MATH 171: Abstract Algebra I

Connor Neely, Fall 2024

* Adapted from David S. Dummit & Richard M. Foote, *Abstract Algebra* (2004) and FA24 Lecture Notes.

1 Groups and Subgroups

1.1 Axioms and Properties

For most of this course, the central object of study will be the group.

Definition: Binary operation

A binary operation on a set G is a function $\star : G \times G \to G$.

- If $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in G$, then we say $\star$ is associative.
- If $a \star b = b \star a$ for all $a, b \in G$, then we say $\star$ is commutative.

For $a, b \in G$ we'll typically write $a \star b$ for $\star(a, b)$.

Definition: Group

A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G such that

- $\star$ is associative,
- there exists an $e \in G$, called an identity, such that $a \star e = e \star a = a$ for all $a \in G$, and
- for each $a \in G$ there is an $a^{-1} \in G$, called an inverse of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

We say the group $(G, \star)$ is commutative (or abelian) if $\star$ is commutative.

We've already encountered many groups in our previous studies! For example, under addition we have $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}/n\mathbb{Z}$ (the integers modulo n), and under multiplication we have $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, and $Z/n\mathbb{Z}^\times$ (where the $\times$ denotes zero-exclusion). These examples help make the following properties a bit more concrete.

Theorem 1.1

If $(G, \star)$ is a group then

(a) the identity of G is unique,

(b) a^{-1} is unique for each $a \in G$,

(c) $(a^{-1})^{-1} = a$,

(d) $(a \star b)^{-1} = b^{-1} \star a^{-1}$, and

(e) for all $a_1, \cdots, a_n \in G$, the value of $a_1 \star \cdots \star a_n$is independent of how the expression is bracketed.

Proof. We prove the first two parts.

(a) Suppose e and e' are both identities. Then we have the chain of equalities

$$e = e \star e' = e'.$$

(b) Suppose some $a \in G$ has two inverses a', a''. Then we have the chain of equalities

$$a' = a' \star e = a' \star (a \star a'') = (a' \star a) \star a'' = a''.$$

Other parts are left as exercises. □

With these properties in mind, we'll make a few notes on notation.

- We read $(G, \star)$ aloud as "G is a group under $\star$". In practice, if the binary operation is self-evident, we'll simply write G to mean $(G, \star)$.
- For a group $(G, \star)$ we'll usually write ab to mean $a \star b$. In the same spirit, we can write a length-n product $x \star \cdots \star x$ as x^n, and $x^{-n} = \left(x^{-1}\right)^n$. (This is called multiplicative notation.)
- When multiplicative notation is being used, we will usually denote the identity of G by 1 and set $x^0 = 1$.

We'll finish off here with a few definitions which will be useful in future discussions.

Definition: Order of an element

Let G be a group and let $x \in G$. The order $|x|$ of x is the smallest $n \in \mathbb{Z}^+$ such that $x^n = 1$.

Definition: Generator

Let G be a group, and let S be a subset of G. We say that S generates G if every element of G can be written as a finite product of elements in S and their inverses.

In this case, S is a set of generators for G and we write $G\langle S\rangle$.

Definition: Presentation

Let G be a group that is generated by S with a set of relations R. G has presentation $\langle S \mid R\rangle$.

1.2 Some Important Groups

Now we'll look at a few different kinds of well-known groups.

Definition: Dihedral group

The dihedral group of order $2n$ is the group D_{2n} of symmetries of a regular n-gon.

In general we'll use $r \in D_{2n}$ to denote clockwise rotation by $2\pi/n$ and $s \in D_{2n}$ for reflection through a fixed line of symmetry. We can get a few nice results from this!

- $D_{2n} = \left\{1, r, r^2, \ldots, r^{n-1}\right\} \cup \left\{s, sr, sr^2, \ldots, sr^{n-1}\right\}$ (where the two sets are disjoint).
- $|r| = n$ and $|s| = 2$.
- $r^i s = sr^{-i}$ for all $i \in \mathbb{Z}$.

Thinking of the elements of D_{2n} as physical transformations is useful. But they're perhaps better understood as *equivalence classes* of physical moves since, for example, r^n is equivalent to r^{2n}.

Definition: Symmetric group

Let Ω be a non-empty set, and let S_Ω be the set of all bijections from Ω to Ω. The set S_Ω forms a group under function composition, and it is called the symmetric group on Ω.

Note that if $\Omega = \{1, 2, \ldots, n\}$ then we write $S_\Omega = S_n$. Permutations on such Ω can be communicated in several different ways—for example, if we had the bijection

$$1 \mapsto 3 \qquad 2 \mapsto 5 \qquad 3 \mapsto 1 \qquad 4 \mapsto 2 \qquad 5 \mapsto 4,$$

then we have the two-line, one-line, and cycle notations, respectively:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{bmatrix}, \qquad \begin{bmatrix} 3 & 5 & 1 & 2 & 4 \end{bmatrix}, \qquad (1\ 3)(2\ 5\ 4).$$

We again have a few important facts about symmetric groups.

- The order of S_n is $n!$ ($|S_n| = n!$).
- S_n is non-abelian for $n \geq 3$, but disjoint cycles always commute.
- The order of a permutation is the least common multiple of the cycle lengths in its decomposition.
- S_n is generated by the adjacent transpositions (the 2-cycles comprised of adjacent elements). The group can also be generated by $\{(1\ 2),\ (1\ 2\ \cdots\ n)\}$.

As a fun fact, S_3 can be used to create a permutation representation of D_6—if we label the vertices of a triangle with 1, 2, and 3, the movements of the vertices are represented by

$$\begin{aligned} e' &\mapsto e & s &\mapsto (2\ 3) \\ r &\mapsto (1\ 2\ 3) & sr &\mapsto (1\ 3) \\ r^2 &\mapsto (1\ 3\ 2) & sr^2 &\mapsto (1\ 2) \end{aligned}$$

Thus S_3 is isomorphic to D_6 ($S_3 \cong D_6$).

Definition: General linear group

For each $n \in \mathbb{Z}^+$ let $GL_n(F)$ be the set of all invertible $n \times n$ matrices whose entries come from a field F. $GL_n(F)$ is a group under matrix multiplication and is called the general linear group of degree n.

Definition: Quaternion group

The quaternion group Q_8 has elements $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, where 1 is the identity. For any $a \in Q_8$, the elements multiply as follows.

$$\begin{gathered} (-1)^2 = 1, \quad (-1) \cdot a = a \cdot (-1) = -a \\ i^2 = j^2 = k^2 = -1 \\ ij = k, \quad jk = i, \quad ki = j \\ ji = -k, \quad kj = -i, \quad ik = -k \end{gathered}$$

1.3 Homomorphisms

Now we'll look at different kinds of maps between groups, starting with the simplest one posible.

Definition: Homomorphism

Let G and H be groups. A homomorphism from G to H is a function $\varphi : G \to H$ such that, for all $x, y \in G$,

$$\varphi(xy) = \varphi(x)\varphi(y).$$

The kernel and image of φ are, respectively,

$$\ker(\varphi) = \{x \in G \mid \varphi(x) = 1\}, \quad \text{image}(\varphi) = \{\varphi(x) \mid x \in G\}.$$

Theorem 1.2

Let $\varphi : G \to H$ be a homomorphism. Then

(a) $\varphi(1)$ is the identity of H.

(b) $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G$.

