Representation theory of finite groups I: A primer on group theory

Justin Campbell

July 1, 2015

1 The definition and examples

The word "group" should be understood as shorthand for "group of symmetries." That is, the symmetries of anything form a group, and a meta-principle says that any group is the symmetries of some (geometric, algebraic, etc.) object. Here "symmetry" means "transformation which leaves the object unchanged." Let's get the formal definition out of the way.

Definition 1.1. A *group* is a set G together with a binary operation $G \times G \to G$, written here as $(x, y) \mapsto xy$, satisfying the conditions

- (identity) there exists $e \in G$ such that $xe = ex = x$ for all $x \in G$,
- (existence of inverses) for any $x \in G$ there exists $y \in G$ satisfying $xy = yx = e$, and
- (associativity) for any $x, y, z \in G$ we have $(xy)z = x(yz)$.

Some comments on the definition are in order. We give them in the form of exercises.

Exercise 1.2. Show that the identity element is unique. We often write 1 for the identity element of a group, or 0 if the notation is additive.

Exercise 1.3. Check that cancellation holds in a group. This means that if $x, y, z \in G$ and $xz = yz$, then $x = y$. Similarly, $zx = zy$ implies $x = y$.

Exercise 1.4. Show that the inverse element of a given element is unique. Thus we can write x^{-1} for the inverse of x without ambiguity.

Why these axioms? The symmetries of a given object form a group under composition, and the axioms capture the general properties of such a composition law. Any object has at least one symmetry, namely the identity transformation, which does nothing at all. Any symmetry of a given object can be undone or reversed, whence the existence of inverses. Associativity is the most subtle condition: it says that the composition of several symmetries (in a given order) is well-defined regardless of how we evaluate the composition. Said more formally, we can move parentheses around freely, so in particular the expression $x_1 \cdots x_n$ makes sense for a finite collection $x_1, \cdots, x_n \in G$.

A fourth axiom which might seem natural is commutativity, which says that any $x, y \in G$ *commute*, meaning $xy = yx$. Groups which have this property are called *abelian*. Abelian groups are in many ways easier to understand than nonabelian groups.

Example 1.5. The symmetry group of a square in the Euclidean (a.k.a Cartesian) plane is called the 4^{th} *dihedral group* and denoted by D_4. For convenience we assume the square is centered at the origin with its sides parallel with the x- and y-axes. The elements of D_4 are as follows:

- the identity (i.e. rotation through 0 radians),
- three nontrivial rotations, through $\frac{\pi}{2}$, π, and $\frac{3\pi}{2}$ radians,

- four reflections, over the horizontal, vertical, and two diagonal axes.

Thus D_4 has eight elements, and for this reason it is sometimes denoted by D_8. Composition in the dihedral group is as follows. Two rotations by θ_1 and θ_2 compose to the rotation by $\theta_1 + \theta_2$ independent of the order in which they are composed, i.e. two rotations commute. Any reflection composed with itself is the identity: such a symmetry is called an *involution*. A rotation composed with a reflection is a reflection, and two reflections compose to a rotation.

Let's be a little more precise by introducing some notation. Write r for rotation through $\frac{\pi}{2}$ and s for reflection over the x-axis. We denote the identity in this group by 1 (as we often will when the notation is "multiplicative"). Keep in mind that composition is written right to left, to agree with the usual convention for composition of functions. The other nontrivial rotations are r^2 and r^3, which are the rotations through π and $\frac{3\pi}{2}$ respectively. As for the remaining reflections, rs is reflection over the diagonal $y = x$, r^2s is reflection over the y-axis, and r^3s is reflection over the diagonal $y = -x$.

Similarly, we can consider the n^{th} *dihedral group* D_n, which is the group of symmetries of a regular n-gon. For convenience, we place the n-gon with its center at the origin (of the Euclidean plane) so that the x-axis passes through the midpoint of at least one side. Write r for rotation through $2\pi/n$ and s for reflection over the x-axis. Then the elements of D_n are the rotations $1, r, \cdots, r^{n-1}$ and the reflections $s, rs, r^2s, \cdots, r^{n-1}s$.

We mentioned that any two rotations commute, but reflections generally do not commute with rotations or other reflections. Thus D_n is nonabelian (for $n \geq 3$). For example, in D_4 we saw that rs is reflection over $y = x$, but sr is reflection over $y = -x$. One shows that in D_n we have $sr = r^{-1}s = r^{n-1}s$, which allows us to "reduce" any string of r's and s's into an expression r^is^j, with $0 \leq i < n$ and $j = 0, 1$.

