

# 18.701: Algebra 1

Jakin Ng, Sanjana Das, and Ethan Yang

Fall 2021

## Contents

<b>1</b>	<b>Groups</b>	<b>5</b>
1.1	Introduction . . . . .	5
1.2	Laws of Composition . . . . .	5
1.3	Permutation and Symmetric Groups . . . . .	7
1.4	Examples of Symmetric Groups . . . . .	8
<b>2</b>	<b>Subgroups and Cyclic Groups</b>	<b>10</b>
2.1	Review . . . . .	10
2.2	Subgroups . . . . .	10
2.3	Subgroups of the Integers . . . . .	11
2.4	Cyclic Groups . . . . .	12
<b>3</b>	<b>Homomorphisms and Isomorphisms</b>	<b>14</b>
3.1	Review . . . . .	14
3.2	Homomorphisms . . . . .	14
3.3	Examples . . . . .	14
<b>4</b>	<b>Isomorphisms and Cosets</b>	<b>18</b>
4.1	Review . . . . .	18
4.2	Isomorphisms . . . . .	18
4.3	Automorphisms . . . . .	18
4.4	Cosets . . . . .	19
4.5	Lagrange's Theorem . . . . .	21
<b>5</b>	<b>The Correspondence Theorem</b>	<b>22</b>
5.1	Review . . . . .	22
5.2	Lagrange's Theorem . . . . .	22
5.3	Results of the Counting Formula . . . . .	22
5.4	Normal Subgroups . . . . .	23
5.5	The Correspondence Theorem . . . . .	25
<b>6</b>	<b>Normal Subgroups and Quotient Groups</b>	<b>27</b>
6.1	Review . . . . .	27
6.2	Normal Subgroups . . . . .	27
6.3	Quotient Groups . . . . .	28
6.4	First Isomorphism Theorem . . . . .	30
<b>7</b>	<b>Fields and Vector Spaces</b>	<b>31</b>
7.1	Review . . . . .	31
7.2	Fields . . . . .	31
7.3	Vector Spaces . . . . .	31
7.4	Bases and Dimension . . . . .	32
<b>8</b>	<b>Dimension Formula</b>	<b>35</b>
8.1	Review . . . . .	35

8.2	Matrix of Linear Transformations . . . . .	35
8.3	Dimension Formula . . . . .	36
<b>9</b>	<b>Dimension Formula</b>	<b>38</b>
9.1	Review . . . . .	38
9.2	Linear Operators . . . . .	38
9.3	Change of Basis . . . . .	39
9.4	Eigenvectors, Eigenvalues, and Diagonalizable Matrices . . . . .	40
9.5	Finding Eigenvalues and Eigenvectors . . . . .	42
<b>10</b>	<b>Eigenbases and the Jordan Form</b>	<b>45</b>
10.1	Review . . . . .	45
10.2	The Characteristic Polynomial . . . . .	45
10.3	Jordan Form . . . . .	47
<b>11</b>	<b>The Jordan Decomposition</b>	<b>49</b>
11.1	Review . . . . .	49
11.2	The Jordan Decomposition, Continued . . . . .	49
11.3	Proof of Jordan Decomposition Theorem . . . . .	50
<b>12</b>	<b>Orthogonal Matrices</b>	<b>54</b>
12.1	Dot Products and Orthogonal Matrices . . . . .	54
12.2	The Special Orthogonal Group . . . . .	55
12.3	Orthogonal Matrices in Two Dimensions . . . . .	55
12.4	Orthogonal Matrices in Three Dimensions . . . . .	57
<b>13</b>	<b>Isometries</b>	<b>60</b>
13.1	Review . . . . .	60
13.2	Isometries . . . . .	60
13.3	Isometries in 2-space . . . . .	62
<b>14</b>	<b>Symmetry Groups</b>	<b>65</b>
14.1	Review . . . . .	65
14.2	Examples of Symmetry Groups . . . . .	65
14.3	Discrete Subgroups of $\mathbb{R}$ . . . . .	66
14.4	Finite subgroups of $O_2$ . . . . .	67
14.5	More Discrete Subgroups . . . . .	68
<b>15</b>	<b>Finite and Discrete Subgroups, Continued</b>	<b>69</b>
15.1	Review . . . . .	69
15.2	Finite Subgroups of $M_2$ . . . . .	69
15.3	Discrete Subgroups of $M_2$ . . . . .	70
15.3.1	Discrete Subgroups of $\mathbb{R}^2$ . . . . .	71
15.3.2	Back to Discrete Subgroups of $M_2!$ . . . . .	72
<b>16</b>	<b>Discrete Groups</b>	<b>73</b>
16.1	Review . . . . .	73
16.2	Examples for $L$ and $\overline{G}$ . . . . .	73
16.3	Crystallographic Restriction . . . . .	75
<b>17</b>	<b>Group Actions</b>	<b>80</b>
17.1	Review . . . . .	80
17.2	Motivating Examples . . . . .	80
17.3	What is a group action? . . . . .	81
17.4	The Counting Formula . . . . .	82
<b>18</b>	<b>Stabilizer</b>	<b>86</b>
18.1	Review . . . . .	86
18.2	Counting Formula . . . . .	86
18.3	Stabilizers of Products . . . . .	86

