

# Algebra Winter Notes

Camila Restrepo

Last updated January 26, 2024

<b>1</b>	<b>Introduction to Groups</b>	<b>2</b>
1.1	What is a group? . . . . .	2
1.2	Subgroups and subgroup tests . . . . .	6
<b>2</b>	<b>Cyclic Subgroups</b>	<b>9</b>
<b>3</b>	<b>Permutation Groups (Symmetric Groups)</b>	<b>15</b>
3.1	Cycle Notation . . . . .	16

*Note:* Theorem numbers come from the order they are presented in lecture, and do not correspond to any textbook or written course material.

## Week 1

# Introduction to Groups

### 1.1 What is a group?

**Definition** of a group:

A **group**  $G$  is a nonempty set together with a multiplication  $G \times G \rightarrow G$  satisfying

1.  $(ab)c = a(bc) \forall a, b, c \in G$ , (Associativity)
2. there exists  $e \in G$  such that  $ea = ae = a \forall a \in G$ , (Identity)
3. and for every  $a \in G$  there exists  $b \in G$  such that  $ab = ba = e$ . (Inverse)

**Example** of a group:

Let  $\mathbb{R}^\times = \mathbb{R}^\dagger = \{a \in \mathbb{R} : a \neq 0\}$  together with multiplication on  $\mathbb{R}$ .

Associativity is immediate.

The identity is  $1 \in \mathbb{R}^\times$ .

For every  $a \in \mathbb{R}^\times$ ,  $\frac{1}{a} \in \mathbb{R}$  and  $a(\frac{1}{a}) = \frac{1}{a}(a) = 1$ .

So  $\mathbb{R}^\times$  is a group.

*Remark:* When we need to highlight the group multiplication we write a group as a pair of the set and the multiplication, e.g.,  $(\mathbb{R}, +)$ ,  $(\mathbb{R}, \cdot)$ .

From now on,  $G$  is **always** a group.

**Theorem 1.1**

There is a unique identity element in  $G$ .

**Theorem 1.2 Cancellation**

Suppose  $ba = ca$  for  $a, b, c \in G$ . Then  $b = c$

*Proof.* Let  $d \in G$  be an inverse for  $a$ , i.e.  $da = ad = e$ . Multiplying on the right by  $d$ , we obtain

$$\begin{aligned}(ba)d &= (ca)d \implies b(ad) = c(ad) \\ &\implies be = ce \\ &\implies b = c.\end{aligned}$$

□

**Theorem 1.3 Uniqueness of Inverses**

For every  $a \in G$  there is a unique element  $a^{-1} \in G$  such that  $aa^{-1} = a^{-1}a = e$ .

*Proof.* Suppose  $a \in G$  and  $b, b' \in G$  are inverses of  $a$ , then

$$ba = e = b'a \implies b = b'$$

(by theorem 1.2)

□

**Example** of inverses in different groups:

1. For  $b \in \mathbb{R}^\times$ ,  $b^{-1} = \frac{1}{b}$ .
2. For  $b \in \mathbb{R}$  under addition  $b^{-1} = -b$ .
3. For  $b \in \mathbb{Z}_n$ ,  $b^{-1} = n - b$ .

**Example** of groups using a field  $F$ :

1.  $(F, +)$  is a group (Imitate  $(\mathbb{R}, +)$ ).
2.  $(F^\times, \cdot)$  where  $F^\times = F^\dagger = \{a \in F : a \neq 0\}$  is a group. In particular, if  $p$  is a prime number, then  $\mathbb{Z}_p^\times = \{1, \dots, p-1\}$  is a group.
3. The set of  $m \times n$  matrices with entries in  $F$ ,  $M_{mn}(F)$  is a group under addition. When  $n = 1$ ,  $M_{m1}(F) = F^m$ .
4. The set of invertible  $m \times n$  matrices with entries in  $F$ ,  $GL(n, F) = \{A \in M_{nn}(F) : \det(A) \neq 0\}$  together with matrix multiplication is called (rank  $n$ ) **general linear group** (over  $F$ ). The identity matrix  $I \in GL(n, F)$  is the identity.  $\det(A) \neq 0 \implies \exists A^{-1} \in GL(n, F)$  such that  $AA^{-1} = A^{-1}A = I$ .

**Example** of the symmetries of the equilateral triangle:

Let  $\sigma$  = flip through the vertical axis. Let  $\rho$  = rotation by  $\frac{2\pi}{3}$ .

We can compose two symmetries, e.g.,  $\sigma\rho = \sigma \cdot \rho$ .

