Algebra course notes

Margaret Bilu

December 20, 2019

Contents

September 4:

1 Quantifiers, sets, maps, equivalence relations

Reference: Judson Chapter 1.

The quantifier $\forall$ should be read "for all", "for every". The quantifier $\exists$ should be read "there exists". You should never use them in a sentence in English, only in mathematical sentences!

1.1 Sets, subsets

A *set* is denoted using curly brackets $\{,\}$,

- either by specifying all of its elements:
$$A = \{2, 3, 7\},$$
$$B = \{0, 1, 2, 3, \ldots\}.$$
(Here, it is implicit that the set B consists of all non-negative integers.)

- or by writing it in the form
$$\{x,\ x \text{ satisfies } \mathcal{P}\}$$
where $\mathcal{P}$ is some property.

Important examples of sets include

$$\begin{aligned}
\mathbf{N} &= \{1, 2, 3, \ldots\} \quad \text{positive integers, or } \textit{natural numbers}\\
\mathbf{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad \text{integers}\\
\mathbf{Q} &= \left\{\frac{p}{q},\ p, q \in \mathbf{Z}, q \neq 0\right\} \quad \text{rational numbers}
\end{aligned}$$

and also the set $\mathbf{R}$ of real numbers and the set $\mathbf{C}$ of complex numbers.

We write $a \in A$ to denote that a is an element of the set A. A set A is a *subset* of another set B if every element of A is also an element of B. We write this $A \subset B$, or $A \subseteq B$. If A is not a subset of B, then we may write $A \not\subset B$. We say that A is a proper subset of B if $A \subset B$ but $A \neq B$. This is denoted $A \subsetneq B$, and in this case there exists an element of B which is not an element of A.

To show that two sets A and B are equal, it is often most convenient to show that $A \subset B$ and $B \subset A$.

The empty set is denoted $\varnothing$.

1.2 Unions, intersections, products

For two sets A and B, we define

- their union to be
$$A \cup B = \{x,\ x \in A \text{ or } x \in B\}$$
.
- their intersection to be
$$A \cap B = \{x,\ x \in A \text{ and } x \in B\}$$
.

One can also consider the union of more than two sets: for sets $A_1, \ldots, A_n$, we denote their union and intersection by

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n, \qquad \bigcap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n.$$

The first one is the set of all x belonging to at least one of the A_i. The second one is the set of all x belonging to all of the A_i.

If $A \cap B = \varnothing$, we say that A and B are *disjoint*.

We write
$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

Given two sets A and B, we define the cartesian product $A \times B$ to be the set of pairs (a, b) such that $a \in A$ and $b \in B$.

$$A \times B = \{(a, b),\ a \in A, b \in B\}.$$

More generally, we can define products of more than two sets:

$$\prod_{i=1}^{n} A_i = A_1 \times \ldots \times A_n.$$

If $A_1 = \ldots = A_n = A$, then we write this A^n.

1.3 Maps

A map $f : A \to B$ is an operation associating to every element $a \in A$ a unique element of B, denoted by $f(a)$. We denote this $f : a \mapsto f(a)$. The set A is called the *domain* of f. The *image* of f, denoted by $f(A)$, is the subset of B defined by

$$f(A) = \{b \in B : \ \exists a \in A, \ f(a) = b\}.$$

More generally, for any subset $A' \subset A$, we may define

$$f(A') = \{b \in B : \ \exists a \in A', \ f(a) = b\}.$$

An important example of the map is the *identity map* $\mathrm{id} : A \to A$, $a \mapsto a$, sending each element of A to itself. We may write it id_A if we want to specify the set it is the identity of.

The map f is said to be *injective*, or *one-to-one*, if distinct elements of A have distinct images in B. In other words:

$$\forall a, a' \in A, \ a \neq a' \ \Rightarrow f(a) \neq f(a'),$$

which is the same as

$$\forall \ a, a' \in A, \quad f(a) = f(a') \Rightarrow a = a'.$$

The map f is said to be *surjective*, or *onto*, if $f(A) = B$. In other words, every element of B is of the form $f(a)$ for some $a \in A$:

$$\forall b \in B, \ \exists a \ \in A, \ f(a) = b.$$

A map which is both injective and surjective is called *bijective*.

Let $f : A \to B$ and $g : B \to C$ be two maps. We define the *composition* of f and g, denoted by $g \circ f$, to be the map $a \mapsto g(f(a))$.

A map $f : A \to B$ is said to be *invertible* if there exists a map $g : B \to A$, called the *inverse* of f, such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. A map is invertible if and only if it is bijective.

1.4 Equivalence relations

A *relation* on a set E is a subset $R \subset E \times E$. If $(x, y) \in R$, we write xRy.

Definition 1.4.1. The relation R is an *equivalence relation* if it satisfies the following:

1. (reflexive) $\forall x \in E$, xRx;
2. (symmetric) $\forall x, y \in E$, if xRy then yRx;
3. (transitive) $\forall x, y, z \in E$, if xRy and yRz then xRz.

Most of the time, we will use some special notation, like $\sim$ or $\equiv$, for equivalence relations, instead of R.

Example 1.4.2. We define a relation $\sim$ on $\mathbf{Z}$ given by $x \sim y$ if $x - y$ is even. It is easy to check that this is an equivalence relation on $\mathbf{Z}$. In fact, it is a special case of the congruence relation which we will encounter later.

Definition 1.4.3. Let X be a set. A *partition* of X is a collection $(X_i)_{i \in I}$ of nonempty subsets of X (indexed by some set I) which are pairwise disjoint (i.e. for all distinct $i, j \in I$, $X_i \cap X_j = \varnothing$) and such that their union is all of X:

$$\bigcup_{i \in I} X_i = X.$$

The X_i are called the *parts* of the partition.

Example 1.4.4. Let E be the set of even integers and O the set of odd integers. Then E and O form a partition of $\mathbf{Z}$.

Example 1.4.5. For every letter $\square$ of the alphabet, we denote by $X_\square$ the set of students in our class whose first name begins with $\square$. Then the collection $X_A, X_B, \ldots, X_Z$ forms a partition of the set of students of this class.

Definition 1.4.6. Let $\sim$ be an equivalence relation on a set X. For every $x \in X$, we define the *equivalence class* of x to be the set

$$[x] := \{y \in X, y \sim x\}.$$

Proposition 1.4.7. *If $y \in [x]$, then $[y] \subset [x]$.*

Proof. Let $z \in [y]$. Then $z \sim y$. By transitivity, we have $z \sim x$, so $z \in [x]$. $\square$

Proposition 1.4.8. *Let $x, x' \in X$. Then either $[x] = [x']$ or $[x] \cap [x'] = \varnothing$.*

Proof. If $[x] \cap [x'] = \varnothing$ we are done. If not, there exists $y \in [x] \cap [x']$. We want to show that $[x] = [x']$. By definition, we have $y \sim x$ and $y \sim x'$. By symmetry and transitivity we then have $x \sim x'$, so $x \in [x']$. This implies $[x] \subset [x']$. Similarly, we show that $[x'] \subset [x]$, whence the result. $\square$

Proposition 1.4.9. *Let $\sim$ be an equivalence relation on a set X. Then the equivalence classes of $\sim$ form a partition of X. Conversely, every partition of the set X induces an equivalence relation on X, by definining $x \sim y$ if x and y lie in the same part of the partition.*

Definition 1.4.10. Let X be a set with an equivalence relation $\sim$. We define the *quotient space* of X for $\sim$ to be the set of equivalence classes of $\sim$, denoted by $X/_\sim$. We define the *quotient map* to be the natural map

$$\begin{array}{ccc} X & \to & X/_\sim \\ x & \mapsto & [x] \end{array}$$

2 Integers

Judson, Chapter 2, Section 2.2.

2.1 Addition and multiplication on the set of integers Z

The set of integers $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is endowed with an *addition operation* (or *addition law*)

$$\begin{array}{rccc} + : & \mathbf{Z} \times \mathbf{Z} & \to & \mathbf{Z} \\ & (m, n) & \mapsto & m + n \end{array}$$

We know that this operation satisfies the following properties:

G1 For all $x, y, z \in \mathbf{Z}$,

$$(x + y) + z = x + (y + z),$$

that is, it is *associative*.

G2 There exists an element in $\mathbf{Z}$, namely 0, such that for all $x \in \mathbf{Z}$,

$$0 + x = x = x + 0.$$

Thus, addition has a *zero element*.

G3 Every element $x \in \mathbf{Z}$ has an *inverse* in $\mathbf{Z}$ with respect to addition, namely $-x$, which satisfies the property that

$$x + (-x) = 0 = (-x) + x.$$

Moreover, addition satisfies the following additional property **GC**: for all $x, y \in \mathbf{Z}$, we have $x + y = y + x$, that is, addition is *commutative*.

The three properties **G1**, **G2**, **G3**, that is, associativity, existence of a zero element and existence of inverses, are characteristic of an important algebraic structure called a *group*. A group satisfying additionally property **GC** is called a *commutative* (or *abelian*) group. The above shows that the set of integers $(\mathbf{Z}, +)$ endowed with addition is a commutative group. We are going to see many other examples of groups in this course, and are going to study groups in general.

Note that integers can not only be added, but also multiplied: the set of integers is also endowed with a *multiplication operation* (or *multiplication law*)

$$\begin{array}{rccc} \cdot : & \mathbf{Z} \times \mathbf{Z} & \to & \mathbf{Z} \\ & (m, n) & \mapsto & mn \end{array}$$

However the set of integers $(\mathbf{Z}, \cdot)$ endowed with this law is not a group. Indeed, whereas **G1** and **G2** are satisfied (multiplication is associative:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$

and the integer 1 is clearly a zero element, since $1 \cdot x = x = x \cdot 1$ for any integer x), inverses do not always exist. For example, an inverse x for the integer 2 should satisfy $2x = 1$ which means that $x = \frac{1}{2}$, but $\frac{1}{2}$ is not an integer.

Exercise 2.1.1. More generally, prove that the only elements of $\mathbf{Z}$ which have inverses (we say they are *invertible*) for the multiplication law are 1 and -1. Check that $(\{1, -1\}, \cdot)$ is a commutative group.

Thus, the set of integers is a group for the addition operation, but not for the multiplication operation. However, we can combine these two operations to get an even richer structure on $\mathbf{Z}$, that of a *ring*. More precisely, we have the following three additional properties:

R1 Multiplication is associative: for all $x, y, z \in \mathbf{Z}$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

R2 Multiplication is distributive with respect to addition: for all $x, y, z \in \mathbf{Z}$,

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

and

$$(y + z) \cdot x = y \cdot x + z \cdot x.$$

R3 Multiplication has a unit element, namely 1, which satisfies for all $x \in \mathbf{Z}$,

$$x \cdot 1 = 1 \cdot x = x.$$

The properties **G1**, **G2**, **G3**, **GC**, **R1** , **R2** and **R3** characterize an algebraic structure called a *ring*. In short, a ring is a commutative group with an extra operation that is well-behaved with respect to the group operation. The multiplication in $\mathbf{Z}$ moreover satisfies property **RC**: for all $x, y \in \mathbf{Z}$,

$$x \cdot y = y \cdot x$$

which makes $(\mathbf{Z}, +, \cdot)$ into a *commutative ring*. In particular, when **RC** is satisfied, then the conditions in **R2** are in fact equivalent.

We are probably not going to talk more about rings in this course, and will rather focus on the theory of groups.

2.2 Divisibility

We are now going to view some arithmetic properties of the set of integers.

Definition 2.2.1. If a and b are integers, we say that *a is divisible by b*, or that *b divides a*, if there exists an integer $k \in \mathbf{Z}$ such that $a = kb$.

Notation 2.2.2. We denote this by $b|a$.

Exercise 2.2.3. Divisibility satisfies the following properties:

(a) For every integer a, the integers 1, -1, a and $-a$ divide a.

(b) Transitivity: If $a|b$ and $b|c$ then $a|c$.

(c) 0 does not divide any non-zero integer.

(d) All integers divide 0.

(e) If a, b are non-zero then $a|b$ and $b|a$ implies $a = b$ or $a = -b$.

(f) If a divides b and a divides c, then a divides $ub + vc$ for all integers $u, v \in \mathbf{Z}$.

2.3 Euclidean division

Proposition 2.3.1. *Let a, b be integers, with $b \neq 0$. There is a unique way of writing a in the form*

$$a = bq + r$$

where q, r are integers, with r satisfying $0 \leq r < |b|$. The integer q is called the quotient, and r is called the remainder.

September 11:

2.4 GCD and Euclid's algorithm

Definition 2.4.1. Let a, b be two integers, not both zero. The *greatest common divisor* of a, b, denoted $\gcd(a, b)$ is the largest positive integer that divides both a and b. We say that a and b are *relatively prime*, or *coprime*, if $\gcd(a, b) = 1$.

Exercise 2.4.2. Let a and b be two integers, with $b \neq 0$, and write

$$a = bq + r$$

the Euclidean division of a by b. Show that $\gcd(a, b) = \gcd(b, r)$.

The greatest common divisor may be computed using *Euclid's algorithm*, which works as follows:

Let a and b be positive integers, with $a > b$. Then we may write a sequence of Euclidean divisions in the following manner:

$$\begin{array}{rcll} a & = & bq_0 + r_1, & 0 \leq r_1 < b \\ b & = & r_1 q_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 & = & r_2 q_2 + r_3, & 0 \leq r_3 < r_2 \\ & \vdots & & \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & r_n q_n. & \end{array}$$

The sequence $r_1, r_2, \dots$ of successive remainders is a strictly decreasing sequence of non-negative integers, therefore it must hit zero at some point. The last non-zero remainder r_n will be the greatest common divisor of a and b.

Proposition 2.4.3. *Let a and b be two integers, not both zero. Then there exist integers u and v such that*

$$ua + vb = \gcd(a, b).$$

Remark 2.4.4. It it obvious that the left-hand side in this proposition must be a multiple of $\gcd(a, b)$. What is remarkable is that we can actually make it equal to $\gcd(a, b)$ by adequately choosing u and v.

Remark 2.4.5. In particular, any integer d which divides both a and b will divide $\gcd(a, b)$.

Exercise 2.4.6. Compute the greatest common divisor of 234 and 51 and find u, v such that

$$234u + 51v = \gcd(234, 51).$$

Proposition 2.4.7 (Bézout's theorem)**.** *Let a and b be two integers, not both zero. Then a and b are coprime if and only if there exist integers u and v such that*

$$au + bv = 1.$$

Proof. If a and b are coprime, the result follows from Proposition 2.4.3. Conversely, assume there exist integers u and v such that $au + bv = 1$. Then $\gcd(a, b)$ divides the left-hand side, so it must divide 1. Since it must be positive, this implies it is equal to 1. □

Proposition 2.4.8 (Gauss lemma)**.** *Let a, b, c be integers. If a divides bc and a is relatively prime to b then a divides c.*

2.5 Unique factorization of integers

Definition 2.5.1. An integer $p > 1$ is a *prime number* (or simply a *prime*) if its only positive divisors are 1 and p.

Proposition 2.5.2 (Fundamental theorem of arithmetic)**.** *Let $n \geq 2$ be an integer. Then the integer n may be written as a product*

$$n = p_1 p_2 \dots p_k,$$

where $p_1, \dots, p_k$ are primes (not necessarily distinct). Furthermore, this factorization is unique, that is, if $n = q_1 q_2 \dots q_l$ where $q_1, \dots, q_l$ are primes, then $k = l$ and the q_i's are just the p_i's rearranged.

Remark 2.5.3. One may use exponents if one wants the primes in the decomposition to be distinct. More precisely, n may be written in the form

$$n = p_1^{a_1} \dots p_r^{a_r}$$

where $p_1, \dots p_r$ are distinct primes, and $a_1, \dots a_r$ are positive integers. This decomposition is unique up to rearranging the p_i's.

