Algebra

May 22, 2017

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

$\square$

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

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

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

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

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

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

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

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

1.2 Week 2

1.2.1 Permutation groups and Dihedral groups

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

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

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

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

(Hint): Let G be a group. Set $B = G$. Consider $a \in G$ as $\sigma_a : G \to G, x \mapsto ax$. 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 $\square$

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

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

Eg 1.2.1. In S_7, $\sigma_1 = (1\ 2\ 3)(4\ 5\ 6)(7), \sigma_2 = (1\ 3\ 5\ 6)(2\ 4\ 7)$.

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

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

Eg 1.2.2. $(1\ 2\ 3) = (1\ 3)(1\ 2), (1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$.

Any permutation is a product of 2 cycles.

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

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

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

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

Case 2: Otherwise, CONCON

$\square$

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

Proof. $(1\ i)^{-1} = (1\ i)$ and $(i\ j) = (1\ i)(1\ j)(1\ i)^{-1}$. $\square$

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

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

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

略... (這邊討論旋轉和反射的矩陣)

<u>Case 1</u>: $A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ is counterclockwise roration w.r.t. α.

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

Easy to show that $\mathrm{L}_A(v) = v - 2\langle v, v_2 \rangle v_2$.

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

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. $\begin{cases} \mathrm{T}\big|_W = -\mathrm{id}_W \\ \mathrm{T}\big|_{W^\perp} = \mathrm{id}_{W^\perp} \end{cases}$

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

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

Ex 1.2.3.

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

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

1.2.2 Cyclic groups and internal direct product

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

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

Eg 1.2.5. Let $A = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \in \mathrm{SO}(2)$. 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. $\overline{i} \times \overline{j} = \overline{i \times j}$.

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

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

Eg 1.2.7. 略... 簡化剩餘系, 原根 (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 $\mathrm{ord}(a) = n$.
- 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 $\mathrm{ord}(a) = n$. 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 $r = 0 \implies n \mid m$. $\square$

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

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

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

$\square$

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

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

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

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

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

$\square$

Ex 1.2.4.

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

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

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

Ex 1.2.5. Show Prop 1.2.4.

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

Remark 4. In this case, we find that

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

Ex 1.2.6. TFAE

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

Eg 1.2.8.

1. $G = \mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}, G_1 = \{\overline{0}, \overline{3}\}, G_2 = \{\overline{0}, \overline{2}, \overline{4}\}$. 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. $G = S_3, G_1 = \langle (1\ \ 2) \rangle, G_2 = \langle (2\ \ 3) \rangle, G_1G_2 = \{1, (1\ \ 2), (2\ \ 3), (1\ \ 2\ \ 3)\} \nleq G$ since $(1\ 3\ 2) = (1\ 2\ 3)^{-1} \notin G_1G_2$.

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

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

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

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

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

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

Ques: How to make $\{ aH : a \in G \}$ to be a group? For aH, bH, we must have $(aH)(bH) = abH$.

In general, $(aH)(bH) = abH$ is not well-defined.

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

If we hope $a_1b_1H = a_2b_2H$, then we need $(a_1b_1)^{-1}a_2b_2 \in H$.

$$b_1^{-1}a_1^{-1}a_2b_2 = b_1^{-1}b_2b_2^{-1}a_1^{-1}a_2b_2$$

Notice that $b_1^{-1}b_2, a_1^{-1}a_2 \in H$, so we need $b_2^{-1}a_1^{-1}a_2b_2 \in H$.

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

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

Ques: How to find a normal subgroup of G?

Prop 1.3.1.

1. If G is abelian, then $\forall\, H \leq G \rightsquigarrow H \lhd G$. (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 $x_1x_2 = a^{k_1+k_2}z_1z_2 = x_2x_1$. ($z_i$ 可以各種交換) □

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

Prop 1.3.3. $[G, G] \lhd G$; $[G, G] = 1 \iff G$ 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: $\mathrm{PSL}(2,\mathbb{C}) = H/H\cap K$.

齊次座標...OTL

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 $\forall\, K\le G$, either (1) $K\le H$ 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 $\{\, H\le G \mid K\le H \,\}$ and $\{$subgroups of $G/K\}$. ($H\lhd G$ ... normal)

   Proof. Define $\varphi : H\mapsto H/K$. ($H/K\le G/K$)

   - 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. $aK = bK \implies b^{-1}a\in K\le H_2 \implies a\in bH_2 = H_2$. So $H_1\le H_2$. By symmetry, $H_2\le H_1$, and thus $H_1 = H_2$.
   - onto: Given a subgroup Q of G/K, consider $H = q^{-1}(Q)$ where $q: G\to G/K$.
     - $H\le G$: $\forall\, a,b\in H, q(a),q(b)\in Q \implies q(a)q(b)^{-1}\in Q \implies q(ab^{-1})\in Q \implies ab^{-1}\in H \implies H\le G$.
     - $K\le H$: $\forall\, a\in K, q(a) = aK = K\in Q \implies a\in H \implies K\le H$.
     - $Q = H/K$: $\forall\, aK\in Q, aK = q(a) \implies a\in H \implies aK\in H/K \implies Q\subseteq H/K$. And $\forall\, aK\in H/K (a\in H), q(a)\in Q \implies H/K\subseteq Q$. So $Q = H/K$.
   - $H\lhd G, K\le H \iff \forall\, g\in G, gHg^{-1} = H, K\le H \iff \forall\,\overline{g}\in G/K, \overline{g}(H/K)\overline{g}^{-1} = H/K \iff H/K\lhd G/K$. □

2. If $H\lhd G$ with $K\le H$, 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. $m\mathbb{Z}+n\mathbb{Z}/m\mathbb{Z}\cong n\mathbb{Z}/m\mathbb{Z}\cap n\mathbb{Z}$. ($m\mathbb{Z}+n\mathbb{Z} = \gcd(m,n)\mathbb{Z}, m\mathbb{Z}\cap n\mathbb{Z} = \mathrm{lcm}(m,n)\mathbb{Z}$)

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

Eg 1.3.9. Q_8 and D_4 交給陳力

Extension problem: given two groups A,B, how to find G and $K\lhd G$, s.t. $K\cong A, G/K\cong B$? ($1\to H\to G\to G/H\to 1$, short exact sequence)

(e.g. $G = A\times B, K = A\times\{1\}$)

1.4 Week 4

1.4.1 Universal property and direct sum & product

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

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

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

Def 22. Given a non-empty family of abelian groups $\{ G_s \mid s \in \Lambda \}$, a (external) direct sum of $\{ G_s \mid s \in \Lambda \}$ is an abelian group $\bigoplus_{s\in\Lambda} G_s$ with the embedding mappings $i_{s_0} : G_{s_0} \to \bigoplus_{s\in\Lambda} G_s, \forall\, s_0 \in \Lambda$ 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. 又一個ㄜ圖

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

Proof. Existence: $\bigoplus_{s\in\Lambda} G_s = \{ (g_s)_{s\in\Lambda} \mid g_s \in G_s,$ almost all of the g_s' 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: $(g_s)_{s\in\Lambda} + (g'_s)_{s\in\Lambda} := (g_s + g'_s)_{s\in\Lambda} \in \bigoplus_{s\in\Lambda} G_s$. 這邊也一個ㄜ圖

Uniqueness: Assume $\exists$ another G satisfies the universal property, 一個大ㄜ圖 ($G, \bigoplus_{s\in\Lambda} G_s$ 互相有唯一個映射可以 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. 又一個ㄜ圖

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: 這邊也一個ㄜ圖 which is uniquely defined.

Uniqueness: Assume $\exists$ another G satisfies the universal property, 一個大ㄜ圖 ($G, \prod_{s\in\Lambda} G_s$ 互相有唯一個映射可以 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.

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

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

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

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

Inverse limit:

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

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)

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

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

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

Eg 1.4.3. $\mathbb{Z}\left[\sqrt{2}\right] = \left\{ a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Z} \right\} \subset \mathbb{R}$.

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.

Fact:

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

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

Prop 1.4.1. TFAE

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

easy to prove.

Def 26.

- $f : R_1 \to R_2$ 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. $\square$

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

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 $p \mid \binom{p}{1} \implies \binom{p}{i} a^{p-i} b^i = 0$. $\square$

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 $F \cong (\mathbb{Z}/p\mathbb{Z})^n \implies |F| = p^n$. $\square$

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 $G_x = \{\, g \mid gx = x \,\} \leq G$ 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: $g_1 x = g_2 x \iff g_2^{-1} g_1 x = x \iff g_2^{-1} g_1 \in G_x \iff g_2^{-1} g_1 G_x = G_x \iff g_1 G_x = g_2 G_x$.
- onto: $\forall\, g \in G, \psi(gx) = gG_x$. □

1.5.2 Action by left multiplication

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

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

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

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

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

Proof. Let $X = \{a_1 H, \ldots, a_p H\}$ (all left coests of H) and $\varphi : G \to S_p$ be the associated group homo. for the group action $(g, a_i H) \mapsto g a_i H$.

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

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

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

If $|G/\ker \varphi| = 1 \implies G = \ker \varphi \leq H \lneq G$, 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

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

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

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

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

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

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

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

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

- For $H \lhd G$, define $G \times H \to H \quad (g, h) \mapsto ghg^{-1}$ with the group homo. $\varphi : G \to \mathrm{Aut}(H)$.

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

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

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

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

1.6 Week 6

1.6.1 Group actions II

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

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

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

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

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. □

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

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) □

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, $\forall\, 0 \le k \le n-1, \exists\, \overline{G_k} \lhd G/\langle a\rangle$ 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

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

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

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

(This is well-defined since $ab = 1 \implies ba = 1$ in a group.) We find that $(a_1, \ldots, a_p) \in \operatorname{Fix} \mathbb{Z}/p\mathbb{Z} \iff a_1 = a_2 \ldots a_p$. 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 $(1, \ldots, 1) \in \operatorname{Fix} \mathbb{Z}/p\mathbb{Z}, |\mathbb{Z}/p\mathbb{Z}| \neq 0 \implies |\mathbb{Z}/p\mathbb{Z}| \ge p$.

So $\exists\, (a, \ldots, a) \in \operatorname{Fix} \mathbb{Z}/p\mathbb{Z} \implies a^p = 1$.

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

So,

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

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

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

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

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

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

So φ is a group homo.

Now if $\ker \varphi = G$ $(\forall\, a \in G, a^p = 1)$, i.e. φ is trivial, then φ is useless. Else, $\exists\, a \in G$ s.t. $\operatorname{ord}(a) = p^2$, then $H = \langle a\rangle \lhd G$. ($[G : H] = p$ 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. $K \lhd G, H \lhd G, K \cap H = \{1\} \implies KH = K \times H$
$(\forall\, k \in K, h \in H, khk^{-1}h^{-1} \in H \cap K = \{1\}, \implies kh = hk)$

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

Observation 1. $K \le G, H \lhd G, K \cap H = \{1\}$ (K 慘 H 好，簡稱慘好集)
$\implies$ elements in KH has unique representation ? 好事喔
$KH \iff K \times H$ 1-1 corresp, $(kh) \leftrightarrow (k, h)$

Group operation : $\forall\, k_1, k_2 \in K, h_1, h_2 \in H, (k_1h_1)(k_2h_2) = k_1k_2(k_2^{-1}h_1k_2)h_2$
Let $\tau : K \to \mathrm{Aut}(H), k \mapsto (\tau(k) : h \mapsto khk^{-1})$ (類似 $\in \mathrm{Inn}(H)$)

Def 35 (Semi-Direct Product (慘好積))**.** $K \times_\tau H = \{(k, h)|k \in K, h \in H\}$ with group operation : $(k_1, h_1)(k_2, h_2) = (k_1k_2, \tau(k_2^{-1})(h_1)(h_2))$ where $\tau : K \to \mathrm{Aut}(H)$ (need not to be inner homomorphism)

Properties:

- Associativity: Good, ex
- The identity $= (1, 1)$
- Inverse : $(k, h)^{-1} = (k^{-1}, \tau(k)(h^{-1}))$
- $K \cong K \times \{1\} \le K \times_\tau H$: $(k_1, 1)(k_2, 1) = (k_1k_2, \tau(k_2^{-1})(1)1) = (k_1k_2, 1) \in K \times \{1\}$
  $H \cong \{1\} \times H \le K \times \tau H : (1, h + 1), (1, h_2) = (1, \tau(1^{-1})(h_1)h_2) = (1, h_1h_2) \in \{1\} \times K$
- $H \lhd K \times_t H : (k, h)(1, h')(k, h)^{-1} = (k, hh')(k^{-1}, \tau(k)(h^{-1})) = (1, \tau(k)(hh')\tau(k)(h^{-1})) \in H$
- $\tau(k)(h) = khk^{-1}$: $(k, 1)(1, h)(k^{-1}, 1) = (k, h)(k^{-1}, 1) = (1, \tau(k)(h))$
- 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 : $\phi_k : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \bar{1} \mapsto \bar{k}$

$\phi_{k_2} \circ \phi_{k_1}(1) = \phi_{k_2}(\bar{k_1}) = \phi_{k_2}(1 + \cdots + 1) = \overline{k_2} + \cdots \overline{k_2} = \overline{k_1k_2}$

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 $\exists\, |Q| = p$, $P \ne Q$ 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 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ 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 $G_2, \ldots, G_n$ 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. $G = \mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle$.

- $G_1 = \langle \bar{2} \rangle, G_2 = \langle \bar{4} \rangle, G_3 = \langle \bar{0} \rangle \rightsquigarrow$ length(3), factors: C_2, C_2, C_3.
- $G_1' = \langle \bar{2} \rangle, G_2' = \langle \bar{6} \rangle, G_3' = \langle \bar{0} \rangle \rightsquigarrow$ length(3), factors: C_2, C_3, C_2.
- $G_1'' = \langle \bar{3} \rangle, G_2'' = \langle \bar{6} \rangle, G_3'' = \langle \bar{0} \rangle \rightsquigarrow$ 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: $C_p, \ldots, C_p$. (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 $K_{ji} = K_{j(i+1)}$. $\square$

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. $\square$

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,

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

$\square$

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 $n = p_1^{m_1}p_2^{m_2}\dots p_r^{m_r}$. $\square$

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

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. $(r_1 + r_2)x = r_1 x + r_2 x \quad r_1, r_2 \in R, x \in M$
3. $(r_1 r_2)x = r_1(r_2 x) \quad r_1, r_2 \in R, x \in M$
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.

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

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

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

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

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

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

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

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 $d = x_1 k_1 c + x_2 k_2 c = (x_1 k_1 + x_2 k_2) c \implies c \mid d$. □

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.

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

Proof. Define the length $l(a)$ of $a \neq 0$ to be r if $a = p_1 p_2 \dots p_r$ where $p_1, \dots, p_r$ are prime elements.

prime elements: $p \mid ab \implies p \mid a$ or $p \mid b$.

1. We may assume $a_{11} \neq 0$ and $l(a_{11}) \leq l(a_{ij}) \forall\, a_{ij} \neq 0$. (換一換就上去了...XD)
2. We may assume $\begin{cases} a_{11} \mid a_{1k} & \forall\, k = 2, \dots, m \\ a_{11} \mid a_{k1} & \forall\, k = 2, \dots, n \end{cases}$. If $a_{11} \nmid a_{1k}$, then we can interchange 2nd and kth columns to assume $a = a_{11} \nmid a_{12} = b$.

   Let $d = \gcd(a, b) \implies \begin{cases} l(d) < l(a) \\ d = ax + by \text{ for some } x, y \in R \end{cases} \implies 1 = \frac{a}{d}x + \frac{b}{d}y$. Write $b' = \frac{b}{d}, a' = -\frac{a}{d}$. Then
   $$\begin{pmatrix} -a' & b' \\ y & -x \end{pmatrix} \begin{pmatrix} x & b' \\ y & a' \end{pmatrix} = I_2$$
   反正就是移一下減掉，length 會一直變小 $\implies$ 這個操作會停.
3. 有這個 $\begin{cases} a_{11} \mid a_{1k} & \forall\, k = 2, \dots, m \\ a_{11} \mid a_{k1} & \forall\, k = 2, \dots, n \end{cases}$ 就可以全部消掉變成
   $$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{n2} & \dots & b_{nm} \end{pmatrix}$$
4. May assume $a_{11} \mid b_{kl} \quad \forall\, k, l$. 不是的話就把該 row 往第一 row 加上去，重複前面的操作，$l(a_{11})$ 總是變小，因此會停.
5. 遞迴下去...

最後就弄出想要的矩陣了. □

1.8 Week 8

1.8.1 Fundamental theorem of finitely generated abelian groups

Theorem 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, $R^n = \bigoplus Rw_i, \ker\varphi = \bigoplus d_i R w_i$ Hence

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

□

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

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 $G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_l\mathbb{Z} \oplus \mathbb{Z}^s, d_i \in \mathbb{Z}$ 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 $I_1 I_2 \dots I_n = I_1 \cap I_2 \cap \dots \cap I_n$.

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

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

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.

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

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. $\varphi(x_i) = (\overline{0}, \dots, \overline{1}, \overline{0}, \dots, \overline{0})$, 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. $\varphi(x) = (\overline{1}, \overline{0}, \dots, \overline{0})$.

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 $x \equiv 1 \pmod{I_1}$.

$\square$

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

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

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 $\iff$ $\mathrm{Exp}(G) = |G|$.

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 $X = \{$ 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 $\begin{array}{c} P\times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G) \\ (\ a, \qquad Q) \mapsto aQa^{-1} \end{array}$ where $P \in \mathrm{Syl}_p(G)$.

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

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

- Consider $\begin{array}{c} G\times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G) \\ (\ a, \qquad Q) \mapsto aQa^{-1} \end{array} \implies$ 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 $n_p = \frac{|G|}{|G_Q|} \mid |G|$. So $n_p \mid p^\alpha r \implies n_p \mid r$.

$\square$

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. 找兩個 normal subgroup (17, 5 or 3)
2. quot 掉後發現剩下的是 abelian $\rightsquigarrow [G, G]$ 在裡面
3. $[G, G] = 1$
4. 唱 f.g. xxx thm. 得到 $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17}$.
5. 中國剩飯定理 $G \cong C_{255}$.

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

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. $P \le Z_G$.

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. $bab^{-1} = a^2$: $a = a^2 a a^{-2} = b^2 a b^{-2} = a^4 \implies a^3 = 1$ 矛盾
      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 $\ker \phi \leq P$, $|P| = 3$ 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 $|\mathrm{Im}\,\phi \cap A_4| \geq 8$. But $|\mathrm{Im}\,\phi \cap A_4| \mid |A_4| = 12 \implies \mathrm{Im}\,\phi = A_4$

  $\square$

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 $y x_1^{\delta_1} x_2^{\delta_2} \cdots x_m^{\delta_m} = y y_1^{\epsilon_1} y_2^{\epsilon_2} \cdots y_m^{\epsilon_m}$. 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 $A = \langle\, \sigma_x : x \in X \,\rangle \leq S_{F(X)}$. 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 $G = \langle a_1, \ldots, a_n \rangle$ and $X = \{x_1, \ldots, x_m\}$. 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 $\langle\, x_1, \ldots, x_n \mid \text{elements of } R \,\rangle$, 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 $R = \{x^n, y^2, xyxy\} \subseteq \ker\phi \implies N(R) \leq \ker\phi$. By factor theorem, $\exists\, \bar{\phi} :: F(X)/N(R) \to D_n$. But notice that

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

since $xyxy = 1 \implies xy = yx^{-1}$, so every element could be turn into $x^i y^j$. 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 $[F(X), F(X)] \leq \ker\phi$. By factor theorem, 一個ㄈ圖.

Claim that $\bar{\phi}$ is 1-1.

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

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

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

Theorem 25. Let $\dim V = n$ and $\beta = \{v_1, \dots, v_n\}$ 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 $f \in B_F(V, V)$, $f(v, w) = \sum_i \sum_j a_i b_j f(v_i, v_j) = \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} \begin{pmatrix} & & \\ & f(v_i, v_j) & \\ & & \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

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 $n > 1$.

<u>Claim 1</u>: $\exists\, v_1 \in V$ s.t. $f(v_1, v_1) \neq 0$. Assume that $f(v, v) = 0 \quad \forall\, v \in V$.

$$f(v, w) = \frac{1}{2}\big(f(v + w, v + w) - f(v, v) - f(w, w)\big) = 0.$$ [1]

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 $W^\perp = \{\, w \in V \mid f(v_1, w) = 0 \,\} \subseteq V$.

