CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	An introduction to group theory
Authors	McKay, Benjamin
Publication date	2022-03-17
Original Citation	McKay, B. (2022) An Introduction to Group Theory, Cork.
Type of publication	Book
Rights	© Benjamin McKay. This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported License - https://creativecommons.org/licenses/by-sa/4.0/
Download date	2025-07-31 10:57:13
Item downloaded from	https://hdl.handle.net/10468/13438

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Benjamin McKay

An Introduction to Group Theory

March 17, 2022

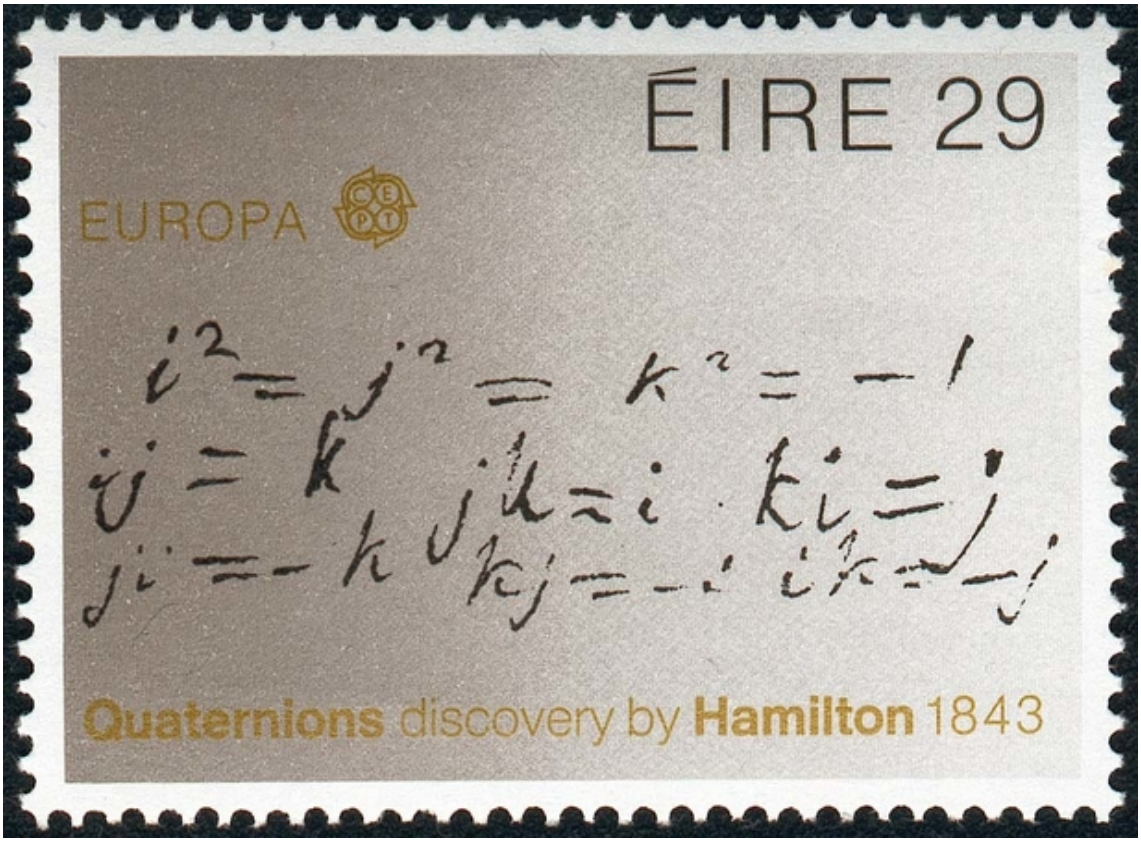
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported License.

Numbers measure quantity, groups measure symmetry

— Mark Armstrong
Groups and Symmetry

The theory of groups is, as it were, the whole of mathematics stripped of its matter and reduced to pure form.

— Henri Poincaré



Contents

Chapter 1

Transformations

Transformation groups

Take a set X, which could be a set of points in the plane, or a set of numbers, or a collection of various geometric figures, or the set of books in a library, or any other set of any sort of things. A *transformation* f of X associates to each element x of X some element $f(x)$ also from X.

Take a square X in the plane, and rotate it around its centre by a right angle. Each point p of X is rotated into some point $f(p)$. Note that the centre point of the square is "fixed", i.e. rotated into itself.

Take any set X. The *identity transformation* is the transformation that leaves every point of X where it is: $f(x) = x$.

Shuffle a deck of cards. If X is the set of cards, the shuffle is a transformation f of X.

Two maps $f\colon X \to Y$ and $g\colon Y \to X$ between sets are *inverses* if $f(g(x)) = x$ and $g(f(x)) = x$ for any element x of X. In other words, $f \circ g$ and $g \circ f$ are both the identity transformation. Recall that a map f is *invertible*, also called a *bijection* or a *permutation* if it has an inverse.

1.1 A map $f\colon X \to Y$ of a set X is *injective* (also called *one-to-one*) if $f(p) = f(q)$ only when $p = q$. It is *surjective* (also called *onto*) if every element y of Y has the form $y = f(x)$ for some element x of X. Prove that a map is a bijection just when it is injective and surjective.

1.2 Prove that a transformation f of a *finite* set X is injective just when it is surjective, and hence just when it is a bijection.

1.3 Prove the *associative law* for transformations: if f, g and h are transformations of a set X, then $(f \circ g) \circ h = f \circ (g \circ h)$.

1.4 Prove that a bijection f has a unique inverse.

The inverse of a bijection f is denoted f^{-1}.

A *transformation group* G on a set X is a nonempty collection of permutations of X so that

a. if f and g are in G then $f \circ g$ is in G.

b. if f is in G then f^{-1} is also in G.

Take X the Euclidean plane. Every rotation of the plane around the origin is by some angle, say θ. Conversely, every angle θ is the angle of some rotation around the origin. So angles form a transformation group G, the group of rotations of the plane X around the origin.

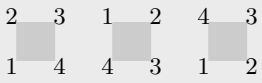
Take X to be three dimensional Euclidean space. Take a line ℓ through the origin, with a chosen direction along that line. Hold the line in your hand, so that your thumb points up the chosen direction. Your fingers curl around the line in a certain direction. In additional, take an angle θ, and rotate the whole space X around in the direction of your fingers, by the angle θ. Every rotation of Euclidean space X arises in this way. (If you change the choice of direction to point your thumb, but keep the same axis of rotation ℓ, then you change θ to $-\theta$.) When you compose a rotation with another rotation, the result is yet a third rotation. The rotations of Euclidean space form a transformation group G.

Take X to be the real number line. Given any real number t, we can define a transformation $f(x) = x + t$. In this way, the real numbers t are associated to the elements of a group G of transformations of the real number line.

A *rigid motion* of Euclidean space is a transformation that preserves distances. For example, rotations, mirror reflections: $(x, y) \mapsto (x, -y)$, and translations $(x, y) \mapsto (x + x_0, y + y_0)$ are rigid motions of the plane. The rigid motions form a transformation group.

Take a geometric figure X in the plane, or in space. A rigid motion preserving X is a *symmetry* of X; the symmetries of a figure constitute a transformation group.

If X is a square, every symmetry permutes the corners somehow, and we can easily see these symmetries:



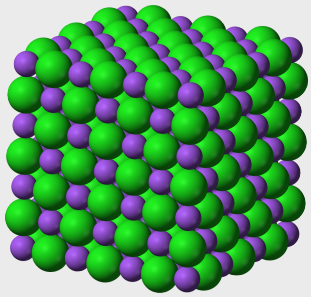
The symmetry group of a non-isosceles triangle consists just of the identity transformation.

For an isosceles, but not equilateral, triangle, the symmetry group is the identity transformation and the reflection across the axis of symmetry.

An equilateral triangle has as symmetries: the identity transformation, the rotation by 120°, the rotation by 240°, and the three reflections in the three axes of symmetry.

1.5 Consider a brick, i.e. a rectangular box whose length, width and height are all unequal. What is its symmetry group?

The symmetry group of an infinitely repeating sodium choride lattice



includes the translations of space that move each green chlorine atom and purple natrium atom to its neighbor, up, down, left, right, forward or back, and mirror reflections around the coordinate planes through the origin, where we put the origin in the middle of any one of these atoms, and also the transformations given by permuting the order of the variables x, y, z of each coordinate axis.

Every 2×2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(with entries from any chosen field) determines a *linear transformation*:

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

of the plane. Similarly, a square matrix A, say $n \times n$, determines a linear transformation of n-dimensional Euclidean space. A linear transformation is a bijection just when the associated matrix A is invertible, i.e. just when A has nonzero determinant. The invertible $n \times n$ matrices form a transformation group G, of linear transformations of n-dimensional Euclidean space.

Chapter 2

Permutations

Permutations

A transformation which is a bijection is also called a *permutation*, especially when it transforms a finite set.

Take X to be the set of numbers $\{1, 2, 3, 4\}$. The *symmetric group* on 4 letters is the group G of all permutations of X. The terminology "on 4 letters" reminds us that we could just as well have taken $X = \{a, b, c, d\}$ to consist of any 4 distinct elements, and then we would get essentially the same story, just relabelling. It is convenient notation to write a permutation of finite sets as, for example,

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

to mean the map f so that $f(1) = 2$, $f(2) = 3$, $f(3) = 1$ and $f(4) = 4$, i.e. reading down from the top row as the input to f to the entry underneath as the output of f. It is often understood that the first row is just 1234 or some such, so we can just write down the second row: 2314, to display the permutation.

2.1 What are the permutations $g \circ f$ and $f \circ g$ where g is 2314 and f is 3124?

2.2 A *regular tetrahedron* is a pyramid with triangular base, all of whose sides are equilateral triangles. Prove that the symmetry group of the regular tetrahedron is the symmetric group on 4 letters.

Another notation for permutations: the *cycle* (1342) means the permutation that takes 1 to 3, 3 to 4, 4 to 2 and 2 to 1, reading from left to right. More generally, the cycle $(a_1 a_2 \dots a_k)$ is the permutation taking a_1 to a_2, a_2 to a_3, and so on, and taking a_k to a_1. So (2314) takes 3 to 1. By definition, if we have a number x which is not among these various $a_1, a_2, \dots, a_k$, then the cycle $(a_1 a_2 \dots a_k)$ fixes the number x: (2354) takes 1 to 1. Two cycles $(a_1 a_2 \dots a_k)$ and $(b_1 b_2 \dots b_\ell)$ are *disjoint* if none of the a_i occur among the b_j and vice versa. So

(1452) is disjoint from (36),

but

(1352) is not disjoint from (36)

since they both have 3 in them. We can write the identity permutation as (). Note that any cycle of length 1 is also the identity transformation: (2) = (1) = (), since (2) takes 2 to 2, and fixes everything else. If two permutations f and g can be expressed as disjoint cycles, then $fg = gf$, since each fixes all of the letters moved by the other.

2.3 Write (123)(234)(543) as (a) a permutation in our first notation and (b) as a product of disjoint cycles.

Sage knows how to multiply cycles:

```
G = SymmetricGroup(5)
sigma = G("(1,3) (2,5,4)")
rho = G([(2,4), (1,5)])
rho^(-1) * sigma * rho
```

prints $(1,2,4)(3,5)$.

Theorem 2.1. *Every permutation of the elements of a finite set is expressed as a product of disjoint cycles, uniquely except for the order in which we write down the cycles, which can be arbitrary.*

Proof. Suppose our finite set is $1, 2, \ldots, n$; write these down in order in a list. Pick a number and see what the permutation takes it to, and what it takes that number to, and so on, until eventually you return to the number you started at: a cycle. Cross out all of those numbers from the list, and start again. □

For example, in cycle notation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (123)$$

and

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (13)(245).$$

2.4 What is the product of cycles (1234)(1423)(324) as a product of disjoint cycles? Explain how you find your answer.

2.5 Let G be the collection of all rotations of a cube. How many rotations lie in G? How does each decompose into a product of disjoint cycles acting on the faces of the cube?

2.6 Prove that any set with n elements has $n!$ permutations, in several ways: by counting

a. how many places to move 1 to, and then how many places there are left to move 2 to, and so on,

b. the number of places to stick object n in between the elements of any given permutation of the numbers $1, 2, \ldots, n-1$, for example: given the permutation 312 of the numbers 123, we can put 4 in there as

$$4312, 3412, 3142, \text{ or } 3124.$$

c. the number of ways to put at the end of a given permutation $a_1 a_2 \ldots a_{n-1}$ some number b from among

$$b = \frac{1}{2}, 1 + \frac{1}{2}, \ldots, n - \frac{1}{2},$$

for example into the permutation 312 we stick

$$312\frac{1}{2}, \quad \text{or } 312\frac{3}{2}, \quad \text{or } 312\frac{5}{2}, \quad \text{or } 312\frac{7}{2}$$

and then replace the numbers in the list by integers from $1, 2, \ldots, n$, but in the same order:

$$4231, 4132, 4123, \text{ or } 3124.$$

d. the possible disjoint cycles.

