GROUP THEORY

JACK DESERRANO

These notes are based on Richard Borcherds's YouTube series on group theory (at https://www.youtube.com/playlist?list=PL8yHsr3EFj51pjBvvCPipgAT3SYpIiIsJ.)

Contents

Date: December 15, 2021.

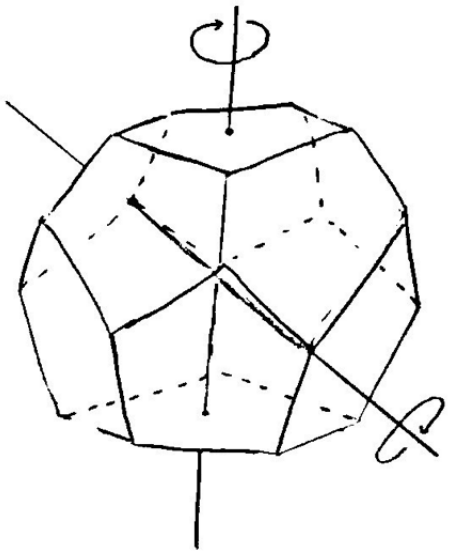


FIGURE 1. The rotational symmetries of a dodecahedron.

1. INTRODUCTION

A symmetry is a way of mapping something to itself while preserving that thing's structure, and a **group** is a collection of the symmetries of something. We can consider the Platonic solids, for instance.

What symmetries does the dodecahedron have? We can rotate it about an axis going through two opposite faces; whenever we rotate it by 1/5 of a revolution about this axis, it will appear the same, so this rotation is a symmetry.

We might also rotate it about an axis going through opposing vertices; if we rotate it by 1/3 of a revolution about this axis, it will appear the same, so this rotation is also a symmetry. Please refer to figure 1 for a rough visual.

We call the first symmetry a symmetry of **order** 5, and the second a symmetry of order 3; this refers to how many times you apply the symmetry to get back to where you started. The dodecahedron also has symmetries of order 2 corresponding to flipping it about opposite edges and one symmetry of order 1 corresponding to doing nothing.

How many symmetries does the dodecahedron have? It turns out that it has 60 symmetries, corresponding to the 5 rotations of each face and the 12 faces.

The cube has 24 symmetries, the octahedron 24, the icosahedron 60, and the tetrahedron 12. We should notice that the cube and the octahedron and the dodecahedron and the icosahedron have the same number of symmetries. This fact is no coincidence, and we will explore it later.

We call the rotational symmetry group of order 5 **cyclic** of order 5, which we will write as $\mathbf{Z}/5\mathbf{Z}$.

We can also form the symmetry group of n identical objects. There are $n!$ of these symmetries, and we call the corresponding group the **symmetric group** on n objects and denote it S_n.

We can also consider the group of symmetries of a vector space over a field. Let's consider $\mathbf{R}^3$ over $\mathbf{R}$. We can let the symmetries here be the maps that preserve addition and multiplication by real numbers, given by all invertible 3×3 matrices (invertible since we do not want to map to a proper subset of the original vector space). We call this group of three-by-three matrices with nonzero determinant $\mathrm{GL}_3(\mathbf{R})$, the **general linear group** of dimension 3.

Now consider the symmetries of the complex numbers. One such symmetry is complex conjugation, and it preserves almost all operations involving the complex numbers that you can think of. So $\mathbf{C}$ has a symmetry group of order 2: the Galois group of $\mathbf{C}/\mathbf{R}$.

In physics, we have 4 dimensional spacetime. The groups of symmetries of spacetime are the Lorentz group and the Poincaré group, where the former fixes a point. These two groups are instrumental in special relativity.

The group SU_3 is useful in QCD: it is the set of three-by-three unitary matrices.

We can even consider the symmetries of a group, for instance, $\mathbf{Z}/5\mathbf{Z} = \{0, 1, 2, 3, 4\}$ and its symmetries. For instance, we have the map

$$\mathbf{Z}/5\mathbf{Z} \to \mathbf{Z}/5\mathbf{Z} : a \mapsto a^2.$$

There are 4 symmetries in total.

Indeed, there are axioms for a group. We know that it must be a set with some multiplication (composition of symmetries), written ab, $a + b$. This multiplication must be associative: $(ab)c = a(bc)$. A group also needs an identity element, often denoted $0, 1, e$, that satisfies $1a = a1 = a$. Lastly, each symmetry in a group needs an inverse $a^{-1}, -a$ that satisfies $a^{-1}a = aa^{-1} = 1$.

What are the goals of group theory? The first is to classify all groups up to isomorphism. (We will digress on what isomorphism means.) If G, H are groups and there is a map f between them that is bijective, $f(1) = 1$, $f(ab) = f(a)f(b)$, $f(a^{-1}) = f(a)^{-1}$, then f is an **isomorphism**. We also want to classify all ways a group can be discussed as the symmetries of something (the concern of representation theory). In particular, if the group acts on a set, it is called a permutation representation. If it acts as the symmetries of a vector space, it is called a linear representation.

2. Cayley's theorem

Essentially, Cayley's theorem states that a group always corresponds to the symmetries of some object.

A group G acts on a set S if there is a function from $G \times S$ to S that takes an element g from the group and s from the set to $g(s)$. We need that $(gh)s = g(hs)$ and $1s = s$. For example, if G is the symmetries of the octahedron and S is 6 vertices of the octahedron then we can define such a function.

You might notice that there is an obvious action of G on itself. Namely, if $S = G$, then we can define $g(s) = gs$. Therefore, G is a subgroup of the permutations of S. (Let's digress

on what a subgroup is.) G is a **subgroup** of H if G is a subset of H with the same product, containing 1, and closed under this product.

We can also define an action that involves a function $S \times G \to S$ with $s, g \mapsto (s)g$ satisfying the axioms as described above. This is called a right action as opposed to the left action that was described prior.

These actions do not need to be the same. When we consider left and right actions of G on itself, we might ask if $gs = sg$ holds. If it does, then s and g are said to commute. If $gs = sg$ for all elements in G, we call G **commutative** or **abelian**. Groups are not commutative, usually. A simple example of a noncommutative group is the symmetries of a triangle.

Suppose G acts on $S = G$ on the left. Then this preserves the right action of G. Symbolically, this means that $g(sh) = (gs)h$, so it becomes clear that this follows from associativity. Hence, we can treat G as the symmetries of an object with structure, where the object is $S = G$ and the structure is the right action of G on S. G is the group of all such symmetries (acting on the left). It is important to note that G preserves the right action of G on S, not the group structure of S.

There are eight ways a group G can act itself (four left actions and four right actions).

1. $g(s) = s$ (trivial).
2. $(s)g = s$ (trivial).
3. $g(s) = gs$ (left translation).
4. $(s)g = sg$ (right translation).
5. $g(s) = sg^{-1}$.
6. $(s)g = g^{-1}s$.
7. gsg^{-1} (conjugation).
8. $g^{-1}sg$ (conjugation).

We cannot take the right actions and turn them into left actions. For example, suppose we have $g(s) = sg$. Then $(gh)s = sgh$, $(gh)s = g(hs)$, and $g(hs) = (sh)g$. But, we see that $sgh \neq (sh)g$ if G is noncommutative. So $g(s)$ cannot be sg.

3. Homomorphisms

A **homomorphism** is a map $f : G \to H$ that preserves multiplication:

$$f(ab) = f(a)f(b).$$

So $f(1) = 1$ and $f(a^{-1}) = f(a)^{-1}$. An isomorphism is a bijective homomorphism, an automorphism is an isomorphism from G to itself, and the kernel of f is the set of elements a with $f(a) = 1$.

Consider the map

$$\exp x = 1 + x + x^2/2 + \cdots .$$

We have $\exp(x + y) = \exp x \exp y$, where the first multiplication is addition in the real numbers, and the second is multiplication in the nonzero real numbers. This is not a bijection as it is not onto. It is an isomorphism from the real numbers under addition to the positive real numbers under multiplication. Here, the inverse map is $\log x$.

Recall the determinant of a matrix, and, specifically, recall that

$$\det AB = \det A \det B.$$

The determinant is a homomorphism from $\mathrm{GL}_n(F)$ to F^*. The kernel of this map is $\mathrm{SL}_n(F)$, the **special linear group** of dimension n.

Consider the group $\mathbf{Z}/4\mathbf{Z}$, which is defined under addition, and $(\mathbf{Z}/5\mathbf{Z})^*$, the nonzero integers modulo 5 under multiplication. They both have 4 elements, and, in fact, they are isomorphic. The isomorphism is defined by

$$\begin{aligned} f : 0 &\mapsto 1 \\ 1 &\mapsto 2 \\ 2 &\mapsto 4 \\ 3 &\mapsto 3. \end{aligned}$$

We can verify that $f(a+b) = f(a)f(b)$. Also, you might notice that $f(a) = 2^a$.

The elements of $\mathbf{Z}/4\mathbf{Z}$ are automorphisms of $\mathbf{Z}/5\mathbf{Z}$. For example, the map $g \mapsto 2g$ is an automorphism of $\mathbf{Z}/5\mathbf{Z}$ since it has an inverse $g \mapsto 3g$. (Since $2 \cdot 3g = 6g \equiv g \pmod 5$.)

We can consider a map from the real numbers to the **circle group** S^1. The multiplication in S^1 is defined by

$$(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1).$$

There is a homomorphism from the real numbers to S^1 which takes an angle θ to $(\cos\theta, \sin\theta)$. In particular, $f(\theta_1 + \theta_2) = f(\theta_1)f(\theta_2)$, where the second multiplication is as written above. The kernel of this homomorphism is the set of all integer multiples of 2π.

Now, consider the group of rotations of an octahedron (of order 24). There is a homomorphism from this group to S_3 (the permutations of three points). If we consider the three diagonals of the octahedron, these are the "points" permuted by any rotation. The kernel of this homomorphism has four elements (three 180 degree rotations about diagonals and the identity).

4. Lagrange's theorem

There is only group of order 1, namely the trivial group. There is only one group of order 2, and it is $\mathbf{Z}/2\mathbf{Z}$. As we go through these groups, we will find Lagrange's theorem useful.

Theorem 4.1 (Lagrange)
The order of a subgroup H of a group G divides the order of G.

Corollary 4.2
The order of an element in G divides the order of G.

The order of an element g is the smallest $n > 0$ such that $g^n = 1$. Therefore, $\{1, g, \ldots, g^{n-1}\}$ is a subgroup of G of order n, which we call the group generated by g.

Now, we can consider groups G of order p prime. The order of an element in G divides p, so it is 1 or p. The identity element corresponds to the element of order 1, and we have elements of order p. So G is cyclic of order p, and any group of order p is cyclic of order p.

Suppose G acts on a set S. We can pick some $s \in S$ and consider the set H of elements g with $gs = s$. H is a subgroup of G. Suppose H is a subgroup of G. Can we find a set S and $s \in S$ so H is the fixed subgroup of s? We can.

Any set acted on by G splits up into orbits. The **orbit** of an element s in S is the set of elements in S to which s can be mapped by elements of G. The action of G on S is called **transitive** if there is only one orbit.

Suppose G acts transitively on S and let H be the group fixing s. How can we reconstruct S from H and G? We pick $s \in S$ and let H the group fixing it. Any other point $t = gs$ for some g. Suppose $t = g_1 s = g_2 s$. This means that $g_2^{-1} g_1 s = s$, so $g_2^{-1} g_1 \in H$. So $g_1 \in g_2 H$ (where $g_2 H$ is called a left coset of H). So $g_1 H = g_2 H$, and we can identify the elements in S with left cosets of H, where this correspondence is satisfied by $t \mapsto \{g : gs = t\}$ and $gs \leftarrow\!\shortmid\, gH$.

This gives the geometric interpretation of cosets. Left cosets can be thought of the elements of a set acted on by G on the left, and similarly for right cosets.

So, given H, G, we can reconstruct a set S acted on by G as the set of left cosets of H. We must do some checks to corroborate this. First, any two cosets $g_1 H, g_2 H$ are the same or disjoint. To show this, if they are not disjoint, they have an element in common, so suppose $g_1 h_1 = g_2 h_2$. This means that $g_1 = g_2 h_2 h_1^{-1}$, so $g_1 H = g_2 h_2 h_1^{-1} H$, and $h_2 h_1^{-1} H = H$, so $g_1 H = g_2 H$. So G is a disjoint union of cosets gH. G acts on the cosets by $g(g_1 H) = (g g_1) H$. This is a group action.

We also need to show that any two cosets have the same size, that is gH has the same size as H. We can map any element $t \in gH$ to $g^{-1} t$, which is in H, and any element $h \in H$ to gh. These are inverse maps. This uses inverses, so a semigroup does not have this property.

Now we have Lagrange's theorem. G is a disjoint union of the cosets of H, and all cosets are of the same order, so $|G| = |H| \times$ the number of cosets. So, the order of H divides the order of G.

We get Fermat's little theorem, namely $x^p \equiv x \pmod{p}$, as a consequence of Lagrange's theorem. Lagrange's theorem says that the order of $g \in G$ divides the order of G, so, in particular, we get $g^{|G|} = 1$. Take $G = (\mathbf{Z}/p\mathbf{Z})^*$. Since there are no zero elements in G, any $a \in G$ is prime to p, so we can solve $ax + bp = 1$, so a has an inverse. Since $|G| = p - 1$, if $x \neq 0$ in $\mathbf{Z}/p\mathbf{Z}$ then $x^{p-1} \equiv 1 \pmod{p}$. Multiplying by x on both sides, we get Fermat's theorem.

Euler: if x is prime to $m > 0$ then $x^{\varphi(m)} \equiv 1 \pmod{m}$. Here, we take $G = (\mathbf{Z}/m\mathbf{Z})^*$, which corresponds to all integers $\mod m$ prime to m. G is a group. So $x^{|G|} \equiv 1 \pmod{m}$ if $x \in G$, that is, x is prime to m. Since $|G| = \varphi(m)$, the result follows.

5. Products

Let's consider groups of order 4. By Lagrange's theorem, a group G of order 4 can have elements only of order 1, 2, or 4. If G has an element g of order 4, then $G = \{1, g, g^2, g^3\}$ is cyclic of order 4.

Therefore, let's assume all elements have order 2 or 1, namely $g^2 = 1$ for all $g \in G$. This implies that G is commutative. Since we have $xyxy = (xy)^2 = 1$ and $x = x^{-1}$, we get $yxy = x$ and then $xy = yx$.

Let's classify all commutative groups G with $g^p = 1$ for all $g \in G$. We write the group operation as addition. The G is a vector space over the field $\mathbf{F}_p$. So G is isomorphic to $\mathbf{F}_p^n$, an n-dimensional vector space, and has order p^n. We call G an **elementary abelian p-group**.

Let's go back to order 4. There are two groups up to isomorphism: $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. We should check that these are distinct, though. $\mathbf{Z}/4\mathbf{Z}$ has 1 element of order 1, 2 of order 4, and 1 of order 2, whereas $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ has 1 element of order 1 and 3 of order 2. The group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is another way of describing the Klein four group V (the symmetries of a rectangle).

The group $\mathbf{Z}/4\mathbf{Z}$ has a subgroup of order 1 and one of order 2. The group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ has three subgroups of order 2 and one of order 1.

Sometimes, it useful to write what are called **exact sequences** of the form

$$0 \to A \to B \to C \to 0.$$

In particular, the above is **exact at B** if the arrows are homomorphisms of groups and the kernel of the map from B to C is the image of the map from A to B. Essentially, this means that A is more-or-less a subgroup of B, B maps onto C, and A is more-or-less the kernel of the map from B to C.

Actually, we have

$$0 \to \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0.$$

The group $\mathbf{Z}/4\mathbf{Z}$ has a homomorphism onto $\mathbf{Z}/2\mathbf{Z}$ and the kernel is a group of order 2. The sequence

$$0 \to \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$$

is exact since the sequence

$$0 \to A \to A \times B \to B \to 0$$

is always exact: the map from $A \times B$ to B is a projection and the map from A to $A \times B$ is the natural inclusion.

The objects A and B in the exact sequence

$$0 \to A \to G \to B \to 0$$

do not determine G.

Any exact sequence of the form

$$0 \to A \to A \times B \to B \to 0$$

is called **split**. You should be careful when assuming that an exact sequence is split.

If G and H are two groups, then we can take the direct product of G and H:

$$G \times H = \{(g, h) : g \in G, h \in H\}.$$

The product $G \times H$ is always a group.

Suppose G has subgroups A, B. Suppose A and B commute and every element in G is of the form ab with $a \in A$ and $b \in B$ uniquely. Then $G \cong A \times B$, since there is a homomorphism $A \times B \to G$ that takes (a, b) to ab, and this homomorphism is bijective.

The group $\mathbf{R}^*$ is isomorphic to $\{\pm 1\} \times \mathbf{R}_{>0}$. This follows rather trivially from the criteria given above.

The group $\mathbf{C}^*$ is isomorphic to $S^1 \times \mathbf{R}_{>0}$, where S^1 is the circle group. We can see how this relates to the polar decomposition of a complex number.

The group $\mathbf{Z}/mn\mathbf{Z}$ is isomorphic to $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ provided m and n are coprime. (Chinese remainder theorem.) There is a homomorphism between these two groups, the kernel of which is the multiples of m and n, and since m and n are coprime, these are the multiples of mn, which correspond to the element 0 in $\mathbf{Z}/mn\mathbf{Z}$. Since the two groups have the same order and the homomorphism is injective, the homomorphism is an isomorphism. So, for instance,

$$\mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

Cayley accidentally wrote that these two groups were not isomorphic[1].

The group $(\mathbf{Z}/mn\mathbf{Z})^*$ is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$ provided m and n are coprime. For example,

$$(\mathbf{Z}/15\mathbf{Z})^* \cong (\mathbf{Z}/5\mathbf{Z})^* \times (\mathbf{Z}/3\mathbf{Z})^*,$$

and since $(\mathbf{Z}/5\mathbf{Z})^*$ is cyclic of order 4 and $(\mathbf{Z}/3\mathbf{Z})^*$ is cyclic of order 2, we also have

$$(\mathbf{Z}/15\mathbf{Z})^* \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

From Euler's theorem, $x^{\varphi(15)} = x^8 \equiv 1 \pmod{15}$ if x is prime to 15. From this decomposition, every element of the group has order dividing 4, so $x^4 \equiv 1 \pmod{15}$ when x is prime to 15.