<u>Claim 2</u>: $V = W \oplus W^\perp$

- $V = W + W^\perp$: 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 $\beta = \{v_1, \ldots, v_n\}$. $\square$

[1] The argument in class requires $\mathrm{char}\, F \geq 4$, omimi...

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 linearly independent, $c_i = 0$. Therefor these vectors are linear independent.

□

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 $M_1, \ldots, M_n, L$ be R-modules.

A function $F : M_1 \times \cdots \times M_n \to L$ is said to be n-multilinear if $\forall\, i$,

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

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

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

Universal property: $\forall\, (x, y) \in M \times N$, $\begin{matrix} R(x, y) \to W \\ r(x, y) \mapsto rf(x, y) \end{matrix}$. 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,

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

□

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

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

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

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

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 $\{R\text{-bilinear maps } M \times N \to L\} \leftrightarrow \mathrm{Hom}_R(M \otimes_R N, L)$.

Similarly,

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

Fact 2.2.1. $f \in \mathrm{Hom}_R(M, M'), g \in \mathrm{Hom}_R(N, N') \rightsquigarrow f \otimes g \in \mathrm{Hom}_R(M \otimes N, M' \otimes N')$ 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

$$\mathrm{Hom}_R\left(M \otimes_R N, U\right) \cong \mathrm{Hom}_R\left(N, \mathrm{Hom}_R(M, U)\right)$$

Proof.

- For $f \in \mathrm{Hom}_R(M \otimes_R N, U)$ 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... ☐

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 satisfying $\mathrm{im}\, f_k = \ker f_{k+1}$.

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

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, $\mathrm{Hom}_F(V,W) \cong \left\langle E_{ij} \middle| \begin{matrix} i = 1, \ldots, m \\ j = 1, \ldots, n \end{matrix} \right\rangle_F$. $V^* \otimes W \cong \left\langle e_j^* \otimes f_i \middle| \begin{matrix} i = 1, \ldots, m \\ j = 1, \ldots, n \end{matrix} \right\rangle_F$. ☐

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 $I = \bigoplus I \cap A_n$. [2]

[2] This is not mentioned in class

Ex 2.2.4. TFAE

(1) I is graded.

(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.

Observation: 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 $f : M_1 \times M_2 \times M_3 \to L$. (拆括號囉)
- By induction, $M_1 \otimes \cdots \otimes M_n$ is well-defined and satisfies the universal property. (n-multilinear map)

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 $\varphi = \psi \circ i$.

Construction:

- $\forall\, k \in \mathbb{N}$, $T^k(M) := \underbrace{M \otimes \cdots \otimes M}_{k \text{ times}}$, 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
  $$T(M) := \bigoplus_{k=0}^{\infty} T^k(M) = R \oplus T^1(M) \oplus \ldots$$

- 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 $f_k : M \times \cdots \times M \to A$
$$\begin{aligned} f_k : M \times \cdots \times M &\to A \\ (x_1, \ldots, x_k) &\mapsto \varphi(x_1) \ldots \varphi(x_k) \end{aligned}$$

f_k is k-multilinear $\rightsquigarrow$
$$\begin{aligned} \exists\,!\tilde{f_k} : M \otimes \cdots \otimes M &\to A \\ x_1 \otimes \cdots \otimes x_k &\mapsto \varphi(x_1) \ldots \varphi(x_k) \end{aligned}$$

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.,

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

- $S : \mathfrak{M}_R \to \mathfrak{Gr}_R$ 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 (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:

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

- $\Lambda(M)$ 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 ontradiction 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 degree 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 $\rho : G \to \mathrm{GL}(\mathbb{C}) \cong \mathbb{C}^\times$.

$\mathrm{ord}(g)$ 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. $G = \mathbb{Z}/p\mathbb{Z}$, $\rho : \overline{1} :: G \mapsto \zeta_p :: S^1$ with $\zeta_p^p = 1$.
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. $\mathsf{T} : V \xrightarrow{\sim} V'$ s.t.

$$\begin{tikzcd} V \arrow[r, "\sim", "\mathsf{T}"'] \arrow[d, "\rho(g)"'] & V' \arrow[d, "\rho'(g)"] \\ V \arrow[r, "\sim", "\mathsf{T}"'] & V' \end{tikzcd}$$

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, since

$$\begin{aligned} \langle \rho(g)x, \rho(g)y \rangle &\triangleq \frac{1}{|G|} \sum_{h \in G} \langle (\rho(h) \circ \rho(g))(x), (\rho(h) \circ \rho(g))(y) \rangle' \\ &= \frac{1}{|G|} \sum_{gh \triangleq h' \in G} \langle (\rho(h'))(x), (\rho(h'))(y) \rangle' \triangleq \langle x, y \rangle \end{aligned}$$

So with the basis of this hermitian form, every $\rho(g)$ has a matrix representation $R(g)$ which is unitary. $\square$

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: $\forall\, y \in W$, $\big(\rho(g)^{-1} \circ \pi_1 \circ \rho(g)\big)(y) = \big(\rho(g)^{-1} \circ \rho(g)\big)(y) = y$ since $\rho(g)(y) \in W$. Also, $\pi^\circ(y) = y, \forall\, y \in W \implies (\pi^\circ)^2 = \pi^\circ$. So π° is a projection and hence $V = \operatorname{Im} \pi^\circ \oplus \ker \pi^\circ$.
- G-equivariant: $\forall\, g' \in G$,

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

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

$$\begin{tikzcd}
V \arrow[r, "\pi^\circ"] \arrow[d, "\rho(g)"'] & W \arrow[d, "\rho(g)"] \\
V \arrow[r, "\pi^\circ"'] & W
\end{tikzcd}$$

□

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 irreducible.

For $\dim V > 1$, if ρ is irreducible, 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 the direct sum of irreducible subrepresentations, and $\rho = \rho^W \oplus \rho^{W^\circ}$, done. □

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

- $\rho \oplus \rho' : G \to \mathrm{GL}(V \oplus V')$. 矩陣是左上右下
- $\rho \otimes \rho' : G \to \mathrm{GL}(V \otimes V')$. 矩陣是密密麻麻 ($\sum_{i,j} r_{ip}, r'_{jq}(e_i \otimes e'_j)$)

3.1.2 Character Theory I

Main goal: To determine all equivalence classes of irreducible representations of a finite group G.

Def 62.

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

The character χ_ρ if ρ is the map $\chi_\rho : G \to \mathbb{C}$ defined by $\chi_\rho(g) = \operatorname{Tr}(R(g))$.

Remark 16.

1. χ_ρ is independent of the choice of $\beta = \{e_i\}$ For another basis $\beta' = \{e_i'\}$. (Notice that $\operatorname{Tr}(BA) = \operatorname{Tr}(AB)$)
2. $\rho \cong \rho' \rightsquigarrow \chi_\rho = \chi_{\rho'}$.
   equivalent

Def 63.

- The degree of χ_ρ is defined to the degree of ρ ($= \dim V$).
- χ_ρ is an irreducible character if ρ is irreducible.

Basic facts:

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 $g^m = 1 \implies R(g)^m = I_n \implies |\lambda_i| = 1 \implies \lambda_i^{-1} = \overline{\lambda_i}$. Thus $\chi_\rho(g^{-1}) = \operatorname{Tr}(R(g)^{-1}) = \overline{\lambda_1 + \cdots + \lambda_n} = \overline{\chi_\rho(g)}$.
4. $\chi_{\rho \oplus \rho'} = \chi_\rho + \chi_{\rho'}$.
5. $\chi_{\rho \otimes \rho'} = \chi_\rho \chi_{\rho'}$.

Def 64. $\mathcal{C}(G, \mathbb{C})$ 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 17. 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 65. $\phi, \psi \in \mathcal{C}(G, \mathbb{C})$, then
$$\langle \phi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}$$
is a positive definite Hermitian form on $\mathcal{C}(G, \mathbb{C})$.

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

$$\begin{tikzcd} V \arrow[r, "\mathsf{T}"'] \arrow[d, "\rho(g)"'] & V' \arrow[d, "\rho'(g)"] \\ V \arrow[r, "\mathsf{T}"'] & V' \end{tikzcd} \qquad (\mathsf{T} : G\text{-equivariant})$$

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 $\mathsf{T} \neq 0$. We only needs to prove that T is an isomorphism, and then ρ, ρ' would be isomorphic by definition. Since T is G-equivariant, $\ker \mathsf{T} \leq V$ and $\operatorname{Im} \mathsf{T} \leq V'$ are G-invariant.

   ρ is irreducible $\implies \ker \mathsf{T} = 0$ or V, but if $\ker \mathsf{T} = V$ then $\mathsf{T} = 0$, so $\ker \mathsf{T} = 0$.

   Similarly, ρ' is irreducible $\implies \operatorname{Im} \mathsf{T} = 0$ or V. And by the fact that $\mathsf{T} \neq 0$, $\operatorname{Im} \mathsf{T} = V$.

   Thus T is an isom, and consequently ρ, ρ' are equivalent.
2. Since the vector field is over $\mathbb{C}$, T has an eigenvalue. Let λ be an eigenvalue of T, say $\mathsf{T}(v) = \lambda v$ with $v \neq 0$ in V. Put $\mathsf{T}' = \mathsf{T} - \lambda 1_V$. Then

   $$\rho(g) \circ \mathsf{T}' = \rho(g) \circ (\mathsf{T} - \lambda 1_V) \overset{*}{=} \rho(g) \circ \mathsf{T} - \rho(g) \circ \lambda 1_V = \mathsf{T} \circ \rho(g) - \lambda 1_V \rho(g) = \mathsf{T}' \rho(g)$$

   Which * is due to the linearity of $\rho(g)$. Hence T' is also G-equivariant.

   But $v \in \ker \mathsf{T}'$, i.e., T' is not 1-1. Similar as in 1., $\ker \mathsf{T}' = \{0\}$ or $V \implies \ker \mathsf{T}' = V \implies \mathsf{T}' = 0 \implies T = \lambda 1_V$.

$\square$

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

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

One could easily checks that T is G-equivariant (i.e., $\mathsf{T} \circ \rho(g) = \rho'(g) \circ \mathsf{T}$). Then

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

Remark 18. Let $\rho \to_\beta R : G \to \mathrm{GL}_n(\mathbb{C})$ and $R(g) = \left[r_{ij}(g)\right]$

$\rho' \to_{\beta'} R' : G \to \mathrm{GL}_{n'}(\mathbb{C})$ and $R'(g) = \left[r'_{ij}(g)\right]$

and let the matrix representation of L is $[\mathsf{L}]_\beta^{\beta'} = \left[x_{\mu\nu}\right] \in M_{n' \times n}(\mathbb{C})$

Then consider the matrix representation of T, which is $[\mathsf{T}]_\beta^{\beta'} = \left[x^\circ_{tl}\right]$ with

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

In case 1., $x^\circ_{tl} = 0, \forall\, t, l$. Since it hold for every L, which is independent of ρ, ρ', fixing i, j and setting $x_{ij} = 1$ and 0 otherwise, we gets

$$\frac{1}{|G|} \sum_{g \in G} r'_{tj}(g^{-1}) r_{il}(g) = 0, \quad \forall\, i, j, t, l$$

In case 2., $\mathsf{T} = \lambda 1_V$, i.e. $x^\circ_{tl} = \lambda \delta_{tl}$. $\lambda = \frac{\operatorname{Tr}(\mathsf{L})}{n} = \frac{1}{n} \sum_{i=1}^n x_{ii} = \frac{1}{n} \sum_{i,j} \delta_{ji} x_{ji}$

Hence,

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

But notice that this equality hold for any L, which is independent of ρ, ρ'. So if we fix i, j and set $x_{ji} = 1$, and $x_{j'i'} = 0$ otherwise, we get

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

Prop 3.1.1.

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

Proof.

1. Let $R(g) = \left[r_{ij}(g) \right]$ be the matrix representation of $\rho(g)$. Then

$$\begin{aligned} \langle \chi_\rho, \chi_\rho \rangle &\triangleq \frac{1}{|G|} \sum_g \chi_\rho(g) \overline{\chi_\rho(g)} = \frac{1}{|G|} \sum_g \chi_\rho(g) \chi_\rho(g^{-1}) \\ &= \frac{1}{|G|} \sum_g \sum_{i,j} r_{ii}(g) r_{jj}(g^{-1}) = \sum_{i,j} \frac{1}{n} \delta_{ij} \delta_{ij} = 1 \end{aligned}$$

2. Let $R(g) = \left[r_{ij}(g) \right], R'(g) = \left[r'_{ij}(g) \right]$ be the matrix representation of $\rho(g), \rho'(g)$. Then

$$\begin{aligned} \langle \chi_\rho, \chi_{\rho'} \rangle &\triangleq \frac{1}{|G|} \sum_g \chi_\rho(g) \overline{\chi'_\rho(g)} = \frac{1}{|G|} \sum_g \chi_\rho(g) \chi_\rho(g^{-1}) \\ &= \frac{1}{|G|} \sum_g \sum_{i,j} r_{ii}(g) r'_{jj}(g^{-1}) = 0 \end{aligned}$$

□

Remark 19. $\langle \chi_\rho, \chi_\rho \rangle = 1 \implies \rho$ 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 $\rho \cong \rho_i$. □

3.2 Week 15

3.2.1 Character Theory II

Prop 3.2.1. Let $\rho : G \to \mathrm{GL}(V)$ and $\rho = \rho^{W_1} \oplus \cdots \oplus \rho^{W_k}$ where $\rho_i = \rho^{W_i}$ is irr. $\forall\, i$. ($V \cong W_1 \oplus \cdots \oplus W_k$)
If $\tilde{\rho} : G \to \mathrm{GL}(\tilde{W})$ is an irr. rep. then the number of ρ_i isomorphic to $\tilde{\rho}$ is equal to $\langle \chi_\rho, \chi_{\tilde{\rho}} \rangle$.

Proof. We know $\chi_\rho = \chi_{\rho_1} + \cdots + \chi_{\rho_k}$, so

$$\langle \chi_\rho, \chi_{\tilde{\rho}} \rangle = \sum_{i=1}^{k} \langle \chi_{\rho_i}, \chi_{\tilde{\rho}} \rangle$$

Recall $\rho_i \cong \tilde{\rho} \implies \langle \chi_{\rho_i}, \chi_{\tilde{\rho}} \rangle = 1$, otherwise $\langle \chi_{\rho_i}, \chi_{\tilde{\rho}} \rangle = 0$. □

Remark 20.

1. The number of W_i isomorphic to $\tilde{W}$ does not depend on the chosen decomposition. ($= \langle \chi_\rho, \chi_{\tilde{\rho}} \rangle$)
2. If $\chi_\rho = \chi_{\rho'}$, then $\rho \cong \rho'$: $\langle \chi_\rho, \chi_{\tilde{\rho}} \rangle = \langle \chi_{\rho'}, \chi_{\tilde{\rho}} \rangle$ The type of irr. subrep of ρ is the same as ρ'.
3. If $\chi_1, \ldots, \chi_l$ are distinct irr. characters of G, then since $x_1, \ldots, x_l$ are orthonormal w.r.t. $\langle \cdot, \cdot \rangle$ in $\mathcal{C}(G)$, $x_1, \ldots, x_l$ are linearly indep. over $\mathbb{C}$ in $\mathcal{C}(G)$.

   But $\dim \mathcal{C}(G) = k = \#$ of conjugacy classes in G. So $l \leq k$ i.e. we conclude that there are at most k mutually non-equivalent irr. rep. of G, say $\rho_1, \ldots, \rho_l, l \leq k$.

   For any $\rho : G \to \mathrm{GL}(V)$, $\rho \cong \rho_1^{\oplus m_1} \oplus \cdots \oplus \rho_l^{\oplus m_l}$ where $m_i = \langle \chi_\rho, \chi_{\rho_i} \rangle \in \mathbb{Z}^{\geq 0}$.

Theorem 33 (Orthogonality relations for χ's)**.** The set of all irr. characters of G forms an orthonormal **basis** $\mathcal{C}(G)$ over $\mathbb{C}$. In particular, the number of irr. rep. of G is equal to $\#$ of conjugacy classes in G. (up to equivalence)

Proof. Let $\chi_i = \chi_{\rho_i}, i = 1, \ldots, l$ be all irr. characters of G and $\mathcal{D} = \langle \chi_1, \ldots, \chi_l \rangle_{\mathbb{C}} \subseteq \mathcal{C}(G)$. Then $\mathcal{C}(G) = \mathcal{D} \oplus \mathcal{D}^\perp$. Claim: $\mathcal{D}^\perp = \{0\}$.

Let $\varphi \in \mathcal{D}^\perp$, i.e. $\langle \varphi, \chi_i \rangle = 0, \forall\, i = 1, \ldots, l$.

Write $\rho^{\mathrm{reg}} \cong \rho_1^{\oplus m_1} \oplus \cdots \oplus \rho_l^{\oplus m_l} \implies \chi^{\mathrm{reg}} = m_1\chi_1 + \cdots + m_k\chi_l$. By assumption, $\langle \varphi, \chi_\rho \rangle = 0$.

For each i, define $\mathsf{T}_{\rho_i} \in \mathrm{Hom}_{\mathbb{C}}(V, V)$ by

$$\mathsf{T}_{\rho_i} \triangleq \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \rho_i(g)$$

Then we have

$$\mathrm{Tr}(\mathsf{T}_{\rho_i}) = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \chi_\rho(g) = \overline{\langle \varphi, \chi_\rho \rangle} = 0$$

Also, for all $h \in G$.

$$\begin{aligned}
\rho_i(h)^{-1} \circ \mathsf{T}_{\rho_i} \circ \rho_i(h) &= \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \rho_i(h)^{-1} \circ \rho_i(g) \circ \rho_i(h) \\
&\overset{*}{=} \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(h^{-1}gh)} \rho_i(h^{-1}gh) \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \rho_i(g) = \mathsf{T}_{\rho_i}
\end{aligned}$$

Where $*$ is because φ is a class function. So T_{ρ_i} is G-equivariant. By Schur's lemma, $\mathsf{T}_{\rho_i} = \lambda_i 1_{W_i}$ where $\rho_i : G \to \mathrm{GL}(W_i)$.
But $\mathrm{Tr}\,\mathsf{T}_{\rho_i} = 0 \implies \lambda_i = 0 \implies \mathsf{T}_{\rho_i} = 0$.
Also, because $\rho \cong \rho_1^{\oplus m_1} \oplus \cdots \oplus \rho_l^{\oplus m_l}$, if we define

$$\mathsf{T}_{\rho^{\mathrm{reg}}} \triangleq \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \rho^{\mathrm{reg}}(g) \implies \mathsf{T}_{\rho^{\mathrm{reg}}} = \mathsf{T}_{\rho_1}^{\oplus m_1} \oplus \cdots \oplus \mathsf{T}_{\rho_k}^{\oplus m_k} = 0$$

Finally, let $\rho = \rho^{\mathrm{reg}} : G \to \mathrm{GL}(V)$ with $V = \bigoplus_{g \in G} \mathbb{C}e_g$. Then $\mathsf{T}_\rho = 0 \implies \mathsf{T}_\rho(e_1) = 0$ and

$$0 = \mathsf{T}_\rho(e_1) = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \rho(g)(e_1) = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} e_g$$

Since $\{e_g\}$ is a basis, $\overline{\varphi(g)} = 0 \quad \forall\, g$. That is, $\varphi \equiv 0$. □

Prop 3.2.2. Each irr. rep. $\rho_i : G \to \mathrm{GL}(W_i)$ is contained in ρ^{reg} with multiplicity equal to $\dim W_i = m_i$, $i = 1, \dots, k$.
In particular, $\bigoplus_{g \in G} \mathbb{C}e_g \cong \underbrace{W_1 \oplus \cdots \oplus W_1}_{m_1 \text{times}} \oplus \cdots \oplus \underbrace{W_1 \oplus \cdots \oplus W_k}_{m_k \text{times}}$. So $|G| = m_1^2 + \cdots + m_k^2$.

Proof. Let $\chi^{\mathrm{reg}} := \chi_{\rho^{\mathrm{reg}}}$ and $\chi_i = \chi_{\rho_i}, i = 1, \dots, k$. Then

$$\langle \chi^{\mathrm{reg}}, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi^{\mathrm{reg}}(g) \chi_i(g^{-1}) = \frac{1}{|G|} |G| \chi_i(1) = m_i$$

□

Theorem 34 (Divisibility)**.** $\forall\, i = 1, \dots, k, \quad \chi_i(1) = m_i \bigm| |G|$.

