Algebra

December 15, 2016

1 Group theory

1.1 Week 1

Def 1. A non-empty set G with a binary function $f : G \times G \to G, (a, b) \mapsto ab$ 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 $H \subseteq G, H \neq \phi$. 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. $\forall a \in H, a^{-1} \in H$.

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

Proof.

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

$\Leftarrow$
1. $H \neq \phi \implies \exists a \in H \implies aa^{-1} = 1 \in H$.
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 $\mathrm{SL}(n, \mathbb{F}) = \{ A \in \mathrm{GL}(n, \mathbb{F}) \mid \det A = 1 \}$
- Orthogonal group $\mathrm{O}(n) = \{ A \in \mathrm{GL}(n, \mathbb{R}) \mid A^{\mathrm{t}} A = I_n \}$
- Unitary group $\mathrm{U}(n) = \{ A \in \mathrm{GL}(n, \mathbb{C}) \mid A^* A = I_n \}$
- Special orthogonal group $\mathrm{SO}(n) = \mathrm{SL}(n, \mathbb{R}) \cap \mathrm{O}(n)$

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

Def 4. Let $f : G_1 \to G_2$. 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.

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

notice that $\mathrm{U}(1) \cong \mathrm{SO}(2)$. $S^1 = \{\, (a,b) \in \mathbb{R}^2 \mid a^2 + b^2 = 1 \,\}$,

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

<u>Quaternion</u>$(\mathbb{H} = \{\, a + bi + cj + dk \mid a,b,c,d \in \mathbb{R} \,\} i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j(\implies ij = -ji)$
$x = a + bi + cj + dk, \bar{x} = a - bi - cj - dk N(x) = x\bar{x} = a^2 + b^2 + c^2 + d^2 x \neq 0, N(x) \neq 0, x^{-1} = \frac{1}{N(x)}\bar{x}$
$x = a + bi + cj + dk = (a + bi) + (c + di)j \mathrm{SU}(2) \cong \{\, x \in \mathbb{H}^\times \mid N(x) = 1 \,\} S^3 = \{\, (a,b,c,d) \in \mathbb{R}^4 \mid a^2 + b^2 + c^2 + d^2 = 1 \,\}$
$\bigstar S^1, S^3$

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 $\mathrm{GL}(n,\mathbb{H})$.

Def 5 (symplectic group)**.** $\mathrm{Sp}(n,\mathbb{F}) = \{\, A \in \mathrm{GL}(2n,\mathbb{F}) \mid A^{\mathrm{t}}JA = J \,\}$ where $J = \begin{pmatrix} O & I_n \\ -I_n & O \end{pmatrix}$.
($A^{\mathrm{t}}JA = J$ preserving non-degenerate skew-symmetric forms)
$\mathrm{Sp}(n) = \{\, A \in \mathrm{GL}(n,\mathbb{H}) \mid A^*A = I_n \,\}$.

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

$\mathrm{SU}(2)\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$

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 $(S_B, \cdot, \mathrm{Id}_B)$ forms a group.
If $B = \{a_1, \ldots, a_n\}$, then $S_B \cong S_{\{1,\ldots,n\}}$ and write $S_n = S_{\{1,\ldots,n\}}$, 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 $\sigma_a : G \to G, x \mapsto ax$. 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. $|S_n| = n!$.

Proof. EASY =O ☐

$\sigma \in S_5 \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \sigma = (1\ 4)(2\ 3\ 5)$
$\Rightarrow$

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.

$\sigma \in S_n \sigma(j_1\ \ldots\ j_m)\sigma^{-1} = (\sigma(j_1)\ \ldots\ \sigma(j_m))$

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

Proof. Note that both sides are functions. For $i \in \{1, \ldots, n\}$,

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

Case 2: Otherwise, CONCON

☐

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

Proof. $(1\ i)^{-1} = (1\ i)$ 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. $S_n = \langle (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle, \quad n \geq 2$.
2. $S_n = \langle (1\ 2), (1\ 2\ \ldots\ n) \rangle, \quad n \geq 2$.

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

Ex 1.2.2.

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

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

$\mathbb{R}^2 \mathrm{O}(2)$
$A = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \in \mathrm{O}(2)$

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \alpha$$

$$A = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} A^2 = I_2 \implies \pm 1$$

$\mathrm{L}_A(v) = v - 2\langle v, v_2 \rangle v_2$

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

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

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

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

$= \langle \text{rotations}, \text{reflections} \rangle$

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

Proof. Let $A = [\mathrm{T}]_\alpha \in M_{n\times n}(\mathbb{R}) \subseteq M_{n\times n}(\mathbb{C})$. Consider $\widetilde{\mathrm{L}_A} : \mathbb{C}^n \to \mathbb{C}^n, v \mapsto Av$.
Then $\exists$ an eigenvalue $\lambda \in \mathbb{C}$ and an eigenvector $v \in \mathbb{C}^n$ for $\widetilde{\mathrm{L}_A}$. Let $\lambda = \lambda_1 + \lambda_2 i, v = v_1 + v_2 i$. By definition, we have

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

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.

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

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 $A = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \in \mathrm{SO}(2)$. 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. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{(n-1)}\}$ with $\overline{j} = \{\, m \in \mathbb{Z} \mid m \equiv j \pmod n \,\}$.
Define $\overline{i} + \overline{j} = \begin{cases} \overline{i+j} & \text{if } 0 \le i+j \le n \\ \overline{i+j-n} & \text{otherwise} \end{cases} \implies (\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ forms a group.

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

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

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

Eg 1.2.7. ... , (generator) $(1, 2, 4, p^k, 2p^k$, p is an odd prime)

Def 14.

- The **order** of a finite gorup 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 $\operatorname{ord}(a) = n$.
- If $a^n \neq 1 \quad \forall n \in \mathbb{N}$, then we call "$a$ has infinte order".

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

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

   Proof.

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

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

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

   Proof. Let $\gcd(r, n) = d, n = dn', r = dr'$ with $\gcd(n', r') = 1$. Plan to show "$\operatorname{ord}(a^r) = n'$."

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

   ☐

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

Proof. Let $G = \langle a \rangle$ and $H \le G$. 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 $m = qd + r, 0 \le r < d$. If $r \neq 0$, then $a^r = a^{m-qd} = a^m(a^d)^{-q} \in H$, which is a contradiction. Hence $r = 0 \implies d \mid m$.

$\square$

Ex 1.2.4.

1. $\mathrm{ord}(a) = \mathrm{ord}(a^{-1}) = n$.
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. $\forall m \mid n, \exists! H \le \langle a \rangle$ s.t. $|H| = m$. Conversely, if $H \le \langle a \rangle$, then $|H| \mid n$.

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

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

Ex 1.2.5. Show Prop 1.2.4.

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

Remark 4. In this case, we find that

- $G = G_1 G_2 = \{\, g_1 g_2 \mid g_1 \in G_1, g_2 \in G_2 \,\}$.
- $G_1 \cap G_2 = \{1\}$. (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 $a = g_1 g_2 = g_1' g_2'$, 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 $g_1 \in G_1, g_2 \in G_2, (g_1, g_2) = (g_1, 1)(1, g_2) = (1, g_2)(g_1, 1) \implies g_1 g_2 = g_2 g_1$.

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. $a = g_1 g_2$; $\forall g_1 \in G_1, g_2 \in G_2, g_1 g_2 = g_2 g_1$.
3. $G_1 \cap G_2 = \{1\}$; $G = G_1 G_2$; $\forall g_1 \in G_1, g_2 \in G_2, g_1 g_2 = g_2 g_1$.

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 $G_1 \times G_2 \ncong G$ since $(1\ 2)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)$.

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

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

Proof.

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

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

$\square$

1.3 Week 3

1.3.1 Coset and Quotient Group

$f : G_1 \to G_2 \mathrm{Im}\, f := f(G_1)$
$\mathrm{Im}\, f \leq G_2$

Proof. Let $z_1 = f(a_1), z_2 = f(a_2)$, then $z_1 z_2^{-1} = f(a_1)f(a_2)^{-1} = f(a_1)f(a_2^{-1}) = f(a_1 a_2^{-1}) \in \mathrm{Im}\, f$. □

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 $H \leq G$, $|H| \mid |G|$.

Proof. □

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.

Proof. □

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

Proof. □

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 $Ha \mapsto a^{-1}H$.

$\{ aH : a \in G \} aH, bH (aH)(bH) = abH$
$(aH)(bH) = abH$

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

$a_1 b_1 H = a_2 b_2 H (a_1 b_1)^{-1} a_2 b_2 \in H$

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

$b_1^{-1} b_2, a_1^{-1} a_2 \in H b_2^{-1} a_1^{-1} a_2 b_2 \in H$

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

Def 19. Let $H \lhd G$. 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 indentity is $H = hH$ and $(aH)^{-1} = a^{-1}H$.)

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

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

(a) $H \lhd G$.

(b) $\forall x \in G, xHx^{-1} = H$.

(c) $\forall x \in G, xH = Hx$.

(d) $\forall x, y \in G, (xH)(yH) = (xy)H$.

G

Prop 1.3.1.

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

   Eg 1.3.2. $n \leq 3, [S_n : A_n] = 2 \implies A_n \lhd S_n$.

   Proof. 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. $Z_G \lhd G$. (by (c) and def.)
2. If G/Z_G is cyclic, then G is abelian.

   Proof. Let $G/Z_G = \langle aZ_G \rangle$, (let $\overline{a} := aZ_G$) 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 $x_1x_2 = a^{k_1+k_2}z_1z_2 = x_2x_1$. ($z_i$) □

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. $[G, G] \lhd G$; $[G, G] = 1 \iff G$ is abelian.

Proof. $\forall x \in G, a \in [G, G], xax^{-1} = xax^{-1}a^{-1}a$ 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 $H \lhd G$ 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 $f : G_1 \to G_2$ be a group homo. Then $G_1/\ker f \cong \operatorname{Im} f$.

Proof. 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: $\varphi\left((a \ker f)(b \ker f)\right) = \varphi(ab \ker f) = f(ab) = f(a)f(b) = \varphi(a \ker f)\varphi(b \ker f)$.
- onto: by def. of $\operatorname{Im} f$.
- 1-1: $f(a) = f(b) \implies a \ker f = b \ker f$ (easy).

$\square$

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

$$\begin{tikzcd} G_1 \arrow[r, "q"] \arrow[dr, "f"'] & G/H \arrow[d, "\varphi"] \\ & G_2 \end{tikzcd}$$

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

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

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

Eg 1.3.6. $\operatorname{sgn} : S_n \to \{\pm 1\} \implies S_n/A_n \cong \{\pm 1\}$

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

Proof. First, $\begin{cases} H \leq G \\ K \lhd G \end{cases} \implies HK = KH \implies HK \leq G$; $K \lhd G \implies K \lhd HK$.
Define $\varphi : H \to HK/K, h \mapsto hK$. which is a group homo.

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

Then by 1st isom. thm. $\square$

Eg 1.3.7. $G = \mathrm{GL}(2, \mathbb{C}), H = \mathrm{SL}(2, \mathbb{C}), K = \mathbb{C}^\times I_2 = Z_G \lhd G$.
By 2nd isom. thm., $G/K \cong H/\{\pm I_2\}$. ($G = HK, \{\pm I_2\} = H \cap K$)
projective linear group: $\mathrm{PGL}(2, \mathbb{C}) = G/K$.
projective special linear group: $\mathrm{PSL}(2, \mathbb{C}) = H/H \cap K$.

Ex 1.3.5.

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

Ex 1.3.6. Let $H \lhd G$ 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 $K \lhd G$.

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

   Proof. 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 $q : G \to G/K$.
     - $H \leq G$: $\forall a, b \in H, q(a), q(b) \in Q \implies q(a)q(b)^{-1} \in Q \implies q(ab^{-1}) \in Q \implies ab^{-1} \in H \implies H \leq G$.
     - $K \leq H$: $\forall a \in K, q(a) = aK = K \in Q \implies a \in H \implies K \leq H$.
     - $Q = H/K$: $\forall aK \in Q, aK = q(a) \implies a \in H \implies aK \in H/K \implies Q \subseteq H/K$. And $\forall aK \in H/K(a \in H), q(a) \in Q \implies H/K \subseteq Q$. So $Q = H/K$.
   - $H \lhd G, K \leq H \iff \forall g \in G, gHg^{-1} = H, K \leq H \iff \forall \overline{g} \in G/K, \overline{g}(H/K)\overline{g}^{-1} = H/K \iff H/K \lhd G/K$. □

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

   Proof. Define $\varphi : G \to (G/K)/(H/K)$ 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., $(G/K)/(H/K) \cong G/H$. □

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

$G/K \cong G'/K'K \cong K' \not\Longrightarrow G \cong G'$

Eg 1.3.9. Q_8 and D_4

$A, BGK \lhd GK \cong A, G/K \cong B1 \to H \to G \to G/H \to 1$
$G = A \times B, K = A \times \{1\}$

1.4 Week 4

1.4.1 Universal property and direct sum & product

$f_1 : G_1 \to G, f_2 : G_2 \to G f_1 \times f_2 : G_1 \times G_2 \to G, (a,b) \mapsto f_1(a)f_2(b)(a,b) = (a,1)(1,b) = (1,b)(a,1)$
$f_1(a)f_2(b) = f_2(b)f_1(a) \implies G$

+0

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 $i_{s_0} : G_{s_0} \to \bigoplus_{s\in\Lambda} G_s, \forall s_0 \in \Lambda$ satisfying the universal property:
for any abelian group H and group homo. $\varphi_s : G_s \to H \forall s \in \Lambda, \quad \exists!$ group homo. $\varphi : \bigoplus_{s\in\Lambda} G_s \to H$ s.t.