Consider the group $\mathbf{Q}^*$ under multiplication. Since every rational number can be written as a product of powers of primes uniquely, we have

$$\mathbf{Q}^* \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z} \oplus \cdots = \mathbf{Z}/2\mathbf{Z} \times \bigoplus_{p \text{ prime}} \mathbf{Z}.$$

Let's digress on some notation here. If A, B, C are infinite abelian groups, then we can take their direct sum

$$A \oplus B \oplus C \oplus \cdots = \{(a, b, c, \ldots) : a \in A, b \in B, c \in C, \ldots\}$$

with the constraint that almost all of a, b, c are 0. Allowing for an infinite number of a, b, c to be nonzero gives a different group (the product, not the direct sum). However, finite direct sums are the same as finite products.

[1]See https://www.jstor.org/stable/2369433.

If $r \in \mathbf{Q}^*$, then we can write $r = \pm 2^{n_2} 3^{n_3} 5^{n_5} \cdots$. The $\pm$ corresponds to the group of order 2 and each p^{n_p} corresponds to $\mathbf{Z}$ since

$$\{p^k : k \in \mathbf{Z}\} \cong \mathbf{Z}.$$

So, each copy of $\mathbf{Z}$ in the direct sum corresponds to the powers of a prime.

Now consider an octahedron. Its group of rotations is of order 24, but its group of symmetries has order 48, since we can also consider reflections. This complete group has a subgroup consisting of the 24 rotations and another with order 2 corresponding to reflections, and, in particular, it can be written as the product of these two groups. We can do the same thing with a icosahedron, dodecahedron, and cube. However, we can't do this with a tetrahedron! It does not have an commutative automorphism taking every point to its opposite.

Now, let's consider the group of all roots of unity in $\mathbf{C}$. We get a root of unity for every point whose argument is a rational multiple of a full rotation, and, when we try to draw it, it certainly looks like S^1. However, unlike S^1, this group splits. It splits into a direct sum of R_ps where each R_p corresponds to roots of order p^f. These subgroups commute. Every root of unity can be written uniquely as a product of elements in these groups, which follows from the Chinese remainder theorem.

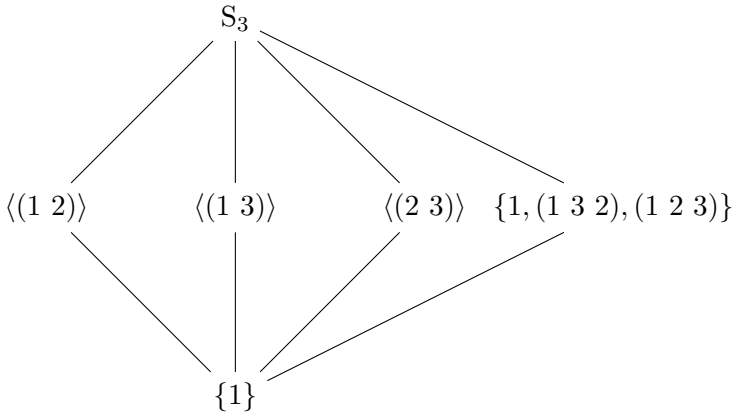
6. Normal subgroups and quotient groups

Remember that S_3 and $\mathbf{Z}/6\mathbf{Z}$ are the only groups of order 6. The group $\mathbf{Z}/6\mathbf{Z}$ has four subgroups. The first two are rather trivial, as they are $\mathbf{Z}/6\mathbf{Z}$ and $\{1\}$. It also has a subgroup isomorphic to $\mathbf{Z}/2\mathbf{Z}$ of the form $\{0, 3\}$ and another isomorphic to $\mathbf{Z}/3\mathbf{Z}$ of the form $\{0, 2, 4\}$.

Recall that

$$S_3 = \{1, (1\ 2), (2\ 3), (3\ 1), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Other than the trivial group and itself, it has a subgroup of order 3 consisting of 1, (1 3 2), and (1 2 3), and three subgroups of order 2. So S_3 has 6 subgroups. Whenever we have a group, we may consider its **lattice of subgroups** to have a better view of the group's subgroup structure. Below is the lattice of subgroups of the group S_3.



These diagrams become much more interesting once we have (non-trivial) inclusions of subgroups.

Suppose H is a subgroup of G. We define the **quotient group** G/H as the group making

$$1 \to H \to G \to G/H \to 1$$

exact. From this, we also have that G/H is the set of left cosets of H.

Can we endow G/H with a well-defined group structure? Consider two left cosets g_1H and g_2H. The sensible thing to do is define $g_1H \times g_2H = g_1g_2H$. But is this well-defined? Suppose $g_3 = g_1h$ for some $h \in H$. We want to show that this implies that $g_3g_2H = g_1g_2H$, that is $g_1hg_2H = g_1g_2H$. We have $g_1hg_2H = g_1g_2(g_2^{-1}hg_2)H$, so the question becomes whether $g_2^{-1}hg_2$ is in H. The following conditions are equivalent:

1. H is the kernel of a map from G to some group X;
2. $gHg^{-1} = H$ for all $g \in G$;
3. $gH = Hg$ for all $g \in G$;
4. left cosets are the same as right cosets;
5. a quotient group G/H exists (as above).

If H satisfies any of these conditions, we call H a **normal subgroup**.

Which subgroups are normal? Clearly, if G is abelian then all subgroups are normal. Take $G = \mathrm{S}_3$. The group S_3 and the trivial group are trivially normal subgroups.

First, recall Theorem 4.1 (Lagrange's theorem). We define the **index of H in G** by

$$[G : H] = |G| \,/\, |H| = \text{number of cosets.}$$

(We have natural one-to-one map from left cosets to right cosets by $gH \mapsto (gH)^{-1} = Hg^{-1}$.)

Now, consider the subgroup $\{1, (1\ 2\ 3), (1\ 3\ 2)\}$ of S_3. It has index 2 in S_3, so it is normal.

Exercise 6.1. Prove that subgroups of index 2 are normal.

The subgroup $\langle (1\ 2) \rangle$ is not normal in S_3. Calculating the cosets explicitly, we find that the set of left cosets is

$$\{\{1, (1\ 2)\}, \{(1\ 2\ 3), (1\ 3)\}, \{(1\ 3\ 2), (2\ 3)\}\}$$

and the set of right cosets is

$$\{\{1, (1\ 2)\}, \{(1\ 2\ 3), (2\ 3)\}, \{(1\ 3\ 2), (1\ 3)\}\}.$$

These are not equal, so the subgroup is not normal.

If H is a subgroup, so is gHg^{-1}, since $(gag^{-1})(gbg^{-1}) = gabg^{-1}$ (so it is closed). We call the subgroup gHg^{-1} the **conjugate** of H by g. G acts on the set of subgroups H by $g(H) = gHg^{-1}$ (by conjugation). Let's figure out what this action looks like for the subgroups of S_3. If a subgroup is normal, then the group acts trivially on it. (Recall the conditions for a normal subgroup.) Also, we calculate that the three subgroups of order 2 form an orbit under conjugation (that is,

$$(1\ 3)^{-1} \langle (1\ 2) \rangle (1\ 3) = \langle (2\ 3) \rangle,$$

etc.) so they are conjugate. Also, if a subgroup is not normal, then all subgroups conjugate to that subgroup are not normal.

Suppose G has a normal subgroup H. Then

$$1 \to H \to G \to G/H \to 1$$

is exact, and H and G/H are usually of lesser order than G.

7. Semidirect products

The group S_3 is not the product of two smaller groups, but it's "quite close" to being one. Suppose $A = \{1, (1\ 2)\}$ and $B = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$. We have that $S_3 = AB$ in the sense that each element in S_3 can be written as a unique product of an element in A and an element in B. So the map $(a, b) \mapsto ab$ is an isomorphism of sets, but not groups. The problem here is that A and B do not commute.

Suppose we try to multiply a_1b_1 by a_2b_2. We find that $(a_1b_1)(a_2b_2) = a_1a_2(a_2^{-1}b_1a_2)b_2$, and $a_2^{-1}b_1a_2 \in B$, so this product is still of the form ab. It is convenient to write conjugation $\alpha^{-1}\beta\alpha = \beta^\alpha$ since this obeys ordinary properties of exponentiation.

We have a subgroup A, a normal subgroup B, and $G = AB$ uniquely. We also have a right action (conjugation) of A on B, which we write b^a with $(b_1b_2)^a = b_1^a b_2^a$ and $b^{a_1a_2} = (b^{a_1})^{a_2}$.

Now suppose we have groups A, B and a right action A on B, and we want to construct a group G such that A is a subgroup, B is a normal subgroup, and the right action is given by conjugation. Take $G = A \times B$ as a set and define $(a_1b_1)(a_2b_2) = (a_1a_2)(b_1^{a_2}b_2)$.

Exercise 7.1. Show that G is associative.

This product is called the **semidirect product** of A and B and written $A \ltimes B$. Again, B is a normal subgroup, A is a subgroup, the action $b \mapsto a^{-1}ba$ in $A \ltimes B$ is the same as the right action of A on B. If we have a left action of A on B instead, we also have a semidirect product, written $B \rtimes A$.

Example 7.2
$S_3 \cong \mathbf{Z}/2\mathbf{Z} \ltimes \mathbf{Z}/3\mathbf{Z}$.

We can use these notions to classify groups G of order 6. Firstly, G has an element g of order 3, since if G has an element of order 6, then G is cyclic, and if not (and G has no elements of order 3), then all non-identity elements are of order 2, which corresponds to $\prod \mathbf{Z}/2\mathbf{Z}$, so G must have an element of order 3. We have $\{1, g, g^2\} \lhd G$ since it is a subgroup of index 2.

Secondly, G has a subgroup of order 2, for if not, then all non-identity elements would have order 3. All elements of order 3 come in pairs, and since there are 5 non-identity elements, there must be 1 element of order 2 (or 6, which we can cube to get an element of order 2).

So G is a semidirect product $A \ltimes B$ where A has order 3 and B has order 2. So $A \cong \mathbf{Z}/3\mathbf{Z}$ and $B \cong \mathbf{Z}/2\mathbf{Z}$. But what is the action of B on A? The only automorphisms of the group

$\mathbf{Z}/3\mathbf{Z}$ are $g \mapsto g$ and $g \mapsto g^{-1}$, so $\mathrm{Aut}(B) \cong \mathbf{Z}/2\mathbf{Z}$. Since there are only two homomorphisms from a group of order 2 to a group of order 2, we have two cases.

The first is that $\mathbf{Z}/2\mathbf{Z}$ acts trivially on $\mathbf{Z}/3\mathbf{Z}$, where we get the direct product $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \cong \mathbf{Z}/6\mathbf{Z}$. The second is that $\mathbf{Z}/2\mathbf{Z}$ acts nontrivially on $\mathbf{Z}/3\mathbf{Z}$. If $\mathbf{Z}/3\mathbf{Z}$ is generated by g and $\mathbf{Z}/2\mathbf{Z}$ is generated by h then we put $g^h = g^{-1}$. We have seen that this group is isomorphic to S_3.

Example 7.3

The **Poincaré group** of relativity is the semidirect product of $\mathbf{R}^{1,3}$ with the Lorentz group.

8. Extensions

Let us start by trying to classify groups G of order 8. The elements g of G must have order 1, 2, 4, or 8. Suppose there are no elements of order 4 or 8. Then all non-identity elements have order 2, so

$$G \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Now, we can assume that G has an element g of order 4. Consider the subgroup $H = \{1, g, g^2, g^3\}$. It is normal in G since it has index 2. We get the exact sequence

$$1 \to H \cong \mathbf{Z}/4\mathbf{Z} \to G \to \mathbf{Z}/2\mathbf{Z} \to 1.$$

Definition 8.1. G is an **extension** of B by A if

$$1 \to A \to G \to B \to 1$$

is exact.

Now, our problem comes down to classifying all possible extensions of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/4\mathbf{Z}$. Working with the notation above, suppose we have an element $a \in A$ with $a^4 = 1$. Pick an element $b \in G$ mapping to an element of order 2 in B. (This does not mean that b has order 2, but rather its image in B has order 2.) Since the group B normalizes A, the conjugation $b^{-1}ab$ must be a generator of A, for a is a generator. So, $b^{-1}ab = a, a^3$ since a, a^3 are the only elements in A of order 4. We also have $b^2 \in A$ since it has image 1 in B. So $b^2 = 1, a, a^2, a^3$. If $b = a^3$, we change a to a^{-1}, so we only consider $b^2 = 1, a, a^2$.

If $b^2 = 1$, then b generates a subgroup of order 2, so we get a semidirect product. If a and b commute, the semidirect product is a product, so we get the group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. If they do not commute, we get the group $\mathbf{Z}/4\mathbf{Z} \ltimes \mathbf{Z}/2\mathbf{Z} \cong \mathrm{D}_8$. If $b^2 = a$, we have $ba = ab$, so the case where a and b do not commute is impossible. When a and b commute, we have $b^8 = 1$, so the group is $\mathbf{Z}/8\mathbf{Z}$. Suppose we have $b^2 = a^2$. If a and b commute and $c = ab$, then $c^2 = 1$ and $c^{-1}ac = a$. So this case is the same as the $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ case. Finally, suppose a and b do not commute. We have $b^4 = 1$ and $a^4 = 1$, and this turns out to be the **quaternion group**, denoted Q_8. The following table shows our results:

	$b^2 = 1$	$b^2 = a$	$b^2 = a^2$
$b^{-1}ab = a$	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$	$\mathbf{Z}/8\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$
$b^{-1}ab = a^{-1}$	$\mathbf{Z}/4\mathbf{Z} \ltimes \mathbf{Z}/2\mathbf{Z}$	impossible	Q_8

Let's confirm the existence of Q_8. We can do this by using a representation of Q_8 in SU(2). Take

$$a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We can check that $a^4 = 1$, $b^4 = 1$, and $b^{-1}ab = a^{-1}$. However, we still need to ensure these elements generate a group of order 8. Now, take

$$c = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \text{and} \quad d = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and $G = \{\pm a, \pm b, \pm c, \pm d\}$ is a group of order 8. It is common to write $a = i$, $b = j$, $c = k$, and $d = 1$, where $i^2 = j^2 = k^2 = ijk = -1$.

9. Quaternions

Recall that $\mathrm{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with the relations $ij = k$, $jk = i$, $ki = j$, and $i^2 = j^2 = k^2 = ijk = -1$. We have the representation $\rho : \mathrm{Q}_8 \hookrightarrow \mathrm{SU}(2)$ where

$$i \mapsto \begin{pmatrix} i & \\ & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, \quad k \mapsto \begin{pmatrix} & i \\ i & \end{pmatrix}, \quad 1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}.$$

We get a ring $\mathbf{H}$ isomorphic to $\mathbf{R}^4$ out of this group by taking

$$\mathbf{H} = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbf{R}\}$$

and defining the multiplication as above. This multiplication is not commutative: $ij = -ji$, $jk = -kj$, $ki = -ik$. This ring is called the **Hamiltonian quaternions**.

The quaternions are a kind of analogue of the complex numbers. We write any complex number $z = a + bi$, where $a, b \in \mathbf{R}$ and $i^2 = -1$. Also, we have complex conjugates $\overline{a + bi} = a - bi$ and the norm $z\overline{z} = a^2 + b^2 \geq 0$, where if $\|z\|$ is the norm of z, $\|z_1 z_2\| = \|z_1\| \, \|z_2\|$.

It's nearly the same in the quaternions. If $z = a + bi + cj + dk$, we have the quaternion conjugate $\overline{z} = a - bi - cj - dk$. We have $z\overline{z} = a^2 + b^2 + c^2 + d^2 \geq 0$. If $\|z\| = z\overline{z}$, then we have $\|z_1 z_2\| = \|z_1\| \, \|z_2\|$.

Exercise 9.1. Prove $\|z_1 z_2\| = \|z_1\| \, \|z_2\|$. (Be careful: $\overline{z_1 z_2} \neq \overline{z_1} \times \overline{z_2}$.)

The complex numbers with norm $1^2 = 1$ form the group S^1. Similarly, the quaternions with norm 1 form the group S^3. The sphere S^n is only a group when $n = 0, 1, 3$.

Quaternions are useful for describing three dimensional rotations. Let

$$\mathbf{R}^3 = \{bi + cj + dk\}.$$

Pick some $v \in \mathbf{R}^3$ and $g \in S^3$. The number gvg^{-1} is in $\mathbf{R}^3$ (is "purely imaginary") and preserves length and parity, so it is a rotation.

The group S^3 is not the group of rotations of three-dimensional space. The sequence

$$1 \to \{\pm 1\} \to S^3 \to \mathrm{SO}_3(\mathbf{R}) \to 1$$

is exact, and, in particular, the homomorphism from S^3 to $\mathrm{SO}_3(\mathbf{R})$ has a nontrivial kernel (of order 2). Since the kernel is of order 2, S^3 is a **double cover** of $\mathrm{SO}_3(\mathbf{R})$. We could get a trivial double cover by taking the product of $\mathrm{SO}_3(\mathbf{R})$ with $\mathbf{Z}/2\mathbf{Z}$, but this is much more interesting.

This is related to the Dirac belt trick, or the soup plate trick[2]. The group S^3 is called the **spin group**. The space of possible wave functions of a particle is not acted on by $\mathrm{SO}_3(\mathbf{R})$ (for fermions, at least), but rather the spin group. (This relates the 1/2 spin of the electron and the spin group being a double cover of $\mathrm{SO}_3(\mathbf{R})$.)

Consider the exact sequence (with the double cover) above. We can take some finite group of rotations in $\mathrm{SO}_3(\mathbf{R})$. (The interesting ones turn out to be the tetrahedral, octahedral, and icosahedral groups.) Taking the inverse image of these groups in the spin group, we get groups of order 24, 48, and 120, which correspond to the **binary tetrahedral**, **octahedral**, and **icosahedral groups**. Each are double covers of the original group. These groups are not a product of $\mathbf{Z}/2\mathbf{Z}$ with the original group. The group S^3 has only one element of order 2.

Identify $\mathbf{R}^4 = a + bi + cj + dk$ and suppose $v \in \mathbf{R}^4$, $g, h \in S^3$. We can map $v \mapsto gvh^{-1}$, which turns out to be an element in $\mathrm{SO}_4(\mathbf{R})$. So

$$1 \to (-1,-1) \to S^3 \times S^3 \to \mathrm{SO}_4(\mathbf{R}) \to 1$$

is exact, and $\mathrm{SO}_4(\mathbf{R}) \cong (S^3 \times S^3)/(\mathbf{Z}/2\mathbf{Z})$.

