

# Course Notes

## Introduction to Abstract Algebra

*Alex Rutar*

BSM Fall 2018

# Contents

<b>1</b>	<b>Fundamentals of Groups</b>	<b>3</b>
1.1	Principles . . . . .	3
1.1.1	Rings . . . . .	3
1.1.2	Groups . . . . .	4
1.1.3	The group $\mathbb{Z}_m$ . . . . .	5
1.2	Basics of Groups . . . . .	5
1.2.1	Functions between Groups . . . . .	5
1.3	Examples of Finite Groups . . . . .	6
1.3.1	Group Definitions . . . . .	6
1.3.2	Cyclic Groups . . . . .	6
1.3.3	Permutation Groups . . . . .	7
1.3.4	Dihedral Groups . . . . .	8
1.4	Subgroups . . . . .	8
1.4.1	Subgroup Tests . . . . .	8
1.4.2	Cosets of Subgroups . . . . .	9
1.4.3	Subgroups of Cyclic Groups . . . . .	10



# Chapter 1

## Fundamentals of Groups

### 1.1 Principles

In general, algebraic structures require three properties:

- A set
- Operations on the set
- Properties of these operations

We develop theories and want to look at examples to demonstrate these properties. This course will focus on properties of rings and groups.

#### 1.1.1 Rings

A ring consists of a set along with two binary operations which satisfy  $(R, +, \cdot)$ . Then for all  $a, b, c \in R$ ,

1.  $(a + b) + c = a + (b + c)$
2.  $a + b = b + a$
3.  $\exists 0 \in R$  so that  $a + 0 = a$
4.  $\forall a \in R$ , there exists  $b \in R$  so that  $a + b = 0$
5.  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
6.  $a \cdot (b + c) = a \cdot b + a \cdot c$  and  $(a + b) \cdot c = a \cdot c + b \cdot c$

There are some common examples:

#### 1. Rings of numbers

- (a)  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- (b)  $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$
- (c)  $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$

#### 2. Rings of polynomials

$$\mathbb{Z}[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid \forall a_i \in \mathbb{Z}\}$$

$\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}[x, y]$  etc.

3. Rings of functions, such that  $C[a, b]$
4. Rings of matrices  $M_n(\mathbb{Z})$ : all  $n \times n$  square matrices with integer entries (more generally matrices with any entries in a ring).
5. Given any set  $X$ , consider  $\mathcal{P}(X)$  and define the symmetric difference

$$A \oplus B = (A \cup B) \setminus (A \cap B)$$

Then  $(\mathcal{P}(X), \oplus, \cap)$  is a ring. Interestingly,  $A = -A$  in this ring.

A ring with identity means we have some  $1 \neq 0$  so that  $a \cdot 1 = 1 \cdot a = a$ . A division ring is a ring with identity such that all nonzero elements have a multiplicative inverse. A field is a commutative division ring  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[\sqrt{2}]$ .

## 1.1.2 Groups

**Def'n. 1.1.1** A group is a set  $G$  together with an operation  $*$  which satisfies

1.  $(a * b) * c = a * (b * c)$
2.  $\exists e \in G : a * e = a = e * a$
3.  $\forall a \in G \exists b \in G : a * b = e = b * a$

Here are some common examples of groups

### 1. Additive groups:

- (a) If  $(R, +, \cdot)$  is a ring, then  $(R, +)$  is a (commutative) group.
- (b) If  $V$  is a vector space, then  $(V, +)$  is a group

### 2. Multiplicative groups:

- (a)  $R$  is a ring with identity, and write

$$R^\times = \{a \in R \mid \exists b \text{ s.t. } a \cdot b = 1 = b \cdot a\}$$

in other words the elements having a multiplicative inverse. These are called the **units** of the ring, and  $R^\times$  is called the **unit group** or the **multiplicative group** of  $R$ .

- (b)  $\mathbb{Z}^\times = \{1, -1\}$ ,  $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$  (similarly for  $\mathbb{R}, \mathbb{C}$ ).
- (c)  $M_n(\mathbb{R})^\times = \text{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$ .
- (d)  $M_n(\mathbb{Z})^\times = \text{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}$ .

### 3. Matrix groups: matrices under addition and multiplication

4. Composition of permutations. Let  $T$  be any set, and  $A : T \rightarrow T$  be bijective. Let  $S_T$  be the collection of all permutations on  $T$ . Then  $(S_T, \circ)$  (composition action) forms a group.

