

# Algebra

October 31, 2016

# 1 Group theory

## 1.1 Week 1

**Def 1.** A non-empty set  $G$  with a binary function  $f : G \times G \rightarrow G, (a, b) \mapsto ab$  is a **group** if it satisfies

1.  $(ab)c = a(bc)$ .
2.  $\exists 1 \in G$  s.t.  $1a = a1 = a, \forall a \in G$ .
3.  $\exists a^{-1} \in G$  s.t.  $aa^{-1} = a^{-1}a = 1$ .

CONCON

**Def 2.** Let  $G$  be a group. Then  $G$  is said to be **abelian** if  $\forall a, b \in G, ab = ba$ .

**Ex 1.1.1.** Let  $G$  be a semigroup. Then TFAE (the following are equivalent)

1.  $G$  is a group.
2. For all  $a, b \in G$  and the equations  $bx = a, yb = a$ , each of them has a solution in  $G$ .
3.  $\exists e \in G$  s.t.  $ae = a \forall a \in G$  and if we fix such  $e$ , then  $\forall b \in G \exists b' \in G$  s.t.  $bb' = e$ .

**Ex 1.1.2.** Let  $G$  be a group. Show that

1.  $\forall a \in G, a^2 = 1$ , then  $G$  is abelian.
2.  $G$  is abelian  $\iff \forall a, b \in G, (ab)^n = a^n b^n$  for three consecutive integer  $n$ .

**Def 3.** Let  $G$  be a group and  $H \subseteq G, H \neq \emptyset$ . Then  $H$  is said to be a subgroup of  $G$ , denoted by  $H \leq G$ , if

1.  $\forall a, b \in H, ab \in H$ .
2.  $1 \in H$ .
3.  $\forall a \in H, a^{-1} \in H$ .

useful criterion:  $H \leq G \iff \forall a, b \in H, ab^{-1} \in H$ .

**pf:**

$\implies b \in H \implies b^{-1} \in H$ , and  $a \in H$ , so  $ab^{-1} \in H$ .

$\Leftarrow$  1.  $H \neq \emptyset \implies \exists a \in H \implies aa^{-1} = 1 \in H$ .

2.  $1, a \in H \implies 1a^{-1} = a^{-1} \in H$ .

3.  $a, b^{-1} \in H \implies a(b^{-1})^{-1} = ab \in H$ . □

**Eg 1.1.1.**  $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0) ; (\mathbb{Q}^\times, \times, 1) \leq (\mathbb{R}^\times, \times, 1) \leq (\mathbb{C}^\times, \times, 1)$

**Eg 1.1.2.**

- Special linear group  $\text{SL}(n, \mathbb{F}) = \{ A \in \text{GL}(n, \mathbb{F}) \mid \det A = 1 \}$
- Orthogonal group  $\text{O}(n) = \{ A \in \text{GL}(n, \mathbb{R}) \mid A^t A = I_n \}$
- Unitary group  $\text{U}(n) = \{ A \in \text{GL}(n, \mathbb{C}) \mid A^* A = I_n \}$
- Special orthogonal group  $\text{SO}(n) = \text{SL}(n, \mathbb{R}) \cap \text{O}(n)$

- Special unitary group  $SU(n) = SL(n, \mathbb{C}) \cap U(n)$

**Def 4.** Let  $f : G_1 \rightarrow G_2$ .  $f$  is called an **isomorphism** if

1.  $f$  is 1-1 and onto.
2.  $\forall a, b \in G_1, f(ab) = f(a)f(b)$ . (**homomorphism**)

, denoted by  $G_1 \cong G_2$ .

**Remark 1.** (practice)

1.  $f(1) = 1$ .
2.  $f(a^{-1}) = f(a)^{-1}$ .
3. If  $f$  is an isomorphism, then  $\exists f^{-1}$  is also a homomorphism.

**Eg 1.1.3.**

- $U(1) = \{ z \in \mathbb{C}^\times \mid \bar{z}z = 1 \}, z = \cos \theta + \sin \theta i$
- $SO(2) = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} : \theta \in \mathbb{R} \right\}$

notice that  $U(1) \cong SO(2)$ .  $S^1 = \{ (a, b) \in \mathbb{R}^2 \mid a^2 + b^2 = 1 \}$ , 可被賦予群的結構.

**Eg 1.1.4.** Let  $A \in SU(2) \implies A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \alpha\bar{\alpha} + \beta\bar{\beta} = 1, \alpha, \beta \in \mathbb{C}$ .

Quaternion(四元數):  $\mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \}$  with  $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j (\implies ij = -ji)$ .

Let  $x = a + bi + cj + dk, \bar{x} = a - bi - cj - dk$ , then  $N(x) = x\bar{x} = a^2 + b^2 + c^2 + d^2$ , For  $x \neq 0, N(x) \neq 0, x^{-1} = \frac{1}{N(x)}\bar{x}$

Now, for  $x = a + bi + cj + dk = (a + bi) + (c + di)j$ . So  $SU(2) \cong \{ x \in \mathbb{H}^\times \mid N(x) = 1 \}$ .  $S^3 = \{ (a, b, c, d) \in \mathbb{R}^4 \mid a^2 + b^2 + c^2 + d^2 = 1 \}$ , 可被賦予群的結構.

★ The only spheres with continuous group law are  $S^1, S^3$ .

**Ex 1.1.3.** Find a way to regard  $M_{n \times n}(\mathbb{H})$  as a subset of  $M_{2n \times 2n}(\mathbb{C})$ , which preserves addition and multiplication, and then there is a way to characterize  $GL(n, \mathbb{H})$ .

**Def 5** (symplectic group).  $Sp(n, \mathbb{F}) = \{ A \in GL(2n, \mathbb{F}) \mid A^t J A = J \}$  where  $J = \begin{pmatrix} O & I_n \\ -I_n & O \end{pmatrix}$ .

( $A^t J A = J$  preserving non-degenerate skew-symmetric forms)

$Sp(n) = \{ A \in GL(n, \mathbb{H}) \mid A^* A = I_n \}$ .

**Ex 1.1.4.** Show  $Sp(n) \cong U(2n) \cap Sp(n, \mathbb{C})$ .

Ques: Find the smallest subgroup of  $SU(2)$  containing  $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ .

## 1.2 Week 2

### 1.2.1 Permutation groups and Dihedral groups

**Def 6.** A permutation of a set  $B$  is a 1-1 and onto function from  $B$  to  $B$ .

Let  $S_B :=$  the set of permutations of  $B$ . Then  $(S_B, \cdot, \text{Id}_B)$  forms a group.

If  $B = \{a_1, \dots, a_n\}$ , then  $S_B \cong S_{\{1, \dots, n\}}$  and write  $S_n = S_{\{1, \dots, n\}}$ , called the symmetric group of degree  $n$ .

**Theorem 1** (Cayley theorem). Any group is isomorphic to a subgroup of some permutation group.

(Hint): Let  $G$  be a group. Set  $B = G$ . Consider  $a \in G$  as  $\sigma_a : G \rightarrow G, x \mapsto ax$ . Then  $\sigma_a \in S_G \implies G \leq S_G$ .

**Fact 1.2.1.**  $S_n$  is a finite group of order  $n!$ , i.e.  $|S_n| = n!$ .

**pf:** EASY =O

□

Cyclic notation:  $\sigma \in S_5$ , say  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$ . Write  $\sigma = (1\ 4)(2\ 3\ 5)$ .

$\Rightarrow$  Any permutation can be written as a product of disjoint cycles.

**Eg 1.2.1.** In  $S_7$ ,  $\sigma_1 = (1\ 2\ 3)(4\ 5\ 6)(7)$ ,  $\sigma_2 = (1\ 3\ 5\ 6)(2\ 4\ 7)$ .  
Then  $\sigma_1\sigma_2 = (2\ 5\ 4\ 7\ 3\ 6)$ ,  $\sigma_1^{-1} = (1\ 3\ 2)(4\ 6\ 5)$ .

**Def 7.** A 2 cycle is called a **transposition**.

**Eg 1.2.2.**  $(1\ 2\ 3) = (1\ 3)(1\ 2)$ ,  $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$ .  
Any permutation is a product of 2 cycles.

Useful formula:  $\sigma \in S_n$ ,  $\sigma(j_1 \dots j_m)\sigma^{-1} = (\sigma(j_1) \dots \sigma(j_m))$ .

**Eg 1.2.3.** Let  $\sigma = (1\ 2\ 3)(4\ 5\ 6\ 7)$ ,  $\sigma(2\ 3\ 4)\sigma^{-1} = (3\ 1\ 5)$ .

**pf:** Note that both sides are functions. For  $i \in \{1, \dots, n\}$ ,

Case 1:  $\exists k$  s.t.  $\sigma(j_k) = i$ , CONCON

Case 2: Otherwise, CONCON

□

**Fact 1.2.2.**  $S_n = \langle (1\ 2), \dots, (1\ n) \rangle$ .

**pf:**  $(1\ i)^{-1} = (1\ i)$  and  $(i\ j) = (1\ i)(1\ j)(1\ i)^{-1}$ .

□

**Def 8.** Let  $G$  be a group and  $S \subset G$ . The subgroup generated by  $S$  defined to be the smallest subgroup of  $G$  which contains  $S$ , denoted by  $\langle S \rangle$ .

**Ex 1.2.1.**

1.  $S_n = \langle (1\ 2), (2\ 3), \dots, (n-1\ n) \rangle$ ,  $n \geq 2$ .

2.  $S_n = \langle (1\ 2), (1\ 2 \dots n) \rangle$ ,  $n \geq 2$ .

**Def 9.**  $A_n = \{\text{even permutations of } S_n\} \leq S_n, |A_n| = \frac{n!}{2}$ .

**Ex 1.2.2.**

1.  $A_n = \langle (1\ 2\ 3), (1\ 2\ 4), \dots, (1\ 2\ n) \rangle, n \geq 3.$
2.  $A_n = \langle (1\ 2\ 3), (2\ 3\ 4), \dots, (n-2\ n-1\ n) \rangle, n \geq 3.$

**Remark 2.**  $\langle S \rangle = \bigcap_{S \subseteq H \leq G} H = \{a_1 a_2 \dots a_k \mid k \in \mathbb{N}, a_i \in S \cup S^{-1}\} \cup \{1\}$

The orthogonal transformations on  $\mathbb{R}^2$ :  $O(2)$ .

Let  $A = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \in O(2).$

略... (這邊討論旋轉和反射的矩陣)

Case 1:  $A = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$  is counterclockwise rotation w.r.t.  $\alpha$ .

Case 2:  $A = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}$  is the reflection.  $A^2 = I_2 \implies$  eigenvalues are  $\pm 1$ .

Easy to show that  $L_A(v) = v - 2\langle v, v_2 \rangle v_2$ .

$O(2) = \{\text{rotations}\} \cup \{\text{reflections}\}.$

**Def 10.** The dihedral group  $D_n$  is the group of symmetries of a regular  $n$ -gon.  
In general,  $D_n = \langle T, R \mid T^n = 1, R^2 = 1, TR = RT^{-1} \rangle \leq O(2) \leq S_n, |D_n| = 2n.$

**Def 11.** Let  $T$  be a linear transformation from  $\mathbb{R}^n \rightarrow \mathbb{R}^n$ .

- $T$  is called a rotation if  $\exists$  a  $T$ -invariant subspace  $W \subseteq \mathbb{R}^n$  with  $\dim W = 2$  s.t.  $\begin{cases} T|_W \text{ is a rotation} \\ T|_{W^\perp} = \text{id}_{W^\perp} \end{cases}$
- $T$  is called a reflection if  $\exists$  a  $T$ -invariant subspace  $W \subseteq \mathbb{R}^n$  with  $\dim W = 1$  s.t.  $\begin{cases} T|_W = -\text{id}_W \\ T|_{W^\perp} = \text{id}_{W^\perp} \end{cases}$

Main result: the group of orthogonal transformations =  $\langle \text{rotations, reflections} \rangle.$

**Prop 1.2.1.** For  $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$ ,  $\exists$  a  $T$ -invariant subspace  $W \subseteq \mathbb{R}^n$  with  $1 \leq \dim W \leq 2$ .

