

# **Course Notes**

## **Introduction to Abstract Algebra**

*Alex Rutar*

BSM Fall 2018

# Contents

<b>0</b>	<b>A Brief Introduction</b>	<b>3</b>
0.1	The group $\mathbb{Z}_m$ . . . . .	3
<b>1</b>	<b>Fundamentals of Groups</b>	<b>5</b>
1.1	Basics of Groups . . . . .	5
1.1.1	Order of an Element . . . . .	5
1.1.2	Group Morphisms . . . . .	6
1.2	Subgroups . . . . .	7
1.2.1	Subgroup Tests . . . . .	7
1.2.2	Cosets of Subgroups . . . . .	8
1.3	Factor Groups . . . . .	9
1.3.1	Normal Subgroups . . . . .	9
1.4	Group Actions . . . . .	10
1.4.1	Center of a Group . . . . .	10
1.5	Conjugacy Classes . . . . .	10
1.5.1	Group Homomorphisms . . . . .	13
1.6	Direct Products of Groups . . . . .	14
<b>2</b>	<b>Examples of Finite Groups and Rings</b>	<b>17</b>
2.1	Examples of Finite Groups . . . . .	17
2.1.1	Cyclic Groups . . . . .	17
2.1.2	Permutation Groups . . . . .	17
2.1.3	Dihedral Groups . . . . .	20



# Chapter 0

## A Brief Introduction

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

To construct  $\mathbb{Z}_m$ , we define  $\mathbb{Z}_m = \mathbb{Z} / \sim$  where  $a \sim b$  if  $a \cong b \pmod{m}$ . 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  $\overline{\cdot}$ . To show that this is a group, we must show that its operations are well defined.

**Prop. 0.1.1** We have  $\overline{a} + \overline{b} = \overline{a + b}$  and  $\overline{a} \cdot \overline{b} = \overline{ab}$ .

PROOF Obvious. □

**Thm. 0.1.2**  $\mathbb{Z}_m^\times = \{\overline{a} \mid \gcd(a, m) = 1\}$ .

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  $xa \cong 1 \pmod{m}$  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  $xa \cong 1 \pmod{m}$  and  $\overline{xa} = \overline{1}$  and  $\overline{x}\overline{a} = \overline{1}$  and we have our multiplicative inverse. □

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



# Chapter 1

## Fundamentals of Groups

### 1.1 Basics of Groups

**Def'n. 1.1.1** 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. 1.1.2** 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. 1.1.3** If  $ab = ba$  for all  $a, b \in G$  then we say that  $G$  is **commutative** or **abelian**.

#### 1.1.1 Order of an Element

One of the most basic properties of an element in a group is its order.

**Def'n. 1.1.4** The **order of an element**  $g \in G$  is  $o(g) := |\{g^d \mid d \in \mathbb{Z}\}|$ . 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  $G = \{g^d : d \in \mathbb{Z}\}$ . The second case is an example of a cyclic group.

**Def'n. 1.1.5** 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. 1.1.6** 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.

Note that cyclic groups are always abelian. We can also determine the order of powers of elements:

**Lemma 1.1.7** *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

$$\begin{aligned} (g^d)^l = 1 &\Leftrightarrow g^{dl} = 1 \Leftrightarrow o(g) | dl \\ &\Leftrightarrow K | dl \Leftrightarrow tK_1 | td_1 l \\ &\Leftrightarrow K_1 | d_1 l \end{aligned}$$

Since  $K_1$  and  $d_1$  are coprime, we must have  $K_1 | l$ . Thus by minimality of  $l$ , we have  $K_1 = l$  and  $o(g^d) = K_1 = \frac{o(g)}{\gcd(o(g), d)}$  as desired.  $\square$

## 1.1.2 Group Morphisms

**Def'n. 1.1.8** *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. 1.1.9** *In each column or row, each element occurs exactly once. Furthermore, if  $M_{ij} = e$ , then  $M_{ji} = e$ .*

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

**Def'n. 1.1.10** *Let  $(G, *)$ ,  $(H, \star)$  be groups. A mapping  $f : G \rightarrow H$  is called an **homomorphism** if*

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

*If  $f$  is also a bijection, then we call  $f$  an **isomorphism**. If  $(G, *) = (H, \star)$ , then we call  $f$  an **endomorphism**. If  $f$  is a bijective endomorphism, then  $f$  is an **automorphism**.*

Note that  $G$  and  $H$  are isomorphic if and only if their Cayley tables are the same up to permutation of elements. Given a group  $G$ , define  $\text{Aut}(G)$  as the set of all automorphisms of a group with composition as an operation.

**Prop. 1.1.11**  *$\text{Aut}(G)$  is a group.*

**PROOF** 1. By properties of functions, composition is associative.

2. Consider the map  $1(x) = x$ . This map is an automorphism since  $1(x * y) = x * y = 1(x) * 1(y)$ , and it is the identity function.

3. For any  $f$ , since  $f$  is bijective, it has an inverse  $f^{-1}$ . Let  $x, y \in G$ ; then  $x = f(u)$  and  $y = f(v)$  by surjectivity. Thus  $f^{-1}(x * y) = f^{-1}(f(u) * f(v)) = f^{-1}(f(u * v)) = u * v = f^{-1}(x) * f^{-1}(y)$  since  $f$  is an automorphism.  $\square$

**Prop. 1.1.12** *Let  $G$  be a cyclic group and  $H$  be an arbitrary group. Then  $G$  and  $H$  are isomorphic if and only if  $H$  is cyclic and  $|H| = |G|$ .*

**PROOF** First suppose  $G$  and  $H$  are isomorphic via  $f$ . We certainly have  $|H| = |G|$  since  $f$  is a bijection and preserves cardinality. Let  $g$  be a generator  $G$ ; I claim that  $f(g)$  is a generator for  $H$ . Write  $G = \{g^n \mid n \in \mathbb{N}\}$ , and for any  $x \in G$ , there exists some  $n$  so  $g^n = x$ . Then for any  $y \in H$ , there exists some  $n$  so that  $y = f(g^n) = f(g)^n$  since  $f$  preserves the group structure.