We write  $S_n = S_{\{1,2,\dots,n\}}$ , the group of permutations on  $n$  elements. We can notate the elements of  $S_n$  by writing

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

Clearly  $|S_n| = n!$ .

### 1.1.3 The group $\mathbb{Z}_m$

**Def'n. 1.1.2** Let  $\sim$  be an equivalence relation. We then define the **quotient group**  $G/\sim$  given by the equivalence classes of elements in  $G$ .

To construct  $\mathbb{Z}_m$ , we define  $\mathbb{Z}_m = \mathbb{Z}/\sim$  where  $a \sim b$  if  $a \equiv b \pmod{m}$ . Since we have a division algorithm in  $\mathbb{Z}$ , for any  $d \in \mathbb{Z}$ , we can write  $d = tm + r$  with  $0 \leq r \leq m-1$ . Thus  $\overline{d} = \overline{r}$ , so we can represent  $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ . As a result we usually do not bother writing  $\overline{\cdot}$ .

**Prop. 1.1.3** We have  $\overline{a} + \overline{b} = \overline{a+b}$  and  $\overline{a} \cdot \overline{b} = \overline{ab}$ .

PROOF Obvious. □

**Thm. 1.1.4**  $\mathbb{Z}_m^\times = \{\overline{a} \mid \gcd(a, m) = 1\}$ .

PROOF Assume  $\overline{a} \in \mathbb{Z}_m^\times$  so there exists  $\overline{x}$  with  $\overline{x} \cdot \overline{a} = \overline{1}$ . Then  $\overline{xa} = \overline{1}$  so  $xa \equiv 1 \pmod{m}$  so  $m \mid xa - 1$ . Let  $d = \gcd(a, m)$  so  $d \mid a$  and  $d \mid m$ . Thus  $d \mid xa - 1$  and  $d \mid xa$  so  $d \mid 1$  and  $\gcd(a, m) = 1$ .

Conversely, suppose  $\gcd(a, m) = 1$ . Then by Bézout's Lemma, get  $x, y$  so that  $xa + ym = 1$ , so  $xa \equiv 1 \pmod{m}$  and  $\overline{xa} = \overline{1}$  and  $\overline{x}\overline{a} = \overline{1}$  and we have our multiplicative inverse. □

We thus have  $|\mathbb{Z}_m^\times| = \phi(m)$ .

## 1.2 Basics of Groups

### 1.2.1 Functions between Groups

**Def'n. 1.2.1** Let  $(G, \diamond), (H, \star)$  be groups. A mapping  $f : G \rightarrow H$  is called an **homomorphism** if

$$f(u \diamond v) = f(u) \star f(v)$$

If  $f$  is also a bijection, then we call  $f$  an **isomorphism**.

**Prop. 1.2.2**  $G$  and  $H$  are isomorphic if and only if their Cayley Tables are the same up to permutation of elements.

PROOF Obvious. □

## 1.3 Examples of Finite Groups

### 1.3.1 Group Definitions

**Def'n. 1.3.1** We say that  $(G, *)$  with  $*$  :  $G \times G \rightarrow G$  is a **group** if for all  $a, b, c \in G$

1.  $(a * b) * c = a * (b * c)$
2.  $\exists e \in G : a * e = a = e * a$
3.  $\exists u \in G : a * u = e = u * a$

We have our first basic proposition:

**Prop. 1.3.2** The identity and inverses are unique.

**PROOF** If  $e, f$  are both identities, then  $e = e * f = f$ . If  $u, v$  are both inverses of  $x$ , then  $u * (x * v) = u * e = u$  and  $(u * x) * v = e * v = v$  so  $u = v$ .  $\square$

**Def'n. 1.3.3** If  $ab = ba$  for all  $a, b \in G$  then we say that  $G$  is **commutative**.

**Def'n. 1.3.4** Let  $G$  be a group with  $G = \{g_1, g_2, \dots, g_n\}$ . Then the **Cayley Table** for  $G$  is the matrix  $M \in M_n(G)$  where  $M_{ij} = g_i g_j$ .

**Prop. 1.3.5** In each column or row, each element occurs exactly once. Furthermore, if  $M_{ij} = e$ , then  $M_{ji} = e$ .

**PROOF** This follows directly by left or right cancellation, and by commutativity of the elements with their inverse.  $\square$

### 1.3.2 Cyclic Groups

**Def'n. 1.3.6** The **order of an element**  $g \in G$  is  $o(g) := |\{g^d | d \in \mathbb{Z}\}|$ . The **order of a group**  $G$  is  $|G|$ .