Example 2.5.4. We have

$$24 = 2^3 \times 3,$$

$$30 = 2 \times 3 \times 5.$$

September 16:

2.6 Congruence classes

Judson Section 3.1 (up to Prop 3.4) Let $n > 1$ be an integer. We define a relation on the integers by

$$a \equiv b \pmod{n} \quad \text{if} \quad n \text{ divides } a - b.$$

We say "a is congruent to b modulo n".

Proposition 2.6.1. *This is an equivalence relation.*

We have the following equivalent characterizations:

$$\begin{aligned} a \equiv b \pmod{n} \quad &\Leftrightarrow \quad a = b + kn \text{ for some } k \in \mathbf{Z} \\ &\Leftrightarrow \quad a \in b + n\mathbf{Z} = \{b + nk,\ k \in \mathbf{Z}\}. \end{aligned}$$

Remark 2.6.2. Write $a = qn + r$, where $0 \leq r < n$, the Euclidean division of a by n. Then n divides $a - r$, so $a \equiv r \pmod{n}$. In particular, any integer is congruent modulo n to some integer in the set $\{0, \dots, n-1\}$.

Exercise 2.6.3. Show that $a \equiv b \pmod{n}$, if and only if a and b have the same remainder in the Euclidean division by n.

Since there are exactly n possible remainders in the Euclidean division by n, this equivalence relation has exactly n equivalence classes, namely

$$n\mathbf{Z},\ 1 + n\mathbf{Z},\ 2 + n\mathbf{Z},\ \dots\ ,\ (n-1) + n\mathbf{Z}.$$

They are called *congruence classes* modulo n. The congruence class modulo n of an integer a will be denoted $[a]_n$, or just $[a]$. We have $[a] = [b]$ if and only if $a \equiv b \pmod{n}$. If C is a congruence class modulo n, any integer a such that $C = [a]$ is called a representative of the class.

Definition 2.6.4. We define

$$\mathbf{Z}/n\mathbf{Z} = \{[0], \dots, [n-1]\}$$

to be the quotient space associated to the above equivalence relation. The quotient map

$$\pi : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$$

sending an integer a to its congruence class $[a]$ is called the *reduction modulo n* map.

Lemma 2.6.5. *Let $n \geq 2$ be an integer. For all integers $a, b, a', b' \in \mathbf{Z}$, if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then*

1. $a + b \equiv a' + b' \pmod{n}$
2. $ab \equiv a'b' \pmod{n}$.

In terms of congruence classes, this lemma can be rewritten as: for all $a, b, a', b' \in \mathbf{Z}$, if $[a] = [a']$ and $[b] = [b']$ then $[a + b] = [a' + b']$ and $[ab] = [a'b']$. In other words, for any two congruence classes A and B modulo n, whatever the choice of representatives $A = [a]$ and $B = [b]$, the classes $[a + b]$ and $[ab]$ will always be the same, they do not depend on the choice of the representatives a and b. This means that the following two operations on $\mathbf{Z}/n\mathbf{Z}$ are well-defined:

$$[a] \oplus [b] = [a + b]$$

and

$$[a] \odot [b] = [ab].$$

Remark 2.6.6. For the moment, we use the notation $\oplus$ and $\odot$ to make a clear distinction between addition and multiplication on classes and addition and multiplication on integers, but later we will simply write $+$ and $\cdot$.

September 18:

Proposition 2.6.7. 1. *$(\mathbf{Z}/n\mathbf{Z}, \oplus)$ is a commutative group. The identity for $\oplus$ is the class $[0]$, and the inverse of an element $[a] \in \mathbf{Z}/n\mathbf{Z}$ is $[-a]$.*

2. *The operation $\odot$ is associative and has an identity given by $[1]$.*

Remark 2.6.8. The previous proposition is in fact a direct consequence of the properties of addition and multiplication on $\mathbf{Z}$ seen in section 2.1. In particular, $(\mathbf{Z}/n\mathbf{Z}, \odot)$ is not a group because for example $[0]$ does not have an inverse.

Remark 2.6.9. In fact, we have that $(\mathbf{Z}/n\mathbf{Z}, \oplus, \odot)$ is a commutative ring in the terminology of section 2.1.

Remark 2.6.10. By definition, the quotient map $\pi : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ is compatible with both binary operations, in the sense that for all integers a, b, we have

$$\pi(a + b) = \pi(a) \oplus \pi(b),$$

$$\pi(a \cdot b) = \pi(a) \odot \pi(b),$$

as well as $\pi(0) = [0]$ and $\pi(1) = [1]$. We say that $\pi : (\mathbf{Z}, +) \to (\mathbf{Z}/n\mathbf{Z}, \oplus)$ is a group homomorphism, and that $\pi : (\mathbf{Z}, +, \cdot) \to (\mathbf{Z}/n\mathbf{Z}, \oplus, \odot)$ is a ring homomorphism.

2.7 Units in $\mathbf{Z}/n\mathbf{Z}$

Motivating question: what do we need to do with $\mathbf{Z}/n\mathbf{Z}$ to turn it into a group for $\odot$?

Definition 2.7.1. A congruence class $[a] \in \mathbf{Z}/n\mathbf{Z}$ is said to be *invertible for* $\odot$, or, *a unit*, if there exists $[b] \in \mathbf{Z}/n\mathbf{Z}$ such that

$$[a] \odot [b] = [b] \odot [a] = [1].$$

Such a class $[b]$ is then called a *(multiplicative) inverse* of $[a]$, and denoted by $[a]^{-1}$.

Remark 2.7.2. A multiplicative inverse is unique: indeed, if $[b']$ is another class satisfying the same property, we have

$$[b] = [b] \odot [1] = [b] \odot [a] \odot [b'] = [1] \odot [b'] = [b'].$$

Notation 2.7.3. The set of units of $\mathbf{Z}/n\mathbf{Z}$ is denoted by $(\mathbf{Z}/n\mathbf{Z})^\times$.

This definition can also be reformulated in terms of congruences modulo n:

Definition 2.7.4. An integer a is said to be invertible modulo n if there exists an integer b such that $ab \equiv 1 \pmod{n}$. The integer b is called an inverse of a modulo n.

Remark 2.7.5. Note that b is not unique: if $ab \equiv 1 \pmod{n}$, then we have $ab' \equiv 1 \pmod{n}$ for all $b' \equiv b \pmod{n}$.

It is clear that a and b are inverses to each other modulo n if and only if $[a]$ and $[b]$ are inverse to each other for $\odot$.

Remark 2.7.6. The class $[0]$ is never a unit, because for any $[b] \in \mathbf{Z}/n\mathbf{Z}$,

$$[0] \odot [b] = [0 \cdot b] = [0] \neq [1]$$

(the latter being true because $n > 1$). The classes $[1]$ and $[n-1] = [-1]$ are always units because $[1] \odot [1] = [1 \cdot 1] = [1]$ and $[-1] \odot [-1] = [(-1) \cdot (-1)] = [1]$.

Example 2.7.7. Let us find the units in $\mathbf{Z}/5\mathbf{Z} = \{[0], [1], [2], [3], [4]\}$. Note that

$$[2] \odot [3] = [6] = [1],$$

so $[2]$ and $[3]$ are units. By remark 2.7.6, we have $(\mathbf{Z}/5\mathbf{Z})^\times = \{[1], [2], [3], [4]\}$.

Example 2.7.8. Let us find the units in $\mathbf{Z}/4\mathbf{Z} = \{[0], [1], [2], [3]\}$. Note that

$$[2] \odot [2] = [4] = [0].$$

This means that $[2]$ cannot be a unit. Indeed, if $[b]$ is a class such that

$$[2] \odot [b] = [1],$$

multiplying by $[2]$ on both sides we get

$$[2] \odot [2] \odot [b] = [2] \odot [1] = [2]$$

which gives the equality $[0] = [2]$, a contradiction since 0 is not congruent to 2 modulo 4. Thus, by remark 2.7.6, we have $(\mathbf{Z}/4\mathbf{Z})^\times = \{[1], [3]\}$.

Exercise 2.7.9. Find the units in $\mathbf{Z}/6\mathbf{Z}$, $\mathbf{Z}/7\mathbf{Z}$, $\mathbf{Z}/9\mathbf{Z}$.

Proposition 2.7.10. *For any $n \geq 2$, $((\mathbf{Z}/n\mathbf{Z})^\times, \odot)$ is a commutative group.*

Theorem 2.7.11. *Let $n \geq 2$ be an integer. The set $(\mathbf{Z}/n\mathbf{Z})^\times$ is given by the congruence classes of integers coprime to n, i.e.:*

$$(\mathbf{Z}/n\mathbf{Z})^\times = \{[k] \in \mathbf{Z}/n\mathbf{Z},\ 1 \leq k \leq n-1 \textit{ and } \gcd(k,n) = 1\}.$$

Proof. Let $k \in \{1, \ldots, n-1\}$ be relatively prime to n. By Bézout's theorem, this is equivalent to the existence of integers u and v such that $uk + vn = 1$. This in turn is equivalent to $uk \equiv 1 \pmod n$, that is, k is invertible modulo n with inverse u. □

Remark 2.7.12. Thus, the set $(\mathbf{Z}/n\mathbf{Z})^\times$ is exactly the set of all non-zero classes in $\mathbf{Z}/n\mathbf{Z}$ if and only if n is a prime number.

September 23:

Remark 2.7.13. Recall the Euler function ϕ from Exercise 5 in Homework 2. By definition, for all $n \geq 2$, $\phi(n)$ is equal to the number of elements of $(\mathbf{Z}/n\mathbf{Z})^\times$.

2.8 Back to congruences

The theory of units allows us to characterize the integers we can divide by when working modulo n.

Proposition 2.8.1. *Let $n \geq 2$ be an integer and let c be an integer coprime to n. For any $a, b \in \mathbf{Z}$, if $ac \equiv bc \pmod n$ then $a \equiv b \pmod n$.*

Remark 2.8.2. The equivalent property at the level of $\mathbf{Z}/n\mathbf{Z}$ is called the *cancellation law*: if A, B, C are elements of $\mathbf{Z}/n\mathbf{Z}$ and C is a unit, then $A \odot C = B \odot C$ implies $A = B$.

Example 2.8.3. Assume we want to find all integers x such that $3x \equiv 2 \pmod 7$. First of all, we compute an inverse of 3 modulo 7. Since $3 \times 5 \equiv 1 \pmod 7$, 5 is such an inverse. We multiply both sides of the equation by 5, to get $x \equiv 10 \pmod 7$, or, in other words $x \equiv 3 \pmod 7$. Conversely, if this condition is satisfied, we clearly have $3x \equiv 2 \pmod 7$. The integers satisfying the initial equation are therefore exactly the integers in the set $3 + 7\mathbf{Z}$, that is, the integers of the form $3 + 7k$, $k \in \mathbf{Z}$.

Example 2.8.4. The coprimeness condition in proposition 2.8.1 is necessary: for example, in the congruence $2 \times 3 \equiv 0 \pmod 6$ we can neither conclude that 2 is congruent to 0 modulo 6, nor that 3 is congruent to 0 modulo 6.

2.9 Conclusion of the chapter

Before going on to the next chapter, make sure you:

- Understand what it means for an integer to divide another integer.
- Know about existence and uniqueness of Euclidean division, and know how to find the quotient and remainder in a concrete example.
- Can find the gcd of two numbers using the Euclidean algorithm, and understand why the Euclidean algorithm works.
- Can compute, for two integers a and b, integers u, v such that $ua + vb = \gcd(a, b)$ using the extended Euclidean algorithm.
- Know about Bézout's theorem.
- Know the fundamental theorem of arithmetic.
- Understand what it means for two integers to be congruent modulo n.
- Understand how congruence classes modulo n look like, and why there are n of them.
- Know how to add and multiply congruence classes.
- Know how to find the units in $\mathbf{Z}/n\mathbf{Z}$ for concrete values of n.

3 Groups

3.1 Laws of composition

Definition 3.1.1. A *law of composition* (or *binary operation*) on a set S is a function

$$S \times S \to S.$$

Notation 3.1.2. The image of a pair $(x, y) \in S \times S$ may be denoted $x * y$, or just xy, or with whatever appropriate symbol there might be.

Example 3.1.3. We have encountered two laws of composition on the set of integers $\mathbf{Z}$, addition and multiplication.

Example 3.1.4. Let X be a set, and consider the set $\mathcal{F}(X, X)$ of functions $X \to X$. For any two such functions f and g, their composition $f \circ g$ is again an element of $\mathcal{F}(X, X)$. Thus, composition of functions defines a law of composition

$$\begin{array}{ccc} \mathcal{F}(X,X) \times \mathcal{F}(X,X) & \to & \mathcal{F}(X,X) \\ (f,g) & \mapsto & f \circ g \end{array}$$

Example 3.1.5. Let $n \geq 1$ be an integer and let $M_n(\mathbf{R})$ be the set of $n \times n$ matrices with real coefficients. Then addition and multiplication of matrices are both laws of composition on $M_n(\mathbf{R})$.

Example 3.1.6. We can also define some less classical laws of composition, e.g., on the set of real numbers $\mathbf{R}$

$$x * y = x + y^2.$$

Definition 3.1.7. Let S be a set and

$$\begin{array}{ccc} S \times S & \to & S \\ (x, y) & \mapsto & x * y \end{array}$$

a law of composition on S. We say the law of composition is

- associative if for all $x, y, z \in S$, we have

$$(x * y) * z = x * (y * z).$$

- commutative if for all $x, y \in S$,

$$x * y = y * x.$$

Remark 3.1.8. If the law of composition is associative, it makes sense to write

$$x_1 * x_2 * \ldots * x_n$$

(without any brackets) for any elements $x_1, \ldots, x_n \in S$.

Exercise 3.1.9. Which of the above examples of laws of composition are associative? Which are commutative?

Notation 3.1.10. Traditionally, we drop the symbol $*$ and denote a law of composition by $(x, y) \mapsto xy$ (this is called the *multiplicative notation*), but if it happens to be commutative, the *additive notation* $(x, y) \mapsto x + y$ may be used. For the moment, for clarity, we will keep using the symbol $*$.

Definition 3.1.11. Let S be a set and

$$\begin{array}{ccc} S \times S & \to & S \\ (x, y) & \mapsto & x * y \end{array}$$

a law of composition on S. An *identity* for this law is an element $e \in S$ such that for all $x \in S$, one has

$$e * x = x \quad \text{and} \quad x * e = e.$$

Notation 3.1.12. The identity element is often denoted 1, or 0 if we are using the additive notation.

Exercise 3.1.13. Any law of composition has at most one identity. Indeed, if we have two identities e and e', then the product $e * e'$ is equal to e because e' is an identity, and to e' because e is an identity, so $e = e * e' = e'$.

Exercise 3.1.14. Find identity elements for the above examples of composition laws in the case they exist.

Definition 3.1.15. Let S be a set and

$$\begin{array}{rcl} S \times S & \to & S \\ (x, y) & \mapsto & x * y \end{array}$$

an associative law of composition on S with identity e. We say an element $x \in S$ is invertible (or has an inverse) with respect to $*$ if there exists an element $y \in S$ such that

$$x * y = e \quad \text{and} \quad y * x = e.$$

Exercise 3.1.16. Show that any element has at most one inverse.

Notation 3.1.17. The inverse of $x \in S$ is denoted x^{-1}.

Proposition 3.1.18. *1. Let $x, y \in S$ be two invertible elements. Then their product is invertible, and $(x * y)^{-1} = y^{-1} * x^{-1}$.*

2. Let $x \in S$ be an invertible element. Then x^{-1} is invertible, and $(x^{-1})^{-1} = x$.

Exercise 3.1.19. Investigate invertible elements for those of the above laws that have an identity.

3.2 Groups

Judson section 3.2

Definition 3.2.1. A group $(G, *)$ is a set G together with a law of composition

$$\begin{array}{rcl} G \times G & \to & G \\ (x, y) & \mapsto & x * y \end{array}$$

such that

G1 The law of composition $*$ is associative.

G2 The law of composition $*$ has an identity.

G3 Every element of G has an inverse with respect to $*$.