Proof. First, we shall proof that for each $\rho = \rho_i$, $\chi = \chi_i$ and j, we have

$$\mathsf{T} \triangleq \sum_{g \in C_j} \rho(g) = \frac{|C_j| \chi(g_0)}{m_i} \mathsf{I}_{m_i}, \quad \text{for any } g_0 \in C_j$$

Observe that $\forall\, h \in G$,

$$\rho(h)^{-1} \circ \mathsf{T} \circ \rho(h) = \sum_{g \in C_j} \rho(h^{-1} g h) = \sum_{g' \in C_j} \rho(g') = \mathsf{T}$$

So T is G-equivariant w.r.t. ρ.
By Schur's lemma, $\mathsf{T} = \lambda \mathsf{I}_{m_i}$ for some $\lambda \in \mathbb{C}$. And $\lambda = \mathrm{Tr}(\mathsf{T})/m_i = \sum_{g \in C_j} \chi(g)/m_i = |C_j| \chi(g_0)/m_i$ for any $g_0 \in C_j$, thus $\sum_{g \in C_j} \rho(g) = \frac{|C_j| \chi(g_0)}{m_j} \mathsf{I}$ for any $g_0 \in C_j$.
Define $\lambda_\mu(C_i) \triangleq |C_i| \chi_\mu(g_i)/m_\mu$. Now, for a $g \in C_l$, define $a_{i,j,l} \triangleq \#\{\, (g_i, g_j) \in C_i \times C_j \mid g_i g_j = g \,\}$, which is indep. of the choice of g.
We claim that $\lambda_\mu(C_i) \lambda_\mu(C_j) = \sum_{l=1}^k a_{i,j,l} \lambda_\mu(C_j), \forall\, i, j, \mu$. Then

$$\lambda_\mu(C_i) \begin{bmatrix} \lambda_\mu(C_1) \\ \vdots \\ \lambda_\mu(C_k) \end{bmatrix} = A \begin{bmatrix} \lambda_\mu(C_1) \\ \vdots \\ \lambda_\mu(C_k) \end{bmatrix}, \quad \text{where } A \triangleq \begin{bmatrix} a_{i,1,1} & \dots & a_{i,1,k} \\ \vdots & \ddots & \vdots \\ a_{i,k,1} & \dots & a_{i,1,k} \end{bmatrix}$$

So $\lambda_\mu(C_j)$ is an eigenvalue of A, i.e., $\lambda = \lambda_\mu(C_j)$ satisfies $\det(\lambda I - A) = 0$. And thus $\lambda_\mu(C_i)$ is an algebraic integer.

We proof the claim by the following calculating.

$$
\begin{aligned}
\lambda_\mu(C_i)\lambda_\mu(C_j)I_{m_\mu} &= \left(\lambda_\mu(C_i)I_{m_\mu}\right)\left(\lambda_\mu(C_j)I_{m_\mu}\right) = \left(\sum_{g\in C_i}\rho(g)\right)\left(\sum_{g'\in C_j}\rho(g')\right)\\
&= \sum_{\substack{g\in C_i\\ g'\in C_j}}\rho(gg') = \sum_{l=1}^{k}\sum_{\bar g\in C_l} a_{i,j,l}\rho(\bar g)\\
&= \sum_{l=1}^{k} a_{i,j,l}\sum_{\bar g\in C_l}\rho(\bar g)\\
&= \sum_{l=1}^{k} a_{i,j,l}\lambda_\mu(C_l)I_{m_\mu}
\end{aligned}
$$

Finally,

$$
\begin{aligned}
\frac{|G|}{m_i} &= \frac{|G|}{m_i}\langle\chi_i,\chi_i\rangle\\
&= \frac{|G|}{m_i}\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_i(g^{-1})\\
&= \sum_{g\in G}\frac{\chi_i(g)}{m_i}\chi_i(g^{-1})\\
&= \sum_{j=1}^{k}\sum_{g\in C_j}\frac{\chi_i(g)}{m_i}\chi_i(g^{-1})\\
&= \sum_{j=1}^{k}\frac{|C_j|\chi_i(g_j)}{m_i}\chi_i(g_j^{-1})\\
&= \sum_{j=1}^{k}\lambda_i(C_j)\chi_i(g_j^{-1})
\end{aligned}
$$

and thus is an algebraic integer.
Also, $|G|/m_i \in \mathbb{Q}$, so we conclude that $|G|/m_i \in \mathbb{Z} \implies m_i \mid |G|$. □

Ex 3.2.1.

1. Show that if $g \in G$ and $g \neq 1$, then $\sum_{i=1}^{k} m_i\chi_i(g) = 0$.
2. Show that each character χ of G with $\chi(g) = 0 \quad \forall\, g \neq 1$ is an integral multiple of χ^{reg}.

Ex 3.2.2.

1. Let $|G| < \infty$. Then G is abelian $\iff$ each irr. rep. of G is of degree 1.
2. $\{$the deg 1 rep. of $G\} = \{$the irr. rep. of $G/[G,G]\}$.

3.2.2 Applications

1. $G = S_3 = D_3$, $6 = 1^2 + 1^2 + 2^2$.

Classes	1	(1 2)	(1 2 3)
size	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

The permutation representation

deg 4: $\tilde{\rho} = \rho^W \otimes \rho^W \rightsquigarrow \chi_{\tilde{\rho}} = \chi_3 \cdot \chi_3 = (4, 0, 1)$.

By inner product with χ_1, χ_2, χ_3, we can find $\chi_{\tilde{\rho}} = \chi_1 + \chi_2 + \chi_3 \rightsquigarrow \tilde{\rho} = \rho_1 \oplus \rho_2 \oplus \rho_3$.

2. $G = D_4 = \langle x, y \mid x^4 = 1, y^2 = 1, yxy^{-1} = x^{-1}\rangle$. $|G| = 8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2$.

Classes	1	y	x	x^2	xy
size	1	2	2	1	2
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	1	1	-1	1	-1
χ_4	1	-1	-1	1	1
χ_5	2	0	0	-2	0

$\chi^{\text{reg}} = (8, 0, 0, 0, 0) = \chi_1 + \chi_2 + \chi_3 + \chi_4 + 2\chi_5$.

3. $G = D_n$, (n even) $[G, G] = H = \langle x^2 \rangle$
4. $G = D_n$, (n odd) $[G, G] = H = \langle x \rangle$
5. $G = S_4$.

Classes	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
size	1	6	8	6	3
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

6. $G = A_4$, $[A_4, A_4] = V_4$.

Classes	1	(1 2 3)	(1 3 2)	(1 2)(3 4)
size	1	4	4	3
χ_1	1	1	1	1
χ_2	1	ω	ω^2	1
χ_3	1	ω^2	ω	1
χ_4	3	0	0	-1

Theorem 35 (Product of groups)**.** For $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G' \to \mathrm{GL}(V')$, write $\rho \otimes \rho' : G \times G' \to \mathrm{GL}(V \otimes V')$. If $\{\rho_i\}$ are irreducible representations of G, $\{\rho'_j\}$ are irreducible representations of G', then $\{\rho_i \otimes \rho'_j\}$ are exactly the irreducible representations of $G \times G'$.

Proof. It is evidence that $\rho_i \otimes \rho'_j$ is a homomorphism, and hence a representation.

Notice that $\chi_{\rho \otimes \rho'} = \chi_\rho \odot \chi_{\rho'}$ where $\chi_\rho \odot \chi_{\rho'}(g, g') = \chi_\rho(g)\chi_{\rho'}(g')$

Now we calculate

$$\begin{aligned}
\langle \chi_{\rho_1} \otimes \chi_{\rho_1'}, \chi_{\rho_2} \otimes \chi_{\rho_2'} \rangle &= \frac{1}{|G||G'|} \sum_{g,g'} \chi_{\rho_1}(g) \chi_{\rho_1'}(g') \chi_{\rho_2}(g) \chi_{\rho_2'}(g') \\
&= \left(\frac{1}{|G|} \sum_g \chi_{\rho_1}(g) \chi_{\rho_2}(g) \right) \left(\frac{1}{|G'|} \sum_{g'} \chi_{\rho_1'}(g') \chi_{\rho_2'}(g') \right) \\
&= \langle \chi_{\rho_1}, \chi_{\rho_2} \rangle \langle \chi_{\rho_1'}, \chi_{\rho_2'} \rangle
\end{aligned}$$

So $\langle \chi_\rho \otimes \chi_{\rho'}, \chi_\rho \otimes \chi_{\rho'} \rangle = 1$ hence each $\chi_\rho \otimes \chi_{\rho'}$ is irreducible. And $\langle \chi_{\rho_1} \otimes \chi_{\rho_1'}, \chi_{\rho_2} \otimes \chi_{\rho_2'} \rangle = 0$ if $\rho_1 \otimes \rho_1' \neq \rho_2 \otimes \rho_2'$, and thus these representations are not isomorphic.

Finally we proof that any irreducible representations of $G \times G'$ is isomorphic to some $\rho \otimes \rho'$.

Let $\{\rho_1, \ldots, \rho_k\}, \{\rho_1', \ldots, \rho_{k'}'\}$ be the sets of irreducible representations of G, G' respectively. Write $\chi_i = \chi_{\rho_i}, \chi_i' = \chi_{\rho_i'}$.

Let $\mathcal{D} \triangleq \mathcal{C}(G \times G') = \langle \chi_i, \chi_j' \mid i = 1, \ldots, k, j = 1, \ldots, k' \rangle_{\mathbb{C}} =$. We claim that $\mathcal{D}^\perp = \{0\}$.

Let $f \in \mathcal{D}^\perp$. Then

$$\begin{aligned}
0 &= \frac{1}{|G \times G'|} \sum_{(g,g') \in G \times G'} f(g,g') \overline{\chi_i(g) \chi_j'(g')} \\
&= \frac{1}{|G'|} \sum_{g'} \left(\frac{1}{|G|} \sum_g f(g,g') \overline{\chi_i(g)} \right) \chi_j'(g') \\
&= \left\langle \frac{1}{|G|} \sum_g f(g, \cdot) \overline{\chi_i(g)}, \chi_j' \right\rangle
\end{aligned}$$

Since ρ_j' are othonogal basis of $\mathcal{C}(G')$, we have $\frac{1}{|G|} \sum_g f(g,g') \overline{\chi_i(g)} = 0$ for all g'. Again,

$$0 = \frac{1}{|G|} \sum_g f(g,g') \overline{\chi_i(g)} = \langle f(\cdot, g'), \chi_i \rangle$$

Hence $f(g,g') = 0$ for all g, g', which implies $f \equiv 0$. $\square$

Ex 3.2.3. Determine all irr. rep. of C_n.

Ex 3.2.4. Calculate the character table of Q_8.

Ex 3.2.5. Calculate the character table of $\mathbb{Z}/2\mathbb{Z} \times S_4$ and $S_3 \times S_4$.

To calculate S_5, $|S_5| = 120 = 1^2 + 1^2 + 4^2 + 4^2 + 5^2 + 5^2 + 6^2$.

4 Extensions of Groups

4.1 Week 16

4.1.1 Extensions of abelian groups

Def 66. If a group E contains a normal subgroup N and $E/N \cong G$, then we call E an extension of N by G, denoted by $1 \to N \to E \to G \to 1$.

Ques: When N and G are given, how to obtain all extensions of N by G.

Now assume that N is abelian.

Def 67. $1 \to N \to E \xrightarrow{p} G \to 1$. $l : G \to E$ is a lifting if $p \circ l = \mathrm{id}_G$ and $l(1) = 1$.

Remark 21. $G \cong E/N = \{ xN \mid x \in E \}$, $p \circ l(\bar{x}) = \bar{x}$, $l(\bar{x})$ is a representative of $xN = \bar{x}$.

Prop 4.1.1.

1. $\forall\, \bar{x} \in G, \theta_{\bar{x}} : N \to N, a \mapsto l(\bar{x})al(\bar{x})^{-1}$. is independent of the choice of l.
2. $\theta : G \to \mathrm{Aut}(N), \bar{x} \mapsto \theta_{\bar{x}}$ is a group homomorphism.

Proof.

1. Suppose $l' : G \to E$ is another lifting. Then $l(\bar{x})N = l'(\bar{x})N$. So $l'(\bar{x}) = l(\bar{x})b$ for some $b \in N$. $\forall\, a \in N$, $l'(\bar{x})al'(\bar{x})^{-1} = l(\bar{x})bab^{-1}l(\bar{x})^{-1} = l(\bar{x})al(\bar{x})^{-1}$ since N is abelian.
2. $\theta_{\bar{x}\bar{y}}(a) = l(\bar{x}\bar{y})al(\bar{x}\bar{y})^{-1}$.

$$\begin{cases} p \circ l(\bar{x}\bar{y}) = \bar{x}\bar{y} \\ p \circ (l(\bar{x})l(\bar{y})) = \bar{x}\bar{y} \end{cases} \rightsquigarrow l(\bar{x}\bar{y}), l(\bar{x})l(\bar{y}) \text{ are liftings of } \bar{x}\bar{y}$$

□

Def 68. An extension $1 \to N \to E \to G \to 1$ splits if $\exists$ a lifting $l : G \to E$ is a group homo.

Prop 4.1.2. TFAE

1. $1 \to N \to E \to G \to 1$ splits.
2. $\exists$ a subgroup $K \leq E$ s.t. $K \cong G$ and $\begin{cases} K \cap N = \{1\} \\ NK = E \end{cases} \rightsquigarrow E \cong N \rtimes K (\cong N \rtimes G)$.

Proof. (1) $\Rightarrow$ (2): Let $K = \mathrm{Im}\, l$ which is a subgroup since l is a group homo.

- l is an isomorphism from G to K: If $l(\bar{x}) = l(\bar{y})$, then $p \circ l(\bar{x}) = p \circ l(\bar{y}) \rightsquigarrow \bar{x} = \bar{y}$. So l is 1-1.
- $E = NK$: $\forall\, x \in E, \bar{x} = p(x) \rightsquigarrow y = l(\bar{x})$ and $p(x) = p(y) \rightsquigarrow \exists\, a \in N$ s.t. $x = ay$.
- $K \cap N = \{1\}$: $a = l(\bar{x}) \in K \cap N \rightsquigarrow 1 = p(a) = p(l(\bar{x})) = \bar{x} \rightsquigarrow a = l(1) = 1$.

(2) $\Rightarrow$ (1):

- $p\big|_K : K \to G$ is an isom.: onto: $p(K) = p(NK) = p(E) = G$, 1-1: $\ker(p\big|_K) = N \cap K = \{1\}$.
- $l = \left(p\big|_K\right)^{-1}$ is a group homo.

  Observation: Let $l : G \to E$ be a lifting. Then $E = \bigcup_{\bar{x} \in G} Nl(\bar{x}), \forall\, x, y \in E$, write $x = al(\bar{x}), y = bl(\bar{y}), a, b \in N, \bar{x}, \bar{y} \in G$.

$$xy = (al(\bar{x})bl(\bar{y})) = al(\bar{x})bl(\bar{x})^{-1}l(\bar{x})l(\bar{y}) = a\theta_{\bar{x}}(b)l(\bar{x})l(\bar{y})$$

Notice that $l(\bar{x})l(\bar{y})$ and $l(\bar{x}\bar{y})$ are liftings, so we can write $l(\bar{x})l(\bar{y}) = f(\bar{x}, \bar{y})l(\bar{x}\bar{y})$ for some $f(\bar{x}, \bar{y}) \in N$. $\square$

Ex 4.1.1. $B^2(G, N) \leq Z^2(G, N)$.

Ex 4.1.2. Show that there are inequivalent extensions of N by G with isomorphic middle groups. (Hint: $N = \mathbb{Z}/p\mathbb{Z}$ with p is odd, $E = \mathbb{Z}/p^2\mathbb{Z}$, $a :: N \mapsto x^p :: E$ and please give another morphism $N \to E$ by yourself.)

Def 69. Given $1 \to N \to E \xrightarrow{p} G \to 1$ and $l : G \to E$, a factor set is a function $f : G \times G \to N$ s.t. $\forall\, \bar{x}, \bar{y} \in G, l(\bar{x})l(\bar{y}) = f(\bar{x}, \bar{y})l(\bar{x}\bar{y})$.

Prop 4.1.3. Let $1 \to N \to E \xrightarrow{p} G \to 1$ and $l : G \to E$. If f is a factor set, then

(1) $f(x, 1) = 1 = f(1, y) \quad \forall\, x, y \in G$.

(2) (cocycle identity) $\forall\, x, y, z \in G, f(x, y)f(xy, z) = \theta_x(f(y, z))f(x, yz)$.
(i.e. $f(x, y) + f(xy, z) = xf(y, z) + f(x, yz)$)

Proof.

(1) Trivial since $l(x)l(1) = l(1 \cdot x)$.

(2) By associativity. $(l(x)l(y))l(z) = l(x)(l(y)l(z))$.
$(l(x)l(y))l(z) = f(x, y)l(xy)l(z) = f(x, y)f(xy, z)l(xyz)$, and
$l(x)(l(y)l(z)) = l(x)f(y, z)l(yz) = l(x)f(y, z)l^{-1}(x)l(x)l(yz) = \theta_x(f(y, z))f(x, yz)l(xyz)$.
Thus $f(x, y)f(xy, z) = \theta_x(f(y, z))f(x, yz)$. $\square$

Theorem 36. Let $\sigma : G \to \mathrm{Aut}(N), x \mapsto \sigma_x$ be a group homo. and $f : G \times G \to N$ satisfies (1),(2) in Prop. 4.1.3. Then $\exists\, 1 \to N \to E \to G \to 1$ and $l : G \to E$ s.t. $\theta = \sigma$ and f is the corresponding factor set.

Proof.

- Define $E = N \times G$ equipped with the operation

$$(a, x)(b, y) = (a\sigma_x(b)f(x, y), xy)$$

  - associativity:

$$\begin{aligned}\big((a, x)(b, y)\big)(c, z) &= (a\sigma_x(b)f(x, y), xy)(c, z)\\ &= (a\sigma_x(b)f(x, y)\sigma_{xy}(c)f(xy, z), xyz)\\ &= (a\sigma_x(b)\sigma_{xy}(c)f(x, y)f(xy, z), xyz) \quad (\because N \text{ abelian})\end{aligned}$$

  and

$$\begin{aligned}(a, x)\big((b, y)(c, z)\big) &= (a, x)(b\sigma_y(c)f(y, z))\\ &= \big(a\sigma_x\big(b\sigma_y(c)f(y, z)\big)f(x, yz), xyz\big)\\ &= \big(a\sigma_x(b)\sigma_{xy}(c)\sigma_x(f(y, z))f(x, yz), xyz\big)\\ &= \big(a\sigma_x(b)\sigma_{xy}(c)f(x, y)f(xy, z), xyz\big)\end{aligned}$$

  - indentity: $(1, 1)$.
  - inverse: $(a, x)^{-1} = (\sigma_{x^{-1}}(a^{-1}f(x, x^{-1})^{-1}), x^{-1})$.

- $p : E \to G, (a,x) \mapsto x$ is a group homo by def.
- $i : N \to E, a \mapsto (a,1)$ is a group homo. $(a,1)(b,1) = (a\sigma_1(b)f(1,1),1) = (ab,1)$.
- $\ker p = \operatorname{Im} i$.
- Fix $l : G \to E, a \in N, x \in G$, say $l(x) = (b,x)$.

$$\begin{aligned} l(x)(a,1)l(x)^{-1} &= (b,x)(a,1)(b,x)^{-1} = (b\sigma_x(a),x)\big(\sigma_{x^{-1}}(a^{-1}f(x,x^{-1})^{-1}),x^{-1}\big) \\ &= (b\sigma_x(a)\cdot(\sigma_x\circ\sigma_{x^{-1}})\big(b^{-1}f(x,x^{-1})^{-1}\big)\cdot f(x,x^{-1}),1) \\ &= (\sigma_x(a),1) \end{aligned}$$

  So $\theta_x = \sigma_x$.
- Let $l : G \to E, x \mapsto (1,x)$. Check $l(x)l(y)l(xy)^{-1} = (f(x,y),1)$. Then f is the corresponding factor set. ☐

Prop 4.1.4. Let $1 \to N \to E \xrightarrow{p} G \to 1$ with two liftings $l_1 : G \to E,\ l_2 : G \to E$ with $f_1 : G\times G \to N,\ f_2 : G \times G \to N$ respectively.