(c) $\varphi(x^n) = \varphi(x)^n$ for all $x \in G$, $n \in \mathbb{Z}$.

If we want to do a better job at preserving structure in our map, we can go a step further.

Definition: Isomorphism

A homomorphism $\varphi : G \to H$ is an isomorphism if it is bijective. In this case we say G and H are isomorphic, and we write $G \cong H$.

The existence of the identity map on G is enough to show that $G \cong G$, but other isomorphisms may exist. For example, we may fix g and define $\varphi_g : G \to G$ by setting $\varphi_g(x) = gxg^{-1}$ for all $x \in G$. (This is a particular kind of isomorphism called an inner automorphism.)

Definition: Automorphism

An automorphism of a group G is an isomorphism from G to G.

Notably, the set $\mathrm{Aut}(G)$ of automorphisms of G forms a group under function composition!

1.4 Group Actions

We'll finish off this preliminary discussion by looking at what might happen when a group acts on a set.

Definition: Group action

A (left) group action of a group G on a set X is a map from $G \times X$ to X, where the image of (g, x) is written as $g \cdot x$ or simply gx, such that

- $g(hx) = (gh)x$ for all $g, h \in G$ and $x \in X$.
- $1x = x$ for all $x \in X$.

There are many easily accessible examples of group actions—here's the most glaring one.

Definition: Left regular action

Every group acts on itself by left multiplication. This is called the left regular action of G.

As for some others: $\mathbb{R}^\times$ acts on $\mathbb{R}^n$ by scaling, S_Ω acts on Ω by permuting, and D_{2n} acts on the vertices of a regular n-gon.

Theorem 1.3

Suppose G acts on X. For each $g \in G$, $\sigma_g(x) = g \cdot x$ defines a permutation of X. Moreover, the map from G to S_X defined by $g \mapsto \sigma_g$ is a homomorphism.

Proof. Let $g \in G$. Since $\sigma_g \circ \sigma_{g^{-1}}$ and $\sigma_{g^{-1}} \circ \sigma_g$ are both the identity map on X, σ_g has a two-sided inverse and is therefore a bijection from X to X. In other words, σ_g is a permutation of X.

Now define a map $\varphi : G \to S_X$ such that $\varphi(g) = \sigma_g$. We have

$$\begin{aligned}\varphi(gh)(x) &= \sigma_{gh}(x) \\ &= (gh) \cdot x \\ &= g \cdot (h \cdot x) \\ &= \sigma_g(\sigma_h(x)) \\ &= (\varphi(g) \circ \varphi(h))(x)\end{aligned}$$

So we have $\varphi(gh) = \varphi(g) \circ \varphi(h)$ for all $g, h \in G$ and φ is a homomorphism. □

All this motivates the following.

Definition: Representation

Let G be a group, and let $n \in \mathbb{Z}^+$.

- A homomorphism $\varphi : G \to S_n$ is called a permutation representation.
- A homomorphism $\rho : G \to GL_n(\mathbb{C})$ is called a linear representation.

1.5 Subgroups

So far we've engaged in a direct study of groups and some of their most important properties. Another way we can discern the structure of these objects, though, is to look at any smaller groups embedded inside.

Definition: Subgroup

Let G be a group. A subset H of G is a subgroup of G if

- H is nonempty,
- $x, y \in H$ implies $xy \in H$, and
- $x \in H$ implies $x^{-1} \in H$.

If H is a subgroup of G then we will write $H \leq G$. If we also have $H \neq G$ then we write $H < G$ and call H a proper subgroup of G.

Notice that every group has $\{1\}$ and itself as subgroups; the latter is called the trivial subgroup of G. If we're working with a finite group, the criteria for subgroups become slightly less strict.

Theorem 1.4

Let G be a finite group. A subset H of G is a subgroup of G if H is both nonempty and closed under multiplication.

Proof. Let $x \in H$ where $x \neq 1$. If H is closed under multiplication then $\{x, x^2, x^3, \ldots\} \subseteq H$. But G is finite, meaning H is also finite and by the pigeonhole principle there exist $a, b \in \mathbb{Z}^+$ such that $x^a = x^b$ with $b - a \geq 2$. Thus $x^{-1} = x^{b-a-1}$, so $x^{-1} \in H$ and $H \leq G$. □

As a side note, we have a handy result about the subgroups of $\mathbb{Z}$.

Theorem 1.5: Subgroups of the integers

Every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Proof. Let $H \leq \mathbb{Z}$. If H is the trivial subgroup then $H = 0\mathbb{Z}$. Otherwise, let a be the smallest positive integer in H. We claim that $H = a\mathbb{Z}$.

Suppose, for contradiction, that there is a $b \in H$ such that $b \notin a\mathbb{Z}$. Then let $d = \gcd(a, b)$; since there exist $x, y \in \mathbb{Z}$ such that $xa + yb = d$, we have $d \in H$. Since $0 < d < a$, we have a contradiction and $H = a\mathbb{Z}$. □

Now we'll look at a few kinds of subgroups which are fundamental to understanding the broader structure of whatever group we're looking at.

Definition: Centralizer

The centralizer of A in G is

$$\begin{aligned} C_G(A) &= \{g \in G \mid ga = ag \text{ for all } a \in A\} \\ &= \left\{g \in G \mid gag^{-1} = a \text{ for all } a \in A\right\}. \end{aligned}$$

That is, it is the set of all elements of G that commute with every element of A.

Definition: Center

The center of G is

$$Z(G) = C_G(G).$$

That is, it is the set of all elements of G that commute with every other element of G.

We may also view these definitions through the lens of conjugations. Consider, for example, the element $r^{-1}sr$ with $r, s \in D_{2n}$. We call this the conjugation of s by r, and we can understand it as application of s from the "perspective" of r. The result is a reflection about line of symmetry running through the vertex just above the horizontal axis. (The interpretation of rsr^{-1} is very similar, in this case just viewed from the perspective of r^{-1} rather than r.)

So conjugation, in a way, entails viewing a group element from the perspective of some other element in the group. The centralizer of A in G, then, is the set of all elements in G that we may go to if we'd like to "preserve" A under a shift in perspective, and the center of G is the set of elements that preserve all of G under such a shift.

We may generalize this notion of preservation slightly by requiring only that conjugacy permutes A rather than preserving it.

Definition: Normalizer

The normalizer of A in G is

$$N_G(A) = \left\{g \in G \mid gAg^{-1} = A\right\},$$

where $gAg^{-1} = \left\{gag^{-1} \mid a \in A\right\}$.

Notice that we've developed a kind of subgroup hierarchy here. For any group G we have

$$Z(G) \leq C_G(A) \leq N_G(A) \leq G.$$

Also notice that if G is abelian then $Z(G) = G$ and all of these are simply equal to G. Two more subgroups!

Definition: Stabilizer

If G acts on X and $x \in X$, then the stabilizer of x in G is

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

Definition: Kernel

If G acts on X then the kernel of the action is

$$\{g \in G \mid g \cdot x = x \ \ \forall x \in X\} = \bigcap_{x \in X} G_x.$$

A nice fact that ties all this together: if $N_G(A)$ acts on A by conjugation, then the kernel of the action is the centralizer of A in G.

1.6 Cyclic Groups

Now we'll look at a very simple kind of group which often appears as a subgroup. The first few results about these groups are pretty straightforward, so we'll fly through them quickly.

Definition: Cyclic group

A group is cyclic if it can be generated by one element.