**pf:** Let  $A = [T]_\alpha \in M_{n \times n}(\mathbb{R}) \subseteq M_{n \times n}(\mathbb{C})$ . Consider  $\widetilde{L}_A: \mathbb{C}^n \rightarrow \mathbb{C}^n, v \mapsto Av$ .

Then  $\exists$  an eigenvalue  $\lambda \in \mathbb{C}$  and an eigenvector  $v \in \mathbb{C}^n$  for  $\widetilde{L}_A$ . Let  $\lambda = \lambda_1 + \lambda_2 i, v = v_1 + v_2 i$ . By definition, we have

$$Av = \widetilde{L}_A(v) = \lambda v = (\lambda_1 + \lambda_2 i)(v_1 + v_2 i) \implies \begin{cases} Av_1 = \lambda_1 v_1 - \lambda_2 v_2 \\ Av_2 = \lambda_2 v_1 + \lambda_1 v_2 \end{cases},$$

so  $W = \langle v_1, v_2 \rangle.$

□

**Ex 1.2.3.**

1. If  $T$  is orthogonal, then  $W^\perp$  is also  $T$ -invariant.
2. Use induction on  $n$  to show the main result.

For  $n = 3, A \in O(3)$ , we have  $A \sim \begin{pmatrix} \cos \alpha & -\sin \alpha & \\ \sin \alpha & \cos \alpha & \\ & & \pm 1 \end{pmatrix}.$

### 1.2.2 Cyclic groups and internal direct product

**Def 12.** If  $G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, a, 1, a, a^2, \dots\} = \{a^n \mid n \in \mathbb{Z}\}$ , then  $G$  is a cyclic group generated by  $a$ .

**Eg 1.2.4.**  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ .

**Eg 1.2.5.** Let  $A = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix} \in \text{SO}(2)$ . Then  $\langle A \rangle = \{I_2, A, A^2, \dots, A^{n-1}\}$  and  $A^n = I_2$ ,  $A^m = A^r$  where  $m \equiv r \pmod{n}$ .

**Eg 1.2.6.**  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{(n-1)}\}$  with  $\bar{j} = \{m \in \mathbb{Z} \mid m \equiv j \pmod{n}\}$ . Define  $\bar{i} + \bar{j} = \begin{cases} \overline{i+j} & \text{if } 0 \leq i+j \leq n \\ \overline{i+j-n} & \text{otherwise} \end{cases} \implies (\mathbb{Z}/n\mathbb{Z}, +, \bar{0})$  forms a group.

**Remark 3.**  $\bar{i} \times \bar{j} = \overline{i \times j}$ .

- 略
- If  $\gcd(j, n) = d, \exists h, k \in \mathbb{Z}$  s.t.  $hj + kn = d$ .

**Def 13.**  $(\mathbb{Z}/n\mathbb{Z})^\times = \{j \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(j, n) = 1\} \implies ((\mathbb{Z}/n\mathbb{Z})^\times, \times, \bar{1})$  forms a group.

**Eg 1.2.7.** 略... 简化剩余系, 原根 (generator)  $(1, 2, 4, p^k, 2p^k, p \text{ is an odd prime})$

**Def 14.**

- The **order** of a finite group  $G$  is the number of elements in  $G$ , denoted by  $|G|$ .
- Let  $a \in G$ , the order of  $a$  is defined to be the least positive integer  $n$  s.t.  $a^n = 1$ , denoted by  $\text{ord}(a) = n$ .
- If  $a^n \neq 1 \quad \forall n \in \mathbb{N}$ , then we call “ $a$  has infinite order”.

**Prop 1.2.2.** Let  $G = \langle a \rangle$  with  $\text{ord}(a) = n$ . Then

1.  $a^m = 1 \iff n \mid m$ .

**pf:**

$\Leftarrow$ : Let  $m = dn$ , then  $a^m = (a^n)^d = 1$ .

$\Rightarrow$ : Let  $m = qn + r, 0 \leq r < n$ . If  $r \neq 0$ , then  $a^r = a^{m-qn} = (a^m)(a^n)^{-q} = 1$ . But  $r < n$ , which is a contradiction. Hence  $r = 0 \implies n \mid m$ .  $\square$

2.  $\text{ord}(a^r) = n / \gcd(r, n)$ .

**pf:** Let  $\gcd(r, n) = d, n = dn', r = dr'$  with  $\gcd(n', r') = 1$ . Plan to show “ $\text{ord}(a^r) = n'$ .”

- $(a^r)^{n'} = a^{r'n'} = (a^n)^{r'} = 1 \implies \text{ord}(a^r) \mid n'$ .
- $1 = (a^r)^{\text{ord}(a^r)} = a^{r \cdot \text{ord}(a^r)} \implies n \mid r \cdot \text{ord}(a^r) \implies n' \mid r' \cdot \text{ord}(a^r) \implies n' \mid \text{ord}(a^r)$ .

$\square$

**Prop 1.2.3.** Any subgroup of a cyclic group is cyclic.

**pf:** Let  $G = \langle a \rangle$  and  $H \leq G$ . If  $H = \{1\}$ , then  $H = \langle 1 \rangle$ , done!

Otherwise,  $d = \min\{m \in \mathbb{N} \mid a^m \in H\}$ , by well-ordering axiom. Claim  $H = \langle a^d \rangle$ .

$\supset$ :  $a^d \in H$  by the definition of  $d$ .

$\subset$ :  $\forall a^m \in H$ , write  $m = qd + r, 0 \leq r < d$ . If  $r \neq 0$ , then  $a^r = a^{m-qd} = a^m(a^d)^{-q} \in H$ , which is a contradiction. Hence  $r = 0 \implies d \mid m$ .

□

**Ex 1.2.4.**

1.  $\text{ord}(a) = \text{ord}(a^{-1}) = n$ .
2.  $\langle a^r \rangle = \langle a^{\gcd(n,r)} \rangle$ .
3.  $\langle a^{r_1} \rangle = \langle a^{r_2} \rangle \iff \gcd(n, r_1) = \gcd(n, r_2)$ .
4.  $\forall m \mid n, \exists! H \leq \langle a \rangle$  s.t.  $|H| = m$ . Conversely, if  $H \leq \langle a \rangle$ , then  $|H| \mid n$ .

**Prop 1.2.4.** Let  $G = \langle a \rangle$ . Then

1.  $\text{ord}(a) = n \implies G \cong \mathbb{Z}/n\mathbb{Z}$
2.  $\text{ord}(a) = \infty \implies G \cong \mathbb{Z}$

**Ex 1.2.5.** Show Prop 1.2.4.

**Def 15.** Let  $G_1, G_2 \leq G$ .  $G$  is the internal direct product of  $G_1, G_2$  if  $G_1 \times G_2 \rightarrow G, (g_1, g_2) \mapsto g_1g_2$  is an isom.

**Remark 4.** In this case, we find that

- $G = G_1G_2 = \{g_1g_2 \mid g_1 \in G_1, g_2 \in G_2\}$ .
- $G_1 \cap G_2 = \{1\}$ . (consider  $a \neq 1 \in G_1 \cap G_2$ , then  $(1, a) \mapsto a, (a, 1) \mapsto a$ , but the function is 1-1, which is a contradiction.)
- If  $a \in G$  with  $a = g_1g_2 = g'_1g'_2$ , then  $(g'_1)^{-1}g_1 = (g'_2)g_2^{-1} \in G_1 \cap G_2 = \{1\} \implies \begin{cases} g_1 = g'_1 \\ g_2 = g'_2 \end{cases}$ .
- For  $g_1 \in G_1, g_2 \in G_2, (g_1, g_2) = (g_1, 1)(1, g_2) = (1, g_2)(g_1, 1) \implies g_1g_2 = g_2g_1$ .

**Ex 1.2.6.** TFAE

1.  $G$  is the internal direct product of  $G_1, G_2$ .
2.  $\forall a \in G, \exists! g_1 \in G_1, g_2 \in G_2$  s.t.  $a = g_1g_2$ ;  $\forall g_1 \in G_1, g_2 \in G_2, g_1g_2 = g_2g_1$ .
3.  $G_1 \cap G_2 = \{1\}$ ;  $G = G_1G_2$ ;  $\forall g_1 \in G_1, g_2 \in G_2, g_1g_2 = g_2g_1$ .

**Eg 1.2.8.**

1.  $G = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}, G_1 = \{\bar{0}, \bar{3}\}, G_2 = \{\bar{0}, \bar{2}, \bar{4}\}$ . We have  $G \cong G_1 \times G_2$ .
2.  $G = S_3, G_1 = \langle (1\ 2) \rangle, G_2 = \langle (1\ 2\ 3) \rangle$ . We have  $G_1 \times G_2 \not\cong G$  since  $(1\ 2)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)$ .

**Eg 1.2.9.**  $G = S_3, G_1 = \langle (1\ 2) \rangle, G_2 = \langle (2\ 3) \rangle, G_1G_2 = \{1, (1\ 2), (2\ 3), (1\ 2\ 3)\} \not\leq G$  since  $(1\ 3\ 2) = (1\ 2\ 3)^{-1} \notin G_1G_2$ .

**Prop 1.2.5.** Let  $H, K \leq G$ . Then  $HK \leq G \iff HK = KH$ .

**pf:**

$$\Rightarrow: \begin{cases} H \leq HK \\ K \leq HK \end{cases} \implies KH \subseteq HK ; \forall hk \in HK, \exists h'k' \in HK \text{ s.t. } (hk)(h'k') = 1 \implies hk = (k')^{-1}(h')^{-1} \in KH \implies HK \subseteq KH.$$

$$\Leftarrow: \text{ For } h_1k_1, h_2k_2 \in HK, (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h'k' \in HK.$$

□



## 1.3 Week 3

### 1.3.1 Coset and Quotient Group

Let  $f : G_1 \rightarrow G_2$  be a group homo. Define  $\text{Im } f := f(G_1)$ .

Notice that  $\text{Im } f \leq G_2$ .

**pf:** Let  $z_1 = f(a_1), z_2 = f(a_2)$ , then  $z_1 z_2^{-1} = f(a_1) f(a_2)^{-1} = f(a_1) f(a_2^{-1}) = f(a_1 a_2^{-1}) \in \text{Im } f$ .  $\square$

**Def 16.**  $\ker f := \{x \in G_1 \mid f(x) = 1\} \leq G_1$ .

**Fact 1.3.1.**

1.  $x \in (\ker f)a \iff f(x) = f(a)$ .
2.  $\ker f = \{1\} \iff f$  is 1-1.

**Def 17.** Let  $H \leq G, \forall a \in G, Ha$  is called a **right coset** of  $H$  in  $G$ .

**Fact 1.3.2.**

1. For 2 right cosets  $Ha, Hb$ , either  $Ha = Hb$  or  $Ha \cap Hb = \phi$  must hold.
2.  $\{Ha : a \in G\}$  forms a partition of  $G$ .

**Theorem 2** (Lagrange). Let  $|G| < \infty$  and  $H \leq G, |H| \mid |G|$ .

**pf:**

$\square$

**Remark 5.**  $r$  is called the **index** of  $H$  in  $G$ , denoted by  $[G : H]$ . (The concept of index can be extended to infinite  $G, H$ .)

**Ex 1.3.1.** no subgroup of  $A_4$  has order 6. (converse of Lagrange thm. is false.)

**Coro 1.3.1.** If  $|G| = p$  is a prime in  $\mathbb{Z}$ , then  $G$  is cyclic.

**pf:**

$\square$

**Coro 1.3.2.** If  $|G| < \infty, a \in G$ , then  $a^{|G|} = 1$ .

**pf:**

$\square$

**Remark 6.**

1. Let  $H \leq G, a \in G, aH$  is called a **left coset**.
2.  $\{\text{right cosets of } H\} \leftrightarrow \{\text{right cosets of } H\}$  by  $Ha \mapsto a^{-1}H$ .

Ques: How to make  $\{aH : a \in G\}$  to be a group? For  $aH, bH$ , we must have  $(aH)(bH) = abH$ .  
In general,  $(aH)(bH) = abH$  is not well-defined.