2.7 Suppose that g is a permutation written as a product of disjoint cycles, say $g = (1487)(235)$ as a permutation of 8 letters. Take any permutation h of 8 letters. Prove that

$$hgh^{-1} = (h(1)\ h(4)\ h(8)\ h(7))(h(2)\ h(3)\ h(5)).$$

2.8 Prove that there is an element g of the symmetric group on 7 letters so that $(147)(23)$ and $(235)(14)$ are conjugate, i.e. $(235)(14) = g(147)(23)g^{-1}$. More generally, prove that two elements of the symmetric group on n letters are conjugate just when, when we write them as products of disjoint cycles, the numbers of cycles of each length are the same.

Transpositions

A *transposition* is a 2-element cycle. Every cycle has an obvious decomposition as a product of transpositions: $(1234) = (12)(23)(34)$, and so on:

2.9 Prove that $(123\ldots n) = (12)(23)(34)\ldots(n-1\ n)$.

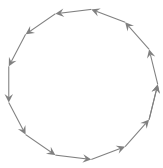
Hence we can break any permutation into an obvious product of transpositions.

2.10 Write the permutation (17) as a product of transpositions of neighboring integers.

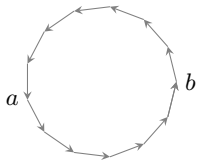
Suppose that n_g elements appear in the cycles of g, and c_g cycles. Each cycle of some length ℓ can be written as a product of $\ell - 1$ transpositions. Hence g can be written as the product of $n_g - c_g$ transpositions. (Or perhaps even fewer in some other way?)

Length of a permutation

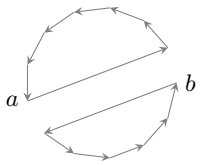
Draw a cycle as a polygon with arrows on its edges:



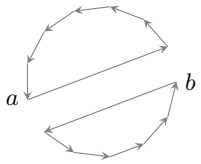
Our cycle is a permutation g of the various integers that we can write beside the arrow heads. Pick two of elements in the cycle, say a and b:



Let $t = (ab)$. What is gt? It first interchanges a with b, and then it applies g. So a goes to b and then to $g(b)$, i.e. an arrow goes out of a to whatever b pointed to. Similarly, b goes to a and then to $g(a)$, i.e. an arrow goes out of b to whatever a pointed to. Everything else is the same as it was for g:



So the product of a cycle g with a transposition t of two entries in g is a pair of cycles. On the other hand, since $t^2 = ()$, it follows that if $h = gt$ is our pair of cycles, $g = ht$: if we take any permutation h which is a pair of disjoint cycles:

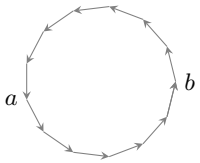


and pick some a on one of them, and some b on the other, and let $t = (ab)$, then $g = ht$ is a single cycle.

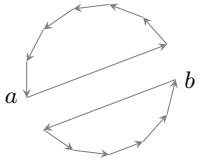
Start with any permutation g, written as a product of disjoint cycles. Multiply by a transposition t to form gt. Four things can happen

a. t is disjoint from all of the cycles in g, so gt is now written as a product of disjoint cycles, with one more cycle in it.

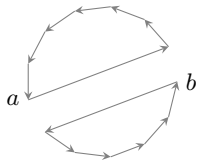
b. t transposes two elements a, b which appear in the same cycle in g;



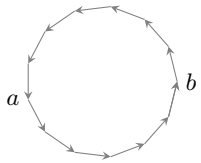
so that cycle splits in two in gt like



c. t transposes two elements a, b which appear in different cycles in g;



so those two cycles join in gt like



d. t transposes an element appearing in a cycle of g with an element which doesn't appear in any cycle of g; then gt is a new longer cycle, like

$$(123\ldots n)(n\ n+1) = (123\ldots\ n+1).$$

Therefore gt is the same as g but with one extra cycle, one less cycle, or one cycle being longer by one.

Lemma 2.2. *If g is a permutation and t a transposition, the number n_g of elements moved by g and number c_g of cycles of g satisfies*

$$n_{gt} - c_{gt} = n_g - c_g \pm 1.$$

2.11 Prove it.

A permutation is *odd* if is product of an odd number of transpositions, *even* if a product of an even number of transpositions.

Theorem 2.3. *Every permutation is either odd or even, but not both.*

The *length* of a permutation is the least number of transpositions of which it is a product. The *distance* between permutations g, h is the length of gh^{-1}.

2.12 Draw a dot for each permutation of integers $1, 2, 3, 4$. Connect two dots by an edge if a transposition takes one permutation to another. What are the longest distances? Our theorem shows that each edge connects an odd permutation to an even. Colour the odd ones.

2.13 Prove that the length of a permutation is the difference between the number of elements moved by the permutation and the number of disjoint cycles.

The sign of a permutation

Given a polynomial $b(t)$ in variables $t_1, t_2, \ldots, t_n$, and a permutation p of n letters, we define $pb(t)$ by the equation

$$pb(t_1, \ldots, t_n) = b(t_{q(1)}, \ldots, t_{q(n)}),$$

where q is the inverse permutation to p.

If $p = 2314$ then $q = 3124$. If

$$b(t_1, t_2, t_3, t_4) = t_1^6 + 8t_2t_4 + t_3^9,$$

then

$$pb(t_1, t_2, t_1, t_4) = t_3^6 + 8t_1t_4 + t_2^9.$$

2.14 If p, r are permutations on n letters prove that $r(pb) = (rp)b$ for any polynomial b in n variables.

The *sign* of a permutation p, denoted $(-1)^p$, is $(-1)^t$ where t is the number of transpositions in some expression of p as a product of transpositions of neighboring integers.

Lemma 2.4. *The map taking a permutation p to its sign, denoted $(-1)^p$, is well defined and satisfies $(-1)^{pq} = (-1)^p(-1)^q$ for any two permutations p, q of the same number of letters. Moreover $(-1)^p = (-1)^t$ if p can be written as as product of t transpositions.*

Proof. This follows trivially from theorem 2.3 on the preceding page, but here is another proof from a different and useful point of view. Consider the polynomial

$$b(t_1, \ldots, t_n) = (t_1 - t_2)(t_1 - t_3)\ldots(t_{n-1} - t_n) = \prod_{i<j}(t_i - t_j).$$

Then $pb(t)$ has various $t_i - t_j$ factors multiplied together, with $i \neq j$, in every possible pairing of i, j or j, i. So $pb(t) = \pm b(t)$. Write this $\pm$ as $(-1)^p$.

Suppose that p is the transposition $(i \;\; i+1)$. Then p changes $t_i - t_{i+1}$ into $t_{i+1} - t_i = -(t_i - t_{i+1})$, one sign change. Otherwise, p leaves everything in $b(t)$ as it is except swapping $t_i - t_j$ and $t_{i+1} - t_j$ for $j \geq i+2$, and swapping $t_j - t_i$ and $t_j - t_{i+1}$ for $j \leq i-1$. So finally, only one sign change: $pb(t) = -b(t)$, so $(-1)^p = -1$.

If p, q are any two permutations of n letters, then $(-1)^p(-1)^q b = p(qb) = (pq)b = (-1)^{pq}b$. Therefore, for any i and j, if we write

$$(i \;\; i+1) = (i+1 \;\; j)(i \;\; j)(i+1 \;\; j),$$

then $(-1)^{(ij)} = (-1)^{(i \;\; i+1)} = -1$. □

2.15 Prove that the sign of any transposition is -1 by writing it as a product number of transpositions of neighboring integers.

2.16 Starting from your favourite definition of determinant of a square matrix, prove that for any square matrix A, say of size $n \times n$, with coefficients in any field,

$$\det A = \sum_p (-1)^p A_{1p(1)} A_{2p(2)} \ldots A_{np(n)},$$

where the sum is over all permutations p of $1, 2, \ldots, n$.

The group of even permutations of n letters is the *alternating group*.

2.17 Write out the elements of the alternating group on 4 letters.

2.18 Prove that the alternating group on n letters contains $n!/2$ elements.

2.19 The 15-puzzle is a 4×4 square containing with 15 slideable tiles (each a 1×1 square), so one square is vacant (i.e. has no tile in it):

7	5	2	11
3	10	1	12
13	9		6
14	4	15	8

Each tile has a number on it, from 1 to 15. We solve the puzzle by sliding the squares around until they lie in order by number, with the vacant square last:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Prove that if the 15-puzzle starts in this order:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

it is not solvable. Hint: associate to each permutation (of tiles and vacant square) a number $x = 0$ or 1, depending on whether the permutation of the order of the tiles (ignoring the vacant spot) is even or odd, and a number $y = 0$ or 1 given by the row of the vacant spot, modulo 2. Let $z = x + y$ modulo 2.

Sage

Sage knows all of the permutations of small symmetric groups, and will print them out for you in cycle notation:

```
H = DihedralGroup(6)
H.list()
```

yields

$$\begin{array}{lll} , & (1,6)(2,5)(3,4), & (1,2,3,4,5,6), \\ (1,5)(2,4), & (2,6)(3,5), & (1,3,5)(2,4,6), \\ (1,4)(2,3)(5,6), & (1,6,5,4,3,2), & (1,4)(2,5)(3,6), \\ (1,2)(3,6)(4,5), & (1,5,3)(2,6,4), & (1,3)(4,6) \end{array}$$

where the identity element is the blank space at the start.

Chapter 3

Groups

Groups

Each symmetry of an equilateral triangle in the plane permutes the vertices. If we label the vertices, say as $1, 2, 3$, then every permutation of the labels $1, 2, 3$ occurs from a unique symmetry of the triangle. So the symmetries of the equilateral triangle correspond to the permutations of the labels, i.e. the symmetry group of the equilateral triangle is, in some sense, the same as the symmetric group on three letters. It is this notion of correspondence that leads us to see that two transformation groups can be "the same" while they are transforming very different sets; in our example, the symmetries of the equilateral triangle transform the infinitely many points of the triangle, while the permutations of three letters transform a set of three letters. In order to say what is "the same" in the two transformation groups, we need a more abstract concept of group.

A *group* is a set G so that

a. To any elements a, b of G there is associated an element ab of G, called the *product* of a and b.

b. The product is associative: if a, b, c are elements of G, then $(ab)c = a(bc)$, so that either expression is denoted as abc.

c. There is an identity element: some element 1 of G, so that $a1 = 1a = a$ for any element a of G.

d. Every element is invertible: if a is an element of G, there is an element, denoted a^{-1}, of G for which $aa^{-1} = a^{-1}a = 1$.

Nonzero rational numbers form a group G under usual multiplication, where a^{-1} means the reciprocal of any rational number a. Note that 0 does not have a reciprocal, so we have to remove it.

Nonzero elements of any field form a group G under usual multiplication, where a^{-1} means the reciprocal of any element a. Note that 0 does not have a reciprocal, so we have to remove it.

Any transformation group G is a group, using composition of transformations as its product, and the identity transformation as its identity element. In particular, as examples of groups: the symmetry groups of geometric figures, the group of invertible matrices (under matrix multiplication), the symmetry group on some letters, the group of rotations of the Euclidean plane, and the

group of rotations of Euclidean space.

It is easier to check if a collection of transformations forms a transformation group than to check if some abstract product operation forms a group; almost all of our examples of groups will be transformation groups in some obvious way.

Two elements a, b of a group *commute* if $ab = ba$. A group is *abelian* if any two elements of the group commute.

Nonzero rational numbers form an abelian group under usual multiplication.

Nonzero elements of any field form an abelian group under usual multiplication.

Invertible 2×2 matrices, with entries drawn from some chosen field, form an non-abelian group under usual matrix multiplication.

The symmetries of the equilateral triangle form a non-abelian group: if we rotate by 120° and the reflect across an angle bisector, we get a different result than if we first reflect across that bisector and then rotate.

3.1 Prove that, for any elements a, b, c, d of a group G,

$$a(b(cd)) = (ab)(cd) = ((ab)c)d.$$

Generalize by induction to prove that parentheses are not needed in expressions of any length.

3.2 For any element a of a group G, define a^0 to mean 1, and define by induction $a^{n+1} = aa^n$. Prove by induction that $a^m a^n = a^{m+n}$ for an integers m, n.

3.3 Suppose that $1, 1'$ are two elements of a group G, and that $a1 = 1a = a$ and also that $a1' = 1'a = a$ for any element a of the group G). Prove that $1 = 1'$.

3.4 Given elements a, b of a group G, prove that the equation $ax = b$ has a unique solution x in G. Prove also that the equation $ya = b$ has a unique solution y in G.

3.5 Prove that $(ab)^{-1} = b^{-1}a^{-1}$ for any elements a, b of any group.

3.6 Suppose that x belongs to a group G and that $x^2 = x$. Prove that $x = 1$.

3.7 Prove that the set of nonzero rational numbers, with product operation defined as usual division, do not form a group. (It might help to write the operation is some funny notation like $a \star b$, instead of ab, which easily gets confused with multiplication.)

Additive notation

When a group is abelian, it is often preferred to write the group operation not as ab but instead as $a + b$, and the identity element as 0 rather than 1, and the inverse as $-a$ rather than a^{-1}.

The set of integers form an abelian group, where the group operation is usual addition.

Any field is an abelian group, where the group operation is usual addition.