Definition 3.2.2. A group $(G, *)$ is said to be *commutative* or *abelian* if its law of composition $*$ is commutative.

Proposition 3.2.3 (Cancellation law)**.** *Let $(G, *)$ be a group, and x, y, z elements of G. If $x * z = y * z$ or $z * x = z * y$, then $x = y$.*

September 25:

Example 3.2.4.
1. The trivial group $\{0\}$ is a set with one element, which is the identity element of the group.
2. $(\mathbf{Z}, +)$ and $(M_n(\mathbf{R}), +)$ are commutative groups. So is $(\mathbf{Z}/n\mathbf{Z}, \oplus)$ for every $n \geq 2$.
3. Whenever we have a set $(S, *)$ with an associative law with identity, the subset $U \subset S$ of invertible elements of this set will give a group $(U, *)$. Indeed, $*$ is a law of composition on U by proposition 3.1.18, it will still be associative as a restriction of an associative law, the identity belong to U because it is its own inverse, and all elements are invertible with their inverses belonging to U by proposition 3.1.18. Examples of this sort include:
   (a) The commutative group of multiplicative units of $\mathbf{Z}$, that is $(\{1, -1\}, \cdot)$.
   (b) The commutative group $(\mathbf{R}^\times, \cdot)$ of nonzero real numbers.
   (c) The commutative group of multiplicative units $((\mathbf{Z}/n\mathbf{Z})^\times, \odot)$ of $\mathbf{Z}/n\mathbf{Z}$.
   (d) The group $(\mathcal{B}(X, X), \circ)$, where $\mathcal{B}(X, X) \subset \mathcal{F}(X, X)$ is the subset of functions $f : X \to X$ which are bijective.
   (e) The group $(GL_n(\mathbf{R}), \cdot)$ of invertible $n \times n$ matrices with real coefficients.

Definition 3.2.5. The *order* of a group G is the number of elements that it contains. We denote it by $|G|$. If the order is finite, we say that G is finite, otherwise G is said to be infinite.

Example 3.2.6. The group $(\mathbf{Z}/n\mathbf{Z}, \oplus)$ is of order n.

Notation 3.2.7. Let $x \in G$ and $n \geq 0$ an integer. We denote by x^n the product $x * x \ldots * x$ where x occurs n times (in particular, $x^0 = e$ is the identity element), and by x^{-n} the element $(x^{-1})^n$.

Proposition 3.2.8. *Let $(G, *)$ be a group. Then for all $x \in G$ and all $m, n \in \mathbf{Z}$, we have*
1. $(x^n)^{-1} = x^{-n}$.
2. $x^m * x^n = x^{m+n}$.
3. $(x^m)^n = x^{mn}$.

Remark 3.2.9. Pay attention to the fact that in general,

$$(x * y)^n = (x * y) * (x * y) * \ldots * (x * y)$$

is not equal to $x^n * y^n$, as $*$ is not commutative in general.

Remark 3.2.10. If the additive notation is used, we write nx instead of x^n.

It is possible to record the structure of a finite group $(G, *)$ in a so-called *Cayley table* (or *multiplication table*), where for every $x, y \in G$, we give the value of $x * y$. Here, for example we have the Cayley table of $(\mathbf{Z}/5\mathbf{Z}, +)$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The commutativity of $\mathbf{Z}/5\mathbf{Z}$ translates into the fact that the table is symmetric with respect to its diagonal.

Moreover, it follows from the cancellation law that every row and column in a Cayley table contains every element of the group exactly once.

3.3 Subgroups

Judson section 3.3.

Sometimes we want to study groups sitting in some larger group.

Definition 3.3.1. Let $(G, *)$ be a group. A *subgroup* of G is a subset $H \subset G$ with the following properties:

- For all $x, y \in H$, we have $x * y \in H$.
- H contains the identity of G.
- For all $x \in H$, we have $x^{-1} \in H$.

Proposition 3.3.2. *Let $(G, *)$ be a group and $H \subset G$ a subgroup of G. Then $*$ defines a law of composition on H and $(H, *)$ is a group.*

Example 3.3.3.
1. Every group G has two obvious subgroups: the group G itself, and the trivial subgroup $\{e\}$ containing only the identity element. We say a subgroup is a *proper subgroup* if it is not one of these two.

   September 30th:

2. The groups $(\mathbf{Z}, +)$ and $(\mathbf{Q}, +)$ are both subgroups of $(\mathbf{R}, +)$.
3. The set $m\mathbf{Z}$ of multiples of an integer $m \geq 1$ defines a subgroup of the group $(\mathbf{Z}, +)$.
4. The set $SL_n(\mathbf{R})$ of matrices of determinant 1 defines a subgroup of the group $(GL_n(\mathbf{R}), \cdot)$ of invertible $n \times n$ matrices with real coefficients.

Proposition 3.3.4. *The only subgroups of $(\mathbf{Z}, +)$ are the trivial subgroup $\{0\}$ and the sets $m\mathbf{Z}$ for all $m \geq 1$.*

3.4 Products of groups

From now on, we will write general groups *multiplicatively*, without the symbol $*$, so that the product of two elements x, y will be simply denoted xy. The identity element will be denoted e.

Let G, H be two groups. Then the cartesian product of the underlying sets $G \times H$ may be endowed with a law of composition by putting, for all $g, g' \in G, h, h' \in H$:

$$(g, h)(g', h') = (gg', hh').$$

Proposition 3.4.1. *The set $G \times H$ with this law of composition is a group.*

More generally, whenever we have a family $(G_i)_{i \in I}$ of groups, we may construct the product group $\prod_{i \in I} G_i$.

Example 3.4.2.

1. The group $(\mathbf{R}^2, +)$ may be seen as the product of the group $(\mathbf{R}, +)$ with itself.
2. The group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ has six elements: $(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)$.

October 2nd:

3.5 Cyclic groups

Judson, Section 4.1

Proposition 3.5.1. *Let G be a group and let $a \in G$. Then the set*

$$\langle a \rangle = \{a^k,\ k \in \mathbf{Z}\}$$

is a subgroup of G. Furthermore, it is the smallest subgroup of G containing a. It is called the (cyclic) subgroup of G generated by a.

Remark 3.5.2. One must pay attention to the fact that different powers of a may represent the same element of the group (see following examples).

Example 3.5.3.

1. The cyclic subgroup generated by the identity e is just the trivial subgroup $\{e\}$.
2. The cyclic subgroup generated by -1 in $(\mathbf{R}^\times, \cdot)$ is $\{1, -1\}$. The cyclic subgroup of $(\mathbf{R}^\times, \cdot)$ generated by 2 is $\{2^n,\ n \in \mathbf{Z}\}$.
3. The cyclic subgroup generated by 1 in $(\mathbf{R}, +)$ is $\mathbf{Z}$.
4. The cyclic subgroup generated by 2 in $(\mathbf{Z}/6\mathbf{Z}, +)$ is $\{0, 2, 4\}$.

Proposition 3.5.4. *Let x be an element of a group G, and let P denote the set*

$$P = \{k \in \mathbf{Z},\ x^k = e\}.$$

Then

1. *The set P is a subgroup of the additive group $(\mathbf{Z}, +)$.*
2. *For any integers $r, s \in \mathbf{Z}$, we have $x^r = x^s$ if and only if $r - s \in P$.*
3. *Assume P is not the trivial subgroup, so that P is of the form $n\mathbf{Z}$ for some integer $n > 0$. Then the powers $e, x, x^2, \ldots, x^{n-1}$ are the distinct powers of the subgroup $\langle x \rangle$, and the order of $\langle x \rangle$ is n.*

Definition 3.5.5. Let G be a group. It is said to be *cyclic* if there exists an element a of G such that $G = \langle a \rangle$. In this case, a is said to be a *generator* of G.

Definition 3.5.6. For an element a of a group G, we define the *order* of a to be the smallest positive integer n such that $a^n = e$. In other words, the order of a is the order of the subgroup $\langle a \rangle$. If such an n does not exist, we say a is of infinite order, otherwise we say a is of finite order.

Using the proposition, we therefore have the following two possible behaviors for an element $x \in G$:

- either x is of infinite order, that is, $P = \{0\}$, the powers $x^r,\ r \in \mathbf{Z}$ are all distinct and $\langle x \rangle$ is infinite.
- or x is of finite order $n > 0$, that is, $P = n\mathbf{Z}$, and $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$ is a finite group of order n.

Example 3.5.7.
1. For every integer $n \geq 2$, the group $(\mathbf{Z}/n\mathbf{Z}, +)$ is a cyclic group of order n, since the class 1 is always a generator. The class -1 is also a generator. We therefore see that the generator of a cyclic group need not be unique.
2. The group $(\mathbf{Z}, +)$ is cyclic, with generators 1 and -1. Moreover, for every $m \in \mathbf{Z}$, $m\mathbf{Z}$ is the cyclic subgroup of $\mathbf{Z}$ generated by m. Therefore, all the subgroups of $\mathbf{Z}$ are cyclic.

October 7th:

3. The group of units $((\mathbf{Z}/9\mathbf{Z})^\times, \cdot)$ is a cyclic group, with generator 2. Indeed, as a set, $(\mathbf{Z}/9\mathbf{Z})^\times = \{1, 2, 4, 5, 7, 8\}$, and

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,$$

$$2^4 \equiv 7 \pmod 9,$$
$$2^5 \equiv 3 \pmod 9,$$
$$2^6 \equiv 1 \pmod 9.$$

4. For every n, $(\mathbf{C}^\times, \cdot)$ has a cyclic subgroup of order n, given by the n-th roots of unity:

$$U_n = \{e^{\frac{2\pi i k}{n}},\ k \in \{0, \dots n-1\}\}.$$

For example, for $n = 2$ we get the subgroup $\{1, -1\}$, for $n = 3$ we get $\{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$, and for $n = 4$ we get $\{1, i, -1, -i\}$. Note that the elements of U_n are the vertices of a regular n-gon in the complex plane.

5. Here are a few non-examples: $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ are not cyclic.

Proposition 3.5.8. *The generators of* $(\mathbf{Z}/n\mathbf{Z}, +)$ *are exactly the units, that is, the classes of integers coprime to* n.

Exercise 3.5.9. Every cyclic subgroup is abelian.

Proposition 3.5.10. *Every subgroup of a cyclic group is cyclic.*

Definition 3.5.11. Let G be a group and let S be a subset of G. The subgroup of G *generated by* S is the smallest subgroup of G containing all the elements of S. If this subgroup is equal to G, we say that S *generates* G, and its elements are called *generators* of G.

Remark 3.5.12. If $S = \{x\}$ is a singleton, then the subgroup of G generated by S is the cyclic subgroup generated by x.

Remark 3.5.13. The elements of the subgroup of G generated by S are exactly the elements of G that can be written in the form $s_1^{a_1} \dots s_k^{a_k}$ where $k \geq 0$ is an integer, $s_1, \dots, s_k$ are (not necessarily distinct) elements of S, and $a_1, \dots, a_k$ are integers.

Example 3.5.14. Let G be the group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. It is not cyclic, but it is generated by the subset $\{(1, 0), (0, 1)\}$.

October 9th:

3.6 Group homomorphisms

Definition 3.6.1. Let G and G' be groups. A *homomorphism* $\phi : G \to G'$ is a map from G to G' such that for all $x, y \in G$,

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

Intuitively, a homomorphism is a map between two groups which is compatible with the laws of composition in both groups.

Example 3.6.2. The following maps are homomorphisms:

1. The map $G \to G'$ given by sending all elements of G to the identity element of G'. It is called the *trivial homomorphism*.

2. The exponential map $(\mathbf{R}, +) \to (\mathbf{R}^\times, \cdot)$, $x \mapsto e^x$, since we have the identity $e^{x+y} = e^x \cdot e^y$ for all $x, y \in \mathbf{R}$.

3. The logarithm map $\log : (\mathbf{R}_+^\times, \cdot) \to (\mathbf{R}, +)$, since for all positive reals x, y, we have $\log(xy) = \log(x) + \log(y)$.

4. The absolute value map $(\mathbf{C}^\times, \cdot) \to (\mathbf{R}^\times, \cdot)$, $x \mapsto |x|$ since we have the identity $|xy| = |x||y|$ for any $x, y \in \mathbf{C}^\times$.

5. The determinant function $\det : (GL_n(\mathbf{R}), \cdot) \to (\mathbf{R}^\times, \cdot)$ since we have the identity $\det(AB) = \det(A)\det(B)$ for any $A, B \in GL_n(\mathbf{R})$.

6. The n-th power map $(\mathbf{C}^\times, \cdot) \to (\mathbf{C}^\times, \cdot)$ sending z to z^n, since for all $z, z' \in \mathbf{C}^\times$, $(zz')^n = z^n z'^n$.

7. For any integer n, the map $(\mathbf{Z}, +) \to (\mathbf{Z}, +)$ sending an integer x to nx, since for all $x, y \in \mathbf{Z}$, $n(x + y) = nx + ny$.

Another important example is the following:

Example 3.6.3. Let G be a group and H a subgroup of G. Then the *inclusion map* $i : H \to G$ sending $h \in H$ to itself is a group homomorphism: indeed, for all $h, h' \in H$, we have $i(hh') = hh' = i(h)i(h')$.

Proposition 3.6.4. *Let G, G' be groups with identity elements e, e', and let $\phi : G \to G'$ be a group homomorphism. We have:*

1. *$\phi(e) = e'$.*

2. *For all $x \in G$, $\phi(x^{-1}) = \phi(x)^{-1}$.*

Definition 3.6.5. The *image* of a homomorphism $\phi : G \to G'$ is the set

$$\operatorname{Im}(\phi) = \{y \in G', y = \phi(x) \text{ for some } x \in G\}.$$

Proposition 3.6.6. *Let $\phi : G \to G'$ be a group homomorphism. Then* $\operatorname{Im}(\phi)$ *is a subgroup of G'.*

Definition 3.6.7. The *kernel* of a homomorphism $\phi : G \to G'$ is the set

$$\operatorname{Ker}(\phi) = \{x \in G, \phi(x) = e'\},$$

where e' is the identity element of G'.

Proposition 3.6.8. *Let $\phi : G \to G'$ be a group homomorphism. Then* $\operatorname{Ker}(\phi)$ *is a subgroup of G.*

Remark 3.6.9. The previous two propositions give us a new method for proving that something is a subgroup, as we can see from some of the following examples.

Example 3.6.10. 1. The kernel of the trivial homomorphism $G \to G'$ is the group G itself. Its image is the trivial subgroup $\{e'\}$ of G'.

2. Let H be a subgroup of a group G. The inclusion homomorphism $H \to G$ has kernel the trivial subgroup $\{e\}$ and image the subgroup H.

3. The exponential map $(\mathbf{R}, +) \to (\mathbf{R}^\times, \cdot)$, $x \mapsto e^x$ has trivial kernel, and its image is the set $\mathbf{R}_{>0}$ of positive reals, which is indeed a subgroup of $(\mathbf{R}^\times, \cdot)$.

4. The kernel of the absolute value map $(\mathbf{C}^\times, \cdot) \to (\mathbf{R}^\times, \cdot)$, $x \mapsto |x|$ is the set

$$U = \{z \in \mathbf{C},\ |z| = 1\}$$

of complex numbers of absolute value one, that is, the unit circle. This shows that it is a subgroup of $(\mathbf{C}^\times, \cdot)$. The image of the absolute value homomorphism is $\mathbf{R}_{>0}$.

5. The determinant map $\det : (GL_n(\mathbf{R}), \cdot) \to (\mathbf{R}^\times, \cdot)$ is surjective, so its image is all of $\mathbf{R}^\times$. Its kernel is the subgroup $SL_n(\mathbf{R})$ of $GL_n(\mathbf{R})$ of matrices with determinant 1. It is called the *special linear group*.

Proposition 3.6.11. *Let $\phi : G \to G'$ be a group homomorphism. It is injective if and only if its kernel is the trivial subgroup of G.*

3.7 Isomorphisms

Judson, section 9.1

Definition 3.7.1. A group homomorphism $\phi : G \to G'$ is called an *isomorphism* if it is bijective.