Conversely, suppose  $H$  is a cyclic group and  $|H| = |G|$ . Let  $g$  be a generator for  $G$  and  $h$  be a generator for  $H$ . For any  $x \in G$ , there exists a minimal  $n$  so  $x = g^n$ ; and define  $f(x) = h^n$ . Such an  $n$  must be unique by minimality. Let's see that  $f$  is well-defined and injective. Let  $x, y \in G$  be arbitrary; by uniqueness

$$\begin{aligned} x = y &\Leftrightarrow x = y = g^n \\ &\Leftrightarrow f(x) = f(y) = h^n \end{aligned}$$

as required. As well,  $f$  is surjective: if  $x = h^n$ , then  $x = f(g^n)$ ; thus  $f$  is a bijection. To see that  $f$  respects the group structure, let  $g^u, g^v \in G$  be arbitrary. Then  $f(g^u g^v) = f(g^{u+v}) = h^{u+v} = h^u h^v = f(g^u) f(g^v)$  as desired.  $\square$

## 1.2 Subgroups

**Def'n. 1.2.1** 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  $G$ .

### 1.2.1 Subgroup Tests

**Prop. 1.2.2 (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.  $x \in H \Rightarrow x^{-1} \in H$

If  $G$  is finite, it suffices to verify (1) and (2).

**PROOF** Associativity follows since elements of  $H$  are elements of  $G$ . Since  $H \neq \emptyset$ ,  $x \in H$ , so  $x^{-1} \in H$  and  $1 = xx^{-1} \in H$ , so  $H$  contains the identity (which, by uniqueness, is the identity in  $G$ ). It is clearly closed under multiplication by (2), and contains inverses by (3). In the finite case, for any  $x \in H$ , there exists some  $n$  so  $x^n = 1$  and  $x^{n-1}x = xx^{n-1} = 1$ , so  $x^{-1} = x^{n-1}$  can be obtained by closure under multiplication.  $\square$

**Prop. 1.2.3 (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  $x(y^{-1})^{-1} = xy \in H$ .

We have the following proposition. The proof is straightforward but it is a good illustration of the first subgroup test.

**Prop. 1.2.4** *Arbitrary intersections of subgroups are also subgroups.*

**PROOF** Let  $\{H_i\}_{i \in I}$ ,  $H_i \leq G$  be an arbitrary collection of subgroups of  $G$ , and define  $H = \bigcap_{i \in I} H_i$ .

We certainly have  $1 \in H$ , so  $H \neq \emptyset$ . If  $x \in H$ , then  $x \in H_i$  for all  $i$ , so  $x^{-1} \in H_i$  for all  $i$ , so  $x^{-1} \in H$ . If  $x, y \in H$ , then  $x, y \in H_i$  for all  $i$  and  $xy \in H_i$ , so  $xy \in H$ .  $\square$

**Thm. 1.2.5** *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. Since  $G$  is cyclic, there exists some minimal  $k \neq 0$  so that  $g^k \in H$ . We will see that  $H = \langle g^k \rangle$ . It is clear that  $\langle g^k \rangle \subseteq H$ ; we show the reverse inclusion.

Let  $x \in H$  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  $d = tk$ ,  $x = g^d = (g^k)^t \in \langle g^k \rangle$ .  $\square$

## 1.2.2 Cosets of Subgroups

**Def'n. 1.2.6** 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  $gH := \{gh : h \in H\}$ .

We have the following theorem about cosets:

**Thm. 1.2.7** 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  $z \in Hx \cap Hy$  so we can 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 let  $x \in Hx$ . Then  $x \in Hy$  as well so  $x = hy$  and  $xy^{-1} = h \in H$ . 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),  $Hx = Hy$ .  $\square$

Thus all the cosets of  $H$  have the same size as  $H$ , and cosets with different elements are disjoint. Therefore the following definition makes sense:

**Def'n. 1.2.8** The **index** of a subgroup  $H$  in a group  $G$  is denoted  $[G : H]$  and denotes the number of distinct right cosets of  $H$ .

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

**Cor. 1.2.9**  $|G| = [G : H] \cdot |H|$

We also have the following theorem:

**Prop. 1.2.10**  $Hx \mapsto x^{-1}H$  is a one-to-one correspondence between right cosets and left cosets.

As an application of the previous results, we have the following theorem.

**Thm. 1.2.11 (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. This follows since  $|G| = [G : H] \cdot |H|$  and  $[G : H]$  is a positive integer.

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

## 1.3 Factor Groups

### 1.3.1 Normal Subgroups

**Def'n. 1.3.1** Let  $H \leq G$ . Then we say  $H$  is a **normal subgroup** of  $G$  and write  $H \triangleleft G$  if  $Hx = xH$  for all  $x \in G$ .

**Def'n. 1.3.2** The **normalizer** of a subgroup  $H$  in  $G$  is

$$N_G(H) = \{x \in G : Hx = xH\} = \{x \in G : x^{-1}Hx = H\} \leq G$$

First note that  $H \leq N_G(H)$ . For any  $x \in H$ ,  $Hx = xH$  since  $H$  is a subgroup. Here are some properties of normal subgroups and normalizers.

- Prop. 1.3.3**
1.  $H \leq N_G(H)$ .
  2.  $N_G(H) = G$  iff  $H$  is normal.

**PROOF** 1. For any  $x \in H$ ,  $Hx = xH$  since  $H$  is a subgroup, so  $H \subseteq N_G(H)$ . Since they are both groups, we have  $H \leq N_G(H)$ .