The set of 2×2 matrices, with integer entries form an abelian group, where the group operation is usual addition. The same for rational entries, real entries, complex entries, entries drawn from any field, and for 2×3 matrices, and so on.

The rotations of the plane around the origin form an abelian group, writing each rotation in terms of its angle of rotation, and using addition of angles, i.e. composition of rotations, as the group operation. (Careful: the rotations of Euclidean 3-dimensional space form a non-abelian group.)

3.8 Define an operation on real numbers b, c by

$$b \star c = \frac{b+c}{1-bc}.$$

With this operation, are the real numbers an abelian group? Consider the collection consisting of all numbers of the form $b = \frac{3p}{q}$ with p, q integers so that 3 does not divide q. Is this collection of numbers a group under this operation?

3.9* Suppose that we turn the real numbers $\mathbb{R}$ into a group using some weird multiplication, say $x * y = p(x, y)$ and with some identity element x_0. Suppose that $p(x, y)$ is a polynomial. Prove that $p(x, y)$ is given by the formula $p(x + x_0, y + x_0) = x + y + x_0$.

Sage knows many finite groups, and can say whether they are abelian:

```
H = SymmetricGroup(6)
H.is_abelian()
```

yields False.

Multiplication tables

If a group G is finite (i.e. has finitely many elements), we let $|G|$ be the number of elements of G, called the *order* of G. We can then write a *multiplication table*, with rows representing some element x, columns some element y, and entries xy For example, if a group G has 2 elements, say 1 and a, then it is easy to see that $a^2 = 1$ so the multiplication table must be

	1	a
1	1	a
a	a	1

3.10 Prove that, for any group, on every row of its multiplication table, every element of the group occurs exactly once. Prove the same for columns instead of rows.

3.11 Prove that any group G of order 3 has (in some labelled of its elements) the multiplication table

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

If G and H are two groups, their *product* is the group $G \times H$ whose elements are pairs (g, h) of elements g of G and h of H, with product

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

and identity element $(1, 1)$. Given a multiplication table for G and one for H, we can make one for $G \times H$ by taking each row a and column b entry ab for G, and each row x and column y entry xy for H, and writing out (a, x) as a row for $G \times H$, (b, y) as a row for $G \times H$, and (ab, xy) as entry. For example, if $G = H$ are both the group of order 2 above, then $G \times H$ has multiplication table:

	1	$(a,1)$	$(1,a)$	(a,a)
1	1	$(a,1)$	$(1,a)$	(a,a)
$(a,1)$	$(a,1)$	1	(a,a)	$(1,a)$
$(1,a)$	$(1,a)$	(a,a)	1	$(a,1)$
(a,a)	(a,a)	$(1,a)$	$(a,1)$	1

An *isomorphism* $\varphi\colon G \to H$ is a bijection between elements of two groups G and H so that $\varphi(xy) = \varphi(x)\varphi(y)$: φ preserves multiplication. If there is some isomorphism between two groups, they are *isomorphic*, and for all purposes of algebra we can treat them as being the same group.

In problem 3.11, we saw that all groups of order 3 are isomorphic.

The remainders modulo 4 form a group G_1, under addition as the group operation. The set of complex numbers $G_2 = \{1, -1, i, -i\}$ form a group under multiplication. The matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

form a group G_3 under multiplication. All of these groups are isomorphic. For example, map $0 \mapsto 1$, $1 \mapsto i$, $2 \mapsto -1$, $3 \mapsto -i$ to map $G_1 \to G_2$.

Let G be the group of order 2 we found above and H the group of remainders modulo 4. The groups $G \times G$ and H are both of order 4, but they are *not* isomorphic, because H contains the element 1 and every element of H is expressed in terms of 1 as precisely one of the 4 elements

$$1,\ 1+1,\ 1+1+1,\ 1+1+1+1.$$

So if G (in multiplication notation!) were isomorphic to H, we would have to

find some element (x, y) of G so that the 4 elements

$$(x, y), (x, y)^2, (x, y)^3, (x, y)^4$$

constitute the whole of G. Check the multiplication table above to see that every (x, y) in G satisfies $(x, y)^2 = (1, 1)$.

3.12 How many groups of order four are there, up to isomorphism?

Sage knows the multiplication tables of many groups. The *dihedral group* D_n is the symmetry group of a regular polygon with n equal sides and angles. If we type

```
H = DihedralGroup(6)
H.cayley_table()
```

we see the multiplication table:

$\cdot$	a	b	c	d	e	f	g	h	i	j	k	l
a	a	b	c	d	e	f	g	h	i	j	k	l
b	b	a	e	h	c	j	k	d	l	f	g	i
c	c	d	f	g	b	i	l	a	k	e	h	j
d	d	c	b	a	f	e	h	g	j	i	l	k
e	e	h	j	k	a	l	i	b	g	c	d	f
f	f	g	i	l	d	k	j	c	h	b	a	e
g	g	f	d	c	i	b	a	l	e	k	j	h
h	h	e	a	b	j	c	d	k	f	l	i	g
i	i	l	k	j	g	h	e	f	a	d	c	b
j	j	k	l	i	h	g	f	e	d	a	b	c
k	k	j	h	e	l	a	b	i	c	g	f	d
l	l	i	g	f	k	d	c	j	b	h	e	a

where a is the identity element.

Quaternions

A *quaternion* is a 4-tuple of real numbers (a, b, c, d). We add quaterions as you might expect:

$$(a_0, b_0, c_0, d_0) + (a_1, b_1, c_1, d_1) = (a_0 + a_1, b_0 + b_1, c_0 + c_1, d_0 + d_1).$$

Multiplication is tricky. Let's start by defining multiplication of a real number times a quaterion:

$$x(a, b, c, d) = (xa, xb, xc, xd).$$

Write $1, i, j, k$ to mean the quaterions

$$\begin{aligned} 1 &:= (1, 0, 0, 0), \\ i &:= (0, 1, 0, 0), \\ j &:= (0, 0, 1, 0), \\ k &:= (0, 0, 0, 1). \end{aligned}$$

As we know from linear algebra, we can write each quaterion uniquely as

$$(a, b, c, d) = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k.$$

Write a to mean $a \cdot 1$, so that every real number a is also thought of as a quaternion $a = (a, 0, 0, 0)$. Write any quaternion

$$q = a + bi + cj + dk$$

more simply as

$$q = a + u,$$

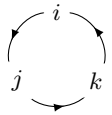
where $u = (0, b, c, d)$ we think of a 3-dimension vector with real number entries

$$u = (b, c, d).$$

So a quaternion is a "formal sum" of a real number and a 3-dimensional vector. Define multiplication by

$$(a + u)(b + v) = ab - u \cdot v + (av + bu + u \times v),$$

using the dot product and cross product of vectors. We can test this multiplication out on i, j, k: $i^2 = j^2 = k^2 = -1$ and



by which we mean that we multiply in order around the circle, or with a minus sign if we go backwards around the circle. For example, $ij = k$ but $ik = -j$ since we go backwards. Usual properties of cross and dot product prove that the multiplication is associative. It is *not* commutative, since $ij = k$ while $ji = -k$.

The *quaternion group* Q_8 is the set

$$Q_8 = \{\, 1, -1, i, -i, j, -j, k, -k \,\}.$$

Clearly Q_8 is a group under quaterion multiplication.

3.13 Prove that the quaternion group is not isomorphic to any dihedral group.

Chapter 4

Cosets

Cyclic groups

A group G is *cyclic* if it consists of the powers of a single element x, i.e. G consists of the powers x^n for integers n. For example, the integers (written additively) are generated by multiplies of 1, as is the group of remainders modulo some integer $n \geq 0$.

Theorem 4.1. *Every cyclic group G is isomorphic to either the integers (when $|G| = \infty$) or to the integers modulo an integer $n \geq 0$, when $|G| = n$.*

Proof. Suppose that G consists of the powers x^k of a single element x. Define a map $f\colon \mathbb{Z} \to G$ by $f(k) = x^k$. Then clearly $f(k+\ell) = x^{k+\ell} = x^k x^\ell = f(k)f(\ell)$. If f is a bijection, then f is our isomorphism. So suppose that f is not a bijection. By definition, f is surjective, so f must fail to be injective, i.e. $f(k) = f(\ell)$ for some $k \neq \ell$, i.e. $x^k = x^\ell$, i.e. $x^{k-\ell} = 0$ i.e. $f(k-\ell) = 1$. Let $K \subset \mathbb{Z}$ be the set of all integers m so that $f(m) = 1$. Note that K contains zero, and K also contains some nonzero element $k - \ell$. If m is in K then $x^m = 1$ so $x^{2m} = 1$ and so on, i.e. if m is in K then all multiples of m are in K. If K contains some integers b, c, take Bézout coefficients $sb + tc = g$ and then

$$f(g) = f(sb+tc) = x^{sb+tc} = (x^b)^s (x^c)^t = 1^s 1^t = 1.$$

Hence g is in K as well: the greatest common divisor n of all elements of K also lies in K. But then every multiple of n also lies in K. Hence K consists precisely of all multiples of n, i.e. $K = n\mathbb{Z}$, and so $G = \{\, 1, x, \ldots, x^{n-1} \,\}$ is isomorphic to the remainders modulo n, taking each remainder b to x^b. □

The *order* of an element a of a group G is the order of the cyclic group consisting of the powers a^k.

4.1 Take any two elements a, b of some group. Prove that ab and ba have the same order.

4.2 Take any two elements a, b of order two in some group. If ab also has order two, prove that a and b commute.

4.3 Take a permutation f of n letters $1, 2, \ldots, n$, expressed as a product of disjoint cycles. Prove that the order of f is the least common multiple of the orders of the disjoint cycles.

4.4 Suppose that G is a finite group in which every element has order 1 or 2. Prove that G is isomorphic to a product of copies of $\mathbb{Z}/2\mathbb{Z}$.

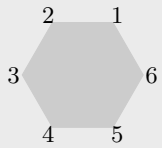
Sage can compute the order of an element of a group:

```
G = SymmetricGroup(5)
sigma = G("(1,3) (2,5,4)")
sigma.order()
```

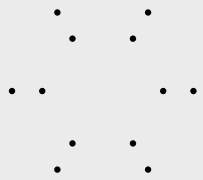
yields 6.

Graphs

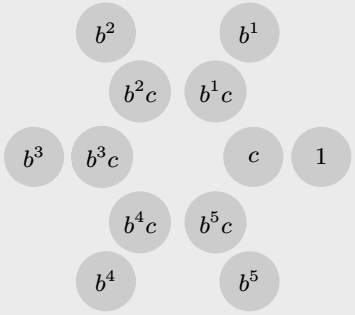
Take a hexagon X in the plane and let G be its symmetry group. Label the vertices of X in order as we travel around the vertices counterclockwise, say as $1, 2, 3, 4, 5, 6$.



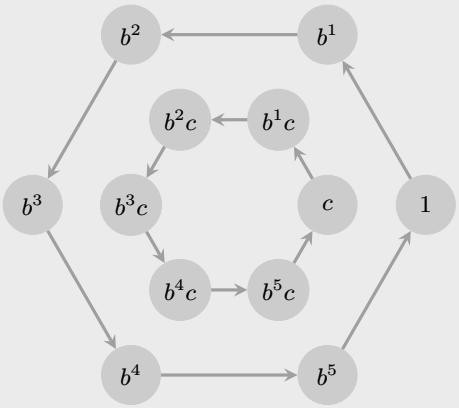
Any symmetry moves 1 to one of the six vertices, and moves 2 to a next door neighbor vertex. We can draw the vertices of the hexagon twice, one for drawing where 1 is taken to, and once again to represent whether 2 is taken to the vertex counterclockwise from 1 or clockwise.



In a sense, this is a picture of the group, since every element of the group is completely determined once we know where vertices 1 and 2 go: the rest are then in order cyclically around the hexagon. Let b be rotation of the hexagon by 60°, and let c be reflection of the hexagon across the axis of symmetry through vertex 1. Label the elements of the group according to how they move vertices 1 and 2, i.e. how much of b and c they contain:



Multiplication of each element by b on the left, i.e. $x \mapsto bx$, spins the hexagon around to right.



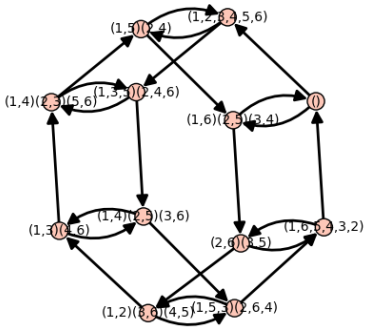
Multiplication of each element by c on the right, i.e. $x \mapsto xc$, moves the inward hexagon points to the outward ones, and vice versa.

Elements $g, h, \ldots$ of a group G *generate* that group if every element can be written as a product of integer powers of those elements. If we fix some elements generating a group G, the *Cayley graph* of G (with respect to those generators) is the set of elements of G, each draw as a dot, together with an arrow from one dot to another, labelled by g, if the first dot is some element k and the second is gk (or kg, depending on which ordering we prefer). These pictures are almost never useful in proving results about groups, but they give us some intuition.