Thus, ϕ is an isomorphism if and only if $\mathrm{Im}(\phi) = G'$ (this ensures surjectivity) and $\mathrm{Ker}(\phi)$ is trivial.

Proposition 3.7.2. *Let $\phi : G \to G'$ be an isomorphism. Then $\phi^{-1} : G' \to G$ is also an isomorphism.*

October 15th:

Definition 3.7.3. Two groups G and G' are said to be isomorphic if there exists an isomorphism $\phi : G \to G'$.

Example 3.7.4. 1. The exponential function defines an isomorphism $(\mathbf{R}, +) \to (\mathbf{R}_+^\times, \cdot)$, where $\mathbf{R}_+^\times$ is the set of positive real numbers. Its inverse is the logarithm function.

2. We have encountered at least two groups of order two, namely $(\mathbf{Z}/2\mathbf{Z}, +)$ and $(\{1, -1\}, \cdot)$. The map

$$\mathbf{Z}/2\mathbf{Z} \to \{1, -1\}$$

sending 0 to 1 and 1 to -1 gives an isomorphism between the two.

Isomorphic groups have exactly the same properties (same order etc.), so we can identify them to each other.

Proposition 3.7.5. *A cyclic group of infinite order is isomorphic to* $\mathbf{Z}$.

Proof. Let $G = \langle a \rangle$ be a cyclic group of infinite order. Define a map $\mathbf{Z} \to G$ by sending n to a^n. We check that it is a group homomorphism. Its kernel is $\{0\}$ because a is of infinite order, and its image is G by definition, so it is an isomorphism. $\square$

Proposition 3.7.6. *Let $n \geq 2$ be an integer. Any cyclic group of order n is isomorphic to $\mathbf{Z}/n\mathbf{Z}$.*

Proof. Let $G = \langle a \rangle$ be a cyclic group of order n, that is a is of order n. Define a map $\mathbf{Z}/n\mathbf{Z} \to G$ by sending $[m]$ to a^m. We check that it is well defined and a group homomorphism. Its kernel is $\{[0]\}$ because a is of order n and its image is $\{e, a, \ldots, a^{n-1}\} = G$. Thus, it is an isomorphism. $\square$

Proposition 3.7.7. *Let $\phi : G \to G'$ be a group homomorphism. If a is of finite order n, then $\phi(a)$ is of finite order dividing n. If moreover ϕ is an isomorphism, then $\phi(a)$ is of order exactly n.*

Proof. Let m be the order of $\phi(a)$. Write the Euclidean division of n by m: $n = qm + r$, with $0 \leq r < m$. We compute

$$\phi(a)^n = \phi(a^n) = e.$$

On the other hand,

$$\phi(a)^n = \phi(a)^{mq+r} = (\phi(a)^m)^q \phi(a)^r = \phi(a)^r.$$

So $\phi(a)^r = e$, but $r < m$, the order of $\phi(a)$. Thus, we must have $r = 0$, so m divides n.

Assume now that ϕ is an isomorphism. We have

$$\phi(a^m) = \phi(a)^m = e.$$

By injectivity, this implies $a^m = e$. Since a is of order n and $m \leq n$, we see that $m = n$. $\square$

Example 3.7.8. It is easy to check that $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ is cyclic of order 6, generated by $(1, 1)$. By Proposition 3.7.6, it is isomorphic to $\mathbf{Z}/6\mathbf{Z}$. Moreover, by proposition 3.7.7, in any isomorphism between these two groups, the element $(1, 1)$ will be sent to a generator of $\mathbf{Z}/6\mathbf{Z}$.

Example 3.7.9. Let us now give some examples of how to prove that two groups are not isomorphic.

1. The groups $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ are not isomorphic by proposition 3.7.7, the first one being cyclic of order 4, whereas the second one has only elements of order at most 2.

2. The groups $\mathbf{Q}$ and $\mathbf{Z}$ are not isomorphic. Indeed, assume we have an isomorphism $\phi : \mathbf{Z} \to \mathbf{Q}$ and denote $\phi(1) = a$. By surjectivity of ϕ, there exists an integer n such that $\phi(n) = \frac{a}{2}$. But since ϕ is a homomorphism, we must have $\phi(2n) = 2\phi(n) = a$, so that by injectivity of ϕ, $2n = 1$, which is a contradiction. Note that here the argument relied on the fact that in the group $\mathbf{Q}$ one can divide by 2 indefinitely, whereas this is not possible in $\mathbf{Z}$.

   Another way of seeing this is by remarking that for all $n \in \mathbf{Z}$, we have $\phi(n) = n\phi(1)$. This means that the denominator of the rational number $n\phi(1)$ is at most the denominator of $\phi(1)$. Since the denominators of elements of $\mathbf{Q}$ can be arbitrarily large, this means that ϕ cannot be surjective.

3. The additive group $(\mathbf{Q}, +)$ is not isomorphic to the multiplicative group $(\mathbf{Q}^\times, \cdot)$. Indeed, let $\phi : (\mathbf{Q}^\times, \cdot) \to (\mathbf{Q}, +)$ be an isomorphism. Put $\phi(2) = a$. By surjectivity of ϕ, there is a rational number x such that $\phi(x) = \frac{a}{2}$. Then $\phi(x \cdot x) = \phi(x) + \phi(x) = a$, so by injectivity, $x^2 = 2$. This is impossible since there is no rational number x satisfying this. This argument is similar to the one in the previous example: here we used that dividing by 2 in the additive setting corresponded to taking square roots in the multiplicative setting, which is not always possible in the rationals.

3.8 Classification of groups of small order

In this paragraph we want to classify the finite groups of orders 1,2,3,4, that is, give a list of all of them up to isomorphism.

Order 1 The only group of order 1 is the trivial group $\{e\}$.

Order 2 We already know one group of order 2, namely $\mathbf{Z}/2\mathbf{Z}$. In fact, we claim that any group of order 2 is cyclic, and therefore isomorphic to $\mathbf{Z}/2\mathbf{Z}$. Indeed, let G be such a group. Then G is of the form $\{e, a\}$ where $a \neq e$. By the cancellation law, we cannot have $a^2 = a$, so necessarily $a^2 = e$. This means that a is of order 2, so that $G = \langle a \rangle$ is cyclic of order 2, as claimed. In particular, the groups $\{1, -1\}$ and $\mathbf{Z}/2\mathbf{Z}$ are isomorphic.

Order 3 We already know the cyclic group of order 3, namely $\mathbf{Z}/3\mathbf{Z}$. Let us show that any group of order 3 is necessarily cyclic, and therefore isomorphic to $\mathbf{Z}/2\mathbf{Z}$. Indeed, let $G = \{e, a, b\}$ a three-element set on which we assume there is a group structure, e being the identity element. Let us find conditions on this group structure. First of all, by the cancellation law, we cannot have $ab = a$ nor $ab = b$, so necessarily $ab = e$. In the same manner, $ba = e$. Recalling that every element of the group occurs only once in every row and column of its Cayley table, we can complete the table in the following way:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

In particular, $b = a^2$ and therefore $G = \{e, a, a^2\}$ is cyclic of order 3.

Order 4 We already know two non-isomorphic groups of order 4, namely $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Our aim is to prove that these are the only possibilities. By proposition 3.7.6, a cyclic group of order 4 is isomorphic to $\mathbf{Z}/4\mathbf{Z}$, so let us start with a non-cyclic group $G = \{e, a, b, c\}$ of order 4. Since G is non-cyclic, all its elements are at most of order 3. Let us show that we cannot have an element of order 3. Without loss of generality, assume that a is of order 3, that is, $a^2 \neq e$ but $a^3 = e$. Since by the cancellation law we cannot have $a^2 = a$, we may assume, without loss of generality, that $a^2 = b$. In other words, the first two lines of the Cayley table of G look like this:

	e	a	b	c
e	e	a	b	c
a	a	b	e	

We see that the last cell of the second line, provides a contradiction: indeed, since all elements in the row and column of a Cayley table must be distinct, in cannot contain a, b, e or c.

Therefore, there are no elements of order 3. This means that a, b, c are all of order 2. Then using the cancellation law, the corresponding Cayley table will be

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Using this table, we see that we can construct an isomorphism $G \to \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, by sending $a \mapsto (1, 0)$, $b \mapsto (0, 1)$ and $c \mapsto (1, 1)$.

Remark 3.8.1. We have proved in particular that all groups of order at most 4 are abelian.

3.9 Conclusion of the chapter

Before going on to studying other aspects of the theory of groups, make sure you

- Can give the definition of a group.
- Can check that something is a subgroup of some larger group.

- Are familiar with the following examples of groups:
  - $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ and $(\mathbf{C}, +)$.
  - $(\mathbf{Z}/n\mathbf{Z}, +)$ for all $n \geq 2$.
  - $(\mathbf{Q}^\times, \cdot)$, $(\mathbf{R}^\times, \cdot)$ and $(\mathbf{C}^\times, \cdot)$.
  - $((\mathbf{Z}/n\mathbf{Z})^\times, \cdot)$ for all $n \geq 2$.
  - $(M_n(\mathbf{R}), +)$ and $(GL_n(\mathbf{R}), \cdot)$.
  - $(\mathcal{B}(X, X), \circ)$.
- Know how to use the cancellation law to fill out a Cayley table.
- Know how to manipulate products of groups.
- Can give the definition of the order of an element of a group.
- Understand why if $x^n = e$ for some x in a group and $n \geq 1$, then x is of finite order and n is divisible by the order of x.
- Know that $\mathbf{Z}$ and $\mathbf{Z}/n\mathbf{Z}$ are cyclic and know how to find generators.
- Can check that some map is a homomorphism.
- Know that a homomorphism preserves the identity element and inverses.
- Know the definitions of kernel and image, and can compute them in some special cases.
- Know that a homomorphism is injective if and only if its kernel is trivial.
- Can check that some map is an isomorphism, by checking it is a homomorphism and computing its kernel and image.
- Understand how homomorphisms and isomorphisms act on orders of elements.
- Can give the list of all groups of order at most 4 up to isomorphism, and know how to prove this list is exhaustive for orders 1,2,3.

Octobers 16th and 21st:

4 Permutation groups

Judson Chapter 5

4.1 Definition

Judson 5.1

Let X be a set. Recall (Example 3.2.4, 3d) that a permutation of X is a bijection $X \to X$ and that bijections from a set to itself form a group for the composition law $\circ$.

Definition 4.1.1. Let $n \geq 1$ be an integer. We define the n-th permutation group $\mathfrak{S}_n$ to be the group of bijections of the set $\{1, \dots, n\}$ to itself.

Notation 4.1.2. We will write a permutation $\sigma \in \mathfrak{S}_n$ in the form

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

The numbers on the bottom line are the integers $1, 2, \dots, n$ in a different order, except if $\sigma = 1$ is the identity permutation.

Example 4.1.3. The group $\mathfrak{S}_1$ is the trivial group. The group $\mathfrak{S}_2$ has two elements, the identity and $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. The group $\mathfrak{S}_3$ has the following six elements:

$$1, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Remark 4.1.4. Recall that the binary operation on $\mathfrak{S}_n$ is *composition* of permutations, seen as functions from $\{1, \dots, n\}$ to $\{1, \dots, n\}$. Thus, the product $\sigma\tau = \sigma \circ \tau$ of two permutations σ and τ is the permutation sending each $i \in \{1, \dots, n\}$ to $\sigma(\tau(i))$. In other words:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \dots & \sigma(\tau(n)) \end{pmatrix}$$

The product has to be taken from right to left, because this is how composition of functions works.

Example 4.1.5. In $\mathfrak{S}_3$, we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Note that, as composition of functions, composition of permutations is not usually commutative:

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

Recall that for an integer $n \geq 1$, its factorial $n!$ is defined to be the product of the integers from 1 to n. We also define, by convention, that $0! = 1$.

Proposition 4.1.6. *The group $\mathfrak{S}_n$ has $n!$ elements.*

Proof. To determine a permutation σ, it suffices to give the values of $\sigma(1), \ldots, \sigma(n)$. For $\sigma(1)$, we have n choices. Now $\sigma(2)$ must be different from $\sigma(1)$, so we have $n-1$ choices for its value. Continuing like this, we find that there are $n-2$ choices for $\sigma(3)$, $n-3$ choices for $\sigma(4)$, etc., $n-(n-2)=2$ choices for $\sigma(n-1)$, and only one possible choice for $\sigma(n)$. We obtain that the total number of permutations is

$$n \times (n-1) \times \ldots \times 2 \times 1 = n!.$$

□

4.2 Cycles

Judson 5.1

Definition 4.2.1. A permutation $\sigma \in \mathfrak{S}_n$ is a *cycle of length k* if there exist distinct elements $a_1, \ldots a_k \in \{1, \ldots, n\}$ such that

$$\begin{aligned}
\sigma(a_1) &= a_2 \\
\sigma(a_2) &= a_3 \\
&\vdots \\
\sigma(a_k) &= a_1
\end{aligned}$$

and such that $\sigma(x) = x$ for all other $x \in \{1, \ldots, n\}$.

Notation 4.2.2. We will write $(a_1, \ldots, a_k)$ to denote the cycle σ.

To have a formula for $\sigma(a_i)$ valid for all values of i (that is, even $i = k$), we may write $\sigma(a_i) = a_{i \pmod k)+1}$. This means that we may have to take the remainder of i in the Euclidean division by k when computing $\sigma(a_i)$.

Example 4.2.3. The element of the group $\mathfrak{S}_2$ which is not the identity is the cycle $(1, 2)$. The above elements of the group $\mathfrak{S}_3$ can all be seen as the following respective cycles:

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

However, there are permutations which are not cycles. For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

is a product of two cycles, but is not a cycle itself. Here is another, larger example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 2 & 6 & 3 & 4 \end{pmatrix} = (1532)(46).$$

Remark 4.2.4. To multiply two cycles σ and τ, take the smallest integer occurring in at least one the two cycles, e.g. 1. Look at $\tau(1)$, then at $\sigma(\tau(1))$. If it is 1, proceed to the next integer occurring in one of the two cycles. If not, write down

$$(1, \sigma(\tau(1))$$

and continue with the integer $a = \sigma(\tau(1))$, looking first at $\tau(a)$ then at $\sigma(\tau(a))$. If you get $\sigma(\tau(a)) = 1$, then close the cycle $(1, a)$ and proceed to the smallest integer occurring in one of the two cycles and which is neither 1 nor a. If not, add $\sigma(\tau(a))$ to the cycle you've started to write down:

$$(1, a, \sigma(\tau(a))$$

and continue the process with $b = \sigma(\tau(a))$. Once your cycle is closed, do the same starting with the smallest integer not in this cycle but occurring in σ or τ. This builds another cycle, which you write down next to the previous one. Then proceed to the next integer which is not in the two cycles you've written down but is in σ or in τ, etc. The process ends when all integers which occur either in σ or in τ have been processed.

Example 4.2.5. We have

$$(1, 5, 3, 2)(2, 3, 4) = (1, 5, 3, 4)$$

and

$$(1, 3)(3, 5, 1, 6, 7) = (1, 6, 7)(3, 5).$$

Proposition 4.2.6. *A cycle of length k is an element of order k of the group $\mathfrak{S}_n$.*

Proof. Let $\sigma = (a_1, \dots, a_k)$ be a cycle of length k. We have

$$\sigma(a_1) = a_2 \quad \sigma^2(a_1) = a_3 \quad \dots \quad \sigma^{k-1}(a_1) = a_k,$$

that is, for all $i \in \{0, \dots, k-1\}$, $\sigma^i(a_1) = a_{i+1}$. In particular, since $\mathrm{id}(a_1) = a_1$, this implies that $\sigma^i \neq \mathrm{id}$ for all $i \in \{1, \dots, k-1\}$.

Now it suffices to show that $\sigma^k = \mathrm{id}$. First of all, note that for all $x \notin \{a_1, \dots, a_k\}$, we have $\sigma^k(x) = x$. Now we are going to compute $\sigma^k(a_i)$ for all i.