2. This follows directly from the definition. □

We have the following characterization of normality for subgroups of  $G$ .

**Prop. 1.3.4** A subgroup  $H$  in  $G$  is normal if and only if

1.  $Hx = xH$  for all  $x \in G$ .

2.  $x^{-1}Hx = H$  for all  $x \in G$ .
3.  $N_G(H) = G$ .
4. For any  $h \in H$ ,  $x \in G$ ,  $x^{-1}hx \in H$ .
5.  $H$  is a union of some conjugacy classes.

PROOF We only see (4)  $\Leftrightarrow$  (5). We have

$$\forall h \in H \forall x \in G x^{-1}hx \in H \Leftrightarrow \forall h \in H C_h \subseteq H$$

which means that all conjugacy classes are either disjoint from  $H$ , or in  $H$ .  $\square$

We will most commonly use condition (4) to check normality.

## 1.4 Group Actions

### 1.4.1 Center of a Group

**Def'n. 1.4.1** For any  $g \in G$ , define

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

the **centralizer** of  $g$  in  $G$ . Then define the **center** of a group  $G$

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

Note that the center of a group is the set of elements which commute with everything in the group. These are indeed groups: 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  $x^{-1}g = gx^{-1}$ .

## 1.5 Conjugacy Classes

This definition inspires the following definition:

**Def'n. 1.5.1** We say that  $f$  is a **conjugate** of  $g$  if and only if there exists  $x \in G$  such that  $x^{-1}gx = f$ .

Denote the binary relation by  $\sim$ : we will show that this is an equivalence relation:

1. Reflexive:  $g \sim g$  by  $x = 1$
2. Symmetric: If  $g \sim f$ , then  $x^{-1}gx = f$  so  $g = xfx^{-1} = (x^{-1})^{-1}fx^{-1}$
3. Transitive: If  $f \sim g$  and  $g \sim h$ , get  $x, y$  so  $x^{-1}gx = f$  and  $y^{-1}fy = h$  so

$$h = y^{-1}x^{-1}gxy = (xy)^{-1}g(xy)$$

**Def'n. 1.5.2** These equivalence classes are called the **conjugacy classes** of  $G$ .

We denote the conjugacy class of  $g \in G$  by  $C_g = \{x^{-1}gx : x \in G\}$ . Note that  $|C_g| = 1$  if and only if  $C_g = \{g\}$  if and only if  $x^{-1}gx = g$  for any  $x \in G$  if and only if  $gx = xg$  and  $g \in Z(G)$ .

**Thm. 1.5.3** For any  $g \in G$ ,  $|C_g| \cdot |C_G(g)| = |G|$ .

PROOF Consider  $\alpha : \{\text{Right cosets of } D_G(g)\} \rightarrow C_g$  defined by  $C_G(g) \cdot x \mapsto x^{-1}gx$ . This is well defined and injective:

$$\begin{aligned} C_G(g)x = C_G(g)y &\Leftrightarrow xy^{-1} \in C_G(g) \\ &\Leftrightarrow g(xy^{-1}) \\ &\Leftrightarrow (xy^{-1})g \end{aligned}$$

so it suffices to show the map is surjective. In fact, any element of  $C_g$  is of the form  $x^{-1}gx = \alpha(C_G(g)x)$ . Thus  $\alpha$  is bijective, so  $|G : C_G(g)| = |C_g|$  and

$$|G| = |G : C_G(g)| \cdot |C_G(g)| = |C_g| \cdot |C_G(g)|$$

□

**Cor. 1.5.4** If  $G$  is finite,  $g \in G$ , then  $|C_g| \mid |G|$ .

We have the following nice application:

**Thm. 1.5.5** If  $|G| = p^2$  for  $p$  prime, then  $G$  is commutative.

PROOF For any  $g \in G$ ,  $|C_g| \mid |G| = p^2$  so  $|C_g|$  there are three cases. Note that  $|C_g| = p^2$  is impossible, since  $C_1 = \{1\}$  and the remainder has fewer elements. Thus let  $a$  denote the number of conjugacy classes of size 1 by  $a$ , and the number of conjugacy classes of size  $p$  by  $b$ . Since  $G$  is a disjoint union of conjugacy classes, we have  $|G| = p^2 = a + bp$  so that  $p \mid a$ . Furthermore,  $a \neq 0$  since  $|C_1| = 1$ , so  $a \geq p$ . Furthermore,  $|C_g| = 1$  if and only if  $g \in Z(G)$ , so  $a = |Z(G)| \geq p$ . Since  $Z(G) \leq G$ , by Lagrange,  $|Z(G)| \mid |G| = p^2$ , so  $|Z(G)| = p$  or  $|Z(G)| = p^2$ . If  $|Z(G)| = p$ , pick any  $x \in G$  with  $x \notin Z(G)$  and consider  $C_G(x)$ . Since  $Z(G) \leq C_G(x)$ , we must have  $p + 1 \leq |C_G(x)|$  and  $|C_G(x)| = p^2$  so  $C_G(x) = G$  and  $x \in Z(G)$ , a contradiction. Thus  $|Z(G)| = p^2$  and the group is commutative. □

Note that if  $|G| = p$  prime, then  $G$  is cyclic. Since  $o(g) \mid |G| = p$ , and  $o(g) \neq 1$  if  $g \neq 1$ ; we must have  $o(g) = p$  and  $\langle g \rangle = G$ .

Now if  $H \leq G$ , then  $x^{-1}Hx = \{x^{-1}hx : h \in H\} \leq G$ , as can be verified.

**Def'n. 1.5.6** A subgroup  $K$  of  $G$  is **conjugate** to  $H$  in  $G$  if and only if there exists  $x \in G$  with  $x^{-1}Hx = K$ . We write  $H \sim K$ , and the equivalence classes are called **conjugacy classes** of subgroups.