18.4 Statement . . . . .	87
18.5 Finding the subgroups . . . . .	88
18.6 The Octahedral Group . . . . .	89
<b>19 Group Actions on <math>G</math></b>	<b>91</b>
19.1 Conjugation . . . . .	91
19.2 $p$ -groups . . . . .	92
<b>20 The Icosahedral Group</b>	<b>96</b>
20.1 Review: The Class Equation . . . . .	96
20.2 Basic Information . . . . .	96
20.3 Conjugacy Classes . . . . .	97
20.4 Simple Groups . . . . .	97
20.5 Conjugacy Classes for Symmetric Groups . . . . .	99
<b>21 Conjugacy Classes for Symmetric and Alternating Groups</b>	<b>101</b>
21.1 Review . . . . .	101
21.2 Cycle Type . . . . .	101
21.3 Conjugacy Classes in $S_n$ . . . . .	102
21.4 Class Equation for $S_4$ . . . . .	103
21.5 Student Question . . . . .	105
<b>22 The Sylow Theorems</b>	<b>107</b>
22.1 Review . . . . .	107
22.2 Motivation . . . . .	107
22.3 The First Sylow Theorem . . . . .	107
22.4 The Second Sylow Theorem . . . . .	108
22.5 The Third Sylow Theorem . . . . .	109
22.6 Applications of the Sylow Theorems . . . . .	109
<b>23 Proofs and Applications of the Sylow Theorems</b>	<b>114</b>
23.1 Review . . . . .	114
23.2 Application: Decomposition of Finite Abelian Groups . . . . .	114
23.3 Proof of Sylow Theorems . . . . .	115
<b>24 Bilinear Forms</b>	<b>119</b>
24.1 Review . . . . .	119
24.2 Bilinear Forms . . . . .	119
24.3 Change of Basis . . . . .	122
24.4 Bilinear Forms over $CC$ . . . . .	123
<b>25 Orthogonality</b>	<b>125</b>
25.1 Review: Bilinear Forms . . . . .	125
25.2 Hermitian Forms . . . . .	125
25.3 Orthogonality . . . . .	127
<b>26 The Projection Formula</b>	<b>130</b>
26.1 Review: Symmetric and Hermitian Forms . . . . .	130
26.2 Orthogonality . . . . .	130
26.3 Orthogonal Bases . . . . .	131
26.4 Projection Formula . . . . .	132
<b>27 Euclidean and Hermitian Spaces</b>	<b>134</b>
27.1 Review: Orthogonal Projection . . . . .	134
27.2 Euclidean and Hermitian Spaces . . . . .	134
27.3 Gram-Schmidt Algorithm . . . . .	134
27.4 Complex Linear Operators . . . . .	136
<b>28 The Spectral Theorem</b>	<b>138</b>
28.1 Review: Hermitian Spaces . . . . .	138