Theorem 1.6

Any two cyclic groups of the same order are isomorphic.

Theorem 1.7: Subgroups of a cyclic group

Every subgroup of a cyclic group is cyclic.

Proof. (Sketch) It suffices to show that if K is a nontrivial subgroup of $\langle x \rangle$, then $K = \langle x^d \rangle$ where d is the smallest positive integer such that $x^d \in K$. This involves showing that if $x^n \in K$ then, by the division algorithm, d divides a. □

Theorem 1.8

Let G be a group, let $x \in G$, and suppose $|x| = n < \infty$. if $m \in \mathbb{Z}^+$ and $x^m = 1$, then n divides m.

Proof. If $x^m = 1$ then, by the definition of order, $m \geq n$. So $m = kn + r$ for some integers $k \geq 1$ and $0 \leq r < n$ and

$$1 = x^m = x^{kn+r} = (x^n)^k x^r = x^r$$

and we must have $r = 0$, meaning $m = kn$. Thus n divides m. □

Now we have a neat connection to an idea from number theory. Let $(m, n) = \gcd(m, n)$, and let φ denote the Euler totient function.

Theorem 1.9

If $G = \langle x \rangle$ is a finite cyclic group of order n, then for every positive integer d that divides n, $\langle x^{n/d} \rangle$ is the unique order-d subgroup of G. Furthermore, $\langle x^m \rangle = \langle x^{(m,n)} \rangle$ for every $m \in \mathbb{Z}$, so the subgroups of G correspond to the divisors of n and G has $\varphi(n)$ generators.

Corollary 1.10

If n is a positive integer then $n = \sum_{d|n} \varphi(d)$.

Finally, one more pair of facts about the orders of elements.

Theorem 1.11

Let G be a group, let $x \in G$, and let a be a nonzero integer. If $|x| = n < \infty$, then $|x^a| = n/(n, a)$.

Corollary 1.12

If $|x| = n < \infty$ and a is a positive integer that divides n, then $|x^a| = n/a$.

2 Quotient Groups

2.1 Fibers and Kernels

At this point we've gotten a broad overview of groups and the subgroups embedded within them. Now we'll do something a little more sophisticated—we'll take a group and collapse it into a smaller group based on a set of characteristics decided ahead of time. We'll begin this discussion in the context of fibers and kernels.

Definition: Fiber

Let $\varphi : G \to H$ be a homomorphism. We can define an equivalence relation $\sim$ on G where if $x, y \in G$, then

$$x \sim y \text{ iff } \varphi(x) = \varphi(y).$$

The resulting equivalence classes are called fibers.

Theorem 2.1

Let $\varphi : G \to H$ be a homomorphism with kernel K, and let $x, y \in G$. We have the equivalent statements

$$\varphi(x) = \varphi(y) \iff y^{-1}x \in K \iff xy^{-1} \in K \iff x^{-1}y \in K \iff yx^{-1} \in K.$$

The latter two bits here can be used to show something important about what fibers have to do with kernels.

Theorem 2.2

Let $\varphi : G \to H$ be a homomorphism with kernel K. The fiber containing $x \in G$ can be expressed in two different ways:

$$xK = \{xk \mid k \in K\}, \qquad Kx = \{kx \mid k \in K\}.$$

In particular, note that

(a) $xK = Kx$ (so x is in the normalizer of K) and

(b) $\varphi(x) = \varphi(y)$ if and only if $xK = yK$.

In this way, each fiber of a homomorphism φ is a "translate" of $\ker(\varphi)$, and these fibers partition G. It turns out that they interact in a very nice way!

Definition

Let $\varphi : G \to H$ be a homomorphism with kernel K. The set of associated fibers, called "G mod K", is denoted by

$$G/K = \{gK \mid g \in G\}.$$

Theorem 2.3

Let $\varphi : G \to H$ be a homomorphism with kernel K. Then G/K forms a group where the binary operation is given by

$$(uK)(vK) = (uv)K.$$

Proof. Showing that the binary operation satisfies the group axioms is straightforward, but we must also show that it is well-defined—that is, it shouldn't depend on which elements we take from uK and vK.

Say $uK = u'K$ and $vK = v'K$, so $\varphi(u) = \varphi(u')$ and $\varphi(v) = \varphi(v')$, and

$$\varphi(uv) = \varphi(u)\varphi(v) = \varphi(u')\varphi(v') = \varphi(u'v').$$

Thus $(uK)(vK) = (uv)K = (u'v')K = (u'K)(v'K)$ and the binary operation is well-defined. □

As a concrete example, consider $\varphi : D_8 \to \mathbb{Z}/2\mathbb{Z}$ where $\varphi(s^i r^j) = \bar{i}$. We can see that $\ker(\varphi) = \langle r \rangle$ and

$$D_8/\langle r \rangle \cong \varphi(D_8) = Z/2\mathbb{Z}.$$

Note that we'll sometimes write $\bar{u}$ to denote the fiber uK, in which case we have $\bar{u}\bar{v} = \overline{uv}$.

2.2 Quotients

We can generalize much of the above discussion to any subgroup of the group we're working with, rather than just the kernel of some homomorphism.

Definition: Coset

Let $N \leq G$. If $g \in G$, then

$$gN = \{gn \mid n \in N\} \quad \text{and} \quad Ng = \{ng \mid g \in N\}$$

are left and right cosets of N in G, respectively.

Note that this time, the left and right cosets are not necessarily equal. We will make statements mostly about left cosets, but bear in mind that every such statement has an analog for right cosets.

Theorem 2.4

If $N \leq G$ then the left cosets of N in G partition G. Furthermore, for $u, v \in G$ then $uN = vN$ if and only if $v^{-1}u \in N$.

Proof. First note that $1 \in N$, meaning $g \in gN$ for all $g \in G$ and the set of all gN "covers" G. Now suppose $uN \cap vN \neq \varnothing$ for some $u, v \in G$; we will show that $uN = vN$.

Let $x \in uN \cap vN$, so $x = un = vm$ for some $n, m \in N$ and $u = v \cdot mn^{-1}$. Thus for a $t \in N$ we can write $ut = v \cdot mn^{-1}t$, meaning $uN \subseteq vN$. By a symmetric argument we also have $vN \subseteq uN$ and $uN = vN$. It follows that the left cosets of N in G partition G.

Finally, by what we saw above, $uN = vN$ if and only if $u = vn$ for some $n \in N$. This happens if and only if $v^{-1}u \in N$. □

For the next two theorems, let G/N (read aloud as "G mod N") denote the left cosets of N in G.

Theorem 2.5

If $N \leq G$ then the binary operation

$$(uN) \cdot (vN) = (uv)N$$

defined on G/N is well-defined if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.

Proof. ($\Rightarrow$) Suppose the binary operation is well-defined. Then both $1, n \in N$ are representatives of the same coset, so for $g \in G$ the expression

$$(1N) \cdot (g^{-1}N) = g^{-1}$$

must be equivalent to

$$(nN) \cdot (g^{-1}N) = (ng^{-1})N.$$

Hence $\left(g^{-1}\right)^{-1} = gng^{-1} \in N$. It follows that $gNg^{-1} \subseteq N$ for all $g \in G$.

