Basic Definitions and Results

> *The axioms for a group are short and natural.... Yet somehow hidden behind these axioms is the monster simple group, a huge and extraordinary mathematical object, which appears to rely on numerous bizarre coincidences to exist. The axioms for groups give no obvious hint that anything like this exists.*
>
> Richard Borcherds, in *Mathematicians: An Outer View....*

> *The one thing I would really like to know before I die is why the monster group exists.*
>
> John Conway, in a 2014 interview on Numberphile.

Group theory is the study of symmetries.

Definitions and examples

DEFINITION 1.1 A ***group*** is a set G together with a binary operation

$$(a,b) \mapsto a * b \colon G \times G \to G$$

satisfying the following conditions:

G1: (associativity) for all $a,b,c \in G$,

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

G2: (existence of a neutral element) there exists an element $e \in G$ such that

$$a * e = a = e * a \tag{1}$$

for all $a \in G$;

G3: (existence of inverses) for each $a \in G$, there exists an $a' \in G$ such that

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

We usually abbreviate $(G,*)$ to G. Also, we usually write ab for $a*b$ and 1 for e; alternatively, we write $a+b$ for $a*b$ and 0 for e. In the first case, the group is said to be ***multiplicative***, and in the second, it is said to be ***additive***.

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

(a) An element e satisfying (1) is called a ***neutral element***. If e' is a second such element, then $e' = e * e' = e$. In fact, e is the unique element of G satisfying $x * x = x$ (apply G3).

(b) If $b * a = e$ and $a * c = e$, then

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

Hence the element a' in (G3) 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 (G1) shows that the product of any ordered triple a_1, a_2, a_3 of elements of G is unambiguously defined: whether we form $a_1 a_2$ first and then $(a_1 a_2) a_3$, or $a_2 a_3$ first and then $a_1(a_2 a_3)$, the result is the same. In fact, (G1) 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

$$(a_1 \cdots a_i)(a_{i+1} \cdots a_n) \tag{2}$$

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

$$(a_1 \cdots a_j)(a_{j+1} \cdots a_n). \tag{3}$$

Note that the expression within each pair of parentheses is well defined because of the induction hypotheses. Thus, if $i = j$, (2) equals (3). If $i \neq j$, we may suppose $i < j$. Then

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

and the expressions on the right are equal because of (G1).

(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) (G3) implies that the cancellation laws hold in groups,

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

(multiply on left or right by a^{-1}). Conversely, if G is *finite*, then the cancellation laws imply (G3): the map $x \mapsto ax\colon G \to G$ is injective, and hence (by counting) bijective; in particular, e 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 are equal.

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

The ***order*** $|G|$ of a group G is its cardinality. 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

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

The usual rules hold:

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad \text{all } m,n \in \mathbb{Z}. \tag{4}$$

It follows from (4) that the set

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

is an ideal in $\mathbb{Z}$, and so equals $m\mathbb{Z}$ for some integer $m \geq 0$. When $m = 0$, $a^n \neq e$ unless $n = 0$, and a is said to have ***infinite order***. When $m \neq 0$, it is the smallest integer $m > 0$ such that $a^m = e$, and a is said to have ***finite order*** m. In this case, $a^{-1} = a^{m-1}$, and

$$a^n = e \iff m|n.$$

Examples

1.3 Let C_∞ be the group $(\mathbb{Z}, +)$, and, for an integer $m \geq 1$, let C_m be the group $(\mathbb{Z}/m\mathbb{Z}, +)$.