**Thm. 1.5.7** 1. Conjugate elements are of the same order.

2. Conjugate subgroups are isomorphic.

PROOF 1. We have

$$\begin{aligned} (x^{-1}gx)^k = 1 &\Leftrightarrow (x^{-1}gx)(x^{-1}gx) \cdots (x^{-1}gx) = 1 \\ &\Leftrightarrow x^{-1}g^kx = 1 \\ &\Leftrightarrow g^kx = x \\ &\Leftrightarrow g^k = 1 \end{aligned}$$

2. I claim that the map  $\alpha : H \rightarrow x^{-1}Hx$  by  $h \mapsto x^{-1}hx$  is an isomorphism. We have  $\alpha(h_1h_2) = x^{-1}h_1h_2x = x^{-1}h_1xx^{-1}h_2x = \alpha(h_1)\alpha(h_2)$ , and bijectivity can be verified easily.  $\square$

For any group  $G$ , we always have  $C_{\{1\}} = \{\{1\}\}$  and  $C_G = \{G\}$ . A particularly nice type of conjugacy class are the ones with only 1 element. We have

$$|C_H| = 1 \Leftrightarrow C_H = \{H\} \Leftrightarrow x^{-1}Hx = H (\forall x \in G) \Leftrightarrow Hx = xH (\forall x \in G)$$

**Def'n. 1.5.8** A subgroup  $H$  which satisfies  $Hx = xH$  for all  $x \in G$  is called a **normal** subgroup. We say  $H \triangleleft G$ .

**Def'n. 1.5.9** The **centralizer** of a subgroup  $H$  in  $G$  is

$$C_G(H) = \{x \in G : hx = xh (\forall h \in H)\} = \bigcap_{h \in H} C_G(h) \leq G$$

Note that intersections of subgroups are subgroups.

**Def'n. 1.5.10** The **normalizer** of a subgroup  $H$  in  $G$  is

$$N_G(H) = \{x \in G : Hx = xH\} = \{x \in G : x^{-1}Hx = H\} \leq G$$

It is easy to verify this is a subgroup. We thus have  $H \triangleleft G$  if and only if  $N_G(H) = G$ . We have some properties:

**Ex. 1.5.11** For example, fix  $G = GL_n(\mathbb{R})$ , so  $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}$ . This is indeed a subgroup: let's also verify that it is a normal subgroup. Also, if  $h \in SL_n(\mathbb{R})$  and  $x \in GL_n(\mathbb{R})$ , then  $\det(x^{-1}hx) = \det(x^{-1})\det(h)\det(x) = \det(h) = 1$  so  $x^{-1}hx \in SL_n(\mathbb{R})$ .

Why are normal subgroups nice? If  $H \triangleleft G$ , and  $x, y \in G$ , then  $(Hx)(Hy) = Hxy$ . We thus have an operation on cosets of  $H$ . Furthermore, this action satisfies the properties of the group. Thus  $\{Hx : x \in G\}$  with the operation  $HxHy = Hxy$  is a group, called the factor group or quotient group of  $G$  by  $H$ .

**Ex. 1.5.12** Consider  $G = \mathbb{Z}_{13}^\times$ ,  $H = \langle 3 \rangle$ . Then  $H2 = \{256\}$ ,  $H4 = \{4, 10, 12\}$ ,  $H7 = \{7, 8, 11\}$ . We

	H	H2	H4	H7
	H	H2	H4	H7
have	H2	H2	H4	H7
	H4	H4	H7	H
	H7	H7	H	H2

**Prop. 1.5.13** 1. Index 2 subgroups are normal.

2. Any subgroup of a commutative group is normal.

3. Any subgroup of the center is normal.

4. If  $H \leq G$ ,  $|H| = K$  and  $H$  is the only subgroup of  $G$  of size  $K$ , then  $H \triangleleft G$ .

**PROOF** 1. If  $H \leq G$  with  $[G : H] = 2$ , we know  $g^2 \in H$  for all  $g \in G$ . Then for  $h \in H$ ,  $x \in G$ ,  $x^{-1}hx = x^{-2}xhxhh^{-1} = (x^{-1})^2(xh)^2h^{-1} \in H$ .

2. If  $H \leq G$ ,  $G$  commutative, if  $h \in H$  and  $x \in G$ , then  $hx = xh$  and  $x^{-1}hx = h \in H$ .

3. Elements of the center commute with everything.

4. For any  $x \in G$ ,  $x^{-1}Hx \leq G$  and  $|x^{-1}Hx| = |H|$  so  $x^{-1}Hx = H$   $\square$

### 1.5.1 Group Homomorphisms

**Def'n. 1.5.14** A map  $\alpha : G \rightarrow H$  is called a **homomorphism** (of groups) iff  $\alpha(xy) = \alpha(x)\alpha(y)$  for every  $x, y \in G$ .

Homomorphisms are isomorphisms that are not (necessarily) bijective.

**Ex. 1.5.15** 1. The identity map ( $g \mapsto g$ ), the constant identity map ( $g \mapsto 1$ ).

2. The map  $\alpha : \mathbb{C}^\times \rightarrow \mathbb{R}^\times$  given by  $z \mapsto |z|$ .

3. The map  $\alpha : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$  by  $A \mapsto \det(A)$ , since  $\det(AB) = \det(A)\det(B)$ .

4. If  $H \triangleleft G$ , the map  $\alpha : G \rightarrow G/H$  by  $x \mapsto Hx$ .

For a homomorphism  $\alpha : G \rightarrow H$  of groups, we have the following properties.