28.2 The Spectral Theorem . . . . .	138
<b>29 Linear Groups</b>	<b>141</b>
29.1 Geometry of groups . . . . .	141
29.2 Geometry of $SU_2$ . . . . .	142
29.2.1 Quaternions . . . . .	143
29.2.2 Geometry of the Sphere . . . . .	143
29.2.3 Latitudes . . . . .	144
<b>30 The Special Unitary Group <math>SU_2</math></b>	<b>147</b>
30.1 Review . . . . .	147
30.2 Longitudes . . . . .	147
30.3 More Group Theoretic Properties . . . . .	148
30.4 Conjugation and the Orthogonal Group . . . . .	148
30.5 One-Parameter Groups . . . . .	149
<b>31 One-Parameter Subgroups</b>	<b>152</b>
31.1 Review . . . . .	152
31.2 Properties of the Matrix Exponential . . . . .	152
31.3 One-Parameter Subgroups . . . . .	153
<b>32 One-Parameter Groups, Continued</b>	<b>156</b>
32.1 Review . . . . .	156
32.2 Examples! . . . . .	156
32.3 The Special Linear Group $SL_n(\mathbb{C})$ . . . . .	157
32.4 Tangent Vectors . . . . .	158
<b>33 Lie Groups</b>	<b>160</b>
33.1 Review . . . . .	160
33.2 Lie Groups . . . . .	161
33.3 Manifolds . . . . .	162
33.4 Lie Bracket . . . . .	163
<b>34 Simple Linear Groups</b>	<b>165</b>
34.1 Review . . . . .	165
34.2 Simple Linear Groups . . . . .	165
34.3 The Special Unitary Group . . . . .	165
34.4 The Special Linear Group . . . . .	168
34.5 Generalizations . . . . .	170
<b>35 Hilbert's Third Problem</b>	<b>171</b>
35.1 Polygons in the Plane . . . . .	171
35.2 The Question . . . . .	171
35.3 Some Algebra . . . . .	172
35.4 Back to Polytopes . . . . .	173

# 1 Groups

## 1.1 Introduction

The lecturer is **Davesh Maulik**. These notes are taken by **Jakin Ng, Sanjana Das, and Ethan Yang**. Here is some basic information about the class:

- The text used in this class will be the 3rd edition of **Algebra**, by Artin.
- The course website is found on **Canvas**, and the problem sets will be submitted on **Gradescope**.
- The problem sets will be due every Tuesday at midnight.

Throughout this semester, we will discuss the fundamentals of *linear algebra* and *group theory*, which is the study of symmetries. In this class, we will mostly study groups derived from geometric objects or vector spaces, but in the next course, 18.702<sup>1</sup>, more exotic groups will be studied.

As a review of basic linear algebra, let's review invertible matrices.

### Definition 1.1

An  $n \times n$  matrix<sup>a</sup>  $A$  is invertible if there exists some other matrix  $A^{-1}$  such that  $AA^{-1} = A^{-1}A = I$ , the  $n \times n$  identity matrix. Equivalently,  $A$  is invertible if and only if the determinant  $\det(A) \neq 0$ .

<sup>a</sup>An array of numbers (or some other type of object) with  $n$  rows and  $n$  columns

### Example 1.2 ( $n = 2$ )

Let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  be a  $2 \times 2$  matrix. Then its inverse  $A^{-1}$  is  $\frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ .

### Example 1.3 ( $GL_n(\mathbb{R})$ )

A main example that will guide our discussion of groups<sup>a</sup> is the **general linear group**,  $GL_n(\mathbb{R})$ , which is the group of  $n \times n$  invertible real matrices.

<sup>a</sup>The concept of a *group* will be fleshed out later in this lecture

Throughout the course, we will be returning to this example to illustrate various concepts that we learn about.

## 1.2 Laws of Composition

With our example in mind, let's start.

### Guiding Question

How can we generalize the nice properties of matrices and matrix multiplication in a useful way?

Given two matrices  $A, B \in GL_n(\mathbb{R})$ , there is an operation combining them, in particular *matrix multiplication*, which returns a matrix  $AB \in GL_n(\mathbb{R})$ .<sup>2</sup> The matrices under matrix multiplication satisfy several properties:

- **Noncommutativity.** Matrix multiplication is noncommutative, which means that  $AB$  is not necessarily the same matrix as  $BA$ . So the order that they are listed in *does* matter.
- **Associativity.** This means that  $(AB)C = A(BC)$ , which means that the matrices to be multiplied can be grouped together in different configurations. As a result, we can omit parentheses when writing the product of more than two matrices.
- **Inverse.** The product of two invertible matrices is also invertible. In particular,

$$(AB)^{-1} = B^{-1}A^{-1}.$$

---

<sup>1</sup>Algebra 2

<sup>2</sup>Since the determinant is multiplicative,  $\det(AB) = \det(A)\det(B)$ , which is nonzero.

Another way to think of matrices is as an *operation* on a different space. Given a matrix  $A \in GL_n(\mathbb{R})$ , a function or transformation on  $\mathbb{R}^n$ <sup>3</sup> can be associated to it, namely

$$T_A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

$$\vec{v} = (x_1, \dots, x_n) \longmapsto A\vec{v}$$
<sup>4</sup>.

Since  $A\vec{v}$  is the matrix product, we notice that  $T_{AB}(\vec{v}) = T_A(T_B(\vec{v}))$ , and so matrix multiplication is the same as function composition.

With this motivation, we can define the notion of a group.

