

# MATH H333 (Algebra I) Lecture Notes

GUILHERME ZEUS DANTAS E MOURA  
gdantasemo@haverford.edu

Haverford College  
Fall 2020  
Last updated: October 6, 2020

This is Haverford College's undergraduate MATH H333, instructed by Tarik Aougab. All errors are my responsibility.

Use these notes only as a guide. There is a non-trivial chance that some things here are wrong or incomplete (especially proofs).

This class is being taught remotely via Zoom.

## Contents

<b>1</b>	<b>Binary Operations (September 09, 2020)</b>	<b>2</b>
1.1	Why Algebra? . . . . .	2
1.2	Places where Algebra arises in Mathematics . . . . .	2
1.3	Binary Operations . . . . .	2
<b>2</b>	<b>Groups (September 11, 2020)</b>	<b>3</b>
2.1	Defining Groups . . . . .	3
<b>3</b>	<b>Subgroups (September 14, 2020)</b>	<b>4</b>
<b>4</b>	<b>Integers (September 16, 2020)</b>	<b>5</b>
<b>5</b>	<b>Cyclic Groups (September 18, 2020)</b>	<b>6</b>
<b>6</b>	<b>Isomorphisms (September 21, 2020)</b>	<b>8</b>
<b>7</b>	<b>Cosets (September 23, 2020)</b>	<b>9</b>
<b>8</b>	<b>Coset Properties (September 25, 2020)</b>	<b>10</b>
<b>9</b>	<b>Normal Subgroups (September 28, 2020)</b>	<b>11</b>
<b>10</b>	<b>Example of Quotients (September 30, 2020)</b>	<b>12</b>
<b>11</b>	<b>Quotient Groups (October 02, 2020)</b>	<b>13</b>
<b>12</b>	<b>First Isomorphism Theorem (October 05, 2020)</b>	<b>14</b>

# 1 Binary Operations (September 09, 2020)

## 1.1 Why Algebra?

Algebra is the study of symmetry. An object has a symmetry when we can do something to it (transform it in some way) and without changing its appearance.

**Example 1.1.** A circle has a rotational symmetry: if we rotate the circle about its center, we get the same circle.

**Example 1.2.** The algebraic equation  $x^2 + y^2 + z^2 - 3xyz = 0$  has a symmetry: for example, we can change the roles of  $x$  and  $z$ , which gives us the same equation.

Symmetry appears all over Mathematics, so Algebra is a prevalent topic abroad Mathematics.

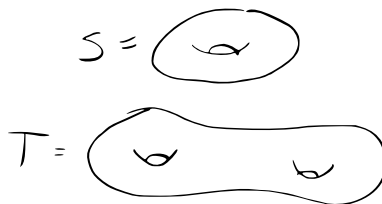
## 1.2 Places where Algebra arises in Mathematics

**Number Theory.** The following theorem will be proven in this course.

**Theorem 1.1 (Fermat's Little Theorem).** Let  $p$  be a prime integer number. Let  $a$  be a positive integer number. Then,  $a^p - a$  is a multiple of  $p$ .

**Topology.**

**Theorem 1.2.** There is no continuous bijection  $f : S \rightarrow T$ .



*Sketch.* Associate a “group” to  $S$  and another to  $T$ . A continuous bijection would send the  $S$ -group perfectly to the  $T$ -group. But the two groups are different.

## 1.3 Binary Operations

**Definition 1.1.** If  $S$  is a set, then a *binary operation* on  $S$  is a function  $f : S \times S \rightarrow S$ . Here,  $S \times S = \{(a, b) \mid a, b \in S\}$ .

**Example 1.3.** If  $S = \mathbb{R}$ , then  $f(a, b) = a + b$  and  $g(a, b) = a \cdot b$  are binary operations.

**Example 1.4.** If  $S = \mathbb{N}$ , then  $h(a, b) = a - b$  is not a binary operation.

**Definition 1.2.** A binary operation  $f : S \times S \rightarrow S$  is *associative* if, for all  $a, b, c \in S$ ,

$$f(f(a, b), c) = f(a, f(b, c)).$$

**Example 1.5.** If  $S = \mathcal{M}_n(\mathbb{R})$ , then  $f(A, B) = AB$  is an associative binary operation.

**Example 1.6.** If  $S = \mathbb{R}$ , then  $f(a, b) = a - b$  is a non-associative binary operation.

A key concept in Algebra is *transformation*.

**Example 1.7.** Let  $S$  be a non-empty set. Define  $g(S) = \{T : S \rightarrow S\}$ . Then, composition is an associative binary operation on  $g(S)$ , i.e.,  $f(T_1, T_2) = T_1 \circ T_2$  is an associative binary operation on  $g(S)$ .

## 2 Groups (September 11, 2020)

In the last class, we focused on binary (associative) operations.

