

# NOTES FOR MATH 503 BY PROF. M. MAZUR

PLUTO WANG

## CONTENTS

1.	Jan. 26	1
2.	Jan. 28	3
3.	Jan. 31	5
4.	Feb. 7	8
5.	Feb. 9	10
6.	Feb. 11	12
7.	Feb. 14	13
8.	Feb. 16	16
9.	Feb. 18	17
10.	Feb. 21	18
11.	Feb. 23	20
12.	Feb. 25	21
13.	Feb. 28	21
14.	Mar. 2	21
15.	Mar. 4	23

This course is an introduction to group theory: the second course in the graduate algebra sequence.

## 1. JAN. 26

**Definition 1.1.** Let  $X$  be a set. A binary operation on  $X$  is a function  $f : X \times X \rightarrow X$ . We will denote  $f(x, y)$  by  $x \square y$ . A binary operation is said to be associative if  $(x \square y) \square z = x \square (y \square z)$ .

**Definition 1.2.** A monoid is a set  $M$  with a binary operation  $\cdot$  which is associative and such that  $\exists e \in M$  s.t.  $e \cdot m = m \cdot e = m$  for all  $m \in M$ .

**Proposition 1.3.**  $e$  in the previous definition of monoid is unique.

*Proof.* Let  $e_1$  be another element so that  $e_1 \cdot m = m \cdot e_1 = m$  for all  $m \in M$ . Then  $e = e_1 \cdot e = e_1$ .  $\square$

We can thus uniquely define such  $e$  to be the identity element or neutral element of  $M$ .

**Example 1.4.** The natural number  $\mathbb{N}$  with addition is a monoid, and  $e = 0$ .

**Definition 1.5.** A group is a monoid  $G$  s.t.  $\forall a \in G \exists b \in G$  s.t.  $a \cdot b = e$ .

**Example 1.6.** The natural number  $\mathbb{N}$  with addition and  $e = 0$  is not a group. But the integers  $\mathbb{Z}$  with addition and  $e = 0$  is a group.

**Proposition 1.7.** Let  $G$  be a group. If  $a \cdot b = 0$ , then  $b \cdot a = e$ .

*Proof.* We have  $c \in G$  s.t.  $b \cdot c = e$ . Then  $a = a \cdot e = a \cdot (b \cdot c) = (a \cdot b) \cdot c = e \cdot c = c$ . Hence,  $b \cdot a = e$ .  $\square$

This also shows that  $b$  is unique of  $a$ . We call it the inverse of  $a$  and denote it  $a^{-1}$ .

**Definition 1.8.** We say that  $a, b$  commute if  $ab = ba$ . In a group, this is the same as  $aba^{-1}b^{-1}$ .

**Definition 1.9.** The commutator of  $a \cdot b$  is  $[a, b] = aba^{-1}b^{-1}$ .

Note that some books use  $[a, b] = a^{-1}b^{-1}ab$  and, in general, they are different.

**Definition 1.10.** A group  $G$  is commutative or abelian if any two elements commute; i.e.,  $ab = ba$  for all  $a, b \in G$ .

In abelian group, we often use additive notation; i.e., denote the operation  $+$ ,  $e = 0$ , and  $a^{-1} = -a$ .

**Example 1.11.** These are some examples of groups.

- (1) The trivial group:  $\{e\}$  where  $e \cdot e = e$ .
- (2) The integers  $\mathbb{Z}$  with addition  $+$ .
- (3) The real  $\mathbb{R}$  with addition  $+$ .
- (4) If  $R$  is a ring, then  $(\mathbb{R}, +)$  is an abelian group. Called the additive group of the ring  $R$ .
- (5) If  $R$  is a ring, the units of  $\mathbb{R}$  is  $\mathbb{R}^\times = \{a \in R : ab = 1 = ba \text{ for some } b \in R\}$ . This is a ring with multiplication and is called the multiplicative group of  $R$ .
- (6) If  $K$  is a field, then the  $n \times n$  matrices over  $K$ ,  $M_n(K)$ , is a ring. Note that  $M_n(K)^\times = \text{GL}_n(K)$ , the general linear group of degree  $n$  over  $K$ .
- (7) We have  $\mathbb{Z}^\times = \{1, -1\}$ . So,  $\text{GL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = \pm 1 \right\}$  as  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ .

**Definition 1.12.** Let  $X$  be a set. Then the symmetry group of  $S$ ,  $S(X) = \text{Sym}(X)$  is the set of all bijections  $X \rightarrow X$  with composition of functions as the binary operation and  $e = \text{id} : X \rightarrow X$  by  $\text{id}(X) = X$ . The inverse of  $f$ ,  $f^{-1}$  is just the inverse function of  $f$  (whose existence is guaranteed by bijectivity).

**Example 1.13.** Let  $X = V$  be a vector space. Then  $\text{GL}(V)$  is the set of all linear bijections of  $V$ .

**Definition 1.14.** Let  $X = \{1, 2, \dots, n\}$ . The symmetry group or permutation group on  $n$  letter is just  $S_n = S(X)$ .

Consider  $X = \{a, b\}$ , then  $S(X) = S_2$  consists of two element, the identity map  $\text{id}$ , and  $f : X \rightarrow X$  by  $f(a) = b$  and  $f(b) = a$ .

**Example 1.15.** Consider a square  $ab - cd$ . Let  $r$  be the action of rotating  $90^\circ$  clockwise and  $s$  be the action of reflecting along the axis across  $ab$  and  $cd$ . Then  $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ .

Multiplication of two actions gives a new rotation or reflecting, for example,  $sr(a) = d$ ,  $sr(b) = c$ ,  $sr(c) = d$ , and  $sr(d) = a$ .

Note that we observe  $rs = sr^3$ , and can thus write the multiplication table as following.

$\cdot$	1	$r$	$r^2$	$r^3$	$s$	$sr$	$sr^2$	$sr^3$
1	1	$r$	$r^2$	$r^3$	$s$	$sr$	$sr^2$	$sr^3$
$r$	$r$	$r^2$	$r^3$	1	$sr^3$	$s$	$sr$	$sr^2$
$r^2$	$r^2$	$r^3$	1	$r$	$sr^2$	$sr^3$	$s$	$sr$
$r^3$	$r^3$	1	$r$	$r^2$	$sr$	$sr^2$	$sr^3$	$s$
$s$	$s$	$sr$	$sr^2$	$sr^3$	1	$r$	$r^2$	$r^3$
$sr$	$sr$	$sr^2$	$sr^3$	$s$	$r^3$	1	$r$	$r^2$
$sr^2$	$sr^2$	$sr^3$	$s$	$sr$	$r^2$	$r^3$	1	$r$
$sr^3$	$sr^3$	$s$	$sr$	$sr^2$	$r$	$r^2$	$r^3$	1

**Definition 1.16.** Let  $G$  be a group. Then a subgroup of  $G$  is a subset  $H \subseteq G$  s.t.  $e \in H$  and if  $a, b \in H$  then  $ab \in H$  and  $a^{-1} \in H$ .

**Proposition 1.17.** With the above definition, the subgroup  $H$  is also a group under the restriction of the operation on  $G$  to  $H$ .

Proof of this is left as an exercise to the reader.

2. JAN. 28

**Example 2.1.** The following are examples of groups:

- (1) Let  $X$  be a set. Then  $S(X) = \text{Sym}(X) = \{f : X \rightarrow X : f \text{ is a bijection}\}$  with function composition is the symmetry group on  $X$ .
- (2) Take  $X = \{1, \dots, n\}$ . Then  $S_n = S(X)$  is the symmetry (permutation) group on  $n$  letter.
- (3) Let  $S$  be a ring. Then  $\text{GL}_n(S) = M_n(S)^\times$  is all invertible  $n \times n$  matrices with entries in  $S$ . Note that  $\text{GL}_1(S) = S^\times$ .

**Definition 2.2.**  $S$  with two binary operations  $+, \cdot$  is a (unitary) ring if

- (1)  $(S, +)$  is an abelian group
- (2)  $(S, \cdot)$  is a monoid
- (3)  $(a + b) \cdot c = a \cdot c + b \cdot c$  and  $c \cdot (a + b) = c \cdot a + c \cdot b$ .

**Definition 2.3.** Let  $G$  be a group. Then  $H \subseteq G$  is a subgroup if  $e \in H$  and  $\forall a, b \in H$ ,  $ab \in H$  and  $a^{-1} \in H$ .

Note that  $e \in H$  follows from the closure under multiplication and inverse, given  $H$  is nonempty.

**Example 2.4.** Let  $G$  be a group. Then  $Z(G) = \{a \in G \text{ s.t. } \forall g \in G \ ag = ga\}$  is the center of the group. As an exercise, check it is a subgroup.

It is easy to see that  $G$  is abelian iff  $G = Z(G)$ .

**Note 2.5.** One objective in group theory is to understand all subgroups of a given group  $G$ . Unfortunately, this is, usually, not easy.

**Theorem 2.6.** A subset  $S$  of  $(\mathbb{Z}, +)$  is a subgroup iff  $S = d\mathbb{Z}$  for some  $d \geq 0$ .

*Proof.* The “if” direction is obvious: every  $S = d\mathbb{Z}$  is a subgroup.

Let  $S$  be a subgroup of  $\mathbb{Z}$ . If  $S = \{0\}$ , then  $d = 0$  has  $S = d\mathbb{Z}$ . Otherwise,  $S$  has positive elements.

Take the smallest positive element  $d \in S$ . Take  $a \in S$ , then  $a = nd + k$  where  $0 \leq k < d$ . But  $k = a - nd \in S$  which is necessarily 0 as  $d$  being the smallest positive element in  $S$  and thus  $a \in d\mathbb{Z}$ ; i.e.,  $S \subseteq d\mathbb{Z}$ .

Since  $d \in S$ , so  $d\mathbb{Z} \subseteq S$ . Thus,  $S = d\mathbb{Z}$ .  $\square$

As an exercise, prove that  $k\mathbb{Z} \cap m\mathbb{Z} = \text{lcm}(k, m)\mathbb{Z}$ .

**Proposition 2.7.** *The intersection of any collection of subgroups of a group  $G$  is also a subgroup.*

*Proof.* Take  $\{H_i\}_{i \in I}$  be a collection of subgroups of  $G$ . Then  $\forall i \in I$ , we have  $e \in H_i$ ; i.e.,  $e \in \cap H_i$ .

Take  $a, b \in \cap H_i$ , then  $\forall i \in I$ ,  $a, b \in H_i$ . Thus,  $ab \in H_i$  and  $a^{-1} \in H_i$ . Therefore,  $ab \in \cap H_i$  and  $a^{-1} \in \cap H_i$ .  $\square$

**Definition 2.8.** Let  $X$  be a subset of  $G$ . Then  $\langle X \rangle$  is the intersection of all subgroups containing  $X$ , called the subgroup generated by  $X$ .

Informally,  $\langle X \rangle$  is the smallest subgroup that contains  $X$ , but subsets might not be comparable under the partial order relation.

**Proposition 2.9.** *Let  $X$  be a subset of group  $G$ . Then  $g \in \langle X \rangle$  iff  $g = e$  or  $g = x_1^{\epsilon_1} \cdot \dots \cdot x_s^{\epsilon_s}$  for  $x_1, \dots, x_s \in X$  and  $\epsilon_i = \pm 1$  for all  $i$ . Note that it is necessary to list the disjoint  $g = e$  as  $X$  could be  $\emptyset$ , in which case,  $\langle \emptyset \rangle = \{e\}$ .*

*Proof.* Let  $T = \{x_1^{\epsilon_1} \cdot \dots \cdot x_s^{\epsilon_s} : x_1, \dots, x_s \in X, \epsilon_i = \pm 1\}$  for  $X \neq \emptyset$ . Then, we have

- (1)  $e = x^1 x^{-1} \in T$ .
- (2) If  $a, b \in T$ , then  $ab \in T$ .
- (3) If  $a = x_1^{\epsilon_1} \cdot \dots \cdot x_s^{\epsilon_s} \in T$ , then  $a^{-1} = x_s^{-\epsilon_s} \cdot \dots \cdot x_1^{-\epsilon_1} \in T$ .