**Definition 1.4 (Group)**

A **group** is a set  $G$  with a composition (or product) law

$$G \times G \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$
<sup>5</sup>

fulfilling the following conditions:

- **Identity.** There exists some element  $e \in G$  such that  $a \cdot e = e \cdot a = a$
- **Inverse.** For all  $a \in G$ , there exists  $b \in G$ , denoted  $a^{-1}$ , such that  $a \cdot b = b \cdot a = e$ .
- **Associative.** For  $a, b, c \in G$ ,

$$(ab)c = a(bc).$$

---

Also denoted  $ab$

In the definition, both the first and second conditions automatically give us a unique inverse and identity. For example, if  $e$  and  $e'$  both satisfy property 1, then  $e \cdot e' = e = e'$ , so they must be the same element. A similar argument holds for inverses.

Why does associativity matter? It allows us to define the product  $g_1 \cdot g_2 \cdots \cdots g_n$  without the parentheses indicating which groupings they're multiplied in.

**Definition 1.5**

Let  $g$  taken to the power  $n$  be the element  $g^n = \underbrace{g \cdots \cdots g}_{n \text{ times}}$  for  $n > 0$ ,  $g^n = \underbrace{g^{-1} \cdots \cdots g^{-1}}_{n \text{ times}}$  for  $n < 0$ , and  $e$  for  $n = 0$ .

**Example 1.6**

Some common groups include:

Group	Composition Law	Identity	Inverse
$GL_n(\mathbb{R})$ <sup>a</sup>	matrix multiplication	$I_n$	$A \mapsto A^{-1}$
$\mathbb{Z}$ <sup>b</sup>	+	0	$n \mapsto -n$
$\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ <sup>c</sup>	×	1	$z \mapsto \frac{1}{z}$

---

<sup>a</sup>The general linear group  
<sup>b</sup>The integers under addition  
<sup>c</sup>The complex numbers (except 0) under multiplication

For the last two groups, there is additional structure: the composition law is *commutative*. This motivates the following definition.

**Definition 1.7**

A group  $G$  is **abelian** if  $a \cdot b = b \cdot a$  for all  $a, b \in G$ . Otherwise,  $G$  is called **nonabelian**.

---

<sup>3</sup>Vectors with  $n$  entries which are real numbers.  
<sup>4</sup>The notation  $A\vec{v}$  refers to the matrix product of  $A$  and  $\vec{v}$ , considered as  $n \times n$  and  $n \times 1$  matrices.

Often, the composition law in an abelian group is denoted  $+$  instead of  $\cdot$ .

### 1.3 Permutation and Symmetric Groups

Now, we will look at an extended example of another family of nonabelian groups.

**Definition 1.8**

Given a set  $S$ , a **permutation** of  $S$  is a *bijection*<sup>a</sup>  $p : S \rightarrow S$ .

<sup>a</sup>A function  $f : A \rightarrow B$  is a bijection if for all  $y \in B$ , there exists a unique  $x \in A$  such that  $f(x) = y$ . Equivalently, it must be one-to-one and onto.

**Definition 1.9**

Let  $\text{Perm}(S)$  be the set of permutations of  $S$ .

In fact,  $\text{Perm}(S)$  is a group, where the product rule is function composition.<sup>6</sup>

- **Identity.** The identity function  $e : x \mapsto x$  is the identity element of the group.
- **Inverse.** Because  $p$  is a bijection, it is invertible. Let  $p^{-1}(x)$  be the unique  $y \in S$  such that  $p(y) = x$ .
- **Associativity.** Function composition is always associative.

Like groups of matrices,  $\text{Perm}(S)$  is a group coming from a set of *transformations* acting on some object; in this case,  $S$ .

**Definition 1.10**

When  $S = \{1, 2, \dots, n\}$ , the permutation group  $\text{Perm}(S)$  is called the **symmetric group**, denoted  $S_n$ .

**Definition 1.11**

For a group  $G$ , the number of elements in the set  $G$ ,  $|G|$ , is called the **order** of the group  $G$ , denoted  $|G|$  or  $\text{ord}(G)$ .

The order of the symmetric group is  $|S_n| = n!$ <sup>7</sup> so the symmetric group  $S_n$  is a *finite* group.

For  $n = 6$ , consider the two permutations  $p$  and  $q$

$$\begin{array}{c|cccccc} i & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline p(i) & 2 & 4 & 5 & 1 & 3 & 6 \\ \\ i & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline q(i) & 3 & 4 & 5 & 6 & 1 & 2 \end{array},$$

where the upper number is mapped to the lower number.

