MATH 1530: Abstract Algebra

Spring 2017

Notes for Abstract Algebra

Nicholas Tomlin

Contents

1 Introduction

1.1 Preliminary definitions

Definition 1.1.1: *A **set** is "a collection of elements," e.g., the integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the real numbers $\mathbb{R}$, and the rational numbers $\mathbb{Q}$ (fractions). Note that we use $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$ to refer to the nonnegative integers.*

Definition 1.1.2: *If A, B are sets, define the **Cartesian product** as*

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

We can abbreviate $A^2 = A \times A$. Similarly, if $A_1, \ldots, A_n$ are sets, then

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}$$

Let $A^n = A \times \cdots \times A$ (n times).

Definition 1.1.3: *A **function** $f : A \to B$, or a **map**, is an association of an element $f(a) \in B$ to every element $a \in A$. We call A the **domain** of f, and B the **codomain** of f. Furthermore, the **range** or **image** of f is*

$$\{f(a) : a \in A\}$$

Example 1: Let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $x \mapsto 2x$.[1] The codomain and domain are both $\mathbb{Z}$, while the image is

$$\{b \in \mathbb{Z} : b = 2a \text{ for some } a \in \mathbb{Z}\}$$

which is the set of even numbers.

Definition 1.1.4: *A **binary operation** on a given set G is a function $* : G \times G \to G$. For example, integer addition ($+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$) is a binary operation.*

[1] The symbol $\mapsto$ means "maps to."

1.2 What is a group?

Definition 1.2.1: *A **group** is a set G together with a binary operation $* : G \times G \to G$ such that the following hold:*
(1) "Associativity": for $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
(2) "Existence of the identity": there is an element $e \in G$ such that for all $g \in G$, $e * g = g$ and $g * e = g$.
(3) "Existence of inverses": for every $g \in G$, there is an element that we'll call $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$, where e is an identity element of G.

Theorem 1.2.2
$(\mathbb{Z}, +)$ forms a group.[a]

[a] We write the ordered pair $(\mathbb{Z}, +)$ to represent the integers along with the binary operation of addition.

Proof. Indeed, we check that $(\mathbb{Z}, +)$ satisfies the three axioms of being a group:
(1) For associativity, we note that $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Z}$.
(2) For existence of the identity, $0 \in Z$ satisfies $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}$.
(3) For existence of inverses, consider some $a \in \mathbb{Z}$. Then assert that $-a \in \mathbb{Z}$ satisfies $a + (-a) = (-a) + a = 0$.
Thus, we have shown that $(\mathbb{Z}, +)$ is a group. □

Definition 1.2.3: *Let $(G, *)$ be a group. Then G is a **commutative** or **abelian** group if $a * b = b * a$ for all $a, b \in G$.*

For example, $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Q}$ with addition are all **commutative groups**. However, below is an example of a non-commutative group.

Example 2: Not all groups are commutative. Let G be the symmetries of a can (cylinder) C which are physically possible, i.e., the rigid motions preserving the can. These are called the orientation-preserving isometries of $\mathbb{R}^3$. More precisely, we can define the set of symmetries

$$\text{Sym}(C) = \{A : \mathbb{R} \to \mathbb{R} : \ \det(A) = 1, A(C) = C\}$$

where A is an linear transformation which is an isometry. Put this together with the binary operation of composition $\circ$, and this forms a group.

However, these motions are not commutative. That is, flipping the can and then rotating it is distinct from rotating the can and then flipping it.

Theorem 1.2.4
Every group has a unique identity element.

1.3 The group $\mathbb{Z}/n\mathbb{Z}$

Definition 1.3.1: *Let A be a nonempty set. Then a* ***relation*** *on A is a subset $R \subseteq A \times A$, which is written $a \sim b$ if and only if $(a, b) \in R$.*

Definition 1.3.2: *A relation R is an* ***equivalence relation*** *if it satisfies the following three properties:*
(1) "Reflexivity": $a \sim a$ for all $a \in A$.
(2) "Symmetry": if $a \sim b$, then $b \sim a$ for all $a, b \in A$.
(3) "Transitivity": if $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in A$.

Let $f : A \to D$ be a function. Given $a, b \in A$, we'll say $a \sim b$ if and only if $f(a) = f(b)$. This is an equivalence relation; moreover, all equivalence relations can be written in this form.

Example 3: Consider the set $A = \{\text{students in Math 1530}\}$. For any two students $a, b \in A$, say $a \sim b$ if and only if a has the same birthday as b. This is an equivalence relation, so we can relate this to the above form as follows. Let $D = \{\text{Jan } 1, \ldots, \text{Dec } 31\}$ be the set of possible birthdays, and $f : A \to D$ be a function mapping students to their birthdays.