1.4 ***Permutation groups.*** Let S be a set and let $\mathrm{Sym}(S)$ be the set of bijections $\alpha\colon S \to S$. We define the product of two elements of $\mathrm{Sym}(S)$ to be their composite:

$$\alpha\beta = \alpha \circ \beta.$$

In other words, $(\alpha\beta)(s) = \alpha(\beta(s))$ for all $s \in S$. For any $\alpha, \beta, \gamma \in \mathrm{Sym}(S)$ and $s \in S$,

$$((\alpha \circ \beta) \circ \gamma)(s) = (\alpha \circ \beta)(\gamma(s)) = \alpha(\beta(\gamma(s))) = (\alpha \circ (\beta \circ \gamma))(s), \tag{5}$$

and so associativity holds. The identity map $s \mapsto s$ is an identity element for $\mathrm{Sym}(S)$, and inverses exist because we required the elements of $\mathrm{Sym}(S)$ to be bijections. Therefore $\mathrm{Sym}(S)$ is a group, called the ***group of symmetries*** of S. For example, the ***permutation group on** n **letters*** S_n is defined to be the group of symmetries of the set $\{1, ..., n\}$ — it has order $n!$.

1.5 When G and H are groups, 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

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

1.6 A group G is ***commutative*** (or ***abelian***)[1] if

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

In a commutative group, the product of any finite (not necessarily ordered) family S of elements is well defined, for example, the empty product is e. Usually, we write commutative groups additively. With this notation, Equation (4) becomes:

$$ma + na = (m+n)a, \quad m(na) = mna.$$

When G is commutative,

$$m(a+b) = ma + mb \text{ for } m \in \mathbb{Z} \text{ and } a,b \in G,$$

[1] "Abelian group" is more common than "commutative group", but I prefer to use descriptive names.

and so the map

$$(m,a) \mapsto ma\colon \mathbb{Z} \times G \to G$$

makes G into a $\mathbb{Z}$-module. In a commutative group G, the elements of finite order form a subgroup G_{tors} of G, called the ***torsion subgroup***.

1.7 Let F be a field. The $n \times n$ matrices with coefficients in F and nonzero determinant form a group $\mathrm{GL}_n(F)$ called the ***general linear group of degree*** n. For a finite-dimensional F-vector space V, the F-linear automorphisms of V form a group $\mathrm{GL}(V)$ called the ***general linear group of*** V. Note that if V has dimension n, then the choice of a basis determines an isomorphism $\mathrm{GL}(V) \to \mathrm{GL}_n(F)$ sending an automorphism to its matrix with respect to the basis.

1.8 Let V be a finite-dimensional vector space over a field F. A bilinear form on V is a mapping $\phi\colon V \times V \to F$ that is linear in each variable. An ***automorphism*** of such a ϕ is an isomorphism $\alpha\colon V \to V$ such that

$$\phi(\alpha v, \alpha w) = \phi(v,w) \text{ for all } v,w \in V. \tag{6}$$

The automorphisms of ϕ form a group $\mathrm{Aut}(\phi)$. Let $\{e_1,\ldots,e_n\}$ be a basis for V, and let

$$P = (\phi(e_i,e_j))_{1 \le i,j \le n}$$

be the matrix of ϕ. The choice of the basis identifies $\mathrm{Aut}(\phi)$ with the group of invertible matrices A such that[2]

$$A^{\mathrm{T}} \cdot P \cdot A = P. \tag{7}$$

When ϕ is symmetric, i.e.,

$$\phi(v,w) = \phi(w,v) \text{ all } v,w \in V,$$

and nondegenerate, $\mathrm{Aut}(\phi)$ is called the ***orthogonal group*** of ϕ.

When ϕ is skew-symmetric, i.e.,

$$\phi(v,w) = -\phi(w,v) \text{ all } v,w \in V,$$

and nondegenerate, $\mathrm{Aut}(\phi)$ is called the ***symplectic group*** of ϕ. In this case, there exists a basis for V for which the matrix of ϕ is

$$J_{2m} = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}, \quad 2m = n,$$

[2] When we use the basis to identify V with F^n, the pairing ϕ becomes

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \mapsto (a_1,\ldots,a_n) \cdot P \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

If A is the matrix of α with respect to the basis, then α corresponds to the map $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto A \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$.Therefore, (6) becomes the statement that

$$(a_1,\ldots,a_n) \cdot A^{\mathrm{T}} \cdot P \cdot A \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = (a_1,\ldots,a_n) \cdot P \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \text{ for all } \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in F^n.$$

On examining this statement on the standard basis vectors for F^n, we see that it is equivalent to (7).

and the group of invertible matrices A such that

$$A^{\mathrm{T}} J_{2m} A = J_{2m}$$

is called the symplectic group Sp_{2m}.