We can also write these in **cycle notation**, which is a shorthand way of describing a permutation that does not affect what the permutation actually is. In cycle notation, each group of parentheses describes a cycle, where the number is mapped to the following number, and it wraps around.

**Example 1.12 (Cycle notation)**

In cycle notation,  $p$  is written as  $(124)(35)$ , where the 6 is omitted. In the first cycle, 1 maps to 2, 2 maps to 4, and 4 maps to 1, and in the second cycle, 3 maps to 5 and 5 maps back to 3.<sup>a</sup>

<sup>a</sup>In fact, we say that  $p$  has *cycle type*  $(3, 2)$ , which is the lengths of each cycle.

<sup>6</sup>We can check that the composition of two bijections  $p \circ q$  is also a bijection.

<sup>7</sup>The number of permutations of the numbers 1 through  $n$  is  $n!$  — there are  $n$  possibilities for where 1 maps to, and then  $n - 1$  for where 2 maps to, and so on to get  $n(n - 1) \cdots (2)(1) = n!$

Similarly,  $q$  is written as  $(135)(246)$ .<sup>8</sup> In cycle notation, it is clear that there are multiple ways to write or represent the same permutation. For example,  $p$  could have been written as  $(241)(53)$  instead, but it represents the *same* element  $p \in S_6$ .

Cycle notation allows us to more easily invert or compose two permutations; we simply have to follow where each number maps to.

**Example 1.13 (Inversion)**

The inverse  $p^{-1}$  flips the rows of the table:

$$\begin{array}{c|cccccc} i & 2 & 4 & 5 & 1 & 3 & 6 \\ \hline p(i) & 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

In cycle notation, it reverses the cycles, since each number should be mapped under  $p^{-1}$  to the number that maps to it under  $p$ :

$$p^{-1} = (421)(53) = (142)(35).$$

**Example 1.14 (Composition)**

The composition is

$$q \circ p = (143)(26).$$

Under  $p$ , 1 maps to 2, which maps to 4 under  $q$ , and so 1 maps to 4 under  $q \circ p$ .<sup>a</sup> Similarly, 4 maps to 3 and 3 maps back to 1, which gives us the first cycle. The second cycle is similar.

<sup>a</sup>Remember that the rightmost permutation is applied first, and then the leftmost, and not the other way around, due to the notation used for function composition.

**Example 1.15 (Conjugation)**

Another example of composition is

$$p^{-1} \circ q \circ p = (126)(345).$$

This is also known as *conjugation* of  $q$  by  $p$ .<sup>a</sup>

<sup>a</sup>Notice that under conjugation,  $q$  retains its cycle type  $(3, 3)$ . In fact, this is true for conjugation of any element by any other element!

## 1.4 Examples of Symmetric Groups

For  $n \geq 3$ ,  $S_n$  is always non-abelian. Let's consider  $S_n$  for small  $n \leq 3$ .

**Example 1.16 ( $S_1$ )**

In this case,  $S_1$  only has one element, the identity element, and so it is  $\{e\}$ , the *trivial group*.

**Example 1.17 ( $S_2$ )**

For  $n = 2$ , the only possibilities are the identity permutation  $e$  and the transposition  $(12)$ . Then  $S_2 = \{e, (12)\}$ ; it has order 2.

Once  $n$  gets larger, the symmetric group becomes more interesting.

<sup>8</sup>It has cycle type  $(3, 3)$ .

**Example 1.18** ( $S_3$ )

The symmetric group on three elements is of order  $3! = 6$ . It must contain the identity  $e$ . It can also contain  $x = (123)$ . Then we also get the element  $x^2 = (132)$ , but

$$\boxed{x^3 = e.}$$

Higher powers are just  $x^4 = x$ ,  $x^5 = x^2$ , and so on. Now, we can introduce  $y = (12)$ , which is its own inverse, and so

$$\boxed{y^2 = e.}$$

Taking products gives  $xy = (13)$  and  $x^2y = (23)$ . So we have all six elements of  $S_3$ :

$$S_3 = \{e, (123), (132), (12), (13), (23)\}.$$

In fact,  $yx = (23) = x^2y$ , so taking products in the other order does not provide any new elements. The relation

$$\boxed{yx = x^2y}$$

holds. In particular, using the boxed relations, we can compute *any* crazy combination of  $x$  and  $y$  and reduce it to one of the elements we listed. For example,  $xyx^{-1}y = xyx^2y = xyyx = xy^2x = x^2$ .