### 2.1 Defining Groups

**Definition 2.1 (Notation).** If  $a, b \in S$ , then  $ab$  or  $a \cdot b$  will commonly be used to denote  $f(a, b)$ . We will also commonly call this operation a *product*.

Associativity allows us to be less careful when writing down long products.

**Example 2.1.** In general,  $a_1a_2a_3a_4a_5a_6a_7$  has no meaning. However, if the binary operation is associative, no matter in which order we do the product, there will be no ambiguity about what value the expression have.

**Definition 2.2.** A binary operation on  $S$  is called *commutative* if for all  $a, b \in S$ ,  $ab = ba$  holds.

**Example 2.2.**

- (i)  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, \cdot)$  have commutative binary operations.
- (ii)  $(\mathcal{M}_n(\mathbb{R}), \text{matrix multiplication})$  has a non-commutative operation.
- (iii)  $(\mathbb{R}, \text{distance})$ , i.e.,  $f(a, b) = |a - b|$ , has a commutative, but non-associative operation.

**Definition 2.3.** Given  $S$  equipped with a binary operation, we say  $(S, \cdot)$ , has an identity element if there exists  $e \in S$  such that, for all  $a \in S$ ,  $a \cdot e = e \cdot a = a$  holds.

**Example 2.3.**

- (i)  $(\mathbb{R}, +)$  has 0 as an identity.
- (ii)  $(\mathbb{R}, \cdot)$  has 1 as an identity.
- (iii)  $(\mathcal{M}_n(\mathbb{R}), \text{matrix multiplication})$  has  $I_n$  as an identity.

**Definition 2.4.** An element  $a$  of  $(S, \cdot)$ , that has an identity element (which we are going to call  $e$ ), is called invertible if there exists  $b \in S$  so that  $ab = ba = e$ .

**Example 2.4.**

- (i) Every element of  $(\mathbb{R}, +)$  is invertible.
- (ii) Every element, except 0, of  $(\mathbb{R}, \cdot)$  is invertible.
- (iii) Some elements, but not all, of  $\mathcal{M}_n(\mathbb{R})$ , equipped with matrix multiplication, are invertible.

**Definition 2.5.** A *group* is a set  $(G, \cdot)$  with a binary operation so that:

- (i) The binary operation is associative.
  - (ii) There exists an identity element in  $G$ .
  - (iii) Every element in  $G$  is invertible.
- If  $\cdot$  is commutative,  $G$  is called an *abelian group*.

**Example 2.5.**

- (i)  $(\mathbb{R}, +)$  is a group.
- (ii)  $(\mathbb{C}, +)$  is a group.
- (iii)  $(\mathbb{Z}, +)$  is a group.
- (iv)  $(\mathbb{R} \setminus \{0\}, \cdot)$  is a group.
- (v)  $(\mathbb{C} \setminus \{0\}, \cdot)$  is a group.
- (vi)  $(\mathbb{Z} \setminus \{0\}, \cdot)$  is not a group, because 2 does not have an inverse element.
  - However,  $(\mathbb{Q} \setminus \{0\}, \cdot)$  is a group.
- (vii)  $\mathcal{M}_n(\mathbb{R})$ , equipped with matrix multiplication is not a group, because the zero matrix does not have an inverse element.
  - However, if we define  $GL_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) : A \text{ is invertible}\}$ , then  $GL_n(\mathbb{R})$ , equipped with matrix multiplication is a group.\*
- (viii) Define  $D_8 = \{\text{affine bijections } T : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \text{ such that } T(\mathcal{S}) = \mathcal{S}\}$ , where  $\mathcal{S} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ , also known as the standard unit square.

---

\*It is important to prove that matrix multiplication is closed under  $GL_n(\mathbb{R})$ . In addition, this is the first example of a non-abelian group.

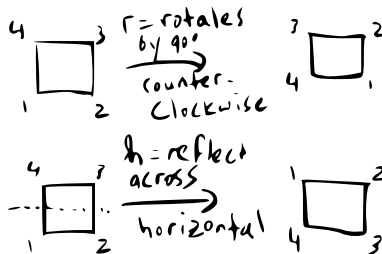
### 3 Subgroups (September 14, 2020)

Let's look more closely to  $D_8 = \{\text{affine bijections } T : \mathbb{R} \rightarrow \mathbb{R} \text{ such that } T(\mathcal{S}) = \mathcal{S}\}$ .

**Proposition 3.1.**  $D_8$  is a group. The order of the group  $D_8$  is 8.

**Proposition 3.2.** Let  $r, h \in D_8$  be described as follows:

- (i)  $r$  denotes the rotation of  $\mathcal{S}$  by  $90^\circ$ , counter-clockwise.
- (ii)  $h$  denotes the reflect across the horizontal perpendicular bisector.