Then $\exists\, h : G \to N$ with $h(1) = 1$ and $\forall\, x,y \in G, f_2(x,y)f_1(x,y)^{-1} = \theta_x(h(y))h(xy)^{-1}h(x)$. $(f_2(x,y) - f_1(x,y) = xh(y) - h(xy) + h(x))$

Proof. For $x \in G$, $\exists\, h(x) \in N$ s.t. $l_2(x) = h(x)l_1(x)$. Since $l_1(1) = l_2(1) = 1$, $h(1) = 1$.

Now, $l_2(x)l_2(y) = f_2(x,y)l_2(x,y) = f_2(x,y)h(xy)l_1(x,y)$. and

$$\begin{aligned} l_2(x)l_2(y) &= h(x)l_1(x)h(y)l_1(y) = h(x)l_1(x)h(y)l_1^{-1}(x)l_1(x)l_1(y) \\ &= h(x)\theta_x(h(y))l_1(x)l_1(y) = f_1(x,y)h(x)\theta_x(h(y))l_1(x,y) \end{aligned}$$

So $f_2(x,y)f_1(x,y)^{-1} = \theta_x(h(y))h(xy)^{-1}h(x)$. ☐

Remark 22. A map which has the form $\tilde{h} : G \times G \to N, (x,y) \mapsto xh(y) - h(xy) + h(x)$ is called a coboundary map.

Def 70. $Z^2(G,N) =$ the abelian group of all factor sets.

$B^2(G,N) =$ the abelian group of all coboundary maps.

$H^2(G,N) = Z^2(G,N)/B^2(G,N)$

Def 71. Two extensions $\begin{cases} 1 \to N \to E \to G \to 1 \\ 1 \to N \to E' \to G \to 1 \end{cases}$ are equivalent if exists an isomorphism $\varphi : E \xrightarrow{\sim} E'$ which let the following diagram comutes.

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] \arrow[d, "1_N"] & E \arrow[r] \arrow[d, "\varphi"', "\wr"] & G \arrow[r] \arrow[d, "1_G"] & 1 \\ 1 \arrow[r] & N \arrow[r] & E' \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

Theorem 37. Two extensions $\begin{cases} 1 \to N \to E \to G \to 1 \\ 1 \to N \to E' \to G \to 1 \end{cases}$ are equivalent $\iff$
Exists mappings $l : G \to E, l' : G \to E'$ with two factor sets f, f' respectively satisfies $f - f' \in B^2(G,N)$.

Proof. "$\Rightarrow$": Choose $l : G \to E$ which has a corresponding factor set $f : G \times G \to N$. Now define $l' : G \to E'$ by $l' = \varphi \circ l$. Since $p' \circ l' = p' \circ \varphi \circ l = p \circ l = 1$, l' is a lifting. Let $f' : G \times G \to N$ be its factor set.

Since $1_N = 1_N \circ \varphi$, $\varphi\big|_N = 1_N$. And

$$\begin{aligned}
&l(x)l(y) = f(x,y)l(xy) \\
\Rightarrow\ &\varphi(l(x)l(y)) = \varphi(f(x,y)l(xy)) \\
\Rightarrow\ &l'(x)l'(y) = \varphi(f(x,y))l'(xy) \\
\Rightarrow\ &f'(x,y) = \varphi(f(x,y))
\end{aligned}$$

But $f(x,y) \in N$, $\varphi(f(x,y)) = \varphi\big|_N(f(x,y)) = f(x,y)$. So $f(x,y) = f'(x,y)$, hence $f - f' = 0 \in B^2(G,N)$.

Ex 4.1.3.

(1) Show that $f' - f \in B^2(G,N)$.

(2) "$\Leftarrow$": Show all details of the following steps:

- $\begin{cases} 1 \to N \to E \to G \to 1 \\ 1 \to N \to E(N,G,f,\theta) \to G \to 1 \end{cases}$ are equivalent.
- Similarly $\begin{cases} 1 \to N \to E' \to G \to 1 \\ 1 \to N \to E(N,G,f',\theta') \to G \to 1 \end{cases}$ are equivalent.
- $f' - f \rightsquigarrow h : G \to N$,

□

4.1.2 1st and 2nd group cohomology

Let N be an abelian group and G be a group with a group homo $\sigma : G \to \mathrm{Aut}(N)$ ($G \curvearrowright N$)

$e(G,N) = \{\text{equivalence classes of } N \text{ by } G\}$
$Z^2(G,N) = \{f : G \times G \to N \mid f(1,v) = f = f(u,1), f(u,v) + f(uv,w) = uf(v,w) + f(u,vw) \quad u,v,w \in G\}$
$B^2(G,N) = \{f : G \times G \to N \mid \exists\, h : G \to N \text{ with } h(1) = 1 \text{ s.t. } f(u,v) = uh(v) - h(uv) + h(u) \quad u,v \in G\}$
$H^2(G,N) = Z^2(G,N)/B^2(G,N)$

Then $e(G,N) \leftrightarrow H^2(G,N)$.

Def 72.

- $\varphi \in \mathrm{Aut}(E)$ stabilizes $1 \to N \to E \to G \to 1$ if

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, "1_N"] & E \arrow[r] \arrow[d, "\varphi"', "\wr"] & G \arrow[r] \arrow[d, "1_G"] & 1 \\
1 \arrow[r] & N \arrow[r] & E \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

- $\mathrm{Stab}_E(G,N) = \{\text{stabilizing automorphisms}\} \le \mathrm{Aut}(E)$

Def 73.

- A derivation is a function $d : G \to N$ s.t. $d(uv) = ud(v) + d(u) \quad \forall\, u,v \in G$.
- $\mathrm{Der}(G,N) = \{\text{derivations} : G \to N\}$ is an abelian group with pointwise addition.

Theorem 38. Let $1 \to N \to E \to G \to 1$ with $\theta = \sigma$. Then $\mathrm{Stab}_E(G,N) \cong \mathrm{Der}(G,N)$. So $\mathrm{Stab}_E(G,N)$ is abelian.

Proof.

- Let $\varphi \in$ LHS and fix $l : G \to E$.

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] \arrow[d, "1_N"] & E \arrow[r] \arrow[d, "\varphi", "\wr"'] & G \arrow[r] \arrow[l, bend left, "l"] \arrow[d, "1_G"] & 1 \\ 1 \arrow[r] & N \arrow[r] & E \arrow[r] & G \arrow[r] & 1 \end{tikzcd} \qquad \varphi(al(u)) = \varphi(a)\varphi(l(u)) = ad(u)l(u)$$

  - For another $l' : G \to E$, say $l'(u) = g(u)l(u)$, where $g(u) \in N$, we have
  $$d'(u) = \varphi(l'(u))(l'(u))^{-1} = \varphi(g(u)l(u))(g(u)l(u))^{-1}) = g(u)\varphi(l(u))l(u)^{-1}g(u)^{-1} = d(u).$$
  - $d \in$ RHS,
  $$\begin{aligned} d(uv) &= \varphi(l(uv))l(uv)^{-1} \\ &= \varphi(f(u,v)^{-1}l(u)l(v))l(v)^{-1}l(u)^{-1}f(u,v) \\ &= f(u,v)^{-1}d(u)l(u)d(v)l(v)l(v)^{-1}l(u)^{-1}f(u,v) \\ &= f(u,v)^{-1}d(u)\big(l(u)d(v)l(u)^{-1}\big)f(u,v) \\ &= \big(ud(v)\big)d(u) \end{aligned}$$

- Conversely,

  Ex 4.1.4. proof it

- group homo: $\varphi_2 \circ \varphi_1(al(u)) = \varphi_2(ad_1(u)l(u)) = ad_1(u)\varphi_2(l(u)) = ad_1(u)d_2(u)l(u)$. That is, $\varphi_2 \circ \varphi_1 \mapsto d_1 d_2$. □

Def 74.

- $\mathrm{Inn}_E(G,N) = \{\varphi \in \mathrm{Stab}_E(G,N) \mid \varphi : E \to E, x \mapsto a_0 x a_0^{-1} \text{ for some } a_0 \in N\}$.
- $\mathrm{PDer}(G,N) = \{d \in \mathrm{Der}(G,N) \mid d(u) = ua_1 - a_1 \text{ for some } a_1 \in N\}$.

Ex 4.1.5. Show that $\mathrm{Inn}_E(G,N) \cong \mathrm{PDer}(G,N)$.

$\mathrm{Stab}_E(G,N)/\mathrm{Inn}_E(G,N) \cong \mathrm{Der}(G,N)/\mathrm{PDer}(G,N) = H^1(G,N)$.

Ex 4.1.6. Fix $1 \to N \to E \to G \to 1$. Show that if $H^2(G,N) = 0, H^1(G,N) = 0$, then for $\begin{matrix} l : G \to E \\ l' : G \to E \end{matrix}$ with $\begin{matrix} K = l(G) \\ K' = l'(G) \end{matrix}$, we get that K and K' are conjugate.

Def 75. Let R be a commutative ring with 1 and G be a group. The group ring

$$R[G] = \left\{ \sum_{g \in G} r_g g \,\middle|\, \text{only finitely many } r_g\text{'s} \neq 0 \text{ in } R \right\}$$

forms an R-algebra via

$$\sum_{g\in G} r_g g + \sum_{g\in G} r'_g g = \sum_{g\in G} (r_g + r'_g) g$$
$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{g'\in G} r'_g g'\right) = \sum_{g,g'\in G} (r_g r'_g) g g'$$
$$r\left(\sum_{g\in G} r_g g\right) = \sum_{g\in G} (r r_g) g$$

Remark 23.

1. - $\{\rho : G \to \mathrm{GL}(V)\} \leftrightarrow \{V : \mathbb{C}[G]\text{-module}\}$.
   - ρ: irr $\leftrightarrow V$: simple $\mathbb{C}[G]$-module (i.e. no nontrivial proper submodule)
   - $W \subset V$: G-invariant $\leftrightarrow W$: $\mathbb{C}[G]$-submodule.
2. N: abelian $\rightsquigarrow N : \mathbb{Z}$-module and $G \curvearrowright N$. $\implies$ $N : \mathbb{Z}[G]$-module.

Def 76. $G \curvearrowright \mathbb{Z}$ trivially. i.e. $g \cdot n = n \quad \forall\, g \in G, n \in \mathbb{Z}$, then $\mathbb{Z} : \mathbb{Z}[G]$-module.

- $B_0 = \mathbb{Z}[G][\ ]$: the free $\mathbb{Z}[G]$-module on the symbol $[\ ]$.
- $B_1 = \bigoplus_{u \in G} \mathbb{Z}[G][u]$: the free $\mathbb{Z}[G]$-module on the set G.
- $B_2 = \bigoplus_{u,v \in G} \mathbb{Z}[G][u|v]$: the free $\mathbb{Z}[G]$-module on the set $G \times G$.
- $B_3 = \bigoplus_{u,v,w \in G} \mathbb{Z}[G][u|v|w]$: the free $\mathbb{Z}[G]$-module on the set $G \times G \times G$.

...

Now apply $\mathrm{Hom}(\cdot, N)$ to it:

...

Theorem 39. $\mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, N) := \ker d_2^* / \ker d_1^* \cong \mathrm{Der}(G, N)/\mathrm{PDer}(G, N) = H^1(G, N)$.

Proof.

- $g \in \ker d_2^* \subseteq \mathrm{Hom}(B_1, N) \implies g \circ d_2 = 0$. ...
- ...
- Let $t \in \mathrm{Hom}(B_0, N)$, say $t([\ ]) = a_0 \in N$.

  $$d_1^*(t)([u]) = t \circ d_1([u]) = t(u[\ ] - [\ ]) = ut([\ ]) - t([\ ]) = ua_0 - a_0$$

  Then $d(u) := d_1^*(t)([u]) \implies d \in \mathrm{PDer}(G, N)$.
- ...

□

Remark 24. $\mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, N) \cong H^2(G, N)$.

5 Fields

5.1 Algebraic extensions

Def 77.

- L/K is called an **field extension** if L is a field and K is a subfield of L.
- $\alpha \in L$ is **algebraic** over K if exists $f(x) \in K[x]$ satisfied $f(\alpha) = 0$.
- L/K is called an **algebraic extension** if $\forall\, \alpha \in L, \exists\, f(x) \in K[x]$ such that $f(\alpha) = 0$.
- $K(\alpha_1, \alpha_2, \ldots, \alpha_n) \triangleq \big\{P(\alpha_1, \ldots, \alpha_n)/Q(\alpha_1, \ldots, \alpha_n) : P, Q \in K[x_1, x_2, \ldots, x_n] \text{ and } Q \neq 0\big\}$

Theorem 40 (Eisenstein criterion)**.**
Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $\gcd(a_0, a_1, \cdots, a_n) = 1$. Assume that there exists a prime p s.t. $p \nmid a_n$ but $p \mid a_i$ for other $i \neq n$, and $p^2 \nmid a_0$, then f is irreducible.

Proof. Since f is primitive, by Gauss lemma, we only need to prove that it is irreducible in $\mathbb{Q}[x]$. Consider $\bar{f}(x)$, by assumption, $\bar{f}(x) = \bar{a}_n x^n$. So if $f(x) = g(x)h(x)$ with $\deg g, \deg h \geq 1$, let $g(x) = b_r x^r + \cdots + b_0, h(x) = c_{n-r} x^{n-r} + \cdots + c_0$, then $\bar{g}(x) = \bar{b}_r x^r, \bar{h}(x) = \bar{c}_{n-r} x^{n-r}$ for some r. But then we would find out that $\bar{b}_0 = \bar{c}_0 = 0$, and thus $p^2 \mid a_0$, which is a contradiction, hence f is irreducible. $\square$

Prop 5.1.1. Given L/K and $\alpha \in L$, if α is algebraic over K, then there exists a unique monic irreducible polynomial $m_{\alpha,K}(x) \in K[x]$ of minimal degree s.t. $m_{\alpha,K}(\alpha) = 0$ and for any other $f(x) \in K[x]$ with $f(\alpha) = 0$, we have $m_{\alpha,K} \mid f$. We call $m_{\alpha,K}$ the **minimal polynomial** of α over K.

Proof. Let I be the set of all polynomials such that $f(\alpha) = 0$, since α algebraic, $I \neq \varnothing$, so pick a monic polynomial $g(x)$ of minimal degree in I. For any other $f(x) \in I$, write $f(x) = g(x)q(x) + r(x)$ with $\deg r < \deg g$. If $r(x) \neq 0$, then $r(\alpha) = f(\alpha) - q(\alpha)g(\alpha)$. But then $r(\alpha) = f(\alpha) - q(\alpha)g(\alpha) = 0$ with $\deg r < \deg g$, which contradicts the minimality of g, thus $r = 0$, and hence $g \mid f$.

Finally, if $g(x) = h_1(x)h_2(x)$ with $\deg h_1, \deg h_2 < \deg g$, then one of them, say $h_1(\alpha) = 0$ again contradicts the minimality of g, hence g is irreducible. $\square$

Prop 5.1.2. Let L/K be an extension and $\alpha \in L$, the following are equivalent:

(1) α is algebraic over K.

(2) $K[\alpha] = K(\alpha)$.

(3) $[K(\alpha) : K] < \infty$.

Proof. (1) $\Rightarrow$ (2): "$\subset$" trivial.
"$\supset$": For all $\beta \in K(\alpha), \beta = g(\alpha)/h(\alpha)$ with $h(\alpha) \neq 0$. So $m_{\alpha,K} \nmid h$. Since $m_{\alpha,K}$ is irreducible, $\gcd(m_{\alpha,K}, h) = 1$, hence there exists $a(x), b(x) \in K[x]$ such that $1 = a(x)h(x) + b(x)m_{\alpha,K}(x)$ Subsitute α and we get $1/h(\alpha) = a(\alpha)$, hence $\beta = g(\alpha)a(\alpha) \in K[\alpha]$.

(2) $\Rightarrow$ (1): Since $1/\alpha \in K[\alpha]$, thus $1/\alpha = f(\alpha)$ for some polynomial f, hence if we set $g(x) = xf(x) - 1$, $g(\alpha) = 0$ which implies α is algebraic.

(1) $\Rightarrow$ (3): Assume that $\deg m_{\alpha,K} = n$, it is easy to see that $K[\alpha] = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_K$. Since (1) $\implies$ (2), we have $[K(\alpha) : K] = [K[\alpha], K] = n$.

(3) $\Rightarrow$ (1): Since $[K(\alpha) : K] = n$, consider $1, \alpha, \alpha^2, \ldots, \alpha^n$. Some of these $n+1$ elements may be coincident, but nevertheless these elements are linearly dependent. Hence there exists $a_0, \ldots, a_n$ not all zero in K s.t. $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0 \implies \alpha$ is algebraic. $\square$

Prop 5.1.3. Given M/L and L/K, $[M : K] = [M : L][L : K]$.

Proof. If $[M : L] = m < \infty$ and $[L : K] = n < \infty$, then $L \cong K^{\oplus n}, M \cong L^{\oplus m}$. So $M \cong (K^{\oplus n})^{\oplus m} \cong K^{\oplus mn}$, thus $[M : K] = mn$.

Now if $[M : K] = l < \infty$, then there exists a basis $\{z_1, z_2, \ldots, z_l\}$ which is a basis for M over K. Then $M = Kz_1 + \cdots + Kz_l \subset Lz_1 + \cdots + Lz_l \subset M \implies M = Lz_1 + \cdots + Lz_l$. Hence $[M : L] < \infty$. Also, since L is a K-linear subspace of M, $[L : K] \leq l \implies [L : K] < \infty$. Thus if $[M : L] = \infty$ or $[L : K] = \infty$, then $[M : K] = \infty$. $\square$

Prop 5.1.4. Given L/K, define $L^{\text{alg}} \triangleq \{\alpha \in L \mid \alpha \text{ is algebraic over } K\}$, then L^{alg} is a subfield of L.

Proof. Notice that if $\alpha, \beta \in L^{\text{alg}}$, then β is algebraic over K implies that β is algebraic over $K(\alpha)$. Thus

$$[K(\alpha, \beta) : K] = [K(\alpha)(\beta) : K(\alpha)][K(\alpha) : K] < \infty$$

Also, since $K(\alpha+\beta), K(\alpha-\beta), K(\alpha\beta), K(\alpha/\beta)$ are all contained in $K(\alpha, \beta)$, they are all algebraic over K, thus these elements are all algebraic, and hence L^{alg} is a subfield. $\square$

Prop 5.1.5. $[L : K] < \infty$ if and only if $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ with each α_i algebraic over K. In this case, L/K is algebraic.

Proof. "$\Rightarrow$": Let $[L : K] = n$, so there is a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ for L over K. It is easy to see that $L = K(\alpha_1, \ldots, \alpha_n)$. Also $[K(\alpha_i) : K] \leq [L : K] < \infty$, thus α_i is algebraic.

"$\Leftarrow$": Since α_i is algebraic over K, α_i is algebraic over $K(\alpha_1, \ldots, \alpha_{i-1})$. Thus

$$[L : K] = [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})][K(\alpha_1, \ldots, \alpha_{n-1}) : K(\alpha_1, \ldots, \alpha_{n-2})] \ldots [K(\alpha_1) : K] < \infty$$

Moreover, $\forall\, \alpha \in L, [K(\alpha) : K] \leq [L : K] < \infty$, so α is algebraic over K. $\square$

Coro 5.1.1. Given L/K, and S a subset of L, if $\forall\, \alpha \in S$, α is algebraic over K, then $K(S)/K$ is algebraic.

Proof. If $\beta \in K(S)$, by definition we know that there exists $\alpha_1, \ldots, \alpha_n$ such that $\beta \in K(\alpha_1, \ldots, \alpha_n)$. Thus β is algebraic over K. $\square$

Prop 5.1.6. If M/L and L/K are algebraic, then M/K is algebraic.

Proof. For all $\alpha \in M$, since α is algebraic over L, there exists $a_{n-1}, \ldots, a_0$ so that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, that is, α is algebraic over $K(a_0, \ldots, a_{n-1})$.

So $[K(a_0, \ldots, a_{n-1}, \alpha) : K] = [K(a_0, \ldots, a_{n-1})(\alpha) : K(a_0, \ldots, a_{n-1})][K(a_0, \ldots, a_{n-1}) : K] < \infty$, thus α is algebraic over K. $\square$

Def 78. Given L/L_1 and L/L_2, L_1L_2 is defined as the smallest subfield of L containing both L_1 and L_2.