Therefore,  $T$  is a subgroup. Now, if  $H$  is a subgroup of  $G$ , then  $X \subseteq H$  implies  $T \subseteq H$ . Therefore,  $T = \langle X \rangle$ .  $\square$

When  $X = \{g\}$ , then we often denote  $\langle X \rangle = \langle g \rangle$ , and it is equal to  $\{g^i : i \in \mathbb{Z}\}$ .

**Definition 2.10.** Let  $g \in G$ . Then  $g^n = \begin{cases} \overbrace{g \cdot \dots \cdot g}^n & n > 0 \\ e & n = 0 \\ \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_{-n} & n < 0 \end{cases}$

As an exercise, show that  $g^m \cdot g^n = g^{m+n}$  and  $(g^m)^n = g^{mn}$  for all  $m, n \in \mathbb{Z}$ .

**Definition 2.11.** Groups generated by one element are called cyclic groups; i.e.,  $G = \langle g \rangle$  is cyclic.

For example,  $\mathbb{Z} = \langle 1 \rangle$  and in  $D_4$ ,  $\langle r \rangle = \{1, r, r^2, r^3\}$ .

**Note 2.12.** (1) If  $g^n \neq g^m$  for all  $n \neq m$ , then  $\langle g \rangle$  is infinite.

(2) If  $g^n = g^m$  for some  $n > m$ , then  $g^{n-m} = e$ .

(3) Let  $k > 0$  be the smallest s.t.  $g^k = e$ , then  $e, g, g^2, \dots, g^{k-1}$  are all different.

If  $l \in \mathbb{Z}$ ,  $l = ak + r$  where  $0 \leq r < k$ , then  $g^l = g^{ak+r} = e \cdot g^r = g^r$ . So,  $\langle g \rangle = \{e, g, \dots, g^{k-1}\}$ .

**Definition 2.13.**  $G$  is finite if  $G$  has finitely many elements; i.e.,  $|G| < \infty$ . Otherwise, it is infinite.

$g \in G$  is of finite order if  $|\langle g \rangle| < \infty$ .

The order of  $g \in G$  is the smallest  $k \in \mathbb{N}$  s.t.  $g^k = e$ .

**Example 2.14.** In  $S_n$ , take  $f$  by  $f(1) = 2, f(2) = 3, \dots, f(n-1) = n, f(n) = 1$ . Then,  $f$  is of order  $n$ . We thus have  $\langle f \rangle$  is a cyclic group of order  $n$ .

**Definition 2.15.** A group  $G_1$  is isomorphic to group  $G_2$  if there is a bijection  $f : G_1 \rightarrow G_2$  s.t.  $f(ab) = f(a)f(b)$ .

**Note 2.16.** If  $e_1 \in G_1$  and  $e_2 \in G_2$  are identities. Then  $e_2 f(e_1) = f(e_1) = f(e_1 e_1) = f(e_1) f(e_1)$ , and so,  $f(e_1) = e_2$ .

Also,  $e_2 = f(a a^{-1}) = f(a) f(a^{-1})$ , and so,  $f(a^{-1}) = (f(a))^{-1}$ .

**Example 2.17.** Suppose that  $\langle g \rangle$  is infinite. Then  $f : \mathbb{Z} \rightarrow \langle g \rangle$  by  $m \mapsto g^m$  is a bijection. Also,  $f(a+b) = g^{a+b} = g^a g^b = f(a) f(b)$ . So,  $f$  is an isomorphism.

Another example is given by  $\{1, -1\}$  with multiplication and  $\{0, 1\}$  with addition. These are isomorphic and can be shown by their multiplication table.

$$\begin{array}{c|cc} \cdot & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array} \quad \text{and} \quad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

**Example 2.18.** Consider  $\mathbb{R}_{>0}$  with multiplication and  $\mathbb{R}$  with addition. These are groups. Also,  $\mathbb{R}_{>0} \subseteq \mathbb{R}^\times = \langle \mathbb{R}_{>0} \cup \{-1\} \rangle$ .

$a \mapsto e^a : (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$  is an isomorphism.

**Definition 2.19.** Let  $G, H$  be groups. A function  $f : G \rightarrow H$  is a homomorphism if  $f(ab) = f(a)f(b)$ .

### 3. JAN. 31

**Definition 3.1.** Let  $G, H$  be groups. A function  $f : G \rightarrow H$  is a homomorphism if  $f(ab) = f(a)f(b)$  for all  $a, b \in G$ .

**Note 3.2.** (1)  $f$  is a homomorphism  $\implies f(e_G) = e_H$  and  $f(a^{-1}) = f(a)^{-1}$  for all  $a \in G$ .

(2)  $f$  is called a monomorphism if  $f$  is injective (1-to-1).

(3)  $f$  is called an epimorphism if  $f$  is surjective (onto).

(4)  $f$  is called an isomorphism if  $f$  is bijective; and  $f^{-1} : H \rightarrow G$  is also an isomorphism.

If there is an isomorphism between  $G$  and  $G$ , we write  $G \cong H$  and consider  $G, H$  “the same.”

**Example 3.3.**  $G$  a group,  $g \in G$ . Then there is a homomorphism  $f : \mathbb{Z} \rightarrow G$  s.t.  $f(n) = g^n$  for all  $n$ .  $f$  is injective iff  $g$  has finite order.

**Example 3.4.** If  $X$  and  $Y$  are sets and  $|X| = |Y|$  then  $S(X) \cong S(Y)$ .

*Proof.* Suppose  $\phi : X \rightarrow Y$  is a bijection, then  $S(X) \rightarrow S(Y)$  by  $f \mapsto \phi f \phi^{-1}$  is an isomorphism.  $\square$

Note that if  $|X| = n$ , then  $|S(X)| = n!$ .

**Example 3.5.**  $R$  a commutative ring. Then  $\det : \text{GL}_n(R) \rightarrow R^\times$  is a homomorphism.

$$\left| \begin{bmatrix} a & & & \\ & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \\ & & & & 1 \end{bmatrix} \right| = a$$

**Example 3.6.** For all  $n$ , for all  $R$  a ring. Let  $P : S_n \rightarrow \text{GL}_N(R)$  be for  $f \in S_n$ , define  $P_f = (a_{ij})$  where  $a_{ij} = \begin{cases} 1 & \text{if } i = f(j) \\ 0 & \text{if otherwise} \end{cases}$ ; i.e.,  $P_f$  has only one non-zero entry in every row and every column, and all non-zero entries are 1. Such matrices are called permutation matrices.

For example, let  $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ,  $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$ . Then  $fg = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ .

Note that  $P_f = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ ,  $P_g = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ ,  $P_{fg} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ .

As an exercise, show that  $P_{fg} = P_f P_g$ .

In  $S_n$ , consider  $r = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$  and  $s = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$ .

Let  $D_n = \langle r, s \rangle$ . This is the dihedral group on regular  $n$ -gon.

$r$  is rotation by  $\frac{2\pi}{n}$  clockwise,  $s$  is reflection in perpendicular bisector of  $\overline{1n}$ , and  $D_n$  is all rigid motions of regular  $n$ -gon.

As an exercise, show  $rs = sr^{n-1}$ , order of  $r = n$ , and order of  $s = 2$ .

Note that  $D_n = \{1, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$ .

When  $n = 5$ , then  $rs^3rs^4 = rsr = sr^{n-1}r = s$ . Note that  $srs = r^{n-1}$ .  $D_n$  is called dihedral group of order  $2n$ .

**Example 3.7.** Let  $G$  be a group. For  $g \in G$ , define  $L_g : G \rightarrow G$  by  $a \mapsto g \cdot a$  (Left multiplication by  $g$ ). Then  $L_g$  is a bijection as  $ga = gb \implies a = b$  and  $g(g^{-1}a) = a$ .

We have that  $L_g \in S(G)$ , so we can define  $\phi : G \rightarrow S(G)$  by  $g \mapsto L_g$ . Then  $L_g \circ L_h(a) = gha = L_{gh}a$ , so, this is an injective homomorphism.

**Theorem 3.8** (Caley). *Every group is isomorphic to a subgroup of  $S(X)$  for some set  $X$ .*

If  $G$  is a group and  $g \in G$ . Define  $C_g : G \rightarrow G$  by  $C_g(a) = gag^{-1}$ . Then,  $C_g$  is a homomorphism as  $C_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = C_g(a)C_g(b)$ . Also,  $C_g$  is a bijection as  $gag^{-1} = gbg^{-1} \implies a = b$  and  $g(g^{-1}ag)g^{-1} = a$ .

These forms a homomorphism  $f : G \rightarrow \text{Aut}(G)$  by  $g \mapsto C_g$  where  $\text{Aut}(G)$  is the group of all automorphisms of  $G$  under compositions.

**Definition 3.9.** Elements of the form  $C_g$  are called inner automorphisms and  $C_g$  is called “conjugation by  $g$ .”

Note:  $\text{Aut}(\mathbb{Z}) = \{\text{id}, x \mapsto -x\}$ .

If  $G = \langle X \rangle$  and  $f, h : G \rightarrow H$  are two automorphisms. Show as an exercise that if  $f(x) = h(x)$  for all  $x \in X$ , then  $f = h$ .

$\text{GL}_2(\mathbb{Z})$  is finitely generated,  $(\mathbb{Q}, +)$  and  $(\mathbb{Q}^\times, \cdot)$  are not.

Show as an exercise that if  $f : G \rightarrow H$  is a homomorphism, then  $f(G)$  is a subgroup of  $H$ .

**Definition 3.10.** Let  $A, B$  be subsets of  $G$ . Then  $AB = \{ab : a \in A, b \in B\}$ .

**Definition 3.11.** Let  $G$  be a group.  $A, B$  are subsets of  $G$ . Then

- (1)  $AB = \{ab \mid a \in A, b \in B\}$ .
- (2)  $A^{-1} = \{a^{-1} \mid a \in A\}$ .
- (3)  $aB = \{a\}B = L_a(B)$

Let  $f : G \rightarrow G$  be a homomorphism. Then  $H = f(G) \leq G$  and we have  $f : G \twoheadrightarrow H \hookrightarrow G$ .

**Definition 3.12.**  $f^{-1}(e) = \{a \in G : f(a) = e\} = \ker(f)$  is the kernel of  $f$ .

**Proposition 3.13.** The kernel of  $f$  is a subgroup of  $G$ .

**Note 3.14.**  $f(a) = f(b) \iff f(ab^{-1})f(a)f(b)^{-1} = e \iff ab^{-1} \in \ker(f)$ . so,  $f^{-1}(f(a)) = a\ker(f) = \ker(f)a$ .

**Definition 3.15.** A subgroup  $N$  of  $G$  is Normal if  $aN = Na$  for all  $a \in G$ ; alternatively,  $aNa^{-1} = N$  for all  $a \in G$ .

( $N$  is normal iff  $N$  is preserved by all inner automorphism)

As an exercise, show that If  $N \leq G$  and  $aNa^{-1} \subseteq N$  for all  $a \in G$ , then  $aNa^{-1} = N$  for all  $a \in G$ .

**Note 3.16.** We denote  $N$  is a subgroup of  $G$  by  $N \leq G$  and  $N$  is a normal subgroup of  $G$  by  $N \trianglelefteq G$ .

**Example 3.17.** (1) Every subgroup of an abelian group is normal.

(2)  $H = \{e, s\} \subseteq D_4$  has  $rH = \{r, rs\} = \{r, sr^3\}$  and  $Hr = \{r, sr\} \neq rH$ , so not normal.

(3)  $N = \{e, r^2\}$  is normal in  $D_4$  as  $r^k N r^k = N$  and  $s N s^{-1} = N$

Show as an exercise that  $Z(D_4) = \{e, r^2\}$ .

**Proposition 3.18.** If  $G = \langle X \rangle$ ,  $X \subseteq G$ , then  $N$  is normal iff  $\forall s \in X \ s N s^{-1} \subseteq N$  and  $s^{-1} N s \subseteq N$ .

