine the normalizer N in $\mathrm{GL}_n(F)$ of the subgroup H of diagonal matrices, and prove that N/H is isomorphic to the symmetric group S_n.

50. Let G be a group with generators x and y and defining relations x^2, y^5, $(xy)^4$. What is the index in G of the commutator group G' of G.

51. Let G be a finite group, and H the subgroup generated by the elements of odd order. Show that H is normal, and that the order of G/H is a power of 2.

52. Let G be a finite group, and P a Sylow p-subgroup. Show that if H is a subgroup of G such that $N_G(P) \subset H \subset G$, then

(a) the normalizer of H in G is H;

(b) $(G : H) \equiv 1$ (mod p).

53. Let G be a group of order $33 \cdot 25$. Show that G is solvable. (Hint: A first step is to find a normal subgroup of order 11 using the Sylow theorems.)

54. Suppose that α is an endomorphism of the group G that maps G onto G and commutes with all inner automorphisms of G. Show that if G is its own commutator subgroup, then $\alpha x = x$ for all x in G.

55. Let G be a finite group with generators s and t each of order 2. Let $n = (G : 1)/2$.

(a) Show that G has a cyclic subgroup of order n. Now assume n odd.

(b) Describe all conjugacy classes of G.

(c) Describe all subgroups of G of the form $C(x) = \{y \in G | xy = yx\}$, $x \in G$.

(d) Describe all cyclic subgroups of G.

(e) Describe all subgroups of G in terms of (b) and (d).

(f) Verify that any two p-subgroups of G are conjugate (p prime).

56. Let G act transitively on a set X. Let N be a normal subgroup of G, and let Y be the set of orbits of N in X. Prove that:

(a) There is a natural action of G on Y which is transitive and shows that every orbit of N on X has the same cardinality.

(b) Show by example that if N is not normal then its orbits need not have the same cardinality.

57. Prove that every maximal subgroup of a finite p-group is normal of prime index (p is prime).

58. A group G is *metacyclic* if it has a cyclic normal subgroup N with cyclic quotient G/N. Prove that subgroups and quotient groups of metacyclic groups are metacyclic. Prove or disprove that direct products of metacyclic groups are metacylic.

59. Let G be a group acting doubly transitively on X, and let $x \in X$. Prove that:

(a) The stabilizer G_x of x is a maximal subgroup of G.

(b) If N is a normal subgroup of G, then either N is contained in G_x or it acts transitively on X.

60. Let x, y be elements of a group G such that $xyx^{-1} = y^5$, x has order 3, and $y \neq 1$ has odd order. Find (with proof) the order of y.

61. Let H be a maximal subgroup of G, and let A be a normal subgroup of H and such that the conjugates of A in G generate it.

(a) Prove that if N is a normal subgroup of G, then either $N \subset H$ or $G = NA$.

(b) Let M be the intersection of the conjugates of H in G. Prove that if G is equal to its commutator subgroup and A is abelian, then G/M is a simple group.

62. (a) Prove that the center of a nonabelian group of order p^3, p prime, has order p.
(b) Exhibit a nonabelian group of order 16 whose center is not cyclic.

63. Show that the group with generators α and β and defining relations

$$\alpha^2 = \beta^2 = (\alpha\beta)^3 = 1$$

is isomorphic with the symmetric group S_3 of degree 3 by giving, with proof, an explicit isomorphism.

64. Prove or give a counter-example:

(a) Every group of order 30 has a normal subgroup of order 15.

(b) Every group of order 30 is nilpotent.

65. Let $t \in \mathbb{Z}$, and let G be the group with generators x, y and relations $xyx^{-1} = y^t$, $x^3 = 1$.

(a) Find necessary and sufficient conditions on t for G to be finite.

(b) In case G is finite, determine its order.

66. Let G be a group of order pq, $p \neq q$ primes.

(a) Prove G is solvable.

(b) Prove that G is nilpotent $\iff$ G is abelian $\iff$ G is cyclic.

(c) Is G always nilpotent? (Prove or find a counterexample.)

67. Let X be a set with p^n elements, p prime, and let G be a finite group acting transitively on X. Prove that every Sylow p-subgroup of G acts transitively on X.