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

Proof. 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

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

group operaion: $(g_s)_{s\in\Lambda} + (g'_s)_{s\in\Lambda} := (g_s + g'_s)_{s\in\Lambda} \in \bigoplus_{s\in\Lambda} G_s$.
Uniqueness: Assume $\exists$ another G satisfies the universal property, $\quad (G, \bigoplus_{s\in\Lambda} G_s$ keep i_{s_0}, $\varphi \circ \psi = \mathrm{id}_G, \psi \circ \varphi = \mathrm{id}_{\bigoplus_{s\in\Lambda} G_s})$ ☐

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 $p_{s_0} : \prod_{s\in\Lambda} G_s \to G_{s_0}, \forall s_0 \in \Lambda$ satifsfying the following universal property:
for any group H with group homo. $\varphi_s : H \to G_s, \forall s \in \Lambda, \exists! \varphi : H \to \prod_{s\in\Lambda} G_s$ s.t.

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

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

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

- group operaion: $(g_s)_{s\in\Lambda} \cdot (g'_s)_{s\in\Lambda} := (g_s g'_s)_{s\in\Lambda} \in \prod_{s\in\Lambda} G_s$.
- Define φ: which is uniquely defined.

Uniqueness: Assume $\exists$ another G satisfies the universal property, $\quad (G, \prod_{s\in\Lambda} G_s$ keep i_{s_0}, $\varphi \circ \psi = \mathrm{id}_G, \psi \circ \varphi = \mathrm{id}_{\prod_{s\in\Lambda} G_s})$ ☐

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.

$\zeta_m m \zeta_m^m = 1$

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

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

$f_{kj} : \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}/2^j\mathbb{Z}$

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

1.4.2 Rings and fields

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

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

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) $\forall a,b,c \in \mathbb{R}, \begin{cases} a(b+c) = ab+ac \\ (b+c)a = ba+ca \end{cases}$

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)

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

A natural ring structure on $\mathrm{End}(G)$ 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. $\mathbb{Z}\left[\sqrt{2}\right] = \left\{ a + b\sqrt{2} \,\middle|\, a,b \in \mathbb{Z} \right\} \subset \mathbb{R}$.

Def 25. Let R be a ring with 1.

(a) $\forall a \in R, a \neq 0$, a in 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.

$\implies$

$\implies$

Proof. Let $R = \{0, a_1, \ldots, a_n\}$, for $a \in R, a \neq 0$, $aa_i = aa_j \implies a(a_i - a_j) = 0 \implies i = j$. So $\{0, aa_1, \ldots, aa_n\} = R \implies \exists a_i$ 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.

- $f : R_1 \to R_2$ is called a ring homomorphism if $\forall a, b \in R, \begin{cases} f(a+b) & = f(a) + f(b) \\ f(ab) & = f(a)f(b) \end{cases}$.
- $\operatorname{Im} f$ 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 $R_1/\ker f \cong \operatorname{Im} f$ (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. $\varphi : \mathbb{Z} \to R$ s.t. $\varphi(1) = 1$.

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

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 $\operatorname{char} R = m$.

Prop 1.4.3.

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

   Proof.
   $$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + b^p = a^p + b^p$$
   because $p \mid \binom{p}{1} \implies \binom{p}{i} a^{p-i} b^i = 0$. □

Ex 1.4.4. Let F be a field. Show that

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

Proof. By Ex. 1.4.4, $\operatorname{char} F = p$, p is a prime and $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$.
We have $\mathbb{Z}/p\mathbb{Z} \times F \to F, (r, v) \mapsto rv$. F can be rearded 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.

Proof. 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 $\operatorname{ord}(b) = h'$, 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 $\gcd(m,p) = 1 \implies \operatorname{ord}\left(a^{p^s}\right) = m$.
Write $h' = qp^r \implies \operatorname{ord}(b^q) = p^r$.
Since $\gcd(m, p^r) = 1, \operatorname{ord}\left(a^{p^s} b^q\right) = mp^r > mp^s = h$, which is a contradiction. $\square$

Ex 1.4.5.

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

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 $G \times X \to X$ with $(g, x) \mapsto gx$ s.t.

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

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

Proof. Given an action $(g, x) \mapsto gx$, consider $\varphi : G \to S_X$ 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. $\varphi : G \to S_X$, consider $(g, x) \mapsto \varphi(g)(x)$.

- $1x = \varphi(1)(x) = \mathrm{Id}(x) = x$.
- $g_1 g_2 x = \varphi(g_1 g_2)(x) = \varphi(g_1) \circ \varphi(g_2)(x) = g_1(g_2 x)$. $\square$

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. $\varphi : G \to \mathrm{GL}(V)$.

Eg 1.5.1.

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

Eg 1.5.2.

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

Remark 8.

1. An action $G \times X \to X$ 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 $G_x = \{\, g \mid gx = x \,\} \le G$ is the isotropy subgroup of G at x. (the stabilizer of G at x)
3. $\varphi : G \to S_X \implies G/\ker\varphi \hookrightarrow S_X$. So $G/\ker\varphi \times X \to X$ is faithful.
4. Let $\mathcal{C}(X) = \{\, f : X \to \mathbb{C} \,\}$. If $G \curvearrowright X$, then $G \curvearrowright \mathcal{C}(X)$ by $G \times \mathcal{C}(X) \to \mathcal{C}(X)$ with $(g, f) \mapsto gf(x) = f(g^{-1}x)$.
   The reason: $(g_1 g_2)f(x) = f((g_1 g_2)^{-1}x) = f(g_2^{-1} g_1^{-1} x) = g_1(g_2 f)(x)$.

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, $|G| < \infty \implies |G| = |Gx||G_x| \quad \forall x \in X$.

Proof. Define $\psi : Gx \to \{\text{left coset of } G_x\}$ 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

$G \times G \to G, (g, x) \mapsto gx\varphi : G \hookrightarrow S_G$

$H \le GX := \{\text{left coset of } H\}(g, xH) \mapsto gxH \rightsquigarrow \varphi : G \to S_X$

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

GH

Proof. If $\begin{cases} N \lhd G \\ N \le H \end{cases}$, $\forall x \in G, xNx^{-1} \le xHx^{-1} \implies N = N(xx^{-1}) = xNx^{-1} \le xHx^{-1}$. □

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

Proof. Let $X = \{a_1H, \dots, a_pH\}$ (all left coests of H) and $\varphi : G \to S_p$ 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 $|G/\ker\varphi| = 1 \implies G = \ker\varphi \le H \lneq G$, which is a contradiction.
So $|G/\ker\varphi| = p \implies [G : \ker\varphi] = p \implies [G : H][H : \ker\varphi] = p \implies [H : \ker\varphi] = 1 \implies H = \ker\varphi \lhd G$. □

1.5.3 Action by conjugation

$G \times G \to G(g, x) \mapsto gxg^{-1}\varphi : G \to S_Gg \mapsto (\tau_g : x \mapsto gxg^{-1})$

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

Fact 1.5.1. τ_g is an automorphism. (isom. $G \to G$)

$\varphi : G \twoheadrightarrow \operatorname{Inn}(G) \le \operatorname{Aut}(G) \le S_G$
$\ker\varphi = \{\, g \in G \mid gxg^{-1} = x\forall x \in G \,\} = Z_G$
$G/\ker\varphi \cong \operatorname{Inn}(G)$

- $Gx = \{\, gxg^{-1} \mid g \in G \,\} = \operatorname{Cl}(x)$
- $xGG_x = \{\, g \in G \mid gxg^{-1} = x \,\} = Z_G(x)$

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

$H \lhd GG \times H \to H(g, h) \mapsto ghg^{-1}\varphi : G \to \operatorname{Aut}(H)$

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

$HGN_G(H) = \{\, g \in G \mid gHg^{-1} = H \,\}$

Theorem 11 (Normalizer-Centralizer theorem)**.** If $H \le G$ then $N_G(H)/Z_G(H) \hookrightarrow \operatorname{Aut}(H)$.

Proof. Define $\varphi = g :: N_G(H) \mapsto (h \mapsto ghg^{-1}) :: \operatorname{Aut}(H)$. Then $\ker\varphi = Z_G(H)$, so $N_G(H)/Z_G(H) \cong \operatorname{Im}\varphi \le \operatorname{Aut}(H)$. □

1.6 Week 6

1.6.1 Group actions II

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

$$x \in \operatorname{Fix} G Gx = \{x\}$$

$$x \notin \operatorname{Fix} G |Gx| = [G : G_x]$$

$\{G_{x_1}, \dots, G_{x_n}\} x_1, \dots, x_r \in \operatorname{Fix} G, x_{r+1}, \dots, x_n \notin \operatorname{Fix} G$

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

Theorem 12 (class equation)**.** Let $|G| < \infty$. Then either $G = Z_G$ or $\exists a_1, \dots, a_m \in G \setminus Z_G$ s.t.

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

Proof. Consider the action $(g, x) \mapsto gxg^{-1}$, then

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

It follows from the above argument. $\square$

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 $Z_G \neq \{1\}$.

Proof. Let $|G| = p^n$. If $G = Z_G$, then done. Otherwise, by the class equation (use action by conjugation), $|G| = |Z_G| + \sum_{i=1}^{n} [G : G_{a_i}], \quad a_i \notin Z_G$.
$G_{a_i} = Z_G(a_i)$, so $a_i \notin Z_G \implies Z_G(a_i) \lneq G \implies p \mid [G : Z_G(a_i)] = \frac{|G|}{|Z_G(a_i)|}$.
So $|Z_G| = |G| - \sum_{i=1}^{n} [G : Z_G(a_i)] \implies p \mid |Z_G| \implies Z_G \neq \{1\}$. $\square$

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

Proof. 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) $\square$

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 $\forall 0 \leq k \leq n, \exists G_k \lhd G$ s.t. $|G_k| = p^k$ and $G_i \lneq G_{i+1}$.
In general, for a finite group G, $\exists \{1\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$ s.t. G_i/G_{i+1} is cyclic.
we call G a solvable group.

Proof. By induction on n, $n = 1$ is trivial. For $n > 1$, assume that the statement a holds for $n - 1$.
By prop 1.6.1, $Z_G \neq \{1\}$. $\exists a \in Z_G, a \neq 1$. Let $\operatorname{ord}(a) = p^l$, then $\operatorname{ord}(a^{p^{l-1}}) = p$. $\implies$ in any case, $\exists a \in Z_G$ with $\operatorname{ord}(a) = p$.
Now $|G/\langle a \rangle| = p^{n-1}$, so by induction hypothesis, $\forall 0 \leq k \leq n-1, \exists \overline{G_k} \lhd G/\langle a \rangle$ s.t. $|\overline{G_k}| = p^k, \overline{G_i} \lneq \overline{G_{i+1}}$.
By 3rd isom. thm., $\exists G_{k+1} \lhd G$ s.t. $\overline{G_k} = G_{k+1}/\langle a \rangle, G_j \lneq G_{j+1}$ and $|G_{k+1}| = p^{k+1}$.
$\square$

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

Theorem 13 (Cauchy theorem)**.** Let $p \mid |G|$. Then $\exists a \in G$ s.t. $\operatorname{ord}(a) = p$. Consider

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

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

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

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

$|G| = p^3 G p |G/Z_G| = p^2 G G/Z_G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \forall a \in G, a^p \in Z_G$

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

$G/Z_G [G,G] \leq Z_G$

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

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

$a^p b^p = a^p b^p [b,a]^p \; p(p-1)/2$

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

So φ is a group homo.
Now if $\ker \varphi = G \quad (\forall a \in G, a^p = 1)$, i.e. φ is trivial, then φ is useless. Else, $\exists a \in G$ s.t. $\operatorname{ord}(a) = p^2$, then $H = \langle a \rangle \triangleleft G$. ($[G : H] = p$ is the smallest prime dividing $|G|$)
Also, in this case, $\varphi : G \twoheadrightarrow Z_G \implies G/\ker \varphi \cong Z_G$. 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 H
$\implies KH$
$KH \iff K \times H$ 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 $\tau : K \to \operatorname{Aut}(H), k \mapsto (\tau(k) : h \mapsto khk^{-1})$ ($\in \operatorname{Inn}(H)$)

Def 35 (Semi-Direct Product (. $K \times_\tau H = \{(k,h) | k \in K, h \in H\}$ with group operation : $(k_1, h_1)(k_2, h_2) = (k_1 k_2, \tau(k_2^{-1})(h_1)(h_2))$ where $\tau : K \to \operatorname{Aut}(H)$ (need not to be inner homomorphism)

Properties:

- Associativity: Good, ex
- The identity $= (1,1)$
- Inverse : $(k,h)^{-1} = (k^{-1}, \tau(k)(h^{-1}))$

- $K \cong K \times \{1\} \leq K \times_\tau H : (k_1,1)(k_2,1) = (k_1k_2, \tau(k_2^{-1})(1)1) = (k_1k_2,1) \in K \times \{1\}$ $H \cong \{1\} \times H \leq K \times \tau H : (1,h+1),(1,h_2) = (1,\tau(1^{-1})(h_1)h_2) = (1,h_1h_2) \in \{1\} \times K$
- $H \lhd K \times_t H : (k,h)(1,h')(k,h)^{-1} = (k,hh')(k^{-1},\tau(k)(h^{-1})) = (1,\tau(k)(hh')\tau(k)(h^{-1})) \in H$
- $\tau(k)(h) = khk^{-1} : (k,1)(1,h)(k^{-1},1) = (k,h)(k^{-1},1) = (1,\tau(k)(h))$
- If τ is trivial $\implies K \times_t H \cong K \times H$

Remark 9. Some definition swaps the order of H and K, i.e. $(h_1,k_1)(h_2,k_2) = (h_1\phi(k_1)(h_2), k_1k_2)$

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. $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$

Sol : $\phi_k : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \bar{1} \mapsto \bar{k}$
$\phi_{k_2} \circ \phi_{k_1}(1) = \phi_{k_2}(\overline{k_1}) = \phi_{k_2}(1 + \cdots + 1) = \overline{k_2} + \cdots \overline{k_2} = \overline{k_1k_2}$
Let $K = C_3, H = C_7$, define $\tau : C_3 \to \mathrm{Aut}(C_7) \cong C_6, a \mapsto \phi_2$
$\phi_k : b \mapsto b^k$
$G = \langle a,b | a^3 = 1, b^7 = 1, aba^{-1} = b^2\rangle$

Eg 1.6.2. p : odd, $|G| = p^3$, G is non-abelian.