REMARK 1.9 A set S together with a binary operation $(a,b) \mapsto a \cdot b \colon S \times S \to S$ is called a ***magma***. When the binary operation is associative, $(S,\cdot)$ is called a ***semigroup***. The product

$$\prod A \overset{\text{def}}{=} a_1 \cdots a_n$$

of any sequence $A = (a_i)_{1 \le i \le n}$ of elements in a semigroup S is well-defined (see 1.2(c)), and for any pair A and B of such sequences,

$$\left(\prod A\right)\left(\prod B\right) = \prod (A \sqcup B). \tag{8}$$

Let $\emptyset$ be the empty sequence, i.e., the sequence of elements in S indexed by the empty set. What should $\prod \emptyset$ be? Clearly, we should have

$$\left(\prod \emptyset\right)\left(\prod A\right) = \prod (\emptyset \sqcup A) = \prod A = \prod (A \sqcup \emptyset) = \left(\prod A\right)\left(\prod \emptyset\right).$$

In other words, $\prod \emptyset$ should be a neutral element. A semigroup with a neutral element is called a ***monoid***. In a monoid, the product of any finite (possibly empty) sequence of elements is well-defined, and (8) holds.

ASIDE 1.10 (a) The group conditions (G2,G3) can be replaced by the following weaker conditions (existence of a left neutral element and left inverses): (G2′) there exists an e such that $e * a = a$ for all a; (G3′) for each $a \in G$, there exists an $a' \in G$ such that $a' * a = e$. To see that these imply (G2) and (G3), let $a \in G$, and apply (G3′) to find a' and a'' such that $a' * a = e$ and $a'' * a' = e$. Then

$$a * a' = e * (a * a') = (a'' * a') * (a * a') = a'' * \left((a' * a) * a'\right) = a'' * a' = e,$$

whence (G3), and

$$a = e * a = (a * a') * a = a * (a' * a) = a * e,$$

whence (G2).

(b) A group can be defined to be a set G with a binary operation $*$ satisfying the following conditions: (g1) $*$ is associative; (g2) G is nonempty; (g3) for each $a \in G$, there exists an $a' \in G$ such that $a' * a$ is neutral. As there is at most one neutral element in a set with an associative binary operation, these conditions obviously imply those in (a). They are minimal in the sense that there exist sets with a binary operation satisfying any two of them but not the third. For example, $(\mathbb{N},+)$ satisfies (g1) and (g2) but not (g3); the empty set satisfies (g1) and (g3) but not (g2); the set of integers with $m * n = m - n$ satisfies (g2) and (g3) but not (g1).

Multiplication tables

A binary operation on a finite set can be described by its multiplication table:

	e	a	b	c	$\ldots$
e	ee	ea	eb	ec	$\ldots$
a	ae	a^2	ab	ac	$\ldots$
b	be	ba	b^2	bc	$\ldots$
c	ce	ca	cb	c^2	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

The element e is an identity element if and only if the first row and column of the table simply repeat the elements. Inverses exist if and only if each element occurs exactly once in each row and in each column (see 1.2e). If there are n elements, then verifying the associativity law requires checking n^3 equalities.

For the multiplication table of S_3, see the front page. Note that each colour occurs exactly once in each row and and each column.