**Prop. 1.5.16** 1.  $\alpha(1_G) = 1_H$

2.  $\alpha(g^{-1}) = \alpha(g)^{-1}$

3.  $\alpha(g^k) = \alpha(g)^k$  for any  $k \in \mathbb{Z}$ .

**PROOF** 1.  $1_H \alpha(1_G) = \alpha(1_G) = \alpha(1_G 1_G) = \alpha(1_G) \alpha(1_G)$

2.  $\alpha(g) \alpha(g^{-1}) = \alpha(gg^{-1}) = \alpha(1_G) = 1_H$ , so they are inverses.

3. Follows directly by above and induction. □

**Def'n. 1.5.17** The **image** of  $\alpha$  is given by  $\text{im}(\alpha) = \{\alpha(g) : g \in G\} \leq H$ .

The image of  $\alpha$  is a subgroup since it is a subgroup. We also define

**Def'n. 1.5.18** The **kernel** of  $\alpha$  is given by  $\ker(\alpha) = \{x \in G : \alpha(x) = 1_H\} \trianglelefteq G$ .

To see it is a normal subgroup, we have  $1_G \in \ker(\alpha)$ , and it is certainly a subgroup. Then by the normality test, if  $x \in \ker(\alpha)$  and  $g \in G$ , then

$$\begin{aligned} \alpha(g^{-1}xg) &= \alpha(g^{-1})\alpha(x)\alpha(g) \\ &= \alpha(g^{-1})\alpha(g) \\ &= \alpha(1_G) \\ &= 1_H \end{aligned}$$

so  $g^{-1}xg \in \ker(\alpha)$  as well.

**Thm. 1.5.19 (First Isomorphism)** For a homomorphism  $\alpha : G \rightarrow H$ ,  $G/\ker(\alpha) \cong \text{im}(\alpha)$ .

**PROOF** Consider the map  $\beta : G/\ker(\alpha) \rightarrow \text{im}(\alpha)$  given by  $\ker(\alpha)x \mapsto \alpha(x)$ .

This map is well defined and injective: we have

$$\begin{aligned}\ker(\alpha)x = \ker(\alpha)y &\Leftrightarrow xy^{-1} \in \ker(\alpha) \\ &\Leftrightarrow \alpha(xy^{-1}) = 1 \\ &\Leftrightarrow \alpha(x)\alpha(y)^{-1} = 1 \\ &\Leftrightarrow \alpha(x) = \alpha(y)\end{aligned}$$

It is also surjective since any element of  $\text{im}(\alpha)$  is of the form  $\alpha(x)$ , which is the image of  $\beta(\ker(\alpha)x)$ . Finally,

$$\begin{aligned}\beta((\ker(\alpha)x)(\ker(\alpha)y)) &= \beta(\ker(\alpha)xy) \\ &= \alpha(xy) \\ &= \alpha(x)\alpha(y) \\ &= \beta(\ker(\alpha)x)\beta(\ker(\alpha)y)\end{aligned}$$

so  $\beta$  is a bijective homomorphism, which is an isomorphism.  $\square$

**Ex. 1.5.20** Consider the map  $\alpha : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$  given by  $A \mapsto \det(A)$ . We have  $\text{im}(\alpha) = \mathbb{R}^\times$  and  $\ker(\alpha) = \text{SL}_n(\mathbb{R})$ , so  $\text{SL}_n(\mathbb{R}) \trianglelefteq \text{GL}_n(\mathbb{R})$ .

**Thm. 1.5.21** Let  $\mathcal{N}$  denote the set of normal subgroups of  $G$ . For any group  $G$ , the set of normal subgroups of  $G$  is equal to the collection of kernels of homomorphisms of  $G$ , and the factor groups of  $G$  are the images of homomorphisms of  $G$ .

**PROOF** We know  $\ker(\alpha) \trianglelefteq G$  for all homomorphisms  $\alpha : G \rightarrow H$ . Conversely, for  $N \trianglelefteq G$ , consider  $\alpha : G \rightarrow G/N$  by  $g \mapsto Ng$ . Then  $\text{im}(\alpha) = \{Ng : g \in G\} = G/N$ , and  $\ker(\alpha) = \{g \in G : Ng = N\} = N$ . This also shows that any factor group is the image of a homomorphism. Conversely, for any  $\alpha : G \rightarrow H$ , and  $\text{im}(\alpha) \cong G/\ker(\alpha)$  by the first isomorphism theorem.  $\square$

## 1.6 Direct Products of Groups

**Def'n. 1.6.1** For groups  $A, B$ , the **direct product group** is the group with set  $A \times B$  and operation  $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$ .

Define an operation  $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2)$ . We have some obvious basic properties:

1.  $1_{A \times B} = (1_A, 1_B)$
2.  $(a, b)^{-1} = (a^{-1}, b^{-1})$
3.  $|A \times B| = |A| \cdot |B|$ .
4.  $o(a, b) = (o(a), o(b))$
5.  $A, B$  are commutative if and only if  $A \times B$  is commutative

6.  $A \times B$  is cyclic if and only if  $A, B$  are both cyclic with coprime order. Note that  $A \times B$  is cyclic if and only if there exists  $(a, b)$  generates  $A \times B$ , so  $|A \times B| = o(a, b)$ . But also  $|A| \cdot |B| = |A \times B| = o(a, b) = (o(a), o(b)) \leq o(a) \cdot o(b) \leq |A| \cdot |B|$ , so equality must hold. Thus  $(o(a), o(b)) = o(a)o(b)$ ; and  $o(a) = |A|$ ,  $o(b) = |B|$ .
7.  $C_k \times C_l \cong C_{kl} \iff \gcd(k, l) = 1$ .
8.  $\bar{A} = \{(a, 1) | a \in A\} \leq A \times B$ ;  $A \cong \bar{A}$ .  $\bar{B} = \{(1, b) | b \in B\} \leq A \times B$ ;  $B \cong \bar{B}$ . Then  $\bar{A} \cdot \bar{B} = A \times B$  since  $\bar{A} \cap \bar{B} = \{1_{A \times B}\}$ .
9. Define projection maps  $\pi_A, \pi_B$  by  $(a, b) \mapsto a$  and  $(a, b) \mapsto b$  respectively. Then  $\text{im}(\pi_A) = A$ ,  $\ker(\pi_A) = \bar{B}$ ,  $\text{im}(\pi_B) = B$ ,  $\ker(\pi_B) = \bar{A}$ . Thus  $\bar{A}, \bar{B} \trianglelefteq A \times B$ .