10. Burnside's lemma

Consider the following problem: how many ways can you arrange 8 rooks on a chessboard with one rook in each row and column? Clearly, there are 8! ways. But, what about up to symmetry? Édouard Lucas was the first to solve this[3].

Consider the group D_8 acting on the set of all possible configurations, which has size 8!. How many orbits are there? Burnside's lemma is useful here.

Lemma 10.1 (Burnside)

Suppose a group G acts on a set S. Then the number of orbits is the average number of fixed points:

$$\frac{1}{|G|}\sum S^g$$

where S^g is the number of elements of S fixed by g.

Cauchy and Frobenius, for instance, knew about Burnside's lemma before Burnside.

Proof. We look at the number of pairs (g, s) with $gs = s$ for $g \in G$ and $s \in S$. We can count this by summing over the elements in G, looking at $\sum_g S^g$. We can also count by

[2] See https://en.wikipedia.org/wiki/Plate_trick or vol. 3 of Feynman's lectures.

[3] *Théorie des nombres*, vol. 1, p. 222.

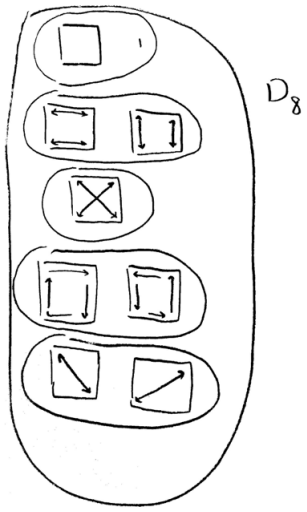


FIGURE 2. The elements of D_8.

summing over the elements in S, considering $\sum_s |G_s|$ where G_s is the subgroup fixing s. The order of G_s is the order of G divided by the size of the orbit of s. We have

$$\begin{aligned}\sum_s |G_s| &= \sum_{\text{orbits}} |\text{orbit}| \frac{|G|}{|\text{orbit}|} \\ &= \sum_{\text{orbits}} |G| \\ &= |G| \cdot \#\text{orbits}.\end{aligned}$$

The result follows. □

Refer to figure 2.

Definition 10.2. The elements a and b are **conjugate** if $a = gbg^{-1}$ for some $g \in G$. This is an equivalence relation where the equivalence classes are called **conjugacy classes**.

You'll notice that there are three pairs of elements that have the same number of fixed points. So we split D_8 into conjugacy classes, and now we can solve our problem.

The conjugacy class corresponding to the identity has 1 element. This fixes 8! elements. The conjugacy class corresponding to horizontal reflections has 2 elements, and it fixes 0 elements. The conjugacy class corresponding to one reflection along each diagonal has 1 element, and it fixes 8!! elements. The conjugacy class corresponding to a rotation has 2 elements and fixes 6×2 elements. The conjugacy class corresponding to a reflection along one diagonal has 2 elements. This one's harder to work out, though. Write C_n for the number of arrangements on an $n \times n$ board. Then

$$C_n = C_{n-1} + (n-1)C_{n-2}.$$

(You should convince yourself of this.) Since $C_0 = C_1 = 1$, we find that $C_8 = 764$. So the last conjugacy class fixes 764 points. So the answer to our problem is

$$(1/8)(8! + 2 \times 0 + 8!! + 2 \times 6 \times 2 + 764 \times 2) = 5282.$$

11. Groups of prime power order

We want to classify groups G of order 9. First, we suppose G is abelian. Now suppose G has an element of order 9. Then G is cyclic isomorphic to $\mathbf{Z}/9\mathbf{Z}$. If G has no element of order 9, then every non-identity element is of order 3, so if we write G additively, G is a vector space over the field $\mathbf{F}_3$. So $G \cong \mathbf{F}_3^2 \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

Now suppose $|G| = p^2$. We want to show that G is abelian, so it is isomorphic to either $\mathbf{Z}/p^2\mathbf{Z}$ or $(\mathbf{Z}/p\mathbf{Z})^2$.

Definition 11.1. The **centre** of a group G is the set of elements in G that commute with every other element in G:

$$\mathrm{Z}(G) = \{g \in G : gg' = g'g,\ g' \in G\}.$$

Proposition 11.2
Every group of order p^f has nontrivial centre.

Proof. Consider the adjoint action of G on G. The orbits here are conjugacy classes. The centre is the set of orbits of size 1. All orbits have size $|G| / |G_s| = p^k$ since G has order p^f. The order of G is the number of orbits of size 1 plus the sum of orbits of size greater than 1. Since $|G|$ is divisible by p, and the sum over all orbits of size greater than 1 is divisible by p since each term is a power of p, the number of orbits of size 1 is divisible by p, and so is the order of the centre. □

Proposition 11.3
If $G/\mathrm{Z}(G)$ is cyclic, then $G = \mathrm{Z}(G)$.

Proof. Exercise. □

Now, take $|G| = p^2$. The order of $\mathrm{Z}(G)$ divides $|G|$, so the centre of G has order 1, p, or p^2. It cannot have order 1 by Proposition 11.2. It cannot have order p by Proposition 11.3. So the centre of G must have order p^2. So $\mathrm{Z}(G) = G$.

So any group of order p^2 is isomorphic to $\mathbf{Z}/p^2\mathbf{Z}$ or $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

Definition 11.4. A group G is **nilpotent** if we can kill the group by repeatedly killing the centre.

Corollary 11.5
All p-groups are nilpotent.

12. Cauchy's theorem

Let's try to classify groups of order 10, or more generally, groups of order $2p$. Cauchy's theorem will help us.

Theorem 12.1 (Cauchy)
If p divides the order of a group G, then G has an element of order p.

Proof. Suppose p divides the order of G, and assume that all smaller groups with p dividing the order have an element of order p. We want to prove that G has an element of order p.

When G is abelian, pick $g \in G$ of prime order q. If $q = p$, we are done. If not, we look at $G/\langle g \rangle$. By induction, there is some $h \in G/\langle g \rangle$ with order p since $G/\langle g \rangle$ has order divisible by p and its order is smaller than $|G|$. Lift h to some $a \in G$. Then a has order a multiple of p, since its image in $G/\langle g \rangle$ has order p. In particular, a has order p or pq. If it has order p, we are done, and if not, then a^q has order p.

Suppose G is not abelian. We can assume that every proper subgroup has order prime to p. So every proper subgroup has index divisible by p. We have

$$\begin{aligned} |G| &= |\mathrm{Z}(G)| + \sum_{C, |C|>1} |C| \\ &= |\mathrm{Z}(G)| + \sum_{C, |C|>1} |G| / |G_s| \end{aligned}$$

where G_s fixes some element of the conjugacy class. Clearly, $|G_s| < |G|$, and since $|G|$ is divisible by p and the sum is divisible by p (since every proper subgroup has index divisible by p), the order of the centre must be divisible by p. The centre of G is abelian, so the centre has an element of order p. □

Proof. Consider the equation

$$g_1 g_2 \cdots g_p = 1.$$

There are $|G|^{p-1}$ solutions to it. And $|G|^{p-1}$ is divisible by p. We have p solutions to the equation unless all g_i are the same. Notice that p must be prime here. So $|G|^{p-1}$ must be something divisible by p plus the number of solutions to $g^p = 1$. So the number of solutions to $g^p = 1$ is divisible by p. So if p divides $|G|$, then the number of solutions to $g^p = 1$ is a multiple of p. One solution is $g = 1$, and all others have order p. So the number of elements of order p is congruent to $-1 \pmod p$. If g is of order p then it generates a group of order p, which has $p - 1$ elements of order p. So the number of subgroups of order p is something $-1 \pmod p$ divided by $p - 1$, and since $p - 1 \equiv -1 \pmod p$, the number of subgroups of order p is $1 \pmod p$. So there must be elements of order p. □

Suppose $|G| = 2p$. Then we pick $a \in G$ of order p and $b \in G$ of order 2. Then $A = \langle a \rangle$ is of order p and has index 2, so is normal in G. So G is a semidirect product $A \ltimes B$, where $A \cong \mathbf{Z}/p\mathbf{Z}$ and $B \cong \mathbf{Z}/2\mathbf{Z}$. Now, we have to figure out all ways that a group of order 2 can act on a cyclic group of order p. The group $\mathbf{Z}/p\mathbf{Z}$ has automorphism group $(\mathbf{Z}/p\mathbf{Z})^*$, which has 2 elements of order 2. The group $\mathbf{Z}/p\mathbf{Z}$ is a field, so $x^2 - 1 \equiv 0 \pmod{p}$ has at most 2 roots (namely ± 1 except when $p = 2$). So there are two automorphisms of order 2 of $\mathbf{Z}/p\mathbf{Z}$ (except when $p = 2$).

So $A \cong \mathbf{Z}/p\mathbf{Z}$ is acted on by $B \cong \mathbf{Z}/2\mathbf{Z}$. This action can be the trivial action, where $bab^{-1} = a$, which implies that we have $A \times B \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \cong \mathbf{Z}/2p\mathbf{Z}$. This action may also be nontrivial, where $bab^{-1} = a^{-1}$, which gives the group D_{2p}.

So: a group of order $2p$ is either $\mathbf{Z}/2p\mathbf{Z}$ or D_{2p} up to isomorphism.

13. Dihedral groups

Definition 13.1. The **dihedral group** of order $2n$, denoted D_{2n}, is the group of symmetries of a regular n-gon.

The group, D_6, corresponds to the symmetries of an equilateral triangle. In fact, $\mathrm{D}_6 \cong \mathrm{S}_3$ (that is, the permutations of the vertices). The group D_8 is the group of symmetries of a square, D_{10} the group of symemtries of a pentagon, D_{12} the symmetries of a hexagon, etc.

The group D_{2n} is generated by two elements a, b where $a^n = 1$, $b^2 = 1$, and $bab^{-1} = a^{-1}$. The element a corresponds to a rotation and b to a reflection.

Let's consider the group D_4. We know that D_4 is generated by a, b with $a^2 = 1$, $b^2 = 1$, and $bab^{-1} = a^{-1} = a$. So $\mathrm{D}_4 \cong (\mathbf{Z}/2\mathbf{Z})^2$. We also have $\mathrm{D}_2 \cong \mathbf{Z}/2\mathbf{Z}$.

Let's explore the conjugacy classes of dihedral groups. We'll start by considering D_{2n} with n even, so let's consider D_{12}. There are three reflections going through vertices and three reflections going through sides. We also have the identity rotation, two rotations by 1/6 of a revolution, two rotations by 1/3 of a revolution, and one more rotation by 180°. In particular, we have three conjugacy classes of involutions: the 180° rotation and the two reflections. The rotation by 180° is also in the centre, so the centre has order 2. Something similar happens for D_{2n} with n even: we get three classes of involutions, one of which is an element in the centre, and pairs of rotations.

Now let's consider D_{2n} when n is odd, for instance, D_{10}. We have 5 reflections of order 2. These are all of the reflections of the pentagon, and they are all in the same conjugacy class. We also have an identity rotation, a pair of rotations going 1/5 of a revolution of order 5, and another pair going 2/5 of a revolution of order 5. None of these elements are in the centre (other than the identity), so the centre is trivial. We see the differences between n even and n odd: the number of involutions, the centre, etc. (not D_2, though).

We can inscribe an equilateral triangle in a regular hexagon, and we see that symmetries of the triangle are contained in the symmetries of a hexagon. So $\mathrm{D}_6 \subset \mathrm{D}_{12}$. Also, $\{\pm 1\} \subset \mathrm{D}_{12}$, and, in fact,

$$\mathrm{D}_{12} \cong \mathbf{Z}/2\mathbf{Z} \times \mathrm{D}_6 \,.$$

All groups D_{4n} with n odd split like this. For instance, $D_{20} \cong \mathbf{Z}/2\mathbf{Z} \times D_{10}$. But why doesn't this work for even n? For instance, if we have the group D_{16}, we find (by looking at the octagon and inscribed squares) that $\{\pm 1\} \subset D_8$.

Proposition 13.2

A group is a dihedral group if and only if it is generated by 2 involutions.

Proof. Nope. Sorry. But Dr. Borcherds's demonstration with turtles and mirrors is cool. □

Anyway, suppose a, b are the generators, so $a^2 = 1$ and $b^2 = 1$. Write $c = ab$ and notice that $aca^{-1} = ba = c^{-1}$. If n the smallest positive integer such that $c^n = 1$, then we get the conditions for the dihedral group D_{2n} (roughly).

If we don't have the condition $(ab)^n = 1$, we get the infinite dihedral group D_∞, which can (sort of) be thought of as the group of symmetries of a straight line.

Proposition 13.3

Suppose G is finite and suppose a, b have order 2 in G. Then either a and b are conjugate or a and b both commute with another involution.

Proof. Pick the smallest n with $(ab)^n = 1$. So a, b generate the dihedral group D_{2n}. If n is odd, a, b are conjugate, and if n is even, then $(ab)^{n/2}$ has order 2 and commutes with a, b. □

14. Sylow theorems

If G is a finite group then any subgroup $H \subset G$ has order dividing G. Suppose d divides G. Does that mean G has a subgroup of order d?

Not in general: if G is the set of rotations of the tetrahedron, $|G| = 12$ but G has no subgroup of order 6. However, the statement is true under certain conditions that the Sylow theorems describe.

Theorem 14.1 (Sylow)

Suppose p^n is the largest power of p dividing $|G|$. Then

1. G has subgroups of order p^n,
2. the number of these subgroups is $1 \pmod p$ and divides $|G|$,
3. all of these subgroups are conjugate (isomorphic),
4. and any subgroup of order p^f is in one of these subgroups.

These subgroups are called **Sylow p-subgroups**.

Proof. (Existence.) Suppose G has a proper subgroup H of index coprime to p. Then p^n divides $|H|$, and $|H| < |G|$, so H has a subgroup of order p^n, so G does.

Suppose G does not have a proper subgroup of index coprime to p. Then all proper subgroups have index divisible by p. The order of G is the order of the centre of G plus the sum over all conjugacy classes of size greater than 1 of the size of the conjugacy class. The size of the conjugacy class is the index of some proper subgroup of G, so the entire sum is divisible by p. Since $|G|$ is also divisible by p, the centre of G has order divisible by p. So G has an element of order p in the centre.

Look at $G/\langle g\rangle$ where $g^p = 1$, $g \neq 1$, and g is in the centre. Pick a Sylow p-subgroup S of $G/\langle g\rangle$, so $|S| = p^{n-1}$. We have the map $G \to G/\langle g\rangle$, and we consider the inverse image S' of S under this map. The inverse image S' has order p^n, so is a Sylow p-subgroup of G. □

Proof. (The number of Sylow p-subgroups is $1 \pmod p$ and conjugacy.) Suppose S and T are Sylow p-subgroups with $S \neq T$. Then S cannot normalize T, that is, we cannot have $sts^{-1} \in T$ for all $s \in S$ and $t \in T$. This is because if S normalizes T, then ST is a subgroup, but $|ST| = p^k$ for some $k > n$, and this is not possible.

We consider the orbits of S on the set of Sylow p-subgroups. There is 1 orbit with 1 element, S, and all other orbits have p^k elements for $k > 1$, since the number of orbits is the order of S divided by the order of the subgroup of S normalizing T, which is strictly less than the order of S. So, the number of conjugates of S is $1 \pmod p$.

Suppose S and T are not conjugate. The number of conjugates of S is $1 \pmod p$ and also $0 \pmod p$. Contradiction. So S must be conjugate to T, and all Sylow p subgroups are conjugate and the number of them is $1 \pmod p$. □

Definition 14.2. The **normalizer** of a subgroup $H \subset G$ is the set

$$\mathrm{N}_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Proof. (Any group of order p^f is in a Sylow p-subgroup.) Pick a maximal subgroup X of order p^f not contained in a Sylow p-subgroup. The normalizer of X has index divisible by p, so the number of conjugates of X is divisible by p. But (by the argument above) the number of conjugates is $1 \pmod p$. Contradiction. So any group of order p^f is contained in a Sylow p-subgroup. □

Example 14.3

Suppose $G = \mathrm{D}_4$. Then G has subgroups isomorphic to $\mathbf{Z}/4\mathbf{Z}$ and subgroups isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$. These are not isomorphic, so they are not conjugate. The number p^n needs to be the largest power of p dividing $|G|$ for Sylow's theorems to work.

15. Groups of order 12

What groups of order 12 can we think of? We have

1. $\mathbf{Z}/12\mathbf{Z}$
2. $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$
3. $\mathbf{Z}/3\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^2$
4. D_{12}

5. $S_3 \times \mathbf{Z}/2\mathbf{Z}$
6. Binary cyclic group
7. Binary dihedral group of order 12
8. $\mathbf{Z}/3\mathbf{Z} \ltimes (\mathbf{Z}/2\mathbf{Z})^2$
9. $\mathbf{Z}/3\mathbf{Z} \ltimes \mathbf{Z}/4\mathbf{Z}$
10. Rotations of a tetrahedron
11. A_4
12. $(\mathbf{Z}/2\mathbf{Z})^2 \ltimes \mathbf{Z}/3\mathbf{Z}$

Definition 15.1. The **alternating group** on n letters A_n is a subgroup of S_n of index two corresponding to the even permutations of S_n.

There are only 5 groups of order 12, though. We have the following isomorphisms.

1. $\mathbf{Z}/12\mathbf{Z} \cong$ binary cyclic group
2. $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \cong \mathbf{Z}/3\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^2$
3. $D_{12} \cong S_3 \times \mathbf{Z}/2\mathbf{Z} \cong \mathbf{Z}/3\mathbf{Z} \ltimes (\mathbf{Z}/2\mathbf{Z})^2$
4. binary dihedral group $\cong \mathbf{Z}/3\mathbf{Z} \ltimes \mathbf{Z}/4\mathbf{Z}$
5. rotations of a tetrahedron $\cong A_4 \cong (\mathbf{Z}/2\mathbf{Z})^2 \ltimes \mathbf{Z}/3\mathbf{Z}$.