We certainly have  $o(g) \leq |G|$  for any  $g \in G$ . Equality holds when  $o(g) = \infty$  and  $G$  is countable, or  $G = \{g^d : d \in \mathbb{Z}\}$ .

**Def'n. 1.3.7** A collection  $H = \{g_1, g_2, \dots, g_k\}$  **generates**  $G$  if we can write any  $g \in G$  as a product of elements in  $H$ .

**Def'n. 1.3.8** We say that  $G$  is **cyclic** if  $G = \{g^d : d \in \mathbb{Z}\}$  for some  $g \in G$ . Equivalently, it is generated by a set of cardinality one.

**Ex. 1.3.9** Note that  $\mathbb{Z}_{13}^\times$  is cyclic with generator 2.

**Lemma 1.3.10** If  $o(g)$  is finite and  $d \in \mathbb{Z}$ , then

$$o(g^d) = \frac{o(g)}{\gcd(o(g), d)}$$

**PROOF** Let  $o(g) = K$  and  $t = \gcd(K, d)$  and write  $K = tK_1$  and  $d = td_1$  with  $K_1, d_1$  coprime. Thus  $o(g^d)$  is the smallest positive integer  $l$  with  $(g^d)^l = 1$ . But then  $(g^d)^l = 1 \Leftrightarrow g^{dl} = 1 \Leftrightarrow o(g) | dl$  and  $k | dl$ , that is  $tK_1 | td_1 l$  and  $k_1 | d_1 l$ . Thus  $K_1 | l$  so the smallest positive integer  $l$  is  $K_1$  and  $o(g^d) = K_1 = \frac{o(g)}{\gcd(o(g), d)}$  as desired.  $\square$

### 1.3.3 Permutation Groups

Recall that  $S_n$  is the symmetric group of degree  $n$ , consisting of all permutations of  $[n]$ . Thus  $|S_n| = n!$ . Instead of using the matrix form, we can write the permutation group using the cycle form.

**Ex. 1.3.11** Write

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 3 & 1 & 2 & 9 & 8 & 5 & 6 \end{pmatrix} = (14)(2785)(3)(69)$$

We can also write  $(14)(2785)(69)$ , in other words excluding elements which map to themselves.

In general, a cycle  $(a_1 a_2 \dots a_k)$  indicates that  $a_1 f = a_2$ ,  $a_2 f = a_3, \dots, a_k f = a_1$ . In  $S_n$ , each permutation can be expressed in a cycle form (using disjoint cycles). The cycle form is unique up to ordering within the cycles, and ordering among the cycles.

**Ex. 1.3.12** In  $S_5$ , the possible cycle structures are

$$I, (ab), (abc), (abcd), (abcde), (ab)(cd), (ab)(cde)$$

We then have

$$\begin{aligned} o(I) &= 1 \\ o((ab)) &= 2 \\ o((abc)) &= 3 \\ o((abcd)) &= 4 \\ o((abcde)) &= 5 \\ o((ab)(cd)) &= 2 \\ o((ab)(cde)) &= 6 \end{aligned}$$

For  $f = (abc)$ ,  $f^2 = (abc)(abc) = (acb)$ ,  $f^3 = (abc)(acb) = abc$ . For  $f = (abcd)$ ,  $f^2 = (ac)(bd)$ ,  $f^3 = (abdc)(ac)(bd)(adcb)$ , and  $f^4 = (abcd)(adcb) = (abcd)$ .

If  $f = (a_1 a_2 \dots a_k)$ ,  $o(f) = k$ .

**Prop. 1.3.13** Suppose  $f = \gamma_1 \gamma_2 \dots \gamma_i$  for disjoint cycles. Then  $o(f) = \text{lcm}(o(\gamma_1), o(\gamma_2), \dots, o(\gamma_i))$ .