We can show that the symmetries given by  $\sigma$  and  $\rho$  under composition are  $\{e, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$  where  $e$  = doing nothing.

We call this set  $D_3$ . It forms a group under composition. Clearly  $\rho^3 = \rho\rho\rho = e$ ,  $\sigma^2 = \sigma\sigma = e$ , and  $\sigma\rho\sigma = \rho^2 = \rho^{-1}$ .

**Definition** of a dihedral group:

The **dihedral group** of order  $2n$  is defined by

$$D_n = \{e, \rho, \dots, \rho^{n-1}, \sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$$

where  $\rho^n = e$ ,  $\sigma^2 = e$ , and  $\sigma\rho\sigma = \rho^{-1}$ . This is a group with the multiplication given by  $\sigma\rho\sigma = \rho^{-1}$ .

*Remark:*  $D_n$  is the group of symmetries of a regular n-gon.

**Definition** of an Abelian Group:

A group  $G$  is **abelian (commutative)** if  $ab = ba$  for all  $a, b \in G$

**Example** of classifying groups:

1.  $(F, +)$  where  $F$  is a field is Abelian.
2.  $(F^\times, \cdot)$  where  $F$  is a field is Abelian.
3.  $(M_{mn}(F), +)$  is Abelian.
4.  $(GL(n, F), \cdot)$  is not Abelian.
5.  $D_n$  is not Abelian.

**Definition** of the group of units:

Let  $n \geq 2$  and  $U(n) = \{1 \leq k \leq n-1 : \gcd(k, n) = 1\}$ .

$U(n)$  is called the **group of units** of  $\mathbb{Z}_n$

*Recall Facts about  $d = \gcd(a, b)$ :*

1.  $d \mid a$  and  $d \mid b$ , and  $d$  is the largest integer with this property
2. There exists  $l, m \in \mathbb{Z}$  such that  $\gcd(a, b) = la + mb$
3.  $\gcd(a, b)$  is the smallest positive  $\mathbb{Z}$ -linear combination of  $a$  and  $b$ .
4. If  $f \mid a$  and  $f \mid b$  then  $f$  divides  $\gcd(a, b) = la + mb \implies f \mid d$

**Example** of  $U(n)$  together with multiplication mod  $n$  is a group:

Facts 2 and 3 tell us that  $\gcd(k, n) = 1 \iff \exists l, m \in \mathbb{Z}$  such that  $lk + mn = 1$ .

So  $U(2) = \{1\}$ ,  $U(3) = \{1, 2\}$ ,  $U(4) = \{1, 3\}$ ,  $U(5) = \{1, 2, 3, 4\}$ , etc.

So  $U(p) = \{1, \dots, p-1\} = \mathbb{Z}_p^\times$  where  $p$  is prime.

**Definition** of exponentiation:

Suppose  $g \in G$ .

1.  $g^0 = e$
2.  $g^n = g \cdots g$  ( $n$  times)
3.  $g^{-n} = (g^{-1})^n$

**Theorem 1.4 Socks and Shoes**

Suppose  $a, b \in G$ . Then  $(ab)^{-1} = b^{-1}a^{-1}$  (only relevant for non-abelian groups)

*Proof.*

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= aea^{-1} = aa^{-1} = e \\ (b^{-1}a^{-1})(ab) &= b^{-1}eb = b^{-1}b = e\end{aligned}$$

□

**Definition** of the order of a group and its elements:

The number of elements in  $G$  is called the **order** of  $G$ . Suppose  $a \in G$ .

Then the **order of  $a$**  is the largest positive integer  $n$  such that  $a^n = e$ .

If no such integer exists, we say  $a$  has **infinite order**. We denote the order of  $a$  by  $|a|$ .

**Example** of the order of  $\{e\}$ :

We know  $|\{e\}| = 1$ , and  $e^1 = e \implies |e| = 1$

**Example** of the order of  $\mathbb{R}^\times$ :

$\mathbb{R}^\times$  is an infinite group so it has infinite order.

Obviously,  $|1| = 1$ .

$|-1| = 2$  since  $(-1)^2 = 1$  and  $(-1)^1 \neq 1$ .

All other real numbers in  $\mathbb{R}^\times$  have infinite order.

**Example** of the order of  $D_3$ :

$|D_3| = 6$ .

$|\sigma| = 2$ ,  $|\rho| = 3$ ,  $|\rho^2| = 3$ ,  $|\sigma\rho| = 2$ ,  $|\sigma\rho^2| = 2$ .

## 1.2 Subgroups and subgroup tests

**Definition** of a subgroup:

A **subgroup** of  $G$  is a subset  $H \subseteq G$  which is a group under the same group multiplication as  $G$ .