Example 1.6. Let X be any set. Then the set of permutations of X, i.e. bijections $X \to X$, forms a group under composition, called the *symmetric group on* X. When $X = \{1, 2, \cdots, n\}$ we denote this group by S_n. Counting permutations, we find that S_n has $n!$ elements, which are most efficiently written in *cycle notation*. Before we give the general algorithm: the cycle notation for $\sigma \in S_3$ given by $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ is (123). The cycle notation for $\sigma \in S_4$ given by $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 3$ is (12)(34).

In general, given $\sigma \in S_n$ we proceed as follows. If σ is not the identity, then there is a smallest $1 \leq m_1 \leq n$ not fixed by σ, i.e. $\sigma(m_1) \neq m_1$. Consider the list $m_1, \sigma(m_1), \sigma^2(m_1), \cdots$. Since one cannot fit infinitely many pigeons into finitely many holes, there exist $i \geq j \geq 0$ such that $\sigma^i(m_1) = \sigma^j(m_1)$, whence $\sigma^{i-j}(m_1) = m_1$. Letting $r_1 = i - j$, the list above now has the form $m_1, \sigma(m_1), \sigma^2(m_1), \cdots, \sigma^{r_1-1}(m_1)$. This becomes the first cycle in our expression for σ:

$$(m_1\sigma(m_1)\sigma^2(m_1)\cdots\sigma^{r_1-1}(m_1)).$$

We call r_1 the *length* of this cycle. If all $1 \leq m \leq n$ are either contained in this cycle or fixed by σ, then we are done and σ itself is a cycle. Otherwise there is a smallest $1 \leq m_2 \leq n$ which does not appear in the cycle above and is not fixed by σ. By the same considerations we obtain another cycle

$$(m_2\sigma(m_2)\sigma^2(m_2)\cdots\sigma^{r_2-1}(m_2)).$$

Repeat the algorithm until all $1 \leq m \leq n$ are either fixed by σ or appear in a cycle. Then compose all the cycles to obtain the cycle notation for σ. Note that the order in which these cycles are composed is irrelevant, since they are pairwise disjoint and therefore commute.

Cycles which are not disjoint need not commute, however. For example, in S_3 we have

$$(12)(23) = (123) \neq (132) = (23)(12).$$

So S_n is nonabelian (for $n \geq 3$).

Permutations of the form (ij) are called *transpositions*. It is not hard to see that any permutation can be written as a composition of transpositions (which will generally not be pairwise disjoint).

Example 1.7. The integers $\mathbb{Z}$ form an abelian group under addition. Although we will mostly work with finite groups, the integers are a very important example of an infinite group.

The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ all form abelian groups under addition as well. These are examples of fields, which means that $\mathbb{Q}^\times$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$ are abelian groups under multiplication.

Example 1.8. Fix $n \geq 1$ and consider the n^{th} *roots of unity* $\mu_n \subset \mathbb{C}^\times$, i.e. those $\zeta \in \mathbb{C}^\times$ satisfying $\zeta^n = 1$, which form an abelian group under multiplication. Note that μ_n has n elements, namely

$$\mu_n = \{1, e^{2\pi i/n}, e^{4\pi i/n}, \cdots, e^{2\pi ki/n}, \cdots, e^{2\pi(n-1)i/n}\}.$$

Example 1.9. Let F be $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or any other field. Then we denote by $\mathrm{GL}_2(F)$ those 2×2 matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

satisfying $ad - bc \neq 0$. For matrices in $\mathrm{GL}_2(F)$ we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

so they form a group under matrix multiplication, called the 2^{nd} *general linear group* over F. More generally, the n^{th} *general linear group* $\mathrm{GL}_n(F)$ consists of invertible $n \times n$ matrices (equivalently, matrices with nonzero determinant).

Exercise 1.10. Show that $\mathrm{GL}_2(F)$ is nonabelian.

Example 1.11. Recall that there are five regular polyhedra in three-dimensional Euclidean space, called the Platonic solids. They are the tetrahedron, cube, octahedron, dodecahedron, and icosahedron. Each of them has an associated symmetry group, which is finite and nonabelian.

Here are a couple of elementary constructions to produce new groups from old ones.

Example 1.12. For any group G, the *opposite group* G^{op} has the same underlying set but with the opposite composition law, i.e. $x \cdot y = yx$. Actually G^{op} is isomorphic to G under inversion $g \mapsto g^{-1}$.

Example 1.13. If G and H are two groups, their *direct product* $G \times H$ is the direct product of the underlying sets with the group operation

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

Similarly, one can define the direct product of an arbitrary collection of groups. If the groups are abelian we sometimes call this operation direct sum and denote it by $\oplus$.