**Thm. 1.6.2** Suppose  $M, N \trianglelefteq G$  with  $M \cap N = \{1\}$  and  $M \cdot N = G$ . Then  $G \cong M \times N$ .

PROOF We first see that  $mn = nm$  for all  $m \in M, n \in N$ . Consider  $[m, n] = (m^{-1}n^{-1}m)n \in N$  since  $N$  is normal. As well,  $[m, n] = m^{-1}(n^{-1}mn) \in M$  since  $M$  is normal. Thus  $m^{-1}n^{-1}mn = 1$  so  $m, n$  commute.

Now consider  $\alpha : M \times N \rightarrow G$  by  $(m, n) \mapsto mn$ .  $\alpha$  is onto since  $\text{im}(\alpha) = MN = G$ , and injective since if  $m_1n_1 = m_2n_2$ , then  $m_2^{-1}m_1 = n_2n_1^{-1} = 1$  so  $m_1 = m_2$  and  $n_1 = n_2$ . Finally, we have

$$\begin{aligned} \alpha((m_1, n_1)(m_2, n_2)) &= \alpha(m_1m_2, n_1n_2) \\ &= m_1m_2n_1n_2 \\ &= m_1n_1m_2n_2 \\ &= \alpha((m_1, n_1))\alpha((m_2, n_2)) \end{aligned}$$

so  $\alpha$  is an isomorphism. □

Furthermore, if  $G$  is finite, it suffices to require  $|M| \cdot |N| = |G|$ . This follows since  $|M \cdot N| = \{m \cdot n | m \in M, n \in N\}$  must have distinct elements. Then  $|M \cdot N| = |G|$ , so  $MN = G$ .

**Thm. 1.6.3** If  $|G| = p^2$ ,  $p$  prime, then

PROOF Suppose  $|G| = p^2$ . Then for any  $g \in G$ , by Lagrange,  $o(g) \in \{1, p, p^2\}$ . If  $o(g) = p^2$  then  $G$  is cyclic. Pick any  $1 \neq x \in G$ , and let  $M = \langle x \rangle$ . Similarly, get  $N = \langle y \rangle$  for  $y \notin M$ . Then  $M \cap N \trianglelefteq N$ , so by Lagrange,  $M \cap N = \{1\}$ . Furthermore,  $M, N$  are normal subgroups, so  $G \cong M \times N \cong C_p \times C_p$ . □

**Thm. 1.6.4 (Fundamental Theorem of Finite Abelian Groups)** Any finite commutative group is isomorphic to a direct product of cyclic groups.

**Thm. 1.6.5** If  $G$  is finite,  $p$  prime, and  $p || |G|$ , then there exists  $g \in G$  with  $o(g) = p$ .

PROOF Consider  $T = \{(g_1, g_2, \dots, g_p) : g_1g_2 \cdots g_p = 1\}$ . Note that  $|T| = |G|^{p-1}$  since we can choose  $g_1, g_2, \dots, g_{p-1}$  arbitrarily and  $g_p$  is uniquely determined. Thus  $p || |T|$ . Now define  $\alpha : T \rightarrow T$  by  $(g_1, g_2, \dots, g_p) \mapsto (g_2, g_3, \dots, g_p, g_1)$ . Since  $\alpha$  also has an inverse, it is a permutation  $\alpha \in S_T$ . As well,  $\alpha^p = 1_T$ , so  $o(\alpha) | p$  and the cycle form of  $\alpha$  is composed of fixed points and  $p$ -cycles. Thus  $|T|$  is given by the number of fixed points of  $\alpha$  plus  $p$  times the number of  $p$ -cycles of  $\alpha$ . Then since  $p || |T|$ ,  $p$  divides the number of fixed points of  $\alpha$ . The fixed points of  $\alpha$  are the elements of the form  $(g, g, \dots, g)$ ; plus there are a non-zero number of fixed points since  $(1, 1, \dots, 1)$  is a fixed point. Thus there exists some  $(g, g, \dots, g) \in T$  with  $g \neq 1$ , so  $g^p = 1$  and  $o(g) \neq 1$ , so  $o(g) = p$ . □



In fact, this shows that  $|\{g \in G : g^p = 1\}| = 0 \pmod{p}$ .

**Thm. 1.6.6** Suppose  $|G| = pq$ , with  $p < q$  primes, and assume  $q \not\equiv 1 \pmod{p}$ . Then  $G \cong C_{pq}$ .

PROOF By Lagrange,  $o(g)$  can be  $1, p, q, pq$ . By Cauchy, there exists  $x, y \in G$  so that  $o(x) = p$ ,  $o(y) = q$ . Now consider  $H \leq G$ , so  $H = \{1\}$ ,  $H \cong C_p$ ,  $H \cong C_q$ , or  $H = G$ .

Since  $|C_g| \mid |G|$ , we have  $|C_g| \cdot |C_G(g)| = |G|$ . So  $|C_g| = 1$  or  $p$  or  $q$ .