**PROOF** Note that the  $\gamma_i$  commute, so that

$$\begin{aligned} f^d = I &\Leftrightarrow (\gamma_1 \gamma_2 \dots \gamma_i)^d = I \\ &\Leftrightarrow \gamma_1^d \gamma_2^d \dots \gamma_i^d = I \\ &\Leftrightarrow \gamma_i^d = I \quad \forall i \end{aligned}$$

The last line holds since the  $\gamma_i^d$  operates on disjoint sets. Thus we have our formula, as desired.  $\square$



### 1.3.4 Dihedral Groups

Fix a regular polygon with  $n$  vertices. Let  $D_n$  be the collection of rigid motions with map the regular  $n$ -polygon to itself. Since  $r^n = 1$  and  $s^2 = 1$ , we have

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

Thus  $|D_n| = 2n$ . We can compute the operations on  $D_n$ :

$$r^a \cdot r^b = r^{a+b}$$

$$sr^a \cdot r^b = sr^{a+b}$$

$$r^a \cdot sr^b = sr^{b-a}$$

$$sr^a \cdot sr^b = r^{b-a}$$

Thus  $o(sr^a) = 2$  and  $o(r^a)$  is given by the usual formula.

## 1.4 Subgroups

**Def'n. 1.4.1** A subset  $H$  of a group  $G$  is called a **subgroup** if  $H$  is also a group with the same operation. We write  $H \leq G$ .

For example,  $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$ . Note that associativity automatically holds since every element of  $H$  is an element of  $G$ . Furthermore,  $1_H = 1_G$  since  $1_H 1_G = 1_H = 1_H 1_H$  where the first equality holds since  $1_G$  is an identity, and the second since  $1_H$  is an identity. As a result, inverses in  $H$  are inverses in  $G$ .

### 1.4.1 Subgroup Tests

**Prop. 1.4.2 (First Subgroup Test)** A subset  $H$  of a group  $G$  is a subgroup if and only if

1.  $H \neq \emptyset$
2.  $x, y \in H \Rightarrow xy \in H$
3.  $x \in H \Rightarrow x^{-1} \in H$

**PROOF** Follows by above discussion. □

**Prop. 1.4.3 (Second Subgroup Test)** A subset  $H$  of a group  $G$  is a subgroup

1.  $H \neq \emptyset$
2.  $x, y \in H \Rightarrow xy^{-1} \in H$

That the first subgroup test implies the second is obvious. Conversely, the identity is in  $H$  since  $xx^{-1} \in H$ . Thus get closure under inversion by choosing  $x$  as the identity to get inverses. Then if  $x, y \in H$ ,  $x, y^{-1} \in H$  so  $x(y^{-1})^{-1} = xy \in H$ .

Furthermore, if  $G$  is finite, it suffices to show closure under multiplication, since inverses can be obtained by repeated multiplication.

**Prop. 1.4.4** *Arbitrary intersections of subgroups are also subgroups.*

PROOF Obvious. □

**Ex. 1.4.5** 1.  $G \leq G, \{1\} \leq G$

2. For any  $g \in G$ , we have  $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$  is a subgroup.

3. For any  $g \in G$ , define

$$C_G(g) = \{x \in G : gx = xg\}$$

the centralizer of  $g$  in  $G$ . We certainly have  $1 \in C_G(g)$ . Also, if  $x, y \in G$ , then  $gx = xg$  and  $gy = yg$  so that  $gxy = xgy = xyg$ . If  $x \in C_G(g)$ , then  $gx = xg$  so  $g = xgx^{-1}$  and  $x^{-1}g = gx^{-1}$ .

4. The center of a group  $G$ :

$$Z(G) = \bigcap_{g \in G} C_G(g) \leq G$$

which is the set of elements commuting with everyone in  $G$ .

## 1.4.2 Cosets of Subgroups

**Def'n. 1.4.6** Let  $H \leq G$ ,  $g \in G$ . Then the **right coset** of  $H$  by  $g$  is the set  $Hg := \{hg : h \in H\}$ . Similarly, the **left coset** of  $H$  by  $g$  is the set  $gH := \{gh : h \in H\}$ .

**Ex. 1.4.7** Consider  $G = \mathbb{Z}_{13}^\times = \{1, 2, \dots, 12\}$  and  $H = \langle 3 \rangle = \{1, 3, 9\}$ . Then the cosets of  $H$  are given by

$H1 = \{1, 3, 9\}$	$H2 = \{2, 5, 6\}$
$H3 = H1$	$H4 = \{4, 10, 12\}$
$H5 = H2$	$H6 = H2$
$H7 = \{7, 8, 11\}$	$H8 = H7$
$H9 = H1$	$H10 = H4$
$H11 = H7$	$H12 = H4$

so there are 4 disjoint cosets of  $H$ .