($\Leftarrow$) Suppose $gNg^{-1} \subseteq N$ for all $g \in G$, and let $uN = vN$ and $xN = yN$. So $u = nv$ and $x = ym$ for some $m, n \in N$, and

$$ux = vn \cdot ym = vy \cdot \left(y^{-1}ny\right) m,$$

and since the parenthetical is in N we have $(ux)N = \left[vy \cdot \left(y^{-1}ny\right) m\right] N = (vy)N$. □

Theorem 2.6

If the binary operation above is well defined on G/N, then G/N forms a group with this binary operation. The identity is $N = 1N$, and $(gN)^{-1} = g^{-1}N$.

We'll often refer to G/N as the quotient of G by N. Now, notice that the condition in Theorem 2.5 is stronger than it seems because conjugation is bijective. So really, our binary operation is well defined if and only if $gNg^{-1} = N$ for all $g \in G$. This evokes the normalizer we discussed earlier!

Definition: Normal subgroup

If $N \leq G$, we say N is normal in G if $gNg^{-1} = N$ for all $g \in G$. In this case we write $N \trianglelefteq G$.

And now, a result that ties the structure we've built here to the theory from earlier.

Theorem 2.7

$N \trianglelefteq G$ if and only if N is the kernel of some homomorphism.

Proof. ($\Rightarrow$) If $N \trianglelefteq G$ then N is the kernel of the "natural projection" homomorphism $\varphi : G \to G/N$ where $\varphi(g) = gN$.

($\Leftarrow$) If N is the kernel of some homomorphism then $gN = Ng$ and $gNg^{-1} = N$ for all $g \in G$. □

2.3 More on Cosets

We'll begin here with a powerful result about the structure of cosets in a group and a couple of corollaries.

Theorem 2.8: Lagrange's theorem

If $G$is a finite group and $H \leq G$, then $|H|$ divides $|G|$ and there are $|G|/|H|$ left cosets of H in G.

Proof. Suppose there are k left cosets of H in G; these left cosets partition G. Now, the map $H \to gH$ defined by $h \mapsto gh$ is a surjection, and it is injective since $gh_1 = gh_2$ implies $h_1 = h_2$. So there is a bijection form H to gH and $|H| = |gH|$.

G is partitioned into k disjoint subsets, each of cardinality $|H|$, so $|G| = k|H|$. Thus $k = |G|/|H|$. □

Corollary 2.9

If G is a finite group and $x \in G$, then $|x|$ divides $|G|$ and $x^{|G|} = 1$.

Corollary 2.10

If G is a finite group of prime order p, then G is cyclic and $G \cong \mathbb{Z}/p\mathbb{Z}$.

Note that the converse to Lagrange's theorem is not, in general, true. Before we give a counterexample, we'll make another straightforward statement about cosets.

Definition: Index of a subgroup

If G is a (potentially infinite) group and $H \leq G$, then the number of left cosets of H in G is the index of H in G. It is denoted by $|G : H|$.

Theorem 2.11

If $H \leq G$ and $|G : H| = 2$ then $H \trianglelefteq G$.

Proof. The left and right cosets of H and G are equal. In particular, if $g \in G - H$, then the set of left cosets of H in G is $\{H, gH\}$, the set of right cosets is $\{G, Hg\}$. □

Now let A be the group of symmetries of a regular tetrahedron (so $|A| = 12$), and suppose A had a subgroup of order 6. Then $|A : H| = 2$, meaning H is a normal subgroup of A and $A/H \cong Z/2\mathbb{Z}$. It follows that $(aH)^2 = H$ for all $a \in A$, implying that $a^2H = H$ and $a^2 \in H$ for all such a. But if $|a| = 3$ then $a = (a^2)^2$ and $a \in H$, so H contains all elements in A of order 3. The fact that A has at least eight elements of order 3 brings us to a contradiction.

Happily, Lagrange's theorem has some good partial converses, neither of which we will prove now.

Theorem 2.12: Cauchy's theroem

If G is a finite group and p is a prime divisor of $|G|$, then G has an element of order p.

Theorem 2.13: First Sylow theorem

If G is a finite group of order $p^\alpha m$ where p is prime and p does not divide m, then G has a subgroup of order p^α.

It turns out that this result from Sylow is provably the strongest partial converse to Lagrange's theorem. We'll come back to this it later—for now, we'll finish off the section with some more useful facts about cosets.

Theorem 2.14

Let H and K be subgroups of G, and define $HK = \{hk \mid h \in H,\ k \in K\}$.

(a) If H and K are finite then $|HK| = |H||K|/|H \cap K|$.

(b) HK is a subgroup of G if and only if $HK = KH$.

(c) If $H \leq N_G(K)$ then $HK \leq G$.

(d) If $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

2.4 The Isomorphism Theorems

Here we'll give a few important results surrounding quotient groups and homomorphisms. The first is essentially a formalization of the ideas we started the chapter with.

Theorem 2.15: First isomorphism theorem

If $\varphi : G \to H$ is a homomorphism then

(a) $\ker(\varphi) \trianglelefteq G$ and

(b) $G/\ker(\varphi) \cong \varphi(G)$.

Proof. (Sketch) We've already proved (a) as Theorem 1.7. For (b), define $\Phi : G/\ker(\varphi) \to \varphi(G)$ via $\Phi(g\ker(\varphi)) = \varphi(g)$. We'd show, from here, that Φ is well-defined and is a bijective homomorphism. □

For our next theorem, let B normalize a subgroup A of G and suppose we want to say something about the "quotient" of A by B. Since B isn't necessarily a subgroup of A, we have to do one of two things first: expand A to include the elements in B, or contract B to exclude elements not in A.

Theorem 2.16: Second isomorphism theorem

Let A, B be subgroups of a group G, where $A \leq N_G(B)$. Then

(a) $B \trianglelefteq AB$ and $A \cap B \trianglelefteq A$.

(b) $AB/B \cong A/(A \cap B)$.

Proof. The first part of (a) will be proved soon. For the second part, if $c \in A \cap B$ and $A \in A$ then $aca^{-1} \in A$ (because $c \in A$) and $aca^{-1} \in B$ (because $a \in N_G(B)$). Thus $aca^{-1} \in A \cap B$, so $A \cap B \trianglelefteq A$.

For (b), define a map $\varphi : AB \to A/(A \cap B)$ via

$$\varphi(ab) = a(A \cap B), \quad a \in A,\ b \in B.$$

We quickly show that φ is well-defined: if $ab = a_1b_1$ then $a_1^{-1}a = b_1b^{-1}$, meaning $a_1^{-1}a \in A \cap B$ and $a(A \cap B) = a_1(A \cap B)$. Now, φ is a homomorphism because

$$\begin{aligned}\varphi\big((ab)(a_1b_1)\big) &= \varphi\big(aa_1 \cdot a_1^{-1}ba_1 \cdot b_1\big)\\ &= aa_1(A \cap B)\\ &= \big(a(A \cap B)\big)\big(a_1(A \cap B)\big)\\ &= \varphi(ab)\varphi(a_1b_1).\end{aligned}$$

The kernel of φ is, by definition,

$$\ker(\varphi) = \{ab \mid a \in A,\ b \in B,\ a \in A \cap B\} = B.$$

Finally, $\varphi(AB) = A/(A \cap B)$ because each coset of $A \cap B$ has a representative in A. So by the first isomorphism theorem, $B \trianglelefteq AB$ and $AB/B \cong A/(A \cap B)$. □

Our third theorem concerns taking quotients of quotients and is a bit more intuitive.