Sage knows the Cayley graphs (for various generators) of many groups. If we type

```
H = DihedralGroup(6)
show(H.cayley_graph())
```

we see the graph:



The graph is labelled by the cycles of each element, thought of as a permutation of the vertices of the hexagon.

Theorem 4.2 (Cayley)**.** *Every group is a group of permutations.*

Proof. We drew the graph of the group above; now imagine more simply just drawing a dot for each element. Each element g of the group then moves each dot k to gk, permuting the dots. □

Subgroups

A subset H of a group G is a *subgroup* if

a. H contains the identity element and

b. if a and b are elements of H then ab is also an element of H,

c. if b is an element of H then b^{-1} is also an element of H.

It follows that H is itself a group.

The even numbers are a subgroup of the integers, under usual integer addition.

The invertible integer 2×2 matrices are a subgroup of the invertible real 2×2 matrices.

If b is an element of any group G, then the set of all elements of G of the form b^k for integers k is a cyclic group, the subgroup generated by b.

The real 2×2 matrices of unit determinant form a subgroup of the group of all invertible real 2×2 matrices, since determinants multiply.

4.5 What are all of the subgroups of the symmetry group of a hexagon?

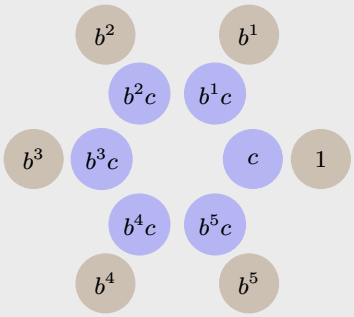
4.6 Prove that every subgroup of a cyclic group is cyclic.

4.7 What are all subgroups of the group $\mathbb{Z}/102\mathbb{Z}$ of integer remainders modulo 102?

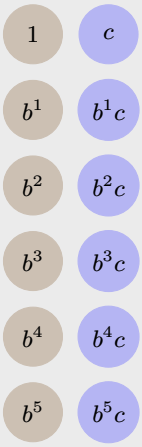
Cosets

If S is any subset of a group G and b is any element of G, denote by bS the set of elements of the form bs for s in S, called a *left translate* or *left coset* of S; if we write *coset*, we mean *left coset*. Denote by Sb the set of elements of the form sb for s in S, called a *right translate* or *right coset* of S. Each coset bS has the same number of elements as S, since $s \mapsto bs$ has inverse $t \mapsto b^{-1}t$, so is a bijection.

The group G of symmetries of the hexagon has a subgroup H of rotations of the hexagon. Divide up G into H-cosets:



We might draw our cosets as columns of a matrix



to emphasize that they are all the same size, each a copy of H.

Let G be the group of rotations and H the subgroup of those rotations which preserve a regular hexagon X around the origin. For each angle θ, which we think of as a rotation g, gH is the set of all rotations gh for $h \in H$, i.e. geometrically the rotations which take the given hexagon X into the hexagon gX.

Let G be the group of integers under addition, and H the subgroup of multiples of 7, i.e. H is the set of all integers of the form $7k$ for any integer k. Our translates in this notation have the form $1+H, 2+H$, and so on. The translate $1 + H$ is the set of all numbers of the form $1 + 7k$ for any integer k. The translate $2 + H$ is the set of all numbers of the form $2 + 7k$ for any integer k, and so on.

Lemma 4.3. *If x and y are elements of a group G and H is a subgroup of G, then $xH = yH$ just when $y^{-1}x$ belongs to H. Any two cosets xH and yH are either disjoint: $xH \cap yH$ empty, or equal: $xH = yH$.*

Proof. Suppose that $xH = yH$. Then every element xh of xH must belong to yH, i.e. have the form yh' for some element h' of H, so $xh = yh'$, i.e. $x = yh'h^{-1}$, and so $y^{-1}x = h'h^{-1}$ is in H.

Conversely, if $y^{-1}x$ is in H, then every element xh of xH has the form

$$\begin{aligned} xh &= (yy^{-1})xh, \\ &= y(y^{-1}xh), \\ &= yh' \end{aligned}$$

where $h' = y^{-1}xh$ is in H. Similarly, every element yh of yH has the form

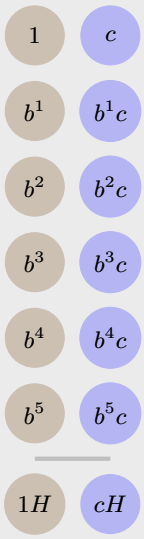
$$\begin{aligned} yh &= (xx^{-1})xh, \\ &= x(x^{-1}yh), \\ &= xh' \end{aligned}$$

where $h' = x^{-1}yh = (y^{-1}x)^{-1}h$ is in H.

If xH intersects yH, say at $xh = yh'$, then $y^{-1}xh = h'$ lies in H so $y^{-1}x$ lies in H, i.e. $xH = yH$. □

If H is a subgroup of a group G, let G/H be the collection of all cosets of H in G, the *coset space* or *quotient space*.

The group G of symmetries of the hexagon has a subgroup H of rotations of the hexagon. If we draw each coset as a column, we draw each point of G/H as a single dot underneath that column:



Let G be the group of all rotations of the plane and H the subgroup of those rotations which preserve a regular hexagon X around the origin. For each angle θ, which we think of as a rotation g, gH is the set of all rotations gh for $h \in H$, i.e. geometrically the rotations which take the given hexagon X into the hexagon gX. So each coset gH in G/H is identified with a rotated hexagon gX, i.e. G/H is the set of all rotated hexagons gX for any rotation g.

Let G be the group of integers under addition, and H the subgroup of multiples of 7, i.e. H is the set of all integers of the form $7k$ for any integer k. Our translates in this notation have the form $1+H, 2+H$, and so on. The translate $1+H$ is the set of all numbers of the form $1+7k$ for any integer k, which we denote by $\bar{1}$. The translate $2+H$ is the set of all numbers of the form $2+7k$ for any integer k, which we denote by $\bar{2}$, and so on. Of course, $\bar{7} = \bar{0}$ is the coset of H. So G/H is the set of remainders modulo 7. Each element of G/H represents "gluing together" all elements of G that differ by a multiple of H.

Theorem 4.4 (Lagrange)**.** *If H is a finite subgroup of a group G then*

$$|G/H| = \frac{|G|}{|H|}.$$

Proof. The set G is divided up into disjoint cosets, each of size $|H|$. □

Corollary 4.5. *The order of any finite subgroup of a group divides the order of the group.*

Corollary 4.6. *The order of any element of a group divides the order of the group.*

Corollary 4.7. *Every finite group of prime order, say order p, is cyclic, isomorphic to the group of remainders modulo p under addition.*

Proof. Take any element which is not the identity element, so cannot have order 1. Since G is finite, the order of the element is finite. Since $|G|$ is prime, the order of the element divides this prime, so equals this prime. □

4.8 Classify all groups of order 6.

Chapter 5

Actions

A group G *acts* on a set X if each element b of G has an associated transformation f_g of X so that $f_{bc} = f_b \circ f_c$ for any elements b, c of G. So then G is a transformation group of X, and write gx to mean $f_g(x)$. The action is *transitive* if any two points p, q of X are connected by some element of G, i.e. $q = gp$ for some g in G. The *stabilizer* of a point x_0 of X is the subset G^{x_0} of G consisting of those g in G so that $gx_0 = x_0$. If a group G acts on two sets X and Y, a map $f\colon X \to Y$ is *equivariant* if $f(gx) = gf(x)$ for any x in X and g in G. An equivariant bijection makes two actions practically identical.

Lemma 5.1. *Given a group action of a group G on a set X, and an element x_0 of X, the stabilizer G^{x_0} of each point is a subgroup.*

Proof. Clearly if $bx_0 = x_0$ and $cx_0 = x_0$ then $(bc)x_0 = b(cx_0) = bx_0 = x_0$ and so on. □

Subgroups correspond to transitive actions; geometrically it is always easier to think about actions, but algebraically it is easier to work with subgroups.

Theorem 5.2. *If H is a subgroup of a group G, and we let $X = G/H$, then G acts on X transitively by $b(cH) = (bc)H$ with stabilizer $G^{x_0} = H$ where x_0 is the coset $1H$. Conversely, if G acts transitively on a set X, and we let $H = G^{x_0}$, there is a unique equivariant bijection $f\colon G/H \to X$, so that $f(gH) = gx_0$.*

Proof. Clearly $b(cH) = (bc)H$ is the set of elements of G of the form bch for h in H. Hence the action of G on G/H is defined.

Take any element gH of G/H. So gH is a coset. By lemma 4.3 on page 23, knowing only the coset gH, we can determine the element g, up to replacing g by gh for any $h \in H$. But then the expression gx_0 will only change to $(gh)x_0 = g(hx_0) = gx_0$, i.e. not at all. So knowledge of the coset gH determines knowledge of gx_0, i.e. f is well defined. It is then easy to check that f is equivariant. Since G acts transitively on X, every element x of X has the form $x = gx_0$ for some g, f is surjective. If $f(bH) = f(cH)$ then $bx_0 = cx_0$ so $c^{-1}bx_0 = x_0$ i.e. $c^{-1}b$ lies in G^{x_0}. But H is by definition G^{x_0}, so $c^{-1}b$ lies in H, i.e. $bH = cH$, so f is injective. □

Take 49 seats, numbered, and 15 people standing, each with name tags. Sit all 15 of those people. Keep track of who sits where. So the group G of permutations of 49 seats acts on the possible seating plans of the 49 people, taking any seating plan to any other. But the seating plan of the 15 people (who sits where) doesn't change if we move around the empty seats: $49 - 15 = 34$ seats. So the group H of permutations of 34 empty seats acts trivially on any given seating plan x_0. So the set X of seating plans of 15 people into 49

chairs is $X = G/H$, and so has order 49!/34!.

5.1 Explain how to count combinations, and how to count permutations, using group actions.

Take a group G acting on a set X. The *orbit* Gx of an element x of X is the set of all elements of X of the form gx for g in G: it is where G takes x. Every orbit is, by definition, acted on transitively by G, so the map $G/G^x \to Gx$ taking $gG^x \mapsto gx$ is an equivariant bijection. Denote the set of all orbits as X/G.

5.2 If X is a hexagon in the plane, and G is the symmetry group of X, what are all of the orbits of G?

A *fixed point* of a group G acting on a set X is a point x fixed by all elements of G, i.e. $gx = x$ for any g in G.

5.3 If a finite group G acts on a finite set X, and the order of X is coprime to the order of G, prove that X contains a fixed point of the G-action.

Theorem 5.3 (Burnside)**.** *Suppose that a finite group G acts on a finite set X. To each element g of G, let X^g be the set of elements of X fixed by g. Write the number of elements of any set S as $|S|$. Then the number of orbits is the average number of fixed points of group elements:*

$$|X/G| = \frac{\sum_{g \in G} |X^g|}{|G|}.$$

Proof. Let S be the set of pairs (g, x) with g in G, x in X, and $gx = x$. Count the elements of S two ways: first by summing over all possible values of g:

$$|S| = \sum_{g \in G} |X^g|,$$

and second by summing over all possible values of x instead:

$$|S| = \sum_{x \in X} |G^x| = \sum_{x \in X} \frac{|G|}{|Gx|}.$$

But if x and y belong to the same orbit, say $o = Gx = Gy$, they have the same value

of $|o| = |Gx| = |Gy|$. There are $|o|$ elements x in that orbit, so we write this as

$$\begin{aligned}
|S| &= \sum_{x\in X} \frac{|G|}{|Gx|}, \\
&= \sum_{o\in X/G} \sum_{x\in o} \frac{|G|}{|Gx|}, \\
&= \sum_{o\in X/G} \sum_{x\in o} \frac{|G|}{|o|}, \\
&= \sum_{o\in X/G} \frac{|G|}{|o|} \sum_{x\in o} 1, \\
&= \sum_{o\in X/G} \frac{|G|}{|o|} |o|, \\
&= |G| \sum_{o\in X/G} 1, \\
&= |G||X/G|.
\end{aligned}$$

□

Theorem 5.4. *Suppose that a finite group G acts on a finite set X. Each element g of G acts as a permutation on X, say with c_g cycles. Suppose we pick n different colours and try to paint X with those colours, but we declare two colourings to be equivalent if they agree after the action of some element of G. Then the number of distinct colourings is*

$$\frac{1}{|G|} \sum_{g\in G} n^{c_g}.$$

Proof. Let C be the set of all colourings of X into n colours, i.e. the set of maps $X \to \{1, 2, \ldots, n\}$. Each G-orbit in C is one colouring of X up to equivalence. Let C' be the set of pairs (c, g) where $c \in C$ is a colouring and $g \in G$ is an element preserving that colouring. On C', we have the action $g_0(c, g) = (g_0 c, g_0 g)$ for any $g_0 \in G$. So $\varphi\colon (c, g) \in C' \mapsto c \in C$ is onto and G-equivariant. So φ takes G-orbits to G-orbits. But the G-stabilizer of any point of C' is trivial, so each G-orbit in C' is a copy of $G/\{1\} \cong G$. Hence each G-orbit in C has preimage with $|G|$ elements in C'. Add up over all G-orbits to find all elements of C': $|C'| = |G||C/G|$.