Definition 1.3.3: *Let $\sim$ be an equivalence relation on A. Then we say*

$$\overline{a} = \{b \in A : a \sim b\}$$

is an ***equivalence class*** *of a. The equivalence classes of A partition it into non-overlapping groups covering all of A.*

Let $n \in \mathbb{Z}$. Say $n \mid a$ (pronounced "n divides a") if $a = kn$ for some $k \in \mathbb{Z}$. Now define a relation $\equiv_n$ on $\mathbb{Z}$ by $a \equiv_n b$ if $n \mid (a - b)$. We call this relation "congruent modulo n." To prove that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$, we must show the following:

(1) $a \equiv_n a$ for all $a \in \mathbb{Z}$.

(2) $a \equiv_n b$ implies $b \equiv_n a$ for all $a, b \in \mathbb{Z}$.

(3) $a \equiv_n b$ and $b \equiv_n c$ implies $a \equiv_n c$ for all $a, b, c \in \mathbb{Z}$.

Proof. Indeed, we will show that $\equiv_n$ satisfies the three axioms of equivalence relations:
(1) For reflexivity, $a - a = 0$ and $n \mid 0$.
(2) For symmetry, $a \equiv_n b \implies n \mid (a - b) \implies a - b = kn$ for some $k \in \mathbb{Z}$. We want to show that $b \equiv_n a$, i.e., $b - a = ln$ for some $l \in \mathbb{Z}$. We may take $l = (-k)$.
(3) For transitivity, there exists $k, l \in \mathbb{Z}$ such that $a - b = kn$ and $b - c = ln$. Then, adding these equations gives $a - c = (k + l)n$. Since $(k + l) \in \mathbb{Z}$, we conclude $n \mid (a - c) \implies a \equiv_n c$.

□

Definition 1.3.4: *$\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes modulo n, i.e., equivalence classes with respect to the equivalence relation $\equiv_n$.*

For example, $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. The choice of "captains" is not important, so we could alternatively write this as $\mathbb{Z}/5\mathbb{Z} = \{\overline{10}, \overline{-4}, \overline{2}, \overline{8}, \overline{24}\}$.

Definition 1.3.5: *We define the binary operation of addition $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ as follows: $\overline{a} + \overline{b} = \overline{a+b}$ for all $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$.*

Lemma 1.3.6
Addition on $\mathbb{Z}/n\mathbb{Z}$ is well-defined, as stated above.

Proof. Given $a_1, a_2 \in \mathbb{Z}$ such that $\overline{a}_1 = \overline{a}_2$ and $b_1, b_2 \in \mathbb{Z}$ such that $\overline{b}_1 = \overline{b}_2$, we want to show that $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. Indeed, $a_1 - a_2 = kn$ and $b_1 - b_2 = ln$ for $k, l \in \mathbb{Z}$. Adding these equations gives

$$(a_1 + b_1) - (a_2 + b_2) = (k + l)n$$

so that $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ since $(k + l) \in \mathbb{Z}$. □

Theorem 1.3.7
$(\mathbb{Z}/n\mathbb{Z}, +)$ is a group.

Proof. Again, we check the three group axioms:
(1) We have

$$\begin{aligned}
\overline{a} + (\overline{b} + \overline{c}) &= \overline{a} + \overline{b + c} \\
&= \overline{a + (b + c)} \\
&= \overline{(a + b) + c} \\
&= \overline{a + b} + \overline{c} \\
&= (\overline{a} + \overline{b}) + \overline{c}
\end{aligned}$$

by associativity of addition.
(2) We have $\overline{0} + \overline{a} = \overline{a} + \overline{0} = \overline{a}$ for all $a \in \mathbb{Z}/n\mathbb{Z}$.
(3) We have $-\overline{a} + \overline{a} = \overline{a} + (-\overline{a}) = \overline{0}$ for all $a \in \mathbb{Z}/n\mathbb{Z}$.

□

Definition 1.3.8: *We define the binary operation of multiplication $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ as follows: $\overline{a} \cdot \overline{b} = \overline{ab}$ for all $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$.*

Theorem 1.3.9
Multiplication on $\mathbb{Z}/n\mathbb{Z}$ is well-defined, as defined above.

1.3.1 The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$

However, $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is not a group unless $n = 1$, as inverses may not exist. Indeed, $\bar{1}$ is an identity, but $\bar{0} \cdot a = \bar{1}$ has no solution, i.e., there is no multiplicative inverse for $\bar{0}$. Now, let:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \bar{a} \cdot \bar{c} = \bar{1} \text{ for some } \bar{c} \in \mathbb{Z}/n\mathbb{Z}\}$$

We call this set "the multiplicative units of $\mathbb{Z}/n\mathbb{Z}$."

Example 4: Given $n = 4$, we say $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$. In particular, $\bar{1} \cdot \bar{1} = \bar{1}$ and $\bar{3} \cdot \bar{3} = \bar{1}$.

Theorem 1.3.10
$((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ is a group.