Theorem 2.17: Third isomorphism theorem

Let H and K be normal subgroups of a group G where $H \leq K$. Then

(a) $K/H \trianglelefteq G/H$.

(b) $(G/H)/(K/H) \cong G/K$.

Proof. Define $\varphi : G/H \to G/K$ by $\varphi(gH) = gK$. Notice that $gH = g_1H$ implies $g_1^{-1}g \in H \leq K$, meaning $gK = g_1K$ and φ is well-defined. It is easy to see that φ is surjective, and the kernel is

$$\begin{aligned}\ker(\varphi) &= \{gH \in G/H \mid gK = K\} \\ &= \{gH \in G/H \mid g \in K\} \\ &= K/H.\end{aligned}$$

Both (a) and (b) follow from the first isomorphism theorem. □

The final theorem here relates the subgroup structure of G to that of G/N. In particular, the subgroups of G/N have the same structure as the subgroups of G containing N.

Theorem 2.18: Fourth isomorphism theorem

Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G containing N onto the set of subgroups $\overline{A} = A/N$ of $\overline{G} = G/N$. This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

(a) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,

(b) if $A \leq B$ then $|B : A| = |\overline{B} : \overline{A}|$,

(c) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$,

(d) $\overline{A \cap B} = \overline{A} \cap \overline{B}$, and

(e) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

3 Group Actions

3.1 Action by Left Multiplication

We've already seen how groups can act on themselves by left multiplication, but they can also act on their own left cosets by left multiplication. If $H \leq G$ then G acts on the left cosets of H in G by setting

$$a \cdot bH = abH$$

for all $a, b \in G$. We might view this as a generalization of G acting on itself—if $H = \{1\}$ then there is a bijection between its cosets and the elements of G.

Theorem 3.1

Consider the above action of G on G/H, and let $\pi_H : G \to S_{G/H}$ denote the permutation representation of G on G/H.

(a) The action is transitive—that is, for any $x, y \in G/H$ there is a $g \in G$ such that $g \cdot x = y$.

(b) The stabilizer $G_{1H} = H$.

(c) $\ker \pi_G = \bigcap_{x \in G} xHx^{-1}$, which is the largest normal subgroup of G contained in H.

Proof. We'll just prove (c). By definition,

$$\begin{aligned}
\ker \pi_H &= \{g \in G \mid g \cdot xH = xH \text{ for all } x \in G\} \\
&= \left\{g \in G \mid x^{-1}gx \in H \text{ for all } x \in G\right\} \\
&= \left\{g \in G \mid g \in xHx^{-1} \text{ for all } x \in G\right\} \\
&= \bigcap_{x \in G} xHx^{-1}.
\end{aligned}$$

Now, if $N \trianglelefteq G$ and $N \leq H$ then $N = xNx^{-1} \leq xHx^{-1}$ for all $x \in G$. Thus

$$N \leq \bigcap_{x \in G} xHx^{-1} = \ker \pi_H \leq H,$$

so $\ker \pi_H$ is the largest normal subgroup of G contained in H. □

We can use this to formalize an observation we made much earlier on, about being able to view some groups through the lens of permuting their elements.

Corollary 3.2: Cayley's theorem

Every group is isomorphic to a subgroup of some symmetric group.

Proof. Let G act on itself by left multiplication. This is equivalent to having G act on the left cosets of $H = \{1\}$, and the associated permutation representation $\pi_H : G \to S_{G/H}$ has a trivial kernel. Thus by the first isomorphism theorem

$$G \cong G/\{1\} \cong \pi_H(G) \leq S_{G/H}$$

and G is isomorphic to a subgroup of $S_{G/H}$. □

We can also generalize our result about subgroups of index 2 being normal.

Corollary 3.3

If $|G| = n$ and p is the smallest prime factor of n, then any subgroup H of index p is normal in G.

Proof. Let $K = \ker \pi_H$ and let $k = |H : K|$. Then

$$|G : K| = |G : H||H : K| = pk.$$

By the first isomorphism theorem G/K is isomorphic to $\pi_H(G)$, a subgroup of $S_{G/H} = S_p$. So by Lagrange's theorem $|G/K| = pk$ must divide $|S_p| = p!$, and $k \mid (p-1)!$.

Now, the prime divisors of $(p-1)!$ are all less than p. But the prime divisors of k are all greater than or equal to p by the minimality of p. Thus k has no prime divisors, $k = 1$, and $H = K \trianglelefteq G$. □

3.2 Action by Conjugation

Groups can also act on themselves by conjugation.

Definition: Conjugacy class

The elements $a, b \in G$ are conjugate in G if there is some $g \in G$ such that $gag^{-1} = b$. In other words, a, b are conjugate if they are in the same orbit under conjugation; these orbits are called conjugacy classes.

We'll make a general statement about group actions and apply it to conjugation. If we have a group acting on a set X, then in order to determine how many elements can be "reached" by acting on an $x \in X$, in a rough sense we can divide out the symmetries that leave x fixed.

Theorem 3.4: Orbit-stabilizer theorem

Let G be a group acting on a nonempty set X. For each $x \in X$, the orbit containing x has size $|G : G_x|$.

Proof. Consider the map from the orbit of x to the left cosets of G_x, where

$$g \cdot x \mapsto gG_x.$$

This map is well-defined: if $g \cdot x = h \cdot x$ then $h^{-1}g$ stabilizes x, meaning $h^{-1}g \in G_x$ and $gG_x = hG_x$. We can trace this argument in reverse to show that the map is injective. It is clearly also surjective, meaning the map is a bijection and

$$\big|\{g \cdot x \mid g \in G\}\big| = |G/G_x| = |G : G_x|,$$

as desired. □

Corollary 3.5

If $a \in G$ then a has $|G : C_G(a)|$ conjugates.

Proof. Under conjugation, $G_a = \{g \in G \mid gag^{-1} = a\} = C_G(a)$. □

Now, if an element commutes with every element in G, it's in its own conjugacy class. Considering how the singleton classes together comprise $Z(G)$, and that the conjugacy classes partition G, we ge the following.

Theorem 3.6: Class equation

Let g be a finite group and $g_1, \dots, g_r$ be representatives of the conjugacy classes that are not in the center $Z(G)$. Then

$$|G| = |Z(G)| + \sum_{j=1}^{r} |G : C_G(g_j)|.$$

Notice how each of the summands here must divide $|G|$ by Lagrange's theorem. This can put some useful constraints on the structure of the group we're working with.

Theorem 3.7

If P is a group of prime-power order p^a for some $a \geq 1$, then $Z(P) \neq \{1\}$.

Proof. We have the class equation

$$|P| = |Z(P)| + \sum_{j=1}^{r} |P : C_P(g_j)|,$$

where the g_i are representatives of distinct non-central conjugacy classes. So $C_P(g_i) \neq P$ by definition, and p divides $|P : C_P(g_i)|$. It follows that p also divides $|Z(P)|$, meaning the center is nontrivial. □

Finally, we have a nice application of this theory to combinatorics—in plain terms, if a group G acts on a set X then the associated number of orbits is equal to the average number of $x \in X$ fixed by the $g \in G$.

