

# MATH 1530: ABSTRACT ALGEBRA

SPRING 2017

---

## Notes for Abstract Algebra

---

NICHOLAS TOMLIN

### Contents

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Introduction</b>  | <b>2</b> |
| 1.1      | Preliminary definitions . . . . .                                    | 2        |
| 1.2      | What is a group? . . . . .   | 3        |
| 1.3      | The group $\mathbb{Z}/n\mathbb{Z}$ . . . . .                         | 4        |
| 1.3.1    | The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ . . . . . | 6        |
| 1.3.2    | Applications of arithmetic in $\mathbb{Z}/n\mathbb{Z}$ . . . . .     | 6        |
| 1.4      | Some general theorems about groups . . . . .                         | 7        |
| 1.5      | The order of a group . . . . .                                       | 7        |
| 1.6      | A brief interlude on functions . . . . .                             | 8        |
| <b>2</b> | <b>Some important groups</b>   | <b>8</b> |
| 2.1      | Dihedral groups . . . . .  | 8        |
| 2.1.1    | Explicit description of $D_{2n}$ . . . . .                           | 9        |
| 2.2      | Symmetric groups . . . . .   | 10       |

# 1 Introduction

## 1.1 Preliminary definitions

**Definition 1.1.1:** A **set** is “a collection of elements,” e.g., the integers  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ , the real numbers  $\mathbb{R}$ , and the rational numbers  $\mathbb{Q}$  (fractions). Note that we use  $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\}$  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  $A_1, \dots, A_n$  are sets, then

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

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

**Definition 1.1.3:** A **function**  $f : A \rightarrow B$ , 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  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  be given by  $x \mapsto 2x$ .<sup>1</sup> 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  $* : G \times G \rightarrow G$ . For example, integer addition  $(+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z})$  is a binary operation.

<sup>1</sup>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  $*$  :  $G \times G \rightarrow G$  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.<sup>a</sup>

<sup>a</sup>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,  $0 \in \mathbb{Z}$  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.  $\square$

**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

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

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  $f : A \rightarrow D$  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  $D = \{\text{Jan 1}, \dots, \text{Dec 31}\}$  be the set of possible birthdays, and  $f : A \rightarrow D$  be a function mapping students to their birthdays.

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

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

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

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

**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  $\bar{a}_1 = \bar{a}_2$  and  $b_1, b_2 \in \mathbb{Z}$  such that  $\bar{b}_1 = \bar{b}_2$ , 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

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

by associativity of addition.

(2) We have  $\bar{0} + \bar{a} = \bar{a} + \bar{0} = \bar{a}$  for all  $a \in \mathbb{Z}/n\mathbb{Z}$ .

(3) We have  $-\bar{a} + \bar{a} = \bar{a} + (-\bar{a}) = \bar{0}$  for all  $a \in \mathbb{Z}/n\mathbb{Z}$ . □

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

**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  $(\mathbb{Z}/n\mathbb{Z})^\times$ .  $\square$

#### 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  $\bar{2}^5 = \bar{2}$ :

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

## 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:

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

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

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

### 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:

$$e = a * b \text{ (since } b \text{ inverse of } a)$$

$$c * e = c * a * b$$

$$c = b \text{ (since } c \text{ inverse of } a)$$

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

### 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.  $\square$

### Lemma 1.4.4

Let  $(G, *)$  be a group. For any  $a_1, \dots, a_n \in G$ ,  $a_1 * \dots * a_n$  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  $180^\circ$  has order 2, a rotation by  $120^\circ$  has order 3, and so on. In fact, for any order  $n \in \mathbb{Q}$ , a rotation by  $(\frac{360}{n})^\circ$  has order  $n$ .

## 1.6 A brief interlude on functions

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

<sup>a</sup>The contrapositive,  $a \neq b \implies f(a) \neq f(b)$  is equivalent.

**Definition 1.6.2:** Let  $f : A \rightarrow C$  be a function on sets. The  $f$  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  $f : A \rightarrow C$  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  $\{1, \dots, n\}$  in clockwise order. A rigid motion of the  $n$ -gon can be recorded as a bijection

$$\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

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

$$D_{2n} \rightarrow \{\text{bijections from } \{1, \dots, n\} \rightarrow \{1, \dots, n\}\}$$

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

### 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:

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

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,  $|D_{2n}| \leq 2n$ .  $\square$

#### 2.1.1 Explicit description of $D_{2n}$

Label an  $n$ -gon  $\{1, \dots, n\}$  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:

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

### Theorem 2.1.3

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

*Proof.* We need only show that

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

Indeed,  $r^{i-j} \neq s$ .  $\square$

- $rs = sr^{-1}$ , i.e., rotating and reflecting is the same as reflecting and rotation backwards.

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:

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

Furthermore, 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  $X = [n] := \{1, \dots, n\}$ , we write  $S_n = S_{\{1, \dots, n\}}$ . 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  $f : A \rightarrow C$  is a bijection if and only if there exists a function  $g : C \rightarrow A$  such that  $f \circ g = \text{id}_C$  and  $g \circ f = \text{id}_A$ .