Consider  $f : G \twoheadrightarrow H \subseteq G$ . We observe that elements of  $H$  are in bijective correspondence with subsets of the form  $a \ker f$  since if  $h \in H$  then  $f^{-1}(h) = a \ker f$  for some  $a \in G$ .

**Definition 3.19.** Let  $K \leq G$ . A subset of  $G$  of the form  $aK$  ( $Ka$ ) is called a left (right) coset of  $K$  in  $G$  for  $a \in G$ .

**Proposition 3.20.**  $c \in aK$  iff  $aK = cK$

*Proof.* If  $cK = aK$ , then  $c = c \cdot e \in cK = aK$ .

If  $c \in aK$ , then  $c = ak$  for some  $k \in K$ . so,  $cK = akK = a(kK) \subseteq aK$ . Also,  $a = ck^{-1} \in cK$ , so  $aK \subseteq cK$ . Hence,  $cK = aK$ .  $\square$

**Corollary 3.21.** Two left (right) cosets either coincide or are disjoint; i.e., the left (right) cosets partition the group.

Show as an exercise that  $(aK)^{-1} = Ka^{-1}$ .

**Definition 3.22.**  $[G : K]$  is the index of  $K$  in  $G$  which is the number of left (right) cosets of  $K$  in  $G$ .

**Proposition 3.23.** Suppose  $G$  is finite, so  $K$  is finite. For  $a \in G$ ,  $|aK| = |K|$ , so all cosets have the same number of elements.

So,  $|G| = [G : K]|K|$ .

**Corollary 3.24.**  $|K| \mid |G|$  if  $K \leq G$ .

**Corollary 3.25.** If  $g \in G$ , then the order of  $g$  divides  $|G|$ .

**Corollary 3.26.**  $g^{|G|} = e$ .

**Theorem 3.27** (Fermat's Last Theorem).  $p$  a prime, if  $p \nmid a$  then  $p \mid a^{p-1} - a$ .

**Note 3.28.**  $\mathbb{Z}/p\mathbb{Z}$  is a field.  $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ , and  $a \in (\mathbb{Z}/p\mathbb{Z})^\times \implies a^{p-1} = e$ .

**Proposition 3.29.**  $N \trianglelefteq G$  iff every left coset of  $N$  is also a right coset.

The proof is left as an exercise.

Consider  $f : G \rightarrow H \subseteq G$ .  $H$  is in a bijection w/ cosets of  $\ker f$ ; i.e.,  $h \leftrightarrow f^{-1}(h)$ .

**Definition 3.30.**  $G/N$  is the set of all cosets of a normal group  $N \trianglelefteq G$ .

**Note 3.31.** We can consider  $f : G \rightarrow H$ . Then  $N = \ker f$ ,  $aN = f(a)$ ,  $bN = f(b)$ , so,  $abN = f(a)f(b) = f(ab)$ . Then,  $G/N$  is a group isomorphic to  $H$ .

**Definition 3.32.** Multiplication on  $G/N$  by  $(aN)(bN) = (ab)N$ . Need to check that if  $aN = a_1N$ ,  $bN = b_1N$ , then  $abN = a_1b_1N$ .

*Proof.* We have  $a_1 = an_1$ ,  $b_1 = bn_2$ . Then  $a_1b_1 = an_1bn_2$ .  $Nb = bN \implies n_1b = bn_3 \implies a_1b = abn_3n_2 = abn_4 \in abN$ .  $\square$

As an exercise, show that  $(aN)(bN) = (ab)N$  as sets.

**Proposition 3.33.**  $(G/N, \dots)$  is a group.

*Proof.* We have  $[(aN)(bN)](cN) = (ab)NcN = (ab)cN = a(bc)N = aN[bNcN]$ .  $e = N$ .  $aN \cdot N = aN$ .  $(aN)(a^{-1}N) = aa^{-1}N = N$ .  $\square$

We have a canonical map called the quotient map.  $\phi : G \rightarrow G/N$  by  $g \mapsto gN$ . It is surjective and is a homomorphism.  $\ker \phi = N$ .

**Example 3.34.** Let  $G = \mathbb{Z}$ . Consider  $n\mathbb{Z}$  where  $n \geq 0$ . Then  $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$ .

$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = ab + n\mathbb{Z} = (a+b \bmod n) + n\mathbb{Z}$  and  $(a+n\mathbb{Z})(b+n\mathbb{Z}) = ab + n\mathbb{Z}$ . So,  $\mathbb{Z}/n\mathbb{Z}$  is a ring.

#### 4. FEB. 7

**Theorem 4.1.** Let  $G$  be a group.  $H \leq G$ , then the following are equivalent

- (1)  $aH = Ha$  for all  $a \in G$
- (2)  $aHa^{-1} = H$  for all  $a \in G$
- (3)  $aHa^{-1} \subseteq H$  for all  $a \in G$
- (4) Every left (right) coset of  $H$  is also a right (left) coset.

If  $H$  has these properties, then we call  $H$  to be normal, denoted  $H \trianglelefteq G$ .

**Proposition 4.2.** Let  $H \leq G$ . Suppose for any  $a, b \in H$ ,  $(aH)(bH)$  is also a left coset. Then  $H \trianglelefteq G$  and  $(aH)(bH) = (ab)H$ .



The proof is left as an exercise.

**Proposition 4.3.** *If  $f : G \rightarrow K$  is a homomorphism, then  $\ker f \trianglelefteq G$ .*

**Definition 4.4.** Let  $N \trianglelefteq G$ , then  $G/N$  is the set of all coset of  $N$  in  $G$ .

With multiplication defined as  $(aN)(bN) = (ab)N$ , this is well-defined and  $G/N$  is a group called the quotient group of  $G$  by  $N$ .

The map  $\phi : G \rightarrow G/N$  by  $g \mapsto gN$  is a surjective group homomorphism, called the quotient map and  $\ker \phi = N$ .

**Proposition 4.5.** *Suppose  $f : G \rightarrow H$  is a surjective homomorphism and let  $K = \ker f$ ,  $\phi : G \rightarrow G/K$  the quotient map.*

*Then there is a unique homomorphism  $\bar{f} : G/K \rightarrow H$  s.t.  $\bar{f}\phi = f$  and  $\bar{f}$  is an*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \phi \downarrow & \nearrow \bar{f} & \\ G/K & & \end{array}$$

isomorphism.

*Proof.* If  $\bar{f}$  exists, then  $\bar{f}(aK) = \bar{f}\phi(a) = f(a)$ . so, it is unique if exists.

Define  $\bar{f}(aK) = f(a)$ . If  $aK = bK$ , then  $a = bk$  for  $k \in K$ , so  $f(a) = f(bk) = f(b)f(k) = f(b)$ . Therefore, it is well-defined.  $\square$

**Proposition 4.6.** (1) *Intersection of any collection of normal subgroups of  $G$  is still normal.*

- (2) *If  $x \subseteq G$  and  $aXa^{-1} \subseteq X$  for all  $a \in G$ , then  $\langle X \rangle$  is normal.*
- (3) *If  $N \trianglelefteq G$  and  $H \leq G$ , then  $NH = HN$  is a subgroup of  $G$ .*
- (4) *If  $N \trianglelefteq G$  and  $H \trianglelefteq G$  then  $NH = HN \trianglelefteq G$ .*
- (5) *If  $N \trianglelefteq G$  and  $H \leq G$ , then  $H \cap N \trianglelefteq H$ .*

*Proof.* (1)  $N_i \trianglelefteq G$ ,  $i \in I$ . Then  $a \cap N_i a^{-1} = \cap a N_i a^{-1} = \cap N_i$ .

(2) Let  $N = \langle X \rangle$ . Then  $aXa^{-1} \subseteq X \subseteq N$ . So,  $\langle aXa^{-1} \rangle = a\langle X \rangle a^{-1} = aNa^{-1} \subseteq N$  and  $\langle X \rangle_n = \langle \bigcap_{a \in G} aXa^{-1} \rangle$ , where  $\langle \cdot \rangle$  is the smallest normal subset containing  $\cdot$ .

(3) Let  $nh = h(h^{-1}nh) = hn' \in HN$  so  $NH \subseteq HN$ . Similarly  $HN \subseteq NH$ . So,  $NH = HN$ .

Note that  $NH = \langle N \cup H \rangle$ .  $nh(n_1h_1) = nhn_1h^{-1}hh_1 \in NH$  and  $nh = h^{-1}n^{-1} = h^{-1}nhh^{-1} \in NH$ .

(4)  $a(HN)a^{-1} = (aHa^{-1})(aN a^{-1}) = HN$ .

(5)  $h(N \cap H)h^{-1} = (hNh^{-1}) \cap (hHh^{-1}) = N \cap H$ .  $\square$

**Theorem 4.7** (First homomorphism theorem). *Let  $\phi : G \rightarrow K$  be a surjective homomorphism and  $f : G \rightarrow H$  a homomorphism s.t.  $\ker f \subseteq \ker \phi$ . Then there is a unique homomorphism  $\bar{f} : K \rightarrow H$  s.t.  $\bar{f}\phi = f$ . Also,  $f(G) = \bar{f}(K)$  and*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \phi \downarrow & \nearrow \bar{f} & \\ K & & \end{array}$$

$\ker \bar{f} = \phi \ker f$ .

*Proof.* if  $\bar{f}$  exists then  $\bar{f}(k) = \bar{f}(\phi g) = f(g)$  for  $\phi g = k$ . So,  $\bar{f}$  is unique if exists.

If  $\phi(g_1) = \phi(g_2) = k$ , then  $g_1g_2^{-1} \in \ker \phi$  and so  $g_1g_2^{-1} \in \ker f$ . Therefore,  $f(g_1) = f(g_2)$  and thus  $\bar{f}$  is well-defined. Define  $\bar{f}(k) = f(g)$  for any  $g \in G$  s.t.  $\phi(g) = k$ .  $\square$

**Corollary 4.8.** *If  $\phi : G \rightarrow G/N$  is a quotient map. and  $N \in \ker f$ , then  $\ker \bar{f} = \ker f/N$ .*

**Theorem 4.9** (Correspondence Theorem). *Let  $f : G \twoheadrightarrow H$  be a surjective homomorphism. Then*

- (1)  $K \leq G \implies f(K) \leq H$  ( $K \trianglelefteq G \implies f(K) \trianglelefteq H$ ).
- (2)  $T \leq H \implies f^{-1}T \leq G$  and  $\ker f \subseteq f^{-1}(T)$ .
- (3) If  $K \leq G$ , then  $f^{-1}(f(K)) = K \ker f$ .
- (4) If  $T \leq H$ , then  $f(f^{-1}(T)) = T$ .

To summarize:  $T \mapsto f^{-1}(T) : \text{subgroups of } H \rightarrow \text{subgroups of } G \text{ containing } \ker f$  is a bijective correspondence that preserves inclusion and intersection with normal subgroups corresponding to normal subgroups. In particular, if  $f : G \rightarrow G/N$  is the quotient map, then subgroups of  $G/N \leftrightarrow$  subgroups of  $G$  containing  $N$ ; i.e.,

$$N \subseteq K \subseteq G \leftrightarrow K/N \subseteq G/N$$

**Theorem 4.10** (Second homomorphism theorem). *If  $K \trianglelefteq G$ ,  $H \leq G$ ,  $A \trianglelefteq H$ . Then  $KH \trianglelefteq G$ ,  $KA \trianglelefteq KH$  and the quotient map  $\phi : KH \rightarrow KH/KA$  takes  $H$  onto  $KH/KA$  and the kernel is  $(H \cap K)A$ .*

Furthermore,  $H/(H \cap K)A \cong KH/KA$  in a canonical way by  $h((H \cap K)A) \mapsto h(KA)$ . If  $A = \{e\}$ , then we have  $H/H \cap K \cong KH/K$ .