**Ex 1.3.1.** Let  $H = \langle (1\ 2) \rangle \leq S_3$ .  $a_1 = (1\ 3), a_2 = (1\ 2\ 3), b_1 = (1\ 3\ 2), b_2 = (2\ 3)$ . 出慘點

If we hope  $a_1 b_1 H = a_2 b_2 H$ , then we need  $(a_1 b_1)^{-1} a_2 b_2 \in H$ .

$$b_1^{-1} a_1^{-1} a_2 b_2 = b_1^{-1} b_2 b_2^{-1} a_1^{-1} a_2 b_2$$

Notice that  $b_1^{-1} b_2, a_1^{-1} a_2 \in H$ , so we need  $b_2^{-1} a_1^{-1} a_2 b_2 \in H$ .

**Def 18.** Let  $H \leq G$ .  $H$  is said to be **normal subgroup** of  $G$  if  $\forall g \in G, h \in H, g^{-1}hg \in H$  (or  $g^{-1}Hg \subseteq H$ ), denoted by  $H \triangleleft G$ .

**Def 19.** Let  $H \triangleleft G$ . The set  $\{aH \mid a \in G\}$  forms a group under  $(aH)(bH) = abH, a, b \in G$ . We call it the **quotient group** of  $G$  by  $H$ , denoted by  $G/H$ .  
(Note: The identity is  $H = hH$  and  $(aH)^{-1} = a^{-1}H$ .)

**Remark 7.** Define  $q : G \rightarrow G/H, a \mapsto aH$ , called the quotient homomorphism.

**Ex 1.3.2.** Let  $H \leq G$ . Then TFAE

- (a)  $H \triangleleft G$ .
- (b)  $\forall x \in G, xHx^{-1} = H$ .
- (c)  $\forall x \in G, xH = Hx$ .
- (d)  $\forall x, y \in G, (xH)(yH) = (xy)H$ .

Ques: How to find a normal subgroup of  $G$ ?

**Prop 1.3.1.**

- 1. If  $G$  is abelian, then  $\forall H \leq G \rightsquigarrow H \triangleleft G$ . (done by (c))
- 2. If  $H \leq G$  with  $[G : H] = 2$ , then  $H \triangleleft G$ .

**Ex 1.3.2.**  $n \leq 3, [S_n : A_n] = 2 \implies A_n \triangleleft S_n$ .

**pf:** We can write  $G = H \cup Ha = H \cup aH \implies aH = Ha, \forall a \notin H$ . □

**Def 20.** Define the center of  $G$  to be  $Z_G = \{a \in G \mid ax = xa, \forall x \in G\} \leq G$ .

**Prop 1.3.2.**

- 1.  $Z_G \triangleleft G$ . (by (c) and def.)
- 2. If  $G/Z_G$  is cyclic, then  $G$  is abelian.

**pf:** Let  $G/Z_G = \langle aZ_G \rangle$ , (let  $\bar{a} := aZ_G$ ) for some  $a \in G$ . For  $x_1, x_2 \in G$ , let  $x_1 = a^{k_1}z_1, x_2 = a^{k_2}z_2$ , then  $x_1x_2 = a^{k_1+k_2}z_1z_2 = x_2x_1$ . ( $z_i$  可以各種交換) □

**Def 21.** The commutator of  $G$  is define to be  $[G, G] = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$ .

**Prop 1.3.3.**  $[G, G] \triangleleft G ; [G, G] = 1 \iff G$  is abelian.

**pf:**  $\forall x \in G, a \in [G, G], xax^{-1} = xax^{-1}a^{-1}a$  and  $xax^{-1}a^{-1}, a \in [G, G]$ . □

**Ex 1.3.3.**

- 1. If  $H \leq S_n$  and  $\exists \sigma \in H$  is odd, then  $[H : H \cap A_n] = 2$ .
- 2. For  $n \geq 3, [S_n, S_n] = A_n$ .

**Ex 1.3.4.** Let  $H \leq G$ . Then  $H \triangleleft G$  and  $G/H$  is abelian  $\iff [G, G] \leq H$ . (hint:  $G/[G, G]$  is "max" among all abelian quotient groups)

### 1.3.2 Isomorphism theorems & Factor theorem

**Theorem 3** (1st isomorphism theorem). Let  $f : G_1 \rightarrow G_2$  be a group homo. Then  $G_1/\ker f \cong \text{Im } f$ .

**pf:** Define  $\varphi : a \ker f \mapsto f(a)$ .

- well-defined:  $a \ker f = b \ker f \implies a^{-1}b \in \ker f \implies f(a^{-1}b) = 1 \implies f(a)^{-1}f(b) = 1 \implies f(a) = f(b)$ .
- group homo:  $\varphi((a \ker f)(b \ker f)) = \varphi(ab \ker f) = f(ab) = f(a)f(b) = \varphi(a \ker f)\varphi(b \ker f)$ .
- onto: by def. of  $\text{Im } f$ .
- 1-1:  $f(a) = f(b) \implies a \ker f = b \ker f$  (easy).

□

**Theorem 4** (Factor theorem). Let  $f : G_1 \rightarrow G_2$  be a group homo. and  $H \triangleleft G_1, H \leq \ker f$ . Then  $\exists$  a group homo.  $\varphi : G/H \rightarrow G_2$  s.t. 一個正圖

**Eg 1.3.3.** Let  $G = \langle a \rangle$  with  $\text{ord}(a) = n$ . Then  $G \cong \mathbb{Z}/n\mathbb{Z}$ . (1st isom. thm.)

**Eg 1.3.4.**  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}, 4\mathbb{Z} \leq 2\mathbb{Z}$ , so by factor thm.,  $\mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ .

**Eg 1.3.5.**  $\det : \text{GL}(n, \mathbb{F}) \rightarrow \mathbb{F}^\times \implies \text{GL}(n, \mathbb{F})/\text{SL}(n, \mathbb{F}) \cong \mathbb{F}^\times$

**Eg 1.3.6.**  $\text{sgn} : S_n \rightarrow \{\pm 1\} \implies S_n/A_n \cong \{\pm 1\}$

**Theorem 5** (2nd isomorphism theorem). Let  $H \leq G, K \triangleleft G$ . Then  $HK/K \cong H/H \cap K$ .

**pf:** First,  $\begin{cases} H \leq G \\ K \triangleleft G \end{cases} \implies HK = KH \implies HK \leq G ; K \triangleleft G \implies K \triangleleft HK$ .

Define  $\varphi : H \rightarrow HK/K, h \mapsto hK$ . which is a group homo.

- onto:  $\forall (hk)K, hK = hK, \text{ so } \varphi(h) = hK = hkK$ .
- Find  $\ker \varphi$ :  $a \in \ker \varphi \iff \begin{cases} a \in H \\ aK = K \end{cases} \iff a \in H \cap K, \text{ so } \ker \varphi = H \cap K$ .

Then by 1st isom. thm.

□

**Eg 1.3.7.**  $G = \text{GL}(2, \mathbb{C}), H = \text{SL}(2, \mathbb{C}), K = \mathbb{C}^\times I_2 = Z_G \triangleleft G$ .

By 2nd isom. thm.,  $G/K \cong H/\{\pm I_2\}$ . ( $G = HK, \{\pm I_2\} = H \cap K$ )

projective linear group:  $\text{PGL}(2, \mathbb{C}) = G/K$ .

projective special linear group:  $\text{PSL}(2, \mathbb{C}) = H/H \cap K$ .

齊次座標...OTL

**Ex 1.3.5.**

1. Let  $H_1 \triangleleft G_1, H_2 \triangleleft G_2$ . Then  $(H_1 \times H_2) \triangleleft (G_1 \times G_2)$  and  $G_1 \times G_2 / H_1 \times H_2 \cong G_1 / H_1 \times G_2 / H_2$ .
2. Let  $H \triangleleft G, K \triangleleft G$  s.t.  $G = HK$ . Then  $G/H \cap K \cong G/H \times G/K$ .

**Ex 1.3.6.** Let  $H \triangleleft G$  with  $[G : H] = p$ , which is a prime in  $\mathbb{Z}$ . Then  $\forall K \leq G$ , either (1)  $K \leq H$  or (2)  $G = HK$  and  $[K : K \cap H] = p$ .

**Theorem 6** (3rd isomorphism theorem). Let  $K \triangleleft G$ .

1. There is a 1-1 correspondence between  $\{H \leq G \mid K \leq H\}$  and  $\{\text{subgroups of } G/K\}$ . ( $H \triangleleft G$  ... normal)

**pf:** Define  $\varphi : H \mapsto H/K$ . ( $H/K \leq G/K$ )

- 1-1: Assume  $H_1/K = H_2/K$ . For  $a \in H_1$ ,  $aK \in H_1/K = H_2/K$ . so  $\exists b \in H_2$  s.t.  $aK = bK \implies b^{-1}a \in K \leq H_2 \implies a \in bH_2 = H_2$ . So  $H_1 \leq H_2$ . By symmetry,  $H_2 \leq H_1$ , and thus  $H_1 = H_2$ .
- onto: Given a subgroup  $Q$  of  $G/K$ , consider  $H = q^{-1}(Q)$  where  $q : G \rightarrow G/K$ .
  - $H \leq G$ :  $\forall a, b \in H, q(a), q(b) \in Q \implies q(a)q(b)^{-1} \in Q \implies q(ab^{-1}) \in Q \implies ab^{-1} \in H \implies H \leq G$ .
  - $K \leq H$ :  $\forall a \in K, q(a) = aK = K \in Q \implies a \in H \implies K \leq H$ .
  - $Q = H/K$ :  $\forall aK \in Q, aK = q(a) \implies a \in H \implies aK \in H/K \implies Q \subseteq H/K$ .  
And  $\forall aK \in H/K (a \in H), q(a) \in Q \implies H/K \subseteq Q$ . So  $Q = H/K$ .
- $H \triangleleft G, K \leq H \iff \forall g \in G, gHg^{-1} = H, K \leq H \iff \forall \bar{g} \in G/K, \bar{g}(H/K)\bar{g}^{-1} = H/K \iff H/K \triangleleft G/K$ .  $\square$

2. If  $H \triangleleft G$  with  $K \leq H$ , then  $(G/K)/(H/K) \cong G/H$ .

**pf:** Define  $\varphi : G \rightarrow (G/K)/(H/K)$  with  $\varphi : a \mapsto aK(H/K)$ .

- onto: ... easy.
- Find  $\ker \varphi$ :  $a \in \ker \varphi \iff aK(H/K) = H/K \iff aK \in H/K \iff a \in H$ .

By 1st isom. thm.,  $(G/K)/(H/K) \cong G/H$ .  $\square$

**Eg 1.3.8.**  $m\mathbb{Z} + n\mathbb{Z}/m\mathbb{Z} \cong n\mathbb{Z}/m\mathbb{Z} \cap n\mathbb{Z}$ . ( $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}, m\mathbb{Z} \cap n\mathbb{Z} = \text{lcm}(m, n)\mathbb{Z}$ )

Ques:  $G/K \cong G'/K'$  and  $K \cong K' \not\Rightarrow G \cong G'$ .

**Eg 1.3.9.**  $Q_8$  and  $D_4$  交給陳力

Extension problem: given two groups  $A, B$ , how to find  $G$  and  $K \triangleleft G$ , s.t.  $K \cong A, G/K \cong B$ ?  
( $1 \rightarrow H \rightarrow G \rightarrow G/H \rightarrow 1$ , short exact sequence)  
(e.g.  $G = A \times B, K = A \times \{1\}$ )

## 1.4 Week 4

### 1.4.1 Universal property and direct sum & product

In general, let  $f_1 : G_1 \rightarrow G, f_2 : G_2 \rightarrow G$  are group homo.  $f_1 \times f_2 : G_1 \times G_2 \rightarrow G, (a, b) \mapsto f_1(a)f_2(b)$ . But we have  $(a, b) = (a, 1)(1, b) = (1, b)(a, 1)$ , so  $f_1(a)f_2(b) = f_2(b)f_1(a) \implies$  need  $G$  to be abelian.

So we intend to define the direct sum in the category of abelian group.

Notation: For abelian groups, we use “+” to denote the group operation and “0” to denote the identity.