Let G be a group and fix $x \in G$. If there does not exist $n \geq 1$ such that $x^n = 1$, then we say that x has *infinite order*. If such an n does exist, then the minimal $n \geq 1$ with $x^n = 1$ is called the *order* of x. Note that if x has infinite order, then G is infinite. This is because in that case the list $1, x, x^2, \cdots$ contains no repetitions: if $x^i = x^j$ then $x^{i-j} = 1$, whence $i = j$.

Example 1.14. In D_4, the identity has order 1 (as always), r and r^3 have order 4, and r^2, s, rs, r^2s, and r^3s have order 2. Note that the order of every element divides the size of the group; we will see that this is true in any finite group.

Example 1.15. In S_n, a cycle of length r has order r. If a permutation is written as a composition of disjoint cycles (this is always possible), its order is the least common multiple of the lengths of the cycles.

Example 1.16. An element of μ_n of order n is called a primitive n^{th} root of unity.

Exercise 1.17. If $x \in G$ has order $n \geq 1$, show the order of x^m is $n/\gcd(m, n)$.

Exercise 1.18. If $x, y \in G$, show that xy and yx have the same order.

2 Homomorphisms and subgroups

In mathematics, and especially in algebra, it is as important to study the relations between objects as the objects themselves. These relations are generally called "morphisms." The point of view of category theory is that in some sense the morphisms carry *all* information about the objects. Morphisms between groups (and most algebraic structures) are called homomorphisms.

Definition 2.1. Let G and H be groups. A *homomorphism* from G to H is a map $\varphi : G \to H$ satisfying $\varphi(xy) = \varphi(x)\varphi(y)$ for any $x, y \in G$. An *isomorphism* is a bijective homomorphism. When $G = H$ a homomorphism $\varphi : G \to G$ is called an *endomorphism* of G, or an *automorphism* if φ is also an isomorphism.

In words, a group homomorphism is a map which respects the group structures of its domain and target. An isomorphism $\varphi : G \to H$ is a way of identifying G and H with each other, so that from the point of view of group theory they are indistiguishable. Isomorphic groups can only differ in their names and the labeling of their elements.

Observe that the automorphisms of a given group G form a group under composition, which we will denote by $\mathrm{Aut}(G)$.

Exercise 2.2. Show that the bijection $G \to G$ given by $g \mapsto g^{-1}$ is an automorphism of G if and only if G is abelian.

Exercise 2.3. Show that a homomorphism $G \to H_1 \times H_2$ is the same as a pair of homomorphisms $G \to H_1$, $G \to H_2$.

Note that the map $G \to H$ which sends all of G to the identity of H is a homomorphism, called the trivial homomorphism.

Exercise 2.4. Check that the composition of two homomorphisms is a homomorphism, and that the inverse of an isomorphism is also a homomorphism (hence an isomorphism). Show that if $\varphi : G \to H$ is a homomorphism then $\varphi(x^{-1}) = \varphi(x)^{-1}$ for any $x \in G$.

Exercise 2.5. If $\varphi : G \to H$ is a homomorphism and $x \in G$ has finite order, show that the order of $\varphi(g)$ divides the order of g.

Now we give some examples of homomorphisms.

Example 2.6. The *sign character* is a homomorphism $\mathrm{sgn} : S_n \to \mu_2$ is defined as follows. For a transposition $(ij) \in S_n$ we define $\mathrm{sgn}((ij)) = -1$. Any permutation can be written (non-uniquely) as a composition of transpositions, which allows us to define sgn on all of S_n. Although the expression of a permutation as a composition of transpositions is not unique, the parity of the number of transpositions is well-defined, so sgn is well-defined also. If $\mathrm{sgn}(\sigma) = 1$ we call σ *even*, and if $\mathrm{sgn}(\sigma) = -1$ then σ is *odd*.

Example 2.7. For any field F the determinant $\det : \mathrm{GL}_n(F) \to F^\times$ is a homomorphism: it is a standard fact from linear algebra that for any $n \times n$ matrices A and B we have $\det(AB) = \det(A)\det(B)$.

Example 2.8. Any $\sigma \in S_n$ determines a *permutation matrix* by permuting the columns of the identity matrix. One checks that the resulting map $S_n \to \mathrm{GL}_n(F)$ is an injective homomorphism. This is our first example of a representation! In fact, the composition

$$S_n \longrightarrow \mathrm{GL}_n(F) \xrightarrow{\det} F^\times$$

lands in μ_2 and is equal to sgn, as long as the characteristic of F is not 2 (i.e. $1 \neq -1$).

Example 2.9. It is a standard fact from analysis that the map $f : \mathbb{R} \to \mathbb{C}^\times$ given by $f(x) = e^{ix}$ is a homomorphism, where $\mathbb{R}$ is a group under addition and $\mathbb{C}^\times$ is a group under multiplication.