(sol) $\phi : G \to Z(G), a \mapsto a^p$ non trivial case $\exists a \in G$ with $\mathrm{ord}(a) = p^2$. Let $H = \langle a\rangle$ here ϕ is onto and $E = \ker\phi \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ And $|H \cap E| = p$ $H \lhd G$ 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. $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$

Sol : $\phi_k : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z}, \bar{1} \mapsto \bar{k}, \gcd(k,p) = 1$
Find a group homo $\tau : K \implies \mathrm{Aut}(H)$ because $(1+p)^p \equiv 1 \mod p^2$, $\mathrm{ord}\left(\overline{1+p}\right) = p$. Let $P = \left\langle \overline{1+p}\right\rangle$ is the only subgroup of order p. (if $\exists |Q| = p$, $P \neq Q$ then $P \cap Q = 1$, $|PQ| = p^2$ but $|G| = p(p-1)$, 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 $h : R^n \to R^n$ 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 $\tau : O(n) \to \mathrm{Aut}(T), A \mapsto L_A : R^n \to R^n, v \mapsto Av$
$\implies \mathrm{Isom}(R^n) = O(n) \times_\tau R^n$

Eg 1.6.4. Quaternium $Q_8 = \{\pm1, \pm i, \pm j, \pm k\}$ is not a semi-deriect 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, $V_4 = \{1, (12)(34), (14)(23), (13)(24)\} \lhd A_4, V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

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

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

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.
- Otherwse, repeat above on G_1 and get $G_2, \dots, G_n$ s.t.

$$G_n = \{1\} \lhd G_1 \lhd \cdots \lhd G_1 \lhd G_0 = G \qquad G_i/G_{i+1} \text{ is simple}$$

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 $\forall 0 \leq k \leq n$, $\exists G_k \lhd G$ with $|G_k| = p^k$ and $G_i \lneq G_{i+1}$.
$\text{length}(G) = n$, factors: $C_p, \dots, C_p$. (n times)

Theorem 14 (Jorden-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 $H' \lhd H \leq G, K' \lhd K \leq G$. Then $(H \cap K')H' \lhd (H \cap K)H', (H' \cap K)K' \lhd (H \cap K)K'$ and

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

Theorem 15 (Schreier theorem)**.** Any two normal series of G have equivalent refinements.
refinements: inserting a finite number of subgroups into the normal series.

Proof. For two normal series:

$$\{1\} = H_r \lhd H_{r-1} \lhd \cdots \lhd H_1 \lhd H_0 = G$$
$$\{1\} = K_s \lhd K_{r-1} \lhd \cdots \lhd K_1 \lhd K_0 = G$$

We define

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

Then we have

$$\{1\} = H_{(r-1)s} \lhd H_{(r-1)(s-1)} \lhd \cdots \lhd H_{(r-1)0} = H_{r-1} = H_{(r-2)s} \lhd \cdots \lhd H_{10} = H_1 = H_{0s} \lhd \cdots \lhd H_{00} = G$$
$$\{1\} = K_{(s-1)r} \lhd K_{(s-1)(r-1)} \lhd \cdots \lhd K_{(s-1)0} = K_{s-1} = K_{(s-2)r} \lhd \cdots \lhd K_{10} = K_1 = K_{0r} \lhd \cdots \lhd K_{00} = G$$

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 $K_{ji} = K_{j(i+1)}$. ☐

proof of Jorden-Hölder theorem. Let

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

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

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

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

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

☐

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

Proof. "$\Leftarrow$": by def.
"$\Rightarrow$": If $G_i/G_{i+1} \cong C_n$ with $n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$. ☐

Observation. Let $K \lhd G$. $K, G/K$ composition series

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

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

Ex 1.7.2. Let $\begin{cases} H \lhd G \\ K \lhd G \end{cases}$ 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 $\{1\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$ be a composition series of length n. Show by induction on n that for every composition series of G:

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

we have $m = n$ and

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

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-moduule is an abelian group M (written additively) on which R acts linearly. $R \times M \to M \quad (r, x) \mapsto rx$

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.

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

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

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

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

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

Def 40. An additive group homo. $\varphi : M_1 \to M_2$ 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 $M \cong R^n = R \oplus \cdots \oplus R$ (or $R \times \cdots \times R$)

Theorem 16. If R is a PID, then any submodule of R^n is free of rank $\leq n$.

Proof. By induction on n. If $n = 1$, notice that any submodule is an ideal I by the closure of submodule. Then since R is a PID, $\forall I \subseteq R, \exists a \in R$ 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

$$\pi_1 : \begin{array}{cc} R^n & \to R \\ (r_1, \ldots, r_n) & \mapsto r_1 \end{array} \quad \text{and} \quad \pi = \pi_1\Big|_N : N \to R$$

case 1: $\operatorname{Im} \pi = \{0\}$. 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: $\operatorname{Im} \pi = \langle a \rangle$, say $\pi(x) = a$. Claim: $N = Rx \oplus \ker \pi, \ker \pi \subseteq \ker \pi_1 \cong R^{n-1}$.

- $Rx \cap \ker \pi = \{0\}$: $rx \in Rx \cap \ker \pi \implies \pi(rx) = 0$, then $r\pi(x) = 0$. But integral domain doesn't have zero divisors, so $r = 0$ and hence $rx = 0$.
- $N \supseteq Rx \oplus \ker \pi$: Obvious since $Rx, \ker \pi \subseteq N$.
- $N \subseteq Rx \oplus \ker \pi$: $\forall y \in N, \pi(y) = r_0 a$ 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

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

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

Proof.

- $a \in \langle d \rangle_R \implies a = rd$ for some $r \in R \implies d \mid a$. $v \in \langle d \rangle_R \implies d \mid b$.
- 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 17. Let R be a PID and $A \in M_{n\times m}(R)$. Then $\exists P \in \mathrm{GL}_n(R)$ and $Q \in \mathrm{GL}_m(R)$ s.t.

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

Proof. Define the length $l(a)$ of $a \neq 0$ to be r if $a = p_1 p_2 \ldots p_r$ where $p_1, \ldots, p_r$ 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 $l(a_{11}) \leq l(a_{ij}) \forall a_{ij} \neq 0$. (

$$\begin{cases} a_{11} \mid a_{1k} \forall k = 2, \ldots, m \\ a_{11} \mid a_{k1} \forall k = 2, \ldots, n \end{cases} a_{11} \nmid a_{1k} ka = a_{11} \nmid a_{12} = b$$

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

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

length $\implies$

$$\begin{cases} a_{11} \mid a_{1k} & \forall k = 2, \ldots, m \\ a_{11} \mid a_{k1} & \forall k = 2, \ldots, n \end{cases}$$

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

4. May assume $a_{11} \mid b_{kl} \quad \forall k, l.$ row row $l(a_{11})$

1.8 Week 8

1.8.1 Fundamental theorem of finitely generated abelian groups

Theorem 18 (Structure theorem of finitely generated module over a PID)**.** 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 $d_i \mid d_{i+1} \quad \forall i = 1, \ldots, l-1$ for some $s \in \mathbb{Z}^{\geq 0}$.

Proof. Let $M = \langle x_1, \ldots, x_n \rangle_R$ and consider

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

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 $\forall x \in \ker\varphi \quad \exists! x_1, \ldots, x_m \in R$ s.t. $x = \sum_{i=1}^m x_i f_i$.
Note that $\ker\varphi \subseteq R^n$. So we can write $f_i = \sum_{j=1}^n a_{ji} e_j \quad \forall i = 1, \ldots, m$. Then $x = \sum x_i \sum a_{ji} e_j = \sum \left(\sum a_{ji} x_i\right) e_j$.
R is a PID $\implies \exists P \in \mathrm{GL}_n(R), Q \in \mathrm{GL}_m(R)$ s.t.

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

So consider $[w_i] = Qe_i$. Since P, Q invertible, $R^n = \bigoplus Rw_i, \ker\varphi = \bigoplus d_i Rw_i$ Hence

$$M \simeq R/ker\varphi = \bigoplus Rw_i / \bigoplus d_i Rw_i = \bigoplus R/d_iR$$

□

$$\begin{aligned} R &\twoheadrightarrow Rw_i/Rd_i'w_i \\ 1 &\to \overline{w_i} \\ r &\to \overline{rw_i} \end{aligned}$$

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

Theorem 19. Let G be a finitely generated abelian group. Then Then $G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_l\mathbb{Z} \oplus R^s, d_i \in \mathbb{Z}$ with $d_i \mid d_{i+1} \quad \forall i = 1, \ldots, l-1$ 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.
$\mathrm{Tor}(G) = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_l\mathbb{Z} \leq G$ and $G/\mathrm{Tor}(G) \cong \mathbb{Z}^s$ (free part of G).

Fact 1.8.1. If $d = p_1^{m_1} p_2^{m_2} \ldots p_s^{m_s}$, 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 20 (Chinese Remainder theorem)**.** Let R be a commutative ring with 1 and $I_1, \ldots, I_n$ be ideals of R. Then

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

and

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

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

(3) φ 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

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

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

Proof. we only need to prove (1), (2).

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

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

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 $(1 - x) + x = 1$, $I_1 + I_2 = R$.

"$\Leftarrow$": $\forall y \in$ RHS, $y = (\overline{r_1}, \dots, \overline{r_n})$. 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. $x_i + y_i = 1 \forall i = 2, \dots, n$.

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

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

Ex 1.8.1.

1. Let G be abelian with $|G| = n$. Show that if $d \mid n$, 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 $\iff \operatorname{Exp}(G) = |G|$.

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. $\overline{f}(x) = \overline{f_i}(x)$ in $\mathbb{Z}/p_i\mathbb{Z}[x] \quad \forall i = 1, \dots k$.
$f(x) = a_d x^d + \dots + a_0, \overline{f}(x) = \overline{a_d} x^d + \dots + \overline{a_0}$

1.8.2 Sylow theorems

Def 44. Let $|G| = p^\alpha r$ with $p \nmid r$.

1. If $H \leq G$ with $|H| = p^\alpha$, then we call H a Sylow p-subgroup of G.
2. $\mathrm{Syl}_p(G) =$ the set of all Sylow p-subgroups of G.
3. $n_p = |\mathrm{Syl}_p(G)|$.

Lemma 2 (Key lemma)**.** Let $P \in \mathrm{Syl}_p(G)$ and Q be a p-subgroup of G. Then $Q \cap N_G(P) = Q \cap P$.

Proof. By Lagrange theorem, $H = Q \cap N_G(P)$ is also a p-subgroup of $N_G(P)$ since $|H| \mid |Q|$.
Since $\begin{cases} P \lhd N_G(P) \\ H \leq N_G(P) \end{cases} \implies HP \leq N_G(P)$, we have

$$|HP| = \frac{|H||P|}{|H \cap P|} = p^{\alpha+k-s}$$

where $|H \cap P| = p^s, s \leq k$. Then $p^{\alpha+k-s} \mid |N_G(P)| \mid |G| = p^\alpha r$.
So $k = s \implies H = H \cap P \implies H \leq P \cap Q$. $\square$

Theorem 21 (Sylow I)**.** $\forall 0 \leq k \leq \alpha, \exists H \leq G$ s.t. $|H| = p^k$. In particular, $\mathrm{Syl}_p(G) \neq \phi$.

Proof. By induction on $|G|$. If $|G| = 1$, then $k = 0$, $H = \{1\}$.
Assume $|G| > 1, k \geq 1, \alpha \geq 1$.

case 1: $p \mid |Z_G|$. By Cauchy theorem, $\exists a \in Z_G$ with $\mathrm{ord}(a) = p$. Then $\langle a \rangle \lhd G$ and $|G/\langle a \rangle| = p^{\alpha-1} r \leq |G|$. If $k = 1$, then $H = \langle a \rangle$. Otherwise, we may assume that $1 \leq k-1 \leq \alpha - 1$. By induction hypothesis, $\exists H' = G/\langle a \rangle$ s.t. $|H'| = p^{k-1}$. By 3rd isom. thm., we can write $H' = H/\langle a \rangle$ and thus $|H| = p^k$.

case 2: $p \nmid |Z_G|$. By the class equation, $|G| = |Z_G| + \sum_{i=1}^m \frac{|G|}{|Z_G(a_i)|}, a_i \in Z_G$.

In this cases, $\exists a_j$ s.t. $p \nmid \frac{|G|}{|Z_G(a_j)|} \implies p^\alpha \mid |Z_G(a_j)|$. And $Z_G(a_j) \lneq G$ since $a_j \notin Z_G$. By induction hypothesis, $\exists H \leq Z_G(a_j) \leq G$ s.t. $|H| = p^k$. $\square$

Theorem 22 (Sylow II)**.** Let $P \in \mathrm{Syl}_p(G)$ and Q be a p-subgroup of G. Then $\exists a \in G$ s.t. $Q \leq aPa^{-1}$. In particular, $\forall P_1, P_2 \in \mathrm{Syl}_p(G), \exists a \in G$ s.t. $P_2 = aP_1a^{-1}$.