**Def 22.** Given a non-empty family of abelian groups  $\{G_s \mid s \in \Lambda\}$ , a (external) direct sum of  $\{G_s \mid s \in \Lambda\}$  is an abelian group  $\bigoplus_{s \in \Lambda} G_s$  with the embedding mappings  $i_{s_0} : G_{s_0} \rightarrow \bigoplus_{s \in \Lambda} G_s, \forall s_0 \in \Lambda$  satisfying the universal property:

for any abelian group  $H$  and group homo.  $\varphi_s : G_s \rightarrow H \forall s \in \Lambda, \exists!$  group homo.  $\varphi : \bigoplus_{s \in \Lambda} G_s \rightarrow H$  s.t. 又一個 $\tau$ 圖

**Theorem 7.**  $\bigoplus_{s \in \Lambda} G_s$  exists and is unique up to isomorphisms.

**pf:** Existence:  $\bigoplus_{s \in \Lambda} G_s = \{(g_s)_{s \in \Lambda} \mid g_s \in G_s, \text{ almost all of the } g_s' \text{ are } 0\}$  and

$$i_{s_0} : G_{s_0} \rightarrow \bigoplus_{s \in \Lambda} G_s, a_{s_0} \mapsto (g_{s_0})_{s \in \Lambda} \text{ with } g_{s_0} = a_{s_0}, g_s = 0, \forall s \neq s_0.$$

group operation:  $(g_s)_{s \in \Lambda} + (g'_s)_{s \in \Lambda} := (g_s + g'_s)_{s \in \Lambda} \in \bigoplus_{s \in \Lambda} G_s$ . 這邊也一個 $\tau$ 圖

Uniqueness: Assume  $\exists$  another  $G$  satisfies the universal property, 一個大 $\tau$ 圖  $(G, \bigoplus_{s \in \Lambda} G_s)$  互相有唯一一個映射可以 keep  $i_{s_0}, \varphi \circ \psi = \text{id}_G, \psi \circ \varphi = \text{id}_{\bigoplus_{s \in \Lambda} G_s}$   $\square$

**Def 23.** Given a non-empty family of groups  $\{G_s \mid s \in \Lambda\}$ , a direct product of  $\{G_s \mid s \in \Lambda\}$  is a group  $\prod_{s \in \Lambda} G_s$  with projections  $p_{s_0} : \prod_{s \in \Lambda} G_s \rightarrow G_{s_0}, \forall s_0 \in \Lambda$  satisfying the following universal property:

for any group  $H$  with group homo.  $\varphi_s : H \rightarrow G_s, \forall s \in \Lambda, \exists! \varphi : H \rightarrow \prod_{s \in \Lambda} G_s$  s.t. 又一個 $\tau$ 圖

**Theorem 8.**  $\prod_{s \in \Lambda} G_s$  exists and is unique up to isomorphisms.

**pf:** Existence:  $\prod_{s \in \Lambda} G_s = \{(g_s)_{s \in \Lambda} \mid g_s \in G_s\}$  and

$$p_{s_0} : \prod_{s \in \Lambda} G_s \rightarrow G_{s_0}, (g_s)_{s \in \Lambda} \mapsto g_{s_0}, \forall s_0 \in \Lambda$$

- group operation:  $(g_s)_{s \in \Lambda} \cdot (g'_s)_{s \in \Lambda} := (g_s g'_s)_{s \in \Lambda} \in \prod_{s \in \Lambda} G_s$ .
- Define  $\varphi$ : 這邊也一個 $\tau$ 圖 which is uniquely defined.

Uniqueness: Assume  $\exists$  another  $G$  satisfies the universal property, 一個大 $\tau$ 圖  $(G, \prod_{s \in \Lambda} G_s)$  互相有唯一一個映射可以 keep  $i_{s_0}, \varphi \circ \psi = \text{id}_G, \psi \circ \varphi = \text{id}_{\prod_{s \in \Lambda} G_s}$   $\square$

**Ex 1.4.1.** Google the definition of the **direct limit** and show the existence and uniqueness.

**Ex 1.4.2.** Google the definition of the **inverse limit** and show the existence and uniqueness.

Motivation:  $\zeta_m$  is called an  $m$ -th root of unity if  $\zeta_m^m = 1$ .

$$\varinjlim_n \mathbb{Z}/2^n \mathbb{Z} \cong \{2^n\text{-th roots of unity} : n \in \mathbb{N}\}$$

$$\varinjlim_n \mathbb{Z}/2^n \mathbb{Z} = \left( \bigoplus_{n \in \mathbb{N}} \mathbb{Z}/2^n \mathbb{Z} \right) / \langle i_k(a) - i_j(f_{kj}(a)) \mid k \leq j, a \in \mathbb{Z}/2^k \mathbb{Z} \rangle$$

where  $f_{kj} : \mathbb{Z}/2^k\mathbb{Z} \rightarrow \mathbb{Z}/2^j\mathbb{Z}$ .  
Inverse limit:

$$\varprojlim \mathbb{Z}/2^n\mathbb{Z} = \left\{ (n_1, n_2, \dots) \in \prod_n \mathbb{Z}/2^n\mathbb{Z} \mid \forall i < j, n_i \equiv n_j \pmod{2^{i+1}} \right\}$$

### 1.4.2 Rings and fields

**Def 24.** A **ring** is a non-empty set  $R$  with two operations  $R \times R \rightarrow R$

$$(a, b) \mapsto a + b \quad \text{and} \quad (a, b) \mapsto ab$$

satisfying

1.  $(R, +, 0)$  is an abelian group.
2.  $(R, \cdot)$  is a semigroup. (if it is a monoid, then it is called “a ring with 1.”)
3. (Distributive laws)  $\forall a, b, c \in R, \begin{cases} a(b + c) = ab + ac \\ (b + c)a = ba + ca \end{cases}$

**Eg 1.4.1.**  $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, M_{n \times n}(\mathbb{F})$

**Eg 1.4.2.** Let  $G$  be an abelian group. Define (endomorphism, automorphism)

$$\text{End}(G) := \{ \text{group homo. } G \rightarrow G \} \quad \text{Aut}(G) := \{ \text{group isom. } G \rightarrow G \}$$

A natural ring structure on  $\text{End}(G)$  is:

$$\forall a \in G, \begin{cases} (f + g)(a) := f(a) + g(a) \\ (f \cdot g)(a) := f(g(a)) \end{cases}$$

**Eg 1.4.3.**  $\mathbb{Z}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} \subset \mathbb{R}$ .

**Def 25.** Let  $R$  be a ring with 1.

- (a)  $\forall a \in R, a \neq 0$ ,  $a$  is called a unit if  $\exists a^{-1} \in R$ .
- (b)  $(R^\times = \{\text{units in } R\}, \cdot, 1)$  forms a group.
- (c)  $R$  is called a division ring if  $R \setminus \{0\} = R^\times$ .
- (d)  $R$  is said to be commutative if  $ab = ba, \forall a, b \in R$ .
- (e)  $R$  is a field if  $R$  is a commutative division ring.
- (f)  $a \neq 0$  is called a left zero divisor if  $\exists b \in R, b \neq 0$  s.t.  $ab = 0$ .
- (g)  $a$  is called a zero divisor if  $a$  is either a left or right zero divisor.
- (h)  $R$  is called an integral domain if  $R$  is a commutative ring without zero divisors.

Fact:

1. fields  $\implies$  integral domains.
2. finite + integral domain  $\implies$  fields.

**pf:** Let  $R = \{0, a_1, \dots, a_n\}$ , for  $a \in R, a \neq 0$ ,  $aa_i = aa_j \implies a(a_i - a_j) = 0 \implies i = j$ . So  $\{0, aa_1, \dots, aa_n\} = R \implies \exists a_i$  s.t.  $aa_i = 1$ .  $\square$

**Prop 1.4.1.** TFAE

1.  $\mathbb{Z}/n\mathbb{Z}$  is an integral domain.
2.  $\mathbb{Z}/n\mathbb{Z}$  is a field.
3.  $n = p$  is a prime.

easy to prove.

**Def 26.**

- $f : R_1 \rightarrow R_2$  is called a ring homomorphism if  $\forall a, b \in R, \begin{cases} f(a+b) = f(a) + f(b) \\ f(ab) = f(a)f(b) \end{cases}$ .
- $\text{Im } f$  is a subring of  $R_2$ .
- $\ker f = \{x \in R_1 \mid f(x) = 0\}$  is an additive group of  $R_1$  and  $\forall r \in R_1, x \in \ker f, f(rx) = f(r)f(x) = f(r)0 = 0 \implies rx \in \ker f, xr \in \ker f$ .
- $R_1/\ker f$  is an additive group and  $R_1/\ker f \cong \text{Im } f$  (additive isomorphism).

**Def 27.** Let  $I$  be an additive subgroup of  $R$ .  $I$  is called an ideal if  $\forall r \in R, x \in I, rx \in I, xr \in I$ .  $(R/I, +, \cdot)$  forms a quotient ring under

$$\forall r_1, r_2 \in R, (r_1 + I)(r_2 + I) = r_1 r_2 + I$$

well-defined: easy to show.

**Ex 1.4.3.** State and show the isomorphism theorems and the factor theorem.

**Prop 1.4.2.** If  $R$  is a ring with 1, then  $\exists!$  ring homo.  $\varphi : \mathbb{Z} \rightarrow R$  s.t.  $\varphi(1) = 1$ .

**pf:** Let  $\varphi : \mathbb{Z} \rightarrow R$  is a ring homo. s.t.  $\varphi(1) = 1$ . Then  $\forall n \in \mathbb{Z}, \varphi(n) = \varphi(1) + \dots + \varphi(1) = n1$ . Now  $\forall n, m \in \mathbb{Z}, \varphi(n)\varphi(m) = (n1)(m1) = n(m1) = (nm)1$  by the distributive law. So  $\varphi$  is well-defined and unique.  $\square$

**Def 28.** In Prop 1.4.2,  $\ker \varphi = m\mathbb{Z}$  for some  $m > 0$ . We call  $m$  the characteristic of  $R$ , denoted by  $\text{char } R = m$ .

**Prop 1.4.3.**

1. If  $R$  is an integral domain, then  $\text{char } R = 0$  or  $p$ , where  $p$  is a prime. (try to prove this)
2. In the case of  $\text{char } R = p, \forall a, b \in R, (a+b)^p = a^p + b^p$ .

**pf:**

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \dots + b^p = a^p + b^p$$

$$\text{because } p \mid \binom{p}{i} \implies \binom{p}{i}a^{p-i}b^i = 0.$$

$\square$

**Ex 1.4.4.** Let  $F$  be a field. Show that

1. if  $\text{char } F = 0$ , then  $\mathbb{Q} \hookrightarrow$  subfield of  $F$ .
2. if  $\text{char } F = p$ , then  $\mathbb{Z}/p\mathbb{Z} \hookrightarrow$  subfield of  $F$ .

**Theorem 9.** If  $F$  is a finite field, then  $|F| = p^n$  for some  $n \in \mathbb{N}$  and  $p$  is a prime.

**pf:** By Ex. 1.4.4,  $\text{char } F = p$ ,  $p$  is a prime and  $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$ .

We have  $\mathbb{Z}/p\mathbb{Z} \times F \rightarrow F, (r, v) \mapsto rv$ .  $F$  can be regarded as a vector space over  $\mathbb{Z}/p\mathbb{Z}$ .

Let  $\dim_{\mathbb{Z}/p\mathbb{Z}} F = n$ , then  $F \cong (\mathbb{Z}/p\mathbb{Z})^n \implies |F| = p^n$ . □

**Theorem 10.** Let  $F$  be a field. Then any finite subgroup  $G$  of  $(F^\times, \cdot, 1)$  is cyclic.

**pf:** Let  $|G| = n$ . Define  $h$  to be the max order of an element in  $G$ , say  $a^h = 1$ .

If  $h = n$ , then  $|\langle a \rangle| = h = n = |G|$  and  $\langle a \rangle \subseteq G$ , so  $G = \langle a \rangle$ .

Otherwise,  $h < n$ . We know that  $x^h - 1$  has at most  $h$  roots. So  $\exists b \in G$  is not a root of  $x^h - 1$ .

Let  $\text{ord}(b) = h'$ , so  $h' \mid n$  and  $h' \nmid h$ . So  $\exists$  a prime  $p$  s.t.  $p^r \mid h'$  but  $p^r \nmid h$ .

Write  $h = mp^s$ ,  $s < r$  and  $\gcd(m, p) = 1 \implies \text{ord}(a^{p^s}) = m$ .

Write  $h' = qp^r \implies \text{ord}(b^q) = p^r$ .

