Appendix A

Group theory

Joshua R. Davis, jdavis @ carleton.edu, Carleton College, Math 354
This is a whirlwind tour of basic group theory, to help topology students who are new to the subject.

A.1 Groups

In a sense, group theory exists to answer the simplest possible algebra problem: Given a and b, find x such that $ax = b$. Here is the solution, with careful attention paid to the algebraic rules being used:

$$\begin{aligned} & b &=& ax & \\ \Rightarrow \quad & a^{-1}b &=& a^{-1}(ax) & \text{(because inverses exist)} \\ & &=& (a^{-1}a)x & \text{(because multiplication is associative)} \\ & &=& 1x & \text{(by the meaning of inverses)} \\ & &=& x & \text{(by the meaning of 1).} \end{aligned}$$

This argument works as long as a, b, and x are understood to be elements of $\mathbb{R} - \{0\}$. It also works if they are elements of $\mathbb{Q} - \{0\}$ or $\mathbb{C} - \{0\}$. That's because all of these sets form groups under multiplication.

Definition A.1.1. *A **group** is a set G equipped with a function $G \times G \to G$, usually written as a multiplication operation $(g, h) \mapsto gh$, such that:*

1. *for all $g, h, j \in G$, $g(hj) = (gh)j$,*
2. *there exists $e \in G$, called the **identity**, such that for all $g \in G$, $eg = g = ge$, and*
3. *for all $g \in G$ there exists $g^{-1} \in G$ such that $gg^{-1} = e = g^{-1}g$.*

*If it is also true that $gh = hg$ for all $g, h \in G$, then G is **commutative** (or **Abelian**).*

In the groups $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, and $\mathbb{C} - \{0\}$, the number 1 plays the role of e. These three groups are commutative, but many important groups are not commutative.

Example A.1.2. *Let $\mathrm{GL}(n, \mathbb{R})$ be the set of invertible real $n \times n$ matrices. Let $\mathrm{SL}(n, \mathbb{R})$ be the set of determinant-1 real $n \times n$ matrices. These are both groups under matrix multiplication, with the identity matrix I playing the role of e. These groups are commutative if and only if $n = 1$.*

In all of the foregoing examples, we call the group operation multiplication, and we write it as multiplication. However, in some groups the operation is not called or written as multiplication. Here are three examples where the group operation is addition.

Example A.1.3. *The integers $\mathbb{Z}$ form a group under addition $+$, with 0 playing the role of e and $-a$ playing the role of a^{-1}. Similarly, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under addition. All of these groups are commutative.*

Example A.1.4. *Let V be any vector space, such as $V = \mathbb{R}^n$. So V has an addition operation and a scalar multiplication operation, which obey some axioms. Forget scalar multiplication and the axioms that involve it. Then you get a commutative group under addition, with $\vec{0}$ playing the role of e and $-\vec{v}$ playing the role of $\vec{v}^{-1}$.*

Example A.1.5. *For any integer m, let $\mathbb{Z}/m\mathbb{Z}$ be the set of equivalence classes of integers, where $a \sim b$ if and only if $a-b$ is a multiple of m. Commonly we focus on $m \geq 2$. In those cases, we can conceptualize $\mathbb{Z}/m\mathbb{Z}$ as the set $\{0, 1, \ldots, m-1\}$. This set carries an operation of addition modulo m, under which it is a group. For example, in $\mathbb{Z}/12\mathbb{Z}$, we can compute $8 + 11 \sim 19 \sim 7$. This group is commutative.*

Here are two more examples, where the group operation is neither addition nor multiplication.

Example A.1.6. *Let X be a set, and let $\mathrm{Aut}(X)$ be the set of all bijections $f : X \to X$. Then $\mathrm{Aut}(X)$ is a group under function composition $\circ$. The identity element is the identity function $i : X \to X$. This group is not commutative except in trivial cases.*

Example A.1.7. *If (X, x) is a pointed topological space, then the fundamental group $\pi_1(X, x)$ is a group under concatenation $*$. The identity element is the constant path class $[e_x]$. Some fundamental groups are commutative and some are not.*

Here are a non-example and an exercise.