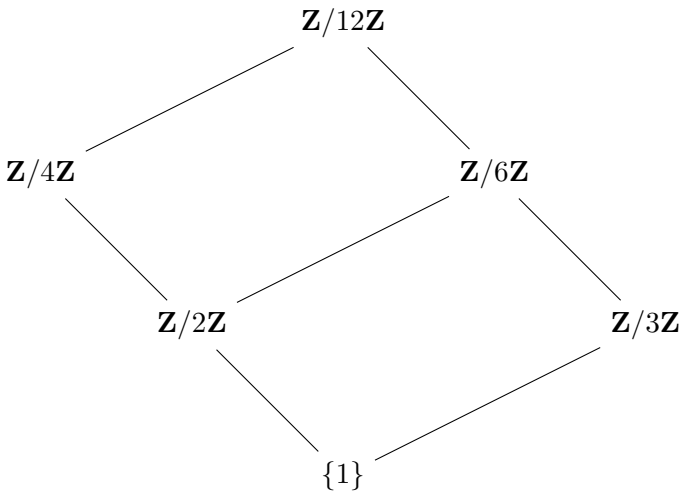
We want to show that any group of order 12 is isomorphic to one of these groups. By Theorem 14.1, a group G of order 12 has Sylow p-subgroups of orders 3 and 4, and the number of 3-Sylow subgroups is either 1 or 4, and the number of 2-Sylow subgroups is either 1 or 3.

Assume G has 1 Sylow 3-subgroup. Then it must be normal (if not, there would be another Sylow 3-subgroup conjugate to it), so G is a semidirect product of a 3-Sylow subgroup with a 2-Sylow subgroup, and there are 4 cases, since the Sylow 2-subgroup is either $\mathbf{Z}/4\mathbf{Z}$ or $(\mathbf{Z}/2\mathbf{Z})^2$ and the Sylow 3-subgroup is $\mathbf{Z}/3\mathbf{Z}$, which only has 2 automorphisms. So an action of a Sylow 2-subgroup on a Sylow 3-subgroup must be a homomorphism from that Sylow 2-subgroup to a group of order 2, and this homomorphism is either trivial or nontrivial.

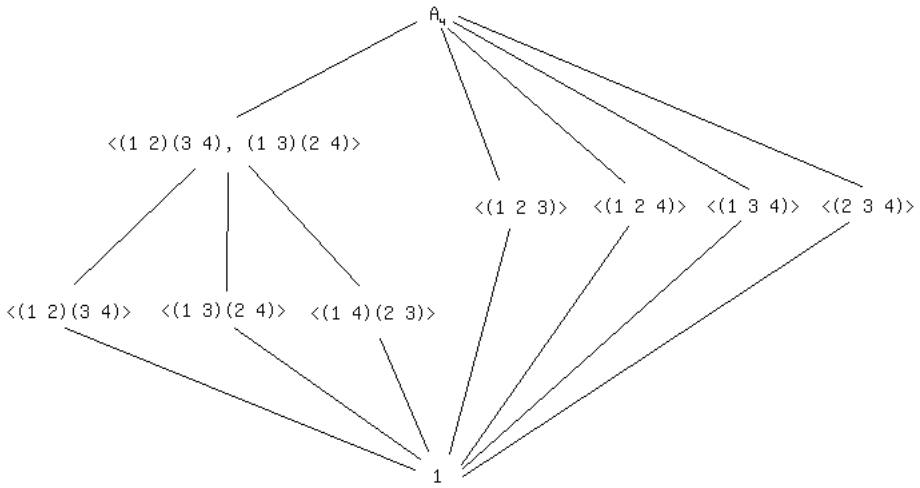
If the Sylow 2-subgroup is $\mathbf{Z}/4\mathbf{Z}$, then we have 2 cases. If the action on $\mathbf{Z}/3\mathbf{Z}$ is trivial then we get $\mathbf{Z}/12\mathbf{Z}$, and if it is nontrivial we get a semidirect product $\mathbf{Z}/3\mathbf{Z} \ltimes \mathbf{Z}/4\mathbf{Z}$. If the Sylow 2-subgroup is $(\mathbf{Z}/2\mathbf{Z})^2$, we also have 2 cases. If the action on $\mathbf{Z}/3\mathbf{Z}$ is trivial then we get $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \cong \mathbf{Z}/3\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^2$, and if it is nontrivial then we get $\mathbf{Z}/2\mathbf{Z} \times S_3 \cong D_{12}$.

Now suppose the subgroup of order 3 is not normal. Then the number of conjugates is 4. So we have 4 subgroups S_1, S_2, S_3, S_4 of order 3. So there are 2 elements of order 3 in each subgroup, and they are distinct (since the subgroups are conjugate), so there are 4 elements of G not of order 3. So, they must form the Sylow 2-subgroup. So it must be normal, and the group is the semidirect product of a group of order 4 by a group of order 3, that is $\mathbf{Z}/4\mathbf{Z} \ltimes \mathbf{Z}/3\mathbf{Z}$ or $(\mathbf{Z}/2\mathbf{Z})^2 \ltimes \mathbf{Z}/3\mathbf{Z}$. But the first case is not possible, since the group of order 4 has no automorphisms of order 3, so the only action is trivial, in which case there would only be 1 subgroup of order 3, which contradicts our assumption. So we get one group $(\mathbf{Z}/2\mathbf{Z})^2 \ltimes \mathbf{Z}/3\mathbf{Z}$.

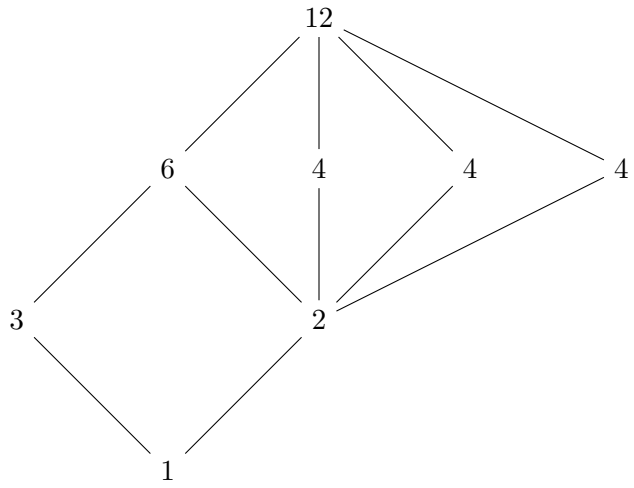
Let's look at the subgroups of some of these groups. For the group $\mathbf{Z}/12\mathbf{Z}$, we have the following lattice of subgroups.



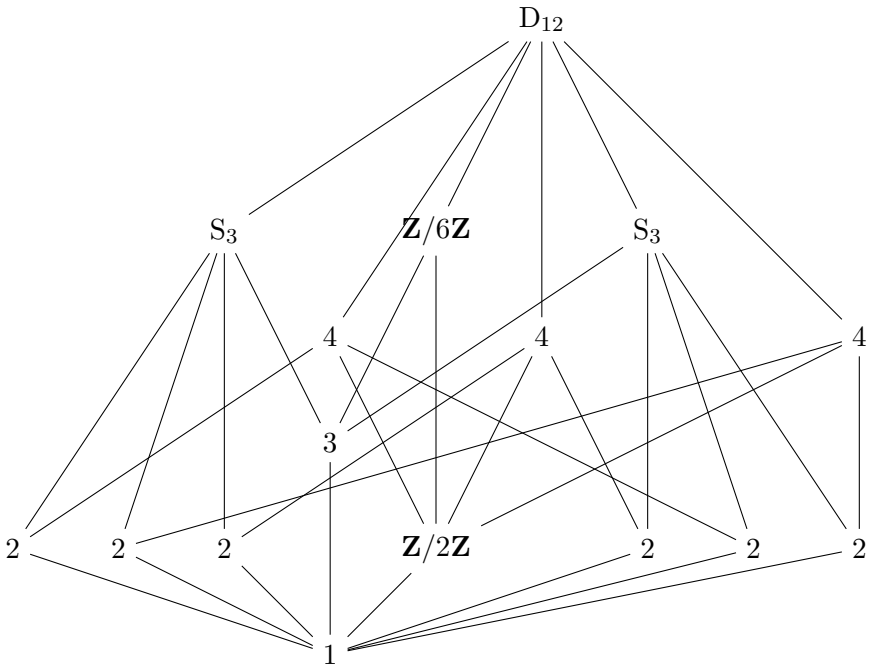
The group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ is also abelian, so its lattice of subgroups is also easy to determine. However, there's no way I'm typesetting that. For A_4, we have the following lattice of subgroups.



The binary dihedral group has a lattice of subgroups like the one below (or on the next page), where the numbers correspond to the order of the subgroup.



Lastly, the group D_{12} has the following lattice of subgroups.



16. Automorphisms of cyclic groups

Definition 16.1. An **automorphism** is an isomorphism from a group G to itself. The set of all automorphisms forms a group that is denoted $\mathrm{Aut}(G)$.

The only group of order 13 is $\mathbf{Z}/13\mathbf{Z}$, and the only groups of order 14 are $\mathbf{Z}/14\mathbf{Z}$ and D_{14}. To classify the groups of order 15, we will consider groups G of order pq where $p < q$.

By Theorem 12.1, G has subgroups of order p and q. The number of subgroups of order q is 1 (mod q) and divides pq, so this number must divide p. Since $p < q$, the number of subgroups of order q is 1, and this subgroup is normal in G. So G is a semidirect product $\mathbf{Z}/q\mathbf{Z} \ltimes \mathbf{Z}/p\mathbf{Z}$. Determining how $\mathbf{Z}/p\mathbf{Z}$ can act on $\mathbf{Z}/q\mathbf{Z}$ will allow us to find all groups of order pq.

An action of $\mathbf{Z}/p\mathbf{Z}$ on the group $\mathbf{Z}/q\mathbf{Z}$ is a homomorphism from $\mathbf{Z}/p\mathbf{Z}$ to $\mathrm{Aut}(\mathbf{Z}/q\mathbf{Z})$. What are the automorphisms of $\mathbf{Z}/q\mathbf{Z}$?

Well, what are the automorphisms of $\mathbf{Z}/n\mathbf{Z}$? The homomorphisms given by $1 \mapsto g \in \mathbf{Z}/n\mathbf{Z}$ are automorphisms if g is invertible in $(\mathbf{Z}/n\mathbf{Z})^*$, that is, the multiplicative group of elements prime to n or the units in the ring $\mathbf{Z}/n\mathbf{Z}$.

Let's look at the first few cases.

1. $(\mathbf{Z}/n\mathbf{Z})^* = \{1\} \cong \mathbf{Z}/1\mathbf{Z}$
2. $(\mathbf{Z}/n\mathbf{Z})^* = \{1\} \cong \mathbf{Z}/1\mathbf{Z}$
3. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 2\} \cong \mathbf{Z}/2\mathbf{Z}$ where 2 is a generator
4. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 3\} \cong \mathbf{Z}/2\mathbf{Z}$ where 3 is a generator
5. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 2, 3, 4\} \cong \mathbf{Z}/4\mathbf{Z}$ where 2 or 3 are generators
6. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 5\} \cong \mathbf{Z}/2\mathbf{Z}$ where 5 is a generator
7. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 2, 3, 4, 5, 6\} \cong \mathbf{Z}/6\mathbf{Z}$ where 3 and 5 are generators
8. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 3, 5, 7\}$ is not cyclic
9. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 2, 4, 5, 7, 8\} \cong \mathbf{Z}/6\mathbf{Z}$
10. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 3, 7, 9\} \cong \mathbf{Z}/4\mathbf{Z}$ where 3 and 7 are generators
11. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \cong \mathbf{Z}/10\mathbf{Z}$ where 2 is a generator
12. $(\mathbf{Z}/n\mathbf{Z})^* = \{1, 5, 7, 11\}$ is not cyclic

Proposition 16.2

If p is prime then $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic of order $p - 1$.

The ring $\mathbf{Z}/p\mathbf{Z}$ is a field. A polynomial of degree n over a field has at most n roots. So $(\mathbf{Z}/p\mathbf{Z})^*$ has at most n elements with $x^n = 1$. Also, the group $(\mathbf{Z}/p\mathbf{Z})^*$ has at most $\varphi(n)$ elements of order n. Also,

$$\sum_{d|n} \varphi(d) = n.$$

When $n = 12$, we have $\mathbf{Z}/n\mathbf{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, and we want will determine the order of each element. 1 is the only element of order 1, 6 is the only element of order 2, the elements of order 3 are 4 and 8, 3 and 9 are the elements of order 4, 2 and 10 are the elements of order 6, and the elements of order 12 are 1, 5, 7, and 11. The number of elements of order 2 is $\varphi(2)$, the number of elements of order 3 is $\varphi(3)$, and so on.

Why? Let's consider the elements of order 4, which are 3 and 9. Now, adding 0 and 6 into the mix, we get $\{0, 3, 6, 9\} = 3(\mathbf{Z}/4\mathbf{Z})$. The elements of order 4 in $\mathbf{Z}/12\mathbf{Z}$ are just the elements of order 4 in $3(\mathbf{Z}/4\mathbf{Z})$. Since $3(\mathbf{Z}/4\mathbf{Z})$ has $\varphi(4)$ elements, so does $\mathbf{Z}/12\mathbf{Z}$. So,

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12.$$

Convince yourself that this works for all other n.

The group $G = (\mathbf{Z}/p\mathbf{Z})^*$ is abelian and has at most $\varphi(n)$ elements of order n. For all n dividing $|G|$, G has at most $\varphi(n)$ elements of order n. Also, $\sum_{n \text{ dividing } |G|} \varphi(n) = |G|$. So G has $\varphi(n)$ elements of order n, and G has some elements with order $|G|$. Therefore G is cyclic, and a generator of this group is sometimes called a **primitive root**.

Okay. Back to classifying groups of order pq. We know that a group G of order pq is the semidirect product $\mathbf{Z}/q\mathbf{Z} \ltimes \mathbf{Z}/p\mathbf{Z}$. We want to find out all ways $\mathbf{Z}/p\mathbf{Z}$ can act on $\mathbf{Z}/q\mathbf{Z}$. The group of automorphisms of $\mathbf{Z}/q\mathbf{Z}$ is $(\mathbf{Z}/q\mathbf{Z})^* \cong \mathbf{Z}/(q-1)\mathbf{Z}$, so we want to find maps from $\mathbf{Z}/p\mathbf{Z}$ to $\mathbf{Z}/(q-1)\mathbf{Z}$.

There are no homomorphisms other than 0 unless p divides $q-1$, and if it does, then we get some homomorphisms that are all sort of equivalent under automorphisms of $\mathbf{Z}/p\mathbf{Z}$. So we have a nontrivial semidirect product $\mathbf{Z}/q\mathbf{Z} \ltimes \mathbf{Z}/p\mathbf{Z}$ unique up to isomorphism.

In summary, there is one group up to isomorphism of order pq with $p < q$ if p does not divide $q-1$ and two groups up to isomorphism if p divides $q-1$. So, if $|G| = 15$, then $G \cong \mathbf{Z}/15\mathbf{Z}$. We can see that if $p = 2$, then we get two groups that we know are isomorphic to either $\mathbf{Z}/2q\mathbf{Z}$ or D_{2q}.

Let's discuss the structure of the group $(\mathbf{Z}/n\mathbf{Z})^*$ for n composite. We proceed for the remainder of this section without proof, so it is a good idea to prove everything that is not transpicuous to you. (And that's always a good idea, Jack.) If $n = p_1^{a_1} p_2^{a_2} \cdots$ then

$$(\mathbf{Z}/n\mathbf{Z})^* \cong \prod_i (\mathbf{Z}/p_i^{a_i}\mathbf{Z})^*.$$

So, we assume n is a prime power. The group $(\mathbf{Z}/p^f\mathbf{Z})^*$ is cyclic of order $\varphi(p^f) = p^{f-1}(p-1)$ unless $p = 2$, when

$$(\mathbf{Z}/p^f\mathbf{Z})^* \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{f-2}\mathbf{Z}$$

where the first group is generated by ± 1 and the second is the powers of 5. When $p \neq 2$, we have

$$(\mathbf{Z}/p^f\mathbf{Z})^* \cong \mathbf{Z}/p^{f-1}\mathbf{Z} \times \mathbf{Z}/(p-1)\mathbf{Z},$$

where the first group is generated by $p+1$.

Why do things go wrong when $p = 2$? We want to show that $1+p$ has order p^{f-1} in $(\mathbf{Z}/p^f\mathbf{Z})^*$, and you start by showing that $(1+p)^{p^{f-2}} \neq 1$ in $(\mathbf{Z}/p^f\mathbf{Z})^*$. This is a good exercise.

Exercise 16.3. Suppose $p \neq 2$ is prime. Show that

$$(\mathbf{Z}/p^f\mathbf{Z})^* \cong (\mathbf{Z}/p^{f-1}\mathbf{Z}) \times (\mathbf{Z}/(p-1)\mathbf{Z}).$$

But it fails when $p = 2$. We have

$$\begin{aligned}(1+p)^{p^{f-2}} &= 1 + p^{f-2}p + \binom{p^{f-2}}{2}p^2 + \binom{p^{f-2}}{3}p^3 + \cdots \\ &= 1 + p^{f-1} + \binom{p^{f-2}}{2}p^2 + \cdots\end{aligned}$$

When $p \neq 2$, the terms after p^{f-1} are divisible by p^f, so that whole sum is not $1 \pmod{p^f}$. However, when $p = 2$, not all of these terms are divisible by p (the third term), so we can't guarantee that the sum is not $1 \pmod{p^f}$.

Example 16.4

We have

$$(\mathbf{Z}/1000000\mathbf{Z})^* \cong (\mathbf{Z}/2^6\mathbf{Z})^* \times (\mathbf{Z}/5^6\mathbf{Z})^*$$

by the Chinese remainder theorem, so

$$(\mathbf{Z}/1000000\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2^4\mathbf{Z}) \times (\mathbf{Z}/5^5\mathbf{Z}) \times (\mathbf{Z}/2^2\mathbf{Z}).$$

17. Finite abelian groups

Let's start with classifying abelian groups of order 16. We have $\mathbf{Z}/16\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

When considering abelian groups we have seen previously, we notice they have been products of cyclic groups. It's not true that every abelian group can be written as the product of cyclic groups; for instance, $\mathbf{Q}$ under addition is not a product of cyclic groups.

Theorem 17.1

Every finitely generated abelian group G is a direct sum of groups $\mathbf{Z}/p^f\mathbf{Z}$ and $\mathbf{Z}$.

More generally, any finitely generated module over a Euclidean domain R is a sum of cyclic modules R/aR.