If  $\phi \in D_8$ , then  $\phi$  can be expressed as  $\phi = \phi_n \circ \phi_{n-1} \circ \cdots \circ \phi_1$ , where  $\phi_i = h$  or  $\phi_i = r$ , for all  $i$ .

The proposition above should resemble the concept of basis in Linear Algebra. In some sense,  $h$  and  $r$  generate the group  $D_8$ .

**Example 3.1.** Let  $d$  be the reflection through the diagonal line through  $(0,0)$  and  $(1,1)$ . We have  $d = h \circ r \circ r \circ r = hr^3$ .



**Example 3.2.** Let  $v$  be the reflection through the vertical perpendicular bisector. We have  $v = hr^2$ .

Note that  $h^2 = r^4 = e$ , and  $2 \cdot 4 = 8$ , which is the number of elements in  $D_8$ . What a coincidence, isn't it?

**Definition 3.1.** A *subgroup*  $H$  of a group  $(G, \cdot)$  is a subset of  $G$  that is a group itself, with respect to the same operation  $\cdot$ .

**Example 3.3.**

- (i) If  $G$  is a group, it has an identity, say  $e$ . Then  $\{e\}$  is a subgroup of  $G$ .
- (ii)  $G$  is always a subgroup of  $G$ .

**Lemma 3.1.** Given a a group  $G$ , a non-empty subset  $H \subset G$  is a subgroup of  $G$  if, and only if, both following conditions are met:

- (i)  $ab \in H$ , for all  $a, b \in H$ .
- (ii)  $a^{-1} \in H$ , for all  $a \in H$ .

**Example 3.4.**  $2\mathbb{Z} = \{\text{even integers}\}$  is a subgroup of  $(\mathbb{Z}, +)$ .

**Definition 3.2 (Symmetric group on  $n$  elements).** Given  $n \in \mathbb{N}$ , define  $S_n = \{\text{bijections } \tau : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}\}$ , equipped with composition.

**Example 3.5.** Let  $n = 5$ , then consider  $\tau : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$ . Then  $\tau \in S_5$ .

Alternatively, we can use the following notation for  $\tau = (13)(24)(5)$ , which is called *cycle notation*.

**Example 3.6.** Consider  $\tau' : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ . We can write  $\tau' = (124)(35)$ , using cycle notation.

**Example 3.7.** Consider  $\tau'' : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ . We can write  $\tau'' = (12345)$ , using cycle notation.

*Remark.* Cycle notation is “not unique”, e.g.,  $(12345) = (34512)$ .

## 4 Integers (September 16, 2020)

**Proposition 4.1.**  $S_n$  is a finite group, and  $|S_n| = n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$ .

*Proof.* An arbitrary element  $\tau \in S_n$  is described by determining  $\tau(1), \tau(2), \dots, \tau(n)$ . We have  $n$  choices for  $\tau(1)$ ; after that, we have  $n-1$  choices for  $\tau(2)$ ;  $\dots$ ; after that, we have 1 choice for  $\tau(n)$ .  $\square$

**Example 4.1.** Suppose  $q, p \in S_5$ ,  $q = (14325)$  and  $p = (15)(34)$ . Determine  $qp$  in cycle notation.

*Answer (Cheat).*  $qp = (14325)(15)(34)$ .

*Answer (More useful).*  $qp = (425)$ .

**Definition 4.1.** Given  $\tau \in S_n$ , define  $M_\tau$  as a  $n \times n$  matrix obtained by permuting the rows of  $I_n$  in accordance with  $\tau$ .

**Example 4.2.** If  $\tau \in S_4$ ,  $\tau = (134)$ , then

$$M_\tau = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$\text{Given } \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \text{ we have } M_\tau \vec{x} = \begin{pmatrix} x_4 \\ x_2 \\ x_1 \\ x_3 \end{pmatrix}.$$

$$\textbf{Theorem 4.1.} \text{ Given } \tau \in S_n, \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \text{ then } M_\tau \vec{x} = \begin{pmatrix} x_{\tau^{-1}(1)} \\ x_{\tau^{-1}(2)} \\ \vdots \\ x_{\tau^{-1}(n)} \end{pmatrix}.$$

**Theorem 4.2.**  $\det(M_\tau) = \pm 1$ .

**Theorem 4.3.** Given  $p, q \in S_n$ , then  $M_{pq} = M_p M_q$ .

**Definition 4.2.** The *sign* of  $\tau \in S_n$  is either  $\pm 1$ , and it is just  $\det(M_\tau)$ .

**Problem 4.1.** If  $G = (\mathbb{Z}, +)$ , what are all subgroups of  $G$ ?

*Solution.* Let  $H$  be a subgroup of  $G$ .  $0 \in H$ , because 0 is the identity element.