Proof. Let $X = \{\text{left cosets of } P\}$ and consider $\begin{matrix} Q \times X \to X \\ (a, xP) \mapsto axP \end{matrix}$.
Observe that $xP \in \mathrm{Fix}\, Q \iff axP = xP \quad \forall a \in Q \iff x^{-1}axP = P \quad \forall a \in Q \iff x^{-1}ax \in P \quad \forall a \in Q \iff a \in xPx^{-1} \quad \forall a \in Q$.
We know $|\mathrm{Fix}\, Q| \equiv |X| \pmod p$ and $p \nmid r \implies |\mathrm{Fix}\, Q| \neq 0 \iff \exists a \in G, Q \leq aPa^{-1}$.
In particular, $\begin{cases} P_2 \leq aP_1a^{-1} \\ |P_2| = |aP_1a^{-1}| \end{cases} \implies P_2 = aP_1a^{-1}$. $\square$

Theorem 23 (Sylow III)**.** $n_p \equiv 1 \pmod p$ and $n_p \mid r$.

Proof.
- Consider $\begin{matrix} P \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G) \\ (\ a, \quad Q) \mapsto aQa^{-1} \end{matrix}$ where $P \in \mathrm{Syl}_p(G)$.

$P' \in \mathrm{Fix}\, P \iff aP'a^{-1} = P' \quad \forall a \in P \iff P \leq N_G(P') \cap P = P' \cap P \iff P' = P$.

So $\mathrm{Fix}\, P = \{P\} \implies n_p \equiv |\mathrm{Fix}\, P| = 1 \pmod p$.

- Consider $\begin{array}{rl} G\times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G) \\ (\ a, \quad\quad Q) \mapsto aQa^{-1} \end{array} \implies$ There is only one orbit $\mathrm{Syl}_p(G)$.

  We know $|\mathrm{Syl}_p(G)| = \frac{|G|}{|G_Q|}$ and $G_Q = N_G(Q)$. Then $n_p = \frac{|G|}{|G_Q|} \bigm| |G|$. So $n_p \bigm| p^\alpha r \implies n_p \bigm| r$. $\square$

Prop 1.8.1. Let $|G| = pq$ where p, q are primes with $\begin{cases} p < q \\ q \not\equiv 1 \pmod p. \end{cases}$ Then $G \cong C_{pq}$.

Proof. $n_p = 1 + kp \mid q \implies n_p = 1$ i.e. $H \in \mathrm{Syl}_p(G) \implies H \lhd G$.
$n_q = 1 + kq \mid p \implies n_q = 1$ i.e. $K \in \mathrm{Syl}_q(G) \implies K \lhd G$.
Since $\gcd(p, q) = 1$, $H \cap K = 1$. Hence $G = H \times K \cong C_p \times C_q \cong C_{pq}$. $\square$

Eg 1.8.2. Consider $|G| = 255 = 3 \times 5 \times 17$.

1. normal subgroup (17, 5 or 3)
2. quot abelian $\rightsquigarrow [G, G]$
3. $[G, G] = 1$
4. f.g. xxx thm. $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$.
5. $G \cong C_{255}$.

Ex 1.8.4. If $|G| = 7 \times 11 \times 19$, then G is abelian.

Eg 1.8.3. No group G of order $48 = 2^4 \times 3$ is simple.

1. $n_2 = 1 + 2k \bigm| 3 \rightsquigarrow n_2 = 1$ or 3.
2. $n_2 = 1$ then OK.
3. Assume $n_2 = 3$. Let $P \in \mathrm{Syl}_2(G), X = \{$ left cosets of $P\}$ ($|X| = 3$).
4. Consider $\begin{array}{rl} G\times \quad X \to X \\ (\ a,\ xP) \mapsto axP \end{array} \rightsquigarrow \varphi : G \to S_3$.
5. $\ker \varphi$.

Ex 1.8.5. No group G of order 36 is simple.

Ex 1.8.6. No group G of order 30 is simple.

Ex 1.8.7. Let $|G| = 385$. Show that $\exists P \in \mathrm{Syl}_7(G)$ s.t. $P \leq Z_G$.

1.9 Week 9

1.9.1 Classification

To classify groups of small orders:

- $|G| = 1$: $G = \{1\}$
- $|G| = 2$: $G \cong C_2$
- $|G| = 3$: $G \cong C_3$
- $|G| = 4$: $G \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$
- $|G| = 5$: $G \cong C_5$
- $|G| = 6$: $n_3 = 1, n_2 = 1$ or 3. Let $H \in \mathrm{Syl}_3(G)$ and $H \lhd G$. Let $K \in \mathrm{Syl}_2(G)$. Also $H \cap K = \{1\}$ and $HK = G$ then $G \cong K \times_\tau H$
  - If τ is trivial: $G \cong K \times H \cong C_2 \times C_3 \cong C_6$
  - $\tau : b \mapsto \phi_2 : \langle a \rangle \to \langle a \rangle$: $G \cong K \times_\tau H \cong \langle a, b \mid a^3 = 1, b^2 = 1, bab^{-1} = a^2 = a^{-1} \rangle \cong D_3$
- $|G| = 7$: $G \cong C_7$
- $|G| = 8$:
  - If abelian: $\mathbb{Z}_8$ or $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
  - If non-abelian:
    * $\nexists a \in G$ with $\mathrm{ord}(a) = 8$
    * Not each $a \in G$ with $a^2 = 1$, otherwise G is abelian.
    * $\exists a \in G$ with $\mathrm{ord}(a) = 4$: Let $H = \langle a \rangle$ and $H \lhd G$ since $[G : H] = 2$. Pick $b \in G \setminus H$ and $K = \langle b \rangle$
      · $\mathrm{ord}(b) = 2$: $H \cap K = \{1\}$ and $HK = G$ then $G \cong K \times_\tau H$, $\tau : b \mapsto \phi : a \mapsto a^3$: $G \cong K \times_\tau H \cong \langle a, b \mid a^4 = 1, b^2 = 1, bab^{-1} = a^3 = a^{-1} \rangle \cong D_4$
      · $\mathrm{ord}(b) = 4$: $H \cap K = \langle a^2 = b^2 \rangle$. Then consider $bab^{-1} \in H \implies bab^{-1} = 1, a, a^2, a^3$
        1. $1, a$ obviously wrong.
        2. $bab^{-1} = a^2$: $a = a^2 a a^{-2} = b^2 a b^{-2} = a^4 \implies a^3 = 1$
        3. So $bab^{-1} = a^3 = a^{-1}$.

        $G \cong \langle a, b \mid a^4 = 1, b^4 = 1, a^2 = b^2, bab^{-1} = a^3 = a^{-1} \rangle \cong Q_8$
- $|G| = 9$: $G \cong \mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$
- $|G| = 10$: $G \cong K \times H \cong C_2 \times C_5 \cong C_{10}$ or $G \cong D_5$
- $|G| = 11$: $G \cong C_{11}$
- $|G| = 12$: Claim: If $|G| = 12$, then either G has a normal Sylow 3-subgroup or $G \cong A_4$.

  Proof. By Sylow 3, $n_3 = 1 + 3k \mid 4 \implies n_3 = 1$ or 4.
  - If $n_3 = 1$, then G has a normal Sylow 3-subgroup.
  - Otherwise, let $P \in \mathrm{Syl}_3(G)$ and $X = \{\text{left cosets of } P\}, |X| = 4$. Consider $G \times X \to X$ defined by $(a, xP) \mapsto axP$ with $\phi : G \to S_4$. And $\ker \phi \le P$, $|P| = 3$ and $P \ntriangleleft G$ (since $n_3 = 4$), so $\ker \phi = \{1\}$.

    And since $n_3 = 4$, there are 8 elements of order 3 which corresponds to 8 3-sycles in A_4, thus $|\mathrm{Im}\, \phi \cap A_4| \ge 8$. But $|\mathrm{Im}\, \phi \cap A_4| \;\big|\; |A_4| = 12 \implies \mathrm{Im}\, \phi = A_4$

  $\square$

Now, for the case where $\exists H \in \mathrm{Syl}_3(G)$ and $H \lhd G$. Let $K \in \mathrm{Syl}_2(G)$, then $K \cap H = \{1\}$ and $KH = G \implies G \cong K \times_\tau H$ for some $\tau : K \to \mathrm{Aut}(H) = \{\mathrm{id}, \phi_2\}$

- τ is trivial: $\mathbb{Z}_{12}$ or $\mathbb{Z}_2 \times \mathbb{Z}_6$.
- $\langle b \rangle = K \cong \mathbb{Z}_4$: $\tau(b) = \phi_2 \implies G = \langle a, b \mid a^3 = 1, b^4 = 1, bab^{-1} = a^{-1} \rangle \ncong D_6, A_4$
- $\langle b \rangle = K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$: Let $K = \langle b, c \mid b^2 = 1, c^2 = 1, bc = cb \rangle$, then $\tau : b \mapsto \phi_2$ and $c \mapsto \mathrm{id}$ (the other cases are equivalent to this one), $G = \langle a, b, c \mid a^3 = 1, b^2 = 1, c^2 = 1, bc = cb, bab^{-1} = a^{-1}, cac^{-1} = a \rangle \cong \langle a, b \mid a^3 = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle \times \langle c \rangle \cong D_3 \times C_2 \cong D_6$

  Fact 1.9.1. For odd n, $D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}$.

  Proof.
  $$D_{2n} = \langle a, b \mid a^{2n} = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$$
  $$H = \langle a^2, b \mid (a^2)^n = 1, b^2 = 1, b(a^2)b^{-1} = a^{-2} \rangle \cong D_n$$
  $$K = \langle a^n \rangle \cong C_2$$
  And n is odd, so $H \cap K = \{1\}$ and $D_{2n} \cong D_n \times C_2$ □

- $|G| = 13$: $G \cong C_{13}$
- $|G| = 14$: $G \cong C_{14}$ or D_7
- $|G| = 15$: $G \cong C_{15}$

Ex 1.9.1. Assume that K is cyclic and H is an arbitrary group. Let $\tau_1 : K \to \mathrm{Aut}(H)$, $\tau_2 : K \to \mathrm{Aut}(H)$ with $\tau_1(K) \sim \tau_2(K)$ (conjugate). If $|K| = \infty$, then assume that τ_1 and τ_2 are injective. Show that $K \times_{\tau_1} H \cong K \times_{\tau_2} H$.

Ex 1.9.2. Classify G if $|G| = p^3$ with p an odd prime and each nontrivial element of G has order p.

Ex 1.9.3. Classify groups of order 30.

1.9.2 Free groups

A free group generate by a non-empty set X is that there are no relations satisfied by any of elements in X.

Def 45. A free group on X is a group F with an inclusion map $i : X \to F$ satisfying the following universal property: For any group G and any map $f : X \to G$, exists a unique group homo $\varphi : F \to G$ that the following diagram commutes.

$$\begin{tikzcd} X \arrow[r] \arrow[dr] & F \arrow[d, "\varphi"] \\ & G \end{tikzcd}$$

Theorem 24. F exists and is unique up to isomorphism. (Denote it as $F(X) = F$).

Proof. For X, we create a new disjoint set $X^{-1} = \{x^{-1} : x \in X\}$ and an element $1 \notin X \cup X^{-1}$. Define $F(X) = \{1\} \cup \left\{ x_1^{\delta_1} x_2^{\delta_2} \cdots x_m^{\delta_m} : m \in \mathbb{N}, x_i \in X, \delta_i = \pm 1, x_{i+1}^{\delta_{i+1}} \neq \left(x_i^{\delta_i}\right)^{-1} \right\}$, and

$$x_1^{\delta_1} x_2^{\delta_2} \cdots x_m^{\delta_m} = y_1^{\epsilon_1} y_2^{\epsilon_2} \cdots y_m^{\epsilon_m} \iff n = m \text{ and } \delta_i = \epsilon_i \text{ and } x_i = y_i, \forall i$$

For each $y \in X \cup X^{-1}$, we define $\sigma_y : F(X) \to F(X)$ by

$$\sigma_y(x_1^{\delta_1} x_2^{\delta_2} \cdots x_m^{\delta_m}) = \begin{cases} y x_1^{\delta_1} x_2^{\delta_2} \cdots x_m^{\delta_m} & \text{if } x_1^{\delta_1} \neq y^{-1} \\ \begin{cases} x_1^{\delta_1} x_2^{\delta_2} \cdots x_m^{\delta_m} & (m \geq 2) \\ 1 & (m = 1) \end{cases} & \text{if } x_1^{\delta_1} = y^{-1} \end{cases}$$

Then σ_y is a permutation of $F(X)$, since if $\sigma_y(x_1^{\delta_1}x_2^{\delta_2}\cdots x_m^{\delta_m}) = \sigma_y(y_1^{\epsilon_1}y_2^{\epsilon_2}\cdots y_m^{\epsilon_m})$.

m = n: either $x_1^{\delta_1} = y_1^{\epsilon_1} = y^{-1}$ or not, then either $x_2^{\delta_1}x_3^{\delta_2}\cdots x_m^{\delta_m} = y_2^{\epsilon_1}y_3^{\epsilon_2}\cdots y_m^{\epsilon_m}$ or $yx_1^{\delta_1}x_2^{\delta_2}\cdots x_m^{\delta_m} = yy_1^{\epsilon_1}y_2^{\epsilon_2}\cdots y_m^{\epsilon_m}$. Both of them leads to $x_1^{\delta_1}x_2^{\delta_2}\cdots x_m^{\delta_m} = y_1^{\epsilon_1}y_2^{\epsilon_2}\cdots y_m^{\epsilon_m}$.

m = n+2: Omimi

Also σ_y is onto since omimi. And notice that $\sigma_{y^{-1}} \circ \sigma_y = id_{F(X)}$
Define $A = \langle \sigma_x : x \in X \rangle \le S_{F(X)}$. and define $\phi : F(X) \to A$ by $\phi(1) = id_{F(X)}$ and $x_1^{\delta_1}\cdots x_m^{\delta_m} \mapsto \sigma_{x_1}^{\delta_1}\cdots\sigma_{x_m}^{\delta_m}$. The it is omimi that ϕ is a bijection. So we define $x :: X \cdot y :: X = \phi^{-1}(\phi(x) \circ \phi(y))$.
The ϕ in the universal property could be defined as $\phi(x_1^{\delta_1}x_2^{\delta_2}\cdots x_m^{\delta_m}) = f(x_1)^{\delta_1}\cdots f(x_m)^{\delta_m}$. □

Prop 1.9.1. Let $G = \langle a_1, \cdots, a_n \rangle$ and $X = \{x_1, \cdots, x_m\}$. Then $G \cong F(X)/K$ for some normal subgroup K. K is called the subgroup of relations connecting the generators.
Define $f = x_i :: X_i \to a_i :: G$. By universal property, $\exists \phi = x_i :: F(X) \mapsto a_i :: G$. Then $F(x)/\ker\phi \cong G$.