Since  $\gcd(m, p^r) = 1$ ,  $\text{ord}(a^{p^s} b^q) = mp^r > mp^s = h$ , which is a contradiction. □

**Ex 1.4.5.**

1. Let  $a, b \in G$  with  $ab = ba$  and  $\text{ord}(a) = m, \text{ord}(b) = n$ . If  $\gcd(m, n) = 1$ , then  $\text{ord}(ab) = mn$ .  
In general, is the order of  $ab$  equal to  $\text{lcm}(m, n)$ ?

2. Let  $G$  be a finite group and  $H, K \leq G$ . Then  $|HK| = \frac{|H||K|}{|H \cap K|}$ .



## 1.5 Week 5

### 1.5.1 Group actions I

**Def 29.** A group  $G$  is said to act on a nonempty set  $X$  if  $\exists$  a map  $G \times X \rightarrow X$  with  $(g, x) \mapsto gx$  s.t.

1.  $1x = x$
2.  $(g_1g_2)x = g_1(g_2x) \quad \forall g_1, g_2 \in G$

**Prop 1.5.1.**  $\{\text{actions of } G\} \leftrightarrow \{\text{group homo. } G \rightarrow S_X\}$

**pf:** Given an action  $(g, x) \mapsto gx$ , consider  $\varphi : G \rightarrow S_X$  s.t.  $\varphi : g \mapsto (\tau_g : x \mapsto gx)$ .

- 1-1:  $gx = gy \implies g^{-1}(gx) = y \implies x = y$ .
- onto:  $\forall y \in X$ , let  $x = g^{-1}y$ , then  $y = gx$ .
- group homo.:  $\varphi(gg') = (\tau_{gg'} : x \mapsto gg'x) = \tau_g \circ \tau_{g'} = \varphi(g)\varphi(g')$ .

Conversely, given a group homo.  $\varphi : G \rightarrow S_X$ , consider  $(g, x) \mapsto \varphi(g)(x)$ .

- $1x = \varphi(1)(x) = \text{Id}(x) = x$ .
- $g_1g_2x = \varphi(g_1g_2)(x) = \varphi(g_1) \circ \varphi(g_2)(x) = g_1(g_2x)$ . □

**Def 30.** A representation of  $G$  on a vector space  $V$  is a group action of  $G$  on  $V$  linearly. i.e.  $\exists$  group homo.  $\varphi : G \rightarrow \text{GL}(V)$ .

**Eg 1.5.1.**

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \text{SO}(2), \quad \bar{k} \mapsto \begin{pmatrix} \cos \frac{2k\pi}{m} & -\sin \frac{2k\pi}{m} \\ \sin \frac{2k\pi}{m} & \cos \frac{2k\pi}{m} \end{pmatrix}$$

**Eg 1.5.2.**

$$S_n \rightarrow \text{GL}(n, \mathbb{R}), \quad \sigma \mapsto (\tau_\sigma : e_i \mapsto e_{\sigma(i)})$$

**Remark 8.**

1. An action  $G \times X \rightarrow X$  is said to be faithful if the corresponding group homo.  $\varphi : G \hookrightarrow S_X$ , denoted by  $G \curvearrowright X$ .
2. In general,  $\ker \varphi = \{g \in G \mid gx = x \quad \forall x \in X\} = \bigcap_{x \in X} \{g \mid gx = x\}$ .  
Define  $G_x = \{g \mid gx = x\} \leq G$  is the isotropy subgroup of  $G$  at  $x$ . (the stabilizer of  $G$  at  $x$ )
3.  $\varphi : G \rightarrow S_X \implies G/\ker \varphi \hookrightarrow S_X$ . So  $G/\ker \varphi \times X \rightarrow X$  is faithful.
4. Let  $\mathcal{C}(X) = \{f : X \rightarrow \mathbb{C}\}$ . If  $G \curvearrowright X$ , then  $G \curvearrowright \mathcal{C}(X)$  by  $G \times \mathcal{C}(X) \rightarrow \mathcal{C}(X)$  with  $(g, f) \mapsto gf(x) = f(g^{-1}x)$ .  
The reason:  $(g_1g_2)f(x) = f((g_1g_2)^{-1}x) = f(g_2^{-1}g_1^{-1}x) = g_1(g_2f)(x)$ .

**Def 31.** Let  $G \curvearrowright X$  and  $x \in X$ .

- The **orbit** of  $x$  is defined to be  $Gx = \{gx \mid g \in G\}$ .
- $G \curvearrowright X$  is said to be transitive if  $\exists$  only one orbit. i.e.  $\forall x, y \in X, \exists g \in G$  s.t.  $y = gx$ .

The set of orbits forms a partition:  $x \sim y \iff \exists g \in G$  s.t.  $y = gx$ .

**Prop 1.5.2.** Let  $G \curvearrowright X$  and  $x \in X$ . Then  $|Gx| = [G : G_x]$ .  
In particular,  $|G| < \infty \implies |G| = |Gx||G_x| \quad \forall x \in X$ .

**pf:** Define  $\psi : Gx \rightarrow \{\text{left coset of } G_x\}$  as  $\psi : gx \mapsto gG_x$ .

- well-defined and 1-1:  $g_1x = g_2x \iff g_2^{-1}g_1x = x \iff g_2^{-1}g_1 \in G_x \iff g_2^{-1}g_1G_x = G_x \iff g_1G_x = g_2G_x$ .
- onto:  $\forall g \in G, \psi(gx) = gG_x$ . □

### 1.5.2 Action by left multiplication

- The action  $G \times G \rightarrow G, (g, x) \mapsto gx$  is associated with  $\varphi : G \hookrightarrow S_G$ . It is faithful (Cayley theorem) and transitive.
- Let  $H \leq G$  and  $X := \{\text{left coset of } H\}$ . The group action  $(g, xH) \mapsto gxH \rightsquigarrow \varphi : G \rightarrow S_X$ .

$$\ker \varphi = \bigcap_{x \in G} \underbrace{xHx^{-1}}_{\text{a conjugate of } H} \leq H$$

which is the largest normal subgroup in  $G$  contained in  $H$ .

**pf:** If  $\begin{cases} N \triangleleft G \\ N \leq H \end{cases}, \forall x \in G, xNx^{-1} \leq xHx^{-1} \implies N = N(xx^{-1}) = xNx^{-1} \leq xHx^{-1}. \quad \square$

**Prop 1.5.3.** Let  $H \leq G$  with  $[G : H] = p$  being the smallest prime dividing  $|G|$ . Then  $H \triangleleft G$ .

**pf:** Let  $X = \{a_1H, \dots, a_pH\}$  (all left coests of  $H$ ) and  $\varphi : G \rightarrow S_p$  be the associated group homo. for the group action  $(g, a_iH) \mapsto ga_iH$ .

By the 1st isom. thm.,  $G/\ker \varphi \hookrightarrow S_p$ .

By Lagrange thm.  $|G/\ker \varphi| \mid |S_p| = p!$  and  $|G/\ker \varphi| \mid |G| \implies |G/\ker \varphi| \mid p$ .

So  $|G/\ker \varphi| = 1$  or  $p$ .

If  $|G/\ker \varphi| = 1 \implies G = \ker \varphi \leq H \leq G$ , which is a contradiction.

So  $|G/\ker \varphi| = p \implies [G : \ker \varphi] = p \implies [G : H][H : \ker \varphi] = p \implies [H : \ker \varphi] = 1 \implies H = \ker \varphi \triangleleft G. \quad \square$

### 1.5.3 Action by conjugation

- The action  $G \times G \rightarrow G, (g, x) \mapsto gxg^{-1}$  is associated with the group homo.  $\varphi : G \rightarrow S_G, g \mapsto (\tau_g : x \mapsto gxg^{-1})$ .

$$\text{Inn}(G) := \{ \tau_g \mid g \in G \}$$

**Fact 1.5.1.**  $\tau_g$  is an automorphism. (isom.  $G \rightarrow G$ )

So  $\varphi : G \twoheadrightarrow \text{Inn}(G) \leq \text{Aut}(G) \leq S_G$ .

$\ker \varphi = \{ g \in G \mid gxg^{-1} = x \ \forall x \in G \} = Z_G$ .

By the 1st isom. thm.,  $G/\ker \varphi \cong \text{Inn}(G)$ .

- The conjugacy class:  $Gx = \{ gxg^{-1} \mid g \in G \} = \text{Cl}(x)$ .
- The centralizer of  $x$  in  $G$ :  $G_x = \{ g \in G \mid gxg^{-1} = x \} = Z_G(x)$ .

$$|\text{Cl}(x)| = [G : Z_G(x)], \text{ if } |G| < \infty, |G| = |\text{Cl}(x)||Z_G(x)|$$

- For  $H \triangleleft G$ , define  $G \times H \rightarrow H, (g, h) \mapsto ghg^{-1}$  with the group homo.  $\varphi : G \rightarrow \text{Aut}(H)$ .

$$\ker \varphi = \{ g \in G \mid gxg^{-1} = x \ \forall x \in H \} = Z_G(H) \implies G/Z_G(H) \leq \text{Aut}(H)$$

- The normalizer of  $H$  in  $G$ :  $N_G(H) = \{ g \in G \mid gHg^{-1} = H \}$

## 1.6 Week 6

### 1.6.1 Group actions II

**Def 32.** Let  $G \curvearrowright X$  and  $|X| < \infty$ . Write  $\text{Fix } G := \{x \in X \mid gx = x \ \forall g \in G\}$ .

- $x \in \text{Fix } G, Gx = \{x\}$ .
- $x \notin \text{Fix } G, |Gx| = [G : G_x]$ .

Let  $\{G_{x_1}, \dots, G_{x_n}\}$  be the set of distinct orbits. After rearrangement, assume  $x_1, \dots, x_r \in \text{Fix } G, x_{r+1}, \dots, x_n \notin \text{Fix } G$ . Then

$$|X| = |\text{Fix } G| + \sum_{i=r+1}^n [G : G_{x_i}]$$

**Theorem 11** (class equation). Let  $|G| < \infty$ . Then either  $G = Z_G$  or  $\exists a_1, \dots, a_m \in G \setminus Z_G$  s.t.

$$|G| = |Z_G| + \sum_{i=1}^n [G : G_{a_i}]$$

**pf:** Consider the action  $(g, x) \mapsto gxg^{-1}$ , then

$$\text{Fix } G = \{x \in G \mid gxg^{-1} = x \ \forall g \in G\} = Z_G$$

It follows from the above argument. □

**Def 33.**  $G$  is called a  $p$ -group if  $|G| = p^n$ , where  $p$  is a prime,  $n \in \mathbb{N}$ .

**Prop 1.6.1.** If  $G$  is a  $p$ -group, then  $Z_G \neq \{1\}$ .

**pf:** Let  $|G| = p^n$ . If  $G = Z_G$ , then done. Otherwise, by the class equation (use action by conjugation),  $|G| = |Z_G| + \sum_{i=1}^n [G : G_{a_i}]$ ,  $a_i \notin Z_G$ .

$$G_{a_i} = Z_G(a_i), \text{ so } a_i \notin Z_G \implies Z_G(a_i) \subsetneq G \implies p \mid [G : Z_G(a_i)] = \frac{|G|}{|Z_G(a_i)|}.$$

$$\text{So } |Z_G| = |G| - \sum_{i=1}^n [G : Z_G(a_i)] \implies p \mid |Z_G| \implies Z_G \neq \{1\}. \quad \square$$

**Prop 1.6.2.** If  $|G| = p^2$ , then  $G$  is abelian. ( $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  and  $\mathbb{Z}/p^2\mathbb{Z}$ )

**pf:** Assume that  $G$  is not abelian. By prop 1.6.1,  $|Z_G| = p \implies |G/Z_G| = p \implies G/Z_G$  is cyclic  $\implies G$  is abelian. (contradiction) □

**Prop 1.6.3.** If  $|G| = p^3$  and  $G$  is not abelian, then  $|Z_G| = p$ .

(Abelian:  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p^3\mathbb{Z}$ )

**Prop 1.6.4.** Let  $|G| = p^n$ . Then  $\forall 0 \leq k \leq n, \exists G_k \triangleleft G$  s.t.  $|G_k| = p^k$  and  $G_i \leq G_{i+1}$ .

In general, for a finite group  $G$ ,  $\exists \{1\} = G_r \triangleleft G_{r-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$  s.t.  $G_i/G_{i+1}$  is cyclic. we call  $G$  a solvable group.