**Example** of subgroups:

1.  $\{\pm 1\} \subseteq \mathbb{R}^\times$  is a subgroup
2.  $\mathbb{Z}_5 \subseteq \mathbb{Z}$  is not a subgroup of  $\mathbb{Z}$  since they have different group multiplications

**Theorem 1.5 2-step subgroup test**

Suppose  $H$  is a non-empty subset of  $G$ . Then  $H$  is a subgroup of  $G$  if and only if:

1.  $a, b \in H \implies ab \in H$  (closure under multiplication)
2.  $a \in H \implies a^{-1} \in H$  (closure under inverse)

**Theorem 1.6 1-test subgroup test**

$\emptyset \neq H \subseteq G$  is a subgroup  $\iff a, b \in H \implies ab^{-1} \in H$

*Proof.* The forward direction is immediate.

" $\Leftarrow$ " Suppose 1 and 2 hold. 1 tells us that the group multiplication on  $G$  restricts to a multiplication on  $H$ . The associativity of this multiplication on  $H$  is inherited from the associativity of the group multiplication on  $G$ .

By 1 and 2, for any  $a \in H$ ,  $a^{-1} \in H$  and  $e = aa^{-1} \in H$ . Therefore  $e \in H$ .

Finally, 2 is the inverse axiom for  $H$ . □

**Example** of showing subgroup-ness:

Let  $\mu_4 = \{a \in \mathbb{C}^\times : a^4 = 1\} = \{1, -1, i, -i\}$ .

$\mu_4 \neq \emptyset$ .

$a, b \in \mu_4 \implies (ab)^4 = a^4 b^4 = (1)(1) = 1 \implies ab \in \mu_4$

$a \in \mu_4 \implies (a^{-1})^4 = a^{-4} = (a^4)^{-1} = 1^{-1} = 1 \implies a^{-1} \in \mu_4$

**Theorem 1.7 Finite subgroup test**

Suppose  $H \neq \emptyset$  is a finite subset  $H \subseteq G$ . Then  $H$  is a subgroup  $\iff a, b \in H \implies ab \in H$ .

*Proof.* " $\implies$ " Follows from 2-step subgroup test.

" $\impliedby$ " By the 2-step subgroup test it is enough to show that if  $a, b \in H \implies ab \in H$  then  $b \in H \implies b^{-1} \in H$  also holds. Suppose  $a, b \in H \implies ab \in H$  (\*). Suppose  $e \neq b \in H$ . Let's prove  $b^{-1} \in H$ . By (\*),  $b^2 = bb \in H$ , and by induction,  $b^n \in H$  for all  $n \geq 1$ .

Since  $H$  is a finite set,  $b^k = b^j$  for some  $k > j \geq 1 \implies b^k b^{-j} = b^j b^{-j} = e \implies b^{k-j} = e$  for  $k - j \geq 1$ .

So  $b^{-1} = b^{k-j-1}$ .  $k - j - 1$  cannot be zero, since then  $b = e$ . So  $k - j - 1 \geq 1$  and so  $b^{-1} = b^{k-j-1} \in H$ . If  $b = e \in H$ , then its inverse (itself) is obviously also in  $H$ .  $\square$

**Example** of a finite subgroup:

Consider  $\{1, i, -1, -i\} \subseteq \mathbb{C}^\times$ . By the finite subgroup test, it suffices to show that  $\{1, i, -1, -i\}$  is closed under multiplication to prove that it is a subgroup. This can be done by brute force.



## Week 2

# Cyclic Subgroups

**Definition** of a cyclic group:

A group  $G$  is called **cyclic** if there is an element  $a \in G$  such that  $G = \{a^j : j \in \mathbb{Z}\}$ .  $a$  is called a **generator** of  $G$ . We indicate that  $G$  is a cyclic group generated by  $a$  with the notation  $G = \langle a \rangle$ .

**Theorem 2.1**

Suppose  $a \in G$ . Then  $\langle a \rangle$  is a subgroup of  $G$ .

*Proof.* Suppose  $a^m, a^n \in \langle a \rangle$  where  $m, n \in \mathbb{Z}$ . Then  $a^m a^n = a^{m+n} \in \langle a \rangle$  since  $m+n \in \mathbb{Z}$ . Also  $a^{-m} \in \langle a \rangle$  for all  $m$  since  $-m \in \mathbb{Z}$ , and  $a^m a^{-m} = a^0 = e = a^0 = a^{-m} a^m$ .

By the 2-step subgroup test  $\langle a \rangle$  is a subgroup.  $\square$

**Definition** of a cyclic subgroup:

The subgroup  $\langle a \rangle \subseteq G$  is called the **cyclic subgroup** generated by  $a \in G$ .