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, then that gives a total of n^{n^2} possible tables very few of which define groups. For example, there are $8^{64} = 6277\,101\,735\,386\,680\,763\,835\,789\,423\,207\,666\,416\,102\,355\,444\,464\,034\,512\,896$ binary operations on a set with 8 elements, but only five isomorphism classes of groups of order 8 (see 4.21).

Subgroups

PROPOSITION 1.11 *Let S be a nonempty subset of a group G. If*

S1: $a,b \in S \implies ab \in S$, *and*
S2: $a \in S \implies a^{-1} \in S$,

then the binary operation on G makes S into a group.

PROOF. (S1) implies that the binary operation on G defines a binary operation $S \times S \to S$ on S, which is automatically associative. By assumption S contains at least one element a, its inverse a^{-1}, and the product $e = aa^{-1}$. Finally (S2) shows that the inverses of elements in S lie in S. □

A nonempty subset S satisfying (S1) and (S2) is called a ***subgroup*** of G. When S is finite, condition (S1) implies (S2): let $a \in S$; then $\{a, a^2, \ldots\} \subset S$, and so a has finite order, say $a^n = e$; now $a^{-1} = a^{n-1} \in S$. The example $(\mathbb{N}, +) \subset (\mathbb{Z}, +)$ shows that (S1) does not imply (S2) when S is infinite.

EXAMPLE 1.12 The ***centre*** of a group G is the subset

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

It is a subgroup of G.

PROPOSITION 1.13 *An intersection of subgroups of G is a subgroup of G.*

PROOF. It is nonempty because it contains e, and (S1) and (S2) obviously hold. □

REMARK 1.14 It is generally true that an intersection of subobjects of an algebraic object is a subobject. For example, an intersection of subrings of a ring is a subring, an intersection of submodules of a module is a submodule, and so on.

PROPOSITION 1.15 *For any subset X of a group G, there is a smallest subgroup of G containing X. It consists of all finite products of elements of X and their inverses (repetitions allowed).*

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 (S1) and (S2) and hence is a subgroup containing X. It therefore equals S. □

The subgroup S given by the proposition is denoted $\langle X\rangle$, and is called the ***subgroup generated by*** X. For example, $\langle\emptyset\rangle = \{e\}$. If every element of X has finite order, for example, if G is finite, then the set of all finite products of elements of X is already a group 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.

EXAMPLES

1.16 ***The cyclic groups.*** A group is said to be ***cyclic*** if it is generated by a single element, i.e., if $G = \langle r\rangle$ for some $r \in G$. If r has finite order n, then

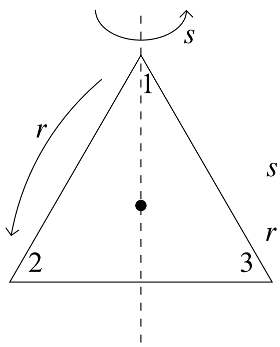
$$G = \{e, r, r^2, ..., r^{n-1}\} \approx C_n, \quad r^i \leftrightarrow i \mod n,$$

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

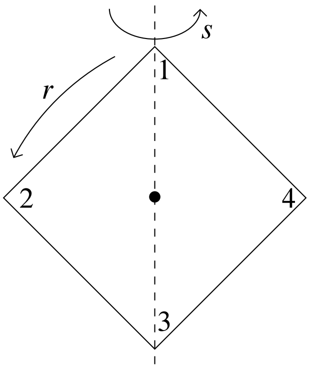
$$G = \{\dots, r^{-i}, \dots, r^{-1}, e, r, \dots, r^i, \dots\} \approx C_\infty, \quad r^i \leftrightarrow i.$$

Thus, up to isomorphism, there is exactly one cyclic group of order n for each $n \leq \infty$. In future, we shall loosely use C_n to denote any cyclic group of order n (not necessarily $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}$).