**pf:** By induction on  $n$ ,  $n = 1$  is trivial. For  $n > 1$ , assume that the statement holds for  $n - 1$ . By prop 1.6.1,  $Z_G \neq \{1\}$ .  $\exists a \in Z_G, a \neq 1$ . Let  $\text{ord}(a) = p^l$ , then  $\text{ord}(a^{p^{l-1}}) = p$ .  $\implies$  in any case,  $\exists a \in Z_G$  with  $\text{ord}(a) = p$ .

Now  $|G/\langle a \rangle| = p^{n-1}$ , so by induction hypothesis,  $\forall 0 \leq k \leq n - 1, \exists \overline{G_k} \triangleleft G/\langle a \rangle$  s.t.  $|\overline{G_k}| = p^k, \overline{G_i} \leq \overline{G_{i+1}}$ .

By 3rd isom. thm.,  $\exists G_{k+1} \triangleleft G$  s.t.  $\overline{G_k} = G_{k+1}/\langle a \rangle, G_j \leq G_{j+1}$  and  $|G_{k+1}| = p^{k+1}$ . □

**Prop 1.6.5.** Let a  $p$ -group  $G \curvearrowright X$  with  $|X| < \infty$ . Then  $|X| \equiv |\text{Fix } G| \pmod{p}$ .

**Theorem 12** (Cauchy theorem). Let  $p \mid |G|$ . Then  $\exists a \in G$  s.t.  $\text{ord}(a) = p$ . Consider

$$X = \{ (a_1, \dots, a_p) \mid a_i \in G, a_1 a_2 \dots a_p = 1 \}$$

and the action  $\mathbb{Z}/p\mathbb{Z} \times X \rightarrow X$ :

$$(\bar{k}, (a_1, \dots, a_p)) \mapsto (a_{k+1}, \dots, a_p, a_1, \dots, a_k)$$

(This is well-defined since  $ab = 1 \implies ba = 1$  in a group.) We find that  $(a_1, \dots, a_p) \in \text{Fix } \mathbb{Z}/p\mathbb{Z} \iff a_1 = a_2 \dots a_p$ . By prop 1.6.5,  $|\text{Fix } \mathbb{Z}/p\mathbb{Z}| \equiv |X| \pmod{p}$ . And  $|X| = |G|^{p-1} \equiv 0 \pmod{p}$ . Since  $(1, \dots, 1) \in \text{Fix } \mathbb{Z}/p\mathbb{Z}$ ,  $|\mathbb{Z}/p\mathbb{Z}| \neq 0 \implies |\mathbb{Z}/p\mathbb{Z}| \geq p$ . So  $\exists (a, \dots, a) \in \text{Fix } \mathbb{Z}/p\mathbb{Z} \implies a^p = 1$ .

Application: Let  $|G| = p^3$  and  $G$  be non-abelian ( $p$  is odd). By prop 1.6.3,  $|G/Z_G| = p^2$ . Since  $G$  is non-abelian, we have  $G/Z_G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ . That is,  $\forall a \in G, a^p \in Z_G$ .

So,

$$\exists \varphi : G \rightarrow Z_G \cong C_p \text{ with } \varphi : a \mapsto a^p$$

Since  $G/Z_G$  is abelian,  $[G, G] \leq Z_G$ . And

$$\begin{cases} |[G, G]| \mid |Z_G| = p \\ G \text{ is non-abelian} \end{cases} \implies [G, G] = Z_G$$

**Def 34.**  $[x, y] = x^{-1}y^{-1}xy \in [G, G], [x, y]^p = 1$ .

So  $a^p b^p = a^p b^p [b, a]^p \dots$  換換換總共需要  $p(p-1)/2$

$$a^p b^p = (ab)^p [b, a]^{\frac{p(p-1)}{2}} = (ab)^p$$

So  $\varphi$  is a group homo.

Now if  $\ker \varphi = G$  ( $\forall a \in G, a^p = 1$ ), i.e.  $\varphi$  is trivial, then  $\varphi$  is useless. Else,  $\exists a \in G$  s.t.  $\text{ord}(a) = p^2$ , then  $H = \langle a \rangle \triangleleft G$ . ( $[G : H] = p$  is the smallest prime dividing  $|G|$ )

Also, in this case,  $\varphi : G \rightarrow Z_G \implies G/\ker \varphi \cong Z_G$ . Let  $E = \ker \varphi$ ,  $|E| = p^2$ . By the def. of  $\ker \varphi$ ,  $E \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

We find that  $H \cap E = \langle a^p \rangle$ . Pick  $b \in E \setminus H$  and let  $K = \langle b \rangle \implies |K| = p, H \cap K = \{1\}, HK = G$ .

## 1.6.2 Semidirect product

**Fact 1.6.1.**  $K \triangleleft G, H \triangleleft G, K \cap H = \{1\} \implies KH = K \times H$   
 $(\forall k \in K, h \in H, khk^{-1}h^{-1} \in H \cap K = \{1\}, \implies kh = hk)$

**Fact 1.6.2.** Let  $K, H$  be two groups, and  $G = K \times H \implies K \times \{1\} \triangleleft K \times H, \{1\} \times H \triangleleft K \times H$

**Observation 1.**  $K \leq G, H \triangleleft G, K \cap H = \{1\}$  (K 慘 H 好, 簡稱慘好集)

$\implies$  elements in  $KH$  has unique representation? 好事喔

$KH \iff K \times H$  1-1 corresp,  $(kh) \leftrightarrow (k, h)$

Group operation :  $\forall k_1, k_2 \in K, h_1, h_2 \in H, (k_1 h_1)(k_2 h_2) = k_1 k_2 (k_2^{-1} h_1 k_2) h_2$

Let  $\tau : K \rightarrow \text{Aut}(H), k \mapsto (\tau(k) : h \mapsto khk^{-1})$  (類似  $\in \text{Inn}(H)$ )

**Def 35** (Semi-Direct Product (慘好積)).  $K \rtimes_{\tau} H = \{(k, h) \mid k \in K, h \in H\}$  with group operation :  $(k_1, h_1)(k_2, h_2) = (k_1 k_2, \tau(k_2^{-1})(h_1)(h_2))$  where  $\tau : K \rightarrow \text{Aut}(H)$  (need not to be inner homomorphism)

Properties:

- Associativity: Good, ex
- The identity =  $(1, 1)$
- Inverse :  $(k, h)^{-1} = (k^{-1}, \tau(k)(h^{-1}))$
- $K \cong K \times \{1\} \leq K \times_{\tau} H : (k_1, 1)(k_2, 1) = (k_1 k_2, \tau(k_2^{-1})(1)1) = (k_1 k_2, 1) \in K \times \{1\}$   
 $H \cong \{1\} \times H \leq K \times_{\tau} H : (1, h+1), (1, h_2) = (1, \tau(1^{-1})(h_1)h_2) = (1, h_1 h_2) \in \{1\} \times K$
- $H \triangleleft K \times_t H : (k, h)(1, h')(k, h)^{-1} = (k, hh')(k^{-1}, \tau(k)(h^{-1})) = (1, \tau(k)(hh')\tau(k)(h^{-1})) \in H$
- $\tau(k)(h) = khk^{-1} : (k, 1)(1, h)(k^{-1}, 1) = (k, h)(k^{-1}, 1) = (1, \tau(k)(h))$
- If  $\tau$  is trivial  $\implies K \times_t H \cong K \times H$

**Remark 9.** Some definition swaps the order of  $H$  and  $K$ , i.e.  $(h_1, k_1)(h_2, k_2) = (h_1 \phi(k_1)(h_2), k_1 k_2)$

**Ex 1.6.1.** Show that  $H \rtimes_{\phi} K$  is a group and satisfies the above properties.

**Eg 1.6.1.** Construct a non-abelian group of order 21.

**Fact 1.6.3.**  $\text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^{\times} \cong C_{p-1}$

Sol :  $\phi_k : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}, \bar{1} \mapsto \bar{k}$   
 $\phi_{k_2} \circ \phi_{k_1}(T) = \phi_{k_2}(\bar{k}_1) = \phi_{k_2}(T + \dots + T) = \bar{k}_2 + \dots + \bar{k}_2 = \overline{k_1 k_2}$   
Let  $K = C_3, H = C_7$ , define  $\tau : C_3 \rightarrow \text{Aut}(C_7) \cong C_6, a \mapsto \phi_2$   
 $\phi_k : b \mapsto b^k$   
 $G = \langle a, b | a^3 = 1, b^7 = 1, aba^{-1} = b^2 \rangle$

**Eg 1.6.2.**  $p : \text{odd}, |G| = p^3, G$  is non-abelian.

(sol)  $\phi : G \rightarrow Z(G), a \mapsto a^p$  non trivial case  $\exists a \in G$  with  $\text{ord}(a) = p^2$ . Let  $H = \langle a \rangle$  here  $\phi$  is onto and  $E = \ker \phi \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  And  $|H \cap E| = p$   $H \triangleleft G$  because  $[G : H] = p$  Pick  $b \in E \setminus H$  and let  $K = \langle b \rangle \implies |K| = p, K \cap H = \{1\}$  so  $|G| = |KH| = p^3$

**Fact 1.6.4.**  $\text{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^{\times}$

Sol :  $\phi_k : \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z}, \bar{1} \mapsto \bar{k}, \gcd(k, p) = 1$   
Find a group homo  $\tau : K \implies \text{Aut}(H)$  because  $(1+p)^p \equiv 1 \pmod{p^2}$ ,  $\text{ord}(\overline{1+p}) \in \mathbb{Z}/p^2\mathbb{Z}$  Let  $P = \langle \overline{1+p} \rangle$  is the only subgroup of order  $p$ . (if  $\exists |Q| = p, P \neq Q$  then  $P \cap Q = 1, |PQ| = p^2$ , miserable.) So let  $\tau : b \mapsto (\phi_{1+p} : a \mapsto a^{1+p})$  so  $G = \langle a, b | a^{p^2} = 1, b^p = 1, bab^{-1} = a^{1+p} \rangle$  is a non-abelian group of order  $p^3$ .

**Eg 1.6.3.** Isometry of  $R^n$

**Def 36** (Isometry). An isometry of  $R^n$  is a function  $h : R^n \rightarrow R^n$  that preserves the distance between vectors.

$h = t \circ k$  where  $t$  is translation,  $k$  is an isometry fixing the origin, i.e.  $k \in O(n)$ . Let  $T$  be the group of translations on  $R^n, T \cong (R^n, +, 0), t \mapsto t(0)$ .  
Let  $\tau : O(n) \rightarrow \text{Aut}(T), A \mapsto L_A : R^n \rightarrow R^n, v \mapsto Av$   
 $\implies \text{Isom}(R^n) = O(n) \times_{\tau} R^n$

**Eg 1.6.4.** Quaternion  $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$  is not a semi-direct product of any two proper subgroups.

pf: since  $\{\pm 1\}$  is contained in any non-trivial subgroups, can't find  $H \cap K = \{1\}$ .

**Eg 1.6.5.**  $A_4, V_4 = \{1, (12)(34), (14)(23), (13)(24)\} \triangleleft A_4, V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Let  $H = \langle (123) \rangle \cong C_3$ , define  $\tau : H \rightarrow \text{Aut}(V_4) \cong GL_2(\mathbb{Z}/2\mathbb{Z})$   $(123) \mapsto (\bar{0}\bar{1}; \bar{1}\bar{1})$  so  $A_4 \cong C_3 \times_{\tau} V_4$ .

**Ex 1.6.2.** Construct  $D_n$  as a semi-direct product of  $\mathbb{Z}/n\mathbb{Z}$  and  $\mathbb{Z}/2\mathbb{Z}$ .

**Ex 1.6.3.**

1. Show that  $S_4$  is a semi-direct product of  $V_4$  and  $H = \{ \sigma \in S_4 | \sigma(4) = 4 \} \sim S_3$ .
2. Show that  $S_n$  is a semi-direct product of  $A_n$  and  $H = \langle (12) \rangle$ .

**Remark 10.**

- $\text{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$  (regarded as a vector space over  $\mathbb{Z}/p\mathbb{Z}$ )
- $\text{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}) \cong \text{Aut}(\mathbb{Z}/p\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong C_{p-1} \times C_{q-1}$

## 1.7 Week 7

### 1.7.1 Composition series

Ques: How to simplify a finite group  $G$ ?