Def 46. Let $X = \{x_1, x_2, \cdots, x_n\}$ and $R \subset F(X)$. Let $N(R)$ be the smallest normal subgroup of $F(X)$ containing R, Then $G = F(X)/N(R)$ is written as $\langle x_1, \cdots, x_n \mid \text{elements of } R\rangle$, which is called a presentation of G. If $|R| < \infty$, then G is said to be finitely presented.

Eg 1.9.1.

$$D_n = \left\langle \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle$$

We find that $x^n, y^2, xyxy \in \ker\phi$. Then $R = \{x^n, y^2, xyxy\} \subseteq \ker\phi \implies N(R) \le \ker\phi$. By factor theorem, $\exists\bar{\phi} :: F(X)/N(R) \to D_n$. But notice that

$$|F(x)/N(R)| \le 2n$$

since $xyxy = 1 \implies xy = yx^{-1}$, so every element could be turn into x^iy^j. Hence $\bar{\phi}$ is an isomorphism.

Prop 1.9.2. Let $X = \{x_1, x_2, \cdots, x_n\}$. Then $F(X)/[F(X), F(X)] \cong \mathbb{Z}^n$.

Proof. Define $f = x_i :: X \mapsto e_i :: \mathbb{Z}^n$. Then $\phi = x_i :: F(X) \mapsto e_i :: \mathbb{Z}^n$. By 1st isomorphism theorem $F(X)/\ker\phi \cong \mathbb{Z}^n$ which is abelian, so $[F(X), F(X)] \le \ker\phi$. By factor theorem,
$\bar{\phi}$

Proof. Since $F(X)/[F(X), F(X)]$ is abelian, $\forall a \in F(X)/[F(X), F(X)]$, we can write $a = \bar{x}_1^{n_1}\bar{x}_2^{n_2}\cdots\bar{x}_m^{n_m}$.
If $\bar{\phi}(\bar{a}) = (m_1, \cdots, m_n) = 0$ in $\mathbb{Z}^n$, then $m_i = 0, \forall i \implies a = 1$ □

2 Multilinear algebra

2.1 Week 11

2.1.1 Bilinear forms & Groups preserving bilinear forms

Def 47. Let V be a vector space over a field F.

- A function $f : V \times V \to F$ is called a bilinear form if

$$\begin{cases} f(rx_1 + x_2, y) & = rf(x_1, y) + f(x_2, y) \\ f(x, ry_1 + y_2) & = rf(x, y_1) + f(x, y_2) \end{cases} \qquad \forall x_1, x_2, x, y_1, y_2, y \in V, r \in F$$

- $B_F(V, V) = \{$ bilinear forms on $V\,\}$ can be regarded as a vector space over F.

Theorem 25. Let $\dim V = n$ and $\beta = \{v_1, \ldots, v_n\}$ be a basis for V. Then $\exists$ an isomorphism $\psi_\beta : B_F(V, V) \to M_{n\times n}(F)$.

Proof. For $v, w \in V$, write $v = \sum_i a_i v_i$, $w = \sum_j b_j v_j$, i.e. $[v]_\beta = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, $[w]_\beta = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

For $f \in B_F(V, V)$, $f(v, w) = \sum_i \sum_j a_i b_j f(v_i, v_j) = \begin{pmatrix} a_1 & \ldots & a_n \end{pmatrix} \begin{pmatrix} & & \\ & f(v_i, v_j) & \\ & & \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

Define $\psi_\beta(f) = A$ with $A_{ij} = f(v_i, v_j)$.

- ψ_β is a linear transformation.
- ψ_β is 1-1.
- ψ_β is onto: $\forall A \in M_{n\times n}(F)$, we define $f(v, w) = [v]_\beta^t A [w]_\beta$. □

Def 48. Let $f \in B_F(V, V)$

- f is said to be symmetric if $f(v, w) = f(w, v) \quad \forall v, w \in V$.
- f is said to be skew-symmetric if $f(v, w) = -f(w, v) \quad \forall v, w \in V$.
- f is said to be alternating if $f(v, v) = 0 \quad \forall v \in V$.

Remark 12.

- Alternating $\implies$ skew-symmetric.
- If $\operatorname{char} F \neq 2$, skew-symmetric $\implies$ alternating.
- If $\operatorname{char} F = 2$, symmetric = skew-symmetric.
- $\forall f \in B_F(V, V)$ with $\operatorname{char} F \neq 2$,

$$f_s(u, v) = \frac{1}{2}\left(f(u, v) + f(v, u)\right)$$
$$f_a(u, v) = \frac{1}{2}\left(f(u, v) - f(v, u)\right)$$

  and $f(u, v) = f_s(u, v) + f_a(u, v)$.

So we only need to study “symmetric” & “alternating”.

Ex 2.1.1.

1. If A and B are congruent ($B = Q^t AQ$) in $M_{n\times n}(F)$, then they define the same bilinear form.

2. f is $\begin{cases}\text{symmetric} \\ \text{skew-symmetric}\end{cases} \iff \psi_\beta(f)$ is $\begin{cases}\text{symmetric}(A^t = A) \\ \text{skew-symmetric}(A^t = -A)\end{cases}$

Observation. Let $f \in B_F(V,V)$ and $v_0 \in V$.

$$\begin{aligned} L_f(v_0) &= f(v_0,\cdot) \in V' = \mathrm{Hom}(V,F) : \text{the dual space of } V \\ R_f(v_0) &= f(\cdot, v_0) \in V' \end{aligned}$$

The left radical of f : $\mathrm{lrad}(f) = N(L_f) = \{\, v \in V \mid f(v,w) = 0 \quad \forall w \in V \,\}$.
The right radical of f : $\mathrm{rrad}(f) = N(R_f) = \{\, w \in V \mid f(v,w) = 0 \quad \forall v \in V \,\}$.

Ex 2.1.2.

1. $\mathrm{rank}(\psi_\beta(f)) = \mathrm{rank}(R_f) = \mathrm{rank}(L_f)$.

2. If $\dim V = n$, then TFAE ($\implies f$: non degenerate)

   (a) $\mathrm{rank}(f) = n$.

   (b) $\forall v \in V, v \neq 0, \exists w \in V$ s.t. $f(v,w) \neq 0$.

   (c) $\mathrm{lrad}(f) = \{0\}$.

   (d) $L_f : V \to V'$ is isom.

   (also, right)

Theorem 26 (Principal Axis theorem)**.** Let $\dim V = n$ and $\mathrm{char}\, F \neq 2$. If $f \in B_F(V,V)$ is symmetric, then $\exists \beta$ s.t. $\psi_\beta(f)$ is diagonal.

Proof. It is sufficient to find $\beta = \{v_1,\ldots,v_n\}$ s.t. $f(v_i,v_j) = 0 \quad \forall i \neq j$.
If $f = 0$, then done! Assume $f \neq 0$. By induction on n: If $n = 1$, done. Let $n > 1$.
Claim 1: $\exists v_1 \in V$ s.t. $f(v_1,v_1) \neq 0$. Assume that $f(v,v) = 0 \quad \forall v \in V$.

$$f(v,w) = \frac{1}{4}f(v+w,v+w) - \frac{1}{4}f(v-w,v-w) = 0$$

So $f = 0$, which is a contradiction.
Now let $v_1 \in V$ with $f(v_1,v_1) \neq 0$. Let $W = \langle v_1\rangle_F$ and $W^\perp = \{\, w \in V \mid f(v_1,w) = 0 \,\} \subseteq V$.
Claim 2: $V = W \oplus W^\perp$

- $V = W + W^\perp$: For all $v \in V$, let $a = f(v,v_1)/f(v_1,v_1)$, then $v = av_1 + (v - av_1) \triangleq w + w'$ where $w \in W$ and $f(w',v_1) = f(v - av_1, v_1) = f(v,v_1) - af(v_1,v_1) = 0$. So $w' \in W^\perp$ and thus $V = W + W^\perp$.

- $W \cap W^\perp = \{0\}$: obviously since if $av_1 \in W$, $f(av_1,v_1) = 0 \iff a = 0 \iff av_1 = 0$.

Since $f\Big|_{W^\perp \times W^\perp}$ is a symmetric bilinear form on $W^\perp$ and $\dim W^\perp < \dim V$. By induction hypothesis, $\exists\{v_2,\ldots,v_n\}$ a basis for $W^\perp$ s.t. $f(v_i,v_j) = 0 \quad \forall i \neq j$. Then $\beta = \{v_1,\ldots,v_n\}$. $\square$

Theorem 27 (Sylvester's theorem)**.** Let $f \in B_{\mathbb{R}}(V,V)$ be symmetric with $\dim V = n$. Then $\exists\beta$ s.t. $\psi_\beta(f) = \begin{pmatrix} 1 &&&&&&&& \\ & \ddots &&&&&&& \\ && 1 &&&&&& \\ &&& -1 &&&&& \\ &&&& \ddots &&&& \\ &&&&& -1 &&& \\ &&&&&& 0 && \\ &&&&&&& \ddots & \\ &&&&&&&& 0 \end{pmatrix}$.

The triple (# of 1, # of -1, # of 0) is well-defined. (called the signature of f)

Proof. Assume $V^+ = \langle v_1, \ldots, v_p \rangle_F, V^- = \langle v_{p+1}, \ldots, v_r \rangle_R, V^\perp = \langle v_{r+1}, \ldots, v_n \rangle_F$. $(V = V^+ \oplus V^- \oplus V^\perp)$
Claim: If W is a subspace of V s.t. f is positive-definite on W, then $W, V^-, V^\perp$ are independent. Let $\langle w_1, w_2, \cdots, w_s \rangle$ be a basis of W. If

$$a_1 w_1 + a_2 w_2 + \cdots + a_s w_s = b_{p+1} v_{p+1} + \cdots + b_r v_r + c_{r+1} v_{r+1} + \cdots + c_n v_n.$$

Let $w \triangleq a_1 w_1 + \cdots + a_s w_s, v \triangleq b_{p+1} v_{p+1} + \cdots + b_r v_r + c_{r+1} v_{r+1} + \cdots + c_n v_n$. Since $w = v$, $f(w,w) = f(v,v)$. but $f(w,w) = \sum a_i^2 \geq 0$ and $f(v,v) = -\sum b_i^2 \leq 0$. Hence $a_i = 0, b_i = 0$. Since $v_{r+1}, \cdots, v_n$ is linear independent, $c_i = 0$. Therefor these vectors are linear independent.

$\square$

Ex 2.1.3. Let $f \in B_F(V,V)$ with $\operatorname{char} F \neq 2$. If f is skew-symmetric, then $\exists\beta$ s.t.

$$\psi_\beta(f) = \begin{pmatrix} 0 & 1 &&&&&&&&& \\ -1 & 0 &&&&&&&&& \\ && 0 & 1 &&&&&&& \\ && -1 & 0 &&&&&&& \\ &&&& \ddots &&&&&& \\ &&&&& 0 & 1 &&&& \\ &&&&& -1 & 0 &&&& \\ &&&&&&& 0 &&& \\ &&&&&&&& \ddots && \\ &&&&&&&&& 0 \end{pmatrix}$$

Ex 2.1.4. Study Hermitian form

$\mathsf{T} : V \xrightarrow{\sim} V, f \in B_F(V,V)$. T preserves f if $f(\mathsf{T}(v), \mathsf{T}(w)) = f(v,w) \quad \forall v, w \in V$.
In matrix form, let β be a basis for V, $M = [\mathsf{T}]_\beta, A = \psi_\beta(f)$, then $A = M^t A M$.

- $f \in B_{\mathbb{R}}(V,V)$ symmetric, non-degenerate: $\exists\beta$ s.t. $\psi_\beta(f) = \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix}$.

  Then $\{\, \mathsf{T} : V \xrightarrow{\sim} V \text{ preserves } f \,\} \leftrightarrow \left\{ M \in \mathrm{GL}_n(\mathbb{R}) \middle| M^t \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} M = \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} \right\} = \mathrm{O}(p,q)$.

- $f \in B_{\mathbb{R}}(V,V)$ skew-symmetric, non-degenerate: $n = 2k$, $\exists\beta$ s.t. $\psi_\beta(f) = J$.

  Then $\{\, \mathsf{T} : V \xrightarrow{\sim} V \text{ preserves } f \,\} \leftrightarrow \{\, M \in \mathrm{GL}_n(\mathbb{R}) | M^t J M = J \,\}$, where

$$J = \begin{pmatrix} 0 & I_k \\ -I_k & 0 \end{pmatrix}$$

2.1.2 Tensor product

From now on, R is assumed to be commutative with 1.

Def 49. Let $M_1, \dots, M_n, L$ be R-modules.
A function $F : M_1 \times \cdots \times M_n \to L$ is said to be n-multilinear if $\forall i$,

$$f(x_1, \dots, rx_i + x_i', \dots, x_n) = rf(x_1, \dots, x_i, \dots, x_n) + f(x_1, \dots, x_i', \dots, x_n) \quad \forall r \in R, x_i, x_i' \in M_i$$

If $n = 2$, f is called a bilinear map.