Prop 5.1.7. Let $[L_1 : K] = m$ and $[L_2 : K] = n$.

(1) $[L_1L_2 : K] \leq mn$.

(2) If $\gcd(m,n) = 1$, then $[L_1L_2 : K] = mn$.

Proof. (1): Assume $L_1 = K(\alpha_1, \ldots, \alpha_m), L_2 = K(\beta_1, \ldots, \beta_n)$. We could find that $L_1L_2 = K(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$. Notice that $[K(\beta_1, \ldots, \beta_m)(\alpha_i) : K(\beta_1, \ldots, \beta_m)] \leq [K(\alpha_i) : K]$, and thus $[L_1L_2 : K] = [K(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) : K(\beta_1, \ldots, \beta_n)][K(\beta_1, \ldots, \beta_m) : K] \leq [K(\alpha_i, \ldots, \alpha_n) : K][K(\beta_1, \ldots, \beta_n) : K] = [L_1 : K][L_2 : K]$.

(2): Notice that $[L_i : K] \mid [L_1L_2 : K]$, so $mn \mid [L_1L_2 : K]$. By (1), $[L_1L_2 : K] \leq nm$, hence $[L_1L_2 : K] = nm$. $\square$

Def 79. Let R be a commutative ring with 1, and I be an ideal of R, then

- I is called a **maximal ideal** if for any ideal J satisfying $I \subseteq J$ we have $J = I$ or $J = R$.
- I is called a **prime ideal** if $I \neq R$ and $ab \in I \implies a \in I$ or $b \in I$.

Prop 5.1.8. Suppose R is a ring and $I \subsetneq R$ is an ideal, then

1. I is maximal $\iff$ R/I is a field.
2. I is a prime ideal $\iff$ R/I is an integral domain.

Proof.

1. "$\Rightarrow$": For any $\bar{r} \in R/I$ with $\bar{r} \neq 0$, then $r \notin I$. Consider $\langle r \rangle + I$ which contains I and is not equal to I because $r \notin I$. Since I is maximal, $\langle r \rangle + I = R$, and thus $\exists\, x \in R, y \in I$ such that $xr + y = 1$, so $\bar{x}\bar{r} = \bar{1}$. Hence every non-zero element has multiply inverse and R/I is a field.

   "$\Leftarrow$": If J is an ideal such that $I \subsetneq J$, pick $x \in J \setminus I$, then $\bar{x} \neq 0$, so $\exists\, r \in J$ such that $\bar{x}\bar{r} = 1$. Then $xr + I = 1 + I \implies \exists\, y \in I$ s.t. $xr + y = 1$. So $1 \in J$, and because J is an ideal, $J = R$.

2. By the fact that $(ab \in I \implies a \in I \text{ or } b \in I) \iff (\bar{a}\bar{b} = 0 \implies \bar{a} = 0 \text{ or } \bar{b} = 0)$ the proof is complete. $\square$

Prop 5.1.9. If $f(x) \in K[x]$ is irreducible, where K is a field, then $\langle f(x) \rangle$ is maximal ideal.

Proof. We know that $K[x]$ is a principle ideal domain, so if $\langle f(x) \rangle \subseteq J$, then J is generated by a element, say $g(x)$. Since $f(x) \in J$, we could write $f(x) = g(x)h(x)$. By the fact that $f(x)$ is irreducible, either $g(x)$ is an unit then $J = R$, or $h(x)$ is an unit then $J = \langle f(x) \rangle$. $\square$

Eg 5.1.1. $f(x) = x^2 + 1$ has roots $\alpha = \pm\sqrt{-1}$, so $\mathbb{R}(\sqrt{-1}) \cong \mathbb{R}[x]/\langle x^2 + 1 \rangle$.

Theorem 41. Let $f(x) \in K[x]$ be monic, irreducible and of degree n. Then there exists L/K and $\alpha \in L$ s.t. $f(\alpha) = 0, L = K(\alpha)$ and $[L : K] = n$.

Proof. Since $f(x)$ is irreducible, by prop. 5.1.9 $\langle f(x) \rangle$ is a maximal ideal. Then by prop. 5.1.8 $L = K[x]/\langle f(x) \rangle$ is a field, and K is a subfield of L by the inclusion map $\alpha \mapsto \bar{\alpha}$. The map is 1-1 since $\bar{1} \neq 0$ and a field homomorphism is either a 1-1 map or a zero（全洪）map.

Notice that $L \cong K[\bar{x}]$, where $\bar{x}$ is the coset $x + \langle f(x) \rangle$. Now let $\alpha = \bar{x}$, and it is easy to see that $f(\alpha) = f(x) + \langle f(x) \rangle = 0$. Also $L \cong K[\bar{x}] \cong K(\alpha)$. Finally, $m_{\alpha,K} \mid f$ and by the fact that f is monic and irreducible, $m_{\alpha,K} = f$ and thus $[L : K] = \deg m_{\alpha,K} = \deg f = n$. $\square$

Theorem 42. Let $f(x) \in K[x]$ be of degree $n > 0$. Then there exists L/K s.t. f splits over L, that is,

$$f(x) = \lambda(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \text{ with } \alpha_1, \alpha_2, \ldots, \alpha_n \in L,\ \lambda \in K$$

In fact, L can be chosen to be the smallest field over which f splits and in this case $[L : K] \leq n!$. L is called a *splitting field* for f over K.

Proof. By induction on n, $n = 1$ is trivial, simply pick $L = K$.

For $n > 1$, let $p(x)$ be an monic irreducible factor of $f(x)$. By theorem 41, there exists an extension $K(\alpha_1)$ s.t. $p(\alpha_1) = 0$. By division algorithm, $f(x) = (x - \alpha_1)f_1(x)$ where $f_1(x) \in K(\alpha_1)[x]$ and $\deg f_1 = n-1$. Using the induction hypothesis, we know that there exists L, which is an extension of $K(\alpha_1)$, s.t. f_1 splits over L. Hence $\exists\, \alpha_2, \alpha_3, \ldots, \alpha_n \in L$ s.t. $f_1(x) = \lambda(x-\alpha_2)\ldots(x-\alpha_n)$, thus $f(x) = \lambda(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$. Compare the coefficient of x^n we know that $\lambda \in K$.

More over, observe that $K(\alpha_1, \ldots, \alpha_n)$ is the smallest field containing K and $\{\alpha_1, \ldots, \alpha_n\}$. So if we choose $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, then

$$[L : K] = [K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})] \cdots [K(\alpha_1) : K] \leq n!$$

Since $[K(\alpha_1, \alpha_2, \ldots, \alpha_k) : K(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})] = [K(\alpha_1, \alpha_2, \ldots \alpha_{k-1})(\alpha_k) : K(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})]$ and α_k is a root of $p(x) \in K(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})[x]$ where $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})p(x)$. $\square$

Eg 5.1.2. Find a splitting field L for $x^8 - 2$ over $\mathbb{Q}$ and determine $[L : \mathbb{Q}]$.

The roots are $\alpha\zeta^k$ where $\alpha = \sqrt[8]{2}$ and $\zeta = e^{2\pi \mathrm{i}/8}$. But $\zeta = \sqrt{2}(1+\mathrm{i})/2$ where $\sqrt{2} = \alpha^4$, so we know that $L = \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\alpha, \mathrm{i})$. Thus $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \mathrm{i}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 8 = 16$.

Remark 25. $\mathbb{Q}[x]/\langle x^8 - 2\rangle = \mathbb{Q}(\bar{x}) \cong \mathbb{Q}(\sqrt[8]{2}) \cong \mathbb{Q}(\sqrt[8]{2}\zeta)$

Prop 5.1.10. Let K, L be two fields and $\tau : K \to L$ be a nontrivial homomorphism. We define $\bar{\tau} : K[x] \to \tau(K)[x] \subseteq L[x]$ by

$$a_n x^n + \cdots + a_0 \mapsto \bar{\tau}(f) \triangleq \tau(a_n)x^n + \cdots + \tau(a_0)$$

which is an isomorphism. Also, f is irreducible implies $\bar{\tau}(f)$ is irreducible in $\tau(K)[x]$.

Lemma 4. Let $K(\alpha)/K$ be algebraic and $\tau : K \to L$ be a nontrivial homo, then there exists an extension σ of τ from $K(\alpha)$ to L if and only if $\exists\, \beta \in L$ s.t. $\bar{\tau}(m_{\alpha,K})(\beta) = 0$.

In this case $m_{\beta,\tau(K)} = \bar{\tau}(m_{\alpha,K})$.

Proof. "$\Rightarrow$": Let $\beta = \sigma(\alpha)$ and $m_{\alpha,K} = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $\bar{\tau}(m_{\alpha,K})(\beta) = \beta^n + \tau(a_{n-1})\beta^{n-1} + \cdots + \tau(a_0) = \tau(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) = 0$

"$\Leftarrow$": Observe that $m_{\beta,\tau(K)} = \bar{\tau}(m_{\alpha,K})$ since $\bar{\tau}(m_{\alpha,K})(\beta) = 0$ and $\bar{\tau}(m_{\alpha,K})$ is monic and irreducible by prop 5.1.10. σ is then given by the following diagram.

$$\begin{tikzcd}
 & K[x] \arrow[r, "\sim", "\bar{\tau}"'] \arrow[d, two heads] & \tau(K)[x] \arrow[d, two heads] & \\
K(\alpha) \arrow[r, Leftrightarrow, "\cong"] & K[x]\big/\langle m_{\alpha,K}\rangle \arrow[r, "\sim", "\sigma"'] & \tau(K)[x]\big/\langle m_{\beta,\tau(K)}\rangle \arrow[r, Leftrightarrow, "\cong"] & \tau(K)(\beta) \subseteq L
\end{tikzcd}$$

$\square$

Coro 5.1.2. Let $K(\alpha)/K$ be an algebraic extension and $\tau : K \hookrightarrow L$. If $\bar{\tau}(m_{\alpha,K})$ has r distinct roots in L, then there are exactly r extensions of τ.

Theorem 43. Let $\tau : K \to K'$ be an isomorphism of fields. If L is a splitting field for f over K and L' is a splitting field for $\bar{\tau}(f)$ over K', then $L \cong L'$

Proof. By induction on $n = \deg f$. When $n = 1$, $L = K, L' = K'$, so $L \cong L'$.

Now if $n > 1$, assume $f(\alpha) = 0$ for $\alpha \in L$. Then $\bar{\tau}(m_{\alpha,K}) \mid \bar{\tau}(f)$ and by the fact that L' is a splitting field for $\bar{\tau}(f)$, $\exists\, \beta \in L'$ s.t. $\bar{\tau}(m_{\alpha,K})(\beta) = 0$. By lemma 4, $\exists\, \tau_\circ : K(\alpha) \xrightarrow{\sim} K'(\beta)$ with $\tau_\circ\big|_K = \tau$.
Now, write $f = (x-\alpha)f_\circ$, then $\bar{\tau}(f) = \bar{\tau}_\circ(f) = (x - \tau_\circ(\alpha))\bar{\tau}_\circ(f_\circ) = (x-\beta)\bar{\tau}_\circ(f_\circ)$. Then L and L' is a splitting field for $f_\circ$ over $K(\alpha)$ and $\bar{\tau}_\circ(f_\circ)$ over $K(\beta)$ respectively. By induction hypothesis, $L \cong L'$. ∎

Coro 5.1.3. Let $\tau : K \xrightarrow{\sim} K'$ be an isomorphism of fields, and L is a splitting field of f over K, L' is a splitting field of $\bar{\tau}(f)$ over K'. Then τ could be extend to $\sigma : L \xrightarrow{\sim} L'$ such that $\sigma\big|_K = \tau$.

5.2 Finite field

Def 80. A polynomial $f(x) \in K[x]$ is said to be *separable* if its irreducible factors have no multiple roots in a splitting field L.

Def 81. If $f(x) = a_n x^n + \cdots + a_1 x + a_0$, then define $f'(x) \triangleq n a_n x^{n-1} + \cdots + 2a_2 x + a_1$.

Theorem 44. Let $f(x) \in K[x]$ be monic, irreducible of positive degree, then all the roots of $f(x)$ in a splitting field are simple if and only if $\gcd(f(x), f'(x)) = 1$.

Proof. "$\Rightarrow$": We can write $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where α_i are distinct roots of f. Then $f'(x) = \sum_{i=1}^n f(x)/(x-\alpha_i)$ and we have $(x-\alpha_i) \nmid f(x)$ for all i.

"$\Leftarrow$": Assume $f(x) = (x-\alpha)^k g(x)$ with $k \geq 2$. Then $f'(x) = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x)$ which implies $(x-\alpha) \mid f(x)$. So $(x-\alpha) \mid \gcd(f(x), f'(x))$ and thus $\gcd(f(x), f'(x)) \neq 1$. □

Remark 26. The following are equivalent:

1. α is a multiple root of $f(x)$.
2. α is a common root of $f(x)$ and $f'(x)$.
3. $m_{\alpha,K} \mid f(x)$ and $m_{\alpha,K} \mid f'(x)$.

Theorem 45. There is a finite field K with $|K| = q \iff q = p^n$ for some prime p and $n \in \mathbb{N}$. In this situation, K is unique up to isomorphism, denote by $\mathbb{F}_{p^n}$.

Proof. "$\Rightarrow$": Let $p = \operatorname{char} K$ and $[K : \mathbb{Z}/p\mathbb{Z}] = n$, then $|K| = p^n$.

"$\Leftarrow$": Let K be a splitting field for $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$. We claim that the set of all roots of $f(x)$ forms a field. Since if α, β are two roots of f, obviously $\alpha\beta, \alpha\beta^{-1}$ are also roots, and by $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$ because $\operatorname{char} K = p$. $\alpha \pm \beta$ are also roots, hence the roots form a field. By definition, K is the smallest field containing $\mathbb{F}_p$ and roots of $f(x)$, so K is exactly the set of roots of $f(x)$.

Also, $f'(x) = -1$ has no root, so $f(x)$ has no multiple root which implies $|K| = p^n$.

Moreover, if K' is another finite field with $|K'| = p^n$, then for all $\alpha \in K'$, $\alpha^{p^n} = \alpha$, so α is a root of $f(x)$, which implies that K' is a splitting field for $f(x)$ over $\mathbb{F}_p$. By theorem 43, $K \cong K'$. □

Theorem 46. Let $n \in \mathbb{N}$ and $\mathbb{F}_q$ be a finite field. Then there exists a unique extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ s.t. $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, and $\operatorname{Aut}\left(\mathbb{F}_{q^n}/\mathbb{F}_q\right) = \langle \sigma_q \rangle$ with $\sigma_q = \alpha :: \mathbb{F}_{q^n} \mapsto \alpha^q :: \mathbb{F}_{q^n}$. σ_q is called the *Frobenius homomorphism* .

Proof. By theorem 45, $q = p^r$ for some prime p and $r \in \mathbb{N}$, so $q^n = p^{nr}$ which is a power of a prime. Again by theorem 45, $\mathbb{F}_{q^n}$ is the splitting field for $x^{p^{nr}} - x$ over $\mathbb{F}_p$. Since $x^q - x \mid x^{q^n} - x$, $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ and thus $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

Then we proof that σ_q is indeed in $\operatorname{Aut}\left(\mathbb{F}_{q^n}/\mathbb{F}_q\right)$. We check that

$$\sigma_q(\alpha+\beta) = (\alpha+\beta)^q = \alpha^q + \beta^q = \sigma_q(\alpha) + \sigma_q(\beta)$$
$$\sigma_q(\alpha\beta) = (\alpha\beta)^q = \alpha^q\beta^q = \sigma_q(\alpha)\sigma_q(\beta)$$

Now σ_q is nontrivial since σ_q send 1 to 1, so σ_q is 1-1 and hence an isomorphism since $\mathbb{F}_q$ is finite. Also, for all $\alpha \in \mathbb{F}_q$, $\sigma_q(\alpha) = \alpha^q = \alpha$, hence σ_q fixes $\mathbb{F}_q$.

Finally we prove that the order of σ_q is n. Assume not, so $\operatorname{ord}(\sigma_q) = m < n$. Then $\sigma_q^m = \mathrm{Id} \implies x^{q^m} - x = 0$ for each $x \in \mathbb{F}_{q^n}$. But $x^{q^m} - x = 0$ has at most $q^m < q^n$ roots, which leads to a contradiction. $\square$

Remark 27. By theorem 10, the multiplication group of $\mathbb{F}_{q^n}$ is cyclic, so $\mathbb{F}_{q^n}^\times = \langle \alpha \rangle \subseteq \mathbb{F}_q(\alpha) \setminus \{0\} \subseteq \mathbb{F}_{q^n} \setminus \{0\}$, hence $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

Lemma 5. Every irreducible polynomial $f(x)$ in $\mathbb{F}_{p^n}[x]$ is separable.

Proof. Without lost of generality, assume $f(x)$ is monic.

Since σ_p is an isomorphism, $\mathbb{F}_{p^n} = \mathbb{F}_{p^n}^p = \{\alpha^p \mid \alpha \in \mathbb{F}_{p^n}\}$. Now assume $f(x)$ has a multiple root α, then $m_{\alpha,\mathbb{F}_p} = f(x)$ since f is irreducible. By theorem 44 we also have $f(x) = m_{\alpha,\mathbb{F}_p} \mid f'(x)$, but $\deg f'(x) < \deg f(x)$ so we must have $f'(x) \equiv 0$.

Write $f(x) = a_n x^n + \ldots + a_1 x + a_0$, then $f'(x) \equiv 0$ implies $k a_k = 0_{\mathbb{F}_p}$ for each k, which means that if $a_k \neq 0 \implies p \mid k$. So

$$f(x) = a_{mp} x^{mp} + a_{(m-1)p} x^{(m-1)p} + \cdots + a_p x^p + a_0 = (a_{mp} x^m + \ldots + a_p x + a_0)^p.$$

But this implies $f(x)$ is reducible, which is a contradiction. $\square$

Theorem 47. $x^{p^n} - x$ equals the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree d where d runs through all divisors of n. i.e.

Proof. By lemma, each irreducible polynomial is separable, and if $f(x), g(x) \in \mathrm{RHS}$, and $f(\alpha) = g(\alpha) = 0$, then $f = m_{\alpha,\mathbb{F}_p} = g$. Thus RHS is separable. LHS is separable since $f' = 1$, so we could prove the equality by checking that they have same roots.

LHS $\mid$ RHS: $\forall\, \alpha \in \mathbb{F}_{p^n}$, $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \mid [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, thus $\deg m_{\alpha,\mathbb{F}_p} \mid n$ and hence $m_{\alpha,\mathbb{F}_p}$ appears in RHS.

RHS $\mid$ LHS: Assume $\deg m_{\alpha,\mathbb{F}_p} = d \mid n$, then $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d$, so $\alpha^{p^d} = \alpha$, and hence $\alpha = \alpha^{p^d} = \alpha^{p^{2d}} = \cdots = \alpha^{p^n}$. $\square$

Def 82. The **Möbius μ-function** is defined as

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n \text{ has a square factor} \\ (-1)^r, & \text{if } n \text{ is a product of } r \text{ distinct primes} \end{cases}$$

Theorem 48 (Möbius inversion formula)**.** If $f(n) = \sum\limits_{d \mid n} g(d)$, then $g(n) = \sum\limits_{d \mid n} \mu(d) f\left(\frac{n}{d}\right)$.

Remark 28. Let $\psi_q(d)$ denote the number of monic irreducible polynomials of degree d in $\mathbb{F}_q$, then $q^n = \sum_{d \mid n} d \psi_q(d)$.

Using the convolution notation, we have $(n \mapsto q^n) = \mathbb{1} * (n \mapsto n\psi_q(n))$. Where $\mathbb{1} \triangleq (n \mapsto 1)$. It could be seen that $\mathbb{1}^{-1} = \mu$. Thus $n\psi_q(n) = \sum_{d \mid n} \mu(d) q^{n/d}$.

5.3 Algebra closure

Def 83.

- L is called an **algebraic closure** of K if L/K is algebraic and each polynomial $f(x) \in K[x]$ splits over L.
- L is said to be **algebraically closed** if for each $f(x) \in L[x]$, $f(x)$ has a root in L.

Prop 5.3.1. Given L/K, if L is algebraically closed, then $L^{\text{alg}} \triangleq \{\, \alpha \in L \,|\, \alpha \text{ is algebraic over } K \,\}$ is an algebraic closure of K.