Strategy:

- If  $G = \{1\}$ , then done.
- Otherwise, check whether  $G$  has a nontrivial proper normal subgroup.
- If no, then  $G$  is said to be a simple group.
- Otherwise, find a normal subgroup  $G_1$  as large as possible s.t.  $G/G_1$  is simple.
- If  $G_1$  is simple, then done.
- Otherwise, repeat above on  $G_1$  and get  $G_2, \dots, G_n$  s.t.

$$G_n = \{1\} \triangleleft G_1 \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G \quad G_i/G_{i+1} \text{ is simple} \quad \searrow \text{composition factors}$$

Say “it is a composition series” with  $\text{length}(G) = n$ .

Hence simple groups can be regarded as basic building blocks of groups.

The classification of all finite simple groups is given as follows:

1.  $\mathbb{Z}/p\mathbb{Z}$ ,  $p$  is a prime.
2.  $A_n$ ,  $n \geq 5$ .
3. simple groups of Lie type.
4. 26 sporadic simple groups.

**Eg 1.7.1.**  $G = S_4$ ,  $G_1 = A_4$ ,  $G_2 = V_4$ ,  $G_3 = \langle (1\ 2)(3\ 4) \rangle$ ,  $G_4 = \{1\} \rightsquigarrow \text{length}(S_4) = 4$ .  
factors:  $C_2, C_3, C_2, C_2$ .

**Eg 1.7.2.**  $G = \mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle$ .

- $G_1 = \langle \bar{2} \rangle$ ,  $G_2 = \langle \bar{4} \rangle$ ,  $G_3 = \langle \bar{0} \rangle \rightsquigarrow \text{length}(3)$ , factors:  $C_2, C_2, C_3$ .
- $G'_1 = \langle \bar{2} \rangle$ ,  $G'_2 = \langle \bar{6} \rangle$ ,  $G'_3 = \langle \bar{0} \rangle \rightsquigarrow \text{length}(3)$ , factors:  $C_2, C_3, C_2$ .
- $G''_1 = \langle \bar{3} \rangle$ ,  $G''_2 = \langle \bar{6} \rangle$ ,  $G''_3 = \langle \bar{0} \rangle \rightsquigarrow \text{length}(3)$ , factors:  $C_3, C_2, C_2$ .

**Eg 1.7.3.** Let  $|G| = p^n$ . We know  $\forall 0 \leq k \leq n$ ,  $\exists G_k \triangleleft G$  with  $|G_k| = p^k$  and  $G_i \not\leq G_{i+1}$ .  
 $\text{length}(G) = n$ , factors:  $C_p, \dots, C_p$ . ( $n$  times)

**Theorem 13** (Jordan-Hölder theorem). If  $G$  has a composition series, then any two composition series have the same length and the same factors up to permutation.

**Lemma 1** (Zassenhaus lemma). Let  $H' \triangleleft H \leq G$ ,  $K' \triangleleft K \leq G$ . Then  $(H \cap K')H' \triangleleft (H \cap K)H'$ ,  $(H' \cap K)K' \triangleleft (H \cap K)K'$  and

$$(H \cap K)H' / (H \cap K')H' \cong (H \cap K)K' / (H' \cap K)K'.$$

**Theorem 14** (Schreier theorem). Any two normal series of  $G$  have equivalent refinements.  
refinements: inserting a finite number of subgroups into the normal series.

**pf:** For two normal series:

$$\begin{aligned}\{1\} &= H_r \triangleleft H_{r-1} \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = G \\ \{1\} &= K_s \triangleleft K_{r-1} \triangleleft \cdots \triangleleft K_1 \triangleleft K_0 = G\end{aligned}$$

We define

$$\begin{aligned}H_{ij} &= (H_i \cap K_j)H_{i+1} \\ K_{ji} &= (H_i \cap K_j)K_{j+1}.\end{aligned}$$

Then we have

$$\begin{aligned}\{1\} &= H_{(r-1)s} \triangleleft H_{(r-1)(s-1)} \triangleleft \cdots \triangleleft H_{(r-1)0} = H_{r-1} = H_{(r-2)s} \triangleleft \cdots \triangleleft H_{10} = H_1 = H_{0s} \triangleleft \cdots \triangleleft H_{00} = G \\ \{1\} &= K_{(s-1)r} \triangleleft K_{(s-1)(r-1)} \triangleleft \cdots \triangleleft K_{(s-1)0} = K_{s-1} = K_{(s-2)r} \triangleleft \cdots \triangleleft K_{10} = K_1 = K_{0r} \triangleleft \cdots \triangleleft K_{00} = G\end{aligned}$$

Both have size  $= rs$ . By lemma,  $H_{ij}/H_{i(j+1)} \cong K_{ji}/K_{j(i+1)}$ . Note that if  $H_{ij} = H_{i(j+1)}$ , then  $K_{ji} = K_{j(i+1)}$ .  $\square$

*proof of Jordan-Hölder theorem.* Let

$$\begin{cases} \{1\} = G_n \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G & (*) \\ \{1\} = G'_m \triangleleft \cdots \triangleleft G'_1 \triangleleft G'_0 = G & (**) \end{cases}$$

be two composition series.

By Schreier theorem, we get two refined equivalent series  $(*)', (**)'$ . Since  $(*), (**)$  are already composition series,  $(*) = (*)', (**') = (**)'$ . So  $(*), (**)$  are equivalent.  $\square$

*proof of lemma.* First prove  $(H \cap K')H' \triangleleft (H \cap K)H'$ .

- $\forall g \in H \cap K, gK'g^{-1} = K' \rightsquigarrow (gHg^{-1}) \cap (gK'g^{-1} = H \cap K' \text{ and } gH'g^{-1} = H'. \text{ So}$

$$g(H \cap K')H'g^{-1} = (H \cap K')H'$$

- $\forall g \in H', ab \in (H \cap K')H',$

To prove

$$(H \cap K)H'/(H \cap K')H' \cong (H \cap K)K'/(H' \cap K)K'.$$

$$\begin{aligned}(H \cap K)H'/(H \cap K')H' &\cong (H \cap K)(H \cap K')H'/(H \cap K')H' \\ &\cong (H \cap K)/(H \cap K) \cap (H \cap K')H' \\ &\cong (H \cap K)/K \cap (H \cap K')H' \\ &\cong (H \cap K)/(H' \cap K)(H \cap K')\end{aligned}$$

$(K \cap (H \cap K')H' = (H' \cap K)(H \cap K')$ , tricky) By symmetry,

$$(H \cap K)K'/(H' \cap K')K' \cong (H \cap K)/(H' \cap K)(H \cap K')$$

$\square$

**Prop 1.7.1.** Let  $|G| < \infty$ . Then  $G$  is solvable  $\iff$  all composition factors are cyclic of prime order.

**pf:** “ $\Leftarrow$ ”: by def.

“ $\Rightarrow$ ”: If  $G_i/G_{i+1} \cong C_n$  with  $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ .  $\square$

**Observation.** Let  $K \triangleleft G$ . 把  $K, G/K$  拆成兩個 composition series 的話, 就可以把兩串串接起來, 長度就是加起來。



**Ex 1.7.1.** Let  $\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$  be a composition series of  $G$  and  $K \triangleleft G$ . Then after we eliminate equalities,

1.  $\{1\} = (K \cap G_n) \triangleleft (K \cap G_{n-1}) \triangleleft \cdots \triangleleft (K \cap G_1) \triangleleft (K \cap G_0) = K$  is a composition series of  $K$ .
2.  $\{\bar{1}\} = KG_n/K \triangleleft KG_{n-1}/K \triangleleft \cdots \triangleleft KG_1/K \triangleleft KG_0/K = G/K$  is a composition series of  $G/K$ .

**Ex 1.7.2.** Let  $\begin{cases} H \triangleleft G \\ K \triangleleft G \end{cases}$  with  $H \neq K$  s.t.  $G/H, G/K$  are simple. Then  $H/H \cap K, K/K \cap H$  are simple too.

**Ex 1.7.3.** Let  $\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$  be a composition series of length  $n$ . Show by induction on  $n$  that for every composition series of  $G$ :

$$\{1\} = H_m \triangleleft H_{n-1} \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = G,$$

we have  $m = n$  and

$$\{H_{n-1}/H_n, \dots, H_0/H_1\} = \{G_{n-1}/G_n, \dots, G_0/G_1\}$$

**Ex 1.7.4.** Exhibit all composition series for  $Q_8, D_4, \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  respectively.

## 1.7.2 Modules over a PID

**Def 37.** Let  $R$  be a ring with 1. A  $R$ -module is an abelian group  $M$  (written additively) on which  $R$  acts linearly.  $R \times M \rightarrow M \quad (r, x) \mapsto rx$

1.  $r(x + y) = rx + ry \quad r \in R, x, y \in M$
2.  $(r_1 + r_2)x = r_1x + r_2x \quad r_1, r_2 \in R, x \in M$
3.  $(r_1r_2)x = r_1(r_2x) \quad r_1, r_2 \in R, x \in M$
4.  $1x = x \quad x \in M$

**Eg 1.7.4.** A  $k$ -vector space is a  $k$ -module.

**Eg 1.7.5.** An abelian group  $G$  can be regarded as a  $\mathbb{Z}$ -module.

$$\begin{aligned} \mathbb{Z} \times G \rightarrow G \\ (n, a) \mapsto na \end{aligned} \quad \text{by} \quad na = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ times}} & \text{if } n \geq 0 \\ \underbrace{(-a) + \cdots + (-a)}_{n \text{ times}} & \text{if } n < 0 \end{cases}$$

**Eg 1.7.6.** Let  $I$  be an ideal of  $R$ . Then  $I$  can be regarded as an  $R$ -module since  $\forall r \in R, a \in I, \quad ra \in I$ .

**Def 38.** A submodule  $N$  of  $M$  is an additive subgroup of  $M$  s.t.  $\forall r \in R, a \in N, \quad ra \in N$ .

**Prop 1.7.2.** Let  $\phi \neq S \subseteq M$ . The submodule generated by  $S$  is defined to be

$$\begin{aligned} \langle S \rangle_R &= \left\{ \sum_{\text{finite}} r_i x_i \mid x_i \in S, r_i \in R \right\} = \text{the least submodule containing } S \\ &= \bigcap_{S \subseteq N \subseteq M} N \end{aligned}$$

**Def 39.** An  $R$ -module  $M$  is said to be finitely generated if  $\exists x_1, \dots, x_n \in M$  s.t.  $M = \langle x_1, \dots, x_n \rangle_R = Rx_1 + Rx_2 + \dots + Rx_n$

**Eg 1.7.7.**  $R$  is generated by 1 as an  $R$ -module.

**Def 40.** An additive group homo.  $\varphi : M_1 \rightarrow M_2$  is called an  $R$ -module homo. if

$$\varphi(rx) = r\varphi(x) \quad \forall r \in R, x \in M_1$$

**Def 41.** An integral domain  $R$  is called a principal ideal domain (PID) if  $\forall I$  ideal in  $R$ ,  $\exists a \in R$  s.t.  $I = \langle a \rangle_R$ .

**Eg 1.7.8.**  $\mathbb{Z}$  is a PID.

For  $I \subseteq \mathbb{Z}$ ,  $I$  is an additive subgroup, so  $I = m\mathbb{Z} = \langle m \rangle_{\mathbb{Z}}$ .

**Def 42.**  $M$  is said to be a free module of rank  $n$  if  $M \cong R^n = R \oplus \dots \oplus R$  (or  $R \times \dots \times R$ )

**Theorem 15.** If  $R$  is a PID, then any submodule of  $R^n$  is free of rank  $\leq n$ .

**pf:** By induction on  $n$ ,  $n = 1$ ,  $\forall I \subseteq R, \exists a \in R$  s.t.  $I = \langle a \rangle_R = Ra \cong R$  (**as a  $R$ -module**).  
Let  $n > 1$  and  $N$  be a submodule of  $R^n$ . Consider

$$\pi_1 : \begin{matrix} R^n & \rightarrow R \\ (r_1, \dots, r_n) & \mapsto r_1 \end{matrix} \quad \text{and} \quad \pi = \pi_1|_N : N \rightarrow R$$

**case 1:**  $\text{Im } \pi = \{0\}$ . In this case,  $N \subseteq \ker \pi_1 \cong R^{n-1}$ . By induction hypothesis,  $N$  is free of rank  $\leq n-1 < n$ .