For $i < k$, we have

$$\sigma^k(a_i) = \sigma^{k-1}(a_{i+1}) = \dots = \sigma^{k-(k-i)}(a_k) = \sigma^i(a_k) = \sigma^{i-1}(a_1) = a_i.$$

Finally,

$$\sigma^k(a_k) = \sigma^{k-1}(a_1) = a_k.$$

Thus, $\sigma^k = \mathrm{id}$. ◻

Definition 4.2.7. Two cycles $\sigma = (a_1, \dots, a_k)$ and $\tau = (b_1, \dots, b_\ell)$ are said to be *disjoint* if

$$\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_\ell\} = \varnothing.$$

Proposition 4.2.8. *Let σ and τ be disjoint cycles. Then they commute, that is, $\sigma\tau = \tau\sigma$.*

Proof. Judson Prop 5.8 $\square$

Theorem 4.2.9. *Every permutation in $\mathfrak{S}_n$ can be written as a product of disjoint cycles.*

Proof. Judson Theorem 5.9 $\square$

Example 4.2.10. See example 4.2.3 above, and Judson, Example 5.10.

Remark 4.2.11. The proof of this statement provides an algorithm for computing these cycles. Since we just proved that they commute, it does not matter in which order we write them.

Definition 4.2.12. A *transposition* is a cycle of length 2.

Lemma 4.2.13. *We have the identities*

$$(a_1, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_3)(a_1, a_2)$$

and

$$(a_1, \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$$

Proposition 4.2.14. *Every permutation in $\mathfrak{S}_n$ is a product of transpositions.*

Proof. Every permutation is a product of cycles, and every cycle is a product of transpositions by the previous lemma. $\square$

Remark 4.2.15. There are many ways of writing a permutation as a product of transpositions (see Judson, Example 5.13). However, as we will see in the next paragraph, for any given permutation, the parity of the number of transpositions used will always be the same.

October 28th:

4.3 Parity of a permutation

Proposition 4.3.1. *If the identity is written as a product of r transpositions, then r is an even number.*

Proof. Judson, Lemma 5.14, or Theorem 2.1 in `https://kconrad.math.uconn.edu/blurbs/grouptheory/sign.pdf`. $\square$

Theorem 4.3.2. *Write a permutation σ as a product of transpositions in two ways:*

$$\sigma = \tau_1 \dots \tau_r = \tau'_1 \dots \tau'_{r'}.$$

Then $r \equiv r' \pmod 2$.

Proof. Judson, Theorem 5.15 □

The theorem shows that in particular, the number $\mathrm{sgn}(\sigma) := (-1)^r$ is well defined. It is called the *sign* of σ.

Definition 4.3.3. A permutation σ is called *even* if $\mathrm{sgn}(\sigma) = 1$, and *odd* if $\mathrm{sgn}(\sigma) = -1$.

Example 4.3.4.
1. By proposition 4.3.1, $\mathrm{sgn}(\mathrm{id}) = 1$, that is, the identity is even.
2. A transposition is always odd.
3. More generally, by lemma 4.2.13, a cycle of length k has sign $(-1)^{k-1}$. In particular, cycles of length 3 are always even.

Proposition 4.3.5. *The map* $\mathrm{sgn} : \mathfrak{S}_n \to \{1, -1\}$ *defined by* $\sigma \mapsto \mathrm{sgn}(\sigma)$ *is a group homomorphism.*

Proof. Let σ, σ' be two permutations. We write them both as products of transpositions:

$$\sigma = \tau_1 \dots \tau_r, \quad \sigma' = \tau_1' \dots \tau_{r'}'.$$

Then $\mathrm{sgn}(\sigma) = (-1)^r$ and $\mathrm{sgn}(\sigma') = (-1)^{r'}$. Moreover,

$$\sigma\sigma' = \tau_1 \dots \tau_r \tau_1' \dots \tau_{r'}'$$

is a product of $r + r'$ transpositions, so

$$\mathrm{sgn}(\sigma\sigma') = (-1)^{r+r'} = (-1)^r(-1)^{r'} = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma').$$

□

Recall that the kernel of any homomorphism is a group by proposition 3.6.8.

Definition 4.3.6. The *alternating group* $\mathfrak{A}_n$ is the group of all even permutations, that is, the kernel of the sign homomorphism.

Example 4.3.7. We have $\mathfrak{A}_2 = \{\mathrm{id}\}$, $\mathfrak{A}_3 = \{\mathrm{id}, (1,2,3), (1,3,2)\}$, and

$$\begin{aligned}\mathfrak{A}_4 \;=\; &\{\mathrm{id},\ (1,2)(3,4),\ (1,4)(2,3),\ (1,3)(2,4),\ (1,2,3),\ (1,3,2),\\ &(1,2,4),\ (1,4,2),\ (1,3,4),\ (1,4,3),\ (2,3,4),\ (2,4,3)\}\end{aligned}$$

October 30th:

Proposition 4.3.8. *Let $n \geq 2$. The number of even permutations in $\mathfrak{S}_n$ is equal to the number of odd permutations, that is, the order of $\mathfrak{A}_n$ is $\frac{n!}{2}$.*

Proof. Judson, Proposition 5.17. □

4.4 Generators of $\mathfrak{S}_n$ and $\mathfrak{A}_n$

By proposition 4.2.14, and identity

$$(ij) = (1i)(1j)(1i),$$

every permutation $\sigma \in \mathfrak{S}_n$ can be written as a finite product of the following transpositions:

$$(1, 2),\ (1, 3), \ldots,\ (1, n).$$

In other words, these transpositions generate $\mathfrak{S}_n$. The aim of this paragraph is to give other sets of generators of $\mathfrak{S}_n$.

Remark 4.4.1. Recall that saying that a group is generated by elements $g_1, \ldots, g_n$ means that every element of the group can be written as a finite product of these elements and their inverses. However, since a transposition is equal to its inverse, in the above case every element can be written simply as a product of the elements in the given set.

The following lemma is very useful:

Lemma 4.4.2. *For every permutation $\sigma \in \mathfrak{S}_n$ and for every cycle $(a_1, \ldots, a_k)$, we have that*

$$\sigma(a_1, \ldots, a_k)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)).$$

In particular, $\sigma(a_1, \ldots, a_k)\sigma^{-1}$ is a cycle of length k.

Lemma 4.4.3. *Every transposition in $\mathfrak{S}_n$ can be written as a product of transpositions of the form $(a, a + 1)$, $a \in \{1, \ldots, n - 1\}$.*

Proof. For a transposition (i, j) with $i < j$, induction on $j - i$ using the identity $(a, b) = (a, a + 1)(a + 1, b)(a, a + 1)$. □

We deduce from this:

Proposition 4.4.4. *Every element of $\mathfrak{S}_n$ can be written as a finite product of the following transpositions:*

$$(1, 2),\ (2, 3),\ \ldots,\ (n - 1, n).$$

Proposition 4.4.5. *For $n \geq 3$, the group $\mathfrak{S}_n$ is generated by the permutations $(1, 2)$ and $(1, 2, \ldots, n)$.*

Proof. We have, by Lemma 4.4.2 that for every $i \in \{2, \ldots, n - 1\}$,

$$(i, i + 1) = (1, \ldots, n)^i(1, 2)(1, \ldots, n)^{-i}.$$

We then use Proposition 4.4.4 to conclude. □

Proposition 4.4.6. *For $n \geq 3$, the alternating group $\mathfrak{A}_n$ is generated by cycles of length 3.*

This comes from the fact that the product of two transpositions can always be written as a product of cycles of length 3. Indeed, we have

$$(ab)(ac) = (acb)$$

and

$$(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd).$$

4.5 Dihedral groups

Judson section 5.2

A *symmetry* of a regular n-gon (that is, a regular polygon with n vertices) is a transformation of the plane which sends the n-gon to itself, but can rearrange the vertices.

Definition 4.5.1. For $n \geq 3$, we define the n-th *dihedral group* to be the group of symmetries of a regular n-gon.

November 6th:

If you number the vertices of the n-gon from 1 to n, then every such symmetry induces a permutation of the vertices, and therefore defines an element of $\mathfrak{S}_n$. Thus, D_n may naturally be seen as a subgroup of $\mathfrak{S}_n$ (i.e., it is isomorphic to a subgroup of $\mathfrak{S}_n$).

As an example, Figure 3.6 in Judson describes all the symmetries of the triangle, and the permutations in $\mathfrak{S}_3$ that they define. One can see that these symmetries are essentially of two kinds: *rotations* and *reflections* (with respect to an axis of symmetry of the triangle). In this case, you can actually obtain all of the permutations in $\mathfrak{S}_3$ in this way, i.e. $D_3 = \mathfrak{S}_3$. For $n \geq 4$, D_n is a proper subgroup of $\mathfrak{S}_n$.

Proposition 4.5.2. *D_n is a subgroup of $\mathfrak{S}_n$ of order $2n$.*

Remark 4.5.3. In particular, as n grows, $2n$ will be very small with respect to $n!$, so the proportion of permutations in $\mathfrak{S}_n$ corresponding to actual symmetries of the regular n-gon will be very small.

Example 4.5.4. Example 5.24 in Judson describes the symmetries of the square (that is, the regular 4-gon). We see that as a subgroup of $\mathfrak{S}_4$, D_4 is given by

$$\{\mathrm{id}, (1,2,3,4), (1,4,3,2), (13)(24), (12)(34), (14)(23), (24), (13)\}.$$

In particular, the transposition (12) for example does not correspond to a symmetry of the square. It is not possible to send the vertex to the vertex 2 without moving some of the other vertices.

As for any group, it is interesting to understand what a minimal set of generators for D_n is. The group D_n is not cyclic (in fact, it is not commutative: a rotation and a reflection usually do not commute). However, it can be generated by two elements, namely a rotation and a reflection:

Theorem 4.5.5. *The group D_n is generated by two elements r and s satisfying the relations*

$$r^n = \mathrm{id}, \quad s^2 = \mathrm{id}, \quad srs = r^{-1}.$$

More precisely, r is of order n, s is of order 2 and rs is of order 2.

Proof. Judson Theorem 5.23 □

It follows from this that D_n can be explicitly described by

$$D_n = \{1, r, \dots r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

Note that the element r constructed in the proof corresponds to the n-cycle $(1, 2, \dots, n)$. As for the element s, if $n = 2k$ is even, it corresponds to the product of disjoint transpositions

$$(2, 2k)(3, 2k-1) \dots (k, k+2)$$

and if $n = 2k+1$ is odd, it corresponds to the product of disjoint transpositions

$$(2, 2k+1)(3, 2k) \dots (k+1, k+2).$$

Example 4.5.6. In particular, for D_3, the generators are $(1, 2, 3)$ and $(2, 3)$, which are also generators of S_3. For D_4, generators are given by $(1, 2, 3, 4)$ and (24).

4.6 Conclusion of the chapter

We are going to use symmetric and alternating groups frequently as examples in the subsequent chapters on groups. Therefore, you should be comfortable with their properties and with manipulating permutations. In particular, make sure you know

- how to multiply permutations.
- how to decompose them into products of disjoint cycles.
- how to decompose them into products of transpositions. You should also have an intuitive understanding of why a permutation is a product of transpositions: if you have n cards numbered from 1 to n placed in fromt of you in some order, you can order them correctly by swapping them two at a time.
- that the order of a cycle is its length.
- how to compute the sign of a permutation.
- how many elements there are in $\mathfrak{S}_n$, $\mathfrak{A}_n$ and D_n.
- the formula $\sigma(a_1, \dots, a_k)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))$ and can use it in concrete cases.
- how to generate D_n by a rotation and a reflection, and what relation they satisfy.

The main interest of the paragraph about generators of $\mathfrak{S}_n$ and $\mathfrak{A}_n$ is in the way the results it contains are proved. Make sure you've read through the proofs several times, so that you understand them well. In particular, though you do not need to know the formulas we have used by heart, it is good to be able to recover them, as it strengthens your intuition on how transpositions behave when they are multiplied or conjugated by other permutations.

5 Cosets and Lagrange's theorem

5.1 Left and right cosets

Judson section 6.1

Definition 5.1.1. Let G be a group and H a subgroup of G. A *left coset* of H is a subset of G of the form

$$gH = \{gh,\ h \in H\}.$$

In the same way, we can define right cosets to be $Hg = \{hg,\ h \in H\}$ for $g \in G$.

Remark 5.1.2. The group H itself is both a left coset and a right coset itself, for $g = e$ the identity element of G: $H = eH = He$. More generally, for all $g \in H$, we have $H = gH = Hg$. Indeed: by closure, we clearly have $gH \subset H$. On the other hand, if $h \in H$, we may write $h = g(g^{-1}h) \in gH$ since $g^{-1}h \in H$. The same works for right cosets.

Remark 5.1.3. Left and right cosets of H are the same if the group G is abelian, but in general they may be different. For an abelian group, we will often use additive notation and write both types of cosets in the form $g + H$.

Example 5.1.4. The cosets of $H = \{0, 3\}$ in $\mathbf{Z}/6\mathbf{Z}$ are

$$0 + H = 3 + H = \{0, 3\}$$

$$1 + H = 4 + H = \{1, 4\}$$

$$2 + H = 5 + H = \{2, 5\}.$$

Example 5.1.5. Let H be the subgroup of $\mathfrak{S}_3$ given by $\{\mathrm{id}, (12)\}$. Left cosets of H are:

$$\mathrm{id}H = (12)H = \{\mathrm{id},\ (12)\}$$

$$(13)H = (123)H = \{(13), (123)\}.$$

$$(23)H = (132)H = \{(23), (132)\}.$$

Computing the right cosets of H, we see that they are different from its left cosets.

November 8th:

Example 5.1.6. Let G be a group. The cosets of the trivial subgroup $\{e\}$ are all of the sets of the form $\{g\}$ for $f \in G$. The group G itself viewed as a subgroup of G has only one coset, namely G.

Remark 5.1.7. What is the condition for the left and right coset of H to be equal? In fact, we do not need that G be commutative. For $gH = Hg$, we only need that $ghg^{-1} \in H$ for all $h \in H$. When this is satisfied for all $g \in G$, we say that the subgroup H is *normal.* We are going to study this notion in the next chapter.

Remark that in all the examples that we considered, the distinct left cosets of H formed a partition of G. This is in fact a general feature of cosets, and can be explained by the fact that they are the equivalence classes of a relation: Consider the relation

$$a \sim b \quad \text{if there exists } h \in H \text{ such that } a = bh.$$

Equivalently, $a \sim b$ if and only if $b^{-1}a \in H$ and if and only if $a \in bH$. It is an equivalence relation, and the left cosets of H are its equivalence classes. Thus, we have the following:

Proposition 5.1.8. *Let H be a subgroup of a group G. Then G is the disjoint union of the left cosets of H. In other words, the left cosets of H form a partition of G.*

Remark 5.1.9. This property is also true for right cosets. This can be seen by introducing another equivalence relation $\sim'$ given by $a \sim' b$ if and only if there exists $h \in H$ such that $a = hb$ (or, equivalently, $ab^{-1} \in H$, or $a \in Hb$). Its equivalence classes are the right cosets. Note moreover that $a \sim b$ if and only if $a^{-1} \sim' b^{-1}$, so that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$.

There is a map

$$\alpha : \{\text{left cosets of } H\} \to \{\text{right cosets of } H\}$$

given by $aH \mapsto Ha^{-1}$, well-defined and injective thanks to the previous remark. It is also surjective since for all $b \in G$, $\alpha(b^{-1}H) = Hb$. We may conclude the following:

Proposition 5.1.10. *Let G be a group and H a subgroup of G. Then the number of left cosets of H is equal to the number of right cosets.*

5.2 Index of a subgroup

Definition 5.2.1. Let H be a subgroup of a group G. The index of H in G, denoted by $[G : H]$, is defined to be the number of distinct left cosets of H in G.

Remark 5.2.2. By proposition 5.1.10, this is the same as the number of distinct right cosets.