Next we discuss subgroups, which are basically the same as injective group homomorphisms respectively.

Definition 2.10. A *subgroup* of a group G is a subset $H \subset G$ which is closed under the group operation and is itself a group. A subgroup $H \subset G$ is called *normal* provided that for any $h \in H$ and $g \in G$ we have $ghg^{-1} \in H$.

Less concisely, a subset $H \subset G$ is a subgroup provided that

- for any $x, y \in H$ we have $xy \in H$,
- $1 \in H$,
- if $x \in H$ then $x^{-1} \in H$.

The significance of normality will be explained shortly.

Exercise 2.11. Check that the intersection of a collection of subgroups is a subgroup, and that the intersection of a collection of normal subgroups is normal.

Notice that if H is a subgroup, the inclusion map $H \to G$ is a homomorphism.

Example 2.12. The rotations $\{1, r, r^2, \cdots, r^{n-1}\} \subset D_n$ form a subgroup. This subgroup is normal, because for any $0 \leq k < n$ we have

$$sr^k s^{-1} = srs = r^{n-k},$$

and similarly for other reflections. On the other hand, the subgroup $\{1, s\}$ is not normal, because for instance $rsr^{-1} = r^2 s$.

Exercise 2.13. The *center* of a group G is the subset

$$\{z \in G \mid zg = gz\}$$

consisting of elements which commute with all elements of G. Check that the center of a group is a normal subgroup.

Exercise 2.14. Is the union of two subgroups always a subgroup?

Exercise 2.15. Show that for any group homomorphism $\varphi : H \to G$, the image $\varphi(H)$ is a subgroup of G.

Actually, a homomorphism determines a subgroup of its domain as well.

Definition 2.16. Let $\varphi : G \to H$ be a group homomorphism. Then the *kernel* of φ is the subgroup of G defined by

$$\ker \varphi := \{g \in G \mid \varphi(g) = 1\}.$$

Intuitively, the kernel is the "information lost" by applying the homomorphism.

Exercise 2.17. Show that $\ker \varphi$ is a normal subgroup of G.

Exercise 2.18. Show that a homomorphism $\varphi : G \to H$ is injective if and only if $\ker \varphi$ is trivial.

When we introduce quotient groups, we will see that the converse is true: any normal subgroup is the kernel of some homomorphism.

Exercise 2.19. Must the image of a homomorphism be normal?

Example 2.20. The kernel of $\mathrm{sgn} : S_n \to \mu_2$ is called the *alternating group* A_n. So A_n consists of all the even permutations of $\{1, 2, \cdots, n\}$.

Example 2.21. The kernel of $\det : \mathrm{GL}_n(F) \to F^\times$ is the n^{th} *special linear group* $\mathrm{SL}_n(F)$, which consists of all $n \times n$ matrices with determinant 1.

Exercise 2.22. Determine the kernel and image of the homomorphism f from Example 2.9.

Exercise 2.23. Find all the subgroups of S_3 and determine whether each is normal.

3 Group actions and conjugacy classes

If we are given an abstract group G, we should ask what kind of object it is the symmetry group of. The simplest symmetries are permutations of a set X, and if elements of G permute X then we say that G acts on X. Since the full group of symmetries is $\mathrm{Sym}(X)$, we arrive at the following definition.

Definition 3.1. A *left (respectively right) action* of G on X is a homomorphism $G \to \mathrm{Sym}(X)$ (respectively $G^{\mathrm{op}} \to \mathrm{Sym}(X)$). We call X a *left (respectively right) G-set*.

A left action $\varphi : G \to \mathrm{Sym}(X)$ is determined by the *action map* $\alpha : G \times X \to X$ defined by

$$g \cdot x := \alpha(g, x) = \varphi(g)(x).$$

Conversely, given an action map such that $x \mapsto g \cdot x$ is bijective for all $g \in G$ and

$$g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x,$$

the formula $\varphi(g)(x) = g \cdot x$ defines a homomorphism $\varphi : G \to \mathrm{Sym}(X)$. In the case of a right action, the action map $\alpha : X \times G \to X$ is written as $x \cdot g := \alpha(x, g)$.

A left action of G on X determines a right action by the formula $x \cdot g := g^{-1} \cdot x$, and similarly inversion makes a right action into a left one (this is because inversion is an isomorphism $G^{\mathrm{op}} \xrightarrow{\sim} G$).

Any $x \in X$ determines a *stabilizer subgroup*

$$G_x := \{g \in G \mid g \cdot x = x\}$$

(one checks that G_x is actually a subgroup of G). If $G_x = 1$ for all $x \in X$, we say that the action is *free*.