**Example** of generators:

Take  $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$  together with addition mod 6.

$\mathbb{Z}_6 = \langle 1 \rangle$  since  $n(1) = n \pmod 6$ . Note that we also have  $\mathbb{Z}_6 = \langle 5 \rangle$ .

*Remark:* In general,  $\mathbb{Z}_n$  is cyclic and generated by  $\langle -1 \rangle$ . All finite cyclic are isomorphic to  $\mathbb{Z}_n$  for some  $n$ .

*Remark:* For  $a \in G$ ,  $\langle a \rangle = \langle a^{-1} \rangle$ .

**Example** of the integers:

Take  $G = \mathbb{Z}$ .

$$\langle 1 \rangle = \{j1 : j \in \mathbb{Z}\} = \mathbb{Z}.$$

$$\langle 2 \rangle = \{j2 : j \in \mathbb{Z}\} = \text{even numbers} \subset \mathbb{Z}.$$

$$\langle m \rangle = \{jm : j \in \mathbb{Z}\} = \text{integers divisible by } m \text{ for } m \neq 0.$$

$$\langle 0 \rangle = \{0\}.$$

*Remark:* Infinite cyclic groups are all isomorphic to  $\mathbb{Z}$ .

**Definition** of the centre of a group:

The **centre** of  $G$  is the subset

$$Z(G) = \{x \in G : xa = ax \forall a \in G\}$$

i.e., the elements that commute with everything in  $G$ .

**Theorem 2.2**

$Z(G)$  is a subgroup of  $G$ .

*Proof.* Suppose  $x, y \in Z(G)$  and  $a \in G$ . Then  $(xy)a = x(ya) = xay = axy = a(xy)$ . Therefore  $xy \in Z(G)$ .

Moreover,  $xa = ax \implies x^{-1}xa = x^{-1}ax \implies a = x^{-1}ax \implies ax^{-1} = x^{-1}axx^{-1} \implies ax^{-1} = x^{-1}a \implies x^{-1} \in Z(G)$ .

By the 2-step subgroup test,  $Z(G)$  is a subgroup of  $G$ .  $\square$

*Remark:* 1.  $G$  is abelian  $\iff Z(G) = G$

2.  $Z(G)$  is abelian (even when  $G$  is not)

3.  $Z(D_3) = \{e\}$  (brute force)

4.  $x \in Z(G) \iff xax^{-1} = a \text{ for all } a \in G \iff axa^{-1} = x \text{ for all } a \in G$

**Example** of a non-trivial center:

$$Z(GL(2, \mathbb{R})) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{R}^\times \right\}$$

**Definition** of the centralizer:

Fix  $b \in G$ . The **centralizer** of  $b$  in  $G$  is

$$\begin{aligned} C_G(b) &= C(b) = \{a \in G : ab = ba\} \\ &= \{a \in G : aba^{-1} = b\} \end{aligned}$$

**Theorem 2.3**

For any  $b \in G$ ,  $C_G(b)$  is a subgroup.

*Proof.* Subgroup test. □

*Remark:* 1.  $C_G(e) = G$

2.  $C_G(b) = G \iff b \in Z(G)$

3.  $e \in C_G(b), \langle b \rangle \subseteq C_G(b)$

**Example** of a centralizer:

$$C_{GL(2, \mathbb{R})} \left( \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right) = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R}^\times \right\}$$

*Recall:*  $G$  is cyclic if  $G = \langle a \rangle = \{a^j : j \in \mathbb{Z}\}$  for some  $a \in G$ .

**Theorem 2.4**

Suppose  $a \in G$ . Then

1. If  $|a| = \infty$ , then  $a^k = a^j \iff j = k$
2. If  $|a| = n$ , then  $a^k = a^j \iff n$  divides  $k - j$

*Proof.* 1. Suppose  $|a| = \infty$ . This means  $a^n \neq e$  for any  $n \geq 1$ . Suppose now  $a^k = a^j$  with  $k \geq j$ . Then  $a^k a^{-j} = a^j a^{-j} = e \implies a^{k-j} = e$  for  $k - j \geq 0$ . Since  $a^n \neq e \forall n \geq 1$ , we have  $k - j = 0 \implies k = j$ .