1.17 ***The dihedral groups*** D_n.[3] For $n \geq 3$, D_n is the group of symmetries of a regular polygon with n-sides.[4] Number the vertices $1, \dots, n$ in the counterclockwise direction. Let r be the rotation through $2\pi/n$ about the centre of polygon (so $i \mapsto i+1 \mod n$), and let s be the reflection in the line (= rotation about the line) through the vertex 1 and the centre of the polygon (so $i \mapsto n+2-i \mod n$). For example, the pictures



$$s = \begin{cases} 1 \leftrightarrow 1 \\ 2 \leftrightarrow 3 \end{cases}$$
$$r = 1 \to 2 \to 3 \to 1$$



$$s = \begin{cases} 1 \leftrightarrow 1 \\ 2 \leftrightarrow 4 \\ 3 \leftrightarrow 3 \end{cases}$$
$$r = 1 \to 2 \to 3 \to 4 \to 1$$

[3] This group is denoted D_{2n} or D_n depending on whether the author is viewing it abstractly or concretely as the symmetries of an n-polygon (or perhaps on whether the author is a group theorist or not; see mo48434).

[4] More formally, D_n can be defined to be the subgroup of S_n generated by $r{:}i \mapsto i+1 \pmod n$ and $s{:}i \mapsto n+2-i \pmod n$. Then all the statements concerning D_n can proved without appealing to geometry.

illustrate the groups D_3 and D_4. In the general case

$$r^n = e; \quad s^2 = e; \quad srs = r^{-1} \quad (\text{so } sr = r^{n-1}s).$$

These equalites imply that

$$D_n = \{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\},$$

and it is clear from the geometry that the elements of the set are distinct, and so $|D_n| = 2n$.

Let t be the reflection in the line through the midpoint of the side joining the vertices 1 and 2 and the centre of the polygon (so $i \mapsto n+3-i \mod n$). Then $r = ts$, because

$$i \overset{s}{\mapsto} n+2-i \overset{t}{\mapsto} n+3-(n+2-i) = i+1 \mod n.$$

Hence $D_n = \langle s, t \rangle$ and

$$s^2 = e, \quad t^2 = e, \quad (ts)^n = e = (st)^n.$$

We define D_1 to be $C_2 = \{1, r\}$ and D_2 to be $C_2 \times C_2 = \{1, r, s, rs\}$. The group D_2 is also called the ***Klein Viserergruppe*** or, more simply, the ***4-group*** and denoted V or V_4. Note that D_3 is the full group of permutations of $\{1,2,3\}$. It is the smallest noncommutative group.

By adding a tick at each vertex of a regular polygon, we can reduce its symmetry group from D_n to C_n. By adding a line from the centre of the polygon to the vertex 1, we reduce its symmetry group to $\langle s \rangle$. Physicist like to say that we have “broken the symmetry”.

1.18 ***The quaternion group*** Q: Let $a = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then

$$a^4 = e, \quad a^2 = b^2, \quad bab^{-1} = a^3 \ (\text{so } ba = a^3 b).$$

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

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

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

$$\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

with the multiplication determined by

$$i^2 = -1 = j^2, \quad ij = k = -ji.$$

The map $i \mapsto a$, $j \mapsto b$ extends uniquely to a homomorphism $\mathbb{H} \to M_2(\mathbb{C})$ of $\mathbb{R}$-algebras, which maps the group $\langle i, j \rangle$ isomorphically onto $\langle a, b \rangle$.

1.19 Recall that S_n is the permutation group on $\{1, 2, ..., n\}$. A ***transposition*** is a permutation that interchanges two elements and leaves all other elements unchanged. It is not difficult to see that S_n is generated by transpositions (see (4.26) below for a more precise statement).

Groups of small order

> *[For] $n = 6$, there are three* (sic) *groups, a group C_6, and two groups $C_2 \times C_3$ and S_3.*
> Cayley, American J. Math. 1 (1878), p. 51.

For each prime p, there is only one group of order p, namely C_p (see 1.28 below). In the following table, $c + n = t$ means that there are c commutative groups and n noncommutative groups (up to isomorphism, of course).