Theorem 3.8: Cauchy-Frobenius lemma

Let G be a finite group acting on a nonempty finite set X. For each $g \in G$, let

$$\operatorname{fix}(g) = \left| \{x \in X \mid g \cdot x = x\} \right|.$$

Then the number of orbits of the action of G on X is

$$\frac{1}{|G|} \sum_{g \in G} \operatorname{fix}(g).$$

Proof. First note that

$$\sum_{g \in G} \operatorname{fix}(g) = \left| \{(g, x) \in G \times X \mid g \cdot x = x\} \right| = \sum_{x \in X} |G_x|.$$

Any $x \in X$ has an orbit of size $|G : G_X|$, meaning the total number of orbits is

$$\sum_{x \in X} \frac{1}{|G : G_x|} = \frac{1}{|G|} \sum_{x \in X} |G_x| = \sum_{g \in G} \operatorname{fix}(g),$$

as desired. □

Suppose we want to count the number of ways we can color the vertices of a 3-cycle using two colors. We can see that there are eight ways to color the vertices, but there are two triplets that are the same up to rigid symmetry. To formalize this observation, let D_6 act on the eight colorings—if we go through each $g \in D_6$, sum the $\operatorname{fix}(g)$, and divide by 6 we get 4, the number of orbits for this action.

3.3 The Sylow Theorems

As mentioned before, the first of the Sylow theorems offer a "sharp" partial converse to Lagrange's theorem. It turns out to be useful in a wide variety of contexts, including in classifying groups and, in particular, in showing when a group is not simple—that is, when a group is not trivial and has no nontrivial normal subgroups. (The simple groups can be thought of as the "prime" groups, the unique building blocks of all others.) We'll define some things before getting into the rest of the theorems.

Definition: p-group

Let G be a finite group and let p be prime.

- A group of order p^a with $a \geq 0$ is called a p-group. Subgroups of G that are p-groups are called p-subgroups.
- If $|G| = p^a m$ where $p \nmid m$ then a subgroup of G of order p^a is a Sylow p-subgroup of G.
- The set of Sylow p-subgroups of G is denoted by $Syl_p(G)$, and the number of these subgroups is denoted by $n_p(G)$.

We also have a useful intermediate result.

Lemma 3.9

Let $P \in Syl_p(G)$. If Q is any p-subgroup of G then $Q \cap N_G(P) = Q \cap P$.

Proof. Let $H = Q \cap N_G(P)$. We can see that $P \leq N_G(P)$, so immediately $Q \cap P \leq H$. We'll get the other inequality if we can show that $H \leq P$ (since we already know $H \leq Q$ by definition).

Since $H \leq N_G(P)$, $PH \leq G$. Also, since $|PH| = |P||H|/|P \cap H|$, we know that PH is a p-subgroup of G. But $P \leq PH$ and P is a maximal p-subgroup of G, so $P = PH$ implying $H \leq P$. □

Theorem 3.10: Sylow theorems

Let G be a finite group of order $p^a m$ where p is prime and $p \nmid m$.

(a) $Syl_p(G)$ is nonempty.

(b) If $P \in Syl_p(G)$ and Q is a p-subgroup of G then Q is contained in a conjugate of P.

(c) $n_p(G) \equiv 1 \bmod p$.

(d) If $P \in Syl_p(G)$ then $n_p(G) = |G : N_G(P)|$, implying that $n_p(G)$ divides m.

Proof. We'll prove part (a) using strong induction. If $|G| = 1$ then we're done; otherwise, suppose every group with order less than $|G|$ has a Sylow p-subgroup. We have two cases.

If p divides $|Z(G)|$ then by Cauchy's theorem $Z(G)$ contains a subgroup N of order p. So $|G/N| = p^{a-1}m$ and, by the inductive hypothesis, G/N has a Sylow p-subgroup $\overline{P}$ of order p^{a-1}. By the fourth isomorphism theorem there is a subgroup P of G such that $P/N = \overline{P}$ and $|P| = p^a$. Thus P is a Sylow p-subgroup of G.

If p does not divide $|Z(G)|$ then consideration of the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

reveals that there must be some g_i such that p does not divide $|G : C_G(g_i)i| = p^a k$ where p does not divide $k < m$. By the inductive hypothesis $C_G(g_i)$ has a Sylow p-subgroup P of order p^a, and P is also a Sylow p-subgroup of G. This proves (a).

As setup for the rest of the proof, let S be the set of conjugates of P in G, and let Q be any p-subgroup of G. Q acts on S by conjugation, partitioning S into s orbits, each denoted by $\mathcal{O}_i$. Label the elements P_i of S so that the first s elements satisfy $P_i \in \mathcal{O}_i$.

We know that $|\mathcal{O}_i| = |Q : N_Q(P_i)|$, where by definition $N_Q(P_i) = Q \cap N_G(P_i)$. By the preceding lemma we also have $Q \cap N_G(P_i) = Q \cap P_i$, so

$$|\mathcal{O}_i| = |Q : Q \cap P_i|.$$

Setting $Q = P_1$ gives $|\mathcal{O}_1| = 1$. For all $i > 1$, however, $P_1 \cap P_i < P_1$. So

$$|\mathcal{O}_i| = |P_1 : P_1 \cap P_i| > 1$$

is a power of p and is thus divisible by p. It follows that

$$|S| = |\mathcal{O}_1| + (|\mathcal{O}_2| + \cdots + |\mathcal{O}_s|) \equiv 1 \bmod p.$$

Now let Q once again be an arbitrary p-subgroup of G. If Q were not contained in any of the P_i then $|\mathcal{O}_i| = |Q : Q \cap P_i| > 1$ for all $1 \leq i \leq s$. So $|\mathcal{O}_i|$ is divisible by p for all $1 \leq i \leq s$, contradicting the fact that $|S| \equiv 1 \bmod p$. So Q must be contained in some P_i, proving (b). Since the Q here may be a Sylow p-subgroup of G, if $P' \in Syl_p(G)$ then $P' \in S$ and so $n_p(G) \equiv 1 \bmod p$. This proves (c). Finally, since the Sylow p-subgroups of G are all conjugate, we have

$$n_p(G) = |G : N_G(P)|.$$

Trivially, $P \leq N_G(P)$, so $n_p(G) \mid m$. This proves (d). □

Corollary 3.11

P is the unique Sylow p-subgroup of G if and only if $P \trianglelefteq G$.

Corollary 3.12

If $P, P' \in Syl_p(G)$ then P is conjugate to P'.

4 Rings

4.1 Axioms and Properties

Now we'll look at a different, more familiar algebraic structure. In this new context we'll quickly go through all the same discussions as we had with groups.

Definition: Ring

A ring R is a set with two binary operations $+$ (addition) and $\times$ (multiplication) such that

- $(R, +)$ is an abelian group,
- $\times$ is associative, and
- the distributive law holds—that is, for all $a, b, c \in R$,

$$(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).$$

R is commutative if $\times$ is commutative. R has an identity if there is an element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.

We'll write ab for $a \times b$. Also, the additive identity of R is 0, and the additive inverse of $a \in R$ is $-a$.

Theorem 4.1

If R is a ring then for all $a, b \in R$:

(a) $0a = a0 = 0$.

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

(c) $(-a)(-b) = ab$.

(d) if R has an identity 1, then it is unique and $-a = (-1)a$.

Proof. (Sketch) We'll motivate proofs for each part.

(a) We have $0a = (0 + 0)a = 0a + 0a$, and cancellation gives $0 = 0a$.

(b) We have $ab + (-a)b = (a - a)b = 0$, and cancellation gives $(-a)b = -(ab)$.

(c) We have $ab - (-a)(-b) = ab + a(-b) = a(b - b) = 0$. and cancellation gives $ab = (-a)(-b)$.