Example A.1.8. *Consider the cross product $\times$ on three-dimensional vectors, which is defined by*

$$\vec{v} \times \vec{w} = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} \times \begin{bmatrix} w_1 \\ w_2 \\ w_3 \end{bmatrix} = \begin{bmatrix} v_2 w_3 - v_3 w_2 \\ v_3 w_1 - v_1 w_3 \\ v_1 w_2 - v_2 w_1 \end{bmatrix}.$$

It is a function $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, and we think of it as a kind of multiplication, but $\mathbb{R}^3$ is not a group under $\times$. For one thing, $\times$ is not associative. (It instead obeys something called the Jacobi identity.) For another thing, there is no identity element for $\times$. So we can't even talk about inverses.

Exercise A.1.9. *Let G be a group. Prove that there is only one $e \in G$ that satisfies the properties of the identity. Prove that, for each $g \in G$, there is only one $g^{-1} \in G$ that satisfies the properties of the inverse.*

A.2 Homomorphisms

In linear algebra, a vector space is a setting where linear behavior can happen, and a linear transformation is a function that respects that linear structure. In topology, a topological space is a setting where

continuity can be defined, and a continuous function is a function that respects that topological structure. Similarly, in group theory, a group is a setting where (generalized) multiplication can happen, and we need a notion of functions that respect that multiplication.

Definition A.2.1. *Let G and H be groups. A function $f : G \to H$ is a **homomorphism** if, for all $g_1, g_2 \in G$,*

$$f(g_1 g_2) = f(g_1) f(g_2).$$

*That is, computing a product $g_1 g_2 \in G$ and then sending it to $f(g_1 g_2) \in H$ produces the same answer as sending g_1, g_2 to $f(g_1), f(g_2) \in H$ and computing their product there. An **isomorphism** is a bijective homomorphism. Two groups are **isomorphic** if there exists an isomorphism from one to the other.*

One can check that the inverse of an isomorphism is an isomorphism, and the composition of two isomorphisms is an isomorphism. It follows that being isomorphic is an equivalence relation on groups. Two groups that are isomorphic are essentially identical.

Example A.2.2. *The function $\exp : \mathbb{R} \to (0, \infty)$ defined by*

$$\exp(x) = e^x = \sum_{k=0}^{\infty} x^k / k!$$

has the property that $\exp(x + y) = \exp(x) \exp(y)$. Therefore it is a homomorphism from the group $\mathbb{R}$ under addition to the group $\mathbb{R} - \{0\}$ under multiplication. It is injective but not surjective onto $\mathbb{R} - \{0\}$.

Example A.2.3. *For any $m \geq 2$, define a function $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ by $f(k) = e^{i2\pi k/m}$. Notice that*

$$f(k + \ell) = e^{i2\pi(k+\ell)/m} = e^{i2\pi k/m} e^{i2\pi \ell/m} = f(k) f(\ell).$$

It follows that f is a homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to the group $\mathbb{C} - \{0\}$ under multiplication. It is injective and not surjective.

Example A.2.4. *The determinant of $n \times n$ matrices obeys $\det(AB) = \det(A) \det(B)$. It follows that $\det$ is a homomorphism from $\mathrm{GL}(n, \mathbb{R})$ to the group $\mathbb{R} - \{0\}$ under multiplication. It is surjective and not injective.*

Example A.2.5. *For any $n \times n$ real matrix A, there is a corresponding linear transformation $f(A) : \mathbb{R}^n \to \mathbb{R}^n$ defined by $f(A)(\vec{v}) = A\vec{v}$. This correspondence obeys $f(AB) = f(A) \circ f(B)$. It follows that f is a homomorphism from $\mathrm{GL}(n, \mathbb{R})$ to $\mathrm{Aut}(\mathbb{R}^n)$. It is injective and not surjective.*

Here's a non-example.

Example A.2.6. *Consider $f(x) = x^2$ as a function from the group $\mathbb{R}$ under addition to itself. To say that it is a homomorphism is to say that $f(x + y) = f(x) + f(y)$, which is to say that $(x + y)^2 = x^2 + y^2$, which isn't true (although countless algebra novices have wished it to be true).*

A.3 Subgroups

When a group is sitting inside another group in a well-behaved, compatible way, we use the following term of jargon.

Definition A.3.1. *Let G be a group and $H \subseteq G$ any subset. Then H is a **subgroup** of G if the group operation on G, when restricted to H, defines a group operation $H \times H \to H$.*

Concretely, to check that a subset H is a subgroup, you need to check that the product of two elements of H is an element of H, that $e \in H$, and that the inverse of any element of H is an element of H. Here are some examples.