If G acts on two sets X and Y (on the left, say), a map $f : X \to Y$ is called *G-equivariant* provided that $f(g \cdot x) = g \cdot f(x)$ for all $g \in G$ and $x \in X$.

Exercise 3.2. Show that the inverse of a bijective G-equivariant map is G-equivariant.

If $\sim$ is an equivalence relation on X, recall that the *quotient set* $X/\!\sim$ is the set of equivalence classes for $\sim$ in X. A right (respectively left) G-action on X determines an equivalence relation on X, where we declare $x_1 \sim x_2$ provided that there exists $g \in G$ with $x_1 \cdot g = x_2$ (respectively $g \cdot x_1 = x_2$). We denote the corresponding quotient set by X/G (respectively $G\backslash X$).

An equivalence class in $G\backslash X$ is called a *G-orbit*, so X is the disjoint union of the orbits. For any $x \in X$ we denote the orbit it belongs to by $G \cdot x$. If X consists of a single orbit then we call the action *transitive*.

Example 3.3. The symmetric group $\mathrm{Sym}(X)$ acts on X on the left. This action is clearly transitive.

Example 3.4. The dihedral group D_n acts (transitively) on the set of vertices of a regular n-gon, which we label with the numbers $1, 2, \cdots, n$. This means we have a homomorphism $D_n \to S_n$, which is injective because a symmetry of the n-gon is determined by what it does to the vertices. When $n = 4$ and the vertices are labeled appropriately this homomorphism sends $r \mapsto (1234)$ and $s \mapsto (12)(34)$. Observe that the stabilizer of any vertex has two elements, namely the identity and reflection over the axis of symmetry which passes through that vertex.

Notice that $D_3 \to S_3$ is actually an isomorphism, which is to say any permutation of the vertices of an equilateral triangle comes from a symmetry of the triangle. On the other hand, if $n > 3$ then $D_n \to S_n$ is not surjective, because the image does not contain any transposition.

This picture is unchanged (up to relabeling) if we use the action of D_n on the edges of the n-gon.

Exercise 3.5. Consider the action of D_4 on the square. What is the stabilizer of a vertex? An edge?

Exercise 3.6. Describe the stabilizer in S_n of a fixed $1 \leq m \leq n$.

Fix a subgroup $H \subset G$ and consider the action of H on G by right (respectively left) translations, meaning $g \cdot h = gh$ (respectively $g \cdot h = gh$) for $g \in G$, $h \in H$. The elements of the quotient set G/H (respectively $H\backslash G$), i.e. the H-orbits in G, are called *left (respectively right) cosets*. Any left coset has the form

$$gH := \{gh \mid h \in H\}$$

for some $g \in G$, and likewise a right coset has the form Hg.

Note that G acts on G/H by left translations. The action is transitive, and the stabilizer of gH is gHg^{-1}. The following result says that any G-orbit can be identified with a coset space in a G-equivariant way.

Proposition 3.7 (Orbit-stabilizer theorem)**.** *If X is a left G-set and $x \in X$, the map $g \mapsto g \cdot x$ induces a G-equivariant bijection $G/G_x \tilde{\to} G \cdot x$.*

Proof. First we must check that $g \mapsto g \cdot x$ descends to a well-defined map $G/G_x \to G \cdot x$. This is because if $h \in G_x$, then

$$gh \mapsto (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x.$$

Now we claim the map $g \cdot x \mapsto gG_x$ is a well-defined inverse $G \cdot x \to G/G_x$. To see that it is well-defined, observe that if $g_1 \cdot x = g_2 \cdot x$ then $g_2^{-1} g_1 \in G_x$, and consequently $g_1 G_x = g_2 G_x$. It is clear that this is the desired inverse and that both maps are G-equivariant.

□

There is another natural action of G on itself (other than translations), namely the *conjugation action*

$$g \cdot x = gxg^{-1}$$

for $g, x \in G$. Observe that conjugation by a fixed $g \in G$ is a group automorphism, since

$$gxyg^{-1} = gxg^{-1}gyg^{-1}.$$

Thus conjugation determines a homomorphism $G \to \mathrm{Aut}(G)$. The orbits of the conjugation action are called *conjugacy classes*, and the stabilizer of an element $x \in G$ under conjugation is the *centralizer* C_x consisting all of elements of G which commute with x. Proposition 3.7 tells us that the conjugacy class of x is G-equivariantly isomorphic to G/C_x.

Note that the center of G is the set of $x \in G$ such that $C_x = G$, or equivalently such that the conjugacy class of x is $\{x\}$. In particular, the conjugation action of an abelian group is trivial.