68. Let $G = \langle a, b, c \mid bc = cb, a^4 = b^2 = c^2 = 1, aca^{-1} = c, aba^{-1} = bc \rangle$. Determine the order of G and find the derived series of G.

69. Let N be a nontrivial normal subgroup of a nilpotent group G. Prove that $N \cap Z(G) \neq 1$.

70. Do not assume Sylow's theorems in this problem.

(a) Let H be a subgroup of a finite group G, and P a Sylow p-subgroup of G. Prove that there exists an $x \in G$ such that $xPx^{-1} \cap H$ is a Sylow p-subgroup of H.

(b) Prove that the group of $n \times n$ matrices $\begin{pmatrix} 1 & * & \cdots \\ 0 & 1 & \cdots \\ & \cdots & \\ 0 & & 1 \end{pmatrix}$ is a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.

(c) Indicate how (a) and (b) can be used to prove that any finite group has a Sylow p-subgroup.

71. Suppose H is a normal subgroup of a finite group G such that G/H is cyclic of order n, where n is relatively prime to $(G : 1)$. Prove that G is equal to the semi-direct product $H \rtimes S$ with S a cyclic subgroup of G of order n.

72. Let H be a minimal normal subgroup of a finite solvable group G. Prove that H is isomorphic to a direct sum of cyclic groups of order p for some prime p.

73. (a) Prove that subgroups A and B of a group G are of finite index in G if and only if $A \cap B$ is of finite index in G.
(b) An element x of a group G is said to be an *FC-element* if its centralizer $C_G(x)$ has finite index in G. Prove that the set of all FC elements in G is a normal.

74. Let G be a group of order p^2q^2 for primes $p > q$. Prove that G has a normal subgroup of order p^n for some $n \geq 1$.

75. (a) Let K be a finite nilpotent group, and let L be a subgroup of K such that $L{\cdot}\delta K = K$, where δK is the derived subgroup. Prove that $L = K$. [You may assume that a finite group is nilpotent if and only if every maximal subgroup is normal.]
(b) Let G be a finite group. If G has a subgroup H such that both $G/\delta H$ and H are nilpotent, prove that G is nilpotent.

76. Let G be a finite noncyclic p-group. Prove that the following are equivalent:

(a) $(G : Z(G)) \leq p^2$.
(b) Every maximal subgroup of G is abelian.
(c) There exist at least two maximal subgroups that are abelian.

77. Prove that every group G of order 56 can be written (nontrivially) as a semidirect product. Find (with proofs) two non-isomorphic non-abelian groups of order 56.

78. Let G be a finite group and $\varphi : G \to G$ a homomorphism.

(a) Prove that there is an integer $n \geq 0$ such that $\varphi^n(G) = \varphi^m(G)$ for all integers $m \geq n$. Let $\alpha = \varphi^n$.
(b) Prove that G is the semi-direct product of the subgroups $\operatorname{Ker}\alpha$ and $\operatorname{Im}\alpha$.
(c) Prove that $\operatorname{Im}\alpha$ is normal in G or give a counterexample.

79. Let S be a set of representatives for the conjugacy classes in a finite group G and let H be a subgroup of G. Show that $S \subset H \implies H = G$.

80. Let G be a finite group.

(a) Prove that there is a unique normal subgroup K of G such that (i) G/K is solvable and (ii) if N is a normal subgroup and G/N is solvable, then $N \supset K$.
(b) Show that K is characteristic.
(c) Prove that $K = [K, K]$ and that $K = 1$ or K is nonsolvable.

C Two-Hour Examination

1. Which of the following statements are true (give *brief* justifications for each of (a), (b), (c), (d); give a correct set of implications for (e)).

(a) If a and b are elements of a group, then $a^2 = 1, \quad b^3 = 1 \implies (ab)^6 = 1$.

(b) The following two elements are conjugate in S_7:

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

(c) If G and H are finite groups and $G \times A_{594} \approx H \times A_{594}$, then $G \approx H$.

(d) The only subgroup of A_5 containing (123) is A_5 itself.

(e) Nilpotent $\implies$ cyclic $\implies$ commutative $\implies$ solvable (for a finite group).

2. How many Sylow 11-subgroups can a group of order $110 = 2 \cdot 5 \cdot 11$ have? Classify the groups of order 110 containing a subgroup of order 10. Must every group of order 110 contain a subgroup of order 10?