Example A.3.2. *In all of the subset relationships $\mathbb{Q} - \{0\} \subseteq \mathbb{R} - \{0\} \subseteq \mathbb{C} - \{0\}$, the subset is a subgroup of the larger group under multiplication.*

Example A.3.3. *In all of the subset relationships $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, the subset is a subgroup of the larger group under addition.*

Example A.3.4. $\mathrm{SL}(n, \mathbb{R})$ *is a subgroup of* $\mathrm{GL}(n, \mathbb{R})$.

Here are some non-examples and an exercise.

Example A.3.5. *Let X be the set of real $n \times n$ matrices of determinant -1. Then X is a subset of $\mathrm{GL}(n, \mathbb{R})$, but it is not a subgroup. For one thing, the product of two matrices in X has determinant 1 and hence is not in X. For another, $I \notin X$. On the other hand, the inverse of a matrix in X is a matrix in X. So, of the three checks that a subgroup must pass, X fails two and passes one.*

Example A.3.6. *$\mathbb{R}$ is a group under addition, $\mathbb{R} - \{0\}$ is a group under multiplication, and the latter is a subset of the former. But $\mathbb{R} - \{0\}$ is not a subgroup of $\mathbb{R}$, because the group operation on $\mathbb{R} - \{0\}$ is not the restriction of the group operation on $\mathbb{R}$. A subgroup is not just a group sitting inside a larger group; it is a group sitting inside a larger group in a compatible way.*

Example A.3.7. *$\mathbb{Z}/m\mathbb{Z}$ is not a subgroup of $\mathbb{Z}$. If $m \geq 2$ and we think of $\mathbb{Z}/m\mathbb{Z}$ as the set $\{0, 1, \ldots, m-1\}$, then we can conceptualize $\mathbb{Z}/m\mathbb{Z}$ as a subset of $\mathbb{Z}$. However, even then the group operation on $\mathbb{Z}/m\mathbb{Z}$ is not the restriction of the group operation on $\mathbb{Z}$.*

Exercise A.3.8. *Let $f : G \to H$ be a homomorphism. Prove that $f(G)$ is a subgroup of H. If G is commutative, then must $f(G)$ be commutative? What about the converse?*

A.4 Kernels and normal subgroups

In this section, we define two concepts that end up being actually the same concept.

Definition A.4.1. *Let $f : G \to H$ be a homomorphism. Then $f^{-1}(e) \subseteq G$ is the **kernel** of f.*

Example A.4.2. *The kernel of* $\exp : \mathbb{R} \to (0, \infty)$ *is* $\{0\}$. *In general, the identity element is always in the kernel, and a homomorphism is injective if and only if there is nothing else in its kernel.*

Example A.4.3. *The kernel of* $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R} - \{0\}$ *is* $\mathrm{SL}(n, \mathbb{R})$.

Example A.4.4. *Consider the map $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ that sends each k to its equivalence class $[k]$ modulo m. The kernel is $m\mathbb{Z} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$.*

In all of the preceding examples, the kernel is a subgroup of the domain. That is no accident. The kernel is always a subgroup. In fact, the kernel is always a special kind of subgroup, which we define now.

Definition A.4.5. *A subgroup H of G is **normal** if, for all $g \in G$ and $h \in H$, $ghg^{-1} \in H$.*

Theorem A.4.6. *If $f : G \to H$ is a homomorphism, then the kernel of f is a normal subgroup of G.*

Proof. Let $K \subseteq G$ be the kernel of f. We have already mentioned that $e \in K$. If $g_1, g_2 \in K$, then

$$f(g_1 g_2) = f(g_1)f(g_2) = ee = e,$$

so $g_1 g_2 \in K$. If $g \in K$, then

$$f(g^{-1}) = ef(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e) = e.$$

These steps establish that K is a subgroup of G. Finally, let $g \in G$ and $k \in K$. Then

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = e.$$

So $gkg^{-1} \in K$, and K is normal. □

So every kernel is a normal subgroup. In the next section, we essentially prove the converse: Every normal subgroup is a kernel, in a canonical way.

Exercise A.4.7. *Let G be a commutative group. Prove that every subgroup of G is normal.*

A.5 Quotients

It's useful to have some ways to build new groups out of old groups. Here's one way.