Example 3.8. Let us describe the conjugacy classes in S_3. As always, the conjugacy class of the identity is $\{1\}$. One nontrivial conjugacy class is the transpositions

$$\{(12), (23), (13)\}.$$

The other consists of the 3-cycles

$$\{(123), (132)\}.$$

Notice that the cardinality of each conjugacy class divides the cardinality 6 of S_3, which we will see is true in general.

More generally, conjugacy classes in S_n correspond to *cycle types*. These are the ways in which permutations decompose into disjoint cycles. For example, representatives of the conjugacy classes in S_4 are given by 1, (12), (123), (1234), and (12)(34).

Example 3.9. Two matrices in $\mathrm{GL}_n(F)$ which are conjugate (i.e. belong to the same conjugacy class) are sometimes called *similar*. The theory of Jordan decompositions provides representatives for the conjugacy classes in $\mathrm{GL}_n(\mathbb{C})$.

Exercise 3.10. Compute the conjugacy classes in D_4. Verify that their cardinalities divide $8 = \#D_4$.

4 Quotient groups and the isomorphism theorem

One might ask whether the set G/H of left cosets can be given the structure of a group. After all, there is a natural formula for an operation on cosets.

Proposition 4.1. *The following are equivalent:*

(i) H is normal,

(ii) $G/H = H\backslash G$,

(iii) the formula $(xH)(yH) = xyH$ *is a well-defined operation on* G/H,

(iv) the formula $(Hx)(Hy) = Hxy$ *is a well-defined operation on* $H\backslash G$.

Proof. Clearly (i) implies (ii), since H is normal if and only if $xHx^{-1} = H$ for any $x \in G$, i.e. $xH = Hx$. Suppose (ii) holds, so for any left coset xH there exists $y \in G$ with $xH = Hy$. Note that $x \in Hx = Hy$ implies that $Hx = Hy$, so $xH = Hy = Hx$ and therefore H is normal.

Now we prove that (i) implies (iii). Suppose that $x_1H = x_2H$ and $y_1H = y_2H$, so we must show that $x_1y_1H = x_2y_2H$, i.e. $x_1y_1y_2^{-1}x_2^{-1} \in H$. We know $y_1y_2^{-1} \in H$, and using normality we get

$$x_1y_1y_2^{-1}x_1^{-1} \in H.$$

Now just multiply on the right by $x_1x_2^{-1} \in H$.

Next we show that (iii) implies (i). Fix $g \in G$ and $h \in H$ and observe that

$$ghg^{-1}H = (ghH)(g^{-1}H) = (gH)(g^{-1}H) = gg^{-1}H = H,$$

so $ghg^{-1} \in H$ as desired. The equivalence of (iv) and (i) is similar.

□

For $N \subset G$ normal, the operation on G/N from the proposition satisfies the group axioms because it comes from the group operation on G. The quotient map $\pi : G \to G/N$, given by $\pi(g) = gN$, has kernel N. We saw in Section 2 that the kernel of a homomorphism is normal, and the quotient construction supplies the converse: any normal subgroup is the kernel of some homomorphism, namely the quotient map.

Example 4.2. For any $n \geq 1$, the cosets in $\mathbb{Z}/n\mathbb{Z}$ are called congruence classes of integers modulo n. These form a group under addition beause $\mathbb{Z}$ is abelian, which implies that all of its subgroups are normal.

This quotient map $\pi : G \to G/N$ is characterized by a universal property.

Proposition 4.3. *If* $\varphi : G \to H$ *is a homomorphism satisfying* $N \subset \ker\varphi$*, then there is a unique homomorphism* $\rho : G/N \to H$ *satisfying* $\rho \circ \pi = \varphi$.

Proof. Put $\rho(xN) := \varphi(x)$, which is well-defined because $xN = yN$ implies

$$\varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}) = 1,$$

i.e. $\varphi(x) = \varphi(y)$. If $\rho' : G/N \to H$ satisfies $\rho' \circ \pi = \varphi$, then

$$\rho'(xN) = \rho'(\pi(x)) = \varphi(x) = \rho(xN).$$

□

Exercise 4.4. Prove that if $\pi' : G \to Q$ is another homomorphism with the the universal property in Proposition 4.3, then there is a unique isomorphism $\rho : G/N \tilde{\to} Q$ satisfying $\rho \circ \pi = \pi'$.

Now we come to the isomorphism theorem (sometimes called the first isomorphism theorem), which is fundamental to everything that follows. It says that any group homomorphism can be canonically written as the composition of a surjection, an isomorphism, and an injection.

Proposition 4.5 (The isomorphism theorem)**.** *Let* $\varphi : G \to H$ *be a group homomorphism. Denote by* $\pi : G \to G/\ker\varphi$ *for the quotient map and* $\iota : \operatorname{im}\varphi \to H$ *the inclusion. There is a unique isomorphism* $\varphi' : G/\ker\varphi \tilde{\to} \operatorname{im}\varphi$ *satisfying* $\iota \circ \varphi' \circ \pi = \varphi$.