$\lvert G\rvert$	$c+n=t$	Groups	Ref.
4	$2+0=2$	C_4, $C_2 \times C_2$	4.18
6	$1+1=2$	C_6; S_3	4.23
8	$3+2=5$	C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$; Q, D_4	4.21
9	$2+0=2$	C_9, $C_3 \times C_3$	4.18
10	$1+1=2$	C_{10}; D_5	5.14
12	$2+3=5$	C_{12}, $C_2 \times C_6$; $C_2 \times S_3$, A_4, $C_4 \rtimes C_3$	5.16
14	$1+1=2$	C_{14}; D_7	5.14
15	$1+0=1$	C_{15}	5.14
16	$5+9=14$	See Wild 2005	
18	$2+3=5$	C_{18}, $C_3 \times C_6$; D_9, $S_3 \times C_3$, $(C_3 \times C_3) \rtimes C_2$	
20	$2+3=5$	$C_{20}, C_2 \times C_{10}$; $D_{10}, C_5 \rtimes C_4, \langle a,b \mid a^5 = b^2 = c^2 = abc\rangle$	
21	$1+1=2$	C_{21}; $\langle a,b \mid a^3 = b^7 = 1, ba = ab^2\rangle$	
22	$1+1=2$	C_{22}; D_{11}	5.14
24	$3+12=15$	groupprops.subwiki.org/wiki/Groups_of_order_24	

Here $\langle a,b \mid a^5 = b^2 = c^2 = abc\rangle$ is the group with generators a and b and relations $a^5 = b^2 = c^2 = abc$ (see Chapter 2). It is the dicyclic group.

Roughly speaking, the more high powers of primes divide n, the more groups of order n there should be. 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 1993).

By 2001, a complete irredundant list of groups of order ≤ 2000 had been found — up to isomorphism, there are exactly 49,910,529,484 (Besche et al. 2001).[5]

[5] In fact Besche et al. did not construct the groups of order 1024 individually, but it is known that there are 49487365422 groups of that order. The remaining 423164062 groups of order up to 2000 (of which 408641062 have order 1536) are available as libraries in GAP and Magma. I would guess that 2048 is the smallest number such that the exact number of groups of that order is unknown (Derek Holt, mo46855; Nov 21, 2010).

Homomorphisms

Definition 1.20 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 $a, b \in G$. An ***isomorphism*** is a bijective homomorphism.

For example, the determinant map $\det\colon \mathrm{GL}_n(F) \to F^{\times}$ is a homomorphism.

1.21 Let α be a homomorphism. For any elements $a_1, \ldots, a_m$ of G,

$$\begin{aligned}\alpha(a_1 \cdots a_m) &= \alpha(a_1(a_2 \cdots a_m)) \\ &= \alpha(a_1)\alpha(a_2 \cdots a_m) \\ &\cdots \\ &= \alpha(a_1) \cdots \alpha(a_m),\end{aligned}$$

and so homomorphisms preserve all products. In particular, for $m \geq 1$,

$$\alpha(a^m) = \alpha(a)^m. \tag{9}$$

Moreover $\alpha(e) = \alpha(ee) = \alpha(e)\alpha(e)$, and so $\alpha(e) = e$ (apply 1.2a). Also

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

and so $\alpha(a^{-1}) = \alpha(a)^{-1}$. It follows that (9) holds for all $m \in \mathbb{Z}$, and so a homomorphism of commutative groups is also a homomorphism of $\mathbb{Z}$-modules.

As we noted above, 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 1.22 (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 $e_L = \mathrm{id}$, 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 1.23 *A finite group of order n can be realized as a subgroup of S_n.*

Proof. List the elements of the group as $a_1, \ldots, a_n$. □

Unfortunately, unless n is small, S_n is too large to be manageable. We shall see later (4.22) that G can often be embedded in a permutation group of much smaller order than $n!$.