(d) If 1 and $1'$ are both identities then $1 = 1 \times 1' = 1'$. Also, $(-1)a = -(1a) = -a$.

Filling in the gaps would complete the proof. □

Definition: Subring

A subring of the ring R is a subgroup of R that is closed under multiplication.

Now we'll run through some new vocabulary.

Definition: Division ring

A ring R with identity $1 \neq 0$ is a division ring if every nonzero element of R has a multiplicative inverse. A commutative division ring is called a field.

Definition: Zero divisor

A nonzero element $a \in R$ is a zero divisor if there is a nonzero $b \in R$ such that $ab = 0$ or $ba = 0$.

Definition: Unit

If R has identity $1 \neq 0$ then $u \in R$ is a unit in R if there is some $v \in R$ such that $uv = vu = 1$. In this case v is unique and is denoted by u^{-1}. The set of units in R is denoted by $R^\times$.

Theorem 4.2

A unit is never a zero divisor.

Proof. Let a be a unit and suppose $ab = 0$. Then $b = (a^{-1}a)b = a^{-1}0 = 0$. A similar approach works when $ba = 0$. Thus a cannot be a zero divisor. □

The ring of integers $\mathbb{Z}$ is a particularly important one, and it is characterized by having no zero divisors and its only units being ± 1. This next class of rings, then, can be viewed as a kind of generalization of $\mathbb{Z}$.

Definition: Integral domain

A commutative ring with identity $1 \neq 0$ is an integral domain if it has no zero divisors.

Theorem 4.3: Cancellation law

Let R be an integral domain and let $a, b, c \in R$. If $ab = ac$ then either $a = 0$ or $b = c$.

Proof. If $ab = ac$ then $a(b-c) = 0$. If $a = 0$ then we're done; if $a \neq 0$ then we must have that $b - c = 0$ (because R has no zero divisors), implying $b = c$. □

Corollary 4.4

Every finite integral domain is a field.

Proof. Let R be a finite integral domain. Suppose $a \in R$ and $a \neq 0$. By the above theorem the map defined by $x \mapsto ax$ is injective on R, and since R is finite, this map is also surjective. So $ab = 1$ for some $b \in R$, and it follows that all nonzero elements of R are units. Thus R is a finite commutative division ring or, in other words, a finite field. □

Here're a few families of rings that frequently appear in applications.

- (Polynomial ring) Let R be a commutative ring with identity and let x be an indeterminate. Denote by $R[x]$ the set of polynomials in x with coefficients in R. These polynomials form a ring under the usual addition and multiplication of polynomials.
- (Matrix ring) Let R be a ring and let n be a positive integer. The set $M_n(R)$ of all $n \times n$ matrices with entries in R forms a ring under the usual addition and multiplication of matrices.
- (Group ring) Let R be a commutative ring with identity $1 \neq 0$ and let $G = \{g_1, \ldots, g_n\}$ be a finite group. The group ring of G with coefficients in R is the set RG of formal sums $a_1 g_1 + \cdots + a_n g_n$ where $a_1, \ldots, a_n \in R$. Addition is componentwise and multiplication uses a distributive property.

Note that we may also think of each element in a group ring RG as a function $\alpha : G \to R$, where each group element is mapped to its ring coefficient.

4.2 Homomorphisms and Quotients

Now we'll fly through a familiar discussion of ring homomorphisms and quotient rings.

Definition: Homomorphism

Let R and S be rings. A map : $R \to S$ is a (ring) homomorphism if for all $a, b \in R$

- $\varphi(a+b) = \varphi(a) + \varphi(b)$ and
- $\varphi(ab) = \varphi(a)\varphi(b)$.

Theorem 4.5

Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

(a) The image of φ is a subring of S.

(b) The kernel of φ is a subring of R.

(c) If $\alpha \in \ker(\varphi)$ then $\alpha r, r\alpha \in \ker(\varphi)$ for all $r \in R$.

Rather than talk about normal subgroups of a group, we will speak of ideals of a ring. (Note that the conditions below are enough to guarantee that ideals are subrings.)

Definition: Ideal

Let R be a ring. A nonempty subset I of R is an ideal of R if

- I is a subgroup of R and
- given $\alpha \in I$ and $r \in R$ then $\alpha r, r\alpha \in I$.

Theorem 4.6

Let I be an ideal of a ring R. Then the (additive) quotient group R/I is a ring under the binary operations

$$(r+I)+(s+I) = (r+s)+I \quad \text{and} \quad (r+I)(s+I) = rs+I.$$

Conversely, if I is any subgroup of R such that the above holds, then I is an ideal of R.

Now we have near-exact analogs of the isomorphism theorems.

Theorem 4.7: First isomorphism theorem

If $\varphi : R \to S$ is a ring homomorphism then $\ker(\varphi)$ is an ideal of R and $R/\ker(\varphi) \cong \varphi(R)$.

Theorem 4.8: Second isomorphism theorem

Let A be a subring of R and let B be an ideal of R. Then $A + B$ is a subring of R, $A \cap B$ is an ideal of A, and

$$(A+B)/B \cong A/A \cap B.$$

Theorem 4.9: Third isomorphism theorem

Let I and J be ideals of a ring R with $I \subseteq J$. Then J/I is an ideal of R/I and

$$(R/I)/(J/I) \cong R/J.$$

4.3 Properties of Ideals

Now we'll take some time to study ideals in their own right, as the structure of a ring's ideals can provide deep insights into the nature of the ring itself. We will limit this discussion to rings with identity $1 \neq 0$.

Definition: Generating ideals

Let A be a subset of a ring R.

- The ideal generated by A, denoted (A), is the smallest ideal of R that contains A. It is the intersection of all ideals containing A.
- The left ideal generated by A is

$$RA = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R,\, a_i \in A,\, n \in \mathbb{Z}^+ \right\}.$$

  The right ideal AR generated by A is defined analogously.

Definition: Principal ideal

An ideal generated by a single element is called a principal ideal.

In general (0) is the trivial ideal 0, (1) is R itself, and if R is commutative then (a) is the set of all R-multiples of $a \in R$. Note that every subring $n\mathbb{Z}$ of $\mathbb{Z}$ is a principal ideal (n).

Theorem 4.10

Let I be an ideal of a ring R.

(a) $I = R$ if and only if I contains a unit.

(b) If R is commutative, then R is a field if and only if its only ideals are 0 and R.

Corollary 4.11

If R is a field then any nonzero ring homomorphism from R to another ring is injective.

Now we'll work toward generalizing the notion of primality to rings other than $\mathbb{Z}$.

Definition: Maximal ideal

An ideal M of R is a maximal ideal if $M \neq R$ and the only ideals containing M are R and M.

Theorem 4.12

Let R be commutative. An ideal M of R is maximal if and only if the quotient group R/M is a field.

Proof. By the fourth isomorphism theorem M is maximal if and only if the only ideals of R/M are 0 and R/M, which is true if and only if R/M is a field. □

It follows that the ideal $n\mathbb{Z}$ is maximal (and is a field) in $\mathbb{Z}$ if and only if n is prime. Note that some rings don't have maximal ideals—if we take $\mathbb{Q}$ with $ab = 0$ for all $a, b \in \mathbb{Q}$ then the ideals are just the (additive) subgroups of $\mathbb{Q}$, none of which are maximal.