Example 5.2.3. The index of $\{0, 3\}$ in $\mathbf{Z}/6\mathbf{Z}$ is 3. So is the index of $\{\mathrm{id}, (12)\}$ in $\mathfrak{S}_3$.

Example 5.2.4. Consider $G = \mathbf{Z}$ and $H = n\mathbf{Z}$. Observe that in this case, the equivalence relation $\sim$ is exactly the relation of congruence modulo n, the cosets being exactly

$$n\mathbf{Z},\ 1 + n\mathbf{Z}, \dots,\ (n-1) + n\mathbf{Z}.$$

Thus, $[\mathbf{Z}, n\mathbf{Z}] = n$.

Note that in general, $[G : H]$ may be infinite. For example, a left coset of the trivial group in a group G is of the form $\{a\}$ for $a \in G$. Thus, if G is infinite, $[G : \{e\}]$ is infinite.

Remark 5.2.5. Let H be a subgroup of H. We have $[G : H] = 1$ if and only if $H = G$.

Example 5.2.6 (Subgroups of index 2)**.** An important special case is that of subgroups of index 2. Let G be a group and H a subgroup of G such that $[G : H] = 2$. This means that we have two left cosets, one of them being H itself, and the other being $G \setminus H$, which should be the equivalence class of all $g \in G \setminus H$, so that G is the disjoint union $G = H \sqcup gH$ for any $g \in G \setminus H$. In exactly the same manner, we have two right cosets, one of them being H, and the other being given by Hg where g is any element of $G \setminus H$. Therefore, for all $g \in G \setminus H$, we have

$$gH = G \setminus H = Hg.$$

On the other hand, for all $g \in H$, we have

$$gH = H = Hg.$$

Therefore, we observe that in this case, the right cosets and the left cosets of H are the same.

Moreover, we can describe quite well how multiplication acts on G. Let $a, b \in G$. If they are both elements of H, then by closure, $ab \in H$. If only one of them (say, a) is an element of H, then $ab \in G \setminus H$. Indeed, if we had $ab \in H$, we would have $b \in H$, which is a contradiction.

Finally, if both a, b are elements of $G \setminus H$, then we can show that $ab \in H$. Indeed, since H is stable under taking inverses, we must have $a^{-1} \notin H$. Then $a^{-1}H$ is the coset $G \setminus H$, and so $b \in a^{-1}H$. Therefore, $ab \in H$.

Let us summarize some properties of subgroups of index 2 in the following proposition:

Proposition 5.2.7 (Subgroups of index 2)**.** *Let G be a group and H a subgroup of G such that $[G : H] = 2$. Then*

1. *H has two cosets, given by H and $G \setminus H$.*
2. *For every $g \in G$, we have $gH = H = Hg$ if $g \in H$ and $gH = G \setminus H = Hg$ if $g \notin H$.*
3. *If $a, b \in G$ are not in H, then $ab \in H$*

Remark 5.2.8. Note that by 2., we have that for all $a \in G$, we have $aH = Ha$. Equivalently, we have that for all $a \in G$ and for all $h \in H$, $aha^{-1} \in H$. Subgroups satisfying these conditions (left cosets equal to right cosets, or stability with respect to conjugation by an element of G) are called normal subgroups, and are going to be important in the next chapter. What we have seen shows that subgroups of index 2 are always normal.

Example 5.2.9. For $n \geq 2$, the subgroup $\mathfrak{A}_n$ in $\mathfrak{S}_n$ is of index 2. Its only cosets are $\mathfrak{A}_n$ itself and its complement, the set of odd permutations. The latter is equal to $\sigma\mathfrak{A}_n$ for any odd permutation σ. The product of two odd permutations is an even permutation, which illustrates property 3 in the above proposition.

Example 5.2.10. We have seen that the dihedral group D_n has a cyclic subgroup H of index 2, given by all rotations, and that $D_n = H \sqcup sH$ where s is a reflection. The elements of sH are reflections. By property 3 above, we may also conclude that the product of two reflections is always a rotation.

November 11th:

5.3 Lagrange's theorem

Judson section 6.2

In this section, we place ourselves in the case where G is finite. Then in particular H and $[G : H]$ are finite.

Proposition 5.3.1. *For every $a \in G$, H and aH have the same number of elements.*

Remark 5.3.2. The proof of this proposition establishes a bijection between H and aH via $h \mapsto ah$. This bijection still exists even if G and H are infinite.

Observing that the group G therefore is partitioned into $[G : H]$ subsets which all have $|H|$ elements, we have the following important *counting formula*:

Theorem 5.3.3 (Counting formula)**.** *Let G be a finite group and H a subgroup of G. Then*

$$|G| = [G : H]|H|.$$

An important consequence of this is Lagrange's theorem:

Theorem 5.3.4 (Lagrange)**.** *Let G be a finite group and H a subgroup of G. Then the order of H divides the order of G.*

Corollary 5.3.5. *Let G be a finite group. The order of any element of G divides the order of G.*

Corollary 5.3.6. *Let G be a finite group with order a prime number p. Then G is cyclic, and any $a \in G$ different from the identity element is a generator.*

Remark 5.3.7. Corollary 5.3.6 implies that up to isomorphism, there is only one group of order a prime p, namely $\mathbf{Z}/p\mathbf{Z}$. Note that we already knew from proposition 3.5.8 that all elements of $\mathbf{Z}/p\mathbf{Z}$ except 0 are generators.

Lagrange's theorem is a powerful tool for imposing restrictions on the possible orders of the elements of a group G, and on the possible orders of a subgroup of G.

Example 5.3.8.

1. By Lagrange's theorem, a subgroup of $\mathbf{Z}/n\mathbf{Z}$ must be of order dividing n. Conversely, for every $d|n$, we have a subgroup of order d (and index $\frac{n}{d}$) of $\mathbf{Z}/n\mathbf{Z}$ defined by

$$H = \left\langle \frac{n}{d} \right\rangle = \left\{ \frac{kn}{d},\ k \in \mathbf{Z} \right\} = \left\{ 0,\ \frac{n}{d},\ \frac{2n}{d}, \ldots,\ \frac{(d-1)n}{d} \right\}.$$

   This is the subgroup of $\mathbf{Z}/n\mathbf{Z}$ generated by $\frac{n}{d}$ (which, one can check, is an element of order d). Its cosets are given by

$$H,\ 1 + H,\ 2 + H, \ldots,\ \frac{n}{d} - 1 + H.$$

In fact, it is the only subgroup of order d in $\mathbf{Z}/n\mathbf{Z}$. To prove this, note that it contains all elements of $\mathbf{Z}/n\mathbf{Z}$ of order dividing d. Indeed, if m is of order dividing d, then $dm \equiv 0 \pmod{n}$, so there exists an integer k such that $dm = kn$, so that $m = \frac{kn}{d}$. Thus, m is an element of the group H. Therefore, assume we have a subgroup K of order d in $\mathbf{Z}/n\mathbf{Z}$. Then all of its elements are of order dividing d, so are contained in H, which means that $K \subset H$. Since they are the same order, they are equal.

Note that the subgroup $\left\langle \frac{n}{d} \right\rangle$ of $\mathbf{Z}/n\mathbf{Z}$ is cyclic of order d, and therefore isomorphic to $\mathbf{Z}/d\mathbf{Z}$. An explicit isomorphism is given by sending $\frac{kn}{d}$ to k.

For example, the subgroup of order 2 and index 3 of $\mathbf{Z}/6\mathbf{Z}$ is given by $\{0, 3\}$. The subgroup of order 3 and index 2 is given by $\{0, 2, 4\}$.

Note that in general, not all non-zero elements of $\left\langle \frac{n}{d} \right\rangle$ are of exact order d. For example, in $\mathbf{Z}/12\mathbf{Z}$, take the subgroup generated by 3: $\langle 3 \rangle = \{0, 3, 6, 9\}$. Then 3 and 9 are of order $\frac{12}{3} = 4$, but 6 is of order 2 (which nevertheless does divide 4).

2. The proper subgroups of $\mathfrak{S}_3$ are all of order 2 and 3. The ones of order 2 are the cyclic groups generated by a transposition, and there is exactly one subgroup of order 3, generated by any of the two cycles of length 3.

November 13th:

Proposition 5.3.9. *Every subgroup of a cyclic group is cyclic.*

Proof. We already know this for infinite cyclic groups, since an infinite cyclic group is isomorphic to $\mathbf{Z}$, and the subgroups of $\mathbf{Z}$ are the trivial group and the subgroups of the form $n\mathbf{Z}$, which are all cyclic.

Now, a finite cyclic group is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ for some n, and we have just seen that all subgroups of $\mathbf{Z}/n\mathbf{Z}$ are cyclic. □

Our study of subgroups of $\mathbf{Z}/n\mathbf{Z}$ can also be applied to deduce a property of the Euler function. Recall the definition of the Euler function

$$\phi(n) = |\{k \in \{1, \ldots, n\},\ k \text{ relatively prime to } n\}|$$

for $n \geq 1$.

Proposition 5.3.10. *Let $n \geq 1$ be an integer.*

1. *Let d be an integer dividing n. The number of elements of $\mathbf{Z}/n\mathbf{Z}$ of order exactly d is $\phi(d)$.*

2. *We have*

$$\sum_{d \mid n} \phi(d) = n.$$

Proof. 1. By the above, we know that all of the elements of order d are contained in $\left\langle \frac{n}{d} \right\rangle$, and that the latter is a cyclic group of order d. Thus, the number of elements of order d is equal to the number of elements of order d in $\mathbf{Z}/d\mathbf{Z}$, which by theorem 3.5.8 is $\phi(d)$.

2. By what we have seen so far, every element of $\mathbf{Z}/n\mathbf{Z}$ has order dividing n, so that we have a disjoint union:

$$\mathbf{Z}/n\mathbf{Z} = \bigsqcup_{d|n} \{\text{elements of order } d\}.$$

Moreover, there are exactly $\phi(d)$ elements in $\mathbf{Z}/n\mathbf{Z}$ of exact order d, so that comparing the sizes of the sets on both sides, we get the result.

□

Example 5.3.11. For $n = 6$, we have $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$ and $\phi(6) = 2$, so the total is indeed 6. This corresponds to the fact that $\mathbf{Z}/6\mathbf{Z}$ has 1 element of order 1, 1 element of order 2, 2 elements of order 3 and 2 elements of order 6.

Remark 5.3.12. Lagrange's theorem gives a quick way of settling classification of groups of small order.

- Let G be of order 3. Then by corollary 5.3.6, we have that G is cyclic, so isomorphic to $\mathbf{Z}/3\mathbf{Z}$.
- Let G be of order 4. Then, either it is cyclic, or it has no element of order 4. In the latter case, since by corollary 5.3.5 it can't have elements of order 3, all its elements other than the identity are of order 2, which gives $G \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
- Let G be of order 5. Then by corollary 5.3.6, we have that G is cyclic, so isomorphic to $\mathbf{Z}/5\mathbf{Z}$.

Remark 5.3.13. The converse of Lagrange's theorem is not true in general. It d divides the order of G, this does not guarantee the existence of a subgroup of order d in G.

For example, one can prove that $\mathfrak{A}_4$, which is of order 12, has no subgroups of order 6. (see Judson Proposition 6.15)

5.4 Some arithmetic applications of Lagrange's theorem

Judson, section 6.3.

Recall the definition of the Euler function

$$\phi(n) = |\{k \in \{1, \ldots, n\},\ k \text{ relatively prime to } n\}|$$

for $n \geq 1$. By theorem 2.7.11, $\phi(n)$ is exactly the order of the group of units $(\mathbf{Z}/n\mathbf{Z})^\times$. In particular, we have the following theorem:

Theorem 5.4.1 (Euler). *Let $n \geq 2$ be an integer, and let a be an integer coprime to n. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Example 5.4.2. Assume we want to compute the remainder of 1775^{200} in the Euclidean division by 12. First of all, $12 = 3 \times 4$, and 1775 is seen to be comprime to both 3 and 4 (use the divisibility criteria), so that Euler's theorem can be applied to $a = 1775$. We have $\phi(12) = |\{1, 5, 7, 11\}| = 4$ and so by Euler's theorem

$$1775^{200} = 1775^{4\times 50} = (1775^4)^{50} \equiv 1 \pmod{12}.$$

Since for $n = p$ a prime number, we have $\phi(p) = p - 1$, we may deduce from this:

Corollary 5.4.3 (Fermat's little theorem). *Let p be a prime number and a an integer not divisible by p. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for any integer b, we have $b^p \equiv b \pmod{p}$.

Example 5.4.4. Assume we want to know the remainder of the Euclidean division of 2347^{1000} by 5. First of all, we see that 2347 is not divisible by 5 since is last digit is not a 0 nor a 5. Therefore, using Fermat's little theorem:

$$2347^{1000} = (2347^4)^{250} \equiv 1^{250} \equiv 1 \pmod{5}.$$

The remainder we are looking for is 1.

November 18th:

5.5 Cosets and homomorphisms

Let $f : G \to G'$ be a homomorphism between two groups. Let us try to understand the cosets of the subgroup $\mathrm{Ker} f$ of G. The equivalence relation $\sim$ in this case is defined by

$$a \sim b \quad \text{if and only if} \quad b^{-1}a \in \mathrm{Ker} f$$

which, by definition of the kernel happens if and only if $f(b^{-1}a) = e'$ (the identity element of G'). Using the fact that f is a homomorphism, this is true if and only if $f(b)^{-1}f(a) = e'$, which, multiplying by $f(b)$ on both sides is true if and only if $f(a) = f(b)$. Thus, the equivalence relation $\sim$ is given by

$$a \sim b \quad \text{if and only if} \quad f(a) = f(b).$$

In other words, two elements of G lie in the same left coset if and only if they are mapped to the same thing by f.

Definition 5.5.1. Let $f : G \to G'$ be a group homomorphism. The fiber of f above $y \in G'$ is the set

$$f^{-1}(y) = \{x \in G,\ f(x) = y\}.$$

By the above, the left cosets of $\operatorname{Ker} f$ are exactly the fibers of f. The coset $a\operatorname{Ker} f$ corresponds to the fibre above $f(a)$.

Remark 5.5.2. By the same argument, we see that the relation $\sim'$ is exactly the same, so left cosets and right cosets coincide in this case.

Proposition 5.5.3. *Let $f : G \to G'$ be a homomorphism between two finite groups. Then*

1. $[G : \operatorname{Ker} f] = |\operatorname{Im} f|$.
2. $|G| = |\operatorname{Ker} f| \cdot |\operatorname{Im} f|$.

Proof. We establish a bijection between the set of cosets of $\operatorname{Ker} f$ and the image of f by mapping a coset $a\operatorname{Ker} f$ to $f(a)$.

- It is well defined because if $b \in G$ defines the same coset, then by the above $f(a) = f(b)$.
- It is surjective because if $y \in \operatorname{Im} f$, then there exists $x \in G$ such that $y = f(x)$, so that y is the image of the coset $x\operatorname{Ker} f$.
- It is injective because if $a, b \in G$ are such that $f(a) = f(b)$, then the cosets $a\operatorname{Ker} f$ and $b\operatorname{Ker} f$ are equal by the above discussion.

□

Example 5.5.4. 1. Let $f : \mathbf{Z}/6\mathbf{Z} \to \mathbf{Z}/6\mathbf{Z}$ be the homomorphism $x \mapsto 2x$. Then

$$\operatorname{Ker} f = \{x \in \mathbf{Z}/6\mathbf{Z},\ 2x = [0]\} = \{0, 3\},$$

and

$$\operatorname{Im} f = \{y \in \mathbf{Z}/6\mathbf{Z},\ y = 2x \text{ for some } x \in \mathbf{Z}/6\mathbf{Z}\} = \{0, 2, 4\}.$$

We computed the cosets of $H = \{0, 3\}$ in example 5.1.4. The coset $0 + H = 3 + H$ corresponds to elements mapping to 0, the coset $1 + H = 4 + H$ corresponds to elements mapping to 2, and the coset $2 + H = 5 + H$ corresponds to elements mapping to 4.