If  $H = \{0\}$ , we have a group – note that  $H = 0\mathbb{Z}$ . Otherwise,  $H$  has an element distinct from 0. Since  $a \in H \iff -a \in H$ , then there is a positive integer in  $H$ .

Let  $h$  be the smallest positive integer in  $H$ . Since addition is a binary operation in  $H$ , we have  $h\mathbb{Z} \subset H$ .

Suppose  $H \neq h\mathbb{Z}$ . Therefore, there is an element  $x \in H$ , such that  $x \notin h\mathbb{Z}$ . Therefore, by Euclid's Algorithm, there is an integer  $q$  such that  $nh < x < (n+1)h$ ; namely,  $q$  the quotient of  $x$  when evenly divided by  $h$ . Therefore,  $0 < x - qh < h$ .

However,  $qh, x \in H$  implies that  $x - qh \in H$ . This is a contradiction, because we have found a positive integer smaller than  $h$  (the smallest positive element of  $H$ ), which is also an element of  $H$ .

Therefore,  $H = h\mathbb{Z}$ , with  $h \in \mathbb{Z}_{\geq 0}$ , are all the subgroups of  $G$ .

Let us see some applications of Problem 4.1.

Given  $a, b \in \mathbb{Z}$ , consider  $S = a\mathbb{Z} + b\mathbb{Z} = \{n \in \mathbb{Z} : n = ra + sb, r, s \in \mathbb{Z}\}$ . Verify that  $S$  is a subgroup of  $\mathbb{Z}$ . Using Problem 4.1, we have that  $S = d\mathbb{Z}$ , for some integer  $d$ .

## 5 Cyclic Groups (September 18, 2020)

Recall that every subgroup  $S$  of  $(\mathbb{Z}, +)$  is of the form  $d\mathbb{Z}$ , for some integer  $d$ .

Also, if  $a, b$  are integers, we can consider  $S = a\mathbb{Z} + b\mathbb{Z}$ , which is a subgroup of  $\mathbb{Z}$ . Therefore,  $S\mathbb{Z} = d\mathbb{Z}$  for some integer  $d$ .

Since  $a, b \in S = a\mathbb{Z} + b\mathbb{Z}$ , then  $a, b \in d\mathbb{Z}$ , which means that  $d$  is a divisor of both  $a, b$ .

Now, let  $n \in \mathbb{Z}$  such that  $n$  divides both  $a$  and  $b$ . Thus,  $n$  divides any number of the form  $sa + rb$ . But,  $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ , which means  $d = ra + bs$ , for right choices of  $r$  and  $s$ . Therefore,  $n$  divides  $d$ .

**Definition 5.1.** For  $a, b \in \mathbb{Z}$ , we define  $d$  as above as the *greatest common divisor* of  $a$  and  $b$ , which we denote by  $\gcd(a, b)$ .

We have shown not only that  $d$  is the greatest common divisor of  $a$  and  $b$ , but also that any other common divisor of  $a$  and  $b$  divides  $d$ .

**Algorithm 5.1 (Euclidean Algorithm).**

**Example 5.1.** Let  $a = 314$  and  $b = 136$ . We divide 314 by 136 and get  $314 = 2 \cdot 136 + 42$ . Thus,

$$\begin{aligned} n \in 314\mathbb{Z} + 136\mathbb{Z} &\iff n = r \cdot 314 + s \cdot 136 \\ &\iff n = r \cdot (2 \cdot 136 + 402) + s \cdot 136 \\ &\iff n = r \cdot (2r + s) \cdot 136 + r \cdot 42 \\ &\iff n \in 136\mathbb{Z} + 42\mathbb{Z}. \end{aligned}$$

Therefore,  $\gcd(314, 136) = \gcd(136, 42)$ . We can further use

**Definition 5.2.** Given  $a, b \in \mathbb{Z}$ ,  $a, b \neq 0$ , then  $a$  and  $b$  are relatively prime if, and only if,  $\gcd(a, b) = 1$ .

**Proposition 5.1.** The  $\gcd(a, b)$  is the product of the prime powers common to prime factorizations of  $a$  and  $b$ .

**Example 5.2.** Let  $a = 52 = 2^2 \cdot 13$ , and  $b = 2^3 \cdot 3$ . Therefore,  $\gcd(52, 24) = 2^2$ .

**Corollary 5.1.** If  $a$  and  $b$  are relatively prime if, and only if, there are integers  $r$  and  $s$  such that  $ra + sb = 1$ .

**Corollary 5.2.** Suppose  $p$  is a prime. Then, given  $a, b \in \mathbb{Z}$ , if  $p$  divides  $ab$ , therefore  $p$  divides  $a$  or  $p$  divides  $b$ .

*Proof.* If  $p$  divides  $a$ , we are done.