Proof. Suppose $g_1, \cdots, g_k$ are generators with enough relations

$$n_{11}g_1 + \cdots + n_{1k}g_k = 0$$
$$n_{21}g_1 + \cdots + n_{2k}g_k = 0 \quad \text{etc.}$$

to specify the group G, which we write as a matrix. What can we do to this matrix without changing the group? We can add a multiple of one column to another, since if g and h are generators, then we can change these to $g + nh$ and h for an integer n. We can also add a multiple of a row to another, since if R_1 and R_2 are relations, then R_1, $R_2 + nR_1$ are equivalent relations.

We perform these operations to minimize n_{11} in absolute value, and then subtract multiples of the first row and column from the others to make all entries $n_{12}, n_{13}, \ldots, n_{21}, n_{31}, \ldots$ equal to 0. We can do this because n_{12} must be a multiple of n_{11}. We repeat this process on the resulting submatrix until the matrix of relations is diagonal.

We conclude that the group has generators $g_1, \ldots, g_k$ with relations $n_{ii}g_i = 0$, so the group is isomorphic to a product of cyclic groups of order n_{ii} that decompose into cyclic groups of prime power order. If $n_{ii} = 0$, then $\mathbf{Z}/n_{ii}\mathbf{Z} \cong \mathbf{Z}$. □

When are two finite abelian groups isomorphic? Suppose

$$G \cong \mathbf{Z}/p_1^{n_1}\mathbf{Z} \times \mathbf{Z}/p_2^{n_2}\mathbf{Z} \times \cdots .$$

Do the p_i, n_i determine the group (up to reordering)? (It turns out they do.)

How many abelian groups are there of order p^f? If we write $f = \sum_i \alpha_i$ with $\alpha_1 \geq \alpha_2 \geq \alpha_3 \geq \cdots > 0$, then we get a group

$$\mathbf{Z}/p^{\alpha_1}\mathbf{Z} \times \mathbf{Z}/p^{\alpha_2}\mathbf{Z} \times \mathbf{Z}/p^{\alpha_3}\mathbf{Z} \times \cdots .$$

So the number of groups is the number of partitions of f. (Partitions are super cool.)

There is a close correspondence between Theorem 17.1 and the following theorem.

Theorem 17.2

Every matrix over the complex numbers has Jordan normal form.

How are they related? Theorem 17.1 works for modules over $\mathbf{Z}$, and Theorem 17.2 works for modules over $\mathbf{C}[x]$. A **module** is a vector space where the scalars form a ring, not necessarily a field. It is a vector space with a linear transformation (which is the action of x). Finite abelian groups are sums of cyclic groups, and the corresponding theorem for modules over polynomial rings says that if $p = (x - \alpha)$ is an irreducible polynomial then $\mathbf{C}[x]/p^f\mathbf{C}[x]$ (where $(x-\alpha)^f = 1$) gives a basis

$$\begin{pmatrix} \alpha & 1 & & \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ & & & \alpha \end{pmatrix}$$

with f rows.

18. Nilpotent groups

Let's list the groups of order 16. There are $p(4) = 5$ abelian groups, namely

1. $\mathbf{Z}/16\mathbf{Z}$,
2. $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$,
3. $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$,
4. $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and
5. $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

We also have 2 products $\mathbf{Z}/2\mathbf{Z} \times \mathrm{D}_8$ and $\mathbf{Z}/2\mathbf{Z} \times \mathrm{Q}_8$, and 4 non-abelian groups with an element of order 8, namely

1. the generalized quaternion group (the binary dihedral group of order 16) and
2. three groups of the form $\mathbf{Z}/8\mathbf{Z} \ltimes \mathbf{Z}/2\mathbf{Z}$ where if $a^8 = 1$ and $b^2 = 1$, then $bab^{-1} = a^3, a^5, a^7$. The group with $bab^{-1} = a^7$ corresponds to D_{16} and the a^3 group is called the semidihedral group.

We also have various semidirect products:

1. $\mathbf{Z}/4\mathbf{Z} \ltimes \mathbf{Z}/4\mathbf{Z}$,
2. $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \ltimes \mathbf{Z}/4\mathbf{Z}$, and
3. $(\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \ltimes \mathbf{Z}/2\mathbf{Z}$, the **Pauli group** on one qubit.

Recall Corollary 11.5.

Proof. All conjugacy classes have order a power of p, so the size is 1 or divisible by p. So the number of conjugacy classes of size 1 is divisible by p. A conjugacy class of size 1 is an element of the centre, so we can mod out by the centre. The result follows by induction. □

So all groups G of order 16 are nilpotent.

Proposition 18.1

The product of 2 nilpotent groups is nilpotent.

Proof. "Easy." □

Proposition 18.2

The following are equivalent for finite groups.

1. A group G is a product of p-groups,
2. G is nilpotent, and
3. all Sylow subgroups of G are normal (there at most 1 Sylow p-subgroup for any p).

19. Wreath products

Let's look at groups G of order 18. By Theorem 14.1 G has a subgroup of order 9. Since it has index 2, it is normal, so G is a semidirect product of a group of order 9 with $\mathbf{Z}/2\mathbf{Z}$. We know that the subgroup of order 9 is either $\mathbf{Z}/9\mathbf{Z}$ or $(\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})$.

If the subgroup is $\mathbf{Z}/9\mathbf{Z}$, the group of order 2 can act as 1, which corresponds to $\mathbf{Z}/18\mathbf{Z}$, or -1, which corresponds to D_{18}.

If the subgroup is $(\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})$, we have to consider how $\mathbf{Z}/2\mathbf{Z}$ can act on it. The subgroup is a vector space V of dimension 2 over $\mathbf{F}_3$. The nontrivial element of $\mathbf{Z}/2\mathbf{Z}$ is an order 2 linear transformation σ. The vector space $V = V_1 \oplus V_2$ is the sum of eigenspaces of σ where $\sigma = 1$ on V_1 and $\sigma = -1$ on V_2. The space V_1 can have dimension $2, 1$, or 0, so, in total, we have

$$\sigma = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$$

corresponding to the 3 conjugacy classes of linear transformations of order 2 over V. This gives us 3 possibilities for G. The first one gives $(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}) \times \mathbf{Z}/2\mathbf{Z}$, the second gives $\mathbf{Z}/3\mathbf{Z} \times \mathrm{S}_3$, and the last gives $(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}) \ltimes \mathbf{Z}/2\mathbf{Z}$. This last one is an example of a Frobenius group, and the second one is an example of a wreath product.

Definition 19.1. A **wreath product** of G and H is given by

$$G \wr H = \left(\underbrace{G \times G \times \cdots \times G}_{|H| \text{ times}} \right) \ltimes H.$$

Example 19.2
1. Take $G = \mathbf{Z}/3\mathbf{Z}$ and $H = \mathbf{Z}/2\mathbf{Z}$. Then $G \wr H = ((\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})) \ltimes \mathbf{Z}/2\mathbf{Z}$ where $\mathbf{Z}/2\mathbf{Z}$ acts by flipping the two groups of order 3.
2. $\mathrm{D}_8 = \mathbf{Z}/2\mathbf{Z} \wr \mathbf{Z}/2\mathbf{Z}$.
3. Automorphisms of trees are often wreath products.

Wreath products also show up in the Sylow subgroups of symmetric groups. For symmetric groups of index p^f you get an f-fold wreath product of $\mathbf{Z}/p\mathbf{Z}$, a sort of tower of wreath products. For instance, if $G = \mathrm{S}_{27}$, then we get $((\mathbf{Z}/3\mathbf{Z}) \wr (\mathbf{Z}/3\mathbf{Z})) \wr (\mathbf{Z}/3\mathbf{Z})$. For others you get products of these towers. See lecture 19 around minute 11 for more detail.

20. Frobenius groups

Let's consider groups of order 20. We know there is a Sylow subgroup of order 5 that is normal, so G is a semidirect product of $\mathbf{Z}/5\mathbf{Z}$ with a group of order 4. We know $\mathrm{Aut}(\mathbf{Z}/5\mathbf{Z}) \cong \mathbf{Z}/4\mathbf{Z}$. If the group of order 4 is $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$, there are two possibilities. If the action is trivial, then we get $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. If it's nontrivial, we get $\mathrm{D}_{10} \times \mathbf{Z}/2\mathbf{Z}$. If the group of order 4 is $\mathbf{Z}/4\mathbf{Z}$, we have 3 possibilities. If the action is trivial, we get $\mathbf{Z}/20\mathbf{Z}$. If $\mathbf{Z}/4\mathbf{Z}$ acts as a group of order 2 on $\mathbf{Z}/5\mathbf{Z}$, we get a semidirect product $\mathbf{Z}/5\mathbf{Z} \ltimes \mathbf{Z}/4\mathbf{Z}$ which is the binary dihedral group of order 20. We also get $\mathbf{Z}/5\mathbf{Z} \ltimes \mathbf{Z}/4\mathbf{Z}$ which is the $ax + b$ group.

This last group is a Frobenius group.

Definition 20.1. A **Frobenius group** G is a group acting transitively on a set S such that no nonidentity element of G fixes at least two elements of S and S is not the regular representation.

Example 20.2
1. The $ax + b$ group over a field F is Frobenius, where S consists of elements in F, $a \in F^*$, and $b \in F$, with order $|F|\,(|F| - 1)$.
2. The group D_n for n odd is Frobenius.
3. The group $(\mathbf{Z}/3\mathbf{Z})^2 \ltimes \mathbf{Z}/2\mathbf{Z}$ is Frobenius.

Definition 20.3. A subgroup $H \neq \{1\}$ of a finite group G is called a **Frobenius complement** if $H \cap H^g = \{1\}$ for all $g \in G \setminus H$. The **Frobenius kernel** is

$$K = \left(G \setminus \bigcup_{g \in G} H^g \right) \cup \{1\}.$$

Theorem 20.4 (Frobenius)
Let G be a finite group, H a Frobenius complement of G, and K the corresponding Frobenius kernel. Then K is a normal subgroup in G and

$$G = K \rtimes H.$$

Proof. Uses character theory[4], so skipped. □

Theorem 20.5 (Thompson)
The Frobenius kernel K is nilpotent.

Example 20.6
Take

$$K = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbf{F}_7)$$

and

$$H = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix} \right\rangle.$$

Then KH is a Frobenius group of order $7^3 \cdot 3$.

There are two possibilities for groups of order 21: $\mathbf{Z}/21\mathbf{Z}$ and $\mathbf{Z}/7\mathbf{Z} \rtimes \mathbf{Z}/3\mathbf{Z}$. The second group is a Frobenius group. We know groups of order 22 are either $\mathbf{Z}/22\mathbf{Z}$ or D_{22}, and the only group of order 23 is $\mathbf{Z}/23\mathbf{Z}$.

21. Groups of order 24

There are 15 groups of order 24. There's a Sylow 3-subgroup, and there might be one such subgroup or 4 subgroups.

Let's look at the case when G has one normal Sylow 3 subgroup. Then G is a semidirect product of $\mathbf{Z}/3\mathbf{Z}$ with a group of order 8 (the Sylow 2-subgroup). The Sylow 2-subgroup can be $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $(\mathbf{Z}/2\mathbf{Z})^3$, Q_8, or D_8. What is the action of the group of order 8 on the group of order 3? We have $\mathrm{Aut}(\mathbf{Z}/3\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z}$.

The action on $\mathbf{Z}/3\mathbf{Z}$ can be trivial or nontrivial. If the action is trivial, then G is a direct product of $\mathbf{Z}/3\mathbf{Z}$ with the mentioned groups of order 8. If the action is nontrivial, then we get two groups from $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and D_8, and 1 from each of the other groups of order 8. We have two groups for these two groups of order 8 because kernel of the map from either

[4] See https://terrytao.wordpress.com/2013/05/24/a-fourier-analytic-proof-of-frobeniuss-theorem/.

$\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ or D_8 to the group of order 3 can be cyclic or a direct product of two cyclic groups.

Now suppose we have 4 Sylow 3-subgroups (not normal). So G acts by conjugation on these four Sylow 3-subgroups. G acts transitively, so we get a homomorphism from G to S_4 (the permutations of the Sylow subgroups). What is the kernel of this homomorphism? The kernel must have order dividing 6 because we have a transitive action of G on a set of 4 elements. The kernel cannot have order 3 or 6, since the order 3 subgroup of the kernel would be normal in G. If the kernel has order 1, then $G \cong \mathrm{S}_4$.

If the kernel has order 2, the image has order 12 and has more than 1 Sylow 3-subgroup (otherwise, G would have a normal Sylow 3-subgroup), so $G \cong \mathrm{A}_4$. The group A_4 has a normal subgroup of order 2, and its preimage in G is a normal subgroup of order 8, so, in this case, G has a normal subgroup of order 8, meaning G is the semidirect product of a group of order 8 with a group of order 3 (with nontrivial action). There are two possibilities here: $(\mathbf{Z}/2\mathbf{Z})^3 \ltimes \mathbf{Z}/3\mathbf{Z}$ or $\mathrm{Q}_8 \ltimes \mathbf{Z}/3\mathbf{Z}$. The first case gives $\mathrm{A}_4 \times \mathbf{Z}/2\mathbf{Z}$, and the other gives the binary tetrahedral group.

Let's consider the binary tetrahedral group. Recall that the group S^3 of unit quaternions maps to $\mathrm{SO}_3(\mathbf{R})$. Inside $\mathrm{SO}_3(\mathbf{R})$ is A_4 (the rotations of the tetrahedron). We have the following **central extension**

$$1 \to \mathbf{Z}/2\mathbf{Z} \to \widehat{\mathrm{A}_4} \to \mathrm{A}_4 \to 1$$

where $\widehat{\mathrm{A}_4}$ denotes the binary tetrahedral group.

The ring of **Hurwitz quaternions**

$$H = \{a + bi + cj + dk : a, b, c, d \in \mathbf{Z} \text{ or } a, b, c, d \in (\mathbf{Z} + 1/2)\}$$

has units $\pm 1, \pm i, \pm j, \pm k$, and all quaternions of the form $(\pm 1 \pm i \pm j \pm k)/2$. These units form the binary tetrahedral group.

The group S_4 doesn't have very many normal subgroups. It has $\{1\} \subset \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \subset \mathrm{A}_4 \subset \mathrm{S}_4$. The group S_4 is the first group with no normal Sylow subgroups.

Definition 21.1. A group G is **solvable** if we can find a series of subgroups

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

such that G_i is normal in G_{i+1} and G_{i+1}/G_i is cyclic of prime order.

All nilpotent groups are solvable. The smallest group that is not solvable is A_5.

The quotient of S_4 by $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ gives a homomorphism from S_4 to S_3. Suppose we have 4 points acted on by S_4. We can construct a set of 3 things acted on by S_3 by taking all ways we can join the four points in pairs. Any permutation of the four points gives a permutation of these three objects.

22. Symmetric groups

The symmetric group S_n is the group of permutations of n letters, where

$$|\mathrm{S}_n| = n!$$

It has a subgroup A_n, the alternating group, with index 2, and $|\mathrm{A}_n| = n!/2$ if $n > 1$. The group A_n consists of the permutations fixing

$$\prod_{0<i<j\leq n} (x_i - x_j).$$

Indeed, we have a homomorphism $\mathrm{S}_n \to \{\pm 1\}$ where the sign depends on the sign of the above polynomial. The group A_n is the kernel of this homomorphism, so we have the exact sequence

$$1 \to \mathrm{A}_n \to \mathrm{S}_n \to \{\pm 1\} \to 1.$$

The group A_n is normal in S_n because it is the kernel of a homomorphism.

The groups S_1 and A_1 are trivial. The group S_2 is cyclic of order 2 and A_2 is trivial. The group $\mathrm{S}_3 \cong \mathrm{D}_6$ is the first nonabelian group, and $\mathrm{A}_3 \cong \mathbf{Z}/3\mathbf{Z}$. We have

$$\mathrm{S}_4 \rhd \mathrm{A}_4 \rhd (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \rhd \{1\},$$

which is the only case when a symmetric group has a nontrivial normal subgroup other than the alternating group. The group A_4 is also the rotations of a tetrahedron, and the group S_4 is the rotations of a cube or octahedron.

Definition 22.1. A group G is a **simple group** if its only normal subgroups are $\{1\}$ and G.

The group A_5 is the rotations of an icosahedron; the group A_5 is the first nonabelian simple group, and the first that isn't cyclic of prime order. The group S_6 has nontrivial automorphisms of an unexpected form.

The conjugacy classes of S_n are easy to describe. Any element of S_n is a product of disjoint cycles, and conjugating a permutation preserves its cycle shape. Conversely, any two elements of the same cycle shape are conjugate. Suppose that $a = (1\ 2\ 3)(4\ 5)(6\ 7)$, $b = (6\ 4\ 3)(2\ 1)(7\ 5)$, and we want to determine g such that $gag^{-1} = b$. We find that g can be the permutation mapping 1 to 6, 2 to 4, 3 to itself, 4 to 2, etc. So $g = (1\ 6\ 7\ 5)(2\ 4)(3)$. This g is not unique.

So the conjugacy classes of S_n correspond to cycle shapes of length n, and the number of conjugacy classes of S_n is $p(n)$. (Partitions again. Yay!)

So what are the conjugacy classes of S_4? We can write $4 = 4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$ where each partition corresponds to a conjugacy class.

How many elements are in each conjugacy class? The size of the conjugacy class is the size of the orbit under G, which is $|G|$ divided by the order of the subgroup fixing a point, which is the order of the subgroup commuting with one permutation. If we have a permutation with cycle shape $(1^3)(2^2)(3^1)(4^2)$, then it commutes with a group of order $1^3 \times 3! \times 2^2 \times 2! \times 3^1 \times 1! \times 4^2 \times 2!$ So the order of the centralizer of a permutation of shape $\prod_i i^{n_i}$ is $\prod_i i^{n_i} n_i!$, so the size of the conjugacy class is

$$\frac{n!}{\prod_i i^{n_i} n_i!}$$

Conjugacy classes in A_n are similar, but classes of S_n sometimes split into 2 classes of A_n. Take, for example, A_3. The set of conjugacy classes of S_3 is

$$\{\{1\}, \{(1\ 2\ 3), (1\ 3\ 2)\}, \{(1\ 2), (2\ 3), (3\ 1)\}\}.$$

The 2-cycles are not elements of A_3, but A_3 has 3 conjugacy classes; that is, the second conjugacy class of S_3 split into two conjugacy classes in A_3. The problem is that the element conjugating the one 3-cycle to the other is a 2-cycle (not in A_3). We have a similar thing with $A_4 \subset S_4$. However, $A_5 \subset S_5$ doesn't have this problem (the 3-cycles form one conjugacy class in A_5.) We can conjugate the first 3-cycle to the second by the permutation $(2\ 3) \notin A_5$. We multiply by $(4\ 5)$ to get the element into the alternating group. There is an algorithm for determining whether A_n does this, but Dr. Borcherds is forgetful, so you will never find out.