## 2 Subgroups and Cyclic Groups

### 2.1 Review

Last time, we discussed the concept of a group, as well as examples of groups. In particular, a group is a set  $G$  with an associative composition law  $G \times G \rightarrow G$  that has an identity as well as inverses for each element with respect to the composition law  $\times$ .

Our guiding example was that of the group of invertible  $n \times n$  matrices, known as the **general linear group** ( $GL_n(\mathbb{R})$  or  $GL_n(\mathbb{C})$ , for matrices over  $\mathbb{R}$  and  $\mathbb{C}$ , respectively.)

#### Example 2.1

Let  $GL_n(\mathbb{R})$  be the group of  $n \times n$  invertible real matrices.

- **Associativity.** Matrix multiplication is associative; that is,  $(AB)C = A(BC)$ , and so when writing a product consisting of more than two matrices, it is not necessary to put in parentheses.
- **Identity.** The  $n \times n$  identity matrix is  $I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$ , which is the matrix with 1s along the diagonal and 0s everywhere else. It satisfies the property that  $AI = IA = A$  for all  $n \times n$  matrices  $A$ .
- **Inverse.** By the invertibility condition of  $GL_n$ , every matrix  $A \in GL_n(\mathbb{R})$  has an inverse matrix  $A^{-1}$  such that  $AA^{-1} = A^{-1}A = I_n$ .

Furthermore, each of these matrices can be seen as a transformation from  $\mathbb{R}^n \rightarrow \mathbb{R}^n$ , taking each vector  $\vec{v}$  to  $A\vec{v}$ . That is, there is a bijective correspondence between matrices  $A$  and invertible transformations  $T_A : \mathbb{R}^n \rightarrow \mathbb{R}^n$  taking  $T_A(\vec{v}) = A\vec{v}$ .

Another example that showed up was the integers under addition.

#### Example 2.2

The integers  $\mathbb{Z}$  with the composition law  $+$  form a group. Addition is associative. Also,  $0 \in \mathbb{Z}$  is the additive identity, and  $-a \in \mathbb{Z}$  is the inverse of any integer  $a$ .

On the other hand, the natural numbers  $\mathbb{N}$  under addition would *not* form a group, because the invertibility condition would be violated.

Lastly, we looked at the symmetric group  $S_n$ .

#### Example 2.3

The **symmetric group**  $S_n$  is the permutation group of  $\{1, \dots, n\}$ .

### 2.2 Subgroups

In fact, understanding  $S_n$  is important for group theory as a whole because *any* finite group "sits inside"  $S_n$  in a certain way<sup>9</sup>, which we will begin to discuss today.

#### Guiding Question

What does it mean for a group to "sit inside" another group?

If a subset of a group satisfies certain properties, it is known as a *subgroup*.

<sup>9</sup>This is known as *Cayley's Theorem* and is discussed further in section 7.1 of Artin.

**Definition 2.4**

Given a group  $(G, \cdot)$ , a subset  $H \subset G$  is called a **subgroup** if it satisfies:

- **Closure.** If  $h_1, h_2 \in H$ , then  $h_1 \cdot h_2 \in H$ .
- **Identity.** The identity element  $e$  in  $G$  is contained in  $H$ .
- **Inverse.** If  $h \in H$ , its inverse  $h^{-1}$  is also an element of  $H$ .

As notation, we write  $H \leq G$  to denote that  $H$  is a subgroup of  $G$ .

Essentially, these properties consists solely of the necessary properties for  $H$  to also be a group under the same operation  $\cdot$ , so that it can be considered a subgroup and not just some arbitrary subset. In particular, any subgroup  $H$  will also be a group with the same operation, independent of the larger group  $G$ .

**Example 2.5**

The integers form a subgroup of the rationals under addition:  $(\mathbb{Z}, +) \subset (\mathbb{Q}, +)$ .

The rationals are more complicated than the integers, and studying simpler subgroups of a certain group can help with understanding the group structure as a whole.

**Example 2.6**

The symmetric group  $S_3$  has a three-element subgroup  $\{e, (123), (132)\} = \{e, x, x^2\}$ .

However, the natural numbers  $\mathbb{N} = \{0, 1, 2, \dots\} \subset (\mathbb{Z}, +)$  are **not** a subgroup of the integers, since not every element has an inverse.

**Example 2.7**

The matrices with determinant 1, called the **special linear group**, form a subgroup of invertible matrices:  $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$ .

The special linear group is closed under matrix multiplication because  $\det(AB) = \det(A)\det(B)$ .

## 2.3 Subgroups of the Integers

The integers  $(\mathbb{Z}, +)$  have particularly nice subgroups.