**Theorem 4.11** (Modular Law).  *$G$  a group.  $H, K, L$  subgroups of  $G$  s.t.  $K \subseteq L$ . Then  $(HK) \cap K = (H \cap L)K$ .*

## 5. FEB. 9

**Theorem 5.1** (Homomorphism Theorems). *The following are the four homomorphism theorems.*

- (1)  $\begin{array}{ccc} G & \xrightarrow{f} & H \\ \phi \downarrow & \nearrow \bar{f} & \\ K & & \end{array}$  If  $\phi : G \twoheadrightarrow K$  is a surjective homomorphism and  $f : G \rightarrow H$

is a homomorphism s.t.  $\ker \phi \subseteq \ker f$ . Then there is a unique homomorphism  $\bar{f} : K \rightarrow H$  s.t.  $\bar{f}\phi = f$ . Hence  $\bar{f}(k) = f(a)$  and  $\ker \bar{f} = \phi(\ker f)$ .

- (2) Let  $f : G \twoheadrightarrow H$  a surjective homomorphism then the assignment  $K \rightarrow f(K)$  is a bijective correspondence between subgroups of  $G$  that contain  $\ker f$  and subgroups of  $H$  which preserves inclusion, intersection, and normality.
- (3) Let  $N \trianglelefteq G, H \leq G, A \trianglelefteq H$ . Then  $H/(H \cap N)A \rightarrow NH/NA$  by  $h(H \cap N)A \mapsto hNA$  is a group isomorphism. In particular, if  $A = \{e\}$ , then  $H/H \cap N \cong NH/N$ .

$$\begin{array}{ccc} NH & \xrightarrow{\phi} & NH/NA \\ \subseteq \downarrow & \nearrow \tilde{\phi} & \uparrow \\ H & & \\ \searrow \text{quotient} & & \\ & H/(H \cap N)A & \end{array} \quad \ker \tilde{\phi} = H \cap NA = (H \cap N)A$$

- (4) Let  $K \trianglelefteq G, H \trianglelefteq G, K \subseteq H$ . Then  $G/H \rightarrow (G/K)/(H/K)$  by  $gH \mapsto (gK)H/K$  is an isomorphism.

**Example 5.2.**  $G$  a group,  $g \in G$ . Consider  $\phi : \mathbb{Z} \rightarrow G$  by  $n \mapsto g^n$ . Then  $\ker \phi = m\mathbb{Z}$  where  $m$  is the order of  $g$ . So,  $\mathbb{Z}/m\mathbb{Z} \cong \langle g \rangle$

Note that in  $\mathbb{Z}/m\mathbb{Z}$ , take  $a \in \mathbb{Z}$ .  $a + m\mathbb{Z}$  generates  $\mathbb{Z}/m\mathbb{Z}$  iff  $\gcd(a, m) = 1$ .

**Example 5.3.**  $\det : \mathrm{GL}_n(K) \rightarrow K^\times$  is a surjective group homomorphism (for any commutative ring). Note that  $\ker(\det) = \mathrm{SL}_n(K)$ .

Scalar notation:  $aI, a \in K^\times$  form a normal subgroup of  $\mathrm{GL}_n(K)$ . This is the center.

The quotient  $\mathrm{GL}_n(K)/\{aI\} = \mathrm{PGL}_n(K) \supseteq \mathrm{PSL}_n(K)$ .

$$\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}) \supseteq (\mathbb{Z}/p\mathbb{Z})^\times I \subseteq \mathrm{GL}_{p-1}(\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/p\mathbb{Z})^\times$$

**Example 5.4.** Consider the permutation group on  $n$  letters.

$$S_n \hookrightarrow \mathrm{GL}_n(\mathbb{Z}) \xrightarrow{\det} \{1, -1\} = \mathbb{Z}^\times$$

This induces  $\pi : S_n \rightarrow \mathbb{Z}^{1,-1}$ .

Note that  $\pi$  is surjective as  $\det \begin{bmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 1 & 0 \\ & 0 & \ddots & \\ & & & 1 \end{bmatrix} = -1$ .

Here  $\ker \pi = A_n$  is the alternating group.  $[S_n : A_n] = 2$  and  $S_n/A_n \cong \{1, -1\} = \mathbb{Z}/2\mathbb{Z}$ .

**Example 5.5.** Let  $\phi : G \rightarrow \mathrm{Aut} G$  by  $g \mapsto C_g$  where  $C_g : a \mapsto gag^{-1}$ .

Then  $\ker \phi = Z(G)$  which is the center of  $G$ .  $\phi(G) = \mathrm{Inn} G$  which are the inner automorphism on  $G$ .

As an exercise, show that  $\mathrm{Inn} G \trianglelefteq \mathrm{Aut} G$ .  $\phi C_g \phi^{-1} = C_{\phi g}$ .

**Definition 5.6.** The outer automorphisms  $\mathrm{Out} G = \mathrm{Aut} G / \mathrm{Inn} G$ .

$G$  is complete if  $G \rightarrow \mathrm{Aut} G$  is an isomorphism.

$G$  is simple if  $\{e\}$  and  $G$  are the only normal subgroups of  $G$ .

**Example 5.7.**  $p$  a prime. Then  $\mathbb{Z}/p\mathbb{Z}$  are simple. These are the only simple abelian simple groups.

**Proposition 5.8.**  $G$  a group.  $N \trianglelefteq G, K \trianglelefteq G$ . If  $N \cap K = \{e\}$  then  $nk = kn$  for all  $n \in N, k \in K$ .

*Proof.* Consider  $nkn^{-1}k^{-1}$ . On one hand,  $nkn^{-1} \in K$  and  $k^{-1} \in K$ , so it is in  $K$ . On the other hand,  $n \in N$  and  $kn^{-1}k^{-1} \in N$ , so it is in  $N$ . Therefore,  $nkn^{-1}k^{-1} \in K \cap N = \{e\}$ . Therefore,  $nk = kn$ .  $\square$

Therefore,  $NK = N \times K$  if  $N, K \trianglelefteq G$  and  $N \cap K = \{e\}$ .

**Definition 5.9.** Given a collection of groups  $(G_i)_{i \in I}$ , we define  $\prod_{i \in I} G_i$  to be the set of all functions  $f : I \rightarrow \cup G_i$  s.t.  $\forall i \in I, f(i) \in G_i$  where  $(g \star f)(i) = f(i)g(i)$ , this is the groups called the product of  $G_i$ .

Note that this definition corresponds to the strings of  $g_i$  where  $f \leftrightarrow (g_i)$  s.t.,  $f(i) = g_i$ .

**Definition 5.10.** For all  $i \in I$ , we have a homomorphism  $\alpha_i : G_i \rightarrow \prod G_i$  by

$$g \mapsto f \text{ where } f(j) = \begin{cases} e & j \neq i \\ g & i = j \end{cases}$$

Also, we have  $\pi_i : \prod G_i \rightarrow G_i$  by  $(g_i) \mapsto g_i$ .

Given  $\phi_i : H \rightarrow G_i$ , there is a unique  $\phi : H \rightarrow \prod G_i$  s.t.  $\phi_i = \pi_i \phi$  for all  $i$

Inside of  $\prod_{i \in I} G_i$ , we have subgroups  $\bigoplus_{i \in I} G_i$ ; the direct sums of  $G_i$  which consists of all those  $f$  s.t.  $f(i) \neq e$  for at most finitely many  $i$ .

**Proposition 5.11.** Given any collection  $\phi_i : G_i \rightarrow A_i$  where  $A_i$  abelian groups. There is a unique  $\phi : \bigoplus_{i \in I} G_i \rightarrow A$  s.t.  $\phi \alpha_i = \phi_i$  by  $\phi((g_i)) = \sum \phi_i(g_i)$ .

**Example 5.12.** Suppose  $\gcd(m, n) = 1$ , then  $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  as we have  $\langle m+mn\mathbb{Z} \rangle \cap \langle n+mn\mathbb{Z} \rangle = \{e\}$  where  $\langle m+mn\mathbb{Z} \rangle = \mathbb{Z}/n\mathbb{Z}$  and  $\langle n+mn\mathbb{Z} \rangle = \mathbb{Z}/m\mathbb{Z}$ .

As an exercise, show that

- (1)  $n = p_1^{k_1} \cdots p_s^{k_s}$ ,  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}$ .
- (2)  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\gcd(m, n)\mathbb{Z} \times \mathbb{Z}/\text{lcm}(m, n)\mathbb{Z}$ .

Consider  $A = \bigoplus_{i \in I} \mathbb{Z}$ , then every element of  $A$  can be uniquely written as  $\sum m_i e_i = (m_i)$  for  $m_i \in \mathbb{Z}$  and finitely many of them are not zero.

Let  $G$  be an abelian group (we use additive notation). Then the elements  $(g_i)_{i \in I}$  have the property that  $G \cong \bigoplus_{i \in I} \langle g_i \rangle$  is an isomorphism iff  $\bigoplus \langle g_i \rangle = G$  ( $\{g_i : i \in I\}$  generates  $G$ ).

If  $m_1 g_1 + \cdots + m_s g_s = 0$  then  $m_1 g_1, \dots, m_s g_s = 0$ .

## 6. FEB. 11

**Definition 6.1.** Let  $G_i, i \in I$  be groups. Then  $\prod_{i \in I} G_i = \{f : I \rightarrow \bigcup_{i \in I} G_i : \forall i \in I, f(i) \in G_i\}$ .

A function  $f$  is often denoted  $(f_i)_{i \in I}$  where  $f_i = f(i)$ . We have  $(f \star g)(i) = f(i)g(i)$ .

There are projections:  $\pi_i : \prod G_i \rightarrow G_i$  by  $\pi_i(f) = f(i)$ .

There are also embeddings:  $e_i : G_i \rightarrow \prod G_i$  by  $e_i(g)(j) = \begin{cases} e & j \neq i \\ g & j = i \end{cases}$ .

**Definition 6.2.** The direct sum  $\bigoplus_{i \in I} G_i \subseteq \prod G_i$  of the groups  $G_i$  consists of  $f$  s.t.  $f(i) = e$  except for finitely many  $i$ .

**Proposition 6.3** (Universal Property). Given an abelian group  $A$  and homomorphisms  $\phi_i : G_i \rightarrow A$ , there is a unique  $\phi : \bigoplus_{i \in I} G_i \rightarrow A$  s.t.  $\phi e_i = \phi_i$  by  $\phi((g_i)) = \sum_i \phi_i(g_i)$ .

**Example 6.4.** (1)  $V$  is a vector space over a field  $K$  then  $(V, +) \cong \bigoplus_{i \in I} K$  for some  $I$ .

(2)  $K$  a field. Then  $K$  contains either  $\mathbb{Q}$  or  $\mathbb{Z}/p\mathbb{Z}$  where  $p$  is a prime as a subfield

$$\left( \text{it is called the prime subfield of } K \right). (K, +) \cong \begin{cases} \bigoplus_{i \in I} \mathbb{Q} & \mathbb{Q} \subseteq K \\ \bigoplus_{i \in I} \mathbb{Z}/p\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \subseteq K \end{cases}$$

**Definition 6.5.** A abelian group,  $(a_i)$ ,  $i \in I$  some elements in  $A$ . The natural homomorphism  $\phi : \bigoplus_{i \in I} \langle a_i \rangle \rightarrow A$  by  $(m_i a_i) \mapsto \sum_{i \in I} m_i a_i$ .

1.  $\phi$  is onto iff  $A$  is generated by  $\{a_i\}_{i \in I}$ .

2.  $\phi$  is injective iff whenever  $\sum_{i \in I} m_i a_i = 0$ , we have  $m_i a_i = 0$  for all  $i \in I$ .

If  $(a_i)$  has property 2, we say that  $a_i$  are independent in  $A$ . If in addition they have property 1, we say they form a basis of  $A$ .

**Example 6.6.**  $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ , we have  $\mathbb{Z}/6\mathbb{Z} \cong \langle 3 + 6\mathbb{Z} \rangle \oplus \langle 2 + 6\mathbb{Z} \rangle$ . So,  $\{1 + 6\mathbb{Z}\}$  is a basis of  $\mathbb{Z}/6\mathbb{Z}$  and  $\{3 + 6\mathbb{Z}, 2 + 6\mathbb{Z}\}$  is also a basis of  $\mathbb{Z}/6\mathbb{Z}$ .