What are the generators of S_n? The generators are the transpositions (an element swapping two letters). We want to show that every permutation is a product of transpositions.

"We use the notorious bubble sort. . . . Anyway, fortunately, bubble sort has been more or less eradicated from computing, but it's still very useful in the theory of the symmetric group."

23. Coxeter-Todd algorithm

The symmetric group is generated by the transpositions. What are the relations between the transpositions? Of course, if τ is any transposition, then $\tau^2 = 1$. If $\tau_1 = (\alpha_1\ \alpha_2)$ and $\tau_2 = (\alpha_2\ \alpha_3)$, then $(\tau_1\tau_2)^3 = 1$. If $\tau_3 = (\alpha_3\ \alpha_4)$, then $(\tau_1\tau_3)^2 = 1$.

Coxeter came up with a compact way of writing relations like these: **Coxeter diagrams**. The Coxeter diagram for S_n is

S_n : 

For each point τ, $\tau^2 = 1$. If τ is connected to τ', then $(\tau\tau')^3 = 1$. If τ is not connected to τ', then $(\tau\tau')^2 = 1$.

Are there any other relations that we can't get from the previous ones? That is, do the relations above define the symmetric group? Suppose G is a group defined by these relations. Then there is a map $G \to S_n$ that is surjective because S_n is generated by the relations. We want to show that the kernel of this map is $\{1\}$ such that the G is isomorphic to S_n. It is enough to show that $|G| \leq |S_n|$.

Suppose we have the Coxeter diagram

G :

Label the points $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. The group G has a subgroup $H = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$, and, by induction, $|H| \leq |S_4|$. We want to show $|G| / |H| \leq 5$. Construct the permutation representation on cosets of H by brute force. This will be an action of G on a set containing a point fixed by H. We write down the representation and find that $|G| / |H| = 5$. So $|G| \leq 5\,|H| \leq 120$, so $G \cong S_5$.

Dr. Borcherds shows the algorithm in action in his lecture.

24. Extra special groups

We will explore some analogues of the Heisenberg group, called extra special groups. Let's consider groups of order 25, 26, 27, 28, and 29. There are only two groups of order 25 are $\mathbf{Z}/25\mathbf{Z}$ and $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$. A group of order 26 is either $\mathbf{Z}/26\mathbf{Z}$ or D_{26}. A group of order 29 is cyclic. The groups of order 28 are similar to those of order 20: we get two abelian groups, a dihedral group, and a binary dihedral group. To classify the groups of order 27, we will classify the groups of order p^3.

We have 3 abelian groups of order p^3: $\mathbf{Z}/p^3\mathbf{Z}$, $\mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$, and $(\mathbf{Z}/p\mathbf{Z})^3$. It turns out that there are two nonabelian groups. The group can have elements of order p^2, or all elements have order 1 or p. If $p = 2$, both D_8 and Q_8 have elements of order p^2, and there are no groups such that all elements have order 2 (otherwise the group would be abelian: $ab = (bb)ab(aa) = b(ba)(ba)a = ba$).

If p is odd, then we have one nonabelian group for each case. Let G be the group. If G has an element of order p^2, the centre Z is cyclic of order p. Then $G/Z = (\mathbf{Z}/p\mathbf{Z})^2$, and we have the extension

$$\{1\} \to \mathbf{Z}/p\mathbf{Z} \to G \to (\mathbf{Z}/p\mathbf{Z})^2 \to \{1\}.$$

First let's look at the case when all elements of G have order 1 or p. The group

$$G = \left\{ \begin{pmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{pmatrix} \right\} \subset \mathrm{GL}_3(\mathbf{F}_p)$$

is nonabelian of order p^3. Do all of its elements have order p, and, if so, why does that fail when $p = 2$? We define the map

$$\exp : \left\{ \begin{pmatrix} & * & * \\ & & * \\ & & \end{pmatrix} \right\} \to G,$$

which, in this case, can be defined

$$\exp : a \mapsto 1 + a + a^2/2.$$

Also, $\log(1 + a) = a - a^2/2$. (Notice that $a^3 = 0$ here.) We have $\exp(a + b) = (\exp a)(\exp b)$ if $ab = ba$, so $\exp(na) = (\exp a)^n$. In the group, we have $g^p = \exp(p \log g) = 1$ since $p \log g = 0$ in $\mathbf{F}_p$. All elements of G have order p except when $p = 2$, since we're dividing by 2 in exp and log. If $p = 2$, we have $G = \mathrm{D}_8$.

We can check that there is only one such group. Any nonabelian group G of order p^3 with $g^p = 1$ for all g must be a semidirect product $(\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}) \ltimes \mathbf{Z}/p\mathbf{Z}$. The automorphisms of the former group in the semidirect product are two-by-two matrices, and the automorphisms of order p are conjugate to the automorphism $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$. We might as well take a generator of $\mathbf{Z}/p\mathbf{Z}$ to act on the two-dimensional vector space by that automorphism. So the group has elements $a^p = 1, b^p = 1$ with $ab = ba$. Take $c \in \mathbf{Z}/p\mathbf{Z}$, so c commutes with a and $cb = abc$. We can check the generators define a group of order p^3 unique up to isomorphism. (That is,

there is one nonabelian group of order p^3 where all nontrivial elements have order p up to isomorphism.)

Suppose G is nonabelian of order p^3 with an element of order p^2. The group G has a normal subgroup $\mathbf{Z}/p^2\mathbf{Z}$ generated by $a : a^{p^2} = 1$. Pick $b \notin (\mathbf{Z}/p^2\mathbf{Z})$. The element b must act nontrivially on a (otherwise the group would be abelian). We choose b such that $bab^{-1} = a^{1+p}$ which is always possible. We must have $b^p = 1, a^p, a^{p^2}, \ldots$. If $b^p = 1$, then $G = (\mathbf{Z}/p^2\mathbf{Z}) \ltimes (\mathbf{Z}/p\mathbf{Z})$. If $p = 2$, then the case $b^p = a^p$ gives a different group (the quaternion group) than the case $b^p = 1$ (the dihedral group). If p is odd, we can change b to $c = ba$ where $cac^{-1} = a^{1+p}$. What is c^p now? We have $c^p = (ba)^p = ba \cdots ba = a^{(p(p+1)/2)p} a^p b^p$. If $p \neq 2$, then the first term in c^p is $a^{p^2(p+1)/2} = 1$, so $c^p = a^p b^p$. If $b^p = a^{np}$ is a power of a, then we get $c^p = a^{(n+1)p}$, and repeatedly doing this will give an element $d^p = 1$, so our group has relations $a^{p^2} = 1$, $dad^{-1} = a^{1+p}$, thus the group is a semidirect product.

So we only get 2 nonabelian groups of order p^3. We can construct them by either taking the upper triangular matrices above or a semidirect product $\mathbf{Z}/p^2\mathbf{Z} \ltimes \mathbf{Z}/p\mathbf{Z}$. The first kind forms a family for all p, and the second forms a family for p odd. When $p = 2$, it turns out that one semidirect product is isomorphic to the group in matrix form (the dihedral group), and another semidirect product is isomorphic to Q_8.

These groups are analogues of the Heisenberg group. Suppose $f : \mathbf{R} \to \mathbf{C}$. We can transform f by $T_\alpha : f(x) \mapsto f(x + \alpha)$ and $T_\beta : f(x) \mapsto e^{2\pi i \beta x} f(x)$ (corresponding to momentum and position operators). We have $T_\alpha T_\beta \equiv T_\beta T_\alpha e^{2\pi i \alpha\beta}$. We get a three dimensional group of transformations where $f(x) \mapsto e^{2\pi i(\gamma + \beta x)} f(x + \alpha)$. The circle group S^1 is a subgroup, so we have the extension

$$\{1\} \to S^1 \to G \to \mathbf{R} \times \mathbf{R} \to \{1\}.$$

Now suppose $f : \mathbf{F}_p \to \mathbf{C}$ with $T_\alpha : f(x) \to (x + \alpha) f(x)$ and $T_\beta : f(x) \mapsto e^{2\pi i \beta x/p} f(x)$, where $\alpha, \beta \in \mathbf{F}_p$. Also, $e^{2\pi i \beta x/p}$ is a well defined pth root of unity. These commute with each other up to multiplication by $e^{2\pi i \gamma/p}$, $\gamma \in \mathbf{F}_p$. We get a group G of order p^3 where

$$\{1\} \to \mathbf{F}_p \to G \to \mathbf{F}_p \times \mathbf{F}_p \to \{1\}.$$

The group G is isomorphic to the group of those upper triangular matrices.

So groups of order p^3 are similar to the Heisenberg group. We can have Heisenberg groups in n dimensions. We have the extension

$$\{1\} \to S^1 \to G \to \mathbf{R}^n \times \mathbf{R}^n \to \{1\},$$

hence the extension

$$\{1\} \to \mathbf{F}_p \to H \to \mathbf{F}_p^n \times \mathbf{F}_p^n \to \{1\}.$$

These groups H are **extra special groups**. Such a group H has order p^{1+2n}, its centre Z has order p, and $H/Z \cong (\mathbf{Z}/p\mathbf{Z})^{2n}$.

We can build all extra special groups from groups of order p. The group $G/Z = (\mathbf{Z}/p\mathbf{Z})^{2n}$ has a skew symmetric form $\langle a, b\rangle \mapsto aba^{-1}b^{-1} \in Z = \mathbf{F}_p$, and $\langle a, b\rangle = \langle b, a\rangle^{-1}$. So we have a vector space of dimension $2n$ over a field with a skew symmetric form. Any nondegenerate skew symmetric over a field can be split up into a sum of two dimensional forms. Also, G splits as a central product of groups of order p^3 (since you can identify any of the centres).

We get 2 extra special groups of order p^{1+2n}. If p is odd, one has all elements of order p and one has an element of order p^2. If p is even, we distinguish the two by the Arf invariant.

If we have an extra special group of order 2^{1+2n}, then

$$G/Z \cong (\mathbf{Z}/2\mathbf{Z})^{2n},$$

which has a quadratic form q, and a map $(\mathbf{Z}/2\mathbf{Z})^{2n} \to \mathbf{Z}/2\mathbf{Z} = Z$, where $q(a) = a^2$. Also, $q(ab) = q(a)q(b)\langle a, b\rangle = q(a)q(b)aba^{-1}b^{-1}$. Quadratic forms $q : \mathbf{F}_2^n \to \mathbf{F}_2$ can be distinguished by the Arf invariant, given by the most common value of q. (It is sometimes called the "democratic invariant.")

25. The transfer homomorphism

Let's classify the groups G of order $30 = 2 \cdot 3 \cdot 5$. We want to show that G has a normal subgroup of index 2. We will construct a transfer homomorphism

$$\tau : G \twoheadrightarrow \mathbf{Z}/2\mathbf{Z}$$

whose kernel is a normal subgroup of G of order 15. The only subgroup of order 15 must be cyclic of order 15, so we get the split exact sequence

$$\{1\} \to \mathbf{Z}/15\mathbf{Z} \to G \to \mathbf{Z}/2\mathbf{Z} \to \{1\}$$

so $G \cong \mathbf{Z}/15\mathbf{Z} \ltimes \mathbf{Z}/2\mathbf{Z}$ classified by how $\mathbf{Z}/2\mathbf{Z}$ acts on $\mathbf{Z}/15\mathbf{Z}$. There are 4 ways this can happen, so we get 4 groups: $\mathbf{Z}/30\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z} \times \mathrm{D}_{10}$, $\mathbf{Z}/5\mathbf{Z} \times \mathrm{D}_6$, D_{30}.

Suppose H is a subgroup of G. Then the transfer homomorphism is the map

$$\tau : H^{\mathrm{ab}} \leftarrow G^{\mathrm{ab}},$$

where G^{ab} is the abelianization of G. Indeed, the transfer "goes the wrong way."

Definition 25.1. The **abelianization** of G denoted G^{ab} is the largest abelian quotient of G.

The set $[G, G] = \{ghg^{-1}h^{-1} : g, h \in G\}$ is the commutator subgroup of G, and

$$G/[G, G] = G^{\mathrm{ab}}.$$

Any homomorphism from G to an abelian group factorizes through G^{ab}.

The most natural way of defining τ is using the fact that G^{ab} is a Tate cohomology group $\hat{H}^{-1}(G, \mathbf{Z})$. For each Tate cohomology group $\hat{H}^n(G, \mathbf{Z})$ one gets a map from the Tate cohomology group of G to that of H. However, we'll avoid defining the transfer this way.

Definition 25.2. Write G as a union of left cosets of H. Pick some $g \in G$ and look at the action of g on all left cosets. (The element g is acting on the set of left cosets by left translation.) Write the cosets a_iH. Then $ga_1 = a_{i1}h_1$, $ga_2 = a_{i2}h_2$, etc. Then we define the **transfer homomorphism** τ by $\tau(g) = \prod_i h_i$.

Let's check if this is well-defined. The order of the h_is does not matter, since $h_i \in H^{\mathrm{ab}}$. Also, what happens if we change a_1 to, say, a_1h, since $a_1H = (a_1h)H$? It turns out that the transfer does not depend on the choice of the left coset, since $g(a_1h) = a_{i1}h_1h$, and

$g(a_j) = a_1 h_j = a_1 h(h^{-1}hj)$. If we replace a_1 by $a_1 h$, we replace $h_1 h_j$ by $h_1 h h^{-1} h_j = h_1 h_j$, so τ does not depend on the choice of coset representative, and it is well-defined.

Also, we better make sure τ is a homomorphism from G to H^{ab}. Suppose $ga_1 = a_{i1}h_i$, etc. So $\tau(g) = h_1 h_2 \cdots$. Also suppose $g'a_1 = a_{j1}h'_1$, etc. So $\tau(g') = h'_1 h'_2 \cdots$. So $g'ga_1 = a_* h_{i1}' h_1$, $g'ga_2 = a_* h_{i2}' h_2$, etc. So $\tau(g'g) = \prod_j h_{ij} h_j$, so it is the product $\tau(g)\tau(g')$.

If $g \in G$, what is $\tau(g)$? Take $g \in H$. We calculate $ga_1 = a_2$, and choose $a_2 = ga_1$, and similarly, $g(a_2) = a_3$, etc. all the way up to $g(a_n)$, but we already have a_1 fixed, so $g(a_n) = a_1 h_1$ for some h_1. Similarly, $g(a_{n+1}) = a_{n+2}$, all the way up to $g(a_{n+k}) = a_{n+1}h_2$. Here, we are splitting up the action of g into cycles, and for each cycle, we get 1 element of H. So $\tau(g) = h_1 h_2 \cdots$. We notice $g^2 a_1 = a_3$, etc., so $g^n a_1 = a_1 h_1$, which means that $h_1 = a_1^{-1} g^n a_1$, etc. So h_1 is a conjugate of g^n.

Now suppose no two distinct elements in H are conjugate in G. From $h_1 = a_1^{-1} g^n a_1$ and $g^n, h \in H$, we get $h_1 = g^n$, $h_2 = g^k$, etc. So $\tau(g) = h_1 h_2 \cdots = g^n g^k \cdots = g^{[G:H]}$ in this case.

If G is abelian, if $H \in \mathrm{Z}(G)$, or if H has order 2, then $\tau(g) = g^{[G:H]}$ for $g \in H$. If H has order 2, then τ acts on H as $g \mapsto g^{[G:H]}$. If $[G : H]$ is odd, then $\tau : G \to H$ is onto. That is, if $|G| = 2n$ with n odd, there is a surjective homomorphism $\tau : G \to H$ where H is a Sylow subgroup. So G is a semidirect product $K \ltimes H$ where K is index 2 and $H \cong \mathbf{Z}/2\mathbf{Z}$, and, in particular, G is not simple. No group of order 2 (mod 4) is simple!

Suppose p is the smallest prime dividing $|G|$. If p^2 does not divide $|G|$, then the Sylow p-subgroup is $\mathbf{Z}/p\mathbf{Z}$, and no 2 distinct elements can be conjugate (if there was such a pair, then there would have to be an inner automorphism of G acting on $\mathbf{Z}/p\mathbf{Z}$ nontrivially, but no nontrivial elements of G have order less than p). So $\tau : G \to \mathbf{Z}/p\mathbf{Z}$ acts as $g \mapsto g^{|G|/p}$ for $g \in \mathbf{Z}/p\mathbf{Z}$, and this map is onto. So G has a normal subgroup of index p (a normal p conjugate), so G is not simple. In fact, this holds even if p^2 divides $|G|$, provided the Sylow p-subgroup is cyclic.

So any simple group must be divisible by the square of some prime.

Suppose G is simple and the Sylow 2-subgroup of G is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (with 3 elements of order 2). All elements of order 2 in G are conjugate (interesting, short exercise). The group G has a normal subgroup of index 2, so G is not simple.

26. Too many p-groups

"We are going to be explaining why we are not going to try to classify p groups." There are 51 groups of order 32, so we will not classify them. Dr. Borcherds displays some diagrams from a book of groups of order 2^n for $n \leq 6$. There are 267 groups of order 64.

It gets even worse! There are 49487365422 groups of order 2^{10}. "Classifying groups of order p^n is rather like trying to classify all the individual grains of sand on a beach."

But why? First, all groups of order p^n are nilpotent, so they may have long series of subgroups generated from repeatedly killing the centre. However, we will suppose G has a centre of the form $(\mathbf{Z}/p\mathbf{Z})^m = \mathrm{Z}(G)$. So $G/\mathrm{Z}(G) = (\mathbf{Z}/p\mathbf{Z})^{m'}$. Both of these groups are elementary abelian groups, and the length of this series is 2:

$$\{1\} \subset \mathrm{Z}(G) \subset G.$$

This is how we will restrict G. So G is an extension $(\mathbf{Z}/p\mathbf{Z})^m \times (\mathbf{Z}/p\mathbf{Z})^{m'}$ where $(\mathbf{Z}/p\mathbf{Z})^{m'}$ can be thought of as a vector space of dimension m' over $\mathbf{F}_p$. We can choose a basis $\{a_1, \ldots, a_{m'}\}$ and look at all the elements $(a_i a_j a_i^{-1} a_j^{-1})$ (that is, the commutator). The commutator must be in the centre, so $(a_i a_j a_i^{-1} a_j^{-1}) \in \mathbf{F}_p^m$. We can define at least one group with these commutator relations by defining an element in $\mathbf{F}_p^m$ to be the commutator.