**Theorem 2.8**

The subgroups of  $(\mathbb{Z}, +)$  are  $\{0\}, \mathbb{Z}, 2\mathbb{Z}, \dots$ .<sup>a</sup>

<sup>a</sup>Where  $n \in \mathbb{Z}$ ,  $n\mathbb{Z}$  consists of the multiples of  $n$ ,  $\{nx : x \in \mathbb{Z}\}$ .

This theorem demonstrates that the condition that a subset  $H$  of a group be a subgroup is quite strong, and requires quite a bit of structure from  $H$ .

*Proof.* First,  $n\mathbb{Z}$  is in fact a subgroup.

- **Closure.** For  $na, nb \in n\mathbb{Z}$ ,  $na + nb = n(a + b)$ .
- **Identity.** The additive identity is in  $n\mathbb{Z}$  because  $0 = n \cdot 0$ .
- **Inverse.** For  $na \in n\mathbb{Z}$ , its inverse  $-na = n(-a)$  is also in  $n\mathbb{Z}$ .

Now, suppose  $S \subset \mathbb{Z}$  is a subgroup. Then clearly the identity 0 is an element of  $S$ . If there are no more elements in  $S$ , then  $S = \{0\}$  and the proof is complete. Otherwise, pick some nonzero  $h \in S$ . Without loss of generality, we assume that  $h > 0$  (otherwise, since  $-h \in S$  as well by the invertibility condition, take  $-h$  instead of  $h$ .) Thus,  $S$  contains at least one positive integer; let  $a$  be the smallest positive integer in  $S$ .

Then we claim that  $S = a\mathbb{Z}$ . If  $a \in S$ , then  $a + a = 2a \in S$  by closure, which implies that  $2a + a = 3a \in S$ , and so on. Similarly,  $-a \in S$  by inverses, and  $-a + (-a) = -2a \in S$ , and so on, which implies that  $a\mathbb{Z} \subset S$ .

Now, take any  $n \in S$ . By the Euclidean algorithm,  $n = aq + r$  for some  $0 \leq r < a$ . From the subgroup properties,  $n - aq = r \in S$  as well. Since  $a$  is the smallest positive integer in  $S$ , if  $r > 0$ , there would be a contradiction, so  $r = 0$ . Thus,  $n = aq$ , which is an element of  $a\mathbb{Z}$ . Therefore,  $S \subset a\mathbb{Z}$ .

From these two inclusions,  $S = a\mathbb{Z}$  and the proof is complete.  $\square$

**Corollary 2.9**

Given  $a, b \in \mathbb{Z}$ , consider  $S = \{ai + bj : i, j \in \mathbb{Z}\}$ . The subset  $S$  satisfies all the subgroup conditions, so by Theorem 2.8, there is some  $d$  such that  $S = d\mathbb{Z}$ . In fact,  $d = \gcd(a, b)$ .

*Proof.* Let  $e = \gcd(a, b)$ . Since  $a \in S$ ,  $a = dk$  and  $b = dl$  for some  $k, l$ . Since the  $d$  from before divides  $a$  and  $b$ , it must also divide  $e$ , by definition of the greatest common divisor. Also, since  $d \in S$ , by the definition of  $S$ ,  $d = ar + bs$  for some  $r$  and  $s$ . Since  $e$  divides  $a$  and  $b$ ,  $e$  divides both  $ar$  and  $bs$  and therefore  $d$ .

Thus,  $d$  divides  $e$ , and  $e$  divides  $d$ , implying that  $e = d$ . So  $S = \gcd(a, b)\mathbb{Z}$ .  $\square$

In particular, we have showed that  $\gcd(a, b)$  can always be written in the form  $ar + bs$  for some  $r, s$ .

## 2.4 Cyclic Groups

Now, let's discuss a very important type of subgroup that connects back to the work we did with  $(\mathbb{Z}, +)$ .

**Definition 2.10**

Let  $G$  be a group, and take  $g \in G$ . Let the **cyclic subgroup generated by  $g$**  be

$$\langle g \rangle := {}^a\{\dots g^{-2}, g^{-1}, g^0 = e, g^1, g^2, \dots\} \leq G.$$

<sup>a</sup>The  $:=$  symbol is usually used by mathematicians to mean "is defined to be." Other people may use  $\equiv$  for the same purpose.

Since  $g^a \cdot g^b = g^{a+b}$ , the exponents of the elements of a cyclic subgroup will have a related group structure to  $(\mathbb{Z}, +)$ .

**Example 2.11**

The identity element generates the trivial subgroup  $\{e\} = \langle e \rangle$  of any group  $G$ .