2. Let f be the sign homomorphism $\operatorname{sgn} : \mathfrak{S}_n \to \{1, -1\}$. Then $\operatorname{Ker} f = \mathfrak{A}_n$ and $\operatorname{Im} f = \{1, -1\}$. The kernel of sgn has two cosets, $\mathfrak{A}_n$ (the even permutations) and $\mathfrak{S}_n \setminus \mathfrak{A}_n$ (the odd permutations), corresponding respectively to the elements 1 and -1 of $\operatorname{Im} f$.

5.6 Conclusion of the chapter

In the next chapter, we are going to work with normal subgroups, and we will define a group structure on the set of cosets of a normal subgroup. Therefore, the contents of this chapter on cosets are quite fundamental to understand the next chapter.

Make sure you

- can define what a left or a right coset is.
- know that the left cosets of a subgroup H of a group G form a partition of G, because they are the equivalence classes of some equivalence relation which you should be able to define.
- know that the same kind of thing is true for right cosets.
- know that the number of left cosets is equal to the number of right cosets.
- can define the index of a subgroup in a group.
- understand well the example of the cosets of the subgroup $n\mathbf{Z}$ in $\mathbf{Z}$.
- understand the example of subgroups of index 2: the fact that for a subgroup H of G of index 2, the two cosets (both left and right) are given by H and $G \setminus H$. Always think of the example $H = \mathfrak{A}_n$ in $G = \mathfrak{S}_n$.
- understand why all left cosets have the same number of elements.
- understand well the counting formula: the group G is partitioned into $[G : H]$ cosets which all have the same size $|H|$, and therefore $|G| = [G : H]|H|$.
- understand how the counting formula implies Lagrange's theorem.
- can give the list of all of the subgroups of $\mathbf{Z}/n\mathbf{Z}$ for concrete values of n.
- are aware of the fact that the converse of Lagrange's theorem is not always true.
- are familiar with Euler's theorem and Fermat's little theorem and can apply them in concrete situations.
- know that the cosets of the kernel of the homomorphism are the fibers of the homomorphism, so that the index of the kernel is equal to the number of elements in the image.
- can deduce from the latter the equality $|G| = |\operatorname{Ker} f||\operatorname{Im} f|$ for a homomorphism $f : G \to G'$.

6 Normal subgroups and quotients of groups

6.1 Normal subgroups

Definition 6.1.1. A subgroup N of a group G is a *normal subgroup* if for every $a \in N$ and for every $g \in G$, the *conjugate* gag^{-1} is in N.

Example 6.1.2. All subgroups of an abelian group are normal.

Example 6.1.3. Recall that the center of a group G is defined by

$$Z(G) = \{a \in G,\ ga = ag \text{ for all } g \in G\}.$$

By definition, it is always a normal subgroup of G.

Example 6.1.4. By proposition 5.2.7, a subgroup of index 2 is always normal. Thus, $\mathfrak{A}_n$ is a normal subgroup of $\mathfrak{S}_n$.

Proposition 6.1.5. *Let $f : G \to H$ be a group homomorphism. Then* $\operatorname{Ker} f$ *is a normal subgroup of G.*

This proposition gives us several examples of normal subgroups of non-abelian groups.

Example 6.1.6.

1. The subgroup $SL_n(\mathbf{R})$ of $(GL_n(\mathbf{R}), \cdot)$ was defined as the kernel of the homomorphism $\det : (GL_n(\mathbf{R}), \cdot) \to (\mathbf{R}^\times, \cdot)$,, therefore it is normal.
2. We can also recover example 6.1.4 in this way: the subgroup $\mathfrak{A}_n$ of $\mathfrak{S}_n$ is the kernel of the sign homomorphism, therefore it is normal.

Definition 6.1.7. Let H be a subgroup of a group G. Then for every $g \in G$, we define the *conjugate* of H by g to be the set

$$gHg^{-1} = \{ghg^{-1},\ h \in H\}.$$

November 20th:

Proposition 6.1.8. *Let H be a subgroup of a group G. Then for every $g \in G$, gHg^{-1} is a subgroup of G.*

Proposition 6.1.9. *Let H be a subgroup of a group G. The following conditions are equivalent:*

1. *H is a normal subgroup.*
2. *For all $g \in G$, $gHg^{-1} = H$.*
3. *For all $g \in G$, the left coset gH is equal to the right coset Hg.*

Proof. We start by proving $1 \Rightarrow 2$. If H is normal, then we have, for every $g \in G$, that $gHg^{-1} \subset H$. It remains to prove the reverse inclusion. Let $h \in H$, and consider the element $k = g^{-1}hg \in g^{-1}Hg$. Since H is normal, we have $k \in H$. Then $h = gkg^{-1}$ is an element of gHg^{-1}.

We now prove $2 \Rightarrow 3$. Let $g \in G$, and let $h \in H$. Then $gh = ghg^{-1} \cdot g \in Hg$. Thus, we have $gH \subset Hg$. In the same manner, we get $Hg \subset gH$.

Finally we prove $3 \Rightarrow 1$. Let $g \in G$ and $x \in H$. We want to show that $gxg^{-1} \in H$, i.e. that $gx \in Hg$. Since $gx \in gH$ which is equal to Hg by assumption, we are done.

□

Proposition 6.1.10. *Let r be an integer. If a group G has exactly one subgroup H of order r, then H is normal.*

6.2 Quotient groups

Recall that whenever we have a set X endowed with an equivalence relation $\sim$, we can define the *quotient set* $X/\sim$, which is the set of equivalence classes of the relation $\sim$. The quotient set comes with a natural *quotient map* $\pi : X \to X/\sim$, sending an element $x \in X$ to its equivalence class. We have encountered one important example of quotient set and quotient map, in the case where $X = \mathbf{Z}$ and $\sim$ is the relation of congruence modulo n. Then the quotient set was $\mathbf{Z}/n\mathbf{Z}$, and the quotient map $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ was given by sending x to its congruence class $[x]$ modulo n. In this case, in fact, we even had something stronger: the group structure of $\mathbf{Z}$ enabled us to define a natural group structure on $\mathbf{Z}/n\mathbf{Z}$, for which the quotient map happened to be a group homomorphism.

The notion of normal subgroup from the previous paragraph provides an answer to the following question: let G be a group and $H \subset G$ a subgroup. What is the condition on H so that the equivalence relation $\sim$ with equivalence classes the left cosets of H is such that the set $G/\sim$ of left cosets of G may be endowed with a group structure such that the quotient map is a group homomorphism?

Notation 6.2.1. For two subsets X, Y of a group G, we define their product set to be

$$XY = \{g \in G,\ g = xy \text{ for some } x \in X \text{ and } y \in Y\}.$$

For example, a coset aH of a subgroup H of G is the product set $\{a\}H$. The conjugate aHa^{-1} is the product set $\{a\}H\{a^{-1}\}$.

Remark 6.2.2. If H is a subgroup of G, then we have $HH = H$. Indeed, $HH \subset H$ follows from closure. On the other hand, any $h \in H$ may be written in the form $h = eh$ where e is the identity element of H, so $h \in HH$.

Lemma 6.2.3. *Let N be a normal subgroup of a group G. The product set $(aN)(bN)$ of two cosets of N is also a coset of N, equal to the coset abN.*

Theorem 6.2.4. *Let G be a group and N a normal subgroup of G. Then there is a law of composition on the set G/N of cosets of N in G which makes it into a group of order*

$[G : N]$, such that the quotient map $\pi : G \to G/N$ sending an element to G to its coset becomes a surjective group homomorphism with kernel N.

November 25th:

Proof. There are several steps.

Step 1: define a law of composition on G/N.
Using lemma 6.2.3, we may define the product of two cosets C_1 and C_2 to be their product set, which is a coset.

Step 2: check that π satisfies the homomorphism property $\pi(ab) = \pi(a)\pi(b)$.
By definition, the map π sends an element a to its coset aN. Thus, $\pi(ab) = abN$, whereas $\pi(a)\pi(b) = (aN)(bN)$, which by lemma 6.2.3 equals abN, so we have $\pi(ab) = \pi(a)\pi(b)$.

Note that for the moment, it does not make sense to say that π is a group homomorphism, because G/N is not a group!

Step 3: Use the surjectivity of π and Step 2 to show that G/N with the law of composition from Step 1 is a group.
First of all, let us check associativity. For all $y_1, y_2, y_3 \in G/N$, by surjectivity of π there exist $x_1, x_2, x_3 \in G$ such that $\pi(x_i) = y_i$ for all i. Then

$$y_1(y_2y_3) = \pi(x_1)(\pi(x_2)\pi(x_3)) = \pi(x_1)\pi(x_2x_3) = \pi(x_1(x_2x_3))$$

By associativity in G, this is equal to

$$\pi((x_1x_2)x_3) = \pi(x_1x_2)\pi(x_3) = (\pi(x_1)\pi(x_2))\pi(x_3) = (y_1y_2)y_3.$$

The identity element is going to be $\pi(e) = N$. Indeed, for all $y \in G/N$, choosing $x \in G$ such that $\pi(x) = y$, we have

$$y\pi(e) = \pi(x)\pi(e) = \pi(xe) = \pi(x) = \pi(ex) = \pi(e)\pi(x) = \pi(e)y,$$

so the fact that e is the identity element in G forces $\pi(e)$ to be the identity element in G/N.

Finally, we need to check existence of inverses. Let $y \in G/N$, and choose $x \in G$ such that $\pi(x) = y$. Then

$$y\pi(x^{-1}) = \pi(x)\pi(x^{-1}) = \pi(xx^{-1}) = \pi(e) = \pi(x^{-1}x) = \pi(x^{-1})\pi(x) = \pi(x^{-1})y.$$

Therefore, the element $\pi(x^{-1})$ is the inverse of y in G/N. We have checked all three group axioms G1, G2, G3, so G/N with the law of composition defined above is a group. Moreover, this gives us immediately that π is a surjective group homomorphism.

Step 4: prove that $\operatorname{Ker}\pi = N$.
An element $x \in G$ is in $\operatorname{Ker}\pi$ if and only if its coset is the identity element N of G/N, so if and only if $x \in N$. □

Remark 6.2.5. We have seen that the kernel of a group homomorphism is always normal. This theorem shows that conversely, any normal subgroup of G is the kernel of some group homomorphism.

Example 6.2.6. 1. The quotient group of $\mathbf{Z}$ by the normal subgroup $n\mathbf{Z}$ is $\mathbf{Z}/n\mathbf{Z}$, which is of order $n = [\mathbf{Z} : n\mathbf{Z}]$.

2. The normal subgroup $\mathfrak{A}_3 = \{\mathrm{id}, (1,2,3), (1,3,2)\}$ of $\mathfrak{S}_3$ has a quotient group of order 2, so isomorphic e.g. to $\{1, -1\}$. The quotient map is given by $\pi : \mathfrak{S}_n \to \{1, -1\}$ with $\pi(x) = 1$ for $x \in \mathfrak{A}_3$, and $\pi(x) = -1$ otherwise. Thus, it is equal to the sign homomorphism.

6.3 First isomorphism theorem

Recall from section 5.5 that the left cosets of the kernel of a homomorphism $\phi : G \to G'$ are exactly the *fibers* of this homomorphism. A homomorphism $\phi : G \to G'$ is constant on every left coset $a\mathrm{Ker}\,\phi$ (sending every element of $a\mathrm{Ker}\,\phi$ to $\phi(a)$), and conversely, whenever we have $\phi(x) = \phi(x')$, this means that x and x' belong to the same left coset of $\mathrm{Ker}\,\phi$ in G. Thus, as proved in proposition 5.5.3, there is a bijection

$$\{\text{left cosets of } \mathrm{Ker}\,\phi\} \to \mathrm{Im}\,\phi$$

sending a coset $a\mathrm{Ker}\,\phi$ to $\phi(a)$.

Now we know more, namely that $\mathrm{Ker}\,\phi$ is a normal subgroup of G, and that therefore the set of its left cosets is a group, the quotient $G/\mathrm{Ker}\,\phi$. Thus, the above bijection can be upgraded into a group isomorphism.

Theorem 6.3.1. *Let $\phi : G \to G'$ be a group homomorphism. Then the quotient group $G/\mathrm{Ker}\,\phi$ is isomorphic to $\mathrm{Im}\,\phi$.*

Proof. We define $\bar{\phi} : G/\mathrm{Ker}\,\phi \to \mathrm{Im}\,\phi$ as above, by $\bar{\phi}(a\mathrm{Ker}\,\phi) = \phi(a)$. We already know that $\bar{\phi}$ is bijective, so it suffices to prove that it is a group homomorphism. We have

$$\bar{\phi}(a\mathrm{Ker}\,\phi)\bar{\phi}(b\mathrm{Ker}\,\phi) = \phi(a)\phi(b) = \phi(ab) = \bar{\phi}(ab\mathrm{Ker}\,\phi) = \bar{\phi}((a\mathrm{Ker}\,\phi)\cdot(b\mathrm{Ker}\,\phi))$$

by definition of the product in $G/\mathrm{Ker}\,\phi$. □

Remark 6.3.2. More precisely, if $\pi : G \to G/\mathrm{Ker}\,\phi$ is the quotient map, note moreover that we have

$$\bar{\phi} \circ \pi(a) = \bar{\phi}(a\mathrm{Ker}\,\phi) = \phi(a)$$

for all $a \in G$, so $\bar{\phi} \circ \pi = \phi$.

Thus, what we have actually proved is that there is a unique isomorphism $\bar{\phi} : G/\mathrm{Ker}\,\phi \to \mathrm{Im}\,\phi$ such that $\phi = \bar{\phi} \circ \pi$, as described by the following diagram:

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & \mathrm{Im}\,\phi \subset G' \\ G/\mathrm{Ker}\,\phi \arrow[ur, dashed, "\bar{\phi}"'] & \end{tikzcd}$$

Remark 6.3.3. When $\phi : G \to G'$ is surjective, it induces an isomorphism $\bar{\phi} : G/\mathrm{Ker}\,\phi \to G'$.

Remark 6.3.4. If $G' = G/N$ for some normal subgroup N of G and if $\phi : G \to G/N$ is the quotient map, then $N = \mathrm{Ker}\,\phi$, and $\bar{\phi} : G/\mathrm{Ker}\,\phi \to G/\mathrm{Ker}\,\phi$ is the identity. For example, if $\phi : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ is the quotient map sending an integer a to its congruence class, then the kernel is $n\mathbf{Z}$ and ϕ induces the identity morphism $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$.

Example 6.3.5.

1. Let G be a group and g an element of G. There is a well-defined surjective group homomorphism
$$\mathbf{Z} \to \langle g \rangle$$
sending an integer n to g^n. If g is of infinite order, then the kernel is $\{0\}$ and we have an isomorphism $\mathbf{Z} \simeq \langle g \rangle$. If g is of finite order a, then the kernel is $a\mathbf{Z}$ and we get an isomorphism
$$\mathbf{Z}/a\mathbf{Z} \to \langle g \rangle.$$
Thus, the first isomorphism theorem gives us a direct way of classifying finite cyclic groups (which we did by hand in proposition 3.7.6).

2. Let $n \geq 2$ and let $\mathrm{sgn} : \mathfrak{S}_n \to \{1, -1\}$ be the sign homomorphism. It is surjective with kernel $\mathfrak{A}_n$, so that it induces an isomorphism
$$\mathfrak{S}_n/\mathfrak{A}_n \simeq \{1, -1\}.$$
By this isomorphism, the coset $\mathfrak{A}_n$ goes to 1, and the coset $(12)\mathfrak{A}_n$ goes to -1.

3. The absolute value morphism $|\cdot| : (\mathbf{C}^\times, \cdot) \to (\mathbf{R}^\times, \cdot)$ has image the group of positive real numbers $\mathbf{R}_{>0}$, and kernel the unit circle
$$U = \{z \in \mathbf{C}^\times,\ |z| = 1\}.$$
Therefore, the corollary gives us an isomorphism
$$\mathbf{C}^\times/U \simeq \mathbf{R}_{>0}.$$
The coset rU corresponding to $r \in \mathbf{R}_{>0}$ is the circle with center 0 and radius r.