2. Suppose  $|a| = n$ . This means  $a^n = e$  and  $n$  is the least positive number satisfying this equation. Suppose  $a^k = a^j$  with  $k \geq j$ . Then  $a^{k-j} = e$  where  $k - j \geq 0$ . By definition of  $n$ ,  $n \leq k - j$ . By the division algorithm,  $k - j = qn + r$  where  $q, r \in \mathbb{Z}$  are unique and  $0 \leq r \leq n - 1$ .  
 $e = a^{k-j} = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r = e^q a^r = e a^r = a^r$ , so  $r = 0$  by the minimality of  $n$ , and so  $k - j = qn \implies \frac{k-j}{n} = q \in \mathbb{Z} \implies n$  divides  $k - j$ .  
 Conversely if  $qn = k - j$ , then  $a^{k-j} = (a^n)^q = e^q = e \implies a^k = a^j$ .

□

*Remark:* In part 2.,  $n$  divides  $k - j \iff (k - j) \bmod n = 0 \iff k \bmod n = j \bmod n$

**Corollary 2.5**

Suppose  $|a| = n$ . Then  $a^k = e$  for some  $k \in \mathbb{Z} \iff k$  is a multiple of  $|a|$

*Proof.* Suppose  $a^k = e$ . Then  $a^k = a^0$ , so  $n$  divides  $k - 0 = k$ .  $\square$

**Corollary 2.6**

Suppose  $a \in G$ . Then

1. If  $|a| = n$  then  $\langle a \rangle = \{e, a^1, a^2, \dots, a^{n-1}\}$  and  $|\langle a \rangle| = |a|$ .
2. If  $|a| = \infty$ , then  $\langle a \rangle$  is infinite and  $|\langle a \rangle| = |a| = \infty$

*Proof.* Didn't take notes for this one.  $\square$

**Corollary 2.7**

Suppose  $G$  is a finite group and  $a, b \in G$ . Then

1.  $|a|, |b|$  are finite
2. If  $ab = ba$  then  $|ab|$  divides  $|a| |b|$

*Proof.* 1. Suppose by way of contradiction that  $|a|$  is infinite. Then  $\langle a \rangle \subseteq G$  is infinite. But  $G$  is finite so  $|\langle a \rangle| \leq |G|$  is a contradiction.

$$2. (ab)^{|a||b|} = a^{|a||b|} b^{|a||b|} = (a^{|a|})^{|b|} (b^{|b|})^{|a|} = e^{|b|} e^{|a|} = e$$

$\square$

2 examples omitted. Sorry, I'm prepping for my tutorial later!

**Theorem 2.8**

Suppose  $a \in G$  and  $|a| = n$ . Then for any  $k \geq 1$ ,  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = \frac{n}{\gcd(n,k)}$

**Theorem 2.9 Fundamental Theorem of Cyclic Groups**

Suppose  $G = \langle a \rangle$  is cyclic and  $|G| = n$ . Then

1. Every subgroup of  $H$  is cyclic and  $k = |H|$  divides  $n = |G|$ , i.e.,  $k$  is a divisor of  $n$
2. For every divisor  $k$  of  $n$ , there is a unique subgroup of  $G$  of order  $k$  and it is equal to  $\langle a^{\frac{n}{k}} \rangle$

*Proof.* 1. Suppose  $H$  is a subgroup of  $G$  and  $H \neq \langle e \rangle$ . Let  $m \geq 1$  be the least power of  $a$  such that  $a^m \in H$ . Since  $H$  is closed under multiplication and inversion,  $\langle a^m \rangle \subseteq H$ . Suppose  $a^j \in H$ . By the division algorithm,  $j = qm + r$  with  $0 \leq r < m \implies a^j = (a^m)^q a^r \implies a^j (a^m)^{-q} = a^r$ , so since  $a^j, (a^m)^{-q} \in H$ ,  $a^r \in H \implies r = 0$  by the minimality of  $m$ .

2. Suppose  $k$  divides  $n$ , i.e.  $\frac{n}{k}$  is an integer. Recall that  $|\langle a^{\frac{n}{k}} \rangle| = |\langle a^{\frac{n}{k}} \rangle| = k$ . It follows that  $|\langle a^{\frac{n}{k}} \rangle| = k$ .

Suppose  $H \subseteq \langle a \rangle$  is a subgroup and  $|H| = k$ . By part 1,  $H = \langle a^m \rangle$  for some  $m \geq 1$ . By Theorem 2.8,  $k = |H| = |\langle a^m \rangle| = \frac{n}{\gcd(m, n)} \implies \gcd(m, n) = \frac{n}{k}$ .