Suppose that  $p$  does not divide  $a$ . Thus,  $\gcd(p, a) = 1$ . It implies that

$$1 = rp + sa,$$

for some integers  $r$  and  $s$ . If we multiply both sides by  $b$ , we have

$$b = rbp + sab.$$

Notice that  $p$  divides both  $rbp$  and  $sab$ , therefore,  $p$  divides their sum, which is  $b$ . □

**Theorem 5.1.** Let  $G = (G, \cdot)$  be a group, let  $I$  be a set, and let  $\{H_i\}_{i \in I}$  be a family of subgroups of  $G$  indexed by  $I$ . Then, the set

$$\bigcap_{i \in I} H_i$$

is a group.

*Proof.* We want to show:

(i)  $\bigcap_{i \in I} H_i \neq \emptyset$ .

For this item,  $e \in \bigcap_{i \in I} H_i$ .

(ii)  $a, b \in \bigcap_{i \in I} H_i \implies ab \in \bigcap_{i \in I} H_i$ .

For this item,  $a, b \in H_i$ , for all  $i \in I$ , which implies  $ab \in H_i$  for all  $i$

□

Back to  $(\mathbb{Z}, +)$ . Given  $a, b \in \mathbb{Z}$ , let  $S = a\mathbb{Z} \cap b\mathbb{Z}$ . By the last theorem,  $S$  is a subgroup. By Wednesday's theorem,  $S = a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$ , for some  $m \in \mathbb{Z}$ . Since  $m \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ ,  $m$  is a multiple of  $a$  and  $b$ .

Now, for any number  $n$  that is multiple of both  $a$  and  $b \implies n \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \implies n$  is a multiple of  $m$ .

**Definition 5.3.** The  $m$  described above is called the *lowest common multiple* of  $a$  and  $b$ , denoted by  $\text{lcm}(a, b)$ .

We have proved above only that  $m$  is the lowest common multiple, but also that  $m$  divides every common multiple of  $a$  and  $b$ .

**Definition 5.4.** Let  $(G, \cdot)$  be a group and  $x \in G$ . Then the cyclic subgroup generated by  $x$ , denoted by  $\langle x \rangle$ , is all powers of  $x$ , i.e.,

$$\langle x \rangle = \{\dots, x^{-1}, e, x^1, x^2, \dots\}.$$

**Theorem 5.2.** In  $G$ , let  $\Gamma(x) = \{H \subseteq G : H \text{ is a subgroup of } G \text{ and } x \in H\}$ . Then

$$\bigcap_{H \in \Gamma(x)} H = \langle x \rangle.$$

## 6 Isomorphisms (September 21, 2020)

This class happened during IMO. The lecture notes are to do.



## 7 Cosets (September 23, 2020)

This class happened during IMO. The lecture notes are to do.

## 8 Coset Properties (September 25, 2020)

**Definition 8.1 (Equivalence Relation).** An *equivalence relation* is a relation on a set  $S$ , i.e., a way to say that certain pairs of elements can be in relationship to one another; so long as the pair satisfies whatever rules we choose for that relationship, AND our rules need to satisfy these properties.

- (i)  $x \sim x$ ;
- (ii) if  $x \sim y$ , then  $y \sim x$ ;
- (iii) if  $x \sim y$  and  $y \sim z$ , then  $x \sim z$ .

*Remark.* If a pair  $(x, y)$  satisfy our rules, we write  $x \sim y$ , “ $x$  is equivalent to  $y$ ”.

**Definition 8.2 (Equivalence Class).** Given a set  $S$ ,  $s \in S$ , and an equivalence relation  $\sim$ , the *equivalence class of  $x$* , denoted  $[x]$ , is  $[x] = \{y \in S : x \sim y\}$ .

**Example 8.1.** Let  $S = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ , and we will say that  $(a, b) \sim (c, d) \iff ad = bc$ . Let us check if the three properties are ensured:

- (i)  $(a, b) \sim (a, b)$ , because  $ab = ba$ ;
  - (ii)  $(a, b) \sim (c, d) \iff ad = bc \iff cb = da \iff (c, d) \sim (a, b)$ ;
  - (iii) If  $(a, b) \sim (c, d)$  and  $(c, d) \sim (r, s)$ . Then,  $ad = bc$  and  $cs = dr$ . Therefore,  $adcs = bcd r$ , which means that  $as = br$  (since  $c \neq 0 \neq d$ ). In other words,  $(a, b) \sim (r, r)$ .
- In this case,  $[(a, b)] = \{(c, d) \in S : ad = bc\}$ .

**Theorem 8.1.** If  $S$  is a set, with an equivalence relation  $\sim$ , then the equivalence classes of  $\sim$  *disjointly partition*  $S$ , i.e., every element of  $S$  is contained in **exactly** one equivalence class.

Given  $S$ , equipped with an equivalence class  $\sim$  on  $S$ , we define  $\bar{S} = \{[x] : x \in S\}$ , i.e., the set of equivalence classes.