How many ways can we write the commutator? There are about $m'(m'-1)/2$ ways of choosing i, j. The dimension of all bilinear maps from $(\mathbf{Z}/p\mathbf{Z})^{m'} \otimes (\mathbf{Z}/p\mathbf{Z})^{m'} \to (\mathbf{Z}/p\mathbf{Z})^m$ is about $mm'^2/2$. So the vector space of all of these maps has size about $p^{mm'^2/2}$. Now, we have $m + m' = n$, where $|G| = p^n$, and we want to maximize $p^{mm'^2/2}$. We get $m' \approx (2/3)n$, $m \approx (1/3)n$. So we seem to be getting about $p^{(2/27)n^3}$ groups, but there are actually less.

We haven't accounted for symmetries. We could have chosen a different basis of a_is that gives us 2 of the elements in the $p^{(2/27)n^3}$ groups. This depends on the automorphisms of the vector spaces $(\mathbf{Z}/p\mathbf{Z})^m$ and $(\mathbf{Z}/p\mathbf{Z})^{m'}$. The automorphism group of the latter vector space is $\mathrm{GL}_{m'}(\mathbf{F}_p)$ whose order is about $p^{m'^2}$. We should have the number of groups, then, being $p^{(2/27)n^3 - O(n^2)}$. So the number of groups of order p^n grows like (not asymptotic to) $p^{(2/27)n^3}$. And that's too many groups.

27. The icosahedral group

Suppose G is a group of order 48. We will show that G is not simple by looking at its Sylow 2-subgroups. The number of these must be 1 or 3. If it's 1, then the Sylow subgroup is normal, so we're done. If it's 3, we get a transitive action of G on the set of 3 Sylow subgroups. Any transitive action of G on a set of 3 elements gives a nontrivial homomorphism from G to S_3, and $|\mathrm{S}_3| < |G|$, so the kernel of this homomorphism is a normal subgroup not $\{1\}$ or G of G, so we're done.

The group $G = \mathrm{GL}_2(\mathbf{F}_3)$ is of order $48 = (3^2-1)(3^2-3)$ (good exercise). The binary octahedral group is a group of 48. (The octahedral group is isomorphic to S_4, and this is the double cover of the octahedral group.) The group $\mathrm{GL}_2(\mathbf{F}_3)$ acts on four points, say, $\{0, 1, 2, \infty\}$ (the projective line over $\mathbf{F}_3$). If τ is one of the four points, then

$$\mathrm{GL}_2(\mathbf{F}_3) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}.$$

This gives a surjective homomorphism $\mathrm{GL}_2(\mathbf{F}_3) \to \mathrm{S}_4$ with kernel $\{\pm I\}$:

$$\{1\} \to \{\pm I\} \to \mathrm{GL}_2(\mathbf{F}_3) \to \mathrm{S}_4 \to \{1\}.$$

The binary octahedral group maps onto the octahedral group $\cong \mathrm{S}_4$ with kernel of order 2, just like $\mathrm{GL}_2(\mathbf{F}_3)$. Are they the same group, then? No. The binary octahedral group only has 1 element of order 2 (since S^3 only has 1 element of order 2) and $\mathrm{GL}_2(\mathbf{F}_3)$ has several elements of order 2.

Now, we'll look at groups of order 60. For example, we have

1. rotations of an icosahedron,
2. $\mathrm{SL}_2(\mathbf{F}_4)$ (of order $(4^2-1)(4^2-4)/(4-1)$),
3. $\mathrm{PSL}_2(\mathbf{F}_5) = \mathrm{SL}_2(\mathbf{F}_5)/\mathrm{Z}(\mathrm{SL}_2(\mathbf{F}_5))$ (where the centre has order 2), and

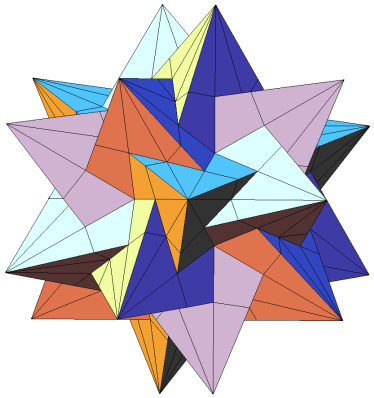


FIGURE 3. A compound of five tetrahedra, forming a stellation of an icosahedron, whose convex hull is a dodecahedron.

4. A_5.

These are all isomorphic, but why? If we can map any of these groups to a group of permutations of 5 elements, we get a map to S_5, and, from there, it would be easy to show that the group is isomorphic to A_5.

The group $SL_2(\mathbf{F}_4)$ acts on $\mathbf{F}_4 \cup \{\infty\}$ (the projective line), so we get a homomorphism $SL_2(\mathbf{F}_4) \to S_5$, and one can check that the image of the homomorphism is A_5. The group of rotations of an icosahedron acts on 5 objects. The dodecahedron has the same rotation group as the icosahedron since the two are dual. There are five ways to embed a cube in a dodecahedron, so each rotation of a dodecahedron gives a permutation of these five cubes. Also, refer to figure 3. The rotations of an icosahedron (or dodecahedron) give permutations of the five tetrahedra. Once again, the image of the homomorphism from the group of rotations to S_5 is A_5. It's not so easy to show the isomorphism from $PSL_2(\mathbf{F}_5)$ to A_5.

Proposition 27.1

The group A_5 is simple.

We'll show that the group of rotations of an icosahedron is simple. We'll start by determining conjugacy classes. We have rotations by $1/5, 2/5$ of a revolution about some axes. There are 12 vertices, so we get 12 of each. If we fix a face, we can rotate by $1/3$ of a revolution, and there are 20 of these. If we fix an edge, we rotate by $1/2$ of a revolution about that edge. Even though there are 30 edges, we get 15 rotations about edges. We also have the identity, and these comprise all conjugacy classes.

The order of a normal subgroup must divide 60 and be $1 + \lambda$, where λ is a sum of elements of $\{12, 12, 20, 15\}$, since any normal subgroup is closed under conjugacy classes. The only way $1 + \lambda$ can divide 60 is if $1 + \lambda = 1, 60$, so there are no nontrivial normal subgroups, and the group of rotations of an icosahedron is simple.

Exercise 27.2. Show that any simple group of order less than 60 is cyclic.

Proposition 27.3
Any simple group of order 60 is isomorphic to A_5.

To prove this proposition, we notice that there must be 6 Sylow 5-subgroups. Each Sylow subgroup contains 4 elements of order 5, and each subgroup is disjoint, so there are 24 elements of order 5. Also, the number of Sylow 3-subgroups might be 4 or 10, but it can't be 4, because then we would have a homomorphism to S_4 with kernel a normal subgroup, so there must be 10 Sylow 3-subgroups. Therefore, we have 20 elements of order 3. Now, consider elements of order 2; there must be 1, 3, 5, or 15 of them. If there were 1, 3, or 5, then we would have a homomorphism to S_3 or S_5, and the first case gives a normal subgroup and the second gives an isomorphism to A_5. So we must have 15 elements of order 2, and (as always) 1 element of order 1. The Sylow 2-subgroup cannot be cyclic, so it is $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$, and all elements of order 2 must be conjugate (recall Section 25). So the centralizer of an element of order 2 has order $60/15 = 4$, hence it must be the Sylow 2-subgroup. Any Sylow 2-subgroups must be disjoint (except for 1). Each Sylow 2-subgroup has 3 elements of order 2, and there are 15 elements of order 2, so there must be exactly 5 Sylow 2-subgroups. Thus, we get a homomorphism $G \to S_5$, and we deduce that $G \cong A_5$.

Proposition 27.4
The group A_n is simple if $n \geq 5$.

Any normal subgroup $N \neq \{1\}$ contains an element fixing a point. We pick $g \in N$ and look at $ghg^{-1}h^{-1}$ where h is a 3-cycle and $ghg^{-1}h^{-1} = g(hg^{-1}h^{-1})$ is nontrivial fixing a point. Suppose $g = (1\ 2\ 3\ \cdots)$. We can conjugate by a 3-cycle to change the 3 to something else. However, we also need h to fix the points $1, 2$ and three other points (that is, we need $n \geq 5$). So if $hg^{-1}h^{-1} = (1\ 2\ \lambda\ \cdots)$ where $\lambda \neq 3$, the quotient of those two elements will fix 1 without being the identity, so we're done. However, if g doesn't have a cycle of length at least 3, we can assume $g = (1\ 2)(3\ 4)(5\ 6)\cdots$, and we can find a 3-cycle h with the same property.

The subgroup fixing a point is A_{n-1} (which is simple if $n \geq 6$). So N contains the A_{n-1} fixing a point. Then N contains all the A_{n-1}s fixing all points (since all subgroups fixing a point are conjugate and N is normal). These A_{n-1}s generate A_n, which is easy to show. So $N = A_n$.

28. Groups of order 120, 168

There are plenty groups of order 120 (47 to be precise), but we will only focus on the ones involving the icosahedral group. We can take $SL_2(\mathbf{F}_5)$ of order $(5^2-1)(5^2-5)/(5-1) = 120$. We also have the binary icosahedral group, the double cover of the icosahedral group, which

has order $2 \times 60 = 120$. The group S_5 has order $5! = 120$, and the group $\mathbf{Z}/2\mathbf{Z} \times A_5$ has order $2 \times 60 = 120$.

Let's sort out these groups by looking at the Sylow 2-subgroup. For $SL_2(\mathbf{F}_5)$ it is Q_8, for the binary icosahedral group it is also Q_8, for S_5 it is D_8, and for $\mathbf{Z}/2\mathbf{Z} \times A_5$ it is $(\mathbf{Z}/2\mathbf{Z})^3$. In fact, $SL_2(\mathbf{F}_5)$ is isomorphic to the binary icosahedral group.

Consider the group of all symmetries of an icosahedron, which also has order 120. Its Sylow 2-subgroup is $(\mathbf{Z}/2\mathbf{Z})^3$, and as we might suspect it is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times A_5$. This isomorphism makes sense: the group A_5 is isomorphic to the group of rotations of an icosahedron, and the group of order 2 corresponds to the reflection part of icosahedral symmetry. There are 3 ways to get a group from a group of order 2 and a group of order 60.

Suppose G is the binary icosahedral group. The group G is a subgroup of the group S^3 of unit quaternions, so we can consider S^3/G. The group S^3 is a 3-manifold and G acts fixed point–freely on it, so S^3/G is a compact 3-manifold, called the **Poincaré homology sphere**. One can take a quotient of S^3 by any discrete group, and S^3/H is always a 3-manifold whose fundamental group is H and whose homology group is H^{ab}. One notices that $G^{\mathrm{ab}} = \{1\}$ (essentially since A_5 is simple). So S^3/G has vanishing first homology.

(Poincaré originally conjectured that if a 3-manifold has the same homology groups as a 3-sphere, then it is a 3-sphere, and later he found this counterexample. The group S^3/G has the same homology as a 3-sphere but different homotopy: its homotopy group is order 120. His infamous conjecture says that any compact 3-manifold with the same homotopy groups as a 3-sphere must be a 3-sphere. This result was proved by the great Grigori Perelman.)

The first noncyclic simple group has order 60, and the next one has order 168. There are two obvious ways of writing groups of order 168, namely $SL_3(\mathbf{F}_2)$ of order $(2^3-1)(2^3-2)(2^3-2^2) = 168$ or $\mathrm{PSL}(\mathbf{F}_7)$ of order $(7^2-1)(7^2-7)/(2\cdot(7-1)) = 168$. These groups are isomorphic, but showing the isomorphism is difficult. These kinds of isomorphisms make the classification of simple groups tricky. The group $SL_3(\mathbf{F}_2)$ acts on the Fano plane, namely $\mathbf{P}^2(\mathbf{F}_2)$ (see figure 4). It has 168 automorphisms isomorphic to $SL_3(\mathbf{F}_2)$. The Klein quadric, namely

$$x^3y + y^3z + z^3x = 0 \subset \mathbf{P}^2(\mathbf{C}),$$

has automorphism group of order 168, too, though this fact is less easy to see. The Klein quadric is an example of a Hurwitz surface: if S is a compact Riemann surface of genus $g > 1$ then $|\mathrm{Aut}(S)| \leq 84(g-1)$. The Klein quadric is the unique genus 3 Riemann surface with automorphism group of order this large.

29. The Jordan-Hölder theorem

If G is a finite group, then we can break it up into simple groups. We find a chain of subgroups

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

such that G_i is normal in G_{i+1} and G_{i+1}/G_i is simple. If G is simple, we are done. If not, we pick a normal subgroup to be one of the G_i and continue applying this to the normal subgroup and the quotient. This is called a **composition series**.

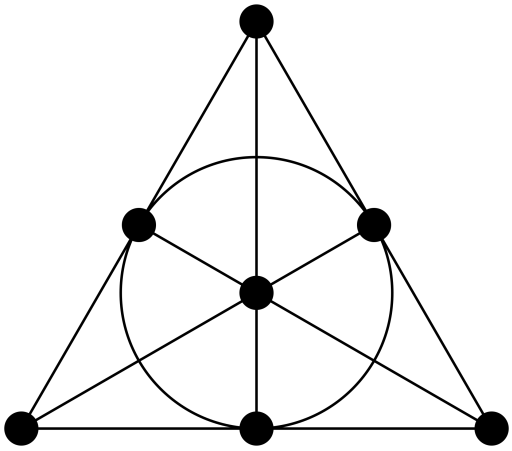


FIGURE 4. The Fano plane, the projective plane over $\mathbf{F}_2$, which has 168 automorphisms as a graph.

If

$$G_0 \subset G_1 \subset \cdots \subset G_n$$

is a composition series, G_i need not be normal in G_j for $i < j$ (unless $i = j - 1$).

Example 29.1

Consider the composition series

$$\{1\} \subset (\mathbf{Z}/2\mathbf{Z}) \subset (\mathbf{Z}/2\mathbf{Z})^2 \subset \mathrm{A}_4\,.$$

The group $\mathbf{Z}/2\mathbf{Z}$ is not normal in A_4. It is called a subnormal subgroup.

Suppose G is the binary icosahedral group. Then G has a composition series

$$\{1\} \subset \mathbf{Z}/2\mathbf{Z} \subset G$$

Clearly $(\mathbf{Z}/2\mathbf{Z})/\{1\}$ is simple, and so is $G/(\mathbf{Z}/2\mathbf{Z}) \cong \mathrm{A}_5$. If $G = \mathrm{S}_5$, then it has a composition series

$$\{1\} \subset \mathrm{A}_5 \subset \mathrm{S}_5$$

where $\mathrm{A}_5\,/\{1\}$ and $\mathrm{S}_5\,/\,\mathrm{A}_5 \cong \mathbf{Z}/2\mathbf{Z}$ are simple. We can also take

$$\{1\} \subset \mathbf{Z}/2\mathbf{Z} \subset \mathrm{A}_5 \times \mathbf{Z}/2\mathbf{Z}$$

or

$$\{1\} \subset \mathrm{A}_5 \subset \mathrm{A}_5 \times \mathbf{Z}/2\mathbf{Z}.$$

We see some notable things: the composition factors do not determine the group, and the group does not determine the order of the composition factors.

Theorem 29.2 (Jordan-Hölder)
Let G be a group. Then any 2 composition series of G have the same number of each simple factor.

Proof. Suppose

$$\{1\} = A_0 \subset \cdots \subset A_m = G$$

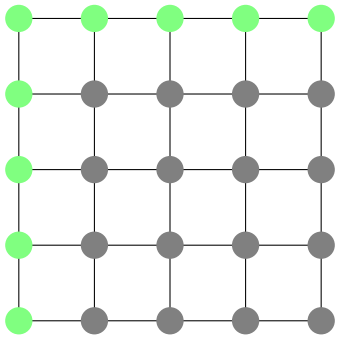
where A_{i+1}/A_i is simple and

$$\{1\} = B_0 \subset \cdots \subset B_n = G$$

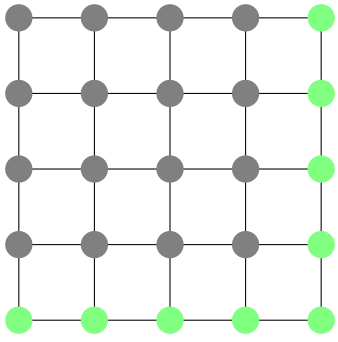
where B_{i+1}/B_i is simple. We want to show that the A_{i+1}/A_i and B_{i+1}/B_i are the same groups, possibly in a different order. Consider the array below.

$$\begin{pmatrix} A_0 \cap B_n & \cdots & A_m \cap B_n \\ \vdots & \vdots & \vdots \\ A_0 \cap B_0 & \dots & A_m \cap B_0 \end{pmatrix}$$

Each group is a normal subgroup of the two groups above it. We can think of this array as a grid where each vertex is a group and each edge is a quotient (either simple or $\{1\}$). Suppose we traverse the following path.

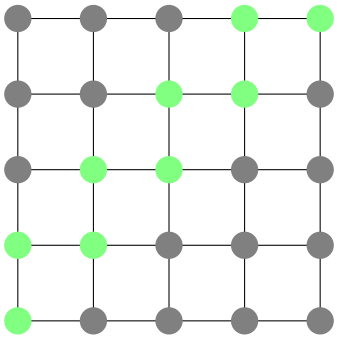


We are interested in the quotients we pass through. On the vertical, we pass through $\{1\}, \{1\}$, etc., and on the horizontal, we pass through $B_1/B_0, B_2/B_1$, etc. This route gives us the second composition series. Consider, instead, the route below.



Here, we go through $\{1\}, \{1\}$, etc. and $A_1/A_0, A_2/A_1$, etc. This corresponds to the first composition series.

Now consider the following path.



Likewise, we will go through other quotients. We want to show that every route has the same quotients up to reordering. We can get from any route to another by repeatedly flipping squares.