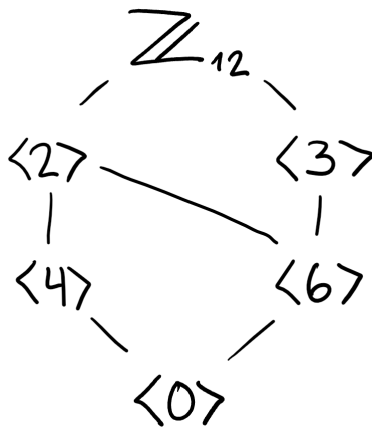
By Theorem 2.8 again,  $H = \langle a^m \rangle = \langle a^{\gcd(m, n)} \rangle = \langle a^{\frac{n}{k}} \rangle$ . □

**Example** of the subgroups of  $\mathbb{Z}_{12}$ :

The divisors of  $n = 12$  are 1, 2, 3, 4, 6, 12

- $k = 1$ :  $\langle 0 \rangle$
- $k = 2$ :  $\langle 6 \rangle = \{0, 6\}$
- $k = 3$ :  $\langle 4 \rangle = \{0, 4, 8\}$
- $k = 4$ :  $\langle 3 \rangle = \{0, 3, 6, 9\}$
- $k = 6$ :  $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$
- $k = 12$ :  $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

*Note:* The lattice of subgroups of  $\mathbb{Z}_{12}$  illustrates the containment relationships.



*Remark:* In  $\mathbb{Z}_n$ , clearly  $\langle m \rangle \subseteq \langle k \rangle \iff m \in \langle k \rangle \iff ka = m \iff k \text{ divides } m$ .

**Example** of subgroups of  $\mathbb{Z}_p$ :

Consider  $\mathbb{Z}_p$  where  $p$  is prime. The only subgroup of  $\mathbb{Z}_p$  is  $\langle 0 \rangle$ .

## Week 3

# Permutation Groups (Symmetric Groups)

**Definition** of the Euler  $\phi$ -function:

The Euler  $\phi$ -function is defined for every positive integer  $d \geq 1$  by

$$\phi(d) = \begin{cases} 1 & \text{if } d = 1 \\ |\{1 \leq j \leq d-1 : \gcd(j, d) = 1\}| & \text{otherwise} \end{cases}$$

**Definition** of:

Suppose  $A \neq \emptyset$  is a set. A **permutation** of  $A$  is a bijection  $\beta : A \rightarrow A$  (1-1, onto). The **permutation group (symmetric group)** of  $A$  is the set of permutations of  $A$  under composition.

*Recall some facts about functions:* Let  $S_A$  be the symmetric group of  $A \neq \emptyset$ .

If  $\alpha, \beta \in S_A$  then  $\alpha \circ \beta(a) = \alpha(\beta(a))$  for all  $a \in A$ .

From MATH1800 composition of 1-1 and onto functions is again 1-1 and onto, i.e.,  $\alpha \circ \beta \in S_A$ .

From MATH1800  $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$  for all  $\alpha, \beta, \gamma \in S_A$ .  $\alpha$  permutation  $\iff \alpha$  is invertible under composition.

*Remark:* Define  $e \in S_A$  by  $e(a) = a$  for all  $a \in A$ . Clearly  $e \circ \alpha(a) = e(\alpha(a)) = \alpha(a)$  for all  $a \in A \implies e \circ \alpha = \alpha$ . We see that  $S_A$  truly is a group.

**Example** of:

Take  $A = \{1, 2, 3\}$ . What are the permutations in  $S_3 = S_A$ ?

- $e \in S_3 : e(1) = 1, e(2) = 2, e(3) = 3$ .
- $\beta \in S_3$  where  $\beta(1) = 2, \beta(2) = 3, \beta(3) = 1$ .

Let's rewrite  $\beta$  as follows:  $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \mathbb{R}$ .

In general for any  $\alpha \in S_3$ , we may rewrite it as  $\begin{bmatrix} 1 & 2 & 3 \\ \alpha(1) & \alpha(2) & \alpha(3) \end{bmatrix} = \mathbb{R}$ .

The number of permutations is given by the number of choices. This is  $3! = 3 \cdot 2 \cdot 1$ . We just proved that  $|S_3| = 3! = 6$ .

Similar reasoning tells us that  $|S_n| = n!$  for every  $n \geq 1$ .

### Question

Paul Mezo said we "know everything" about linear algebra. What does that mean?

### Answer

There are no unsolved problems in finite linear algebra.

## 3.1 Cycle Notation

Consider  $S_3$  and  $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \in S_3$ . We rewrite this permutation as follows:  $(1\ 2\ 3)$ .

Notice that  $\alpha = (1\ 2\ 3) \neq (1\ 3\ 2) = \beta$ , but they are both 3-cycles.