Proof. Clearly φ factorizes uniquely into $\iota \circ \rho = \varphi$, where $\rho : G \to \operatorname{im}\varphi$. Since $\ker\rho = \ker\varphi$, the universal property of π says that there is a unique homomorphism $\varphi' : G/N \to \operatorname{im}\varphi$ satisfying $\varphi' \circ \pi = \rho$. This relation implies that φ' is surjective because ρ is, and also that $\ker\varphi'$ is trivial, so φ' is an isomorphism.

□

Example 4.6. The sign homomorphism factors through an isomorphism $S_n/A_n \tilde{\to} \mu_2 = \{\pm 1\}$.

Example 4.7. The determinant factors through an isomorphism $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \tilde{\to} F^\times$.

Exercise 4.8. Produce an isomorphism $\mathbb{C}^\times/\mu_n \tilde{\to} \mathbb{C}^\times$.

Exercise 4.9. Identify the quotient $\mathbb{C}^\times/S^1$, where S^1 is the *circle group* consisting of complex numbers of absolute value 1.

Exercise 4.10. Prove that $G \times 1$ is a normal subgroup of $G \times H$, isomorphic to G, and produce an isomorphism $(G \times H)/(G \times 1) \tilde{\to} H$.

5 Some loose ends

The *index* of a subgroup $H \subset G$, often written $|G : H|$, is the cardinality of the set G/H (which is the same as the cardinality of $H\backslash G$). In particular, if G/H is finite one says that H has finite index in G. If G is finite then every subgroup has finite index. Infinite groups may have subgroups of finite index, e.g. for $n \geq 1$ the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ has index n.

Up to this point everything we have said applies to infinite as well as finite groups. The following result is one of the most important basic facts about finite groups.

Proposition 5.1 (Lagrange's theorem)**.** *If H is a subgroup of a finite group G then*

$$|G : H| \cdot \#H = \#G.$$

In particular $|G : H|$ and $\#H$ divide $\#G$.

Proof. For any $g \in G$, the map $H \to gH$ which sends $h \mapsto gh$ is bijective with inverse $x \mapsto g^{-1}x$. Thus for H finite we have $\#(gH) = \#H$, i.e. all cosets have the same cardinality as H. The proposition follows immediately.

□

An immediate corollary is the analogue for finite groups of the rank-nullity theorem from linear algebra.

Corollary 5.1.1. *If $\varphi : G \to H$ is a homomorphism and G is finite then*

$$\#\ker\varphi \cdot \#\operatorname{im}\varphi = \#G.$$

Proof. Combine Propositions 4.5 and 5.1.

□

Corollary 5.1.2. *Let G be a finite group, X a left G-set, and $x \in X$. Then*

$$\#G_x \cdot (\#G \cdot x) = \#G.$$

In particular $\#G \cdot x$ is finite and divides $\#G$.

Proof. Combine Propositions 3.7 and 5.1.

□

Example 5.2. Corollary 5.1.2 implies that the cardinality of any conjugacy class in a finite group G divides $\#G$ (the former is the index of the centralizer of any representative for the conjugacy class).

The previous example has an interesting consequence. For a fixed prime number p, a *p-group* is a finite group with p^n elements for some $n \geq 1$.

Proposition 5.3. *A p-group has nontrivial center.*

Proof. Say $\#G = p^n$. Suppose the center of G is trivial, or equivalently the only conjugacy class in G with one element is $\{1\}$. The rest of the conjugacy classes must have cardinality dividing p^n, so their cardinalities are divisible by p. Since the conjugacy classes partition G, we have $p^n = 1 + pm$ for some $m \geq 1$, a contradiction.

□

Let G be a group and $S \subset G$ a subset. The subgroup $\langle S \rangle$ *generated by* S is the intersection of all subgroups of G which contain S. Thus $\langle S \rangle$ is the unique subgroup of G with the property that if $H \subset G$ is a subgroup containing S, then $\langle S \rangle \subset H$. It is not hard to see that $\langle S \rangle$ consists of all (strings of) compositions in G of elements of S and and their inverses, including the empty string, which is the identity. If $S = \{x\}$ has a single element, we write $\langle x \rangle$ instead of $\langle \{x\} \rangle$.

Example 5.4. The *commutator subgroup* $[G, G] \subset G$ is the subgroup generated by the commutators

$$[x, y] := x^{-1}y^{-1}xy$$

for all $x, y \in G$. Observe that $[G, G]$ is normal because

$$g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}].$$

The quotient $G^{\mathrm{ab}} := G/[G, G]$ is called the *abelianization* of G.