3. Let G be a finite nilpotent group. Show that if every commutative quotient of G is cyclic, then G itself is cyclic. Is the statement true for nonnilpotent groups?

4. (a) Let G be a subgroup of $\mathrm{Sym}(X)$, where X is a set with n elements. If G is commutative and acts transitively on X, show that each element $g \neq 1$ of G moves every element of X. Deduce that $(G : 1) \leq n$.
(b) For each $m \geq 1$, find a commutative subgroup of S_{3m} of order 3^m.
(c) Show that a commutative subgroup of S_n has order $\leq 3^{\frac{n}{3}}$.

5. Let H be a normal subgroup of a group G, and let P be a subgroup of H. Assume that every automorphism of H is inner. Prove that $G = H \cdot N_G(P)$.

6. (a) Describe the group with generators x and y and defining relation $yxy^{-1} = x^{-1}$.
(b) Describe the group with generators x and y and defining relations $yxy^{-1} = x^{-1}$, $xyx^{-1} = y^{-1}$.

You may use results proved in class or in the notes, but you should indicate clearly what you are using.

Solutions

1. (a) False: in $\langle a, b | a^2, b^3 \rangle$, ab has infinite order.

(b) True, the cycle decompositions are (1357)(246), (123)(4567).

(c) True, use the Krull-Schmidt theorem.

(d) False, the group it generates is proper.

(e) Cyclic $\implies$ commutative $\implies$ nilpotent $\implies$ solvable.

2. The number of Sylow 11-subgroups $s_{11} = 1, 12, \ldots$ and divides 10. Hence there is only one Sylow 11-subgroup P. Have

$$G = P \rtimes_\theta H, \quad P = C_{11}, \quad H = C_{10} \text{ or } D_5.$$

Now have to look at the maps $\theta : H \to \mathrm{Aut}(C_{11}) = C_{10}$. Yes, by the Schur-Zassenhaus lemma.

3. Suppose G has class > 1. Then G has quotient H of class 2. Consider

$$1 \to Z(H) \to H \to H/Z(H) \to 1.$$

Then H is commutative by (4.17), which is a contradiction. Therefore G is commutative, and hence cyclic.

Alternatively, by induction, which shows that $G/Z(G)$ is cyclic.

No! In fact, it's not even true for solvable groups (e.g., S_3).

4. (a) If $gx = x$, then $ghx = hgx = hx$. Hence g fixes every element of X, and so $g = 1$. Fix an $x \in X$; then $g \mapsto gx : G \to X$ is injective. [Note that Cayley's theorem gives an embedding $G \hookrightarrow S_n$, $n = (G:1)$.]

(b) Partition the set into subsets of order 3, and let $G = G_1 \times \cdots \times G_m$.

(c) Let $O_1, \ldots, O_r$ be the orbits of G, and let G_i be the image of G in $\mathrm{Sym}(O_i)$. Then $G \hookrightarrow G_1 \times \cdots \times G_r$, and so (by induction),

$$(G:1) \le (G_1:1) \cdots (G_r:1) \le 3^{\frac{n_1}{3}} \cdots 3^{\frac{n_r}{3}} = 3^{\frac{n}{3}}.$$

5. Let $g \in G$, and let $h \in H$ be such that conjugation by h on H agrees with conjugation by g. Then $gPg^{-1} = hPh^{-1}$, and so $h^{-1}g \in N_G(P)$.

6. (a) It's the group .

$$G = \langle x \rangle \rtimes \langle y \rangle = C_\infty \rtimes_\theta C_\infty$$

with $\theta \colon C_\infty \to \mathrm{Aut}(C_\infty) = \pm 1$. Alternatively, the elements can be written uniquely in the form $x^i y^j$, $i, j \in \mathbb{Z}$, and $yx = x^{-1}y$.

(b) It's the quaternion group. From the two relations get

$$yx = x^{-1}y, \quad yx = xy^{-1}$$

and so $x^2 = y^2$. The second relation implies

$$xy^2x^{-1} = y^{-2}, = y^2,$$

and so $y^4 = 1$.

Alternatively, the Todd-Coxeter algorithm shows that it is the subgroup of S_8 generated by $(1287)(3465)$ and $(1584)(2673)$.

Index