Proof. By prop 5.1.4, L^{alg} is a field, and by definition, L^{alg}/K is algebraic.

Now we show that for any $f(x) \in K[x]$, $f(x)$ splits over L. Using induction, $\deg f = 1$ is trivial. If $\deg f > 1$, then since $f(x) \in K[x] \subseteq L[x]$, f has a root in L, say α. so we could write $f(x) = (x-\alpha)g(x)$. Then $g(x) \in K(\alpha)[x] \subseteq L[x]$. By induction, $g(x)$ splits and hence $f(x)$ splits.

So for any $f(x) \in K[x]$, f splits over L. Write $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, then each α_i is algebraic over $K \implies \alpha_i \in L^{\text{alg}}$ and hence $f(x)$ splits over $L^{\text{alg}}[x]$. □

Coro 5.3.1. If K is algebraically closed, then K is an algebraic closure of K itself.

Prop 5.3.2. If L is an algebraic closure of K, then L is algebraically closed.

Proof. For $f(x) \in L[x]$, let α be a root of $f(x)$. Since $L(\alpha)/L$ and L/K is algebraic, by prop 5.1.6, $L(\alpha)/K$ is algebraic. So α must be in L, hence $f(x)$ has a root in L. □

Prop 5.3.3. The following are equivalent.

1. K has no nontrivial algebraic extension.
2. For all irreducible polynomial in $K[x]$ has degree 1.
3. Every polynomial of positive degree in $K[x]$ has at least one root in K.
4. Every polynomial of positive degree in $K[x]$ splits over K.

In below we would use the Zorn's lemma heavily.

Lemma 6 (Zorn's lemma)**.** Suppose a partially order set P has the property that every chain (i.e., a total order subset) has an upper bound in P, then the set P contains at least one maximal element.

Lemma 7. In a commutative ring R with 1, any proper ideal $I \subsetneq R$ is contained in a maximal ideal.

Proof. Consider $S = \{\, J \subsetneq R \mid I \subseteq J \,\} \neq \varnothing$ since $I \in S$. Define a partial order on S by $J_1 \preceq J_2 \iff J_1 \subseteq J_2$.

Given a chain $\{\, J_i \mid i \in \Lambda \,\}$, let $J = \bigcup_{i\in\Lambda} J_i$. J is an ideal, since if $x, y \in J$, then $x \in J_1, y \in J_2$. Let $\tilde{J} = \max(J_1, J_2)$, then $x, y \in \tilde{J}$ which implies $x + y \in \tilde{J}$, and it is easy to check that for any $x \in R, y \in J$, $xy \in J$.

Also, J is proper since $1 \notin J$, or else $1 \in J_i$ and thus $J_i = R$ which leads to a contradiction.

By Zorn's lemma, there exists a maximal element in S, and thus it is a maximal ideal which contains I. □

Theorem 49. If K is a field, then there exists an algebraic closure L of K.

Proof. Let $S = \{ x_f \mid f(x) \in K[x] \text{ with } \deg f \geq 1 \}$ be the set of variables indexed by non-constant polynomial in $K[x]$. Consider the polynomial ring $K[S]$ and $I = \langle f(x_f) : f \in K[x] \text{ with } \deg f \geq 1 \rangle$, which is an ideal in $K[S]$.

We claim that $I \neq K[S]$. If not, then $1 \in I \implies 1 = \sum_{i=1}^{n} g_i f_i(x_{f_i})$. Write $x_i \triangleq x_{f_i}$ for $i = 1, 2, \cdots, n$. Also, by definition g_i only involves a finite number of variable in S, so we could set $g_i \in K[x_1, x_2, \ldots, x_m]$ with $m \geq n$. That is, $1 = \sum_{i=1}^{n} g_i(x_1, x_2, \ldots, x_m) f_i(x_i)$. Let Σ be a splitting field for $f(x) = f_1(x) f_2(x) \cdots f_n(x)$ and define $\alpha_i \in \Sigma$ which satisfies $f_i(\alpha_i) = 0$ and $a_i = 0$ for $n + 1 \leq i \leq m$. Then $1 = \sum_{i=1}^{n} g(\alpha_1, \alpha_2, \ldots, \alpha_m) f_i(\alpha_i) = 0$, which leads to a contradiction.

By lemma 7, there exists a maximal ideal M s.t. $I \subseteq M$.

Consider $K \hookrightarrow F_1 \triangleq K[S]/M$, and then for all $f \in K[x]$, $f(\bar{x}_f) = \bar{0}$ in F_1. By induction, $\exists\, F_1 \subseteq F_2 \subseteq F_3 \subseteq \cdots$ which satisfies $f(x) \in F_n[x]$ has a root in F_{n+1} Let $F = \bigcup_{i=1}^{\infty} F_i$ which is algebraically closed since if $f(x) \in F[x]$ then $f(x) \in F_m[x]$ for some m and thus $f(x)$ has a root in $F_{m+1} \subseteq F$.

Finally $L \triangleq \{ \alpha \in F \mid \alpha \text{ is algebraic over } K \}$ is an algebraic closure of K. $\square$

Lemma 8. If L_1/K is algebraic and $\tau : K \to L_2$ is a non-zero homomorphism with L_2 being algebraically closed, then τ could be extend to $\sigma : L_1 \to L_2$.

Proof. Consider $S = \left\{ (M, \theta) \,\middle|\, K \subset M \subset L_1,\ \theta : M \to L_2 \text{ with } \theta\big|_K = \tau \right\}$, which is not an empty set since $(K, \tau) \in S$.

Define a partial order on S by $(M_1, \theta_1) \preceq (M_2, \theta_2) \iff M_1 \subseteq M_2 \wedge \theta_2\big|_{M_1} = \theta_1$. Given any chain $\{ (M_i, \theta_i) \colon i \in \Lambda \}$, let $N = \bigcup_{i=1}^{\infty} M_i$ and $\theta = \alpha :: N \mapsto \theta_i(\alpha)$ if $\alpha \in M_i$. It could be check easily that this map is well defined, and (N, θ) is a least upper bound in S for this chain. By Zorn's lemma, there exists a max element (M, σ) in S.

Now, if $M \neq L_1$, then pick $\alpha \in L_1 \setminus M$. Since L_1/K is algebraic, the minimal polynomial $m_{\alpha,K}$ exists. Since L_2 algebraically closed, $\bar{\sigma}(m_{\alpha,K})$ has a root in L_2, and thus by lemma 4, σ could be extend to $\sigma' : M(\alpha) \to L_2$ which contradicts the maximality of (M, σ). Thus $M = L_1$. $\square$

Theorem 50. Any two algebraic closures L_1, L_2 of K are isomorphic.

Proof. Consider the inclusion map $\mathrm{Id}_K :: K \hookrightarrow L_1$. By Lemma 8, Id_K could be extend to $\sigma :: L_2 \to L_1$ such that $\sigma\big|_K = \mathrm{Id}_K$. Since $\sigma \neq 0$, $\sigma(L_2) \cong L_2$. Also, L_2 is algebraically closed implies $\sigma(L_2)$ is algebraically closed. So for any $\alpha \in L_1$, α is algebraic over K and thus over $\sigma(L_2)$, which implies $\alpha \in \sigma(L_2)$, so σ is onto, hence σ is an isomorphism between L_1 and L_2. $\square$

Eg 5.3.1. Let p be a prime.

- Any finite field L with $\operatorname{char} L = p$, $L \cong \mathbb{F}_{p^n}$ for some $n \in \mathbb{N}$.
- $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle$ with $p = \alpha :: \mathbb{F}_{p^n} \mapsto \alpha^p :: \mathbb{F}_{p^n}$.
- A subfield L of $\mathbb{F}_{p^n}$ is isomorphic to $\mathbb{F}_{p^m}$ with $m \mid n$ since $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = d \rightsquigarrow p^{md} = p^n$.
- $\bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ is a field, and it is the algebraic closure of $\mathbb{F}_p$.

5.4 Separable extension

Def 84.

- α is separable over K if $m_{\alpha,K}$ is separable over K.

- L/K is called a **separable extension** if $\forall\, \alpha \in L$, α is separable over K.

Eg 5.4.1. Let $\operatorname{char} K = p$ and $K^p \subsetneq K$. Pick $b \in K \setminus K^p$ and consider L to be the splitting field of $x^p - b$ over K, say $\alpha \in L$ with $\alpha^p = b$. Notice that $x^p - b = x^p - a^p = (x-a)^p$, and $x^p - b$ is irreducible in K, or else if $x^p - b = g(x)h(x)$ in $K[x]$, then write $g(x) = (x-\alpha)^k, h(x) = (x-\alpha)^{n-k}$, but then expand $g(x)$ and we would get $\alpha^k \in K$, since $\alpha^p \in K$ and $\gcd(k,p) = 1$ implies $\alpha \in K$ which leads to a contradiction.

By above we know that $x^p - b$ is inseparable.

Def 85. K is said to be *perfect* if either $\operatorname{char} K = 0$ or "$\operatorname{char} K = p$ and $K = K^p$".

Eg 5.4.2. If $\operatorname{char} K = p$ and $K/\mathbb{F}_p$ is algebraic, then K is perfect.

Proof. Consider $\begin{aligned}\sigma_p : K &\to K \\ \alpha &\mapsto \alpha^p\end{aligned}$, which is a monomorphism which fixes $\mathbb{F}_p$. Since $K/\mathbb{F}_p$ is algebraic, by the exercise problem, σ_p is an automorphism, so $K = K^p$. □

Fact 5.4.1. K is perfect if and only if for any irreducible polynomial $f(x) \in K[x]$, f is separable.

Also, we can find that an irreducible polynomial $f(x) \in K[x]$ is not separable over K if and only if $\operatorname{char} K = p > 0$ and $f(x) = g(x^p)$ for some $g(x) \in K[x]$, where $g(x)$ is irreducible and not all coefficients of g is in K^p.

Finally, if $\operatorname{char} K = 0$, then K is separable.

Prop 5.4.1. Give $K(\alpha)/K$ with degree $m_{\alpha,K} = d$ and $\tau :: K \to L \neq 0$. If α is separable over K and $\bar{\tau}(m_{\alpha,K})$ splits over L, then there are exactly d monomorphisms $\sigma :: K(\alpha) \to L$ with $\sigma\big|_K = \tau$.

Otherwise, if α is not separable or $\bar{\tau}(m_{\alpha,K})$ doesn't split over L, then there are $r < d$ such monomorphisms.

Proof. Observe that $m_{\alpha,K}$ is separable over K if and only if $\bar{\tau}(m_{\alpha,K})$ is separable over $\tau(K)$. Extend K to Σ, $\tau(K)$ to Σ', where Σ, Σ' are the splitting field of $m_{\alpha,K}$ and $\bar{\tau}(m_{\alpha,K})$, respectively. Since $K \cong \tau(K)$, by theorem 43, $\Sigma \cong \Sigma'$. Let τ' be the isomorphism which is an extension of τ.

If $m_{\alpha,K} = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_d)$, then $\bar{\tau}(m_{\alpha,K}) = (x-\tau'(\alpha_1))(x-\tau'(\alpha_2))\cdots(x-\tau'(\alpha_n))$. where $\tau' :: \Sigma \xrightarrow{\sim} \Sigma'$ and $\alpha_i \neq \alpha_j \iff \tau'(\alpha_i) \neq \tau'(\alpha_j)$. Thus if α is separable, $\bar{\tau}(m_{\alpha,K})$ has d distinct roots in L. By corollary 5.1.2, there are exactly d monomorphisms σ with $\sigma\big|_K = \tau$.

Otherwise, there are r roots in L where $r < d$, and thus there are $r < d$ such monomorphisms. □

Prop 5.4.2. Let $[K' : K] = d$ and $\tau :: K \to L \neq 0$. Then K'/K is separable and $\forall\, \alpha \in K'$, $\bar{\tau}(m_{\alpha,K})$ splits over L, if and only if there are exactly d monomorphisms $\sigma :: K' \to L$ with $\sigma\big|_k = \tau$. Otherwise $\exists\, r < d$ of such monomorphisms.

Proof. By induction on d, if $d = 1$ we could simply let $\sigma = \tau$.

For $d > 1$, consider $\alpha \in K' \setminus K$. By prop 5.4.1, there exists exactly $[K(\alpha) : K]$ monomorphisms $\tau_1 : K(\alpha) \to L$.

Now, for any $\beta \in K'/K(\alpha)$, $m_{\beta,K(\alpha)} \mid m_{\beta,K}$ and thus $m_{\beta,K(\alpha)}$ is separable and $\bar{\tau}_1(m_{\beta,K(\alpha)})$ splits over L since $\bar{\tau}(m_{\beta,K})$ splits. These imply that $K'/K(\alpha)$ is separable and $\forall\, \beta \in K'$, $m_{\beta,K(\alpha)}$ splits over L. Thus, $K(\alpha)$ satisfies the hypothesis, and by induction, there are exactly $[K' : K(\alpha)]$ monomorphisms $\sigma :: K' \to L$ such that $\sigma\big|_{K(\alpha)} = \tau_1$, thus there are $[K' : K(\alpha)][K(\alpha) : k] = [K' : K]$ such monomorphisms.

Otherwise, we could choose $\alpha \in K'$ such that $\bar{\tau}(m_{\alpha,K})$ has fewer then $[K(\alpha):K]$ roots in L, then there are $r' < [K(\alpha):K]$ monomorphism $\tau_1 :: K(\alpha) \to L$. By induction, each τ_1 has r'' extensions $\sigma :: K' \to L$ and $r'' \leq [K' : K(\alpha)]$ Hence the number of monomorphism equals $r'r'' < [K' : K]$. $\square$

Lemma 9. If $K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K$ is algebraic and L is a splitting field of $f(x) = \prod_{i=1}^{n} m_{\alpha_i,K}$ over K, then for all $\beta \in K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $m_{\beta,K}$ also splits over L.

Proof. Let $L = K(R)$ with R being the set of all roots of $f(x)$. Pick any root γ of $m_{\beta,K}$. Observe the following diagram:

$$\begin{tikzcd}
K(R) \arrow[rr, "\sim", "(2)\ \sigma"'] & & K(R,\gamma) \\
K(\beta) \arrow[u, hook] \arrow[rr, "\sim", "(1)\ \tau"'] & & K(\gamma) \arrow[u, hook] \\
& K \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Where (1) holds because these fields are both isomorphic to $K[x]/\langle m_{\beta,K} \rangle$.
(2) holds because τ obviously fixes K, and hence $K(R)$ is a splitting field of f and $K(R,\gamma)$ is a splitting field of $\bar{\tau}(f)$. By theorem 43, $K(R)$ and $K(R,\gamma)$ are isomorphic.

Thus we have $[K(R):K] = [K(R,\gamma):K]$ along with $[K(R,\gamma):K] = [K(\gamma,R):K(R)][K(R):K]$. This implies $[K(\gamma,R):K(R)] = 1$, hence $\gamma \in R$. $\square$

Theorem 51. Given $K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K$, if α_i is separable over $K_{i-1} \triangleq K(\alpha_1, \ldots, \alpha_{i-1})$, then $K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K$ is separable.

Proof. Let L be a splitting field of $f(x) = \prod m_{\alpha_i,K}$.

We claim that there are $[K_j : K]$ monomorphisms $\tau_j :: K_j \to L$ with $\tau_j\big|_K = \mathrm{Id}_K$. Use induction on j, if $j = 0$, then there are only 1 such monomorphism, namely itself Id_K.

For $j > 0$, observe that $m_{\alpha_j,K_{i-1}} \mid m_{\alpha_j,K}$, and since $\bar{\tau}_{j-1}(m_{\alpha_j,K}) = m_{\alpha_j,K}$ splits over L, $m_{\alpha_j,K_{i-1}}$ also splits over L. By hypothesis, α_j is separable over K_{j-1}, so by prop 5.4.1, there are $[K_j : K_{j-1}]$ such monomorphisms $\tau_j :: K_j \to L$ with $\tau_j\big|_{K-1} = \tau_{j-1}$. By induction, there are $[K_{j-1} : K]$ monomorphisms $\tau_{j-1} :: K_{j-1} \to L$ with $\tau_j\big|_K = \mathrm{Id}_K$. Compose these monomorphisms, we know that there exist exactly $[K_j : K_{j-1}][K_{j-1} : K] = [K_j : K]$ monomorphisms $\tau_j :: K_j \to L$ such that $\tau_j\big|_K = \mathrm{Id}_K$.

So there are exactly $[K_n : K]$ monomorphisms $\tau :: K(\alpha_1, \ldots, \alpha_n) \to L$ with $\tau\big|_K = \mathrm{Id}_K$. By prop 5.4.2, $K(\alpha_1, \ldots, \alpha_n)$ is separable. $\square$

Theorem 52. L/K is separable if and only if L/M, M/K are separable.

Proof. "$\Rightarrow$": If L/K is separable, then M/K is obviously separable. For any $\beta \in L$, $m_{\beta,M} \mid m_{\beta,K}$ so $m_{\beta,M}$ is separable which implies L/M is separable.

"$\Leftarrow$": For any $\alpha \in L$, write $m_{\alpha,M} = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then $m_{\alpha,M}$ is separable implies α is separable over $K(a_0, \ldots, a_{n-1})$. Note that $a_0, \ldots, a_{n-1} \in M$ are separable over K. By theorem 51, $K(a_0, a_1, \ldots, a_{n-1}, \alpha)/K$ is separable, hence each α is separable over K, thus L/K is separable. $\square$

Theorem 53 (Primitive element theorem)**.**

- A finite extension is simple if and only if there are only finitely many intermediate fields.
- If L/K is finite and separable, then L/K is simple.

5.5 Normal extension

Def 86. L/K is called a **normal extension** if $\forall\, \alpha \in L$, $m_{\alpha,K}$ splits over L.

Theorem 54. L is a splitting field of some polynomial $f(x)$ over K if and only if L/K is finite and normal.

Proof. "$\Rightarrow$": Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f, so $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, and L is also a splitting field of $\prod m_{\alpha_i,K}$ since $m_{\alpha_i,K} \mid f$. By lemma 9, for any β in L, $m_{\beta,K}$ splits, thus L/K is normal and also finite obviously.

"$\Leftarrow$": Since L/K is a finite extension, we could write $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let $f = \prod m_{\alpha_i,K}$, then since L/K normal, each $m_{\alpha_i,K}$ splits. It is also easy to see that L is the smallest field where f splits, thus L is a splitting field of f. $\square$

Remark 29. If L/K is normal, then for any M with $K \subset M \subset L$, we have L/M is normal, this is because $\forall\, \alpha$, $m_{\alpha,M} \mid m_{\alpha,K}$, and thus $m_{\alpha,M}$ splits since $m_{\alpha,K}$ splits.

But M/K need not to be normal. For example, Let $K = \mathbb{Q}$, L be the splitting field of $x^3 - 2$, by theorem 54 L/K is normal. Then $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega \triangleq \mathrm{e}^{2\pi \mathrm{i}/3}$. Let $M = \mathbb{Q}(\sqrt[3]{2})$ then $m_{\sqrt[3]{2},K}$ doesn't split in M, so M/K is not normal.

Prop 5.5.1. Let L/K be a finite, normal extension and $L \supset M \supset K$, then the following are equivalent.

(a) M/K is normal.

(b) $\forall\, \sigma \in \operatorname{Aut}(L/K)$, $\sigma(M) \subset M$.

(c) $\forall\, \sigma \in \operatorname{Aut}(L/K)$, $\sigma(M) = M$.

Proof. (a) $\Rightarrow$ (b): $\forall\, \alpha \in M$, $m_{\alpha,K}(\sigma(\alpha)) = \sigma(m_{\alpha,K}(\alpha)) = 0$. So $\sigma(\alpha)$ is a root of $m_{\alpha,K}$. Since M/K normal, $m_{\alpha,K}$ splits in M and thus each root of $m_{\alpha,K}$ is in M, hence $\forall\, m$, $\sigma(m) \in M \implies \sigma(M) \subset M$.

(b) $\Rightarrow$ (c): Since L/K is algebraic and σ is 1-1, by a homework problem, σ onto.