Def 50. Let M, N be R-modules. A tensor product of M and N is an R-module $M \otimes_R N$ with a bilinear map $\rho : M \times N \to M \otimes_R N$ satisfying the following universal property:
for any R-momdule W and any bilinear map $f : M \times N \to W$, $\exists!$ R-module homomorphism $\varphi : M \otimes_R N \to W$,

$$\begin{tikzcd} M \times N \arrow[r, "\rho"] \arrow[dr, "f"'] & M \otimes_R N \arrow[d, "\varphi"] \\ & W \end{tikzcd}$$

Theorem 28 (Main theorem)**.** $M \otimes_R N$ exists and is unique up to isom.

Proof. Let $X = M \times N$. First we construct the free module $V_1 = \bigoplus_{(x,y) \in X} R \cdot (x, y)$.

Notice that in V_1,

- $(x_1, y_1) + (x_2, y_2) \neq (x_1 + x_2, y_1 + y_2)$.
- $r(x, y) \neq (rx, ry)$.
- $r(r_1(x_1, y_1) + \cdots + r_n(x_n, y_n)) = rr_1(x_1, y_1) + \cdots + rr_n(x_n, y_n)$.

Let $V_0 = \left\langle \begin{array}{c} (x_1 + x_2, y) - (x_1, y) - (x_2, y), \\ (x, y_1 + y_2) - (x, y_1) - (x, y_2), \\ r(x, y) - (rx, y), r(x, y) - (x, ry) \end{array} \middle| x_1, x_2, x \in M, y_1, y_2, y \in N, r \in R \right\rangle_R$.

Define $M \otimes_R N = V_1/V_0$ which is an R-module and $\begin{array}{c} \rho : M \times N \to M \otimes_R N \\ (x, y) \mapsto (x, y) + V_0 = x \otimes y \end{array}$ which is R-bilinear. (check yourself)

Universal property: $\forall (x, y) \in M \times N$, $\begin{array}{c} R(x, y) \to W \\ r(x, y) \mapsto rf(x, y) \end{array}$. So, by the universal property of $\oplus$, $\exists!$ R-module homo. $\varphi_1 : V_1 \to W$:

$$\begin{tikzcd} M \times N \arrow[r, "i"] \arrow[dr, "f"'] & V_1 \arrow[d, "\varphi_1"] \\ & W \end{tikzcd}$$

Claim: $V_0 \subseteq \ker \varphi_1$. (check yourself) Then by factor theorem,

$$\begin{tikzcd} \exists! \varphi : V_1/V_0 \arrow[rr] & & W \\ & M \times N \arrow[ul] \arrow[ur] & \end{tikzcd}$$

$\square$

Eg 2.1.1. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$.

Eg 2.1.2. $\mathbb{R}[x, y] \cong \mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{R}[y]$.

Proof. $\begin{array}{c} \mathbb{R}[x] \times \mathbb{R}[y] \to \mathbb{R}[x, y] \\ (f(x), g(y)) \mapsto f(x)g(y) \end{array}$ is bilinear $\rightsquigarrow$ $\begin{array}{c} \exists! \varphi : \mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{R}[y] \to \mathbb{R}[x, y] \\ f(x) \otimes g(y) \mapsto f(x)g(y) \end{array}$.

Conversely, $\begin{array}{c} \mathbb{R}[x, y] \to \mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{R}[y] \\ h(x, y) = \sum a_{ij} x^i y^j \mapsto \sum a_{ij} x_i \otimes y_j \end{array}$. $\square$

Prop 2.1.1. If $M = \langle x_1, \dots, x_n \rangle_R$ and $N = \langle y_1, \dots, y_m \rangle_R$. Then

$$M \otimes_R N = \langle x_i \otimes y_j \mid i = 1, \dots, n; j = 1, \dots, m \rangle_R.$$

In particular, if R is a field F, then $\dim_F M \otimes_F N = (\dim_F M)(\dim_F N)$.

Proof. Note that $M \otimes_R N = \langle x \otimes y \mid x \in M, y \in N \rangle$. Let $x = \sum_i a_i x_i, y = \sum_j b_j y_j$. Then $x \otimes y = \sum_i \sum_j a_i b_j x_i \otimes y_j$. □

Some canonical isomorphisms:

- $(M \otimes_R N) \otimes_R L \cong M \otimes_R (N \otimes_R L)$.

  Proof. $\forall z \in L$, $\begin{array}{c} M \times N \to M \otimes_R (N \otimes_R L) \\ (x, y) \mapsto x \otimes (y \otimes z) \end{array}$ is bilinear. $\exists!$ R-mod homo. $\varphi_z : M \otimes_R N \to M \otimes_R (N \otimes_R L)$. Similarly, $\begin{array}{c} (M \otimes_R N) \times L \to M \otimes_R (N \otimes_R L) \\ (\sum x_i \otimes y_i, z) \mapsto \sum x_i \otimes (y_i \otimes z) \end{array}$ is bilinear. (The right is due to φ_z linear, and the left is because $x \otimes (y \otimes (rz_1 + z_2)) = rx \otimes (y \otimes z_1) + x \otimes (y \otimes z_2)$.) Hence exists unique R-mod homo. $\varphi : (M \otimes_R N) \otimes_R L \to M \otimes_R (N \otimes_R L)$. By the symmetric construction, we have φ^{-1} and $\varphi^{-1} \circ \varphi = \varphi \circ \varphi^{-1} = 1$, so the two are isomorphic. □

- $(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$.

  The mapping $\psi :: (M \oplus M') \times N \to (M \otimes_R N) \oplus (M' \otimes_R N)$ by $\psi = ((x, x'), y) \mapsto (x \otimes y, x' \otimes y)$ is biliear, hence exists R-mod homomorphism $\varphi :: (M \oplus M') \otimes_R N \to (M \otimes_R N) \oplus (M' \otimes_R N)$.

  On the other hand, The mapping $(x, y) :: M \times N \mapsto (x, 0) \otimes y :: (M \oplus M') \otimes_R N$ is bilinear. So exists $\phi_1 :: M \otimes N \to (M \oplus M') \otimes_R N$, similarly there exists $\phi_2 :: M' \otimes N \to (M \oplus M') \otimes_R N$. Now by the universal property of direct sum, there exists $\phi :: (M \otimes_R N) \oplus (M' \otimes_R N) \to (M \oplus M') \otimes_R N$. After a careful examine, we have

  $$\varphi = (x, x') \otimes y \mapsto (x \otimes y, x' \otimes y), \phi = (x \otimes y, x' \otimes y) \mapsto (x, x') \otimes y$$

  Thus $\phi = \varphi^{-1}$ and hence the two are isomorphic.

Ex 2.1.5.

1. $R \otimes_R M \cong M$.
2. $M \otimes_R N \cong N \otimes_R M$.

Ex 2.1.6. $R/I \otimes_R N \cong N/IN$ where $IN := \{\sum a_i x_i \mid a_i \in I, x_i \in N\}$.

Ex 2.1.7. Compute $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}), \dim_{\mathbb{R}}(\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C}), \dim_{\mathbb{R}}(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}), \dim_{\mathbb{C}}(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C})$

2.2 Week 12

2.2.1 Tensor product II

By universal property, we get $\{R\text{-bilinear maps } M \times N \to L\} \leftrightarrow \operatorname{Hom}_R(M \otimes_R N, L)$.
Similarly,

$$\operatorname{Hom}\left(\bigoplus_{s\in\Lambda} M_s, L\right) \cong \prod_{s\in\Lambda} \operatorname{Hom}(M_s, L)$$
$$\operatorname{Hom}\left(N, \prod_{s\in\Lambda} M_s\right) \cong \prod_{s\in\Lambda} \operatorname{Hom}(N, M_s)$$

Fact 2.2.1. $f \in \operatorname{Hom}_R(M, M'), g \in \operatorname{Hom}_R(N, N') \rightsquigarrow f \otimes g \in \operatorname{Hom}_R(M \otimes N, M' \otimes N')$ by $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.

Proof. Define $\begin{aligned} h : M \times N &\to M' \otimes_R N' \\ (x, y) &\mapsto f(x) \otimes g(y) \end{aligned}$ □

Restrition and extension of scalars.
Let $f : R \to S$ be a ring homomorphism and R, S be commutative with 1. Then S can be regarded as an R-module. $\begin{pmatrix} R \times S \to S \\ (r, x) \mapsto f(r)x \end{pmatrix}$.
If M is a S-module, then M is also an R-module. $\begin{pmatrix} R \times M \to M \\ (r, a) \mapsto f(r)a \end{pmatrix}$.
If N is an R-module, then $S \otimes_R N$ an S-module. $\begin{pmatrix} S \times (S \otimes_R N) \to S \otimes_R N \\ (r, \quad x \otimes a) \mapsto rx \otimes a \end{pmatrix}$.

Eg 2.2.1 (Important example)**.** Let V be a real vector space. The complexification of V is $V^{\mathbb{C}} := \mathbb{C} \otimes_{\mathbb{R}} V$ which is a $\mathbb{C}$-vector space.

Ex 2.2.1. Let $K \subseteq L$ be an inclusion of fields and let E be a vector space over K. Show that $E^L := L \otimes_K E$ satisfies the following universal property: For any vector space U over L and any K-linear map $f : E \to U$, $\exists!$ L-linear map φ:

$$\begin{tikzcd} \varphi : 1 \otimes x :: E^L \arrow[rr] & & f(x) :: U \\ & x :: E \arrow[ul] \arrow[ur, "f"'] & \end{tikzcd}$$

Ex 2.2.2. $E \to E^L$ is a covariant functor from the category of vector spaces over K to the category of vector spaces over L.

Eg 2.2.2. $\mathbb{Z}^n \cong \mathbb{Z}^m \rightsquigarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^m \rightsquigarrow n = m$.

Eg 2.2.3. $G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_l\mathbb{Z} \oplus \mathbb{Z}^s, \mathbb{Q} \otimes_{\mathbb{Z}} G = \mathbb{Q}^s$.

Let M, N and U be R-module. Then

$$\operatorname{Hom}_R(M \otimes_R N, U) \cong \operatorname{Hom}_R(N, \operatorname{Hom}_R(M, U))$$

Proof.

- For $f \in \operatorname{Hom}_R(M \otimes_R N, U)$ and $a \in N$, define $f_a = x :: M \mapsto f(x \otimes a) :: U$.
  - linear: easy.

- $\overline{f} : a \mapsto f_a$ is an R-mod homo.: easy.
- $\tau : f \mapsto \overline{f}$ is an R-mod homo.: $\tau(rf+g)(a)(x) = (rf+g)_a(x) = (rf+g)(x \otimes a) = rf(x \otimes a) + g(x \otimes a) = \cdots = r\tau(f)(a)(x) + \tau(g)(a)(x)$

- For $g \in \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, U))$, define $g' = (x, a) :: M \times N \mapsto g(a)(x) :: U$.
  - g' is R-bilinear: easy.
  - $\exists! \tilde{g} : x \otimes a \mapsto g(a)(x)$.
  - $\sigma : g \mapsto \tilde{g}$ is an R-mod homo.: easy.
- $\sigma\tau = \mathrm{id}, \tau\sigma = \mathrm{id}$: easy... $\square$

Ex 2.2.3. $\mathrm{Hom}_R(M, \cdot), M \otimes_R \cdot$ are covariant functors from the category of R-modules to itself. (is an adjoint pair)

Fact 2.2.2. $\mathrm{Hom}_R(R, M) \cong M$. By $f \mapsto f(1)$.

Def 51. An exact sequence $A \xrightarrow{f_1} B \xrightarrow{f_2} \cdots$ is a sequence satisfied $\mathrm{im}\, f_k = \ker f_{k+1}$.

- $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z}$.
- $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

Let V, W be vector spaces over F. Then $V^* \otimes_F W \cong \mathrm{Hom}_F(V, W)$.

Proof. Let $\alpha = \{e_1, \ldots, e_n\}$ and $\beta = \{f_1, \ldots, f_m\}$ be bases for V and W respectively. Via α, β, $\mathrm{Hom}_F(V, W) \cong \left\langle E_{ij} \,\middle|\, \begin{matrix} i = 1, \ldots, m \\ j = 1, \ldots, n \end{matrix} \right\rangle_F$. $V^* \otimes W \cong \left\langle e_j^* \otimes f_i \,\middle|\, \begin{matrix} i = 1, \ldots, m \\ j = 1, \ldots, n \end{matrix} \right\rangle_F$. $\square$

2.2.2 Tensor algebra

Def 52.

- Let R be a commutative ring with 1. An R-algebra is a ring A which is also an R-module s.t. the multiplication map $A \times A \to A$ is R-bilinear. ($r(ab) = (ra)b = a(rb)$)
- Let A be an R-algebra. A grading of A is a collection of R-submodules $\{A_n\}_{n=0}^{\infty}$ (n-th homogeneous part) s.t.

$$A = \bigoplus_{n=0}^{\infty} A_n \quad \text{and} \quad A_n A_m \subseteq A_{n+m} \quad \forall n, m$$

- A graded R-algebra is an R-algebra with a chosen grading.
- $\mathfrak{M}_R$ is the category of R-modules.
- $\mathfrak{Gr}_R$ is the category of graded R-algebras. ($f : A \to A'$ with $f(A_n) \subseteq A'_n$)

Eg 2.2.4. $A = R[x], A_n = \langle x^n \rangle_R$. If $I = \langle x+1 \rangle_A$, I is not graded. $I = \langle x^2 \rangle_A$ is graded.

Def 53. An ideal I is graded in a graded ring A if and only if $I = \bigoplus I \cap A_n$. [1]

Ex 2.2.4. TFAE

(1) I is graded.

[1] This is not mentioned in class

(2) $\forall a \in I$ write $a = a_{k_1} + a_{k_2} + \cdots + a_{k_m}, a_{k_i} \in A_{k_i} \implies a_{k_i} \in I$. ($a_{k_i}$ is the homogenuous component of a)

(3) A/I is a graded ring with $(A/I)_n = (A_n + I)/I \cong A_n/I \cap A_n$.