Definition A.5.1. *Let H be a normal subgroup of G. Define an equivalence relation on G by declaring that $g_1 \sim g_2$ if $g_1 g_2^{-1} \in H$. Let $[g]$ denote the equivalence class of $g \in G$, and let G/H denote the set of equivalence classes. This G/H is called the **quotient** of G by H. It is pronounced "G mod H".*

Example A.5.2. *What we've been calling $\mathbb{Z}/m\mathbb{Z}$ really is the quotient of the group $\mathbb{Z}$ (under addition) by the normal subgroup $m\mathbb{Z}$.*

Theorem A.5.3. *The quotient G/H is a group under the operation $[g_1][g_2] = [g_1 g_2]$, and the function $f : G \to G/H$ defined by $f(g) = [g]$ is a group homomorphism with kernel H.*

Proof. First we should check that the operation $[g_1][g_2] = [g_1 g_2]$ is well-defined. To that end, suppose that $j_1 \sim g_1$ and $j_2 \sim g_2$. Then $g_2 j_2^{-1} \in H$, so $g_1 g_2 j_2^{-1} g_1^{-1} \in H$ by normality. And $g_1 j_1^{-1} \in H$, so

$$(g_1 g_2 j_2^{-1} g_1^{-1})(g_1 j_1^{-1}) = g_1 g_2 j_2^{-1} j_1^{-1} = (g_1 g_2)(j_1 j_2)^{-1}$$

is also an element of H. Thus $g_1 g_2 \sim j_1 j_2$, and the operation is well-defined.

With well-definedness out of the way, the rest of the proof is easier. It is not difficult to check that G/H is a group under that operation. For example, the identity in G/H is $[e]$, and $[g]^{-1} = [g^{-1}]$, and so on. Also, f is a homomorphism because $f(g_1 g_2) = [g_1 g_2] = [g_1][g_2] = f(g_1)f(g_2)$. Finally, $[g] = [e]$ if and only if $ge^{-1} \in H$, which happens if and only if $g \in H$. So the kernel is H. □

In the preceding proof, it is crucial that H be a normal subgroup. Otherwise, the set of equivalence classes does not inherit a group structure from G in any obvious way.

Exercise A.5.4. *My definition of the quotient G/H is a little unusual. The usual way to define the quotient is like this: For any $g \in G$, define $Hg = \{hg : h \in H\}$; then $g_1 \sim g_2$ if $Hg_1 = Hg_2$. Prove that this new $\sim$ is actually identical to the $\sim$ used above. Does your proof require H to be normal?*

A.6 Miscellany

While we're at it, here's another way to make a new group out of old groups.

Definition A.6.1. *Let G and H be groups. Define an operation $\cdot$ on the Cartesian product set $G \times H$ by*

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

*Then $G \times H$ is the **product** group.*

Example A.6.2. *The product of the group $\mathbb{R}$ (under addition) with itself is the group $\mathbb{R} \times \mathbb{R}$ with group operation $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$. In other words, it is $\mathbb{R}^2$ without scalar multiplication.*

Let's prove one final theorem that ties together several of the ideas in this whirlwind tutorial.

Theorem A.6.3. *Let $f : G \to H$ be a homomorphism with kernel $K \subseteq G$. Then the map $i : G/K \to f(G) \subseteq H$ defined by $i([g]) = f(g)$ is an isomorphism between G/K and $f(G)$.*

Proof. First we should check that i is well-defined. Suppose that $j \sim g$. Then $jg^{-1} \in K$, so

$$e = f(jg^{-1}) = f(j)f(g^{-1}) = f(j)f(g)^{-1}.$$

But inverses are unique (check), so it must be that $f(j) = f(g)$. Thus i is well-defined. Second, i is a homomorphism because

$$i([g_1][g_2]) = i([g_1 g_2]) = f(g_1 g_2) = f(g_1)f(g_2) = i([g_1])i([g_2]).$$

Third, i is surjective onto $f(G)$ because any element of $f(G)$ is of the form $f(g)$ for some $g \in G$, and $i([g]) = f(g)$ for that g. Finally, is i injective? Well, let $[g]$ be an element of the kernel of i. Then $e = i([g]) = f(g)$, so $g \in K$, which means that $[g]$ is the identity element of G/K. Thus i has trivial kernel and is injective. □

Example A.6.4. *The determinant tells us that $\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R})$ isomorphic to $\mathbb{R} - \{0\}$.*

Example A.6.5. *The projection $G \times H \to G$ is a surjective homomorphism with kernel $\{e\} \times H$. Therefore the quotient $(G \times H)/(\{e\} \times H)$ is isomorphic to G.*