4. Let $\det : (GL_n(\mathbf{R}), \cdot) \to (\mathbf{R}^\times, \cdot)$ be the determinant homomorphism. It is surjective because for every $\lambda \in \mathbf{R}^\times$ the diagonal matrix D_λ with entries $\lambda, 1, \ldots, 1$ has determinant λ. Its kernel is $SL_n(\mathbf{R})$, and therefore it induces an isomorphism
$$GL_n(\mathbf{R})/SL_n(\mathbf{R}) \simeq \mathbf{R}^\times.$$
The coset $D_\lambda SL_n(\mathbf{R})$ corresponding to $\lambda \in \mathbf{R}^\times$ contains exactly all the matrices with determinant λ.

6.4 Correspondence theorem

Let G be a group and N a normal subgroup of G, so that we have a quotient $\pi : G \to G/N$. In this section, we want to understand the subgroups of G/N in terms of those of G.

If H is a subgroup of G containing N, then it is easy to see that N is a normal subgroup of H. Thus we can consider the quotient group H/N, which in fact will be a subgroup of G/N, corresponding to the image $\pi(H)$.

Conversely, let K be a subgroup of G/N, and consider the inverse image $\pi^{-1}(K)$. We can check that it is a subgroup of G, and it clearly contains H, since any element of H gets sent to the identity element of G/N, which is an element of G/N.

This gives us an exact correspondence between subgroups of G containing N and subgroups of G/N. Moreover, we may check that under this correspondence, normal subgroups of G containing N correspond to normal subgroups of G/N.

We may summarize this in the following:

Proposition 6.4.1 (Correspondence theorem)**.** *Let G be a group and N a normal subgroup of G, and denote by $\pi : G \to G/N$ the quotient morphism. Then there is a bijection*

$$\{\textit{subgroups of } G \textit{ containing } N\} \to \{\textit{subgroups of } G/N\}$$

given by sending H to H/N. Its inverse is given by sending a subgroup K of G/N to $\pi^{-1}(K)$.

Remark 6.4.2. Via this correspondence, N goes to the trivial subgroup of G/N, and G goes to the whole group G/N.

Example 6.4.3. Let $G = \mathbf{Z}$ and $N = 6\mathbf{Z}$. The subgroups of G containing N are $\mathbf{Z}$, $2\mathbf{Z}$, $3\mathbf{Z}$ and $6\mathbf{Z}$. They correspond, respectively, to the following subgroups of $Z/6\mathbf{Z}$: the group $\mathbf{Z}/6\mathbf{Z}$ itself, $\langle 2\rangle$, $\langle 3\rangle$, $\{0\}$.

More generally, for $G = \mathbf{Z}$ and $N = n\mathbf{Z}$, the subgroups of G containing N are the subgroups $m\mathbf{Z}$ for m a divisor of N. Every $m\mathbf{Z}$ corresponds via the bijection to the subgroup $\langle m\rangle = \left\{0, m, 2m, \ldots, \left(\frac{n}{m} - 1\right) m\right\}$ of $\mathbf{Z}/n\mathbf{Z}$ (see example 5.3.8, taking $d = \frac{n}{m}$.)

6.5 Conclusion of the chapter

To check that you have grasped the gist of the chapter, make sure you

- know the definition of a normal subgroup, and the other properties equivalent to it (listed in proposition 6.1.9).
- are familiar with several examples of normal subgroups, e.g. subgroups of abelian groups, subgroups of index 2, kernels.
- know what the quotient set by an equivalence relation, and the quotient map, are.

- know that for normal subgroup, the product set of two cosets is again a coset, and that this defines a group law on the set of cosets making the quotient map into a group homomorphism.

- understand the first isomorphism theorem thanks to the picture in remark 6.3.2 (and can reproduce this picture yourself). The cosets of the kernel of a homomorphism are the fibres of the homomorphism (the coset $a\mathrm{Ker}f$ is exactly the set of points with image $f(a)$ and the isomorphism $G/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ is given by sending $a\mathrm{Ker}f$ to $f(a)$)

- know how to apply the first isomorphism theorem to recover the fact that all cyclic groups are isomorphic to $\mathbf{Z}$ or $\mathbf{Z}/n\mathbf{Z}$.

- understand the bijection in the correspondence theorem, and can write it down explicitly when $G = \mathbf{Z}$ and N is some concrete subgroup of $\mathbf{Z}$.

7 Further topics: towards a classification of abelian finite groups

7.1 Elements with prime order in an abelian group

Let G be a group of order n. Lagrange's theorem implies that the order of any element of G divides n. The converse to Lagrange's theorem is false, in the sense that if d divides n, this does not mean that G has an element of order d. For example, if G is not cyclic, G does not contain an element of order n. As another, more striking, example, the group $(\mathbf{Z}/2\mathbf{Z})^{100}$ is of order 2^{100}, but all of its elements other than the identity element are of order 2.

The following proposition provides nevertheless a partial converse to Lagrange's theorem in the case when G is abelian: if we take p a *prime* divisor of n, then G will have an element of order p. The proof is by induction and uses quotients of groups.

Proposition 7.1.1. *Let G be an abelian group of order n. The group G has an element of order p for every prime divisor p of n.*

December 4th:

Proof. Judson lemma 13.6 □

The proof of this result (which you can find in Judson) uses the following lemma, which is interesting on its own:

Lemma 7.1.2. *Let G be a finite group which has no proper subgroups. Then G is cyclic and the order of G is prime.*

Proof. Let g be an element of G other than the identity, so that $\langle g \rangle$ is not the trivial subgroup. Since G has no proper subgroups, we must have $\langle g \rangle = G$, so that G is cyclic. Let n be the order of G, so that G is isomorphic to $\mathbf{Z}/n\mathbf{Z}$. By our study of the subgroups of $\mathbf{Z}/n\mathbf{Z}$, we know that $\mathbf{Z}/n\mathbf{Z}$ has a subgroup of order d for every divisor n of d (and these subgroups are proper for $d \neq 1, n$). Thus, since G has no proper subgroups, we must have that n is prime. □

7.2 Abelian finite groups

We know that every finite cyclic group is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ for some n. Moreover, we have the following:

Proposition 7.2.1. *Let m, n be relatively prime integers. Then $\mathbf{Z}/mn\mathbf{Z}$ is isomorphic to $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$.*

Note that we proved this in Homework 5, Exercise 4.

Proof. We know that $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ is of order mn. Thus, it suffices to show that it is cyclic. For this, we will show that $(1, 1)$ if of order mn. Let k be an integer such that $k \cdot (1, 1) = (0, 0)$. Then we have $(k, k) = (0, 0)$ in $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$. This means that k is a multiple of both m and n. Since m and n are relatively prime, this means that k is a multiple of mn. (See e.g. Homework 2, Exercise 6). In particular, this means that $k(1, 1)$ is non-zero for $k \in \{1, \ldots, mn - 1\}$. On the other hand, $mn(1, 1) = (0, 0)$, so $(1, 1)$ is indeed of order mn. □

Remark 7.2.2. More generally, we may show that for any integers m, n, all of the elements of $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ have order at most the least common multiple of m and n. In particular, whenever m and n are not relatively prime, this group is not cyclic.

Example 7.2.3. We have that $\mathbf{Z}/12\mathbf{Z}$ is isomorphic to $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. On the other hand, $\mathbf{Z}/12\mathbf{Z}$ is not isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$, as we may see by e.g. noting that all of the elements in the latter group are of order at most 6.

Theorem 7.2.4. *Let G be a finite abelian group. Then G is isomorphic to a group of the form*

$$\mathbf{Z}/p_1^{a_1} \times \ldots \times \mathbf{Z}/p_r^{a_r}\mathbf{Z}$$

where $p_1, \ldots, p_r$ are (not necessarily distinct) prime numbers, and $a_1, \ldots, a_1 \geq 1$ are integers.

Remark 7.2.5. Moreover, the list of prime powers appearing in the decomposition is unique up to reordering.

Remark 7.2.6. What are the constraints on the prime powers p^{a_i}? If G has order n, we must have

$$n = p_1^{a_1} \ldots p_r^{a_r}.$$

This means that to determine all finite abelian groups of order n, it suffices to look at all possible ways of writing n as a product of prime powers (of not necessarily distinct primes).

Remark 7.2.7. If the primes $p_1, \dots, p_r$ happen to be distinct, then the different prime powers are relatively prime, and we get that the group $\mathbf{Z}/p_1^{a_1} \times \dots \times \mathbf{Z}/p_r^{a_r}\mathbf{Z}$ is cyclic, isomorphic to $\mathbf{Z}/n\mathbf{Z}$ where $n = p_1^{a_1} \dots p_r^{a_r}$.

Example 7.2.8.

1. Let G be an abelian group of order 4. We have $4 = 2^2 = 2^1 \times 2^1$. Thus, by the theorem, any group of order 4 is isomorphic to $\mathbf{Z}/2^2\mathbf{Z}$ or to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$. We recover what we knew about groups of order 4.

2. Let G be an abelian group of order 6. The only way of writing 6 as a product of prime powers is $6 = 2^1 \times 3^1$. Thus the only abelian group of order 6 is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, which by lemma 7.2.1 is isomorphic to $\mathbf{Z}/6\mathbf{Z}$. Thus, any abelian group of order 6 is cyclic. On the other hand, we know that there exists another non-abelian group of order 6, namely $\mathfrak{S}_3$.

3. Let G be an abelian group of order 12. We have $12 = 2^2 \times 3 = 2^1 \times 2^1 \times 3$. Thus, an abelian group of order 12 is isomorphic either to $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ ($\simeq \mathbf{Z}/12\mathbf{Z}$), or to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ ($\simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$).

4. Let G be an abelian group of prime order p. The only way of writing p as a product of prime powers is $p = p^1$, and therefore G is isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Of course, we already know something stronger, namely that any group of prime order p (without commutativity assumption) is isomorphic to $\mathbf{Z}/p\mathbf{Z}$.

December 9th:

How does one prove such a theorem? As a first motivation, let's look at at a group of the form given in the statement of the theorem, e.g. $G = \mathbf{Z}/2^3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3^2\mathbf{Z}$.

What can we observe? Elements of this group of the form $(x, 0, 0)$ (i.e. with coordinate with respect to the $\mathbf{Z}/3\mathbf{Z}$ and $\mathbf{Z}/3^2\mathbf{Z}$-component equal to zero) are all of order $1, 2, 4$ or 8. In fact, they are the only elements of G which are of order a power of 2. On the other hand, all of the elements of the form $(0, x, y)$ (i.e. with coordinates with respect to the $\mathbf{Z}/2^3\mathbf{Z}$-component equal to zero) are of order a power of 3.

Thus, to come up with a decomposition of a group G into cyclic subgroups of prime power order, it will be useful to consider, for every prime p dividing the order of G, the subset $G(p)$ of elements of G of order a power of p. The plan is then the following:

1. Show that $G(p)$ is a subgroup of G for every p. It will be also useful to know, for step 3, that the order of $G(p)$ is the largest power of p dividing the order of G.

2. Show that for every p, $G(p)$ is isomorphic to a product of groups of the form $\mathbf{Z}/p^k\mathbf{Z}$. In other words, there exist integers $b_1, \dots b_s$ such that $G(p)$ is isomorphic to

$$\mathbf{Z}/p^{b_1}\mathbf{Z} \times \dots \times \mathbf{Z}/p^{b_s}\mathbf{Z}.$$

3. Show that G is isomorphic to the product of the $G(p)$ over all primes p dividing its order.

Combining Steps 2 and 3, we get the theorem. We won't be saying much more about Steps 2 and 3 as their proofs are more involved, but we will explain Step 1 completely.

Lemma 7.2.9. *Let G be an abelian group and x, y two elements such that $x^n = y^n = e$. Then $(xy)^n = e$, and therefore xy has order dividing n.*

Proof. We have $(xy)^n = x^n y^n = e$ because the group is abelian, so the order of xy divides n. $\square$

Remark 7.2.10. This fails badly if the group is not abelian. See e.g. homework 5, exercise 5. In that setting, though we have $A^{12} = B^{12} = I_2$, we have $(AB)^{12} \neq I_2$, and in fact, AB is of infinite order.

Lemma 7.2.11. *Let G be an abelian finite group and let p be a prime number. Let H be the subset of all elements of G having order a power of p. Then H is a subgroup of G of order p^α where p^α is the highest power of p dividing the order of G.*

Proof. We first prove that H is a subgroup of G.

Closure: Let $x, y \in H$, and let p^r, p^s be their respective orders. Without loss of generality, we may assume $r \geq s$. Then we have $x^{p^r} = e$, and $y^{p^r} = y^{p^s \cdot p^{r-s}} = \left(y^{p^s}\right)^{p^{r-s}} = e$. Then by lemma 7.2.9, the order of xy divides a power of p, so is a power of p itself.

Identity: The identity e has order $1 = p^0$, so $e \in H$.

Inverses: Let $x \in H$ be of order p^r. Then x^{-1} is of order p^r as well, so is also an element of H.

We may conclude that H is a subgroup of G.

We now determine the order of H. Note first of all that its order must be some power of p, say p^β: indeed, if its order had any other prime divisor q, it would have an element of order q by 7.1.1. Moreover, by Lagrange's theorem, we must have $\beta \leq \alpha$.

Since G is abelian, H is normal and we may consider the quotient group G/H. If we assume, for the sake of contradiction, that $\beta < \alpha$, then the order of G/H is divisible by p and so by lemma 7.1.1, it must have an element of order p. In other words, there exists $g \in G$ such that the coset gH is of order p. This means that $g \notin H$, but $(gH)^p = H$, i.e. $g^p H = H$, so that $g^p \in H$. Now, since $g^p \in H$, its order divides the order of H, so that there exists a power of p, say p^r, such that $(g^p)^{p^r} = e$. Then $g^{p^{r+1}} = e$. This in turn implies that the order of g is a power of p, so that by definition of H we should have $g \in H$, which is a contradiction. $\square$

Example 7.2.12. Let G be a group of order $12 = 2^2 \times 3$. From what we have proved, we know that G has (at least) the following two subgroups:

- $G(2)$, of order 4, containing all elements of order a power of 2 (i.e., in fact just of orders $1, 2, 4$ in this case).
- $G(3)$, of order 3, containing all elements of order a power of 3 (i.e., in fact just of orders 1 or 3 in this case).

In this special case, we already have a proof of Step 2: since $G(2)$ is of order 4, we know it is isomorphic to $\mathbf{Z}/4\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and since $G(3)$ is of order 3, we know it is isomorphic to $\mathbf{Z}/3\mathbf{Z}$. It remains to prove that G is isomorphic to the group of order 12 given by $G(2) \times G(3)$, which is what would follow from Step 3 of the proof. We thus recover that G is isomorphic to either to $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ or to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

7.3 Conclusion of the chapter

Here are a few guidelines on what you really need to remember from this chapter:

- Know that if G is an abelian group of order n and p is a prime dividing n, then G has an element of order p. It is important to note that we require G to be abelian! Remember a few details of the proof, e.g. the fact that we do an induction and that we use quotients.

- Know how to prove that if G is a group with no proper subgroups, then G is cyclic, isomorphic to $\mathbf{Z}/p\mathbf{Z}$ for some prime p.

- Know that when m and n are relatively prime, $\mathbf{Z}/mn\mathbf{Z}$ is isomorphic to $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, and can apply it for concrete values of m and n. You should also understand why this fails if m and n are not relatively prime.

- Can state the classification theorem for abelian finite groups and can apply it in concrete cases to classify abelian groups of some order n, as in the examples given.

- Remember that if $x, y \in G$ are elements of an abelian group G, you can deduce information about the order of xy from the orders of x and y, but are aware that this doesn't work in general if the group is not abelian.

- Know that for any abelian group G, the subset $G(p)$ of elements of order a power of p is a subgroup.