Ex 2.2.5.

(1) If I is a f.g. graded ideal, then I has a finite system of generators consisting of homogeneous elements alone.

(2) I, J are graded $\implies I + J, IJ, I \cap J$ are graded.

<u>Observation</u>: Let $\{M_i\}_{i=1}^{\infty}$ be a collection of R-modules.

- $M_1 \otimes_R M_2$ exists.
- $(M_1 \otimes_R M_2) \otimes_R M_3 \cong M_1 \otimes_R (M_2 \otimes_R M_3) \implies M_1 \otimes_R M_2 \otimes_R M_3$ is well-defined. Universal property: for any R-module L and a 3-multilinear map $f : M_1 \times M_2 \times M_3 \to L$. (

  $M_1 \otimes \cdots \otimes M_n n$

Goal: For a given R-module M, we intend to construct an graded R-algebra $T(M)$ containing M that is "universal" w.r.t. R-algebras containing M.
That is, a tensor algebra is a pair $(T(M), i)$ where $T(M)$ is an R-algebra and $i :: M \to T(M)$, such that for any R-algebra A containing M, which is to say that exist a R-module homomorphism $\varphi : M \to A$, then exists an R-algebra homomorphism $\psi :: T(M) \to A$ such that $\varphi = \psi \circ i$.

<u>Construction</u>:

- $\forall k \in \mathbb{N}$, $T^k(M) := \underbrace{M \otimes \cdots \otimes M}_{k \text{ times}}$, each $x_1 \otimes x_2 \otimes \cdots \otimes x_k \in T^k(M)$ is called a k-tensor.

  $T^0(M) := R$ and
  $$T(M) := \bigoplus_{k=0}^{\infty} T^k(M) = R \oplus T^1(M) \oplus \dots$$
- define multiplication on $T(M)$ by:
  $$\begin{aligned} T^i(M) \times T^j(M) &\longrightarrow T^{i+j}(M) \\ (x_1 \otimes \cdots \otimes x_i, y_1 \otimes \cdots \otimes y_j) &\longmapsto x_1 \otimes \cdots \otimes x_i \otimes y_1 \otimes \cdots \otimes y_j \end{aligned}$$
- Distribution law: easy.

Proving the universal property: For any R-algebra A containing M and an R-module homo. $\varphi : M \to A$. $\forall k \geq 2$, we define $f_k : M \times \cdots \times M \to A$
$$\begin{aligned} f_k : M \times \cdots \times M &\to A \\ (x_1, \dots, x_k) &\mapsto \varphi(x_1) \dots \varphi(x_k) \end{aligned}$$
f_k is k-multilinear $\rightsquigarrow$
$$\begin{aligned} \exists! \tilde{f}_k : M \otimes \cdots \otimes M &\to A \\ x_1 \otimes \cdots \otimes x_k &\mapsto \varphi(x_1) \dots \varphi(x_k) \end{aligned}$$
By the universal property of $\bigoplus$, exists a unique R-module homo. $\tilde{\varphi} :: T(M) \to A$ which make the following diagram commutes.
$$\begin{tikzcd} \tilde{\varphi} : T(M) \arrow[rr] & & A \\ & T^k(M) \arrow[ul, "i"] \arrow[ur, "f_k"'] & \end{tikzcd}$$
$\tilde{\varphi}$ is an R-algebra homomorphism.

Def 54. $T(M)$ is called the tensor algebra of M.

Ex 2.2.6. T is a covariant functor from $\mathfrak{M}_R$ to $\mathfrak{Gr}_R$.

Prop 2.2.1. Let V be a vector space over F with a basis $\beta = \{v_1, \ldots, v_n\}$. Then

$$\{v_{i_1} \otimes \cdots \otimes v_{i_k} \mid \forall j = 1, \ldots, k,\ i_j = 1, \ldots, n\}$$

forms a basis for $T^k(V)$. $\dim_F T^k(V) = n^k$.

$T(V)$ can be regarded as a non-commutative polynomial algebra over F.

$\odot$ Symmetrization ($\operatorname{char} F = 0$)

$$\begin{aligned} V \times \cdots \times V &\longrightarrow T^n(V) \\ (x_1, \ldots, x_n) &\longmapsto \frac{1}{n!} \sum_{\tau \in S_n} x_{\tau(1)} \otimes \cdots \otimes x_{\tau(n)} \end{aligned}$$

is n-multilinear.
The symmetrizer operator $\sigma : T^n(V) \to T^n(V)$, $\tilde{S}^n(V) := \sigma(T^n(V)) \subseteq T^n(V)$.
<u>Claim</u>: $T^n(V) = \tilde{S}^n(V) \oplus C^n(V)$ where

$$C^n(V) = C(V) \cap T^n(V) \quad C(V) = \langle v \otimes w - w \otimes v \mid v, w \in V \rangle$$

2.3 Week 13

2.3.1 Symmetric and Exterior algebra

Symmetric algebra Define

$$\begin{aligned} S : \mathfrak{M}_R &\to \mathfrak{Gr}_R \\ M &\mapsto T(M)/C(M) \end{aligned} \qquad S(M) := T(M)/C(M)$$

where $C(M)$ is the gradded two-sided ideal generated by $u \otimes v - v \otimes u$ with $u, v \in M$.

- $C^k(M) := C(M) \cap T^k(M)$ is the submodule of $T^k(M)$ generated by all

$$x_1 \otimes \ldots \otimes x_k - x_{\sigma(1)} \otimes \ldots \otimes x_{\sigma(k)} \quad \forall x_i \in M, \sigma \in S_k.$$

  "$\subseteq$": $x_1 \otimes \ldots \otimes x_s \otimes (u \otimes v - v \otimes u) \otimes y_1 \otimes \ldots \otimes y_t \in C(M) \cap T^k(M)$ with $s + 2 + t = k$.

  "$\supseteq$": bubble sort

- $k \geq 2, S^k(M) = T^k(M)/C^k(M) = \langle \overline{x}_1 \otimes \ldots \otimes \overline{x}_k \mid x_i \in M \rangle_R$ with $\overline{x}_1 \otimes \ldots \otimes \overline{x}_k = \overline{x}_{\sigma(1)} \otimes \ldots \otimes \overline{x}_{\sigma(k)} \quad \forall \sigma \in S_k$

Hence, $S(M) = \bigoplus_{k=0}^{\infty} S^k(M)$ is a graded commutative R-algebra.

Def 55. $f : M \times \cdots \times M \to L$ is a symmetric k-multilinear map if f is k-multilinear and

$$f(x_1, \ldots, x_k) = f(x_{\sigma(1)}, \ldots, x_{\sigma(k)}) \quad \forall \sigma \in S_k$$

- $k \geq 2$, $S^k(M)$ is universal w.r.t. symmetric k-multilinear maps on M: By the universal property of $T^k(M)$, $\exists!$ R-module homo. $\tilde{f} : T^k(M) \to L$. Now $C^k(M) \subseteq \ker \tilde{f} \implies \exists!$ R-module homo. $\overline{f} : S^k(M) \to L$ by factor thm.

- $S(M)$ satisfies the universal property for maps to a commutative R-algebra: given a commmutative R-algebra A and $f : M \to A$ R-module homo.,

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, hook] & A \\ T(M) \arrow[ur, "\exists! f'"] \arrow[r] & T(M)/C(M) \arrow[u] \end{tikzcd}$$

- $S : \mathfrak{M}_R \to \mathfrak{Gr}_R$ is a covariant functor.
  - $\varphi : M \to N$: R-module homo. $\rightsquigarrow T(\varphi) : T(M) \to T(N) \to T(N)/C(N) = S(N)$

Ex 2.3.1. Let E be a vector space over F with $\dim E = n$.

1. Show that $S(E) \cong F[x_1, \ldots, x_n]$.
2. Compute $\dim_F S^k(E)$.

Exterior algebra ($\operatorname{char} R \neq 2$)

$$\begin{aligned} \Lambda : \mathfrak{M}_R &\to \mathfrak{Gr}_R \\ M &\mapsto \Lambda(M) = T(M)/A(M) \end{aligned}$$

where $A(M)$ is the two sided graded generated by $v \otimes v \quad \forall v \in M$.

- $A^k(M) := A(M) \cap T^k(M)$ is the submodule of $T^k(M)$ generated by all $x_1 \otimes \ldots \otimes x_k$ with $x_i = x_j$ for some $i \neq j$.

  (Note: $(x_1 + x_2) \otimes (x_1 + x_2) = x_1 \otimes x_1 + x_1 \otimes x_2 + x_2 \otimes x_1 + x_2 \otimes x_2 \rightsquigarrow x_1 \otimes x_2 + x_2 \otimes x_1 \in A(M)$)

- $\Lambda^k(M) \cong T^k(M)/A^k(M) = \langle \overline{x_1 \otimes \ldots \otimes x_k} \mid x_i \in M \rangle$ with $\overline{x_1 \otimes \ldots \otimes x_k} = \overline{0}$ if $x_i = x_j$ for some $i \neq j$. We use $x_1 \wedge \cdots \wedge x_k := \overline{x_1 \otimes \ldots \otimes x_k}$.

  Note: $x_1 \wedge x_2 = -x_2 \wedge x_1$.

Def 56. $f : M \times \cdots \times M \to L$ is an alternating k-multilinear map if f is k-multilinear and $f(x_1, \ldots, x_k) = 0$ when $x_i = x_j$ for some $i \neq j$.

- $k \geq 2$, $\Lambda^k(M)$ is universal w.r.t. alternating k-multilinear maps on M:

$$\begin{tikzcd} M \times \cdots \times M \arrow[r] \arrow[d] & L \\ T^k(M) \arrow[r] \arrow[ur, "\exists! f'"'] & \Lambda^k(M) \arrow[u] \end{tikzcd}$$

- $\Lambda(M)$ satisfies the universal property for maps to an R-algebra A with $a^2 0 \quad \forall a \in A$: given an R-algebra A and $f : M \to A$ R-module homo.,

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, hook] & A \\ T(M) \arrow[r] \arrow[ur, "\exists! f'"] & \Lambda(M) \arrow[u] \end{tikzcd}$$

- $\Lambda : \mathfrak{M}_R \to \mathfrak{Gr}_R$ is a covariant functor.
  - $\varphi : M \to N$: R-module homo. $\rightsquigarrow T(\varphi) : T(M) \to T(N) \to T(N)/A(N) = \Lambda(N)$

Ex 2.3.2. Let V be a vector space over F with $\dim V = n$ and $\varphi : V \to V$ be a linear transformation.

(1) Compute $\Lambda^k(V)$.

(2) Determine the map $\Lambda^k(\varphi) : \Lambda^k(V) \to \Lambda^k(V)$.

Symmetrization and Skew-symmetrization

$$T^k(V) \longrightarrow T^k(V)$$

$$\mathrm{Sym} = \sigma : x_1 \otimes \ldots \otimes x_k \longmapsto \frac{1}{k!} \sum_{\tau \in S_k} x_{\tau(1)} \otimes \ldots \otimes x_{\tau(k)}$$

$$\mathrm{Alt} = \sigma' : x_1 \otimes \ldots \otimes x_k \longmapsto \frac{1}{k!} \sum_{\tau \in S_k} \mathrm{sgn}(\tau) x_{\tau(1)} \otimes \ldots \otimes x_{\tau(k)}$$

$\tilde{S}^k(V) = \sigma(T^k(V)) \quad \tilde{\Lambda}^k(V) = \sigma'(T^k(V))$

- $\sigma^2 = \sigma$ easy $\rightsquigarrow T^k(V) = \operatorname{Im} \sigma \oplus \ker \sigma = \tilde{S}^k(V) \oplus \ker \sigma$.
- $\ker \sigma = C^k(V)$. $C^k(V) \subseteq \ker \sigma$ is obvious. Assume $\supsetneq$, i.e., $\exists t \in \ker \sigma$ s.t. $t \notin C^k(V)$. Recall $q : T^k(V) \twoheadrightarrow S^k(V)$, since q is the quotient map. Also $q|_{\tilde{S}^k(V)} \twoheadrightarrow S^k(V)$, since if $q(x) = y$, then it could be easily checked that $q(\sigma(x)) = y$, so exists $t' \in \tilde{S}^k(V)$ satisfies $q(t') = q(t) \neq 0$. But then $q(t - t') = 0 \implies t - t' \in \ker q = C^k(V) \subseteq \ker \sigma$ and because of $\sigma(t) = 0 \implies \sigma(t') = 0$. Hence $t' \in \ker \sigma$. But then $t' \in S^k(V) \subseteq \operatorname{Im} \sigma \implies t' \in \operatorname{Im} \sigma \cap \ker \sigma$, which leads to an contradiction since σ is a projection.

Ex 2.3.3. $T^k(V) = \tilde{\Lambda}^k(V) \oplus A^k(V)$.

3 Introduction to the linear representation theory of finite groups

3.1 Week 14

3.1.1 Generatlities on linear representations

Notation

- G: finite group
- V: vector space of finite dim over $\mathbb{C}$
- $\mathrm{GL}(V)$: the group of all linear isom. $V \to V$

Def 57. A group homo. $\rho : G \to \mathrm{GL}(V)$ is called a linear representation of G. $\dim V$ is called the dgree of ρ. (V is a representation space)
For a fixed basis $\beta = \{ e_i \}$,

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[dr, "R"'] & \mathrm{GL}(V) \arrow[d, "\beta", "\wr"'] \\ & \mathrm{GL}_n(\mathbb{C}) \end{tikzcd}$$

(R is a matrix representation)

Eg 3.1.1. A representation of degree 1 of G is $\rho : G \to \mathrm{GL}(\mathbb{C}) \cong \mathbb{C}^*$.
$\mathrm{ord}(g)$ is finite $\rightsquigarrow \rho(g)^m = 1$ for some $m \in \mathbb{N} \rightsquigarrow \rho(g)$ is a root of unity, i.e. $|\rho(g)| = 1$.
Note: So, $\rho : G \to S^1$, S^1 is the unit circle.