Proof. Given $\bar{a}, \bar{c} \in (\mathbb{Z}/n\mathbb{Z})^\times$, we must show that $\bar{a} \cdot \bar{c} \in (\mathbb{Z}/n\mathbb{Z})^\times$. First, we will show that $\cdot$ defines a binary operation on $(\mathbb{Z}/n\mathbb{Z})^\times$, i.e., $(\mathbb{Z}/n\mathbb{Z})^\times$ is closed under multiplication. Indeed, $\bar{a} \cdot \bar{b} = \bar{1}$ and $\bar{c} \cdot \bar{d} = \bar{1}$ for some $\bar{b}, \bar{d} \in \mathbb{Z}/n\mathbb{Z}$. Multiplying these equations gives:

$$\begin{aligned} \bar{1} &= (\bar{a} \cdot \bar{b})(\bar{c} \cdot \bar{d}) \\ &= (\bar{a} \cdot \bar{c})(\bar{b} \cdot \bar{d}) \end{aligned}$$

In addition, associativity holds as in $\mathbb{Z}/n\mathbb{Z}$. There is an identity element, namely $\bar{1}$, and inverses exist as in $\mathbb{Z}/n\mathbb{Z}$ based on the definition of $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Theorem 1.3.11
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} : a \in \mathbb{Z}, (a, n) = 1\}$

1.3.2 Applications of arithmetic in $\mathbb{Z}/n\mathbb{Z}$

Example 5: *What is the last digit of* 2^{50}*?* To calculate this, work in $\mathbb{Z}/10\mathbb{Z}$:

$$\begin{aligned} \bar{2} \cdot \bar{2} &= \bar{4} \\ \bar{2} \cdot \bar{2} \cdot \bar{2} &= \bar{8} \\ \bar{2} \cdot \bar{2} \cdot \bar{2} \cdot \bar{2} &= \bar{6} \\ \bar{2} \cdot \bar{2} \cdot \bar{2} \cdot \bar{2} \cdot \bar{2} &= \bar{2} \end{aligned}$$

and so on. Hence this cycles through $(\bar{2}, \bar{4}, \bar{8}, \bar{6})$ as demonstrated above. We can use this pattern to see the last digit is $\boxed{4}$. Alternatively, since $\overline{2^5} = \bar{2}$:

$$\begin{aligned} \overline{2^{50}} &= \overline{(2^5)^{10}} \\ &= \overline{2^{10}} \\ &= \overline{2^5} \cdot \overline{2^5} \\ &= \bar{2} \cdot \bar{2} = \bar{4} \end{aligned}$$

1.4 Some general theorems about groups

Lemma 1.4.1
Let $(G, *)$ be a group. Then G has a unique identity element.

Proof. Let $e, f \in G$ be identity elements. Then:

$$\begin{aligned} e &= e * f \text{ (since } f \text{ is an identity element)} \\ e * f &= f \text{ (since } e \text{ is an identity element)} \end{aligned}$$

Therefore $e = f$ and there is exactly one identity element. □

Lemma 1.4.2
Let $(G, *)$ be a group. Then G has a unique inverse.

Proof. Given $a \in G$, suppose that $b, c \in G$ are inverses of a. Then:

$$\begin{aligned} e &= a * b \text{ (since } b \text{ inverse of } a) \\ c * e &= c * a * b \\ c &= b \text{ (since } c \text{ inverse of } a) \end{aligned}$$

Since $b = c$, every element of a group must have a unique inverse. □

Lemma 1.4.3
Let $(G, *)$ be a group. Then $(a * b)^{-1} = (b^{-1}) * (a^{-1})$ for all $a, b \in G$.

Proof. We need to check that $(a * b) * ((b^{-1}) * (a^{-1})) = e$ is the identity element. This is left as an exercise to the reader. □

Lemma 1.4.4
Let $(G, *)$ be a group. For any $a_1, \ldots, a_n \in G$, $a_1 * \cdots * a_n$ has a well-defined value, i.e., is independent of bracketing.

Theorem 1.4.5
Given $(G, *)$ a group and $a, b \in G$, the equation $ax = b$ has a unique solution.

1.5 The order of a group

Definition 1.5.1: *Let $(G, *)$ be a group. The **order of a group** G denoted $|G|$ is the number of elements. If G is infinite, say $|G| = \infty$.*

Definition 1.5.2: *Let $(G, *)$ be a group. The **order of an element** $a \in G$ is the smallest $n \in \mathbb{Z}_{>0}$ such that $a^n = e$.*

Example 6: The symmetries of a can $Sym(C)$ has order $|Sym(C)| = \infty$, but it has elements of finite order. For instance, the identity has order $|e| = 1$. A rotation by 180° has order 2, a rotation by 120° has order 3, and so on. In fact, for any order $n \in \mathbb{Q}$, a rotation by $2\pi/n$ has order n.

1.6 A brief interlude on functions

Definition 1.6.1: *Let $f : A \to C$ be a function on sets. Then f is **injective** (one-to-one) if given any two elements $a, b \in A$, then $f(a) = f(b) \implies a = b$.*[a]

[a] The contrapositive, $a \neq b \implies f(a) \neq f(b)$ is equivalent.