By Cauchy, get  $o(x) = p$ ,  $o(y) = q$  and let  $A = \langle x \rangle$ ,  $B = \langle y \rangle$ . If  $C \leq G$ , then  $|C| = q$ ,  $C \cong C_q$ ,  $C = \langle z \rangle$  cyclic.  $BG$ , and it is the only subgroup of order  $q$  in  $G$ : if  $C \leq G$  and  $|C| = q$ , then  $C = 1, z, z^2, \dots, z^{q-1}$ . Since  $p < q$ ,  $B, Bz, \dots, Bz^{q-1}$  is a set of  $q$  cosets, so some of them must overlap, say  $Bz^a = Bz^b$ . Then  $z^{b-a} \neq 1$  and  $z^{b-a} \in C$ , so  $\{1\} \neq B \cap C \leq B$ . Then  $|B \cap C| = q$  by Lagrange and  $|B \cap C| = |B|$  so  $B = C$ . Since  $BG$  (since it is the only subgroup of order  $q$ ),  $B$  is a union of some conjugacy classes of size 1 or  $p$ . Let  $m$  denote the number of conjugacy classes of size 1, so  $m = |B \cap Z(G)|$ , so  $m|B| = q$  so  $m = q$ . Thus there are at least 2 conjugacy classes of size 1, so there exists  $1 \neq w \in B$  with  $|C_w| = 1$  and  $w \in Z(G)$ . Thus  $|Z(G) \cap B| > 1$ , so  $Z(G) \cap B = B$  so  $B \leq Z(G)$ .

Recall that  $B = \langle x \rangle$ ,  $A = \langle x \rangle$  and  $o(y) = q$  and  $o(x) = p$ , so  $x \notin B$ . Consider  $C_G(x)$ .  $Z(G) \leq C_G(x)$ , so  $B \leq C_G(x)$ , and since powers of  $x$  commute with  $x$ ,  $A \leq C_G(x)$ . Then  $q|C_G(x)$  and  $p|C_G(x)$ , so  $|C_G(x)| = pq$ . Thus  $C_G(x) = G$  so  $x \in Z(G)$ . Thus  $Z(G) = G$ .

Now  $A \trianglelefteq G$  and  $B \trianglelefteq G$ ,  $A \cap B = \{1\}$  by Lagrange, and  $|A| \cdot |B| = |G|$ . Thus  $G \cong A \times B = C_p \times C_q \cong C_{pq}$ .  $\square$

**Thm. 1.6.7 (First Sylow)** If  $G$  is a finite group and  $p^d \mid |G|$  for  $p$  prime, then there exists  $H \leq G$  with  $|H| = p^d$ .

If  $d$  is maximal, then  $H$  is called a Sylow  $p$ -subgroup of  $G$ . We say  $\text{Syl}_p(G) = \{H \leq G : |H| = p^d\}$ .

**Ex. 1.6.8** Consider  $|D_6| = 12$ . Then

$$\text{Syl}_2(G) = \{\{1, r^3, s, sr^3\}, \{1, r^3, sr, sr^4\}, \{1, r^3, sr^2, sr^5\}\}$$

and

$$\text{Syl}_3(G) = \{\{1, r^2, r^4\}\}$$

# Chapter 2

## Examples of Finite Groups and Rings

### 2.1 Examples of Finite Groups

#### 2.1.1 Cyclic Groups

**Ex. 2.1.1** Consider  $G = \mathbb{Z}_{13}^\times = \langle 2 \rangle$ ,  $|\mathbb{Z}_{13}^\times| = 12 = o(2)$ .

Divisor of 12	Subgroup of $\mathbb{Z}_{13}^\times$
1	$\langle 2^1 \rangle = \langle 2 \rangle = \mathbb{Z}_{13}^\times$
1	$\langle 2^2 \rangle = \langle 4 \rangle = \{1, 4, 3, 12, 9, 10\}$
1	$\langle 2^3 \rangle = \langle 8 \rangle = \{1, 8, 12, 5\}$
1	$\langle 2^4 \rangle = \langle 3 \rangle = \{1, 3, 9\}$
1	$\langle 2^6 \rangle = \langle 12 \rangle = \{1, 12\}$
1	$\langle 2^{12} \rangle = \langle 1 \rangle = \{1\}$

#### 2.1.2 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. 2.1.2** 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. 2.1.3** 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. 2.1.4** 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.  $\square$

Note that any finite permutation of  $f \in S_n$  can be expressed as a composition of 2-cycles. For example,  $(abc) = (ab)(ac)$  and in general  $(a_1 a_2 \dots a_k) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_k)$ . In general, any  $k$ -cycle can be replaced by a composition of  $(k - 1)$  2-cycles. This motivates the following definition:

**Def'n. 2.1.5** A permutation  $f \in S_n$  is **even** if it can be expressed as a composition of an even number of 2-cycles. Then  $f \in S_n$  is **odd** if it can be expressed as a composition of an odd number of 2-cycles.

For example,  $(15362)(4798) = (15)(13)(16)(12)(47)(49)(48)$  can be written as a composition of 7 2-cycles. This is certainly not unique: for example  $(26) = (21)(16)(21)$ .

**Lemma 2.1.6** The identity permutation is not odd.

PROOF For contradiction, assume

$$I = \alpha_1 \alpha_2 \dots \alpha_k$$

and assume that such an odd  $k$  is a minimal counterexample. We certainly have  $k \geq 3$ . Say  $\alpha_1 = (cd)$ , so  $c$  must be involved in another  $\alpha_i$ , or  $d$  is mapped to  $c$ . Let  $\alpha_r$  be the last 2-cycle involving  $c$ , say  $\alpha_r = (cx)$ . Now we rewrite  $\alpha_{r-1}$  without changing  $\alpha_{r-1} \alpha_r$ .