In this situation, there exists a map  $\pi : S \rightarrow \bar{S}$ , defined by  $x \mapsto [x]$ .

**Example 8.2.** Let  $S = \mathbb{Z}$ , and  $a \sim b \iff a - b$  is a multiple of 5. (You should verify that this is an equivalence relation.)

Then  $\bar{S} = \{[0], [1], [2], [3], [4]\}$ . E.g.,  $\pi(7) = [2]$ .

**Definition 8.3.** Let  $H \leq G$  be groups, and  $a \in G$ . Then, *the right coset of  $H$  with respect to  $a$  is*

$$Ha = \{g \in G : \exists h \in H \text{ such that } ha = g\} = \{ha : h \in H\}.$$

**Lemma 8.1.**

$$Ha = Hb \iff ab^{-1} \in H$$

**Lemma 8.2.** Given  $H \leq G$  groups, the relation defined by  $a \sim b \iff ab^{-1} \in H$  is an equivalence relation.

*So, what are the equivalence classes of this equivalence relation?* They are exactly the right cosets of  $H$ , i.e,  $[a] = Ha$ .

Therefore, right cosets, if distinct, share no elements in common.

On Monday, we'll prove the following theorem.

**Theorem 8.2 (Lagrange's Theorem).** If  $G$  is a finite group and  $H$  is a subgroup of  $G$ , then  $|H|$  divides  $|G|$ .

## 9 Normal Subgroups (September 28, 2020)

**Lemma 9.1.** Given  $H \leq G$ , if  $|G| < \infty$ , then given  $a, b \in G$ , it holds  $\#(Ha) = \#(Hb)$ .

*Proof.* Note that  $H$  is a right coset ( $H = He$ ). So, suffices to show that for all  $a \in G$ ,  $\#(Ha) = |H|$ . Define a function  $\varphi : H \rightarrow Ha$ , defined by  $h \mapsto ha$ . We shall prove that  $\varphi$  is a bijection.

Let's show that  $\varphi$  is onto. Given  $g \in Ha$ , then  $g = ha$  for some  $h \in H$ . But  $\varphi(h) = ha = g$ , which means that  $g \in \text{Im}(\varphi)$ .

Let's show that  $\varphi$  is one-to-one. If  $\varphi(h_1) = \varphi(h_2) \implies h_1a = h_2a \implies h_1aa^{-1} = h_2aa^{-1} \implies a =$   
Therefore  $\varphi$  is a bijection, which implies that  $\#(Ha) = |H|$ , and we're done!  $\square$

**Theorem 9.1 (Lagrange's Theorem).** If  $H \leq G$  are finite groups, then  $|H|$  divides  $|G|$ .

*Proof.* The right cosets of  $H$  partitionate  $G$ , i.e., they are disjoint and their union is  $G$ ; and they all have the same number of elements. Let  $[G : H]$  denote the number of right cosets of  $H$  sitting inside  $G$ , which is called index of  $H$  in  $G$ . Therefore,

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

$\square$

**Corollary 9.1.** Given a group  $G$  and  $a \in G$ , if  $|G| < \infty$ , then  $\text{order}(a)$  divides  $|G|$ .

*Proof.* Consider  $\langle a \rangle \leq G$ , then, by Lagrange's Theorem,  $|\langle a \rangle| = \text{order}(a)$  divides  $|G|$   $\square$

**Definition 9.1.** A subgroup  $H$  of  $G$  is called *normal*, denoted by  $H \triangleleft G$  if, for all  $g \in G$ , the image of  $H$  under the  $g$ -conjugation isomorphism (the  $g$ -conjugation isomorphism is the map  $\phi_g : G \rightarrow G$  defined by  $a \mapsto gag^{-1}$ ) is contained in  $H$ , i.e,  $\phi_g(H) \subset H$ , for all  $g \in G$ .

**Lemma 9.2.** If  $G$  and  $G'$  are subgroups,  $\phi : G \rightarrow G'$  a homomorphism, then  $\text{Ker}\phi \triangleleft G$ .

**Example 9.1.**  $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ .

Use Lemma 9.2 with  $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ .

**Example 9.2.**  $\langle (1\ 2) \rangle \not\triangleleft G$ , because  $\phi_{(2\ 3)}(\langle (1\ 2) \rangle) = \{e, (1\ 3)\} \not\subset H$

**Theorem 9.2.** The following are equivalent:

- (i)  $H \triangleleft G$ ;
- (ii)  $gHg^{-1} = H$ , for any  $g \in G$ ;
- (iii)  $gH = Hg$ , for any  $g \in G$ ;
- (iv) Every left coset of  $H$  is a right coset of  $H$ .