Suppose two routes differ by one square. That is, we have

$$\begin{array}{ccc} A_i \cap B_{j-1} & \longrightarrow & A_i \cap B_j \\ \downarrow & & \downarrow \\ A_{i-1} \cap B_{j-1} & \longrightarrow & A_{i-1} \cap B_j \end{array}$$

We will just quotient out by B_{j-1} since it is a normal subgroup of everything, so we get

$$\begin{array}{ccc} A & \longrightarrow & X \\ \downarrow & & \downarrow \\ \{1\} & \longrightarrow & B \end{array}$$

where X is a group and A and B are subgroups of X. If $A = B$, then either route gives A and X/A (in the same order), so the factors don't change. Suppose $A \neq B$. We know A, B are simple normal subgroups of X, so $X = A \times B$. Now, either route gives A and B (in opposite orders). Therefore, every time we change a route, we either keep the order of factors the same or switch them.

So any two routes have the same factors up to reordering. □

This also works for groups with operators (for example, modules over a ring).

Now we have a framework for transforming many problems involving groups into problems involving simple groups.

How do we classify simple groups? There are 18 infinite series of them, including A_n for $n \geq 5$ and $\mathrm{PSL}_n(\mathbf{F}_q)$ for $n \geq 2$ or $n \geq 3$ if $q = 2, 3$. There are also 26 sporadic groups, and the smallest is M_{11} of order 7920 while the largest is the monster group M of order approximately 10^{54}. This classification is one of the greatest feats of mathematics. The proof kind of works by looking at the centralizers of an involution. (A group has an involution if and only if it has even order, so the proof starts by showing that all noncyclic simple groups have even order.)

30. Outer automorphisms

Definition 30.1. An **inner automorphism** of a group G is an automorphism that takes an element $x \in G$ to gxg^{-1} for some $g \in G$.

The group of inner automorphisms is $\mathrm{Inn}(G) = G/\mathrm{Z}(G)$. The quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the **outer automorphisms** of G, and we get an exact sequence

$$\{1\} \to \mathrm{Z}(G) \to G \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to \{1\}.$$

Since we generally know G and $\mathrm{Z}(G)$, determining $\mathrm{Aut}(G)$ depends on determining $\mathrm{Out}(G)$.

Example 30.2

Suppose $G = (\mathbf{Z}/2\mathbf{Z})^2$. Then $\mathrm{Z}(G) = G$, so $\mathrm{Inn}(G) = \{1\}$. So $\mathrm{Out}(G) = \mathrm{Aut}(G)$, and we know $\mathrm{Aut}(G) = \mathrm{S}_3$.

For most groups, the automorphisms are usually easy to find. Suppose $G = \mathrm{PSL}_n(\mathbf{F}_q)$. Then $\mathrm{Aut}(G)$ consists of inner automorphisms, conjugations by elements of $\mathrm{GL}_n(\mathbf{F}_q)$, field automorphisms $\mathbf{F}_q \to \mathbf{F}_q$, and $g \mapsto (g^{-1})^{\mathrm{T}}$. Indeed, $\mathrm{Aut}(G)$ is generated by these obvious automorphisms, and this is usually the case.

Suppose $G = \mathrm{A}_n$. Then the obvious automorphisms are S_n, and if $n \neq 6$, this gives all automorphisms of G, so $\mathrm{Out}(G) = \mathbf{Z}/2\mathbf{Z}$. When $n = 6$, we find $\mathrm{Out}(\mathrm{A}_n) = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. (The sporadic group M_{11} has subgroup fixing a point of order 720 and is composed of A_6 with an unexpected automorphism of it.)

Let's consider outer automorphisms of S_6. Observe that S_5 has a subgroup of index 6 of order 20, which is a Frobenius group of order 20. This gives a nontrivial homomorphism $\mathrm{S}_5 \to \mathrm{S}_6$ (S_5 acts transitively on a set of 6 elements), so $\mathrm{S}_5 \subset \mathrm{S}_6$ not fixing a point. In fact, S_6 has $6 + 6$ subgroups of S_5 (usually S_n has n subgroups S_{n-1}). The group S_6 has a transitive S_5 subgroup of index 6. This gives a homomorphism $\mathrm{S}_6 \to \mathrm{S}_6$ acting on the 6 cosets of this subgroup. This is not an inner automorphism, so S_6 has an outer automorphism.

We want to write down an outer automorphism explicitly. The group S_6 is generated by the 5 transpositions:

S_6 :

(So for the transpositions $\tau_1, \ldots, \tau_5$, if $i < j$, then $\tau_i^2 = 1$, $(\tau_i\tau_j)^2 = 1$ if $j \neq i+1$, and $(\tau_i\tau_j)^3 = 1$ if $j = i+1$.) We want to find $\sigma_1, \ldots, \sigma_5$ with the same relations. Then we can get a homomorphism $\mathrm{S}_6 \to \mathrm{S}_6$ by $\tau_i \mapsto \sigma_i$. This automorphism will not be inner since the σ_i are not transpositions. So each σ_i is of the form $(* *)(* *)(* *)$ (a product of three transpositions), since the product will be of order 3 or order 2. Consider $\sigma_1 = (1\ 2)(3\ 4)(5\ 6)$. Then σ_2 can have no transposition in common with σ_1, so $\sigma_2 = (2\ 3)(4\ 5)(6\ 1)$. The element σ_3 must have no transposition in common with σ_2 and one in common with σ_1, so $\sigma_3 = (1\ 2)(3\ 5)(4\ 6)$. The element σ_4 must have one transposition in common with σ_1 and σ_2 but none in common with σ_3, so $\sigma_4 = (3\ 4)(6\ 1)(2\ 5)$. Finally, σ_5 must have one transposition in common with $\sigma_1, \sigma_2, \sigma_3$ but none in common with σ_4, so we get $\sigma_5 = (1\ 2)(4\ 5)(6\ 3)$. So we get our explicit outer automorphism of S_6:

$$\begin{aligned}
(1\ 2) &\mapsto (1\ 2)(3\ 4)(5\ 6),\\
(2\ 3) &\mapsto (2\ 3)(4\ 5)(6\ 1),\\
(3\ 4) &\mapsto (1\ 2)(3\ 5)(4\ 6),\\
(4\ 5) &\mapsto (3\ 4)(6\ 1)(2\ 5),\\
(5\ 6) &\mapsto (1\ 2)(4\ 5)(6\ 3).
\end{aligned}$$

(Dr. Borcherds provides illustrations at around 16:00 of lecture 30.)

No other symmetric groups have nontrivial outer automorphism group. Let $G = \mathrm{S}_n$. Suppose $\sigma \in \mathrm{Aut}(G)$ takes transpositions to transpositions. Then σ is inner. We can reconstruct n points from the transpositions (though $n = 3$ takes some more work), by knowing the transpositions, so any σ also acts on the n points of S_n and must be an inner automorphism of S_n. Are there automorphisms that do not preserve transpositions? The number of transpositions of S_n is $n(n-1)/2$, and the number of products of two transpositions is $n(n-1)(n-2)(n-3)/2^3 2!$. The number of products of three transpositions is similarly derived.

G	# transpositions	# products of two transpositions	# products of three transpositions
S_1	0	0	0
S_2	1	0	0
S_3	3	0	0
S_4	6	3	0
S_5	10	15	0
S_6	15	45	15
S_7	21	105	105
S_8	28	210	420

We notice that the number of transpositions is the same as the number of products of three transpositions for S_6. If an outer automorphism takes transpositions to some other conjugacy class, these conjugacy classes must have the same order. This happens for S_6. Extending this table, we get

G	$\#\{(*\,*)\}$	$\#\{(*\,*)(*\,*))\}$	$\#\{(*\,*)(*\,*)(*\,*)\}$	$\#\{(*\,*)(*\,*)(*\,*)(*\,*)\}$
S_1	0	0	0	0
S_2	1	0	0	0
S_3	3	0	0	0
S_4	6	3	0	0
S_5	10	15	0	0
S_6	15	45	15	0
S_7	21	105	105	0
S_8	28	210	420	105

There are no outer automorphisms for any other S_n, since the numbers in the last (three) columns are greater than $n(n-1)/2$ for $n > 6$. This computation is straightforward.

31. Free groups

Definition 31.1. The **free abelian group** G on commutative elements $\alpha_1, \ldots, \alpha_n$ is the universal abelian group generated by the α_i (with basis $\{\alpha_i\}$). That is, $G = \bigoplus_n \mathbf{Z}$.

(Universal property.) If F is a free abelian group and A is an abelian group then there is a unique homomorphism from F to A. In particular, $\operatorname{rank} F$ (the number of generators) is well-defined. We can see this by observing that there are 2^n homomorphisms from the free group on n generators to $\mathbf{Z}/2\mathbf{Z}$.

Let $\mathbf{Z}^n$ be a free abelian group. All of its subgroups are free abelian of rank $\leq n$. We can choose a basis $\{a_1, \ldots, a_n\}$ so that the subgroup is of the form $\langle r_1 a_1, \ldots, r_n a_n \rangle$ where the r_i are nonnegative integers.

Proof. See the classification of finitely generated abelian groups. □

A free abelian group corresponds to a lattice.

We want to consider the nonabelian analogues to free abelian groups, but first, we should consider "free monoids" (monoids are groups without inverses). The obvious way to construct a free monoid on elements $\alpha, \beta, \gamma, \ldots$ is to take all words on $\alpha, \beta, \gamma, \ldots$. If $F(\alpha, \beta)$ is a free monoid and M is a monoid, then if we choose two elements in M, then there is a unique homomorphism from $F(\alpha, \beta)$ to M where α maps to the first element and β to the second.

Suppose M is a monoid. We form the smallest equivalence relation $\sim$ on M such that if $x \sim a$ and $y \sim b$ then $xy \sim ab$ and $yx \sim ba$ for all $x, y, a, b \in M$.

Now we form a free group by taking a free monoid on $\alpha, \alpha^{-1}, \beta, \beta^{-1}, \ldots$ and modding out by $\sim$ such that $\alpha\alpha^{-1} \sim \alpha^{-1}\alpha \sim 1$, etc. If G is a group with elements α, β, γ, we have a unique homomorphism $F(a, b, c) \to G$ defined by $a \mapsto \alpha$, $b \mapsto \beta$, $c \mapsto \gamma$, etc. for more generators. (This is the universal property.) Again, the rank is well-defined in the same way (the free group on 2 generators is distinct from the free group on 3 generators, for example).

Let's try to write down the elements of a free group. In the free monoid, we might have elements like $1, \alpha, \beta, \alpha^{-1}, \beta^{-1}, \alpha^2, \alpha\beta, \alpha\beta^{-1}, \alpha\alpha^{-1}$, etc. In the free monoid, the element $\alpha\alpha^{-1}$ is distinct from 1, but in the free group, $\alpha\alpha^{-1} = 1$. Another element like $\alpha\alpha\beta\beta^{-1}\alpha^{-1}\beta\alpha^{-1}$ is just $\alpha\beta\alpha^{-1}$ in the free group. Every word is equivalent to a reduced word (that does not contain xx^{-1} or $x^{-1}x$).

Proposition 31.2

If 2 reduced words are distinct they are distinct in the free group. That is, if a reduced word is nonempty, then it is nontrivial in the free group.

Proof. This reduces to showing that, given a reduced word in $\alpha, \alpha^{-1}, \beta, \beta^{-1}, \dots$ one can always find a group G with elements $a, a^{-1}, b, b^{-1}, \dots$ such that this word is not 1. If the word has length n, take $G = \mathrm{S}_{n+1}$. □

Example 31.3

Take the reduced word $\alpha^2\beta\alpha^{-1}\beta\alpha\beta\alpha^2\beta^{-3}$. Can you find a group with elements a, b such that this reduced word is not equal to 1? This is a word of length 12, so we take 13 points and and draw arrows such that α, β correspond to a right-pointing arrow between points, and α^{-1}, β^{-1} correspond to a left-pointing arrow. We now have a partial permutation on 13 points, and since no triplet of points has $\alpha\alpha^{-1}$ or $\beta\beta^{-1}$ (the word is reduced), we can complete the permutation. Hence we see that this reduced word is not the identity in S_{13}.

Definition 31.4. A group G is **residually finite** if for any nonidentity element $g \in G$ we can define a homomorphism from G to a finite group H such that g has nonidentity image.

We have actually proven that free groups are residually finite.

Example 31.5

The groups $(\mathbf{Q}, +)$ and $(\mathbf{R}, +)$ are not residually finite (neither is any infinite simple group).

Why not define the free group as the set of reduced words? Well, proving associativity is a nightmare.

The free group on two generators impossible to draw in Euclidean space, so we need to draw it in hyperbolic space. See figure 5. In some sense, free abelian groups live in Euclidean space whereas free groups live in hyperbolic space.

We know that any subgroup of a free abelian group is free abelian of rank less than or equal to the free abelian group. Any subgroup of a free group is free, but the rank can increase. (The abelian group on 3 generators is a subgroup of the free group on 2 generators, for example.)

32. Subgroups of free groups

Proposition 32.1

Subgroups of free groups are free.

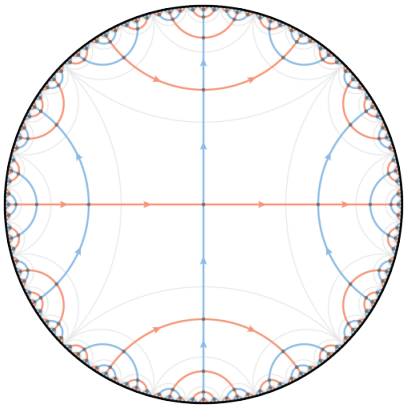
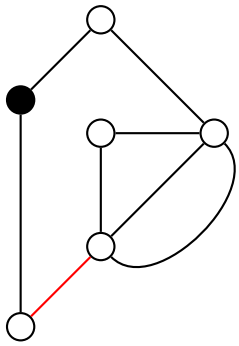


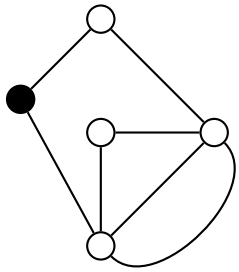
FIGURE 5. The Cayley graph of the free group on two generators embedded in the Poincaré disk model.

An index n subgroup of any group G is a transitive action of G on n points (where one is marked). Transitive actions of a free group on n points are easy to imagine. If we draw n points, draw arrows between these points corresponding to actions of the generators, and mark one point, we get an index n subgroup defined by all paths from the marked point to itself up to homotopy. This subgroup, therefore, is the fundamental group of the previously described path with respect to the base point.

What is the fundamental group of a graph? Consider the graph below, where the black node is the base point.



We can simplify this graph without changing the fundamental group. We can take the red edge and contract it to a point:

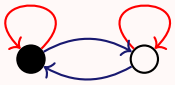


"Any loop in the first graph corresponds to a loop in the second graph," so the fundamental group is the same. If we continue to contract edges, we wind up with one vertex with five distinct edges from it to itself. The fundamental group of that graph is clearly the free group on five generators (since we have five loops). So the fundamental group is a free group on the "loops." So any subgroup of a free group is free. □

How do we write down the set of generators for this free group?

Example 32.2

Consider the free group on 2 generators and the action of it on two points. If we fix a point, each generator either fixes the points or swaps them, and both generators cannot fix a point since the graph is connected, so we get three possible ways to make the two points into a connected graph with two generators. Suppose a (red) and b (blue) are the generators:



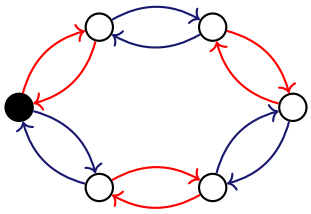
We contract this graph by annihilating the bottom blue line, and then we get a point with three distinct loops (three generators). The first a-loop remains a. The second a-loop is not a: it actually corresponds to going from the marked point to the unmarked point, then around the second a-loop, so we get bab^{-1}. The remaining loop corresponds to b^2, not b, since we have to go from the marked point to the unmarked point back to the marked point. So the subgroup of index 2 is a free group on 3 generators (a, bab^{-1}, b^2). That is, the free group on three generators is a subgroup of the free group on two generators.

Suppose G is index k in F_n (the free group on n generators). How many generators does G have? We draw the graph for G with k points and nk edges. The Euler characteristic of the graph is $\chi = k - kn$, so χ does not change when we contract an edge of the graph. So the graph with one point has characteristic $\chi = k - nk$, which is $1 -$ the number of loops. So the number of loops is $1 + nk - k$, and the number of loops is the number of generators.

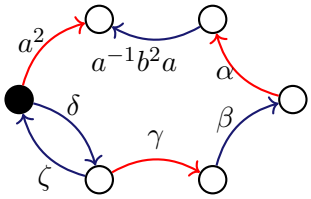
Suppose we have a map $F_2 \twoheadrightarrow \mathrm{S}_3$. (Recall that S_3 has two generators a and b satisfying $a^2 = 1$, $b^2 = 1$, and $(ab)^3 = 1$.) Suppose we want to find the generators for the kernel of

this map. "Well that sounds like a completely daft question: I just told you the relations that give you S_3 are these three elements, so surely the kernel is just the free group on these three elements: a^2, b^2, and $(ab)^3$. Well, no: that's wrong." These three elements do not generate the kernel, but these elements together with their conjugates do (the kernel must be normal, and these elements do not generate a normal subgroup). The subgroup is index 6, so the kernel should be a free group on 7 generators.

To find these generators, we write down an action of F_2 on 6 points:



This particular graph looks very symmetric. In particular, there is a symmetry taking any vertex to any other vertex, corresponding to the fact that the subgroup is normal. The conjugate of the fundamental group of the marked point by some element of the free group will be the fundamental group of another point. The fundamental group of each point is the same, so there is a symmetry taking a point to another. Now we contract some edges to get seven arrows, and each will correspond to a generator:



where

$$\alpha = a^{-1}b^{-1}a^2ba,$$
$$\beta = a^{-1}b^{-1}a^{-1}b^2aba,$$
$$\gamma = a^{-1}b^{-1}a^{-1}b^{-1}a^2baba$$
$$\delta = a^{-1}b^{-1}a^{-1}b^{-1}a^{-1}b, \text{ and}$$
$$\zeta = bababa.$$

So the set of seven generators is $\{a^2, a^{-1}b^2a, \alpha, \beta, \gamma, \delta, \zeta\}$.

33. Other definitions