**Definition 6.7.** An abelian group  $F$  is called free abelian if it has a basis consisting of elements of infinite orders (then every element  $\neq e \in F$  has infinite orders).

$$F \text{ is free abelian} \iff F \cong \bigoplus_{i \in I} \mathbb{Z}$$

**Corollary 6.8.** Every abelian group is a quotient of a free abelian group. An abelian group can be generated by  $n$  elements iff it is a quotient of  $\mathbb{Z}^n$ .

*Proof.* If  $a_i, i \in I$  generates  $A$ , then the maps  $\phi_i : \mathbb{Z} \rightarrow A$  by  $i \mapsto a_i$  gives surjective homomorphism  $\bigoplus_{i \in I} \mathbb{Z} \rightarrow A$ .

If  $A$  is generated by  $n$  elements then we get  $\mathbb{Z}^n \rightarrow A$ . Conversely, if  $\mathbb{Z}^n \rightarrow A$ , then since  $\mathbb{Z}^n$  is generated by  $n$  elements, we have  $A$  is generated by their images.  $\square$

Idea: in order to understand  $n$ -generated abelian groups, we need to understand subgroups of  $\mathbb{Z}^n$ .

**Example 6.9.**  $n = 1$ , subgroups of  $\mathbb{Z}$  are  $k\mathbb{Z}$  where  $k \geq 0$ , so they are all cyclic.

**Proposition 6.10.** Let  $N \trianglelefteq G$ , if  $N$  can be generated by  $s$  elements and  $G/N$  can be generated by  $t$  elements, then  $G$  can be generated by  $s + t$  elements.

*Proof.* Let  $a_1, \dots, a_s$  generates  $N$  and  $b_1N, \dots, b_tN$  generates  $G/N$ . Consider  $H = \langle a_1, \dots, a_s, b_1, \dots, b_t \rangle$ . Note that  $N \subseteq H$

Also, let  $\pi : G \rightarrow G/N$ , then  $\pi(H)$  contains  $b_1N, \dots, b_tN$ . So,  $\langle g_1N, \dots, g_tN \rangle \subseteq \pi(H)$ . So,  $\pi(H) = G/N$ . By correspondence,  $H = G$ .  $\square$

**Corollary 6.11.** A subset of  $\mathbb{Z}^n$  can be generated by  $n$ -elements.

*Proof.* Induction on  $n$ . If  $n = 1$ ,  $d\mathbb{Z}$  can be generated by  $d$ .

Define  $K \leq \mathbb{Z}^n$ , let  $e_1, \dots, e_n$  be the standard basis.

$\mathbb{Z} \cong \langle e_1 \rangle \subseteq \mathbb{Z}^n \xrightarrow{\pi} \mathbb{Z}^{n-1}$ . Also,  $K \cap \langle e_1 \rangle \subseteq K \rightarrow \pi(K)$ . Note that  $K \cap \langle e_1 \rangle$  is a subgroup of  $\langle e_1 \rangle$ , so it is cyclic.

By induction,  $\pi(K)$  can be generated by  $n - 1$  elements, and  $\pi(K) \cong K/(K \cap \langle e_1 \rangle)$ .  $\square$

**Note 6.12.** Let  $F$  be a free abelian group with basis  $e_1, \dots, e_n$  and  $A$  be subgroups generated by  $w_1, \dots, w_m$  (we don't necessarily have  $m \leq n$ ).

Now,  $w_i = \sum_{j=1}^n m_{i,j} e_j$  where  $m_{i,j} \in \mathbb{Z}$ . Let  $M = (m_{i,j})$  a  $m \times n$  matrix.

Pick  $i \neq j, 1$ . if we replace  $w_i$  by  $w_i + kw_j$  and keep the rest unchanged, then we get another generating set and the new matrix  $M$  which is obtained from  $m$  by adding  $k \cdot j$ th row to the  $i$ th row.

2. if we replace  $e_j$  by  $e_j - k \cdot e_i$  and keep the rest unchanged, then we get a new basis of  $F$  and the corresponding  $M$  is obtained from  $M$  by adding  $k \cdot j$ th column to  $i$ th column of  $M$ .

3. Permuting  $e_i$ 's permutes the column and permuting  $w_i$ 's permutes the rows.

We start with  $M$ . Find the non-zero entry of the smallest absolute value of  $M$  and permute, so it is the 1-1 entry. Replacing  $e_i$  by  $-e_i$  we may assume that  $k_{1,1} > 0$ .

Suppose  $k_{i,1} \nmid k_{1,1}$  for some  $i$ . Then  $k_{i,1} = pk_{1,1} + r$  for  $0 < r < k_{1,1}$ . Subtracting  $p \cdot$  1st row from  $i$ th and have  $k_{i,1} = r < k_{1,1}$ .

Repeat the process, then we have the resulting  $\bar{e}_1, \dots, \bar{e}_n$  is a basis,  $\bar{w}_1 = k_{1,1}\bar{e}_1$  and  $\{\bar{w}_2, \dots, \bar{w}_m\} \subseteq \langle \bar{e}_2, \dots, \bar{e}_n \rangle$ .

**Theorem 6.13.** *There is a basis  $\{\bar{e}_1, \dots, \bar{e}_n\}$  of  $F$  and  $k_1|k_2|k_3|\dots|k_r$  s.t.  $k_1\bar{e}_1, \dots, k_r\bar{e}_r$  generate  $A$ .*

**Corollary 6.14.**  *$A$  is free with basis  $k_1\bar{e}_1, \dots, k_r\bar{e}_r$ .*

**Corollary 6.15.**  *$F/A \cong \mathbb{Z}/k_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/k_r\mathbb{Z} \oplus \mathbb{Z}^{n-s}$ .*

## 7. FEB. 14

**Theorem 7.1.** *Let  $F$  be a free abelian group with basis of size  $n$ , and let  $\{0\} \neq A < F$ . Then there is a basis  $e_1, \dots, e_n$  of  $F$  and positive integers  $k_1|k_2|\dots|k_s$  for some  $s \leq n$  s.t.  $k_1e_1, k_2e_2, \dots, k_se_s$  generate  $A$ .*

The idea of the proof is to start with a basis  $b_1, \dots, b_n$  of  $F$  and generating set  $w_1, \dots, w_v$  of  $A$ . Write  $w_i = \sum_j m_{ij}b_j$  and consider  $M = (m_{ij})$ . By a sequence of operations of the form

- (1) For  $i \neq j$ , replace  $w_i$  by  $w_i + kw_j$  for some  $k \in \mathbb{Z}$ .
- (2) For  $i \neq j$ , replace  $e_i$  by  $e_i + kw_j$  for some  $k \in \mathbb{Z}$ .
- (3) Permute the basis basis elements or the generators of  $A$ .
- (4) Replace a basis element or generator by its inverse.

transform the bases and generating set, so that the corresponding  $M$  is

$$\left[ \begin{array}{ccc|c} k_1 & & 0 & \\ 0 & \ddots & & 0 \\ & & k_s & \\ \hline 0 & & 0 & 0 \end{array} \right].$$

We often call the bases in the theorem a compatible choice of bases of  $F$  and  $A$ .

**Corollary 7.2.**  *$A$  is free abelian. In general, a subgroup of any free abelian group is free abelian.*

**Theorem 7.3.** *Let  $G$  be a finitely generated abelian group. Then  $G \cong \mathbb{Z}/k_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/k_r\mathbb{Z} \oplus \mathbb{Z}^t$  for some  $1 < k_1|k_2|\dots|k_r$  and  $t \geq 0$ .*

*Proof.* Since  $G$  is  $n$ -generated, then we have a surjective map  $\mathbb{Z}^n \xrightarrow{\pi} G$ . If  $\ker(\pi) = A$ , choose compatible basis  $\{e_1, \dots, e_n\}$  of  $\mathbb{Z}^n$  and  $l_1e_1, \dots, l_se_s$  of  $A$  so that  $l_1|l_2|\dots|l_s$ . Then we have  $\mathbb{Z}/A \cong \mathbb{Z}/l_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/l_s\mathbb{Z} \oplus \mathbb{Z}^{n-s}$  and if we remove all  $l_i = 1$ , we have the result.  $\square$

**Proposition 7.4.**  *$\mathbb{Z}^n$  can not be generated by fewer than  $n$  elements.*

*Proof.*  $\mathbb{Z}^n \subseteq \mathbb{Q}^n$  and if  $e_1, \dots, e_k$  generates  $\mathbb{Z}^n$  as abelian group, then  $e_1, \dots, e_k$  span  $\mathbb{Q}^n$  as  $\mathbb{Q}$ -vector space.

If  $v \in \mathbb{Q}^n$  then  $N \cdot v = \mathbb{Z}^n$  and thus  $N \cdot v = \sum m_i e_i$ ,  $v = \sum \frac{m_i}{N} e_i$ . Therefore,  $k \geq n$ .)  $\square$

**Corollary 7.5.** *If  $k \neq n$  then  $\mathbb{Z}^k \not\cong \mathbb{Z}^n$ .*

*Proof.* If  $k < n$ , then  $\mathbb{Z}^k$  is generated by  $k$  elements, but  $\mathbb{Z}^n$  cannot be generated by  $n$  elements.  $\square$

**Definition 7.6.** The number of basis elements of a finitely generated abelian group  $F$  is unique, and is called the rank of  $F$ .

Let  $G \cong \mathbb{Z}/k_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/k_r\mathbb{Z} \oplus \mathbb{Z}^t$ , where  $1 < k_1|k_2|\dots|k_r$ . Then

- (1)  $\mathbb{Z}/k_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/k_r\mathbb{Z}$  are the elements of finite order, we call it the torsion of  $G$ , and denote  $T(G)$ .
- (2)  $\mathbb{Z}^t \cong G/T(G)$ , so  $t$  is the rank of  $G/T(G)$ .
- (3)  $k_r$  is the exponent of  $T(G)$ .
- (4) Let  $r$  be the smallest number of generator of  $T(G)$ ,  $T(G) = \mathbb{Z}/k_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/k_r\mathbb{Z}$  can be generated by  $r$  elements.

Let  $p|k_1$  be a prime. Then  $T(G)/pT(G) = (\mathbb{Z}/p\mathbb{Z})^r$ . This is a vector space over  $\mathbb{Z}/p\mathbb{Z}$ . So cannot be spanned by fewer than  $r$  elements.

As an exercise show that  $k_i$  is the smallest positive integers so that  $k_i \cdot T(G)$  can be generated by  $r - i$  elements.

**Corollary 7.7.**  *$k_i$  are unique for  $G$ , and called the invariant factors of  $G$ .*

Show as an exercise that  $r + t$  is the smallest number of generators of  $G$ .

**Definition 7.8.** Let  $A$  be an abelian group. Then  $T(A)$  is all the elements of finite order in  $A$ . This is a subgroup of  $A$ .

**Definition 7.9.** A subgroup  $N$  of  $G$  is characteristic if for every  $\phi(N) = N$ .

As an exercise, show

- (1)  $N$  is characteristic in  $G$  implies that  $N$  is normal in  $G$ .
- (2)  $T(A)$  is characteristic in  $A$ .

**Definition 7.10.**  $A$  is torsion if  $A = T(A)$ .  $A$  is torsion free if  $T(A) = \{0\}$ .

**Proposition 7.11.**  $A/T(A)$  is torsion free.

**Definition 7.12.** Given  $n \in \mathbb{N}$ . Then  $nA = \{na : a \in A\} \leq A$ , and  $A[n] = \{a \in A : na = 0\} \leq A$ .

Note that there is a natural injection from  $A[n]$  into  $A$ , and a natural surjection from  $A$  onto  $nA$ .

**Definition 7.13.** Let  $p$  be a prime, then  $A_p = \{a \in A : p^k a = 0 \text{ for some } k \in \mathbb{N}\} = \bigcup_{k=1}^{\infty} A[p^k]$ . We call it the  $p$ -primary part of  $A$ .

Note that  $A[p] \subseteq A[p^2] \subseteq \dots \subseteq A[p^n] \subseteq \dots$

**Definition 7.14.** Let  $H_i$  for  $i \in I$  be a family of subgroups of  $G$ . It is a chain if for any  $i, j \in I$ , either  $H_i \subseteq H_j$  or  $H_j \subseteq H_i$ .