(c) $\Rightarrow$ (a): For any $\alpha \in M$, let $\beta \in L$ be a root of $m_{\alpha,K}$. By theorem 54, we could assume L is a splitting field of f over K. Consider the following diagram,

$$\begin{tikzcd}
L \arrow[rr, "\sim", "\sigma"'] & & L \\
K(\alpha) \arrow[u, hook] \arrow[rr, "\sim", "\tau"'] & & K(\beta) \arrow[u, hook] \\
& K \arrow[ul, hook] \arrow[ur, hook] &
\end{tikzcd}$$

Where isomorphism τ with $\tau(\alpha) = \beta$ exists since α, β share the same minimal polynomial, and σ with $\sigma\big|_K = \tau$ exists by theorem 43. Since $\sigma \in \operatorname{Aut}(L/K)$, $\beta = \sigma(\alpha) \in M$, thus M/K normal. $\square$

Def 87. Let L/K is called a *Galois* extension if L/K is finite, normal and separable. That is, L is a splitting field of some separable polynomial over K.

Theorem 55. If L/K is Galois, then $|\operatorname{Aut}(L/K)| = [L:K]$. Otherwise, $|\operatorname{Aut}(L/K)| < [L:K]$.

Proof. Since L/K is normal, for any α, $m_{\alpha,K}$ splits over L. Since L/K is separable, $m_{\alpha,K}$ has no multiple roots. So there are exactly $[L:K]$ extensions $\sigma :: L \to L$ of Id_K. $\square$

Def 88. Given a field L, define the **fixed field** of G by $L^G \triangleq \{\, \alpha \in L \mid \sigma(\alpha) = \alpha, \forall\, \sigma \in G \,\}$.

Theorem 56. If G is a subgroup of $\mathrm{Aut}(L)$ with $|G| < \infty$, then $|G| = [L : L^G]$, $G = \mathrm{Aut}(L/L^G)$ and L/L^G is Galois.

Proof. First we prove that $[L : L^G] \le |G|$ by contradiction. Assume $|G| < [L :^G]$.
Let $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ and $\alpha_1, \alpha_2, \dots, \alpha_{n+1} \in L$ with $\{\, \alpha_i \,\}$ are linearly independent over L^G.

Consider the equations

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ \sigma_2(\alpha_1)x_1 + \cdots + \sigma_2(\alpha_{n+1})x_{n+1} &= 0 \\ \qquad\qquad \vdots & \ \vdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{cases}$$

Since the number of variables is more than the number of equations, there is a non-trivial solution. Choose one solution $(a_1, \dots, a_{n+1})$ having the least amount of nonzero element. By reordering, we could assume the solution is $(a_1, a_2, \dots, a_m, 0, 0, \dots, 0)$ and it is no harm to assume $\sigma_1 = 1_G$. If $m = 1$, then $\sigma_1(\alpha_1)a_1 = \alpha_1 a_1 = 0 \implies a_1 = 0$, which is a contradiction.

So assume that $m > 1$, we have

$$\begin{cases} \sigma_1(\alpha_1)a_1 + \cdots + \sigma_1(\alpha_m)a_m &= 0 \\ \sigma_2(\alpha_1)a_1 + \cdots + \sigma_2(\alpha_m)a_m &= 0 \\ \qquad\qquad \vdots & \ \vdots \\ \sigma_n(\alpha_1)a_1 + \cdots + \sigma_n(\alpha_m)a_m &= 0 \end{cases}$$

By multipling a_m^{-1}, we could assume $a_m = 1$. The equation about σ_1 gives $\alpha_1 a_1 + \cdots + \alpha_m a_m = 0$, since α_i is linearly independent, one of $\{\, a_i \,\}$, say a_k is not in L^G, and thus there exists t such that $\sigma_t(a_k) \ne a_k$. Apply σ_t to each equation, we have

$$\sigma_t\sigma_i(\alpha_1)\sigma_t(a_1) + \cdots + \sigma_t\sigma_i(\alpha_m)\sigma_t(a_m) = 0, \quad \forall\, 1 \le i \le n$$

But since $\{\sigma_t\sigma_1, \dots, \sigma_t\sigma_n\} = \{\sigma_1, \dots, \sigma_n\}$, $(\sigma_t(a_1), \sigma_t(a_2), \dots, \sigma_t(a_m), 0, \dots, 0)$ is a solution and thus $(a_1 - \sigma_t(a_1), \dots, a_m - \sigma_t(a_m), 0, \dots)$ is also a solution of the equations. Since $\sigma_t(a_k) \ne a_k$, the solution is not trivial, and because $a_m = 1$, $a_m - \sigma_t(a_m) = 0$. Hence this solution has $m-1$ nonzero element, which contradicts the minimality of the original solution. Thus $[L : L^G] \le \mathrm{Aut}(L/L^G)$.

Finally, $|\mathrm{Aut}(L/L^G)| \le [L : L^G]$ by theorem 51, thus $|G| \le |\mathrm{Aut}(L/L^G)| \le [L : L^G] \le |G|$, hence they are all equal. ☐

Def 89. Let $f(x) \in K[x]$ and L be a splitting field of $f(x)$ over K. We use $\mathrm{Gal}(L/K)$ to denote $\mathrm{Aut}(L/K)$ and call it the **Galois group** of $f(x)$.

Prop 5.5.2. Let $f(x) \in \mathbb{Q}[x]$ be irreducible polynomial of degree p where p is a prime. If $f(x)$ has exactly $p-2$ roots and 2 complex roots, then the Galois group of $f(x)$ is S_p.

Proof. Let L be a splitting field of f over $\mathbb{Q}$ and $R = \{\alpha_1, \alpha_2, \dots, \alpha_p\}$ be the set of all roots of $f(x)$. Since $f(x)$ is irreducible, $f(x)/a_p = m_{\alpha_i,\mathbb{Q}}$, $\forall\, i$. By lemma 4, for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, σ sends α_i to another root α_j. Also, $\{\alpha_i\}$ generates L so $G \triangleq \mathrm{Gal}(L/\mathbb{Q}) \le S_p$.

Now, we define an equivalence relation on R such that $\alpha_i \sim \alpha_j \iff (\alpha_i\ \alpha_j) \in G$, that is, $\exists\, \sigma \in G$ such that $\sigma(\alpha_i) = \alpha_j, \sigma(\alpha_j) = \alpha_i$ and $\sigma(\alpha_t) = \alpha_t$, $\forall\, t \ne i, j$.

We claim that each equivalence class has the same size. Let $[\alpha_i], [\alpha_j]$ be two equivalence classes. Since α_i, α_j share the same minimal polynomial, by lemma 4, $\exists\, \sigma$, $\sigma(\alpha_i) = \alpha_j$, and σ sends $[\alpha_i]$

to $[\alpha_j]$, since if $\alpha_k \in [\alpha_i]$, $(\alpha_i\ \alpha_k) \in G$ and thus $\sigma(\alpha_i\ \alpha_k)\sigma^{-1} = (\alpha_j\ \sigma(\alpha_k)) \in G$. Since σ is 1-1, $\big|[\alpha_i]\big| \le \big|[\alpha_j]\big|$, and by symmetry we have $\big|[\alpha_i]\big| = \big|[\alpha_j]\big|$.

But then if $[\alpha_i] = n$, $p = |R| = \sum\big|[\alpha_j]\big| = kn$, so either there are p equivalence classes with size of 1, which is impossible since the two complex root are equivalent by conjugation, or there are is one equivalence class, which means that every 2 cycle is in G, and thus $G = S_p$. $\square$

5.6 Fundamental theorem of Galois theory

Theorem 57 (Main theorem). Let L/K be a Galois extension, where L be a splitting field of a separable polynomial f, and let $G = \mathrm{Gal}(L/K)$. Then:

(1) There is a 1-1 correspondence from the set of intermediate field to the set of subgroup:

$$\begin{array}{ccc} \{M : K \subseteq M \subseteq L\} & \longleftrightarrow & \{H : H \le G\} \\ M & \longmapsto & \mathrm{Gal}(L/M) \\ L^H & \longleftarrow\!\shortmid & H \end{array}$$

Proof. We check these two mappings are the inverse of each other.

By theorem 56, $\mathrm{Gal}(L/L^H) = H$.

Now we have $M \subseteq L^{\mathrm{Gal}(L/M)}$. Since L/M is galois, $[L : M] = |\mathrm{Gal}(L/M)|$. By theorem 56 again, $|\mathrm{Gal}(L/M)| = [L : L^{\mathrm{Gal}(L/M)}]$, thus $[L : M] = [L : L^{\mathrm{Gal}(L/M)}] \implies M = L^{\mathrm{Gal}(L/M)}$. $\square$

(2) If $M_1 = L^{H_1}, M_2 = L^{H_2}$, then $M_1 \subseteq M_2 \iff H_2 \le H_1$.

Proof. Obvious. $\square$

(3) If $M = L^H$, then M/K is normal if and only if $H \lhd G$.

Proof. For any $\sigma \in G$,

$$\begin{aligned} \tau \in \mathrm{Gal}(L/\sigma(M)) &\iff \tau(\sigma(x)) = \sigma(x),\ \forall\, x \in M \\ &\iff \sigma^{-1}\tau\sigma(x) = x,\ \forall\, x \in M \\ &\iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M) \\ &\iff \tau \in \sigma\,\mathrm{Gal}(L/M)\sigma^{-1} \end{aligned}$$

By prop 5.5.1, M/K is normal if and only if for all $\sigma \in G$, $\sigma(M) = M \iff \mathrm{Gal}(L/M) = \mathrm{Gal}(L/\sigma(M))$. By the discussion above, $\mathrm{Gal}(L/\sigma(M)) = \sigma\,\mathrm{Gal}(L/M)\sigma^{-1} = \sigma H\sigma^{-1}$. Hence M/K is normal $\iff H = \sigma H \sigma^{-1}, \forall\, \sigma \in G \iff H \lhd G$. $\square$

(4) If $H \lhd G$, then $G/H \cong \mathrm{Gal}(M/K)$.

Proof. Since $H \lhd G$, by (3) we know that M/K is Galois. Define $\varphi = \sigma :: \mathrm{Gal}(L/K) \mapsto \sigma\big|_M :: \mathrm{Gal}(M/K)$. The mapping is well defined since $\sigma(M) = M$ (by prop 5.5.1). Also, this map is onto since by corollary 43, each $\tau \in \mathrm{Gal}(M/K)$ could be extended to $\sigma \in \mathrm{Gal}(L/K)$ because $\bar{\tau}(f) = f$. Finally, notice that $\ker\varphi = H$, thus by the first isomorphism theorem, $G/H \cong \mathrm{Gal}(M/K)$. $\square$

(5) If $M_1 = L^{H_1}, M_2 = L^{H_2}$, then $M_1 \cap M_2 = L^{\langle H_1, H_2\rangle}$ and $M_1M_2 = L^{H_1 \cap H_2}$.

Theorem 58. Let L/K be Galois, and N/K be any extension, then LN/N is galois and $\mathrm{Gal}(LN/N) \cong \mathrm{Gal}(L/L \cap N)$ by the isomorphism $\varphi : \sigma \mapsto \sigma\big|_L$.

Proof. Let L be a splitting field of the separable polynomial $f(x)$ over K, say $L = K(\alpha_1, \ldots, \alpha_n)$. Then $LN = N(\alpha_1, \ldots, \alpha_n)$, which can be regarded as a splitting field of $f(x)$ over N. Thus by theorem 54, LN/N is Galois.

Now we check that φ is well defined, notice that $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0$ since σ fixes K, and thus f sends α_i to some α_j. Also, $\{\alpha_i\}$ generate L over K, thus $\sigma\big|_L(L) = L$.

If $\sigma\big|_L = \mathrm{Id}_L$, then $\sigma(\alpha_i) = \alpha_i$, $\forall\, i$. Since $\{\alpha_i\}$ generate LN over N, $\sigma = \mathrm{Id}_{LN}$. Thus φ is 1-1.

Finally, let $H = \operatorname{Im} \varphi$, we claim that $L^H = L \cap N$, since

$$\begin{aligned}
\alpha \in L^H &\iff \alpha \in L \text{ and } \forall\, \sigma \in \mathrm{Gal}(LN/N),\ \sigma\big|_L(\alpha) = \alpha \\
&\iff \alpha \in L \text{ and } \forall\, \sigma \in \mathrm{Gal}(LN/N),\ \sigma(\alpha) = \alpha \\
&\iff \alpha \in L \text{ and } \alpha \in (LN)^{\mathrm{Gal}(LN/N)} \\
&\iff \alpha \in L \text{ and } \alpha \in N \iff \alpha \in L \cap N
\end{aligned}$$

□

Remark 30. If L/K is Galois and N/K is finite, then $[LN : K] = [L : K][N : K]/[L \cap N : K]$.

Proof.

$[LN : K]/[N : K] = [LN : N] = \mathrm{Gal}(LN/N) = \mathrm{Gal}(L/L \cap N) = [L : L \cap N] = [L : K]/[L \cap N : K]$

and the proof is completed. □

5.7 Abelian extension

Def 90. L/K is called an abelian extension if L/K is Galois and $\mathrm{Gal}(L/K)$ is abelian.

Eg 5.7.1. For an extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of a finite field, $\mathbb{F}_{q^n}$ is a splitting field of $x^{q^n} - x$ over $\mathbb{F}_p$, so $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois by theorem 54. By theorem 46, we know that $\mathrm{Gal}(F_{q^n}/F_q) = \langle \sigma_q \rangle$ is a cyclic group.

Def 91.

- The cyclotomic field $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$.
- ζ is called an nth root of unity if $\zeta^n = 1$. $\mathcal{U} = \langle \zeta \rangle$ is the multiplicative group of nth roots of unity.
- ζ_n is called a primitive nth root of unity if $\zeta^n = 1$ but $\zeta^m \neq 1$, $\forall\, 0 < m < n$.
- The nth cyclotomic polynomial is defined as

$$\Phi_n \triangleq \prod_{\gcd(k,n)=1} (x - \zeta_n^k) \implies \deg \Phi_n = \varphi(n)$$

Prop 5.7.1.

- $x^n - 1 = \prod_{d|n} \Phi_d$.

  Proof. First, Both sides have no multiple root. Then since $\alpha^n = 1 \iff \mathrm{ord}_\times(\alpha) \mid n$, we know that two sides has equal roots. □

- $\Phi_n \in \mathbb{Z}[x]$.

  Proof. By induction on n. $n = 1$ is trivial. Assume that the statement is true for all $k < n$, then since

$$x^n - 1 = \Phi_n \prod_{d|n, d<n} \Phi_d \triangleq \Phi_n \Phi_{<n}$$

  But notice that $\Phi_{<n}$ is monic, so by the long division algorithm, it is easy to see that $\Phi_n = (x^n - 1)/\Phi_{<n}$ has all coefficients in $\mathbb{Z}$. □

- Φ_n is irreducible.

  Proof. Suppose $\Phi_n = f(x)g(x)$ with f irreducible, and both f, g are monic. By Gauss's lemma, we could assume $f(x), g(x) \in \mathbb{Z}[x]$. Let ζ_n be a primitive nth root of unity which satisfied $f(\zeta_n) = 0$ and p be a prime with $p \nmid n$.

  Assume that $g(\zeta_n^p) = 0$, $m_{\zeta_n, \mathbb{Q}} = f \implies f \mid g(x^p)$, say $g(x^p) = f(x)h(x)$. By the long division algorithm, we know that $h(x) \in \mathbb{Z}[x]$, since $f(x) \in \mathbb{Z}[x]$ and monic.

  In $\mathbb{Z}/p\mathbb{Z}[x]$, we have $\bar{g}(x)^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$, which implies $\bar{g}, \bar{f}$ has common root, thus $\bar{\Phi}_n = \bar{f}\bar{g}$ and hence $x^n - \bar{1}$ has a multiple root. But $(x^n - \bar{1})' = nx^{n-1} \neq 0$, and 0 is not a root of $x^n - \bar{1}$, which leads to a contradiction.

  So we conclude that $f(\zeta_n^p) = 0$ for any $p \nmid n$, which could be extended and show that $f(\zeta_n^k) = 0$ for any $\gcd(k, n) = 1$, thus $f = \Phi_n$. □

- $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois with $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$.
- $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Let $\sigma_k = (\zeta_n \mapsto \zeta_n^k) \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The isomorphism is given by $\sigma_k \mapsto \bar{k}$. Clearly, it is a homomorphism since $\sigma_k\sigma_h = (\zeta_n \mapsto \zeta_n^{kh}) = \sigma_{kh}$. Also $\sigma_k = 1 \iff \bar{k} = 1$. Finally, $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |\mathbb{F}_n^\times| = \varphi(n)$, so the map is onto. $\square$

- Suppose $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ with $p_1, \ldots, p_k$ are distinct primes. Define $L_i \triangleq \mathbb{Q}\big(\zeta_{p_i^{n_i}}\big)$. Obviously, $L_i \subseteq \mathbb{Q}(\zeta_n)$ hence $L_1 L_2 \cdots L_k \subseteq \mathbb{Q}(\zeta_n)$, but $\zeta_n = \zeta_{p_1^{n_1}} \zeta_{p_2^{n_2}} \cdots \zeta_{p_k^{n_k}}$, so $L_1 L_2 \cdots L_k \supseteq \mathbb{Q}(\zeta_n)$. Thus we have $L_1 L_2 \cdots L_k = \mathbb{Q}(\zeta_n)$.

Eg 5.7.2. Let $n = p$ be a prime.

- $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \mathbb{F}_p^\times = \mathbb{Z}/(p-1)\mathbb{Z}$.
- For $H \leq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we shall find $\mathbb{Q}(\zeta_p)^H$. Let $\alpha = \sum_{\tau \in H} \tau(\zeta_p)$, then it is easy to see that $\alpha \in \mathbb{Q}(\zeta_p)^H$. Also, since $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ is linearly independent, so if some $\sigma \in G$ satisfy $\sigma(\alpha) = \alpha$, then since both $\sigma(\alpha), \alpha$ are a sum of linearly independent elements, σ must send ζ_p to an element $\tau(\zeta_p)$ for some $\tau \in H$, then $\sigma = \tau \implies \sigma \in H$. Thus $\mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\alpha)$.

Lemma 10. If L_1/K, L_2/K are Galois, then $L_1 \cap L_2/K$, L_1L_2/K are Galois and

$$\mathrm{Gal}(L_1L_2/K) \cong \left\{ (\sigma, \tau) \mid \sigma\big|_{L_1 \cap L_2} = \tau\big|_{L_1 \cap L_2} \right\} \leq \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

In particular, if $L_1 \cap L_2 = K$, then $\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

Proof. We know that $L_1 \cap L_2/K$ is finite and separable. Also, for each $\alpha \in L_1 \cap L_2$, $m_{\alpha,K}$ splits in both L_1, L_2 since they are normal, thus $m_{\alpha,K}$ splits in $L_1 \cap L_2$, hence $L_1 \cap L_2/K$ is galois.

Similary, L_1L_2 is finite and separable. Let L_1 be the splitting field of f_1, and L_2 be the splitting field of f_2, then L_1L_2 is the splitting field of the square-free part of f_1f_2, hence L_1L_2/K normal.

Define $\varphi = \sigma :: \mathrm{Gal}(L_1L_2/K) \mapsto \left(\sigma\big|_{L_1}, \sigma\big|_{L_2}\right) :: \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$. Since L_1, L_2 are normal, by proposition 5.5.1, $\sigma\big|_{L_i}(L_i) = L_i$ so they are well-defined. Also, it is clear that the map is 1-1.

Now we count the number of the pair $(\sigma\big|_{L_1}, \sigma\big|_{L_2})$, There are $[L_1 : K]$ of $\tau = \sigma\big|_{L_1}$, and fixing one, each $\sigma\big|_{L_2}$ is an extension of $\tau\big|_{L_1 \cap L_2}$, so there are $[L_2 : L_1 \cap L_2]$ of such. On the other hand, we have $|\mathrm{Gal}(L_1L_2/K)| = [L_1L_2 : K] = [L_1L_2 : L_1][L_1 : K] = [L_2 : L_1 \cap L_2][L_1 : K]$, thus $\mathrm{Gal}(L_1L_2/K)$ and $\{ (\sigma\big|_{L_1}, \sigma\big|_{L_2}) \}$ has the same size, and hence the map is onto. $\square$

Back to our problem, $[L_1L_2 \cdots L_k : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \varphi(p_1^{n_1}) \cdots \varphi(p_k^{n_k}) = [L_1 : \mathbb{Q}][L_2 : \mathbb{Q}] \cdots [L_k : \mathbb{Q}]$, thus

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \cong \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p_1^{n_1}})/\mathbb{Q}\right) \times \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p_1^{n_2}})/\mathbb{Q}\right) \times \cdots \times \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p_1^{n_k}})/\mathbb{Q}\right)$$

Theorem 59. Let G be a finite abelian group. Then there exists a subfield L of a cyclotomic field satisfying $\mathrm{Gal}(L/\mathbb{Q}) \cong G$.