Definition 1.6.2: *Let $f : A \to C$ be a function on sets. Then f is **surjective** (onto) if for all $c \in C$, there exists $a \in A$ with $f(a) = c$.*

Definition 1.6.3: *A function is **bijective** if it is both injective and surjective.*

Given a function $f : A \to C$ between finite sets A and C, then we write $|A|$ to denote the number of elements (i.e., the **cardinality**) of A. Then, we can say:

1. f injective $\implies |A| \leq |C|$
2. f surjective $\implies |A| \geq |C|$
3. f bijective $\implies |A| = |C|$

2 Some important groups

2.1 Dihedral groups

Definition 2.1.1: *The **dihedral group**, denoted D_{2n}, is the group of rigid motions of a regular n-gon. The group operation is composition.*

The $2n$ subscript in the name for the dihedral group refers to the order of the group. We can rotate the n-gon by integer multiples of $2\pi/n$, and we can "flip" the n-gon in $\mathbb{R}^3$. These combinations of rotations and flips are specifically the $2n$ elements of the dihedral group.

More rigorously, we can label the vertices of an n-gon $\{1, \ldots, n\}$ in clockwise order. A rigid motion of the n-gon can be recorded as a bijection

$$\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

i.e., a permutation of $\{1, \ldots, n\}$. Therefore, $\sigma(j)$ records the new position of vertex j. We claim that the map of sets

$$D_{2n} \to \{\text{bijections from } \{1, \ldots, n\} \to \{1, \ldots, n\}\}$$

is injective. The intuition here is that the rigid motions of the n-gon are a subset of the possible permutations. Now, note that D_{2n} has at least $2n$ elements (as shown above).

Theorem 2.1.2
$|D_{2n}| = 2n$ *(i.e., D_{2n} is the dihedral group of order $2n$)*

Proof. We know that $|D_{2n}| \geq 2n$, so we want to show $|D_{2n}| \leq 2n$. Define a map:

$$\begin{aligned} D_{2n} &\to \{(1,2), \ldots, (n-1,n), (n,1), (2,1), \ldots, (n,n-1), (1,n)\} \\ \sigma &\mapsto (\sigma(1), \sigma(2)) \end{aligned}$$

where the target has cardinality $2n$. This map is injective, since any two adjacent elements uniquely define a rigid motion of the n-gon. Thus, $|D_{2n}| \leq 2n$. □

2.1.1 Explicit description of D_{2n}

Label an n-gon $\{1, \ldots, n\}$ on its vertices. Let r be clockwise rotation by $2\pi/n$, and let s be a reflection about the central line bisecting the angle at vertex 1. Note that:

- $1, \ldots, r^{n-1} \in D_{2n}$ are distinct rotations.
- s is distinct from $1, \ldots, r^{n-1}$.
- $s, sr, sr^2, \ldots, sr^{n-1} \in D_{2n}$ are all distinct.

Theorem 2.1.3
$D_{2n} = \{1, \ldots, r^{n-1}, s, \ldots, sr^{n-1}\}$

Proof. We need only show that

$$r^i \neq sr^j \text{ for any } i, j \in \{1, \ldots, n-1\}$$

Indeed, $r^{i-j} \neq s$. □

Furthermore, $rs = sr^{-1}$, i.e., rotating and reflecting is the same as reflecting and rotating by the same amount in the opposite direction.

Given these observations, we now know how to multiply in D_{2n}. For example, we can multiply the rigid motions (sr^6) and (sr^9) on an arbitrary regular n-gon:

$$\begin{aligned}(sr^6)(sr^9) &= s(r^6 s)r^9 \\ &= s(r^5 sr^{-1})r^9 \\ &= s(sr^{-6})r^9 \\ &= r^3\end{aligned}$$

Alternatively, we can define D_{2n} in terms of generators and relations as follows:

$$D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle$$

In particular, any relation on elements of D_{2n} can be obtained from the given relations.

2.2 Symmetric groups

Definition 2.2.1: *Let X be a non-empty set, and let S_X be the permutations of X. When $X = [n] := \{1, \ldots, n\}$, we write $S_n = S_{\{1,\ldots,n\}}$. Then S_X is a group under composition, where $f * g = g \circ f$.*

Example 7: $S_3 = \{\{1,2,3\}, \{1,3,2\}, \{2,1,3\}, \{2,3,1\}, \{3,1,2\}, \{3,2,1\}\}$.

Lemma 2.2.2
A map $f : A \to C$ is a bijection if and only if there exists a function $g : C \to A$ such that $f \circ g = \mathrm{id}_C$ and $g \circ f = \mathrm{id}_C$.

Theorem 2.2.3
The order $|S_n| = n!$, i.e., the factorial of n.