Show as an exercise that the union of any chain of subgroups is a subgroup.

**Proposition 7.15.** *If  $A$  is a torsion abelian group, then  $A \cong \bigoplus_{p \text{ prime}} A_p$*

*Proof.* Since  $A_p$  are subgroups, we have the natural embeddings  $A_p \hookrightarrow A$ . Take the induced homomorphism  $\bigoplus_p A_p \rightarrow A$ . Then  $(a_p) \mapsto \sum_p a_p$ .

Let  $a \in A$ , and  $n$  be the order of  $a$ . Then  $n = p_1^{k_1} \cdots p_s^{k_s}$  is its prime factorization. Then  $\frac{n}{p_i^{k_i}} a \in A_{p_i}$  since  $p_i^{k_i} \cdot \frac{n}{p_i^{k_i}} a = na = 0$ .

We observe that  $\frac{n}{p_1^{k_1}}, \dots, \frac{n}{p_s^{k_s}}$  have non trivial common divisors, so  $m_1 \frac{n}{p_1^{k_1}} + \dots + m_s \frac{n}{p_s^{k_s}} = 1$  for some  $m_1, \dots, m_s$ . So,  $a = m_1 \frac{n}{p_1^{k_1}} a + \dots + m_s \frac{n}{p_s^{k_s}} a$ .

Suppose  $a_{p_1} \in A_{p_1}$  and  $a_{p_1} + \dots + a_{p_s} = 0$ . There is  $N$  s.t.  $p_i^N \cdot a_{p_i} = 0$  for all  $p_i$ . Then  $p_2^N \cdots p_t^N (a_{p_1} + \dots + a_{p_t}) = 0 = p_2^N \cdots p_t^N a_{p_1}$ , so order of  $a_{p_1} | p_2^N \cdots p_t^N$  and so order of  $a_{p_1} | p_1^s$ , therefore,  $s=0$ .  $\square$

**Note 7.16.**  $G$  a finite abelian group. Then  $G = G_{p_1} \oplus \dots \oplus G_{p_s}$  for some  $p_i$ . Then  $G_{p_i} \cong \mathbb{Z}/p_1^{m_{i1}} \mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_i^{m_{ik_i}} \mathbb{Z}$ ,  $m_{i1} \leq \dots \leq m_{ik_i}$ .

$$G_{p_i} = p_i^{m_{i1} + \dots + m_{ik_i}} = p_i^{k_i} \text{ where } |G| = N = p_1^{k_1} \cdots p_s^{k_s}.$$

**Corollary 7.17.** *Every finite abelian group is a direct sum of cyclic groups of prime power orders and the collection of all prime power order is unique for the group. We call the prime powers appearing elementary divisors.*

**Example 7.18.**  $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z}$

8. FEB. 16

**Theorem 8.1.**  $G$  finitely generated abelian group. Then

- (1)  $G \cong T(G) \times \mathbb{Z}^t$  for some  $t$  which is unique and called the (torsion free) rank of  $G$ .
- (2)  $T(G) \cong \mathbb{Z}/k_1\mathbb{Z} \times \dots \times \mathbb{Z}/k_s\mathbb{Z}$  is finite, where  $1 < k_1 | k_2 | \dots | k_s$  are unique for  $G$  and called the invariant factors of  $G$ .
- (3)  $T(G) \cong T(G)_{p_1} \times \dots \times T(G)_{p_k}$  where  $|T(G)| = p_1^{m_1} \cdots p_k^{m_k}$ , and the invariant factors of  $T(G)_{p_i}$  together are unique for  $G$  and called the elementary divisors of  $G$ .

So,  $T(G)$  is a direct sum of cyclic groups of prime power order in an essentially unique way.

**Definition 8.2.**  $G$  abelian group,  $n \in \mathbb{N}$ . Then

- (1)  $G[n] = \{g \in G : ng = 0\}$  is a subgroup.
- (2)  $nG = \{ng : g \in G\}$  is a subgroup.
- (3)  $p$  a prime.  $G_p = \{g \in G : p^k g = 0 \text{ for some } k\} = \bigcup_k G[p^k]$  is a subgroup called the  $p$ -primary component.
- (4)  $T[G] = \{g : ng = 0 \text{ for some } n > 0\} = \bigcup_n G[n!]$  is a subgroup.

Note, we have  $G/T(G)$  is torsion-free.

**Theorem 8.3.** If  $G$  torsion, then  $G \cong \bigoplus_{p \text{ prime}} G_p$ .

Show as an exercise that if  $G$  is abelian and  $G/A$  is free abelian, then  $G \cong A \times G/A$ .

Warning:  $T(G)$  is not always a direct summand to  $G$  ( $G \not\cong T(G) \times G/T(G)$ )

**Example 8.4.** Consider  $(\mathbb{Q}, +)$ . Every 2 elements of  $\mathbb{Q}$  are dependent, for  $\frac{p}{q}, \frac{m}{n}$ , we have  $mq\frac{p}{q} - pn\frac{m}{n} = 0$ . So,  $\mathbb{Q}$  is not free abelian, it is torsion-free, not cyclic.



**Example 8.5.** Consider  $S^1 = \{z \in \mathbb{C} : |z| = 1\}$  with  $\cdot$ .

$T(S^1) = \mu_\infty$  is all roots of unity which is  $\{e^{2\pi i \frac{m}{n}} : \frac{m}{n} \in \mathbb{Q}\}$ .

$T(S^1)_p = \mu_p^\infty$  is all roots of unity of  $p$ -power order.

We have a surjective homomorphism,  $E : (\mathbb{R}, +) \rightarrow S^1$  by  $t \mapsto e^{2\pi i t} = \cos(2\pi t) + i \sin(2\pi t)$ . Here,  $\ker E = \mathbb{Z}$ . So,  $S^1 \cong \mathbb{R}/\mathbb{Z}$  with  $E^{-1}(T(S^1)) = \mathbb{Q}$ .

So,  $\mu_\infty \cong \mathbb{Q}/\mathbb{Z}$  and  $\mu_p^\infty = \{\text{rational numbers with } p\text{th power denominators}\}/\mathbb{Z}$

$S^1/T(S^1) \cong (\mathbb{R}/\mathbb{Z})/(\mathbb{Q}/\mathbb{Z}) \cong \mathbb{R}/\mathbb{Q} \cong \bigoplus \mathbb{Z}$ .

As an exercise. show that  $S^1 \cong T(S^1) \times \mathbb{R}/\mathbb{Q}$  where  $\mathbb{R}/\mathbb{Q} \cong S^1/T(S^1)$ .

Note that  $\mu_p^\infty$  is infinite but every proper subgroup is finite and cyclic.

**Definition 8.6.**  $G$  abelian,  $n \in \mathbb{N}$ . Then

- (1)  $a \in G$  is  $n$ -divisible if  $a = nb$  for some  $b \in G$ .
- (2)  $G$  is  $n$ -divisible if all elements of  $G$  are  $n$ -divisible.
- (3)  $G$  is divisible if it is  $n$ -divisible for every  $n$ .

**Example 8.7.**  $\mathbb{Q}$  is divisible,  $\mathbb{Q}/\mathbb{Z}$  is divisible,  $\mu_p^\infty$  are divisible,  $S^1$  is divisible.

Show as an exercise that if  $G$  is divisible then  $G/A$  is divisible for any  $A \leq G$ . Also, if  $A$  is divisible then  $A \leq G \implies G \cong A \oplus G/A$ .

**Definition 8.8.**  $G$  is abelian.  $A \leq G$ , then  $A$  is called pure in  $G$  if for any  $a \in A$  and any  $n \in \mathbb{Z}$  if  $a = ng$  for some  $g \in G$  then  $a = nb$  for some  $b \in A$  (i.e.,  $A \cap nG = nA$ ).

**Theorem 8.9.** Every divisible group is a direct sum of groups isomorphic to  $\mathbb{Q}$  or  $\mu_p^\infty$  for some prime  $p$ .

**Note 8.10.**  $A$  torsion and  $A[n] = \{0\}$  then  $A = nA$ . If  $|g| = k$ ,  $\gcd(n, k) = 1$  then  $\langle g^n \rangle = \langle g \rangle$ .

**Theorem 8.11.**  $G$  abelian,  $A < G$  pure,  $G/A$  a direct sum of cyclic groups (i.e.,  $G/A$  has a basis), then  $G \cong A \oplus G/A$ .

**Theorem 8.12.**  $G = G_p$  is an abelian  $p$ -group of finite exponent ( $G = G[p^k]$  for some  $k$ ) then  $G$  is a direct sum of cyclic groups.

**Corollary 8.13.** If  $G$  abelian of finite exponent, then  $G$  is a direct sum of cyclic groups.

Show as an exercise that  $T(G)$  is always pure in  $G$ .

**Theorem 8.14.** If  $T(G)$  is of finite exponent then  $G \cong T(G) \times G/T(G)$ .

9. FEB. 18

**Theorem 9.1.** An abelian group of finite exponent is a direct sum of cyclic groups.

**Theorem 9.2.** If  $A \leq G$  and  $A$  is pure in  $G$  and  $G/A$  is a direct sum of cyclic group, then  $G \cong A \times G/A$ .

**Theorem 9.3.**  $A \leq G$  pure and of finite exponent, then  $G \cong A \oplus G/A$ .

**Theorem 9.4.** If  $T(A)$  is of finite exponent then  $A \cong T(A) \times A/T(A)$ .

**Theorem 9.5** (Kulikov).  $G$  torsion abelian then  $G$  has a pure subgroup  $A$  which is a direct sum of cyclic groups and  $G/A$  is divisible.

$$A \hookrightarrow G \twoheadrightarrow G/A$$

Let  $G$  be a group.  $X \subseteq G$  s.t.  $G = \langle X \rangle$ . This means that every element of  $G$  is of the form  $g_1^{\epsilon_1} \dots g_k^{\epsilon_k}$  with  $g_i \in X$ ,  $\epsilon_i = \pm 1$ .

Usually there are many ways a given element can be written like.

Trivial reasons: We can always insert somewhere  $gg^{-1}$  or  $g^{-1}g$ ;  $g \in X$ .

Question: Are there groups  $G$  and  $X \subseteq G$  where this is the only reason?

**Definition 9.6.**  $X$  a set. A word of length  $n$  over  $X$  is a sequence of  $n$  elements from  $X$  (repetition allowed):  $a_1 a_2 \dots a_n$  where  $a_i \in X$ . Note, word of length 0 is the empty word.

$W(X)$  is the set of all finite words. Given 2 words,  $u, w \in W(X)$ , we can concatenate them with  $u \star w = uw$ . This is an associative binary operation, and it makes  $W(X)$  a monoid. It is called the free monoid on  $X$ .

Show as an exercise that given any monoid  $M$  and any function  $f : X \rightarrow M$  it extends uniquely to a homomorphism  $W(X) \rightarrow M$ .

**Definition 9.7.**  $X$  a set. Consider  $X \times \{1, -1\}$ . We write  $x$  for  $(x, 1)$  and  $x^{-1}$  for  $(x, -1)$ . Consider  $W(X \times \{1, -1\})$ .

A word  $x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$  in  $W(X \times \{1, -1\})$  is reduced if whenever  $x_i = x_{i+1}$  we have  $\epsilon_i \neq -\epsilon_{i+1}$ .

$R(X)$  is the set of all reduced words in  $W(X \times \{1, -1\})$ .

**Note 9.8.**  $M$  is a group and  $f : X \rightarrow M$  then it extends to  $f : X \times \{-1, 1\} \rightarrow M$  by  $(x, 1) \mapsto f(x)$  and  $(x, -1) \mapsto f(x)^{-1}$  and it extends to monoid homomorphism  $W(X \times \{1, -1\}) \rightarrow M$ . Clearly equivalent words have the same images in  $M$ .

$R(X)$  is the set of reduced words in  $W(X \times \{1, -1\})$  and it has a binary operation  $u \star w = uw$  and reduced.

This operation has inverses as  $(x_1^{\epsilon_1} \dots x_n^{\epsilon_n})^{-1} = x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1}$ . We have  $(x_1^{\epsilon_1} \dots x_n^{\epsilon_n})(x_n^{-\epsilon_n} \dots x_1^{-\epsilon_1}) = \emptyset$

Problem is that is this operation associative? Yes, but technical complication.