1. If  $\alpha_{r-1} = (yz)$  disjoint from  $\alpha_r = (cx)$ , then  $(yz)(cx) = (cx)(yz)$ .
2. If  $\alpha_{r-1} = (cy)$  with  $y \neq x$ , then  $(cy)(cx) = (xc)(xy)$ .

3. If  $\alpha_{r-1} = (xy)$ ,  $y \neq c$ , then  $(xy)(cx) = (yc)(yx)$ .

4.  $\alpha_{r-1} = \alpha_r$  so  $(cx)(cx) = I$ , contradicting minimality.

We can repeat this process until the last 2-cycle involving  $c$  is  $\alpha_1$ , a contradiction.  $\square$

**Prop. 2.1.7** *A permutation cannot be both even and odd.*

**PROOF** Suppose  $f$  can be written as an even and odd permutation:

$$f = \alpha_1 \alpha_2 \dots \alpha_m$$

$$f = \beta_1 \beta_2 \dots \beta_n$$

but then

$$I = \alpha_1 \alpha_2 \dots \alpha_m \alpha_m \dots \alpha_2 \alpha_1 = \beta_1 \beta_2 \dots \beta_n \alpha_m \alpha_{m-1} \dots \alpha_1$$

so  $I$  is odd, a contradiction.  $\square$

**Def'n. 2.1.8** We define the **signature**  $\text{sgn}(f)$  to be 1 if  $f$  is even, and  $-1$  if  $f$  is odd.

**Prop. 2.1.9** 1.  $\text{sgn}(f^{-1}) = \text{sgn}(f)$

2.  $\text{sgn}(fg) = \text{sgn}(f)\text{sgn}(g)$

**PROOF** Follows directly from the 2-cycle decomposition.  $\square$

**Def'n. 2.1.10** The **alternating group** of degree  $n$  is the group  $A_n = \{f \in S_n : \text{sgn}(f) = 1\} \leq S_n$ .

**Thm. 2.1.11**  $|A_n| = \frac{n!}{2}$ .

**PROOF** We see two separate proofs.

1. Consider  $\phi : A_n \rightarrow S_n \setminus A_n$  by  $f \mapsto f(12)$ . This is injective since if  $\phi(f) = \phi(g)$ , then  $f(12) = g(12)$  and  $f = g$ . It is surjective: if  $g$  is odd, then  $g(12)$  is even that  $\phi(g(12)) = g$ . Thus  $\phi$  is bijective and  $|A_n| = |S_n \setminus A_n| = |S_n| - |A_n|$  so  $|A_n| = |S_n|/2 = n!/2$ .

2. We claim that  $|S_n : A_n| = 2$ . For  $f \in S_n$  even,  $f \in A_n$  so  $A_n f = A_n$ . For  $f \in S_n$  odd,  $f^{-1}$  is odd and  $(12)f^{-1}$  is even and  $(12)f^{-1} \in A_n$ . Thus  $A_n(12) = A_n f$ , so there are only two cosets of  $A_n$ :  $A_n$  and  $A_n(12)$ , and the result follows by Lagrange's Theorem.  $\square$

As well, we also have  $A_n \triangleleft S_n$ , and  $S_n/A_n \cong C_2$ .

## Centralizers of Permutation Groups

**Ex. 2.1.12** Consider  $g = (12)(34) \in S_4$ . Then

$$C_{S_4}(g) = \{x \in S_4 \mid gx = xg\} = \{I, (12)(34), (12), (34), (14)(23), (1324), (1423)\}$$

The key idea is to observe that  $x^{-1}gx = g$ , which is called the conjugate of  $g$  by  $x$ .

**Ex. 2.1.13** Consider  $f = (34)(1572)(86)(9)$ ,  $g = (194)(368)(257)$ .

$$\begin{aligned} g^{-1}fg &= (752)(863)(491)(34)(1572)(86)(194)(368)(257) \\ &= (16)(2597)(38)(4) \\ &= (3g)(4g)(1g5g7g2g)(8g6g)(9g) \end{aligned}$$

In general, if  $f, g \in S_n$  and  $(a_1 a_2 \dots a_k)$  is a cycle in the cycle form of  $f$ , then  $(a_1 z a_2 z \dots a_k z)$  is a cycle in the cycle form of  $z^{-1} f z$ . To see this,  $a_1 z (z^{-1} f z) = a_1 f z = a_2 z$ , so  $a_1 z$  maps to  $a_2 z$ , and similarly for all the pairs of elements in the cycle.

If we now return to  $(12)(34)x = x(12)(34)$ , we have  $x^{-1}(12)(34)x = (12)(34)$  so

$$(1x \ 2x)(3x \ 4x) = (12)(34)$$

Since the cycle form is unique up to rearranging within cycles, we have

LHS	1x	2x	3x	4x	x
$(12)(34)$	1	2	3	4	$I$
$(21)(34)$	2	1	3	4	$(12)$
$(12)(43)$	1	2	4	3	$(34)$
$(21)(43)$	2	1	4	3	$(12)(34)$
$(34)(12)$	3	4	1	2	$(13)(24)$
$(34)(21)$	3	4	2	1	$(1324)$
$(43)(12)$	4	3	1	2	$(1423)$
$(43)(21)$	4	3	2	1	$(14)(23)$

Let's now compute the conjugacy classes of  $S_n$ . Let's do  $S_3$  first: The conjugacy classes are given by

$$\{1\}, \{(12), (13), (23)\}, \{(123)\}$$

In general, the conjugacy classes in  $S_n$  correspond to the possible cycle structures in  $S_n$ . None

### 2.1.3 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  $D_n$ :

$$\begin{aligned} r^a \cdot r^b &= r^{a+b} \\ sr^a \cdot r^b &= sr^{a+b} \\ r^a \cdot sr^b &= sr^{b-a} \\ sr^a \cdot sr^b &= r^{b-a} \end{aligned}$$

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