Proof. To choose a permutation of $\{1, \ldots, n\}$, we can choose any of n mappings for 1, $n-1$ remaining mappings for 2, and so on. Since there is no "overlap," this is an injective function. Furthermore, since this is injective and the domain and range have the same number of elements, it is also a bijection. □

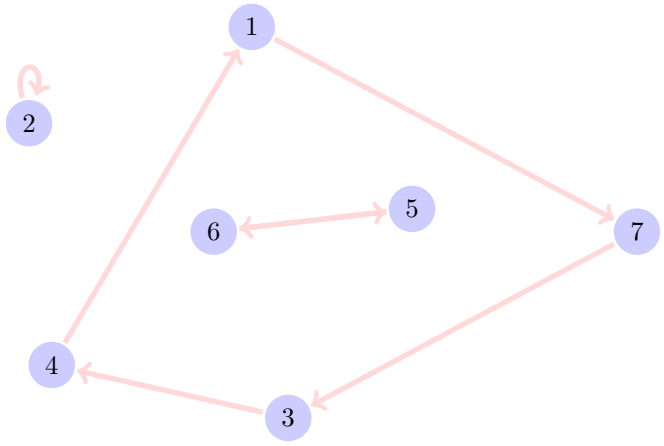
2.2.1 Cycle notation for permutations

Let $\sigma \in S_n$. Using the two-line notation style for permutations, we can write:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 4 & 1 & 6 & 5 & 3 \end{pmatrix}$$

This maps $1 \mapsto 7$, $2 \mapsto 2$, and so on. Alternatively, it can be represented with a directed graph, as in the following example:

Example 8: Given $\sigma = \{7, 2, 4, 1, 6, 5, 3\}$, the corresponding directed graph is as follows:



The above directed graph can be divided into three disjoint cycles $\sigma = (1734)(56)(2)$, or just $\sigma = (1734)(56)$.[2] More generally, we'll claim that any such permutation must produce a graph of disjoint cycles. This notation allows us to calculate inverses and powers:

- **Inverses** - $\sigma^{-1} = (4371)(65)$, which is calculated by going in the reverse direction
- **Powers** - $\sigma^2 = (13)(47)(5)(6) = (13)(47)$, where we count every other element of each cycle. To calculate σ^n, count every nth element.

Theorem 2.2.4
Let $\sigma \in S_n$. Then, draw an arrow from i to $\sigma(i)$ for each $i \in \{1, \ldots, n\}$. The resulting directed graph is a collection of disjoint cycles.

Theorem 2.2.5
In general, for $\sigma \in S_n$, $|\sigma|$ is the least common multiple of all cycle lengths in the cycle decomposition of σ.

[2] It is a convention to remove 1-element cycles from the notation, just as a convenience. The order of these cycles is not important, and σ could equivalently be written as $\sigma = (65)(3417)$, or one of many other possible combinations.

Definition 2.2.6: *Say that $\sigma \in S_n$ is an **m-cycle** if its cycle notation has just one cycle of length m (and all other cycles length 1).*

We can also use this notation to calculate products (i.e., composition) of permutations. For example, consider the case of $(154)(23) \circ (12345)$:[3] since $1 \mapsto 2$ in (12345) and then $2 \mapsto 3$ in $(154)(23)$, it must be the case that $1 \mapsto 3$ in their composition. This general principle can be applied repeatedly to calculate that

$$(154)(23) \circ (12345) = (13)(2)(4)(5) = (13)$$
$$(1734) \circ (56) = (1734)(56)$$

where in the second example, composition is nothing more than concatenation since the two permutations are non-overlapping. Such disjoint cycles always commute, but not all permutations commute. For example, $(12) \circ (13) = (132)$ but $(13) \circ (12) = (123)$.

Theorem 2.2.7
S_n is nonabelian for $n \geq 3$.

2.3 Homomorphisms and isomorphisms

2.3.1 Motivation

Consider the following groups:

1. $(\mathbb{Z}/2\mathbb{Z}, +) = \{\bar{0}, \bar{1}\}$
   - $\bar{0} + \bar{0} = \bar{0}$
   - $\bar{0} + \bar{1} = \bar{1}$
   - $\bar{1} + \bar{0} = \bar{1}$
   - $\bar{1} + \bar{1} = \bar{0}$
2. $S_2 = \{\text{id}, (12)\}$, with $\circ$:
   - $\text{id} \circ \text{id} = \text{id}$
   - $\text{id} \circ (12) = (12)$
   - $12 \circ \text{id} = (12)$
   - $(12) \circ (12) = \text{id}$
3. A group $(P, +)$ with elements $P = \{\text{even}, \text{odd}\}$, with $+$ given by:
   - even + even = even
   - even + odd = odd
   - odd + even = odd
   - odd + odd = even

Are these groups all the same? Not exactly (they have different elements), but they are all *isomorphic*. This is described formally in the next section.

[3] $\sigma \circ \tau$ means first τ, then σ

2.3.2 Formal definitions and theorems

Definition 2.3.1: *A **homomorphism** of groups $(G, *)$ and $(H, \cdot)$ is a map $\phi : G \to H$ such that for all $g, g' \in G$, $\phi(g) \cdot \phi(g') = \phi(g * g')$. Equivalently, for all $a, b, c \in G$, if $a * b = c$, then also $\phi(a) \cdot \phi(b) = \phi(c)$.*

Example 9: Given groups G and H, there is always a homomorphism

$$\begin{aligned} \phi : G &\to H \\ g &\mapsto e \text{ (identity in } h) \end{aligned}$$

Then ϕ is a homomorphism since $\phi(g_1) \cdot \phi(g_2) = \phi(g_1 g_2) = \phi(e)$.