**Definition 9.9.**  $G$  a group.  $X \subseteq G$  a subset. We say  $X$  generates  $G$  freely if the natural map  $R(X) \rightarrow G$  is bijective (So,  $X$  generates  $G$ ).

If this happens then  $R(X)$  is a group.

Note that if  $X$  generates freely  $G$ ,  $Y$  generates freely  $H$ .  $f : X \rightarrow Y$  is a bijection, then it extends to an isomorphism  $G \rightarrow H$ .

**Example 9.10.** Let  $X = \{1\}$ , we have  $G = \mathbb{Z}$  and  $\{1\}$  generates freely  $\mathbb{Z}$ .

Show as an exercise that if  $X$  generates freely  $G$ ,  $f : X \rightarrow H$  any function to a group  $H$ , then it extends uniquely to a homomorphism  $G \rightarrow H$ .

10. FEB. 21

**Definition 10.1.**  $X$  a set.  $W(X \times \{1, -1\})$  is the free monoid. Then  $R(X)$  is all reduced words in  $X \cup X^{-1}$  which is a subgroup of  $W(X \times \{1, -1\})$ .  $R(X)$  has a binary operation with every element “invertible,” but not yet established that it is surjective.

Given any group  $G$  and a function  $X : X \rightarrow G$ , there is a unique monoid homomorphism  $f : W(X \times \{1, -1\}) \rightarrow G$  by  $x \mapsto f(x)$  and  $x^{-1} \mapsto f(x^{-1})$  for  $x \in X$  and it restricts to a “homomorphism” on  $R(X)$ .

**Definition 10.2.** Let  $G$  be a group with generating set  $X$ . We say that  $X$  generates freely  $G$  if the natural map  $R(X) \rightarrow G$  is a bijection.

If such a group exists, then  $R(X)$  is a group.

**Note 10.3.** If  $R(X)$  is not a bijection, then there is a non trivial reduced word  $w$  which is mapped onto  $e \in G$ .

*Proof.* Choose shortest reduced word  $u$  s.t.  $f(u) = f(v)$  for some  $v \neq u$ . If  $u = \emptyset$ , then  $w = v$  works.

Otherwise, suppose  $u$  starts with  $x^\epsilon$ ,  $x \in X$ ,  $\epsilon = \pm 1$  and  $u = x^\epsilon u_1$ . If  $v = x^\epsilon v_1$ , then  $f(u) = f(x)^\epsilon f(u_1) = f(x)^\epsilon f(v_1)$ . So  $f(u_1) = f(v_1)$  and  $u_1$  is shorter which is a contradiction. So,  $v \neq x^\epsilon v_1$  and therefore  $u^{-1}v$  is reduced and  $f(u^{-1}v) = f(u)^{-1}f(v) = e$ . So  $G$  is freely generated by  $X$  iff  $G$  is generated by  $X$  and no non-trivial reduced word in  $X$  represents  $e$ .  $\square$

**Definition 10.4.** Assume free group on 2 elements exists,  $G = \langle a, b \rangle$  is freely generated by  $a, b$ .

$$\text{Notation, for } x \text{ a letter, } n \in \mathbb{Z}_{\neq 0} \text{ define } X^n = \begin{cases} \overbrace{x \cdot \dots \cdot x}^n & n > 0 \\ \underbrace{x^{-1} \cdot \dots \cdot x^{-1}}_{-n} & n < 0 \end{cases}$$

**Note 10.5.** Reduced words in  $a, b$  are of the form  $a^{n_1}b^{n_2}\dots c^{n_k}$  where  $c = a$  or  $b$ , or  $b^{n_1}a^{n_2}\dots c^{n_k}$  where  $c = a$  or  $b$ .

**Theorem 10.6.** Let  $a = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ ,  $b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})$ . The subgroup  $\langle a, b \rangle$  of  $SL_2(\mathbb{Z})$  is freely generated by  $\{a, b\}$ .

*Proof.* Let  $w$  be a non-trivial reduced word in  $F(\{a, b\})$ . We need to show  $w \neq e$  in  $\langle a, b \rangle$ .

First, assume that  $w$  starts with  $b$  or  $b^{-1}$ ; i.e.,  $w = b^i \dots c^\epsilon$  where  $i, \epsilon \in \{1, -1\}$  and  $c \in \{a, b\}$ . Take  $\delta = \begin{cases} 1 & \text{if } c^\epsilon = a, b, b^{-1} \\ -1 & \text{if } c^\epsilon = a^{-1} \end{cases}$ , and  $u = a^{-\delta} w a^\delta$ . Since  $a^{-\delta}$  and  $a^\delta$  does not cancel with  $b^i$  and  $c^\epsilon$  respectively,  $u$  is also a reduced word. If  $w = e$ , then  $u = a^{-\delta} e a^\delta = e$ ; and if  $u = e$ , then  $w = a^\delta e a^{-\delta}$ . So,  $w = e$  iff.  $u = e$ . So, it suffices to show that  $w = a^{d_1} b^{d_2} \dots c^{d_k}$  where  $c \in \{a, b\}$ ,  $d_1, \dots, d_k \in \mathbb{Z}_{\neq 0}$  is not  $e$ .

We will first show by induction that  $a^d = \begin{bmatrix} 1 & dz \\ 0 & 1 \end{bmatrix}$  and  $b^d = \begin{bmatrix} 1 & 0 \\ dz & 1 \end{bmatrix}$  for  $d \in \mathbb{Z}$ . By definition,  $a^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  and  $b^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ . If  $a^d = \begin{bmatrix} 1 & dz \\ 0 & 1 \end{bmatrix}$  and  $b^d = \begin{bmatrix} 1 & 0 \\ dz & 1 \end{bmatrix}$ , then  $a^{d+1} = \begin{bmatrix} 1 & dz \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & (d+1)z \\ 0 & 1 \end{bmatrix}$  and similarly,  $b^{d+1} = \begin{bmatrix} 1 & 0 \\ dz & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ z & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (d+1)z & 1 \end{bmatrix}$ . So, by PMI, this is true for  $d \in \mathbb{N}$ . Now, since  $\begin{bmatrix} 1 & dz \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -dz \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ , we have  $a^{-dz} = \begin{bmatrix} 1 & -dz \\ 0 & 1 \end{bmatrix}$ ; and similarly, we have  $b^{-dz} = \begin{bmatrix} 1 & 0 \\ -dz & 1 \end{bmatrix}$ . Therefore,  $\forall d \in \mathbb{Z}$ ,  $a^d = \begin{bmatrix} 1 & dz \\ 0 & 1 \end{bmatrix}$  and  $b^d = \begin{bmatrix} 1 & 0 \\ dz & 1 \end{bmatrix}$ .

Now, define  $(\alpha_i)$  recursively by  $\alpha_0 = 1$ ,  $\alpha_1 = d_1 z$ , and for  $n \geq 2$ ,  $\alpha_n = \alpha_{n-2} + d_n z \alpha_{n-1}$  where  $d_n$  are such powers that are defined in  $w = a^{d_1} b^{d_2} \dots c^{d_k}$ . We will

now induct on  $k$  to show that  $w = \begin{cases} \begin{bmatrix} \alpha_k & \alpha_{k-1} \\ \cdot & \cdot \end{bmatrix} & \text{if } k \text{ is even} \\ \begin{bmatrix} \alpha_{k-1} & \alpha_k \\ \cdot & \cdot \end{bmatrix} & \text{if } k \text{ is odd} \end{cases} \text{ for } k \in \mathbb{N}.$

$$\text{If } k = 1, \text{ then } w = a^{d_1} = \begin{bmatrix} 1 & d_1 z \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha_0 & \alpha_1 \\ \cdot & \cdot \end{bmatrix}.$$

$$\text{If } k = 2, \text{ then } w = a^{d_1} b^{d_2} = \begin{bmatrix} \alpha_0 & \alpha_1 \\ \cdot & \cdot \end{bmatrix} \begin{bmatrix} 1 & 0 \\ d_2 z & 1 \end{bmatrix} = \begin{bmatrix} \alpha_0 + \alpha_1 d_2 z & \alpha_1 \\ \cdot & \cdot \end{bmatrix} = \begin{bmatrix} \alpha_2 & \alpha_1 \\ \cdot & \cdot \end{bmatrix}.$$

$$\text{Now, assume for some odd } k > 2, \text{ we have } a^{d_1} b^{d_2} \dots b^{k-1} = \begin{bmatrix} \alpha_{k-1} & \alpha_{k-2} \\ \cdot & \cdot \end{bmatrix}.$$

$$\text{Then } a^{d_1} b^{d_2} \dots b^{d_{k-1}} a^{d_k} = \begin{bmatrix} \alpha_{k-1} & \alpha_{k-2} \\ \cdot & \cdot \end{bmatrix} \begin{bmatrix} 1 & d_k z \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha_{k-1} & \alpha_{k-2} + d_k z \alpha_{k-1} \\ \cdot & \cdot \end{bmatrix} = \begin{bmatrix} \alpha_{k-1} & \alpha_k \\ \cdot & \cdot \end{bmatrix}.$$

$$\text{Similarly, assume for some even } k > 2, \text{ we have } a^{d_1} b^{d_2} \dots a^{k-1} = \begin{bmatrix} \alpha_{k-2} & \alpha_{d_{k-1}} \\ \cdot & \cdot \end{bmatrix}$$

$$\text{Then } a^{d_1} b^{d_2} \dots a^{k-1} b^k = \begin{bmatrix} \alpha_{k-2} & \alpha_{k-1} \\ \cdot & \cdot \end{bmatrix} \begin{bmatrix} 1 & 0 \\ d_k z & 1 \end{bmatrix} = \begin{bmatrix} \alpha_{k-2} + d_k z \alpha_{k-1} & \alpha_{k-1} \\ \cdot & \cdot \end{bmatrix} = \begin{bmatrix} \alpha_k & \alpha_{k-1} \\ \cdot & \cdot \end{bmatrix}.$$

$$\text{Therefore, by PMI, } w = \begin{cases} \begin{bmatrix} \alpha_k & \alpha_{k-1} \\ \cdot & \cdot \end{bmatrix} & \text{if } k \text{ is even} \\ \begin{bmatrix} \alpha_{k-1} & \alpha_k \\ \cdot & \cdot \end{bmatrix} & \text{if } k \text{ is odd} \end{cases}.$$

Consider  $|\alpha_i|$ , we will show that  $|\alpha_i|$  is an increasing sequence and thus never = 0.

Since  $|z| \geq 2$ ,  $\alpha_1 = |d_1 z| = |d_1| |z| \geq 2 > |\alpha_0|$  as  $d_1 \neq 0$ . If  $|\alpha_{k-1}| > |\alpha_{k-2}|$ , then  $|\alpha_k| = |\alpha_{k-2} + d_k z \alpha_{k-1}| > |d_k z| |\alpha_{k-1}| - |\alpha_{k-2}| > (|d_k z| - 1) |\alpha_{k-1}| > (2 - 1) |\alpha_{k-1}| = |\alpha_{k-1}|$ . Therefore,  $|\alpha_i|$  is an increasing sequence by PMI. So,  $\forall k$ ,  $|\alpha_k| \neq 0$  and thus  $w \neq e$ .