There are also nontrivial cyclic subgroups.

**Example 2.12**

In  $S_3$ ,  $\langle (123) \rangle = \{e, (123), (132)\}$ .

Evidently, a cyclic subgroup of any finite group must also be finite.

**Example 2.13**

Let  $\mathbb{C}^\times$  be the group of nonzero complex numbers under multiplication. Then  $2 \in \mathbb{C}$  will generate

$$\langle 2 \rangle = \{\dots, 1/4, 1/2, 1, 2, 4, \dots\}$$

On the other hand,  $i \in \mathbb{C}$  will generate

$$\langle i \rangle = \{1, i, -1, -i\}.$$

This example shows that a cyclic subgroup of an infinite group can be either infinite or finite.<sup>10</sup>

<sup>10</sup>Can you work out the cases for which  $g \in \mathbb{C}$  the cyclic subgroup of  $\mathbb{C}^\times$  is finite or infinite?

**Guiding Question**

What does a cyclic subgroup look like? Can they be classified?

**Theorem 2.14**

Let  $S = \{n \in \mathbb{Z} : g^n = e\}$ . Then  $S$  is a subgroup of  $\mathbb{Z}$ , so  $S = d\mathbb{Z}$  or  $S = \{0\}$ , leading to two cases:

- If  $S = \{0\}$ , then  $\langle g \rangle$  is infinite and all the  $g^k$  are distinct.
- If  $S = d\mathbb{Z}$ , then  $\langle g \rangle = \{e, g, g^2, \dots, g^{d-1}\} \subset G$ , which is finite.

*Proof.* First,  $S$  must be shown to actually be a subgroup of  $\mathbb{Z}$ .

- **Identity.** The identity  $0 \in S$  because  $g^0 = e$ .
- **Closure.** If  $a, b \in S$ , then  $g^a = g^b = e$ , so  $g^{a+b} = g^a g^b = e \cdot e = e$ , so  $a + b \in S$ .
- **Inverse.** If  $a \in S$ , then  $g^{-a} = (g^a)^{-1} = e^{-1} = e$ , so  $a \in S$ .

Now, consider the first case. If  $g^a = g^b$  for any  $a, b$ , then multiplying on right by  $g^{-b}$  gives  $g^a \cdot g^{-b} = g^{a-b} = e$ . Thus,  $a - b \in S$ , and if  $S = \{0\}$ , then  $a = b$ . So any two powers of  $g$  can only be equal if they have the same exponent, and thus all the  $g^i$  are distinct and the cyclic group is infinite.

Consider the second case where  $S = d\mathbb{Z}$ . Given any  $n \in \mathbb{Z}$ ,  $n = dq + r$  for  $0 \leq r < d$  by the Euclidean algorithm. Then  $g^n = g^{dq} \cdot g^r = g^r$ , which is in  $\{e, g, g^2, \dots, g^{d-1}\}$ . □

**Definition 2.15**

So if  $d = 0$ , then  $\langle g \rangle$  is infinite; we say that  $g$  has **infinite order**. Otherwise, if  $d \neq 0$ , then  $|\langle g \rangle| = d$  and  $g$  has **order  $d$** .

It is also possible to consider more than one element  $g$ .

**Definition 2.16**

Given a subset  $T \subset G$ , the subgroup generated by  $T$  is

$$\langle T \rangle := \{t_1^{e_1} \dots t_n^{e_n} \mid t_i \in T, e_i \in \mathbb{Z}\}.$$

Essentially,  $\langle T \rangle$  consists of all the possible products of elements in  $T$ . For example, if  $T = \{t, n\}$ , then

$$\langle T \rangle = \{\dots, t^2 n^{-3} t^4, n^5 t^{-1}, \dots\}.$$

**Definition 2.17**

If  $\langle T \rangle = G$ , then  $T$  **generates  $G$** .<sup>a</sup>

<sup>a</sup>Given a group  $G$ , what is the smallest set that generates it? Try thinking about this with some of the examples we've seen in class!

**Example 2.18**

The set  $\{(123), (12)\}$  generates  $S_3$ .

**Example 2.19**

The invertible matrices  $GL_n(\mathbb{R})$  are generated by elementary matrices<sup>a</sup>.

<sup>a</sup>The matrices giving row-reduction operations.

MIT OpenCourseWare  
<https://ocw.mit.edu>

Resource: Algebra I Student Notes  
Fall 2021  
Instructor: Davesch Maulik  
Notes taken by Jakin Ng, Sanjana Das, and Ethan Yang

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.