Definition 2.3.2: *Let $(G, *)$ and $(H, \cdot)$ be groups. An **isomorphism** is a map $\phi : G \to H$ such that the following are true:*

- *ϕ is a bijection.*
- *for all $g, g' \in G$, $\phi(g) \cdot \phi(g') = \phi(g * g')$.*

In this case, we say that $G \cong H$. An isomorphism is a bijective homomorphism.

Example 10: Here are some examples of isomorphisms:

- $G \cong G$ via identity map.
- Consider the exponential function $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ bijection taking addition to multiplication: $e^{x+y} = e^x e^y$. This yields the isomorphism $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.

Theorem 2.3.3
If $G \cong H$ and G is abelian, then H is abelian.

Lemma 2.3.4
Let $\phi : G \to H$ be a homomorphism. Then $\phi(e_G) = e_H$.

Proof. Indeed, $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$. Given $x \in H$ a group, $x \cdot x = x$ if and only if x is the identity. Thus $\phi(e_G) = e_H$. □

Lemma 2.3.5
Let $\phi : G \to H$ be a homomorphism. Then for all $a \in G$, $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof. Given $a \in G$, $\phi(e_G) = \phi(a \cdot a^{-1}) = \phi(a)\phi(a^{-1}) = e_H$ by the previous lemma. Therefore, $\phi(a^{-1}) = \phi(a)^{-1}$. □

2.3.3 Homomorphisms of $\mathbb{Z}$

Let H be any group. What are the homomorphisms $\mathbb{Z} \to H$? We claim that given $b \in H$, there is a unique homomorphism $\phi : \mathbb{Z} \to H$ with $\phi(1) = b$. This means that a homomorphism $\mathbb{Z} \to H$ exists and is uniquely determined by the element it sends 1 to.

Theorem 2.3.6
Let H be any group. Then given an element $b \in H$, there exists a unique homomorphism ϕ from the additive group $(\mathbb{Z}, +)$ to H such that $\phi(1) = b$.

Proof. For uniqueness, if $\phi : \mathbb{Z} \to H$ with $\phi(1) = b$, then $\phi(1+1) = \phi(1)\phi(1) = b^2$. Continuing in this way, $\phi(1 + \cdots + 1) = \phi(1) \cdots \phi(1) = b^n$. Furthermore, $\phi(0) = e_H$ and $\phi(-1) = b^{-1}$; as before, $\phi(-n) = b^{-n}$. Thus $\phi(n) = b^n$ for all $n \in \mathbb{Z}$. For existence, we'll show that the following is a homomorphism:

$$\begin{aligned} \phi : \mathbb{Z} &\to H \\ n &\mapsto b^n \end{aligned}$$

Indeed, given $x, y \in \mathbb{Z}$, then $\phi(x)\phi(y) = b^x b^y = b^{x+y} = \phi(x + y)$ as desired. □

2.4 Subgroups

Definition 2.4.1: *Let G be a group. A subset $H \subseteq G$ is a **subgroup** of G if:*
- *$H \neq \emptyset$*
- *Given $g_1, g_2 \in H$, then $g_1 g_2 \in H$.*
- *Given $g \in H$, $g^{-1} \in H$.*

Equivalently, the operator on G restricts to an operation on H, and H is a group with respect to this. Write $H \leq G$ if this is true.

Example 11: Here are some examples of subgroups (and non-subgroups):

1. The additive group $2\mathbb{Z} = \{\ldots, -2, 0, 2, \ldots\}$ is a subgroup of $\mathbb{Z}$; this holds for any $n\mathbb{Z}$.
2. $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\} \subseteq \mathbb{Z}$ is not a subgroup since additive inverses do not exist.
3. For any group G, G and the trivial subgroup e_G are always groups.

Lemma 2.4.2: Subgroup Criterion
Given a group G, say $H \subseteq G$ for some nonempty subset H. Then H is a subgroup if for all $x, y \in H$, $xy^{-1} \in H$.

Definition 2.4.3: *Let G be a group. We define the* ***center*** *of G as*

$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$$

If G is abelian, then $Z(G) = G$ and conversely $Z(G) = G \implies G$ is abelian.

Theorem 2.4.4
The center of a group is always a subgroup, i.e., $Z(G) \leq G$ for any G.