Therefore,  $\langle a, b \rangle$  is free.  $\square$

**Proposition 10.7.** *Let  $x_n = a^n b a^n$  where  $n = 1, 2, 3, \dots$ . Then  $H = \langle x_1, x_2, \dots \rangle$  is freely generated by  $x_1, x_2, \dots$ .*

*Proof.*  $x_n^{-1}$  is represented in  $G$  by  $a^{-n} b^{-1} a^{-n}$ . Elements of  $X \cup X^{-1}$  are of the form,  $a^m b^{\epsilon_m} a^m$  where  $m \in \mathbb{Z}$  and  $m \neq 0$ . Now reduced words in  $R(x_1, \dots)$  look like  $a^{m_1} b^{\epsilon_1} a^{m_2} b^{\epsilon_2} a^{m_2} \dots a^{m_k} b^{\epsilon_k} a^{m_k}$ ;  $\epsilon_i = \text{sign } m_i$  and  $m_i + m_{i+1} \neq 0$ . So these are also non-trivial reduced words of  $a, b$  and hence non-zero.  $\square$

**Corollary 10.8.** *For any finite set  $X$ ,  $R(X)$  is a group (i.e., the operation is associative).*

**Corollary 10.9.** *For every  $X$ ,  $R(X)$  is a group.*

*Proof.* Take 3 reduced words,  $u, v, w$ . We need  $(uv)w = u(vw)$ . But  $u, v, w \in R(Y)$  for some finite subset  $Y$  of  $X$  which we know is a group.  $\square$

**Definition 10.10.** A group is free if it is freely generated by a subset  $X$ . Then  $A = R(X) = \text{Free}(X)$ .

**Theorem 10.11.** Every group is isomorphic to a quotient of a free group.

*Proof.* We have a surjective homomorphism  $\text{Free}(G) \rightarrow G$ , so  $G \cong \text{Free}(G)/\ker$ .  $\square$

**Definition 10.12.** Let  $(w_i)_{i \in I}$  be words of  $\text{Free}(X)$ . Let  $H$  be the smallest normal subgroup of  $\text{Free}(X)$  generated by  $\{w_i : i \in I\}$ . Then  $\langle X | w_i, i \in I \rangle$  is the group  $\text{Free}(X)/H$ .

**Example 10.13.**  $\langle \{a\} | a^n \rangle = \mathbb{Z}/n\mathbb{Z}$ , for  $n > 0$

**Theorem 10.14.** A subgroup of a free group is free.

11. FEB. 23

**Theorem 11.1.** Let  $a = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ ,  $b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \in \text{SL}_2(\mathbb{Z})$  and  $H = \langle a, b \rangle$ . Then this is freely generated by  $\{a, b\}$ .

**Corollary 11.2.** For any set  $X$ , the structure  $R(X)$  is a group, denoted  $\text{Free}(X)$  and called the free group on  $X$ .

**Theorem 11.3.** Any group is isomorphic to a quotient of a free group.

**Definition 11.4.** Given a set  $X$  and a collection of reduced words  $w_i$ ,  $i \in I$  in  $\text{Free}(X)$ . Then  $\langle X | w_i, i \in I \rangle = \text{Free}(X)/N$  with  $N$  is the smallest normal subgroups of  $\text{Free}(X)$  which contains all  $w_i, i \in I$ . If a group  $G$  is isomorphic to  $\langle X | w_i, i \in I \rangle$ . Then any isomorphism  $\langle X | w_i, i \in I \rangle \rightarrow G$  is called a presentation of  $G$ .

**Example 11.5.**  $D_\infty = \langle a, b | a^2, b^2 \rangle = \langle c, d | d^2, dcd^{-1}c \rangle$ .

**Definition 11.6.**  $G$  is called finitely presented if it has a presentation of finitely generators and finitely many relations.

**Theorem 11.7.** Any finite group is finitely presented.

*Proof.*  $G$  finite.  $G \cong \text{Free}(X)/N$  where  $X$  is finite. So  $N$  is of finite index in  $\text{Free}(X)$ .  $\square$

**Theorem 11.8.** A subgroup of finite index in a finitely generated group is finitely generated.

**Example 11.9.**  $\mathbb{Z}^2 \cong \langle a, b | a^{-1}b^{-1}ab \rangle = \text{Free}(\{a, b\})/N$  but  $N$  is not finitely generated as  $N = [\text{Free}(a, b), \text{Free}(a, b)]$

Goal: To prove the Nielsen-Schreier theorem. A subgroup of any free group is free.

$G$  a group.  $X$  a generating set,  $H \leq G$ . Let  $S$  be the set of choice of left coset representatives for  $H$  in  $G$  s.t.  $e \in S$ .

For any  $g \in G$ , there is a unique  $\bar{g} \in S$  s.t.  $gH = \bar{g}H$ .

**Note 11.10.**  $(\bar{g}) = \bar{g}$ ,  $g_1\bar{g}_2 = g_1\bar{g}_2$ . For  $s \in S$ ,  $\bar{s} = s$  and  $\forall g, \bar{g}^{-1}g \in H$  and for all  $h \in H$ ,  $\bar{h} = e$ ,

Given  $g \in G$ ,  $s \in S$ , there is unique  $t \in S$  s.t.  $t^{-1}gs \in H$  with  $t = \bar{g}s$ . We denote  $t^{-1}gs$  by  $h(g, s) = (\bar{g}s)^{-1}(gs)$ ; i.e.,  $h(g, s) = t^{-1}gs$ .

Here,  $h(g, s)^{-1} = s^{-1}g^{-1}t = h(g^{-1}, t)$ .

**Proposition 11.11.** Let  $Y = \{h(x, s) : x \in X, s \in S\}$ , then  $Y' = \{h(x^{-1}, s) : x \in X, s \in S\}$ . Thus,  $H = \langle Y \rangle$ .

**Definition 11.12.** Let  $G = \text{Free}(X)$ ,  $H \leq G$ . A set  $S$  is called a Schreier set for  $H$  if it is a set of left coset representatives for  $H$  in  $G$  and if a reduced word  $x_1^{\epsilon_1} \mu \in S$ , then also  $\mu \in S$ . (with any reduced word in  $S$ , all its final sequences are in  $S$ ).

12. FEB. 25

13. FEB. 28

14. MAR. 2

We constructs 2 non-abelian group of order  $p^3$ , where  $p$  is an odd prime. One is of exponent  $p$ , the other is of exponent  $p^2$

$\text{Aut}(D_\infty) \cong D_\infty$ ,  $\text{Out}(D_\infty) = \mathbb{Z}/2/\mathbb{Z}$ , and  $\text{Inn}(D_\infty) \cong D_\infty$ .

**Note 14.1.** If  $H$  and  $K$  are characteristic in  $H \times K$ , then  $\text{Aut}(H \times K) \cong \text{Aut}(H) \times \text{Aut}(K)$  as  $\eta(h, k) = \phi(h)\psi(k)$ .

**Example 14.2** (Non-example).  $G = (\mathbb{Z}/p\mathbb{Z})^k$ ,  $\text{Aut}(G) = \text{GL}_k(\mathbb{Z}/p\mathbb{Z}) \supset \text{Aut}(\mathbb{Z}/p\mathbb{Z}) \times \dots \times \text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p\mathbb{Z})^\times$ .

$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} : \gcd(a, n) = 1\}$  where  $\phi_a(k) = ak$ .

**Example 14.3.** If  $n = p_1^{k_1} \dots p_s^{k_s}$ , then  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}$  and each factor is characteristic, so  $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \text{Aut}(\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \dots \times \text{Aut}(\mathbb{Z}/p_s^{k_s}\mathbb{Z})$ .

**Note 14.4.** What is  $\text{Aut}(\mathbb{Z}/p^k\mathbb{Z})$ ?  $|\text{Aut}(\mathbb{Z}/p^k\mathbb{Z})| = p^k - p^{k-1}$ .

**Definition 14.5.** The Euler's function  $\phi(n) = |\text{Aut}(\mathbb{Z}/n\mathbb{Z})|$ . We have  $\phi(p_1^{k_1} \dots p_s^{k_s}) = \phi(p_1^{k_1}) \dots \phi(p_s^{k_s})$ .

If  $\gcd(m, n) = 1$ , then  $\phi(mn) = \phi(m)\phi(n)$ .

**Lemma 14.6.** 1. If  $k \geq 2$ , then  $\bar{5} \in (\mathbb{Z}/2^k\mathbb{Z})^\times$  has order  $2^{k-2}$ .

2. If  $k \geq 1$ , then  $p + 1 \in (\mathbb{Z}/p^k\mathbb{Z})^\times$  has order  $p^{k-1}$ .

*Proof.* 2. if  $K = 1$ , then  $p + 1 = 1$  has order  $p^{k-1}$  in  $(\mathbb{Z}/p^k\mathbb{Z})^\times$

Assume  $p + 1$  has order  $p^{k-1}$  in  $(\mathbb{Z}/p^k\mathbb{Z})^\times$ . Then  $(p + 1)^{p^{k-1}} = 1 + Ap^k$  and assume  $p \nmid A$ .

Look at  $(p - 1)^{p^k} = [(p + 1)^{p^{k-1}}]^p = (1 + Ap^k)^p = 1 + \binom{p}{1}Ap^k + \binom{p}{2}A^2p^{2k} + \dots = 1 + p^{k+1}B$  for some  $p \nmid B$ .

From this, we have  $(1 + p)^{p^{k-1}} \equiv 1 \pmod{p^k}$  and  $(1 + p)^{p^{k-2}} = 1 + Ap^{k-1} \not\equiv 1 \pmod{p^k}$  since  $p \nmid A$ .  $\square$

**Corollary 14.7.**  $(\mathbb{Z}/2^k\mathbb{Z})^\times = \begin{cases} 1 & k = 1 \\ \mathbb{Z}/2\mathbb{Z} & k = 2 \\ \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle \bar{5} \rangle \times \langle \bar{-1} \rangle & k \geq 3 \end{cases}$

What about  $(\mathbb{Z}/p\mathbb{Z})^\times$ ?

**Theorem 14.8.** *If  $F$  is a field and  $A \subseteq F^\times$  is a finite subgroup then  $A$  is cyclic.*

*Proof.* Let  $N$  be the exponent of  $A$ . So,  $a^N = 1$  for all  $a \in A$ .

Recall that a polynomial of degree  $k$  has at most  $k$  roots in a field  $x^N - 1$  is of degree  $N$  so  $|A| \leq N$ .

$A$  abelian of exponent  $N$ , so  $A$  has an element  $a$  of order  $N$  so  $|A| \geq |\langle a \rangle| = N$ . So,  $a = \langle a \rangle$ .  $\square$

**Corollary 14.9.**  *$(\mathbb{Z}/p\mathbb{Z})^\times$  is cyclic of order  $p-1$ ; i.e., there is a  $a \in \mathbb{Z}$  s.t.  $a, a^2, \dots, a^{p-1}$  are all distinct mod  $p$ . Any such  $a$  is called a primitive root module  $p$ .*

**Theorem 14.10.**  *$(\mathbb{Z}/p^n\mathbb{Z})^\times$  is cyclic for odd primes  $p$ ,  $n \geq 1$ .*

*Proof.*  $(\mathbb{Z}/p\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$  and any  $b$  which maps to a generator has order divisible by  $p-1$  so some power of  $b$  has order  $(p-1)$ . Here,  $(\mathbb{Z}/p^n\mathbb{Z})^\times$  has an element  $u$  of power  $p-1$  and an element  $w = 1+p$  of order  $p^{n-1}$ .

So,  $uw$  has order  $p^{n-1}(p-1) = \phi(p^n)$ . So,  $(\mathbb{Z}/p^n\mathbb{Z})^\times = \langle uw \rangle$ .  $\square$

**Theorem 14.11** (Euler). *If  $\gcd(a, n) = 1$ , then  $a^{\phi(n)} \equiv 1 \pmod{n}$ . Here,  $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ .*

**Example 14.12.**  $(\mathbb{Z}/20\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ . Notice  $\phi(20) = 8$ .

**Definition 14.13.** A representation of a group  $G$  is a homomorphism  $\phi : G \rightarrow \text{Aut}(M)$  where  $\text{Aut}(M)$  are “symmetries” (or “automorphism”) of some sort of object. A representation is faithful if  $\phi$  is injective.

**Example 14.14.**  $M$  a vector space over a field.

$\phi : G \rightarrow GL(M)$  where  $GL(M)$  is the group of all invertible linear maps  $M \rightarrow M$  are linear representations.

**Example 14.15.**  $M$  is a metric space, then  $\text{Aut}(M)$  are isometries of  $M$ .

**Example 14.16.** Permutation representations is  $G \rightarrow \text{Sym}(X) = S(X)$  where  $S(X)$  is the group of all permutations of  $X$ .

15. MAR. 4

**Definition 15.1.**