Let $\psi\colon (c, g) \in C' \mapsto g \in G$. Again ψ is G-equivariant. Each $\psi^{-1}g$ is the set of all colourings invariant under g, i.e. with the same colour in all g-orbits. There are $n^{c(g)}$ such colourings:

$$|C'| = \sum_{g\in G} n^{c(g)}.$$

Put the two together:

$$|C/G| = \frac{1}{|G|} \sum_{g\in G} n^{c(g)}.$$

□

5.4 Find the number of distinct colourings of a cube (where we declare two colourings equivalent if they agree up to rotation) with 5 colours of paint.

Actions on group elements and on subgroups

Take a group G. For each element $g_0 \in G$, the elements which commute with it form a subgroup, the *centralizer* $C_{g_0,G}$ of g_0. Suppose that H is a subgroup of G. The *centralizer* $C_{H,G}$, also denoted C_H if G is understood, is the set of elements of G which commute with every element of H, clearly a subgroup. The *center* of a group G is $C_{G,G}$, i.e. the elements which commute with all others, an abelian group. The *normalizer* $N_{H,G}$, also denoted N_H if G is understood, is the set of elements g of G for which $gHg^{-1} = H$.

5.5 Prove that $C_H \subset N_H$.

5.6 Prove that every subgroup is a normal subgroup of its normalizer, i.e. $H \subset N_H$ is a normal subgroup.

5.7 Prove that $N_{H,G} = G$ just when H is a normal subgroup of G.

The action of a group on itself by conjugation is suprisingly complicated. Each element $g_0 \in G$ has stabilizer G^{g_0} precisely the elements $g \in G$ so that $gg_0g^{-1} = g_0$. Multiply on the right by g to see that this is precisely the condition that g_0, g commute. So $G^{g_0} = C_{g_0}$. The orbit through g_0 is therefore identified with $G/G^{g_0} = G/C$. So the conjugation orbit through an element $g_0 \in G$ has $[G : C]$.

A very sophisticated example of a group action: if H is a subgroup of a group G, then so is the conjugate gHg^{-1}, for any $g \in G$. For simplicity, we often write conjugates as H^g to mean gHg^{-1}. So if we let X be the set of all subgroups of G, then G acts on X by this conjugation action. We want to be very careful with the notation: if $x \in X$ is a point, then x represents some subgroup, say $H = H_x$ of G. But then gx represents H^g, so $H_{gx} = H_x^g$ in our notation.

5.8 Under the conjugation action of G on the set of its subgroups, prove that the orbit through a subgroup H has $[G : N]$ elements where $N = N_{H,G}$.

5.9 For any prime p, a *p-group* is a group whose order is a power p^k, some integer $k \geq 1$. Prove that the center of any p-group has order a positive integer multiple of p.

Chapter 6

Presentations

The symmetries of an equilateral triangle can all be expressed in terms of the rotation, call it b, by 120°, and the reflection, call it c, about any one the axes of symmetry through one of the vertices. Clearly $b^3 = 1$, i.e. if we rotate three times by 120°, the resulting rotation by 360° moves every point back where it started. Similarly $c^2 = 1$. The reader can draw pictures to see that $bc = cb^2$. Once we have these three rules, any expression in the group in terms of b and c can be successively simplified by these three rules, to an expression in which c only appears to the first power, i.e. no c^2 or c^{-1} or c^{-13} appears, and b appears only to the power 1 or 2, and b always appears after c. Hence the group is precisely

$$1, b, c, b^2, cb, cb^2.$$

Take an abstract set X. A *word* on the *alphabet* X is a finite sequence of choices of element of X and integer power. We write each word as a string of symbols

$$x_1^{a_1} x_2^{a_2} \dots x_k^{a_k}.$$

We allow the empty string, and write it as 1. *Reduce* a word by deleting any x^0 symbols and replacing any subword $x^p x^q$ by x^{p+q}. The *free group* $\langle X \rangle$ on an alphabet X is the collection of all reduced words on X. The multiplication operation: multiply two words by writing down one after the other, called *concatenation* and then reduce. The inverse operation: write down the word in reverse order, with opposite signs for the powers. A group F is a *free group* if F is isomorphic to the free group on some alphabet.

6.1 In any free group, prove that if two elements a, b satisfy an equation $a^2 = b^2$ then $a = b$.

6.2 Suppose that X and Y are two sets with the same number of elements. Prove that the free groups they generate are isomorphic.

6.3 Suppose that F is the free group on one generator. Prove that $F \times F$ is not a free group.

Take an abstract set X with associated free group $\langle X \rangle$. Take a set R of words in the alphabet X. The group *generated* by X with *relations* R, denoted $\langle X | R \rangle$, is the quotient of $\langle X \rangle$ by the equivalence relation that two words are equivalent if we can repeatedly insert words from R or inverses of such, and then delete words from R or inverses of such, and eventually get from one word to another. The expression of a group in the form $\langle X | R \rangle$ is a *presentation* of the group with *generators* S and *relations*

R. In practice, we usually write the relations not as a set R, but as a collection of equations like

$$w_1 = w_2$$

between words. This equation means that we require $w_2^{-1}w_1 \in R$. A presentation $\langle X|R\rangle$ is *finite* if both X and R are finite sets.

Lemma 6.1. *For any set X and set R of words in X, $\langle X|R\rangle$ is a group.*

Proof. We can clearly multiply equivalence classes of words, and invert them. Associativity and existence of inverses are clear because they hold for words. □

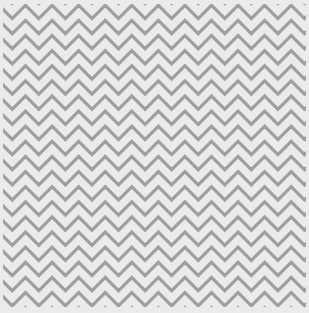
The two transformations

$$T\colon (x, y) \mapsto (x, y + 1)$$

and

$$F\colon (x, y) \mapsto (x + 1, -y)$$

of the plane, a translation and a flip, satisfy $TFT = F$, and generate some group H, the symmetries of the infinite wallpaper pattern on the infinite plane:



Let $G := \langle f, t|tft = f\rangle$; in other words G is the group generated by alphabet $\{ t, f \}$ with relation $tft = t$, i.e. with $R = \{ t^{-1}tft \}$. So we have a surjective map $G \to H$, mapping $t \mapsto T$ and $f \mapsto F$. Here t is a formal symbol, not an actual transformation of the plane, while T is the actual transformation. Take any word in G. Wherever we find tf we replace it by ft^{-1}. Wherever we find $t^{-1}f$ we replace it by ft. Wherever we find tf^{-1} we replace it by $f^{-1}t^{-1}$. Wherever we find $t^{-1}f^{-1}$ we replace it by $f^{-1}t$. The reader can check that these are all consequences of $tft = f$. Therefore any word in G can be written uniquely as $f^p t^q$. If the corresponding transformation $F^p T^q$ is the identity, then it fixes the origin, and so the translations of the x variable cancel each other out, i.e. $p = 0$. But then $T^q(x, y) = (x, y + q)$ fixes the origin just when $q = 0$. So the only element of G mapping to the trivial transformation of the plane is 1. We can see that $G \to H$ is an isomorphism.

The group G of symmetries of a hexagon contains a rotation b by 1/6 of a revolution, and a reflection c through one vertex. Clearly $b^6 = 1$ and $c^2 = 1$.

We let the reader check (by drawing a hexagon with labelled vertices and playing with it) that $bcbc = 1$. So we might guess that G is equal to the group $H := \langle b, c | 1 = b^6 = c^2 = bcbc \rangle$. Using $bcbc = 1$, we can write this as $cbc = b^{-1} = b^5$, so $cb = b^5 c$. Using this rule, any powers of b and c can be inductively rewritten so that b powers always come before c powers. For example, $b^7 c^2 b^{-3} c^3 b^2 = b^2 b^{-3} c b^2$ since $c^2 = 1$. But then $b^2 b^{-3} c b^2 = b^{-1} c b^2$ combining powers of b. Next, $b^{-1} c b^2 = b^5 c b^2$ since $b^6 = 1$ so $b^5 = b^{-1}$. Next, $cb = b^5 c$ so $b^5 c b^2 = b^5 c b b = b^5 b^5 c b = b^5 b^5 b^5 c = b^{15} c = b^3 c$. So clearly H has at most 12 elements. But G has 12 elements, and satisfies the equations of H, so we guess that $G = H$. (We will prove this true soon.)

6.4 Prove that the group G of invertible 2×2 real matrices generated by

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

has presentation

$$G = \langle a, b | a^{-1} b a = b^3 \rangle$$

6.5 Let

$$G = \langle x, y, z | xy = yx, xz = zx, yz = zy \rangle.$$

Prove that G is isomorphic to the product of three infinite cyclic groups.

When different presentations yield the same group

One group may have many presentations. A *consequence* of relations R in a presentation $\langle X | R \rangle$ is a word in R. A *Tietze transformation* of a presentation is one of the following:

a. *Adding an irrelevant relation* to a presentation $\langle X | R \rangle$ means adding a consequence of R: $\langle X | R, r \rangle$.

b. Obversely, *removing an irrelevant relation* from a presentation $\langle X | R, r \rangle$ means, if r is a consequence of R, take it out: $\langle X | R \rangle$.

c. *Adding an irrelevant generator* to a presentation $\langle X | R \rangle$ means:

$$\langle X, x | R, x^{-1} w \rangle$$

where x is some new variable, not already in X, and w is a word on the alphabet X, so x can be replaced wherever it appears by w.

d. *Removing an irrelevant generator* to a presentation $\langle X, x | R, x^{-1} w \rangle$ with w a word in X means: $\langle X | R \rangle$.

Adding an irrelevant relation: $\langle x, y | x^2 = y^3 \rangle$ can become $\langle x, y | x^2 = y^3, x^4 = y^6 \rangle$.

Removing an irrelevant relation: $\langle x, y | x^2 = y^3, x^4 = y^6 \rangle$ can become $\langle x, y | x^2 = y^3 \rangle$.

Adding an irrelevant generator: $\langle x, y | x^2 = y^3 \rangle$ can become $\langle x, y, z | x^2 = y^3, z = x^2 y^5 \rangle$.

Removing an irrelevant generator: $\langle x, y, z | x^2 = y^3, z = x^2 y^5 \rangle$ can become $\langle x, y | x^2 = y^3 \rangle$.

Theorem 6.2. *Any two finite presentations of the same group are related by a finite sequence of Tietze transformations.*

Proof. Take two finite presentations $\langle X|R \rangle$, $\langle Y|S \rangle$. To avoid confusion, we can suppose that the alphabets X and Y are represented by disjoints sets of symbols. Each y in Y represents some element in the group, given by some word in X, say $y = w(x)$ in the group. Take one such expression $y^{-1}w(x)$ in the alphabet $X \cup Y$ for each y in Y. Let U be the set of all these expressions. Then $\langle X|R \rangle$ becomes, after adding irrelevant generators, $\langle X \cup Y | R \cup U \rangle$.

Each x in X represents some element in the group, given by some word in Y, say $x = w(y)$ in the group. Take one such expression $x^{-1}w(y)$ in the alphabet $X \cup Y$ for each x in X. Each such expression is a consequence of the relations, because it is true in the group. Let V be the set of all these expressions. Then $\langle X \cup Y | R \cup U \rangle$ becomes, after adding irrelevant relations, $\langle X \cup Y | R \cup U \cup V \rangle$.

For each $s \in S$, the relation $s = 1$ holds in the group, so adding irrelevant relations to $\langle X \cup Y | R \cup U \cup V \rangle$ gives $\langle X \cup Y | R \cup U \cup V \cup S \rangle$.

By the same argument, starting again but reversing roles of $\langle X|R \rangle$, $\langle Y|S \rangle$, we can get from $\langle Y|S \rangle$ to

$$\langle Y \cup X | S \cup V \cup U \cup R \rangle = \langle X \cup Y | R \cup U \cup V \cup S \rangle.$$

□

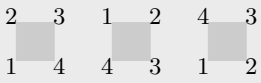
Morphisms

A *morphism* of groups is a map $\varphi\colon G \to H$ so that $\varphi(xy) = \varphi(x)\varphi(y)$: φ preserves multiplication. We have seen several of these.

Label the vertices of an equilateral triangle as $1, 2, 3$. Identify the group G of symmetries of the triangle with the symmetric group H on 3 letters, by taking each symmetry g of the equilateral triangle to the permutation $h = \varphi(g)$ of its vertices.

Label the vertices of any polygon X in the plane, or polyhedron X in Euclidean 3-dimensional space, with n vertices. Map the group G of symmetries of X to the symmetric group H on n letters, by taking each symmetry g of X to

the permutation $h = \varphi(g)$ of its vertices. This map might not be surjective. For example, if X is a square in the plane



no rotation or reflection will ever put 1 and 2 diagonally across from each other, because that would pull them apart to a greater distance.

Every element g of any group G has associated a morphism

$$\varphi\colon \mathbb{Z} \to G,$$

given by $\varphi(k) = g^k$. This map is surjective just when G is cyclic generated by g, and injective just when g has infinite order.