This inspires the following theorem:

**Thm. 1.4.8** Let  $H \leq G$ . Then

1.  $|Hg| = |H|$
2.  $Hg = H \Leftrightarrow g \in H$
3. For any  $x, y \in G$ , either  $Hx = Hy$  or  $Hx \cap Hy = \emptyset$
4.  $Hx = Hy \Leftrightarrow xy^{-1} \in H$

PROOF 1. The map  $\cdot g : H \rightarrow Hg$  is bijective since it has an inverse.

2. This is a special case of (4) with  $x = g, y = 1$ .

3. Suppose  $Hx \cap Hy \neq \emptyset$ . Thus let  $z \in Hx \cap Hy$  and write  $z = h_1x = h_2y$ . Then for any  $hx \in Hx$ ,  $hx = hh_1^{-1}h_1x = hh_1^{-1}h_2y \in Hy$  so  $Hx \subseteq Hy$ . The identical argument works in reverse, so equality holds.
4. Assume  $Hx = Hy$ , and if  $x \in Hx$ , then  $x \in Hy$  so  $x = hy$  and  $xy^{-1} = h$ . Conversely, suppose  $xy^{-1} \in H$ , then  $xy^{-1}y \in Hy$  so  $x \in Hy$ . Also,  $x \in Hx$  so  $x \in Hx \cap Hy \neq \emptyset$  so by (3),  $Hx = Hy$ .  $\square$

**Def'n. 1.4.9** The **index** of a subgroup  $H$  in a group  $G$  is denoted  $|G : H|$  and denotes the number of distinct right cosets of  $H$ .

**Prop. 1.4.10**  $Hx \mapsto x^{-1}H$  is a one-to-one correspondence between right cosets and left cosets.

Thus  $G$  is a disjoint union of  $|G : H|$  right cosets of  $H$ , each of size  $|H|$ . Therefore we have

**Cor. 1.4.11**  $|G| = |G : H| \cdot |H|$

**Thm. 1.4.12 (Lagrange)** Suppose  $G$  is a finite group. Then

1. For any  $H \leq G$ ,  $|H| \mid |G|$ .
2. For any  $g \in G$ ,  $o(g) \mid |G|$ .

**PROOF** 1. Since  $|G| = |G : H| \cdot |H|$ ,  $|G : H|$  is a positive integer.

2.  $o(g) = |\langle g \rangle|$  and it follows by (1).  $\square$

### 1.4.3 Subgroups of Cyclic Groups

**Thm. 1.4.13** Any subgroup of a cyclic group is also cyclic.

**PROOF** Let  $G = \langle g \rangle$  be a cyclic group,  $H \leq G$ . If  $H = \{1\}$ , then  $H = \langle 1 \rangle$  is cyclic. Otherwise, there exists some  $0 \neq m \in \mathbb{Z}$  with  $g^m \in H$ . Now, there exists a smallest positive integer  $k$  with  $g^k \in H$ . We see that  $H = \langle g^k \rangle$ . The reverse inclusion is obvious since  $(g^k)^t \in H$  for all  $t \in \mathbb{Z}$ . For the forward inclusion, pick  $x \in H$  so  $x = g^d$  for some  $d$ . Then division with remainder yields  $d = tk + r$  with  $0 \leq r < k$  so that  $g^d = g^{tk+r}$  and  $x = (g^k)^t g^r$  so  $g^r = x(g^k)^{-t} \in H$ . Minimality of  $k$  forces  $r = 0$ , so  $d = tk$ ,  $x = g^d = (g^k)^t \in \langle g^k \rangle$ .  $\square$

If  $|G| = o(g) = n$  finite, write  $n = tk + r$ , for  $0 \leq r < k$ . Then  $g^r = g^n(g^k)^{-t} = (g^k)^{-t} \in H$ , and again  $r = 0$ ,  $n = tk$ ,  $k \mid n$ .

Now suppose  $G = \langle g \rangle$  with finite order  $n$ . Then  $G = \{1, g, g^2, \dots, g^{n-1}\}$ , and subgroups of  $G$  correspond to positive divisors of  $n$ . Then  $k \mid n \leftrightarrow \langle g^k \rangle = \{1, g^k, g^{2k}, \dots, g^{n-k}\}$ . Now suppose  $G = \langle g \rangle$  is infinite, and  $G = \{\dots, g^{-1}, 1, g, g^2, \dots\}$ . Then subgroups of  $G$  correspond to nonnegative integers, and  $k \geq 0 \leftrightarrow \langle g^k \rangle = \{\dots, g^{-k}, 1, g^k, g^{2k}, \dots\}$ .