## 10 Example of Quotients (September 30, 2020)

From last time, we discussed the following theorem:

**Theorem 10.1.** The following are equivalent:

- (i)  $H \triangleleft G$ ;
- (ii)  $gHg^{-1} = H$ , for any  $g \in G$ ;
- (iii)  $gH = Hg$ , for any  $g \in G$ ;
- (iv) Every left coset of  $H$  is a right coset of  $H$ .

*Proof (i  $\implies$  ii).*  $H \triangleleft G \implies \phi_g(H) \in H \implies gHg^{-1} \subset H$ . Analogously,  $g^{-1}Hg \subset H$ . This last one implies that  $H \subset gHg^{-1}$ .

Therefore,  $gHg^{-1} = H$ . □

*Proof (ii  $\iff$  iii).*  $gHg^{-1} = H \iff gH = Hg$ . □

*Proof (iii  $\implies$  iv).* If  $gH = Hg$ , then  $gH$  is a right coset. □

*Proof (iv  $\implies$  iii).* Assume that, given  $aH$ , then there is  $b$  such that  $aH = Hb$ . Note that  $gH$  shares an element (namely,  $g$ ) with  $Hg$ . Since  $gH$  is a left coset, then  $gH = Hb$  for some  $b$ .

Since  $g \in gH = Hb$ , then  $Hb$  intersects with  $Hg$ , then  $Hb = Hg$  (because, if two left cosets share an element, then they are equal). □

*Proof (ii  $\implies$  i).*  $gHg^{-1} = \phi_g(H) = H$ , then  $\phi_g \subset H$ , which implies  $H \triangleleft G$ . □

Recall from Linear Algebra:

**Theorem 10.2.** Let  $T : V \rightarrow W$  a linear map, then

$$\dim V = \dim \ker T + \dim \operatorname{Im} T.$$

If  $T$  is onto, then

$$\dim V = \dim \ker T + \dim W.$$

The goal is to reproduce this idea with groups and homomorphisms, i.e., given  $G, G'$  groups, and an onto homomorphism  $\phi : G \rightarrow G'$ , then understand  $G$  as being a "stacking" of cosets of  $\ker(\phi)$  and when we collapse each coset to a point, we get  $G'$ .

Our goal will be related to the following theorem:

**Theorem 10.3.** Given  $G$  and a subgroup  $H$ , then  $H \triangleleft G$  if, and only if, there is a group  $G'$  and a homomorphism  $\phi : G \rightarrow G'$  such that  $\ker \phi = H$ .

**Definition 10.1 (Notation).** Let  $G/H$  (" $G \bmod H$ ") be the set of all right cosets of  $H$  sitting inside  $G$ .

**Theorem 10.4.** When  $H \triangleleft G$ , there exists a binary operation on  $G/H$  and an homomorphism  $\phi : G \rightarrow G/H$  such that  $\ker \phi = H$ .

*Spoiler:* The operation  $*$  will be, for  $A, B \in G/H$ ,  $A * B = AB = \{g \in G : \exists a_1 \in A, b_1 \in B, g = a_1 b_1\}$ .

## 11 Quotient Groups (October 02, 2020)

Here's a rephrasing of our motivation from Linear Algebra:

Suppose  $V$  is a vector space, and  $S \subset V$  a subspace. Let  $\vec{x} \in V$ . In Linear Algebra, we learned we write  $\vec{x}$  as a sum of a vector in  $S$  with an vector  $\vec{z}$  orthogonal to  $S$ , a.k.a.,  $\vec{z} \in S^\perp$ .

$V$  can be decomposed into parallel copies of  $S$ , and there exists a vector space  $W$  and a linear map  $T : V \rightarrow W$  so that  $T$  has the effect of collapsing each parallel copy of  $S$  to a point. And,  $\ker T = S$ .

To summarize: Given  $S$  a subspace of  $V$ , there exists a decomposition of  $V$  into parallel copies of  $S$  and there exists a vector space  $W$  and a linear map  $T : V \rightarrow W$  so that  $T$  collapses the parallel copies to points and  $\ker T = S$ .

Our goal in the Group Theory setting: Given  $H \triangleleft G$ , there exists a decomposition of  $G$  into right cosets of  $H$  in  $G$  and there exists a group  $G'$  and a homomorphism  $\phi : G \rightarrow G'$  so that  $\phi$  collapses a right cosets of  $H$  to a point and  $\ker \phi = H$ .

On Wednesday, we defined  $G/H = \{\text{right cosets of } H \text{ in } G\}$  as our candidate for  $G'$ .

Given  $Ha, Hb \in G/H$ , we defined  $Ha * Hb = (Ha)(Hb) = \{h_1 a h_2 b : h_1, h_2 \in H\}$ .

We know that  $aH = Ha$ , then  $HaHb = HHab$ . Since  $H$  is closed under operation and  $He = H$ , we have that  $HH = H$ . Thus,

$$Ha * Hb = (Ha)(Hb) = H(ab),$$

which means that  $*$  is a binary operation.