1. $G = \mathbb{Z}/p\mathbb{Z}$, $\rho : \overline{1} :: G \mapsto s_p :: S^1$ with $s_p^p = 1$.
2. $G = S_3, V = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3$.
   A permutation representation is $\rho : \tau :: S_3 \mapsto (\rho(\tau) : e_i \mapsto e_{\tau(i)}) :: \mathrm{GL}(V)$.
3. $G = S_3, V = \bigoplus_{\sigma \in S_3} \mathbb{C}e_\sigma$. The regular representation is

$$\rho^{\mathrm{reg}} : \tau :: G \mapsto (\rho^{\mathrm{reg}}(\tau) : e_\sigma \mapsto e_{\tau\sigma}) :: \mathrm{GL}(V).$$

For general G, with $V = \bigoplus_{g \in G} \mathbb{C}e_g$,

$$\rho^{\mathrm{reg}} : h :: G \mapsto (\rho^{\mathrm{reg}}(h) : e_g \mapsto e_{hg}) :: \mathrm{GL}(V).$$

Def 58.

- $\rho : g :: G \mapsto \mathrm{id} :: \mathrm{GL}(V)$: trivial representation.
- $\rho : G \hookrightarrow \mathrm{GL}(V)$: faithful representation.
- ρ, ρ' are said to be equivalent if $\exists$ a linear isom. $T : V \xrightarrow{\sim} V'$ s.t.

Remark 13. When we choose two bases β, β' for V,

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[dr, "R"'] & \mathrm{GL}(V) \arrow[d, "\beta", "\wr"'] \\ & \mathrm{GL}_n(\mathbb{C}) \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r, "\rho'"] \arrow[dr, "R"'] & \mathrm{GL}(V) \arrow[d, "\beta'", "\wr"'] \\ & \mathrm{GL}_n(\mathbb{C}) \end{tikzcd}$$

then ρ, ρ' are equivalent.

Let $T : e_i :: V \mapsto e_i' :: V$. For $g \in G, R(g) = \big(a_{ij}\big)$.
$T \circ \rho(g) = \rho'(g) \circ T$

Def 59. Let $\langle \cdot, \cdot \rangle$ be a positive definite Hermitian form on V.
Then $T : V \to V$ is called a unitary operator if $\langle T(x), T(y) \rangle = \langle x, y \rangle \quad \forall x, y \in V$.
or $\forall \beta$: orthonormal basis, $[T]_\beta^*[T]_\beta = [T]_\beta[T]_\beta^* = I_n$.

Theorem 29. $\forall \rho : G \to \mathrm{GL}(V)$, $\exists$ a matrix representation $R : G \to U_n$.

Proof. We only need to G-invariant positive definite Hermitian form on V. ($\forall g \in G, \langle \rho(g)x, \rho(g)y \rangle = \langle x, y \rangle \quad \forall x, y \in V$)
We start with an arbitrary positive definite Hermitian form $\langle \cdot, \cdot \rangle'$ on V.
Define a new form $\langle \cdot, \cdot \rangle$ by

$$\langle x, y \rangle := \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)(x), \rho(g)(y) \rangle'$$

which is a positive definite Hermitian form. (easy to check) $\square$

Def 60. Let $\rho : G \to \mathrm{GL}(V)$, For $W \subset V$ (we use $\subset$ to denote subspace), if $\forall x \in W$, $\rho(g)(x) \in W, \forall g \in G$, then W is said to be G-invariant and

$$\begin{aligned} \rho^W : G &\to \mathrm{GL}(W) \\ g &\mapsto \rho(g)\big|_W \end{aligned}$$

is called a subrepresentation of ρ.

W is G-invariant $\rightsquigarrow \rho(g)\big|_W : W \xrightarrow{\sim} W$.

Eg 3.1.2. Let ρ be the regular rep. of S_3.
$W^\circ = \{\, \alpha_1 e_1 + \cdots + \alpha_6 e_6 \mid \alpha_1 + \cdots + \alpha_6 = 0 \,\}$ is G-invariant.
$W^1 = \langle e_1 + \cdots + e_6 \rangle_{\mathbb{C}}$ is G-invariant.

Theorem 30. Let $\rho : G \to \mathrm{GL}(V)$ and $W \subset V$ be G-invariant. Then $\exists W^\circ \subset V$ is still G-invariant and $V = W \oplus W^\circ$.

Proof. We can pick an arbitrary W' with $V = W \oplus W'$ and $\pi_1 : V \to W$ is the projection to W. Then $W' = \ker \pi_1$.
Now we need π_1 preserves the G action (G-equivariant). Define

$$\pi^\circ = \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} \circ \pi_1 \circ \rho(g) : V \to W$$

- well-defined: $\rho(g)(V) \subset V \rightsquigarrow \pi_1 \circ \rho(g)(V) \subset W \rightsquigarrow \rho(g)^{-1} \circ \pi_1 \circ \rho(g)(V) \subseteq W$.
- surjective: $\forall y \in W, \rho(g)^{-1} \circ \pi_1 \circ \rho(g)(y) = y$ since $\rho(g)(y) \in W$. Also, $(\pi^\circ)^2 = \pi^\circ$. So $V = \operatorname{Im} \pi^\circ \oplus \ker \pi^\circ$.
- G-equivariant: $\forall g' \in G$,

$$\begin{aligned} \pi^\circ \circ \rho(g')(x) &= \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} \circ \pi_1 \circ \rho(g)(\rho(g')(x)) \\ &= \rho(g') \frac{1}{|G|} \sum_{gg' \in G} \rho(gg')^{-1} \circ \pi_1 \circ \rho(gg')(x) \\ &= \rho(g') \circ \pi^\circ(x) \end{aligned}$$

- $W^\circ :== \ker \pi^\circ$ is G-invariant: $\forall x \in W^\circ$, $\pi^\circ(\rho(g)(x)) = \rho(g)(\pi^\circ(x)) = \rho(g)(0) = 0$. So $\rho(g)(x) \in W^\circ$.

$\square$

Remark 14. If $W \subset V$ is G-invariant, then $W^\perp$ is also G-invariant. (w.r.t. a G-invariant positive definite Hermitian form)

Def 61. $\rho : G \to \mathrm{GL}(V)$ is irreducible if ρ has no proper notrivial subrepresentations.

Theorem 31. Each $\rho : G \to \mathrm{GL}(V)$ is a direct sum of irreducible subrepresentations.

Proof. By induction on $\dim V$. For $\dim V = 1$, then ρ is irr.
For $\dim V > 1$, if ρ is irr., then done. Otherwise, $\exists W, W^\circ$ are G-invariant s.t. $V = W \oplus W^\circ$ with $\dim W \geq 1, \dim W^\circ \geq 1$. By induction hypothesis, ρ^W, ρ^{W° are direct sum of irr. subrep., and $\rho = \rho^W \oplus \rho^{W^\circ}$, done. $\square$

Remark 15. Let $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(V')$.

- $\rho \oplus \rho' : G \to \mathrm{GL}(V \oplus V')$.
- $\rho \otimes \rho' : G \to \mathrm{GL}(V \otimes V')$. $(\sum_{i,j} r_i p, r'_{jq}(e_i \otimes e'_j))$

3.1.2 Character Theory 1

1. $\chi_\rho(1) = n$.
2. χ_ρ is a class function, i.e., it is constant on each conjugacy class.
3. $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$: Assume that the eigenvalues of $R(g)$ are $\lambda_1, \ldots, \lambda_n$. Then the eigenvalues of $R(g^{-1})$ are $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$.
$$0 = \det(\lambda I_n - A) = \det(\lambda I_n(A^{-1} - \lambda^{-1} I_n)A) = \det(\lambda I_n)\det(A^{-1} - \lambda^{-1} I_n)\det(A)$$
So $\det(A^{-1} - \lambda^{-1} I_n) = 0$. Then
4. $\chi_{\rho\oplus\rho'} = \chi_\rho + \chi_{\rho'}$.
5. $\chi_{\rho\otimes\rho'} = \chi_\rho \chi_{\rho'}$.

Def 62. $\mathcal{C}(G, \mathbb{C})$ is the vector space of complex functions on G.
$\chi_\rho \in \mathcal{C}(G) \subset \mathcal{C}(G, \mathbb{C})$ is the vector space of complex class functions of G.

Remark 16. Assume that $\{C_1, \ldots, C_k\}$ is the set of distinct conjugacy classes in G. Then $\{ f_i(C_j) = \delta_{ij} \mid \forall i = 1, \ldots, k \}$ forms a basis for $\mathcal{C}(G)$ over $\mathbb{C}$.

- $\forall f \in \mathcal{C}(G)$, let $f(C_i) = a_i$, then $f = \sum a_i f_i$.
- $\sum a_i f_i = 0$, pick $x_j \in C_j$, then $(\sum a_i f_i)(x_j) = a_j = 0 \quad \forall j = 1, \ldots k$.

So $\dim \mathcal{C}(G) = k$.

Def 63. $\phi, \psi \in \mathcal{C}(G, \mathbb{C})$, then
$$\langle \phi, \psi \rangle := \sum_{g \in G} \phi(g)\overline{\psi(g)}$$
is a positive definite Hermitian form on $\mathcal{C}(G, \mathbb{C})$.

Theorem 32 (Main theorem)**.** The set of all irr. characters of G forms an orthonormal basis for $\mathcal{C}(G)$ over $\mathbb{C}$. So there are only k irr. rep. up to equivalent.

Lemma 3 (Schur's lemma)**.** Let $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(V')$ be two irr. rep. of G.

Then

1. ρ, ρ' are not equivalent $\implies \mathsf{T} = 0$.
2. $V = V', \rho = \rho' \implies \mathsf{T} = \lambda 1_V$ for some $\lambda \in \mathbb{C}$.

Proof. 1. Assume $\mathsf{T} \neq 0$. Since T is G-equivariant, $\ker \mathsf{T} \leq V$ and $\operatorname{Im} \mathsf{T} \leq V'$ are G-invariant.
ρ is irr $\rightsquigarrow \ker \mathsf{T} = 0$ or V.
ρ' is irr $\rightsquigarrow \operatorname{Im} \mathsf{T} = 0$ or V.
T is an isom.
ρ, ρ' are equivalent.

2. Let λ be an eigenvalue of T, say $\mathsf{T}(v) = \lambda v$ with $v \neq 0$ in V. Put $\mathsf{T}' - \mathsf{T} - \lambda 1_V$.
Also, since $\rho(g0$ is $\mathbb{C}$-linear.
So T' is also G-equivariant. But $v \in \ker \mathsf{T}'$, i.e. T' is not 1-1. By 1., $\mathsf{T}' = 0$.

□

Coro 3.1.1. ρ, ρ' as above. Let $\mathsf{L} : V \to V'$ be a linear transformation. Define

$$\mathsf{T} = \frac{1}{|G|} \sum_{g \in G} \rho'(g)^{-1} \mathsf{L} \rho(g)$$

is G-equivariant. Then

1. ρ, ρ' are not equivalent $\implies \mathsf{T} = 0$.
2. $V = V', \rho = \rho' \implies \mathsf{T} = \lambda 1_V, \lambda \frac{\mathrm{trace}(\mathsf{L})}{\dim V}$.

Remark 17. Let $\rho \to_\beta R : G \to \mathrm{GL}_n(\mathbb{C})$ and $R(g) = (r_{ij}(g))$
$\rho' \to_{\beta'} R' : G \to \mathrm{GL}_{n'}(\mathbb{C})$ and $R'(g) = (r'_{ij}(g))$
Let $\mathsf{L}..... > [\mathsf{L}]_\beta^{\beta'} = (x_{\mu\nu} \in M_{n' \times n}(\mathbb{C})$
Then $\mathsf{T}... > [\mathsf{T}]_\beta^{\beta'} = (x_{tl}^0)$ with

$$x_{tl}^0 = \frac{1}{|G|} \sum_{\substack{g \in G \\ i=1,\dots,n \\ j=1,\dots,n'}} r'_{tj}(g^{-1}) x_{ji} r_{il}(g)$$

In case 1. of coro, $x_{tl}^0 = 0 \quad \forall t, l$.
In case 2. of coro, $\mathsf{T} = \lambda 1_V$, i.e. $x_{tl}^0 = \lambda \delta_{tl}$. $\lambda = \frac{\mathrm{trace}(\mathsf{L})}{n} = \frac{1}{n} \sum_{i=1}^n x_{ii} = \frac{1}{n} \sum_{i,j} \delta_{ji} x_{ji}$
Hence,

$$\frac{1}{|G|} \sum_{g \in G} r_{tj}(g^{-1}) r_{il}(g) = \frac{1}{n} \delta_{ji} \delta_{tl}$$

Prop 3.1.1.

1. If χ_ρ is irr., then $\langle \chi_\rho, \chi \rangle_{=1}$.
2. If two irr. rep. ρ, ρ' are not equivalent, then $\langle \chi_\rho, \chi_{\rho'} \rangle = 0$.

Proof. 1.

2.

□

OMIMI above

Remark 18. $\langle \chi_\rho, \chi_\rho \rangle = 1 \implies \rho$ is irr.

Proof. We write $\rho = \rho_1^{\oplus m_1} \oplus \cdots \oplus \rho^{\oplus m_l}$ where $\rho_1, \ldots, \rho_l$ are non-equivalent irr. rep.

$$\chi_\rho = \sum_{i=1}^{l} m_i \chi_{\rho_i}$$

$$1 = \langle \chi_\rho, \chi_\rho \rangle = \sum_{i=1}^{l} m_i^2 \implies \exists m_i = 1 \text{ and } m_j = 0 \text{ for } j \neq i$$

So $\rho \cong \rho_i$. $\square$