Also,  $\gamma = (1\ 2)$  is the permutation such that  $\gamma(1) = 2, \gamma(2) = 1, \gamma(3) = 3$ . It's a 2-cycle.

We omit 1-cycles.

The six permutations in  $S_3$  in cycle notation are  $e, (12), (13), (23), (123), (132)$ .

**Example** of cycles of  $S_4$ :

Consider  $S_4$ .  $|S_4| = 24 = 4!$ .

- $e$ ,
- $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$
- $(1\ 2\ 3), (1\ 3\ 4), \dots$
- $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), \dots$
- $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$

**Definition** of disjoint cycles:

Two cycles  $(a_1\ a_2\ \dots\ a_m), (b_1\ b_2\ \dots\ b_k) \in S_n$  are **disjoint** if  $a_j \neq b_l$  for any  $j, l$ . Their product can be written equally in either order.

Composition of permutations is interpreted as products of cycles as follows:



**Example** of compositions in  $S_7$ : •  $(6\ 2\ 3)(1\ 2) = (1\ 3\ 6\ 2)$

- $(1\ 2)(3\ 4\ 7)(2\ 3) = (2\ 4\ 7\ 3\ 1)$
- $(1\ 3)(2\ 4\ 5\ 6\ 7)(3\ 2)(1\ 2\ 5) = (2\ 6\ 7)(5\ 3\ 4)$

*Remark:* 1. Some authors move from left to right, one cycle to the next. We move from right to left.

2. Cycles don't tell us which  $S_n$  they live in.

**Example** of powers of a  $k$ -cycle:

Consider  $(a_1 \dots a_k) \in S_n$ .

1.  $(a_1 \dots a_k)^2 = (a_1\ a_2\ a_3 \dots a_k)(a_1\ a_2\ a_3 \dots a_k)$  sends  $a_1$  to  $a_3$ , and  $a_l$  to  $a_{l+2}$  if  $l \leq k-2$ . Sends  $a_{k-1} \rightarrow a_1$ ,  $a_k \rightarrow a_2$ .
2.  $(a_1 \dots a_k)^j$  sends  $a_l$  to  $a_{(l+j) \bmod k}$ .

In particular  $(a_1 \dots a_k)^k$  sends  $a_l$  to  $a_{(l+k) \bmod k} = a_{l \bmod k} = a_l$  for  $1 \leq l \leq k$ , so  $(a_1 \dots a_k)^k = e \implies |(a_1 \dots a_k)| = k$ .

### Theorem 3.1

Every permutation in  $S_n$  is a product of disjoint cycles. The products of disjoint cycles  $\alpha, \beta \in S_n$  commute, i.e.,  $\alpha\beta = \beta\alpha$ .

*Proof.* Proof omitted. □

*Remark:* Products of disjoint cycles can be written in more than one way to represent a single permutation in  $S_n$ .

$$(1\ 2\ 3)(5\ 6) = (5\ 6)(1\ 2\ 3) = (5\ 6)(2\ 3\ 1)$$

### Question

Dr. Mezo said they were unique "modulo" changing the order. Why use this language? What's the connection to modulo here?

**Definition** of the least common multiple:

The **least common multiple** of  $m, n \geq 1$  is the smallest positive integer  $k$  such that  $m$  divides  $k$  and  $n$  divides  $k$ . We write  $k = \text{lcm}(m, n)$ .

**Example** of finding LCM:

1.  $\text{lcm}(2, 3) = 6$

2.  $\text{lcm}(6, 12) = 12$

3.  $\text{lcm}(12, 8) = \text{lcm}(2^3 \cdot 3^1, 2^3 \cdot 3^0) = 2^3 \cdot 3^1 = 24$

**Theorem 3.2**

Let  $\alpha_1, \dots, \alpha_k \in S_n$  be disjoint cycles. Then  $|\alpha_1 \dots \alpha_k| = \text{lcm}(|\alpha_1|, \dots, |\alpha_k|)$

*Proof.* Proof omitted. □

**Example** of the theorem:

$$|(15)(37124)(986)| = 12 = \text{lcm}(2, 4, 3)$$

**Definition** of a transposition:

A **transposition** in  $S_n$  is a 2-cycle.

**Example** of transpositions:

Note

- $(1\ 2) = (2\ 1) = (1\ 2)^{-1}$
- $(1\ 2)(1\ 2) = (1)(2) = e$
- Similarly,  $(a\ b) = (b\ a) = (ab)^{-1}$
- $(1\ 2\ 3) = (1\ 3)(1\ 2)$
- $(1\ 2\ 3) = (a\ c)(a\ b)$

**Theorem 3.3**

Every permutation in  $S_n$  is a product of transpositions.