Definition: Prime ideal

Let R be commutative. An ideal $P \neq R$ is a prime if $a, b \in R$ and $ab \in P$ imply $a \in P$ or $b \in P$.

Theorem 4.13

Let R be commutative. An ideal P is prime if and only if R/P is an integral domain.

Proof. Let $\overline{r} = r + P \in R/P$. By definition, P is prime if and only if $R/P \neq 0$ and $\overline{ab} = \overline{a}\overline{b} = 0$ implies $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, i.e., if R/P is an integral domain. □

Corollary 4.14

If R is commutative then every maximal ideal of R is prime.

Proof. If M is a maximal ideal then R/M is a field, which is an integral domain. □

So in $\mathbb{Z}$, the ideals $p\mathbb{Z}$ where $p \in \mathbb{Z}$ is prime are both maximal and prime. (Also, the zero ideal is prime in $\mathbb{Z}$, but not maximal.) The ideal (x) in $\mathbb{Z}[x]$ is another example of a prime (not maximal) ideal, since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ (which is an integral domain).

4.4 Euclidean Domains

Now we'll look at a particular class of integral domains that preserve a lot of the basic number theoretic ideas we might be familiar with.

Definition: Norm

If R is an integral domain, then a function $N : R \to \mathbb{N} \cup \{0\}$ with $N(0) = 0$ is a norm.

Definition: Euclidean domain

An integral domain R is a Euclidean domain if there is a norm N on R such that for all $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ with

$$a = qb + r$$

where $r = 0$ or $N(r) < N(b)$.

All fields are Euclidean domains, and any norm works—simply take $q = ab^{-1}$. As a couple of examples, $\mathbb{Z}$ is a Euclidean domain with norm $N(a) = |a|$, and for any field F the polynomial ring $F[x]$ is a Euclidean domain with the norm $N(p(x))$ being the degree of $p(x) \in F[x]$.

Theorem 4.15

Every ideal in a Euclidean domain is principal. In particular, if I is a nonzero ideal in a Euclidean domain and a nonzero $d \in I$ has minimum norm in I then $I = (d)$.

Proof. If I is the zero ideal then we're done. Otherwise, let $d \in I$ be nonzero with minimum norm; clearly, $(d) \subseteq I$. To show the reverse, let $a \in I$ and write $a = qd + r$ where $r = 0$ or $N(r) < N(d)$. Since $a, qd \in I$ we have $r \in R$. By the minimality of $N(d)$ we also have $r = 0$, meaning $a = qd \in (d)$ and thus $I = (d)$. □

Now we'll see how this helps us generalize some basic arithmetic.

Definition: Divisor

Let R be commutative and let $a, b \in R$.

- b divides a if there is an $x \in R$ such that $a = bx$. In this case we write $b \mid a$.
- A greatest common divisor of a and b is a nonzero d such that $d \mid a$ and $d \mid b$, and if $d' \mid a$ and $d' \mid b$ then $d' \mid d$.

Note that $a \in (d)$ and $(a) \subseteq (d)$ are both equivalent to $d \mid a$.

Definition: Greatest common divisor

The element d is a greatest common divisor of a and b if $(a, b) \subseteq (d)$ and if $(a, b) \subseteq (d')$ implies $(d) \subseteq (d')$.

Definition: Prime

A nonzero element p is prime if (p) is a prime ideal. This if p is prime then p is not a unit and $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Theorem 4.16

Let R be commutative and let $a, b \in R$ be nonzero. If $(a, b) = (d)$ then (d) is a greatest common divisor of a and b.

Theorem 4.17

Let R be an integral domain and let $d, d' \in R$. If $(d) = (d')$ then $d' = ud$ for some unit $u \in R$. In particular, if d and d' are GCDs of $a, b \in R$, then $d' = ud$ for some unit $u \in R$.

Proof. If either d or d' is zero then we're done. Otherwise, since $d \in (d')$ there is some $x \in R$ such that $d = xd'$. Similarly, since $d' \in (d)$ there is some $y \in R$ such that $d' = yd$. Thus $d = xyd$ and so $d(1 - xy) = 0$; since $d \neq 0$, $xy = 1$ and x, y are both units. □

One of the great advantages of working in Euclidean domains is that they allow us to employ the well-known division algorithm—if we have two elements $a, b \in R$ then by successive "divisions"

$$\begin{aligned} a &= q_0 b + r_0, \\ b &= q_1 r_0 + r_1, \\ r_0 &= q_2 r_1 + r_2, \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Theorem 4.18

Let R be a Euclidean domain, and consider nonzero $a, b \in R$. If $d = r_n$ is the last nonzero remainder in the division algorithm for a, b, then d is a greatest common divisor of a, b and $(d) = (a, b)$.

Proof. (Sketch) We need only show that $(d) = (a, b)$. By going backwards in the algorithm we see that d divides a and b, so $(a, b) \subseteq (d)$. We can also see that each r_i is in (a, b), meaning $(d) \subseteq (a, b)$. □

4.5 Principal Ideal Domains

Now we'll generalize a bit and consider the class of integral domains for which every ideal is principal. Note that we've already seen this to be true for Euclidean domains.

Definition: Principal ideal domain

A principal ideal domain is an integral domain in which every ideal is principal.

Theorem 4.19

Every nonzero prime ideal in a PID is a maximal ideal.

Proof. Let R be a PID and let (p) be a nonzero prime ideal contained in a maximal ideal (m). (The existence of such a maximal ideal relies on Zorn's lemma.) Since $(p) \subseteq (m)$, $p = rm$ for some $r \in R$ and either $r \in (p)$ or $m \in (p)$. If $r \in (p)$ then $r = ps$ for some $s \in R$, so $p = psm$ and m is a unit, a contradiction since (m) is a proper ideal. Thus $m \in (p)$ and so $(p) = (m)$. □

Theorem 4.20

If $R[x]$ is a PID then R is a field.

Proof. If $R[x]$ is a PID then R must be an integral domain, since $R \subset R[x]$. The ideal (x) is a nonzero prime ideal since $R[x]/(x) \cong R$ is an integral domain, so by the above theorem (x) is maximal and $R[x]/(x) \cong R$ is a field. □

Note that this corollary is useful when showing that $R[x]$ is a Euclidean domain if and only if R is a field.

Definition: Irredicubility

Let R be an integral domain.

- Let $r \in R$ be nonzero and not a unit. We say r is irreducible if $r = ab$ implies a or b is a unit.
- If $a, b \in R$, $u \in R^*$, and $a = ub$, then we say a and b are associates.

Theorem 4.21

In an integral domain, prime elements are irreducible.

Proof. Let R be an integral domain, let (p) be a nonzero prime ideal, and suppose $p = ab$ so either $a \in (p)$ or $b \in (p)$. Without loss of generality, suppose $a \in (p)$; then $a = pr$ for some $r \in R$, meaning $p = ab = prb$ and so b is a unit. Thus the prime p is irreducible. □

Theorem 4.22

In a PID, a nonzero element is prime if and only if it is irreducible.

Proof. Let R be a PID, suppose $p \in R$ is irreducible, and let $M = (m)$ be an ideal containing p. Then $p = rm$ for some $r \in R$ and since p is irreducible, r or m is a unit. Thus $(m) = (p)$ or $(m) = R$, which shows that the only ideals containing (p) are (p) and R. Thus (p) is maximal and therefore prime, so p is prime. The reverse direction follows from the previous result. □