Take an integer $m \geq 1$ and write the cyclic group C_m in additive notation as integers modulo m. Take integers $n_1, n_2 \geq 1$ and let $G_1 := C_m^{n_1}$ and $G_2 := C_m^{n_2}$ be the product of cyclic groups; we write each element of each of G_1, G_2 in additive notation as a vector of integers modulo m:

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n_1} \end{pmatrix}.$$

Take an $n_2 \times n_1$ matrix A with coefficients integers modulo m. Define a map $\varphi\colon G_1 \to G_2$ by $\varphi(x) = Ax$. Clearly φ is a morphism of groups. On the other hand, every morphism $\varphi\colon G_1 \to G_2$ is "linear", i.e.

$$\varphi(2x) = \varphi(x + x) = \varphi(x) + \varphi(x) = 2\varphi(x)$$

and so on, for all scalar coefficients in place of 2, so adding up, using the standard "basis" vectors $e_1, \ldots, e_{n_1}$,

$$\begin{aligned} \varphi(x) &= \varphi(\sum x_i e_i), \\ &= \sum x_i \varphi(e_i). \end{aligned}$$

So if we let A be the matrix whose columns are the vectors

$$A = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n_1} \end{pmatrix},$$

where $a_i := \varphi(e_i)$, we find that $\varphi(x) = Ax$ for all x. So the morphisms $\varphi\colon G_1 \to G_2$ are precisely the $n_2 \times n_1$ matrices with entries integers modulo m.

6.6 Find all morphisms from symmetric groups to abelian groups.

6.7 Suppose that G is a group and that H and K are subgroups of G. Prove that the following are equivalent:

a. The map $\varphi\colon H \times K \to G$, $\phi(h,k) = hk$ is a morphism.

b. Every element of H commutes with every element of K.

If this occurs, then prove that the following are equivalent:

a. The map $\phi\colon H \times K \to G$, $\phi(h,k) = hk$ is an isomorphism.

b. Every element of G is expressible as a product hk, and $H \cap K = \{1\}$.

6.8 Prove that every subgroup G of any group H is the image of a morphism of groups $\varphi\colon G \to H$.

We can already apply the concept of morphism to reexamine group presentations:

Lemma 6.3. *Every map of sets $f\colon X \to G$ to a group extends uniquely to a morphism of groups $f\colon \langle X\rangle \to G$. If $R \subset \langle X\rangle$ is a set consisting entirely of words*

$$w = x_1^{a_1} x_2^{a_2} \dots x_k^{a_k}$$

on the alphabet X for which

$$f(x_1)^{a_1} \dots f(x_k)^{a_k} = 1,$$

then there is a unique morphism of groups $\langle X|R\rangle \to G$ extending f. In particular, if R generates of all such words, then f is injective.

Proof. We extend f to words by taking any word

$$w = x_1^{a_1} x_2^{a_2} \dots x_k^{a_k}$$

on the alphabet S to

$$f(x_1)^{a_1} \dots f(x_k)^{a_k}.$$

By induction, f is a group morphism. If R is as above, then $f(w) = 1$ for all $w \in \langle X\rangle$ so we can unambiguously define f on equivalence classes of words, as altering a word by an element of R or its inverse has no effect on $f(w)$. Finally, if R generates all words for which $f(w) = 1$ then $f(w_1) = f(w_2)$ just when $f(w_1 w_2^{-1}) = 1$, just when $w_1 w_2^{-1}$ is generated by R just when $w_1 w_2^{-1} = 1$ in $\langle X|R\rangle$. □

We saw above that the presentation $H := \langle b, c | 1 = b^6 = c^2 = bcbc\rangle$ gives a group which has at most 12 elements. We also saw that the group G of symmetries of a regular hexagon has exactly 12 elements. By lemma 6.3, there is a morphism $H \to G$ taking b, c to b, c, and hence onto G. But then H maps onto G, so has at least as many elements, and the morphism is therefore a bijection, so an isomorphism.

Almost everything we know about any group arises from looking at morphisms to that group and from that group. The *kernel* of a morphism $\varphi\colon G \to H$ is the set of all elements g of G for which $\varphi(g) = 1$, i.e. the elements "killed" by φ. The *image* of a morphism $\varphi\colon G \to H$ is the set of all elements h of H for which $h = \varphi(g)$ for some g in G.

6.9 Prove that the kernel of any morphism of groups $\varphi\colon G \to H$ is a subgroup of G.

6.10 Prove that the kernel of any morphism of groups $\varphi\colon G \to H$ is $\{1\}$ just when φ is injective.

6.11 Prove that the image of any morphism of groups $\varphi\colon G \to H$ is a subgroup of H.

It seems natural to ask which subgroups arise as kernels and as images.

Normal subgroups

A subgroup K of a group G is *normal* if $gKg^{-1} = K$ for any g in G.

6.12 Every rigid motion f of three dimensional Euclidean space can be written uniquely as $f(x) = Ax + b$ where A is an orthogonal matrix and b is a vector in three dimensional Euclidean space. A *translation* is a rigid motion f of the form $f(x) = x + b$. An *orthogonal transformation* is a rigid motion f of the form $f(x) = Ax$. Let G be the group of all rigid motions three dimensional Euclidean space. Let T be the set of all translations. Prove that T is a normal subgroup of G. Let U be the set of all orthogonal transformations. Prove that U is *not* a normal subgroup of G.

Theorem 6.4. *A subset K of a group G is a normal subgroup if and only if K is the kernel of some morphism $\varphi\colon G \to H$ to some group H. Indeed, if K is normal, then there is a unique group operation on G/K so that the map $\varphi\colon G \to G/K$ given by $\varphi(g) = gK$ is a group morphism with kernel K.*

Call G/K, with this group operation, the *quotient group* and $\varphi\colon G \to G/K$ the *quotient morphism*.

Proof. If K is the kernel of a morphism $\varphi\colon G \to H$ to some group H, then an element k of G belongs to K just when $\varphi(k) = 1$. But

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1}$$

so $\varphi(k) = 1$ implies $\varphi(gkg^{-1}) = 1$ i.e. if k lies in K then gkg^{-1} does too. Similarly,

$$\begin{aligned}\varphi(k) &= \varphi(g^{-1}g\,k\,g^{-1}g),\\ &= \varphi(g)^{-1}\varphi(g\,k\,g^{-1})\varphi(g),\end{aligned}$$

so $\varphi(gkg^{-1}) = 1$ implies $\varphi(k) = 1$ i.e. k lies in K just when gkg^{-1} does too. Hence K is normal.

Suppose that K is normal. Define on G/K the operation $(bK)(cK) = bcK$. It is convenient to write each coset bK of K as $\overline{b}$. Then the operation is $\overline{b}\overline{c} = \overline{bc}$, with identity $\overline{1}$. To see that this is well defined, note that knowledge of the coset bK determines b precisely up to replacing b by bk for some k in K. Hence $\overline{b}$ determines b uniquely up to the equation $\overline{b} = \overline{bk}$ for k in K. So given $\overline{b}$ and $\overline{c}$, we know b and c precisely up to replacing them with bk_0 and ck_1 for some k_0, k_1 in K. Hence this replaces bc by

$$bk_0ck_1 = bc(c^{-1}k_0c)k_1.$$

But then taking K-cosets,

$$\overline{bk_0ck_1} = \overline{bc}.$$

Hence the resulting product $\bar{bc}$ comes out the same for b, c and for bk_0 and ck_1, i.e. the operation is well defined. The kernel of this operation is the set of elements b of G for which $\bar{b} = \bar{1}$ i.e. $bK = K$ i.e. b in K. □

In a group presentation $\langle X|R\rangle = \langle X\rangle / N$ where $N \subset \langle X\rangle$ is the normal subgroup generated by R.

Sage can tell you whether the subgroup H generated by some elements r_1, r_2, r_3 is a normal subgroup:

```
A4 = AlternatingGroup(4)
r1 = A4("(1,2) (3,4)")
r2 = A4("(1,3) (2,4)")
r3 = A4("(1,4) (2,3)")
H = A4.subgroup([r1, r2, r3])
H.is_normal(A4)
```

yields True.

Theorem 6.5. *The image of any morphism of groups $\varphi\colon G \to H$ with kernel K is isomorphic to G/K by the isomorphism*

$$\bar{\varphi}\colon G/K \to H$$

given by $\bar{\varphi}(gK) = \varphi(g)$. If φ is onto, then $\bar{\varphi}$ is onto.

Proof. When we map g to $\varphi(g)$, if we replace g by gk for any k in K, this replaces $\varphi(g)$ by $\varphi(gk) = \varphi(g)\varphi(k) = \varphi(g)1 = \varphi(g)$. Hence $\bar{\varphi}(\bar{g}) = \varphi(g)$ is well defined. It is morphism of groups because $\bar{\varphi}(\bar{bc}) = \varphi(bc) = \varphi(b)\varphi(c) = \bar{\varphi}(\bar{b})\bar{\varphi}(\bar{c})$. Its kernel is $\{\,\bar{1}\,\}$, because $\bar{\varphi}(\bar{b}) = 1$ just when $\varphi(b) = 1$ just when b is in K, so just when $\bar{b} = \bar{1}$ is the identity element of G/K. □

Sage knows how to construct the quotient group G/H:

```
A4 = AlternatingGroup(4)
r1 = A4("(1,2) (3,4)")
r2 = A4("(1,3) (2,4)")
r3 = A4("(1,4) (2,3)")
H = A4.subgroup([r1, r2, r3])
A4.quotient(H)
```

yields $\langle (1,2,3)\rangle$, meaning that the quotient group is isomorphic to the group of permutations generated by the cycle (1 2 3).

Lemma 6.6. *Suppose that $\varphi\colon G \to H$ is a morphism of groups and that N_G and N_H are normal subgroups of G and H and that $\varphi(N_G)$ lies in N_H. Then there is a unique morphism $\bar{\varphi}\colon G/N_G \to H/N_H$ so that $\bar{\varphi}(gN_G) = \varphi(g)N_H$.*

Proof. If we replace g by gn for some n in N_G, then we alter $\varphi(g)$ to $\varphi(gn) = \varphi(g)\varphi(n)$. So we don't change $\varphi(g)N_H$. Hence $\bar{\varphi}$ is defined. It is easy to check that $\bar{\varphi}$ is a morphism of groups. □

6.13 The *kernel* K of the action of a group G on a set X is the set of elements g of G so that $gx = x$ for every x in X, i.e. the kernel is the set of elements that act trivially. Prove that the kernel of any action is a normal subgroup, and that there is a unique action of G/K on X so that $(gK)x = gx$ for any g in G and x in X.

Theorem 6.7. *Suppose that N is a normal subgroup of a group G and lies inside another normal subgroup H of G. Then G/H is isomorphic to $(G/N)/(H/N)$ via the map $f(gH) = (gN)(H/N)$.*

Proof. Note that H/N is a normal subgroup of G/N because its elements are hN for h in H and so, for any gN in G/N, so

$$(gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N) = ghg^{-1}N$$

lies in H/N. Therefore by the above result, the surjective morphism $\varphi\colon G \to G/N$ descends to a surjective morphism $\bar{\varphi}\colon G/H \to (G/N)/(H/N)$. The kernel of this morphism consist of the gH so that $\varphi(g)$ lies in H/N, i.e. g lies in H, i.e. $gH = H$ is the identity element. □

Amalgamations

Suppose that G and H are two groups. We would like to define a group $G * H$, which contains G and H, and is otherwise "as unconstrained as possible". The product $G \times H$ is not "unconstrained", because the elements of G commute with those of H inside $G \times H$.

First, note that any group G has an obvious group morphism $\langle G \rangle \to G$ given by $g \mapsto g$. It will help to write out concatenations using some symbol like

$$g_1 * g_2 * \cdots * g_n \in \langle G \rangle .$$

Then we can write our group morphism as

$$g_1 * g_2 * \cdots * g_n \in \langle G \rangle \mapsto g_1 g_2 \dots g_n \in G.$$

This group morphism is clearly surjective, with kernel precisely the group $N_G \subset \langle G \rangle$ whose elements are the concatenations

$$g_1 * g_2 * \cdots * g_n$$

for which $g_1 g_2 \dots g_n = 1$. So we can write

$$G = \langle G | N_G \rangle.$$

Think of N_G as encoding all of the equations satisfied inside the group G.

The *free product* $G * H$ to be the group $\langle G \sqcup H | N_G \sqcup N_H \rangle$ generated by the elements of G and H, subject to the relations consisting of all equations satisfied by elements of G together with all equations satisfied by elements of H.

Another way to look at this: a *word* in G, H is a finite sequence of elements of G and of H (perhaps empty), written beside one another with $*$ symbols inbetween, like

$$g_1 * g_2 * h_1 * g_3 * h_2 * h_3 * g_4,$$

et cetera. We denote the empty sequence as 1. We *reduce* a word by deleting any appearance of the identity element (of either group), and also by replacing any two neighboring elements from the same group by their product in that group:

$$g_1 * g_2 \mapsto g_1 g_2.$$

A word is *reduced* if we cannot further reduce it. The group $G * H$ is the set of reduced words, with multiplication being simply writing down one word after another and then reducing. In practice, we never write the $*$ in expressions $g_1 * g_2$.