*Proof.*  $e = (1\ 2)(2\ 1) = (1\ 2)(1\ 2)$ .

Suppose  $\sigma \in S_n, \sigma \neq e$ . Then by a previous theorem,  $\sigma = \beta_1 \dots \beta_k$  for disjoint cycles  $\beta_1, \dots, \beta_k \in S_n$ . If each  $\beta_j$  is a product of transpositions then so is  $\sigma$ .

Let  $\beta = (a_1 \dots a_k)$  be a  $k$ -cycle in  $S_n$ . Let's prove by induction on  $k \geq 2$  that  $(a_1 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_2)$ .

Base case is obvious. Assume it's true for  $k$ .

Let  $\beta = (a_1 \dots a_{k+1}), \alpha = (a_1 a_{k+1}), \gamma = (a_1 \dots a_k)$ .

By induction  $\gamma = (a_1 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_2)$ .

It suffices to show that  $\beta = \alpha\gamma$ .

Let  $1 \leq l \leq k-1$ . Then  $\beta(a_l) = a_{l+1}$ , and  $\alpha\gamma(a_l) = \alpha(a_{l+1}) = a_{l+1} \implies \beta(a_l) = \alpha\gamma(a_l)$ .

So  $\beta(a_k) = a_{k+1}$  and  $\alpha\gamma(a_k) = \alpha(a_1) = a_{k+1} \implies \beta(a_k) = \alpha\gamma(a_k)$ .

So  $\beta(a_{k+1}) = a_1$  and  $\alpha\gamma(a_{k+1}) = \alpha(a_{k+1}) = a_1 \implies \beta(a_{k+1}) = \alpha\gamma(a_{k+1})$ .

Rest of the proof was erased before I could get to it :( □

#### Lemma 3.4

If  $e = \alpha_1 \dots \alpha_k$  is a product of transpositions  $\alpha_1, \dots, \alpha_k \in S_n$ , then  $k$  is even.

*Proof.* Proof omitted. □

#### Theorem 3.5

Suppose  $\alpha \in S_n$  and  $\beta_1 \dots \beta_r = \alpha = \gamma_1 \dots \gamma_s$  where  $\beta_1, \dots, \beta_r, \gamma_1, \dots, \gamma_s \in S_n$  are transpositions.

Then either  $r$  and  $s$  are both even, or they are both odd (i.e.,  $r \bmod 2 = s \bmod 2$ ).

*Proof.*  $\gamma_1 \dots \gamma_s = \beta_1 \dots \beta_r \implies \gamma_1^{-1} \gamma_1 \dots \gamma_s = \gamma_1^{-1} \beta_1 \dots \beta_r \implies e = \gamma_s \dots \gamma_1 \beta_1 \dots \beta_r$ , so the identity is a product of transpositions.

By the lemma,  $r + s$  is even. □

#### Definition of parity:

We say that  $\alpha \in S_n$  is **even** if it is a product of even number of transpositions, we say  $\alpha$  is odd if it is a product of an odd number of transpositions.

**Example** of parity of cycles:

1.  $(a\ b)$  odd
2.  $(a_1\ a_2\ a_3) = (a_1\ a_3)(a_1\ a_2)$  even
3.  $(a_1\ a_2\ a_3\ a_4) = (a_1\ a_4)(a_1\ a_3)(a_1\ a_2) = (a_1\ a_4)(a_1\ a_2\ a_3)$

*Remark:* A  $k$ -cycle is even for odd  $k$  and is odd for even  $k$ .

### Theorem 3.6

Let  $A_n \subseteq S_n, n \geq 2$  be the subset of even elements in  $S_n$ . Then  $A_n$  is a subgroup (called the **alternating group**).

*Proof.*  $e \in A_n$  so  $A_n \neq \emptyset$ . Suppose  $\alpha = \beta_1 \dots \beta_s$  and  $\sigma = \gamma_1 \dots \gamma_r$  for transpositions  $\beta_1, \dots, \beta_s, \gamma_1, \dots, \gamma_r \in S_n$ , i.e.,  $s$  and  $r$  are even. Then  $\alpha\sigma = \beta_1, \dots, \beta_s, \gamma_1, \dots, \gamma_r$  is a product of  $r + s$  transpositions. Since  $r + s$  is even,  $\alpha\sigma \in A_n$ .  
 $\alpha^{-1} = (\beta_1 \dots \beta_s)^{-1} = \beta_s^{-1} \dots \beta_1^{-1} = \beta_s \dots \beta_1$  a product of  $s$  transpositions. Since  $s$  is even,  $\alpha^{-1} \in A_n$ .  $\square$