Proof. Given $x, y \in Z(G)$, we want to show that $xy^{-1} \in Z(G)$. Namely, given $z \in G$, we want $(xy^{-1})z = z(xy^{-1})$. Indeed, since x, y commute with all members of G:

$$\begin{aligned}(xy^{-1})z &= x(y^{-1}z)\\ &= (y^{-1}z)x\\ &= (z^{-1}y)^{-1}x\\ &= (yz^{-1})^{-1}x\\ &= (zy^{-1})x\\ &= z(y^{-1}x)\\ &= z(xy^{-1})\end{aligned}$$

as desired. Hence, the center of a group is always a subgroup. □

2.5 Generators

Definition 2.5.1: *Let G be a group, and let $S \subseteq G$ be any subset. Then the subgroup* ***generated by*** *S, denoted $\langle S \rangle$, is the collection of all (finite) products[a] of elements in S and their inverses in G. If $\langle S \rangle = G$, we say S* ***generates*** *G.*

[a] We say e is the product of exactly 0 elements.

Example 12: In $\mathbb{Z}$, $\langle 1 \rangle = \mathbb{Z}$. Furthermore, $\langle 3, 4 \rangle = \mathbb{Z}$ since $4 - 3 = 1$, which has already been shown to generate $\mathbb{Z}$. However, $\langle 2 \rangle = 2\mathbb{Z}$ does not generate $\mathbb{Z}$. Notice that $\langle a, b \rangle = \mathbb{Z}$ if and only if a, b are relatively prime.

Theorem 2.5.2
The generated set $\langle S \rangle$ is a subgroup.

Theorem 2.5.3
The subgroup $\langle S \rangle$ is the smallest subgroup of G containing S.[a]

[a] That is, for any subgroup $H \leq G$ such that $S \subseteq H$, then $\langle S \rangle \subseteq H$.

Proof. Indeed, given a subgroup $H \leq G$ with $S \subseteq H$, then H must contain all products of elements in S as well as inverses. Hence, $\langle S \rangle \subseteq H$. □

2.5.1 Properties of $\mathbb{Z}$

Recall that $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is generated by a single element $\langle 1 \rangle$:

- **Well-ordering principle** - Every nonempty subset of $\mathbb{Z}_{>0}$ has a least element.
- For $a, b \in \mathbb{Z}$, say $a \mid b$ ("a divides b") if $b = ac$ for some $c \in \mathbb{Z}$.
- Given $a, b \in \mathbb{Z} - \{0\}$, there exists a unique integer $d \geq 1$ (called the **greatest common divisor**) such that:
  - $d \mid a$ and $d \mid b$
  - if $e \in \mathbb{Z}$ such that $e \mid a$ and $e \mid b$, then $e \mid d$

  We notate this as $d = \gcd(a, b) = (a, b)$.
- Given $a, b \in \mathbb{Z} - \{0\}$, there exists a unique integer $l \geq 1$ (called the **least common multiple**) such that:
  - $a \mid l$ and $b \mid l$
  - if $m \in \mathbb{Z}$ such that $a \mid m$ and $b \mid m$, then $l \mid m$

  We notate this as $l = \text{lcm}(a, b) = [a, b]$.

  Theorem 2.5.4
  Given $a, b \in \mathbb{Z}$, the product $a \cdot b = (a, b) \cdot [a, b]$.

- **Division algorithm** - Given $a, b \in \mathbb{Z} - \{0\}$, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.
- **Euclidean algorithm** - repeated use of the division algorithm can be used to compute the greatest common denominator. For example:

$$\begin{aligned} 39 &= 2(15) + 9 \\ 15 &= 1(9) + 6 \\ 9 &= 1(6) + 3 \\ 6 &= 2(3) + 0 \end{aligned}$$

  so we conclude that the greatest common denominator $(39, 15) = 3$.

Theorem 2.5.5
Given $a, b \in \mathbb{Z} - \{0\}$, compute the following steps:

$$\begin{aligned} a &= q_0 b + r_0 & 0 \le r_0 < b \\ b &= q_1 r_0 + r_1 & 0 \le r_1 \le r_0 \\ r_0 &= q_2 r_1 + r_2 & 0 \le r_2 \le r_1 \\ &\vdots & \vdots \\ r_{k-2} &= q_k r_{k-1} + r_k & 0 \le r_k \le r_{k-1} \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$

We make the following three claims about this algorithm:

1. *The algorithm terminates.*
2. *$r_k = ma + nb$ for some $m, n \in \mathbb{Z}$*
3. *$r_k = (a, b)$*

Proof. Indeed, we'll show the three claims:

1. Suppose for the sake of contradiction that the algorithm doesn't terminate. Then the sequence $r_0 > r_1 > r_2 > \cdots > 0$ has no least element, violating the well-ordering principle.
2. Working backwards along the Euclidean algorithm:

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} \\ &= r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2}) \\ &\vdots \\ &= am + bn \end{aligned}$$

   where we reach the final form by iterating substitution until the beginning of the algorithm.[a]
3. Note $r_k \mid r_{k-1}$ by the last equation. Also, $r_k \mid r_{k-2}$ by the second-to-last equation. Iterating this process, we get $r \mid a$ and $r \mid b$.
   It remains to show that if $s \in \mathbb{Z}$, $s \mid a$, and $s \mid b$, then $s \mid r$. Indeed, $s \mid a$ and $s \mid b \implies s \mid (am + bn)$ for $m, n \in \mathbb{Z}$, so $s \mid r$ by (2).