6.14 Let G be the cyclic group of order 2 and H the cyclic group of order 3. Prove that every element of $G * H$ has order $1, 2, 3$ or ∞.

A further wrinkle: suppose that $K \subset G$ is a subgroup which also appears as a subgroup of H: $K \subset H$. The *amalgamation* of G and H over K, denoted $G *_K H$, is

$$G *_K H = \langle G \sqcup H | N_G \sqcup N_H \sqcup E \rangle$$

where E is the collection of equations $k_G = k_H$ where k_G is an element of K as a subgroup of G, and k_H is the associated element of $K \subset H$.

Again, elements of $G *_K H$ are written as words, but we allow ourselves, to treat any expression $g * h$ as equal to $gk * k^{-1}h$, and $h * g$ as equal to $hk^{-1} * kg$ for any $k \in K$, and again we won't write explicitly the $*$ symbol when we compute.

Chapter 7

Automorphisms

Automorphisms

An *automorphism* of a group G is an isomorphism of G with itself.

7.1 What are all of the automorphisms of a cyclic group with a prime number of elements?

Consider a product $G = C_m^n$ of cyclic groups of some order m. Write C_m in additive notation as integers modulo m. As we have seen, the morphisms $\varphi\colon G \to G$ are identified with matrices A with elements being integers modulo m, each morphism mapping $x \in G \mapsto Ax \in G$. So the automorphism group consists of the invertible matrices with such entries. When we take determinant, $\det A$ is an integer modulo m. The determinant of a product is still the product of determinants, since this is true in integers, and then just reduce both sides of the equation by multiples of m. So in particular, if our matrix A has an inverse, then its determinant is an integer modulo m which has an inverse integer modulo m. This condition is necessary, and is sufficient if m is a prime (since then integers modulo m form a finite field, which the reader may be familiar with). For example, for $G = C_2^2$, these are 2×2 matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

so that $ad - bc = 1$ in the arithmetic of integer remainders modulo 2. The reader can check that these are the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

So there are six different automorphisms of C_2^2.

The *automorphism group* of a group G is the group Aut_G of all automorphisms of G.

Above we found $\mathrm{Aut}_{C_2^2}$ to be a group of order 6, i.e. with 6 elements.

Inner automorphisms

If N is a normal subgroup of a group G, then G acts on N by conjugation, since $gNg^{-1} = N$, i.e. each $g \in G$ takes each $n \in N$ to $gng^{-1} \in N$, often also denoted $n^g := gng^{-1}$ to save ink, and sometimes also written $\mathrm{ad}_g\, n$ (as the conjugation action is also called the *adjoint* action). This defines a morphism $\mathrm{ad} \colon G \to \mathrm{Aut}_N$. Note that g commutes with n just when $gn = ng$, so just when $gng^{-1} = n$, so just when $\mathrm{ad}_g\, n = n$, so just when ad_g fixes n. In particular, ad_g is trivial on all of N just when $g \in C_N$. Hence the conjugation action drops to an action of G/C_N:

$$\mathrm{ad} \colon G/C_N \to \mathrm{Aut}_N\,.$$

More generally, if H is any subgroup of a group G, then we can define in exactly the same way an action

$$\mathrm{ad} \colon N_H/C_H \to \mathrm{Aut}_H\,.$$

(The quotient N_H/C_H is often encountered, sometimes called the *Weyl group* of H as a subgroup of G.)

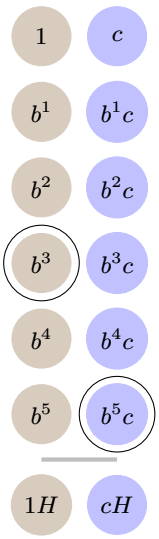
Semidirect products

Take a group G acting transitively on a set X, and pick a point $x_0 \in X$. Let $H := G^{x_0}$ be the stabilizer, so we can identify $X = G/H$. A *section* is a choice, for each $x \in X$, of element $g(x) \in G$ so that $g(x)x_0 = x$.

Let X be the plane, and G the group of rigid motions of the plane. Pick some point $x_0 \in X$ of the plane, call it the origin, and then let $g(x)$ be the unique translation that translates the origin to the point x. If we think of the plane as a vector space and write its origin x_0 simply as 0, as we usually would in linear algebra, then $g(x) = x$, i.e. the translation that takes the origin 0 to the point x in the plane is the translation by adding the constant vector x to every vector.

If X is the circle and G the rotations of the circle, associate to each point $(x, y) \in X$ of the circle the angle θ (defined up to 2π integer multiple) from $(1, 0)$ to (x, y). Let $g(x, y)$ be rotation by angle θ, a section.

Writing $X = G/H$, we can think of each $x \in X$ as a coset gH. A section is a choice of some $g \in G$ inside that coset, i.e. a choice of one element inside each coset. So a section is just a subset of G which has one element in each coset, a cross section of the cosets, hence the name "section" short for "cross section". The map $g \in G \mapsto gH \in G/H$ then identifies the section, say $Q \subset G$, with the quotient space G/H.



Let X be the plane, and G the group of rigid motions of the plane. The group H is the group of rigid motions fixing a point, i.e. the group of orthogonal transformations (with that point taken as origin). The section we described above, as a cross section of the cosets $X = G/H$, is just exactly the set of translations. In particular, in our example, the section is a subgroup of G.

Let X be the rotations of the plane, and G the group of rigid motions of the plane, acting on X by the orthogonal transformation part, ignoring the translation part, i.e. to a rigid motion $g\colon x \mapsto Ax + b$, we associate A. The stabilizer group H is the group of translations: $x \mapsto x + b$, so $A = I$. The cosets gH consists of all rigid motions with a given orthogonal transformation A. Hence the orthogonal transformations form a section. In particular, in our example, the section is a subgroup of G. Even better: the group H in this example is a normal subgroup, and the quotient $X = G/H$ is therefore a group. Better still: the section, i.e. the set of rotations, is a subgroup of G isomorphically mapped to the quotient group G/H by the quotient map.

Clearly this is a special event; in our picture above, our section is not a subgroup, since it doesn't even contain the identity element. We designate this with a special name: a group G is a *semidirect product* of subgroups N and Q if N is a normal subgroup of G and every N-coset in G contains a unique element of Q.

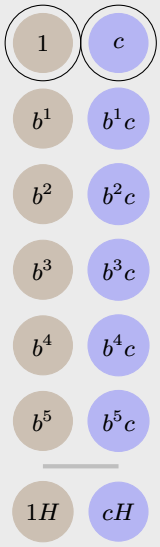
The group of rigid motions of the plane is a semidirect product of the translations with the orthogonal transformations.

Careful: as we have seen, being a semidirect product of N, Q is *not* the same as being a semidirect product of Q, N. Another way of thinking about semidirect

products is that Q is a subgroup which "lifts" up G/N to live inside G, not just a quotient of G but also a subgroup.

7.2 Prove that a group G is a semidirect product of subgroups N, Q just when N is a normal subgroup of G and $N \cap Q = \{1\}$ and every element of G is a product of one from N and one from Q. (It is easier to check this.)

The dihedral group D_6, i.e. the group of symmetries of the hexagon in the plane, is the semidirect product of (1) the group consisting of the identity and the transformation given (if the hexagon is centered at the origin) by mapping each vector in the plane to its negative $(x, y) \mapsto (-x, -y)$ and (2) the rotations of the hexagon. More abstractly, we can say that D_6 is the semidirect product of the cyclic group of order 6 and the cyclic group of order 2.



Let G be the group of all invertible $n \times n$ matrices with real number coefficients which are zero above the diagonal: the *upper triangular*. Let N be the subgroup of G consisting of those matrices in G which have 1 in every diagonal entry, the *strictly upper triangular*. Let Q be the subgroup of G consisting of those matrices in G which are zero except along the diagonal. Clearly $N \cap Q = \{1\}$. The reader can check that we can write every element of G as a product of an element of N and one of Q. So G is a semidirect product of Q, N. Note that Q is not a normal subgroup of G, so G is not a semidirect product of N, Q.

Hints

1.2. Denote by ${}^{\#}S$ the number of elements in a set S. We use the basic fact that if $S \subseteq T$ is a subset of a finite set T, then ${}^{\#}S \leq {}^{\#}T$, with equality just when $S = T$. The image of f is $f(X) \subseteq X$, equality just when f is surjective, i.e. just when ${}^{\#}f(X) = {}^{\#}X$. Each element maps somewhere, i.e. lies in $f^{-1}(x)$ for some $x \in f(X)$:

$$ {}^{\#}X = \sum_{x \in f(X)} {}^{\#}f^{-1}\{\, x \,\} \geq \sum_{x \in f(X)} 1 = {}^{\#}f(X), $$

with equality, i.e. f surjective, just when $f^{-1}\{\, x \,\}$ has one element for every $x \in f(X)$, i.e. just when f is injective.

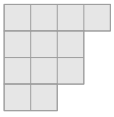
2.2. We can simply permutate the vertices in any way at all by symmetries, as we can rotate any one vertex to any other, and then fixing that vertex, the symmetries of the opposite faceare arbitrary symmetries of an equilateral triangle, so carry out any permutation of its vertices.

2.3. Apply each cycle in succession to 1: $(543)1 = 1$, $(234)1 = 1$, $(123)1 = 2$. So $(123)(234)(543)1 = 2$. Similarly apply them to 2: $(543)2 = 2$, $(234)2 = 3$, $(123)3 = 1$. So $(123)(234)(543)2 = 1$. Continue in this way to find (a) $(123)(234)(543) = 21543$. Clearly this takes $1 \to 2 \to 1$ and $3 \to 5 \to 3$ and $4 \to 4$, so (b) as a product of disjoint cycles $(123)(234)(543) = (12)(35)$.

2.4. (234):

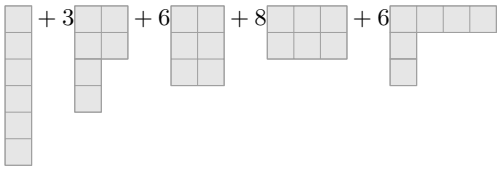
$$ \begin{aligned} &1 \to 4 \to 1, \\ &2 \to 4 \to 2 \to 3, \\ &3 \to 2 \to 3 \to 4, \\ &4 \to 3 \to 1 \to 2. \end{aligned} $$

2.5. Indicate cycle lengths in a permutation by drawing boxes, a row of them to indicate a cycle of that length, arranged successively shorter: the *Young diagram* of a permutation. For example,



indicates a permutation which has cycles of lengths $4, 3, 3, 2$. The group G of rotations of a cube moves any vertex to any other (8 in all), and rotates a vertex around taking any edge at that vertex to any other (3 in all), but once we fix a vertex and edge, we fix everything, so the group has exactly $8 \cdot 3 = 24$ elements. Every rotation is a rotation around an axis, through the centre of the cube. It is determined completely by how it acts on the centres of the faces, as they contain a basis of vectors. The

identity 1 fixes every face, so has 6 cycles (all of length 1) as permutation of the faces. A rotation of angle π around an axis through the center of a face fixes two faces and permutes two others, so a pair of disjoint cycles of length 2; there are 3 such, as there are three choices of axis. A rotation of angle π around an axis through the center of an edge permutes three pairs of faces, so a triple of disjoint cycles of length 2; there are 6 such rotations. An element of order 3 is a rotation around an axis through two opposite corners: it is a cycle of order 3 on the three faces touching one corner, and also of order 3 on the opposite three faces touching the opposite corner. There are 4 choices of a pair of opposite corners, and then 2 directions of rotation, so 8 such rotations. An element of order 4 is a rotation by angle $\pi/2$, so around some axis through two opposite faces, giving one cycle of length 4; there are 3 choices of axis, but we can point the axis in either direction, so 6 such rotations. We can sum the various permutations of the faces of cube arising from rotations as:



2.7. In general, if

$$g = \dots (a_1 a_2 \dots a_k) \dots$$

where the $\dots$ indicate other cycles, in a product of disjoint cycles, then hgh^{-1}, when applied to $h(a_i)$ gives

$$\begin{aligned}(hgh^{-1})(h(a_1)) &= hgh^{-1}h(a_1),\\ &= hg(h^{-1}h)(a_1),\\ &= hg(a_1),\\ &= h(a_2),\end{aligned}$$

and so on: hgh^{-1} takes $h(a_i)$ to $h(a_{i+1})$ and takes $h(a_n)$ to $h(a_1)$. If g is a product of cycles, the same thing works applied one at a time.

2.8. Start with just one cycle, say $(a_1 a_2 \dots a_k)$ and one cycle $(b_1 b_2 \dots b_k$. Then let $ga_1 := b_1, \dots, ga_k := b_k$, and let $gx := x$ for x not among $a_1, \dots, a_k$. Let's check that $(b_1 \dots b_k) = g(a_1 \dots a_k)g^{-1}$. The left hand side acts on b_1 by moving it to b_2, and so on. The right hand side takes b_1, applies g^{-1} to it, so gives a_1, then moves a_1 to a_2, and then applies g to that, giving b_2, and so on. Now for two disjoint cycles, say

$$g_1 = (a_1 a_2 \dots a_k)(\alpha_1 \alpha_2 \dots \alpha_\ell)$$

and

$$g_2 = (b_1 b_2 \dots b_k)(\beta_1 \beta_2 \dots \beta_\ell),$$

let $ga_i := b_1$ and $g\alpha_i := \beta_i$ and $gx = x$ for any other x. Again check that $g_2 = gg_1g^{-1}$. Proceed by induction.