Exercise 5.5. Let $\pi : G \to G^{\mathrm{ab}}$ be the quotient map and suppose $\varphi : G \to A$ is a homomorphism, where A is an abelian group. Show that there exists a unique homomorphism $\varphi' : G^{\mathrm{ab}} \to A$ with the property that $\varphi' \circ \pi = \varphi$. As with all universal properties, this one characterizes π.

Exercise 5.6. Check that the order of an element $x \in G$ is the cardinality of $\langle x \rangle$.

Definition 5.7. A group G is *cyclic* provided that it is generated by a single element $x \in G$, i.e. $G = \langle x \rangle$.

Cyclic groups are classified by their cardinality.

Proposition 5.8. *Any infinite cyclic group is isomorphic to* $\mathbb{Z}$. *A finite cyclic group with* n *elements is isomorphic to* $\mathbb{Z}/n\mathbb{Z}$.

Proof. Let G be cyclic and fix a generator $x \in G$. Then the homomorphism $\mathbb{Z} \to G$ which sends $k \mapsto x^k$ is surjective, because the image is a subgroup containing x. The kernel of this homomorphism, being a subgroup of $\mathbb{Z}$, has the form $n\mathbb{Z}$ for some $n \geq 0$. If $n = 0$ then $\mathbb{Z} \tilde{\to} G$, and otherwise $\mathbb{Z}/n\mathbb{Z} \tilde{\to} G$ by Proposition 4.5.

□

Example 5.9. For any $n \geq 1$, a primitive n^{th} root of unity $\zeta \in \mu_n$ determines an isomorphism $\mathbb{Z}/n\mathbb{Z} \tilde{\to} \mu_n$, namely $k \mapsto \zeta^k$.

Exercise 5.10. Let G be a cyclic group with $n \geq 1$ elements. Show that every subgroup of G is cyclic, and that if m divides n there is a subgroup of G with m elements.

Clearly a cyclic group is abelian. The next result says that any finite abelian group is a sum of cyclic groups.

Theorem 5.11. *A finite abelian group is isomorphic to*

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z}$$

for some $n_1, \cdots, n_r \geq 2$.

Proof. This is a special case of Theorem 12.6.4 in Artin's *Algebra*.

□

Exercise 5.12. Prove that for $m, n \geq 2$, the natural homomorphism $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is an isomorphism if and only if m and n are relatively prime.

Next we introduce simple groups. They will not be very important for us but need to be included for cultural reasons.

A group G is called *simple* provided that its only normal subgroups are the trivial subgroup and G itself.

Exercise 5.13. Prove that a simple abelian group is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime number p (in particular, is finite).

Simple groups are important because they are the "building blocks" of all other groups. Notice that a group is simple if and only if its only quotients are the trivial one and G itself.

Finite simple groups have been completely classified, although this classification is spread out over thousands of pages. Here is a nonabelian example (actually infinitely many examples).

Theorem 5.14. *For any $n \geq 5$, the alternating group A_n is simple.*

Proof. This is Theorem 4.6.25 in Dummit and Foote's *Abstract Algebra*.

□

Exercise 5.15. Show that A_4 is not simple.

In fact, the smallest nonabelian simple group is A_5, which has 60 elements.

How are other groups built out of simple groups? One way is by taking direct products. There is a more general way of taking products which produces more examples.

Let G and H be groups and suppose H acts on G on the left by group automorphisms, i.e. we are given a homomorphism $H \to \mathrm{Aut}(G)$.

Definition 5.16. The *semidirect product* $G \rtimes H$ has the same underlying set as $G \times H$, but with the group operation defined by

$$(g_1, h_1)(g_2, h_2) = (g_1(h_1 \cdot g_2), h_1 h_2).$$

Exercise 5.17. Check that $G \rtimes H$ is a group. Show that $G \times 1 \subset G \rtimes H$ is a normal subgroup isomorphic to G, and produce an isomorphism $(G \rtimes H)/(G \times 1) \tilde{\to} H$.

Exercise 5.18. Let G be a group with a normal subgroup $N \subset G$ and put $H = G/N$. Write $\pi : G \to H$ for the projection and suppose there exists $\rho : H \to G$ such that $\pi \circ \rho = \mathrm{id}_H$ (we say that ρ is a *splitting* of π). Exhibit an isomorphism $N \rtimes H \tilde{\to} G$.

Exercise 5.19. Write down an isomorphism $A_n \rtimes \mu_2 \tilde{\to} S_n$. In particular, give the action of μ_2 on A_n used to define the semidirect product. Hint: this construction is noncanonical in the sense that both the action and the isomorphism depend on a choice of transposition.