So far, we have that  $G/H$  has a binary operation. We also have a candidate for  $\phi$ ! Define  $\phi : G \rightarrow G/H$ , with  $g \rightarrow Hg$ . Given,  $a, b \in G$ ,

$$\phi(ab) = H(ab) = (Ha)(Hb) = \phi(a)\phi(b),$$

thus  $\phi$  has the homomorphism property. Note also that  $\phi$  is onto.

**Lemma 11.1.** If  $G$  is a group,  $Y$  is a set with a binary operation,  $\phi : G \rightarrow Y$  such that  $\phi$  has the homomorphism property, and  $\phi$  is onto. Then  $Y$  is a group and  $\phi$  is a homomorphism.

*Proof.* We need to show the following items:

- (i) Associativity. Given  $a, b, c \in Y$ , since  $\phi$  is onto, we have  $a = \phi(a'), b = \phi(b'), c = \phi(c')$ , for some  $a', b', c' \in G$ . So

$$\begin{aligned} (ab)c &= (\phi(a')\phi(b'))\phi(c') \\ &= \phi(a'b')\phi(c') \\ &= \phi((a'b')c') \\ &= \phi(a'(b'c')) \\ &= \phi(a')\phi(b'c') \\ &= \phi(a')(\phi(b')\phi(c')) \\ &= a(bc). \end{aligned}$$

- (ii) Identity. The same strategy as above.

- (iii) Inverses. The same strategy as above.

Thus,  $Y$  is a group. □

## 12 First Isomorphism Theorem (October 05, 2020)

Summary of our work from last week:

Start with a group  $G$  and a normal subgroup  $H$  in  $G$ . Then, we showed that there exists a way to turn  $G/H$  into a group, and, the “natural” map  $\phi : G \rightarrow G/H$ , defined by  $g \mapsto Hg$  is an onto homomorphism. The identity of  $G/H$  is  $H$ . Also,  $\ker(\phi) = H$ . AND,  $\phi$  has the effect of collapsing each coset of  $H$  to a single element.

So, starting with  $H \triangleleft G$ , we constructed an onto homomorphism  $\phi : G \rightarrow G/H$ .

**Question.** If we start with an onto homomorphism  $\phi : G \rightarrow G'$ , when is it the case that  $\phi$  arose via what we did last week?

**Theorem 12.1 (1<sup>st</sup> Isomorphism Theorem).** If  $\phi : G \rightarrow G'$  is an onto homomorphism, and  $N$  denotes  $\ker(\phi)$ , then  $G'$  is isomorphic to  $G/N$ .

And, there exists a unique isomorphism  $\bar{\phi} : G/N \rightarrow G'$  so that  $\bar{\phi}$  commutes with the natural map  $\pi : G \rightarrow G/N$ , defined by  $g \mapsto gN$ , i.e.,

$$\bar{\phi} \circ \pi = \phi.$$

*Proof.* We want to find a map  $\bar{\phi} : G/N \rightarrow G'$ . Let's define

$$\bar{\phi}(Ng) = \phi(g).$$

There is a subtle problem: what if  $Ng = Nh$ ? As we defined  $\bar{\phi}$ , it sends  $Ng$  to  $\phi(g)$ , and  $Nh$  to  $\phi(h)$ . This is a problem unless  $\phi(g) = \phi(h)$ .

This definition is coherent, because

$$\begin{aligned} Ng = Nh &\implies gh^{-1} \in N = \ker \phi \\ &\implies \phi(gh^{-1}) = e' && (e' \text{ is the identity element of } G') \\ &\implies \phi(g)\phi(h)^{-1} = e' \\ &\implies \phi(g) = \phi(h). \end{aligned}$$

Let's show that  $\bar{\phi}$  is a homomorphism:

$$\begin{aligned} \bar{\phi}(NaNb) &= \bar{\phi}(Nab) && (N \text{ is normal}) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) && (\phi \text{ is a homomorphism}) \\ &= \bar{\phi}(Na)\bar{\phi}(Nb). \end{aligned}$$

Let's show that  $\bar{\phi}$  is onto: Given  $g' \in G'$ , there exists  $y \in G$  such that  $\phi(y) = g'$ , since  $\phi$  is onto. So, consider  $\pi(y) = Ny \in G/N$ . Then,  $\bar{\phi}(Ny) = \phi(y) = g'$ .

Let's show that  $\bar{\phi}$  is one-to-one:

$$\begin{aligned} \bar{\phi}(Na) = \bar{\phi}(Nb) &\implies \phi(a) = \phi(b) \\ &\implies \phi(a)\phi(b)^{-1} = e' \\ &\implies \phi(ab^{-1}) = e' \\ ab^{-1} &\in N \\ Na &= Nb. \end{aligned}$$

□