2.10. (12)(23)(34)(45)(56)(67)(56)(45)(34)(23)(12)

2.11. The four things that can happen above: gt has some numbers n_{gt}, c_{gt} of elements and cycles:

case	n_{gt}	c_{gt}	$n_{gt} - c_{gt}$
1)	$n_g + 2$	$c_g + 1$	$(n_g - c_g) + 1$
2)	n_g	$c_g + 1$	$(n_g - c_g) - 1$
3)	n_g	$c_g - 1$	$(n_g - c_g) + 1$
4)	$n_g + 1$	c_g	$(n_g - c_g) + 1$

2.13. Take a permutation g. Write each cycle as a product of transpositions as we have done: g is a product of $n-c$ transpositions. But maybe there is a shorter way to write g as a product of transpositions; denote by ℓ the length of g. So $n-c-\ell \geq 0$, and we need only prove that $n-c-\ell = 0$. Clearly if $\ell = 0$, $g = ()$, $n-c-\ell = 0-0-0 = 0$. Similarly if $\ell = 1$, g is a transposition, $n - c - \ell = 2 - 1 - 1 = 0$. Suppose that we find some counterexample permutation g, so $n - c - \ell > 0$. Write g as product of ℓ transpositions, say $g = ht$ where t is a transposition. So $\ell_h \leq \ell_g - 1$, and as above, $n_h - c_h \geq n_g - c_g - 1$, so $n_h - c_h - \ell_h \geq n_g - c_g - \ell_g$, and we have a shorter counterexample. By induction, construct a counterexample with $\ell = 1$, a contradiction.

2.14. Let $q := p^{-1}$ and $s := r^{-1}$, so

$$\begin{aligned}
(r(pb))(t_1, \ldots, t_n) &= pb(t_{s(1)}, \ldots, t_{s(n)}), \\
&= b(t_{q(s(1))}, \ldots, t_{q(s(n))}), \\
&= b(t_{q\circ s(1))}, \ldots, t_{q\circ s(n))}), \\
&= (q \circ s)^{-1} b(t_1, \ldots, t_n), \\
&= (s^{-1} \circ q^{-1}) b(t_1, \ldots, t_n), \\
&= (rp) b(t_1, \ldots, t_n).
\end{aligned}$$

2.15. We can transpose i and $i+1$ as $(i \;\; i+1)$. We can transpose i and $i+2$, as a product $(i \;\; i+1)(i+1 \;\; i+2)(i \;\; i+1)$. Similarly, we can write any transposition as a product of an odd number of transpositions of neighboring integers: if $i < j$,

$$(i \;\; j) = (i \;\; i+1)(i+1 \;\; i+2)\ldots(j-2 \;\; j-1)(j-1 \;\; j)\ldots(i+1 \;\; i+2)(i \;\; i+1).$$

2.19. If we make a move by sliding a tile left or right, we don't change x or y, so z is the same. If we make a move by sliding a tile up or down, we change y and also carry out a cycle in the order of the tiles. If that tile is in the first column, we are making a cycle of length 4:

and the same for any other column, since we have one less square above and one more below. So the value of x always changes. So z stays the same. The initial picture:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

differs from the final one:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

by a single transposition, with no row swap, so different value of z.

3.9. Suppose first that $x_0 = 0$. For any $y \in \mathbb{R}$, let p_y be the polynomial $p(x, y)$. Let y' be the inverse of y in the group. Then $p_y \circ p_{y'}(x) = x$, so that $\deg p_y \deg p_{y'} = 1$. So $p(x, y)$ has degree 1 in x, and by the same argument has degree 1 in y. So $p(x, y) = a + bx + cy + dxy$ for some numbers a, b, c, d. Since $p(x, 0) = x$ and $p(0, y) = y$, $a = 0$ and $b = c = 1$.

If $d \neq 0$, then pick x_0 to be the unique solution to $1 + dx = 0$, i.e. $x_0 := -1/d$. Let x_0' be the inverse of x_0 in the group. The map taking y to $x_0 * y = p(x_0, y)$ has inverse map $y \mapsto x_0' * y$, so is a bijection. But

$$\begin{aligned} x_0 * y &= p(x_0, y), \\ &= x_0 + y + dx_0 y, \\ &= x_0 + y(1 + dx_0), \\ &= x + 0, \end{aligned}$$

is constant, not a bijection, a contradiction, so $d = 0$, i.e. $p(x, y) = x + y$.

If the identity element is x_0 instead, then the operation $x \otimes y = p(x+x_0, y+x_0) - x_0$ is a new group operation with identity element 0, so $p(x + x_0, y + y_0) = x + y + x_0$.

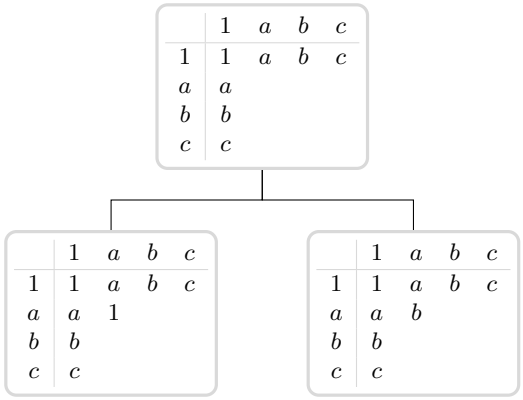
3.12.

We start only knowing that $1a = a$, and so on:

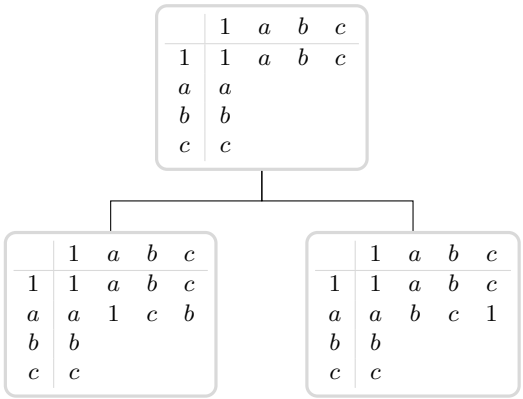
	1	a	b	c
1	1	a	b	c
a	a			
b	b			
c	c			

In the first blank, entry, we have to put $1, a, b$ or c; we are choosing the value of a^2. If you pick b and I pick c, we could just swap the letters b and c in the alphabet to get your choice to agree with mine. If we pick $a^2 = a$ then cancel an a from both sides to get $a = 1$, not possible since our group has 4 distinct elements. So $a^2 = 1, b$ or c, and

swap letters to get $a^2 = 1$ or b:



Since every element of the group occurs exactly once in each row and column, in the left hand table, the next element across is b or c. But there is already a b in the column, so c, forcing the next entry to be b. In the right hand table, the next element is either 1 or c. But we have a c in the final column, so



Going down the 2nd columns, we have (in the left hand table) already used $a, 1$, and in the 3rd row we already have a b, so c, and then b. Similarly (in the right hand table), in the 2nd column, we have already used a, b, and we have a c in the last row,

so we must use 1 in the 2nd column, last row, and so a c above that.

	1	a	b	c
1	1	a	b	c
a	a			
b	b			
c	c			

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c		
c	c	b		

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c		
c	c	1		

On the left hand table, we can next pick a 1 or a, b On the right hand, either a 1 or an a, but we have a 1 in the last row, so we can't put another 1 in that row, so must be $1, a$:

	1	a	b	c
1	1	a	b	c
a	a			
b	b			
c	c			

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c		
c	c	b		

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	a	1
c	c	b	1	a

If we swap the letters a, b, we find the second and third tables become the same, so drop the second one:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	a	1
c	c	b	1	a

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

One then has to check that these are in fact groups, as they both turn out to be.

4.4. If a and b are elements of G then $a^2 = 1$ so $a = a^{-1}$, and the same for b. But also $1 = (ab)^2 = abab$, so $ab = b^{-1}a^{-1} = ba$, hence G is abelian. Since G is finite, G is finitely generated, and we take a minimal set of generators, say $g_1, \ldots, g_n$. Because G is abelian, these commute with each other, so in any expression in these generators, we commute them past each other until they are in "alphabetical order", so every element of G has an expression $g_1^{k_1} \ldots g_n^{k_n}$. Reduce using $x^2 = 1$ until each exponent k_i is zero or one. Each such expression is unique, since two such expressions, after cancelling from both sides, give us some relation among the generators allowing us to expression one generator in terms of others, i.e. to use fewer generators.

4.6. Take a subgroup H of a cyclic group G. Suppose that G is generated by an element x, i.e. consists of the integer powers of x. The elements of H consist only of certain powers of x; let $S \subset \mathbb{Z}$ be the set of integers k so that x^k belongs to H. Clearly $x^k x^\ell = x^{k+\ell}$ and $(x^k)^{-1} = x^{-k}$, and $1 = x^0$, so S is a subgroup of $\mathbb{Z}$ under addition. If $S = \{\,0\,\}$, clearly $H = \{\,1\,\} \subset G$ is cyclic. But if $S \neq \{\,0\,\}$, then S contains a least positive element, say n. Then S contains all integer multiples of n. If S contains some integer k, then S contains $uk + vn$ for any integers u, v, and in particular (if u, v are the Bézout coefficients of k, n), S contains the greatest common divisor of k, n, which is at most as large as n. But n is the smallest positive integer in S, so that greatest common divisor of k, n is n, i.e. n divides k. So n divides all elements of S: S is the set of all integer multiples of n, and so H is generated by x^n, so cyclic.

4.8. There is a cyclic group $\mathbb{Z}/6\mathbb{Z}$ of order 6 and a dihedral group D_3. Take a group G of order 6 and an element g of G of largest order. Note that g has order 6 just when G is the cyclic group of order 6. Also, the order of g divides the order of G, i.e. divides 6, so is 1, 2 or 3. If g has order 1, being of maximal order, so do all other elements of G. But then all elements are the identity element, so G has order 1, a contradiction. Hence g has order 2 or 3. If g has order 2, by problem 4.4 on page 19, G is a product of copies of $\mathbb{Z}/2\mathbb{Z}$, so has order a power of 2, a contradiction. So finally g has order 3. Take an element h which is not a multiple of g. There are 2 cosets of the subgroup $1, g, g^2$, so every element is $1, g, g^2, h, hg, hg^2$. So h^2 is one of these. If $h^2 = hg^k$ then cancel an h to find h in the subgroup $1, g, g^2$. So $h^2 = g^k$ for some $k = 0, 1, 2$. Replacing g by g^2 if needed, we can assume $k = 0, 1$. If $k = 1$, h does not have order 2, so has order 3. Multiply both sides by h to get $1 = hg$, so $h = g^2$, not possible. Hence $k = 0$: $h^2 = 1$.

The element gh must be among $1, g, g^2, h, hg, hg^2$. If among $1, g, g^2$, we solve for h as a power of g, a contradiction. If $gh = h$, $g = 1$, a contradiction. So gh is among hg, hg^2.

If $gh = hg$, then G is abelian and

$$(gh)^2 = g^2h^2 = g^2 \neq 1,$$

so gh has order 3, but

$$(gh)^3 = g^3h^3 = h,$$

a contradiction.

We conclude that $gh = hg^2$. This completely determines the multiplication table. Indeed, the dihedral group D_3, the symmetry group of an equilateral triangle, is isomorphic to G, as h acts by reflection, and g by rotation.

5.4. We have numbers n of group elements g with various numbers c_g of cycles:

n	c_g
1	6
3	4
6	3
8	2
6	3

Hence

$$\frac{1}{|G|}\sum_{g\in G} n^{c_g} = \frac{1}{24}(n^6+3n^4+6n^3+8n^2+6n^3) = \frac{1}{24}n^2(n+1)(n^3-n^2+4n+8),$$

so for various values of n:

n	$\lvert C\rvert$
1	1
2	10
3	57
4	240
5	800

5.8. Let X be the set of subgroups and take some point $x_0 \in X$ representing some subgroup H_0. The map $G/G^{x_0} \to Gx_0$ is onto the orbit through x_0. So the orbit has $[G : G^{x_0}]$ elements, where G^{x_0} is the stabilizer, i.e. the set of elements $g \in G$ which fix H_0 under conjugation, i.e. $H_0^g = H_0$, i.e. $gH_0g^{-1} = H_0$, i.e. $g \in N_H$.

5.9. The center consists precisely of the elements whose conjugacy orbit is a single element. Any other orbit has order $[G : G^{x_0}] = |G|/|G^{x_0}|$ an integer dividing $|G|$, so a power of p. Hence all the union of those other orbits has number of elements a multiple of p, as does $|G|$. So the difference does as well, i.e. p divides the order of the center of G. But 1 is in the center, so the center has positive order.

Bibliography

Index