□

[a] As an aside, we can use this to write 3 as a linear combination of 39 and 15:

$$\begin{aligned} 3 &= 9 - 1(6) \\ &= 9 - 1(15 - 9) \\ &= 2(9) - 1(15) \\ &= 2(39 - 2 \cdot 15) - 1(15) \end{aligned}$$

This gives us $3 = 2 \cdot 39 - 5 \cdot 15$ as desired.

2.5.2 Cyclic groups

Definition 2.5.6: *A group G is **cyclic** if it can be generated by a single element, i.e., $G = \langle x \rangle$ for some $x \in G$. Then $G = \{x^n : n \in \mathbb{Z}\}$.*

Example 13: Here are some examples of cyclic groups (and non-cyclic groups):

- $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ is a cyclic group.
- $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ is also a cyclic group.
- $\mathbb{R}/\mathbb{Z}$ is not a cyclic group. However, a dense cover can be generated by an irrational number. That is, for example, any element in $\mathbb{R}/\mathbb{Z}$ is arbitrarily close to but not confined in $\langle \pi \rangle$.
- D_{2n} is not cyclic.
- Fix $n \geq 1$. Then $\{z \in \mathbb{C} : z^n = 1\}$ under multiplication is a cyclic group.
- There are no uncountable cyclic groups.

Lemma 2.5.7
If $H = \langle x \rangle$, then $|H| = |x|$ (i.e., if $|x| = \infty$, then $|H| = \infty$)

Proof. First, consider the case that $|x| = n$ is finite. Then we claim that

$$H = \{1, x, \ldots, x^{n-1}\}$$

and these are all distinct. If instead $x^a = x^b$ for some $0 \leq a < b < n$, then $1 = x^{b-a}$, contradicting $|x| = n$. To show that H does indeed equal this set,[a] we need to show that $H \supseteq \{1, x, \ldots, x^{n-1}\}$ (the reverse direction is by definition). Indeed, given $x^t \in H$ for some $t \in \mathbb{Z}$, then by the division algorithm $t = qn + r$ for some $0 \leq r < n$. Then:

$$x^t = x^{qn+r} = x^{nq}x^r \in \{1, \ldots, x^n\}$$

Now, suppose $|x|$ infinite. Then, we'll claim $\{\ldots, x^{-1}, 1, x, x^2, \ldots\}$ are all distinct. Indeed, if $x^a = x^b$ for $a < b$, then $x^{b-a} = 1$ is a contradiction. □

[a] In general, to show that any two sets A and E are equal, it is standard to show that $A \subseteq E$ and $E \subseteq A$.

Lemma 2.5.8
Let G be any group, and $x \in G$. If $x^m = 1$ and $x^n = 1$, then $x^{(m,n)} = 1$.

Proof. Let $d = (m, n)$. Note that $d = am + bn$ for $a, b \in \mathbb{Z}$. Then $x^d = x^{am}x^{bn} = 1$. □

Lemma 2.5.9
If $x^m = 1$, then $(|x|) \mid m$.

Proof. Let $n = |x|$. We want to show that $n \mid m$. If $m = 0$, then indeed $n \mid m$. Otherwise, let $d = (m, n)$. Then by the previous lemma, $x^d = 1$ so $d \geq n$; hence $d = n$. □

Theorem 2.5.10
Let $G = \langle x \rangle = \{x^k : k \in \mathbb{Z}\}$. Then the following are true:

1. *Let $|G| = n$. Then the map*

$$\begin{aligned} \varphi : G &\to \mathbb{Z}/n\mathbb{Z} \\ x^k &\mapsto \bar{k} \end{aligned}$$

   is well-defined and an isomorphism.
2. *Let $|G| = \infty$. Then the map*

$$\begin{aligned} \varphi : G &\to \mathbb{Z} \\ x^k &\mapsto k \end{aligned}$$

   is well-defined and an isomorphism.

This is equivalent to saying that every cyclic group is isomorphic to $\mathbb{Z}$ or some $\mathbb{Z}/n\mathbb{Z}$.

Proof. We'll show this in two cases:

1. ($|G| = n$) To show well-definedness, if $x^r = x^s$ then $n \mid r - s$ by the lemma. Then $\varphi(x^r) = \varphi(x^s) = \bar{r} = \bar{s}$. Further, this is a surjection of sets of order n, and therefore a bijection. To show it's a homomorphism:

$$\begin{aligned} \varphi(x^k \cdot x^l) &= \varphi(x^{k+l}) \\ &= \overline{k + l} \\ &= \bar{k} + \bar{l} \\ &= \varphi(x^k) \cdot \varphi(x^l) \end{aligned}$$

   as desired. Hence this is a bijective homomorphism, which is an isomorphism.
2. ($|G| = \infty$) Omitted.

□