**case 2:**  $\text{Im } \pi = \langle a \rangle$ , say  $\pi(x) = a$ . Claim:  $N = Rx \oplus \ker \pi$ ,  $\ker \pi \subseteq \ker \pi_1 \cong R^{n-1}$ .

- $Rx \cap \ker \pi = \{0\}$ :  $rx \in Rx \cap \ker \pi \implies \pi(rx) = 0 \implies r = 0 \implies rx = 0$
- $\forall y \in N, \pi(y) = r_0 a$  for some  $r_0 \in R$ ,  $\pi(y - r_0 x) = 0 \implies y - r_0 x \in \ker \pi$ . So  $N \subseteq Rx \oplus \ker \pi$ .  $\square$

Recall that the elementary matrices are

- $D_i(u) = \text{diag}(1, \dots, 1, u, 1, \dots, 1)$ .  $D_i(u) \in \text{GL}(n, R)$  if  $u$  is a unit.
- $B_{ij}(a) = I_n + ae_{ij}$ ,  $a \in R, i \neq j$ .  $B_{ij}(a)^{-1} = B_{ij}(-a) \implies B_{ij}(a) \in \text{GL}(n, R)$ .
- $P_{ij} = I_n - e_{ii} - e_{jj} + e_{ij} + e_{ji}$ .

**Fact 1.7.1.** If  $R$  is a PID and  $\langle a, b \rangle_R = \langle d \rangle_R$ , then  $d = \gcd(a, b)$ .

**pf:**

- $a \in \langle d \rangle_R \implies a = rd$  for some  $r \in R \implies d \mid a$ .  $v \in \langle d \rangle_R \implies d \mid v$ .
- Let  $c \mid a, c \mid b$ , say  $a = k_1 c, b = k_2 c$ .  $d \in \langle a, b \rangle_R \implies d = x_1 a + x_2 b$  for some  $x_1, x_2 \in R$ . So  $d = x_1 k_1 c + x_2 k_2 c = (x_1 k_1 + x_2 k_2) c \implies c \mid d$ .  $\square$

**Theorem 16.** Let  $R$  be a PID and  $A \in M_{n \times m}(R)$ . Then  $\exists P \in \text{GL}_n(R)$  and  $Q \in \text{GL}_m(R)$  s.t.

$$PAQ = \begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix} \quad \text{with} \quad d_i \mid d_{i+1} \quad \forall i = 1, \dots, r-1$$

**pf:** Define the length  $l(a)$  of  $a \neq 0$  to be  $r$  if  $a = p_1 p_2 \dots p_r$  where  $p_1, \dots, p_r$  are prime elements.  
 prime elements:  $p \mid ab \implies p \mid a$  or  $p \mid b$ .

1. We may assume  $a_{11} \neq 0$  and  $l(a_{11}) \leq l(a_{ij}) \forall a_{ij} \neq 0$ . (換一換就上去了...XD)

2. We may assume  $\begin{cases} a_{11} \mid a_{1k} & \forall k = 2, \dots, m \\ a_{11} \mid a_{k1} & \forall k = 2, \dots, n \end{cases}$ . If  $a_{11} \nmid a_{1k}$ , then we can interchange 2nd and  $k$ th columns to assume  $a = a_{11} \nmid a_{12} = b$ .

Let  $d = \gcd(a, b) \implies \begin{cases} l(d) < l(a) \\ d = ax + by \text{ for some } x, y \in R \end{cases} \implies 1 = \frac{a}{d}x + \frac{b}{d}y$ . Write  $b' = \frac{b}{d}, a' = -\frac{a}{d}$ . Then

$$\begin{pmatrix} -a' & b' \\ y & -x \end{pmatrix} \begin{pmatrix} x & b' \\ y & a' \end{pmatrix} = I_2$$

反正就是移一下減掉, length 會一直變小  $\implies$  這個操作會停.

3. 有這個  $\begin{cases} a_{11} \mid a_{1k} & \forall k = 2, \dots, m \\ a_{11} \mid a_{k1} & \forall k = 2, \dots, n \end{cases}$  就可以全部消掉變成

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{n2} & \dots & b_{nm} \end{pmatrix}$$

4. May assume  $a_{11} \mid b_{kl} \quad \forall k, l$ . 不是的話就把該 row 往第一 row 加上, 重複前面的操作,  $l(a_{11})$  總是變小, 因此會停.

5. 遞迴下去...

最後就弄出想要的矩陣了.

□

## 1.8 Week 8

### 1.8.1 Fundamental theorem of finitely generated abelian groups

**Theorem 17** (Main theorem). Let  $R$  be a PID and  $M$  be a finitely generated  $R$ -module. Then  $M \cong R/d_1R \oplus \cdots \oplus R/d_lR \oplus R^s$ ,  $d_i \in R$  with  $d_i \mid d_{i+1} \quad \forall i = 1, \dots, l-1$  for some  $s \in \mathbb{Z}^{\geq 0}$ .

**pf:** Let  $M = \langle x_1, \dots, x_n \rangle_R$  and consider

$$\begin{aligned} \varphi : R^n &\rightarrow M \\ e_i &\rightarrow x_i \end{aligned}$$

By 1st isom. thm.,  $R^n / \ker \varphi \cong M$ .

We know  $\ker \varphi \cong R^m$  ( $e'_i \mapsto f_i, e'_i \in R^m$ ) for some  $m \leq n$  and  $\forall x \in \ker \varphi \quad \exists! x_1, \dots, x_m \in R$  s.t.

$$x = \sum_{i=1}^m x_i f_i.$$

Note that  $\ker \varphi \subseteq R^n$ . So we can write  $f_i = \sum_{j=1}^n a_{ji} e_j \quad \forall i = 1, \dots, m$ . Then  $x = \sum x_i \sum a_{ji} e_j = \sum (\sum a_{ji} x_i) e_j$ .

$R$  is a PID  $\implies \exists P \in \text{GL}_n(R), Q \in \text{GL}_m(R)$  s.t.

$$PAQ = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \\ & & & & \ddots \end{pmatrix} \quad \text{with } d_i \mid d_{i+1} \quad \forall i = 1, \dots, r-1$$

□

$$R \twoheadrightarrow R w_i / R d_i' w_i$$

$$1 \mapsto \overline{w_i}$$

$$r \mapsto \overline{r w_i}$$

**Remark 11.** If  $R$  is commutative, then “ $R^n \cong R^m \implies n = m$ .”

**Theorem 18.** Let  $G$  be a finitely generated abelian group. Then  $G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_l\mathbb{Z} \oplus \mathbb{Z}^s$ ,  $d_i \in \mathbb{Z}$  with  $d_i \mid d_{i+1} \quad \forall i = 1, \dots, l-1$  for some  $s \in \mathbb{Z}^{\geq 0}$ .

Since  $G$  can be regarded as a f.g.  $\mathbb{Z}$ -module and  $\mathbb{Z}$  is a PID, it follows from the main theorem.

$\text{Tor}(G) = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_l\mathbb{Z} \leq G$  and  $G/\text{Tor}(G) \cong \mathbb{Z}^s$  (free part of  $G$ ).

**Fact 1.8.1.** If  $d = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$ , then  $\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{m_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{m_s}\mathbb{Z}$ .

**Theorem 19** (Chinese Remainder theorem). Let  $R$  be a commutative ring with 1 and  $I_1, \dots, I_n$  be ideals of  $R$ . Then

$$\begin{aligned} \varphi : R &\rightarrow R/I_1 \times \cdots \times R/I_n \text{ is a ring homo.} \\ r &\mapsto (\overline{r}, \dots, \overline{r}) \end{aligned}$$

and

(1) if  $I_i, I_j$  are coprime  $\forall i \neq j$ , then  $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$ .

(2)  $\varphi$  is surjective  $\iff I_i, I_j$  are coprime  $\forall i \neq j$ .

(3)  $\varphi$  is injective  $\iff I_1 \cap I_2 \cap \cdots \cap I_n = \{0\}$ .

So if  $I_i, I_j$  are coprime  $\forall i \neq j$ , then

$$R/I_1 I_2 \cdots I_n \cong R/I_1 \times \cdots \times R/I_n.$$

$I_i, I_j$  are coprime  $\iff I_i + I_j = R$ .

**pf:** we only need to prove (1), (2).

- (1) By induction on  $n$ .  $n = 2$ , need  $I_1 \cap I_2 = \subseteq I_1 I_2$ . Indded,  $I_1 \cap I_2 = (I_1 \cap I_2)R = (I_1 \cap I_2)(I_1 + I_2) \subseteq I_1 I_2$ .

For  $n > 2$ , since  $I_i + I_n = R \quad \forall i = 1, \dots, n-1$ ,  $\exists x_i \in I_i, y_i \in I_n$  s.t.  $x_i + y_i = 1 \quad \forall i = 1, \dots, n-1$ .

So  $x_1 x_2 \dots x_{n-1} = (1 - y_1)(1 - y_2) \dots (1 - y_{n-1}) (I_1 I_2 \dots I_{n-1} = 1 + I_n) \implies I_1 I_2 \dots I_{n-1} + I_n = R$ .

Now,  $I_1 I_2 \dots I_n = (I_1 \dots I_{n-1}) I_n = (I_1 \dots I_{n-1}) \cap I_n = I_1 \cap \dots \cap I_n$ .

- (2) “ $\Rightarrow$ ”: WLOG, we may let  $I_i = I_1, I_j = I_2$ . We have  $x \in R$  s.t.

$$\varphi(x) = (\bar{1}, \bar{0}, \dots, \bar{0}) \quad \text{i.e. } \bar{x} = \bar{1} \text{ in } R/I_1$$

Write  $x \equiv 1 \pmod{I_1}$ . Since  $1 - x \in I_1, x \in I_2$  and  $(1 - x) + x = 1, I_1 + I_2 = R$ .

“ $\Leftarrow$ ”:  $\forall y \in \text{RHS}, y = (\bar{r}_1, \dots, \bar{r}_n)$ . If we may find that  $x_i \in R$  s.t.  $\varphi(x_i) = (\bar{0}, \dots, \bar{1}, \bar{0}, \dots, \bar{0})$ , then

$$\varphi\left(\sum_{i=1}^n r_i x_i\right) = y$$

It is enough to show, for example,  $\exists x \in R$  s.t.  $\varphi(x) = (\bar{1}, \bar{0}, \dots, \bar{0})$ .

Since  $I_1 + I_i = R \quad \forall i = 2, \dots, n$ ,  $\exists x_i \in I_1, y_i \in I_i$  s.t.  $x_i + y_i = 1 \quad \forall i = 2, \dots, n$ .

So let  $x = y_2 \dots y_n = (1 - x_2) \dots (1 - x_n)$ . We have  $x \in I_2, \dots, I_n$  and  $x \equiv 1 \pmod{I_1}$ .

□

**Eg 1.8.1.**  $|G| = 72$  and  $G$  is abelian:

$$72 = 2 \times 36 = 3 \times 24 = 2 \times 2 \times 18 = 6 \times 12 = 2 \times 6 \times 6$$

Invariant factors

Elementary divisors

**Def 43.** The exponent of  $G$  with  $|G| < \infty$  is

$$\text{Exp}(G) := \min \{m \in \mathbb{N} | g^m = 1 \quad \forall g \in G\}$$

**Ex 1.8.1.**

1. Let  $G$  be abelian with  $|G| = n$ . Show that if  $d \div n$ , then  $\exists H \leq G$  s.t.  $|H| = d$ .
2. If  $n = 540, d = 90$ , then construct all possible  $G$  and corresponding  $H$ .

**Ex 1.8.2.** Let  $G$  be abelian with  $|G| < \infty$ . Show that  $G$  is cyclic  $\iff \text{Exp}(G) = |G|$ .

**Ex 1.8.3.** Let  $f_i(x) \in \mathbb{Z}[x], i = 1, \dots, k$  with  $\deg f_i = d$  and  $p_1, \dots, p_k$  be distinct primes. Show that  $\exists f(x) \in \mathbb{Z}[x]$  with  $\deg f = d$  s.t.  $\bar{f}(x) = \bar{f}_i(x)$  in  $\mathbb{Z}/p_i\mathbb{Z}[x] \quad \forall i = 1, \dots, k$ .