Proof. By the FTFGAG,

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

By dirichlet theorem, there are infinitely many prime p such that $n \mid p-1$. Let p_i be a prime such that $n_i \mid p_i - 1$ and all p_i are distinct. Then G is a subgroup of $\mathbb{Z}/(p_1-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_k-1)\mathbb{Z} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ where $n = p_1p_2 \cdots p_k$. $\square$

5.7.1 Kummer extension

In this section, we assume that $\operatorname{char} K \nmid n$ and ζ is a primitive nth root of unity.

Def 92.

- L/K is called a kummer extension of exponent n if $\zeta \in K$ and L is a splitting field of $(x^n - a_1)(x^n - a_2)\cdots(x^n - a_k)$ over K.
- Let $|G| < \infty$, the exponent $e(G)$ of G is the least positive integer m satisfying $g^m = 1$ for any $g \in G$.

Theorem 60. Let L be a splitting field of $x^n - a$ over K, then $\operatorname{Gal}(L/K(\zeta))$ is cyclic of degree dividing n. More over $x^n - a$ is irreducible over $K(\zeta) \iff [L : K(\zeta)] = n$.

Proof. If α is a root of $x^n - a$, then $\alpha, \alpha\zeta, \ldots, \alpha\zeta^{n-1}$ are roots of $x^n - a$, so $L = K(\alpha, \zeta) = K(\zeta)(\alpha)$.

Consider $\begin{array}{rcl} \varphi : \operatorname{Gal}(L/K(\zeta)) & \to & \mathbb{Z}/n\mathbb{Z} \\ (\alpha \mapsto \alpha\zeta^k) & \mapsto & \bar{k} \end{array}$. It is easy to see that φ is a homomorphism. Also, if $\varphi(\sigma) = 0$, $\sigma = (\alpha \mapsto \alpha) = \mathrm{Id}$. Thus φ is 1-1 and $\operatorname{Gal}(L/K(\zeta)) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$. $\square$

Def 93. L/K is called a cyclic extension if L/K is Galois and $\operatorname{Gal}(L/K)$ is cyclic.

Theorem 61. If L/K is a cyclic extension of degree n and $\zeta \in K$, then L is a splitting field of some irreducible polynomial $x^n - a$ over K.

Proof. Recall a result proved in HW problem: Distinct automorphisms of L are linearly independent over L.

Let $\operatorname{Gal}(L/K) = \langle \sigma \rangle$ with $\operatorname{ord}(\sigma) = n$. Then $\mathrm{Id}_L + \zeta\sigma + \zeta^2\sigma^2 + \cdots + \zeta^{n-1}\sigma^{n-1} \neq 0$

$$\implies \exists\, c \in L, \text{ s.t. } \alpha = c + \zeta\sigma(c) + \zeta^2\sigma^2(c) + \cdots + \zeta^{n-1}\sigma^{n-1}(c) \neq 0$$

Observe that $\sigma(\alpha) = \zeta^{-1}\alpha$, so $\alpha \notin K$. Also $\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^{-n}\alpha^n = \alpha^n$, so α^n is fixed by $\operatorname{Gal}(L/K)$, thus $a \triangleq \alpha^n \in K$, and hence $K(\alpha)$ is a splitting field of $x^n - a$ over K.

Now $\sigma(\alpha) = \zeta^{-1}\alpha \in K(\alpha)$, so $\sigma\big|_{K(\alpha)} \in \operatorname{Gal}(K(\alpha)/K)$. Also $\sigma^k(\alpha) = \zeta^{-k}\alpha \implies \operatorname{ord}(\sigma) = n$. Thus

$$n = [L : K] \geq [K(\alpha) : K] = \operatorname{Gal}(K(\alpha)/K) \geq n \implies L = K(\alpha)$$ $\square$

Theorem 62. Let L/K be a Galois extension such that $\operatorname{Gal}(L/K)$ is abelian of exponent n and $\zeta_n \in K$, then L/K is a Kummer extension.

Proof. By induction on $[L : K]$. If $[L : K] = 1$ then $L = K$ and is trivial.

Assume $[L : K] > 1$, then by FTFGAG, $G \triangleq \operatorname{Gal}(L/K) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$ with $d_i \mid d_{i+1}$. If $s = 1$ then the theorem degenerates to theorem 61.

So assume $s > 1$. Let $H = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{s-1}\mathbb{Z}, N = \mathbb{Z}/d_s\mathbb{Z}$ be the corresponding subgroup in $\operatorname{Gal}(L/K)$. Set $M = L^N$, we have $[M : K] \lneq [L : K]$. Since any subgroup of abelian group is normal, we have $\operatorname{Gal}(M/K) \cong \operatorname{Gal}(L/K)/\operatorname{Gal}(L/M) = G/N = H$.

Denote $m = d_{s-1}, n = d_s$, we have $m \mid n$. Then $\zeta_n \in K \implies \zeta_m = \zeta_n^{n/m} \in K$, thus we could pass down the induction, and assume M is a kummer extension which is a splitting field of $g = (x^m - b_1)(x^m - b_2)\cdots(x^m - b_{k-1})$ over K with each $b_i \in K$. Let $\alpha_1, \ldots, \alpha_{k-1}$ be all the roots of g, then α_i is also a root of $(x^n - b_1^{n/m})$. Thus if we define $a_i \triangleq b_i^{n/m}$, then M is also the splitting field of $(x^n - a_1)(x^n - a_2)\cdots(x^n - a_{k-1})$ over K since $\zeta_n \in K$.

Now, if $N = \langle \sigma \rangle$, then $G \cong H \times N = \{\sigma^k \tau : 0 \leq k < n, \tau \in H\}$. Since automorphisms are linearly independent, exists $c \in L$ satisfied

$$0 \neq \alpha = \sum_{\tau \in H} \tau(c) + \zeta \sum_{\tau \in H} \sigma\tau(c) + \cdots + \zeta^{n-1} \sum_{\tau \in H} \sigma^{n-1}\tau(c)$$

Then $\sigma(\alpha) = \zeta^{-1}\alpha$, so $\alpha \notin M$. Also $\sigma(\alpha^n) = \alpha^n$ and $\tau(\alpha^n) = \tau(\alpha)^n = \alpha^n$, so $a_k \triangleq \alpha^n \in K$. Thus $M(\alpha)$ is a splitting field of $(x^n - a_k)$ over M.

Finally, $n = [L : M] \geq [M(\alpha) : M] = |\mathrm{Gal}(M(\alpha)/M)| \geq n$, thus $L = M(\alpha)$, and hence L is a splitting field of $(x^n - a_1)(x^n - a_2) \cdots (x^n - a_k)$. □

Theorem 63. If L/K is a kummer extension of exponent n, then $\mathrm{Gal}(L/K)$ is abelian of exponent dividing n.

Proof. Let L be the splitting field of $(x^n - a_1)(x^n - a_2) \cdots (x^n - a_k)$ with $\alpha_i = \sqrt[n]{a_i}$. If $\sigma \in \mathrm{Gal}(L/K)$, then σ sends each α_i to some $\zeta^{k_{\sigma,i}}\alpha_i$. So $\sigma^n = \alpha_i \mapsto \zeta^{k_{\sigma,i} n}\alpha_i = \alpha_i \mapsto \alpha_i = \mathrm{Id}$ and $\sigma \circ \tau = \alpha_i \mapsto \zeta^{k_{\sigma,i}+k_{\tau,i}}\alpha_i = \tau \circ \sigma$. by the fact that $\{\, \alpha_i \,\}$ is the generating set of L. Hence $\mathrm{Gal}(L/K)$ is abelian and of exponent dividing n. □

5.7.2 Cubic equations

Lemma 11. Let $\mathrm{char}\, K \neq 2$ and $f(x) \in K[x]$ with $\deg f = n$. Let $L = K(\alpha_1, \ldots, \alpha_n)$ be a splitting field of L over K.

Define $\delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$, then $L^{\mathrm{Gal}(L/K) \cap A_n} = K(\delta)$. (Here $\mathrm{Gal}(L/K) \hookrightarrow S_n$)

Proof. Notice that any transposition maps δ to $-\delta$, so $\forall\, \sigma \in \mathrm{Gal}(L/K) \cap A_n$, $\sigma(\delta) = \delta$, thus $K(\delta) \subseteq L^{\mathrm{Gal}(L/K) \cap A_n}$.

Now, $\left|\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K) \cap A_n\right|$ is either 1 or 2. If it is 1, then $\mathrm{Gal}(L/K) \leq A_n$,thus $\delta \in K$ and is trivial. Assume it is 2, then δ is not fixed by all permutation, thus $\delta \notin K$. But $D = \delta^2 \in K$ is the discriminant. So we have $2 = [K(\delta) : K] \leq [L^{\mathrm{Gal}(L/K) \cap A_n} : K] = \left|\mathrm{Gal}\left(L^{\mathrm{Gal}(L/K) \cap A_n}/K\right)\right| = 2$, thus $K(\delta) = L^{\mathrm{Gal}(L/K) \cap A_n}$. □

Prop 5.7.2. Let $f(x) = x^3 + px + q$ be irreducible in $K[x]$ and L be a splitting field,

- If $\mathrm{Gal}(L/K) \cong S_3$ then $\sqrt{D} \notin K$.
- If $\mathrm{Gal}(L/K) \cong A_3$ then $\sqrt{D} \in K$.

Def 94. $H \leq S_n$ is said to be transitive if for any i, j, there exists $\sigma \in H$ such that $\sigma(i) = j$.

Fact 5.7.1. Let $f(x)$ be a separable polynomial with degree n, then

$$f(x) \text{ is irreducible} \iff \text{The Galois group of } f \text{ is transitive in } S_n$$

5.8 Solution by radicals

Def 95.

1. Given L/K and $\alpha \in L$, α is called a radical over K if $\alpha^n \in K$ for some $n \in \mathbb{N}$.
2. L/K is called an extension by radicals if there exist $L = L_n \supset L_{n-1} \supset \cdots \supset L_1 \supset L_0 = K$ s.t. $\forall\, i = 1, \ldots, n, \quad L_i = L_{i-1}(\alpha_i)$ with α_i a radical over L_{i-1}.
3. $f(x) \in K[x]$ is solvable by radicals if there exists L/K, an extension by radicals, s.t. f splits over L.

Def 96. (Recall) Let G be a finite group. G is solvable if $\exists\ \{1\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_0 = G$ s.t. G_{i-1}/G_i is cyclic $\forall\, i$.

Lemma 12. Given a Galois extension L/K and $M = L(\alpha)$ is an extension by a radical, where $\alpha^n = a \in L$. Assume that $\operatorname{char} K \nmid n$. Then $\exists\ N$ s.t. N/M is an extension by radicals and N/K is Galois and N contains ζ_n.

Proof. We know that $M(\zeta_n) = L(\zeta_n, \alpha)$ is a splitting field of $x^n - a$ over L. If we set

$$f(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (x^n - \sigma(a)),$$

then the coefficients of $f(x)$ are elementary symmetric polynomials in $\{\, \sigma(a) \mid \sigma \in \mathrm{Gal}(L/K) \,\}$, which are fixed by $\mathrm{Gal}(L/K)$, so $f(x) \in K[x]$.

Let L be a splitting field of $g(x)$ over K. (since L/K is Galois) Choose N as a splitting field of $f(x)g(x)$ over K. By def., N/K is Galois. Let $L = K(\beta_1, \ldots, \beta_s)$ where $\beta_1, \ldots, \beta_s$ are the roots of $g(x)$, then

$$N = K\big(\beta_1, \ldots, \beta_s, \zeta_n, \alpha_\sigma : \sigma \in \mathrm{Gal}(L/K)\big), \qquad \alpha_\sigma^n = \sigma(a) \in L$$

So $N = M(\zeta_n, \alpha_\sigma : \sigma \in \mathrm{Gal}(L/K) \setminus \{\mathrm{Id}\}) \implies N/M$ is an extension by radicals. □

Lemma 13. Let $L = L_m \supset L_{m-1} \supset \cdots \supset L_0 = K$ s.t. $L_i = L_{i-1}(\alpha_i)$ with $\alpha^{n_i} = a_i \in L_{i-1}$. If $\operatorname{char} K \nmid n_1 n_2 \cdots n_m$, then there exists N/L s.t. N/K is a Galois extension by radicals and $\zeta_{n_i} \in N$, $\forall\, i = 1, \ldots, m$.

Proof. By induction on m. For $m = 1$, $L_1 \supset L_0 = K$ and $L_1 = L_0(\alpha_1) = K(\alpha_1)$ where $\alpha_1^{n_1} \in K$ for some $n_1 \in \mathbb{N}$. Set $N = L(\zeta_{n_1}) = K(\zeta_{n_1}, \alpha_1)$, done.

For $m > 1$, by induction hypothesis, $\exists\ N'/L_{m-1}$ s.t. N'/K is Galois extension by radicals and N' contains ζ_{n_i}, $\forall\, i = 1, \ldots, m-1$. By lemma 12, $\exists\ N/N'(\alpha_m)$ is an extension by radicals s.t. N/K is Galois and N contains ζ_{n_m}. □

Prop 5.8.1. Let $H \lhd G$. Then G is solvable $\iff$ $H, G/H$ are solvable.

Proof. "$\Leftarrow$": Let $q : G \to G/H$ be the quotient map, $Q = G/H$. The solvable series is given by

$$G = q^{-1}(Q) = q^{-1}(Q_0) \rhd q^{-1}(Q_1) \rhd \cdots \rhd q^{-1}(Q_n) = H = H_0 \rhd H_1 \rhd \cdots \rhd H_m = \{1\}$$

"$\Rightarrow$":
<u>Claim:</u> Define $G^{(i)} = [G^{(i-1)}, G^{(i-1)}], \quad i \in \mathbb{N}; G^{(0)} = G$. Then G is solvable $\iff$ $G^{(n)} = \{1\}$ for some n.

Proof. "$\Leftarrow$": O.K.

"$\Rightarrow$": Given $G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\}$ with G_{i-1}/G_i abelian. We have $G^{(1)} \leq G_1 \rightsquigarrow G^{(2)} \leq [G_1, G_1] \leq G_2 \rightsquigarrow \cdots \rightsquigarrow G^{(n)} \leq G_n = \{1\} \rightsquigarrow G^{(n)} = \{1\}$. $\square$

By the claim above:

- $H^{(n)} \leq G^{(n)} = \{1\} \rightsquigarrow H^{(n)} = \{1\} \implies H$ is solvable.
- $q([G,G]) = [q(G), q(G)] = [G/H, G/H] = (G/H)^{(1)} \rightsquigarrow \cdots \rightsquigarrow q(G^{(n)}) = (G/H)^{(n)} \implies G/H$ is solvable.

$\square$

Theorem 64 (Main Theorem)**.** Under some proper assumption on $\operatorname{char} K$, a separable polynomial $f(x) \in K[x]$ is solvable by radicals $\iff$ the Galois group of f is solvable.

Part A: Let $L = L_m \supset \cdots \supset L_0 = K$ s.t. $L_i = L_{i-1}(\alpha_i)$ with $\alpha^{n_i} = a_i \in L_{i-1}$ and $\operatorname{char} K \nmid n_1 \cdots n_m$. If a separable poly. $f(x) \in K[x]$ splits over L, then the Galois group of f over K is solvable.

Proof. By lemma 13, we can first extend the extension tower and thus assume that L/K is Galois with each ζ_{n_i} in L. Then each L/L_i is Galois. If we set $n = \operatorname{lcm}(n_1, \ldots, n_m)$, L also contains $\zeta = \zeta_n = \zeta_{n_1}^{r_1} \cdots \zeta_{n_m}^{r_m}$.

Consider $L = L(\zeta) \supset L_{m-1}(\zeta) \supset \cdots \supset L_0(\zeta) = K(\zeta)$ (Note that $K(\zeta) \supset K$ and L/K is Galois) and let $G_i = \operatorname{Gal}(L/L_i(\zeta))$ for each $i = 0, \ldots, m$.

Define $L_i' \triangleq L_i(\zeta)$ for all i. We can find that

- $G_m = \{1\}, G_0 = \operatorname{Gal}(L/K(\zeta))$.
- Since $\zeta_n \in L_{i-1}$, L_i/L_{i-1} is normal, so

$$G_{i-1}/G_i = \operatorname{Gal}(L/L_{i-1}')/\operatorname{Gal}(L/L_i') \cong \operatorname{Gal}(L_{i-1}'/L_i') = \operatorname{Gal}(L_i'(\alpha_i)/L_i')$$

  is cyclic.

So G_0 is solvable. Moreoevr, $K(\zeta)$ is a splitting field of $x^n - 1$ over K and $\operatorname{Gal}(K(\zeta)/K) \leq (\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian, so it is solvable. Also, $\operatorname{Gal}(K(\zeta)/K) \cong \operatorname{Gal}(L/K)/G_0$ is solvable. $\implies \operatorname{Gal}(L/K)$ is solvable. Let N be a splitting field of f over $K \rightsquigarrow L \supset N \rightsquigarrow \operatorname{Gal}(N/K) \cong \operatorname{Gal}(L/K)/\operatorname{Gal}(L/N)$.

By prop 5.8.1, $\operatorname{Gal}(N/K)$ is solvable. $\square$

Part B: Let $f \in K[x]$ be separable and L be a splitting field of f over K. Assume $\operatorname{char} K \nmid |\operatorname{Gal}(L/K)|$. If $\operatorname{Gal}(L/K)$ is solvable, then f is solvable by radicals.

Proof. Let $n = |\operatorname{Gal}(L/K)|$ and $\zeta = \zeta_n$. Let N be a splitting field of f over $K(\zeta)$, i.e. $N = LK(\zeta)$. $\implies \operatorname{Gal}(N/K(\zeta)) \cong \operatorname{Gal}(L/L \cap K(\zeta)) \leq \operatorname{Gal}(L/K)$.

So $\operatorname{Gal}(N/K(\zeta))$ is solvable, say $\operatorname{Gal}(N/K(\zeta)) = G_0 \rhd G_1 \rhd \cdots \rhd G_m = 1$, G_{i-1}/G_i is cyclic.

If we set $N_j = N^{G_j}$, then $N = N_m \supset N_{m-1} \supset \cdots \supset N_0 = K(\zeta)$ and $G_j = \operatorname{Gal}(N/N_j)$, $G_{i-1}/G_i \cong \operatorname{Gal}(N_i/N_{i-1})$ is cyclic $\implies N_i = N_{i-1}(\alpha_i), \alpha_i^{n_i} \in N_{i-1}$. (kummer extension)

Note that $n_i = [L_i : L_{i-1}] = \lvert G_{i-1}\rvert / \lvert G_i \rvert$ dividing $\lvert G_0\rvert$ and $\lvert G_0 \rvert \mid n$, so ζ_n generates ζ_{n_i} and $\operatorname{char} K \nmid n_i$.

$\implies N/K(\zeta)$ is an extension by radicals $\rightsquigarrow N/K$ is an extension by radicals. $\square$

Remark 31. In Part A of theorem 64, $\operatorname{Gal}(K(\zeta)/K) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ may be proper subgroup. We can check the if $[K(\zeta) : K] \overset{?}{=} 4 = \varphi(5)$.

5.9 Ruffini-Abel theorem

Theorem 65 (Main theorem)**.** Assume $\operatorname{char} F = 0$. The general equation of the n-th degree is not solvable by radicals if $n \geq 5$. In fact, let $f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^n t_n \in \underbrace{F(t_1, \ldots, t_n)}_{=K}[x]$ with $t_1, \ldots, t_n$ variables and L be a splitting field of f over K. Then $\operatorname{Gal}(L/K) \cong S_n$. S_n is not solvable for $n \geq 5$.

Lemma 14. Let $L = F(x_1, \ldots, x_n)$ and $s_1, \ldots, s_n$ be the elementary symmetric polynomials in $x_1, \ldots, x_n$.

$$s_k = \sum_{1 \leq j_1 < \cdots < j_k \leq n} \prod_{i=1}^{k} x_{j_i}$$

If $K = F(s_1, \ldots, s_n) \subset L$, then L/K is Galois and $\operatorname{Gal}(L/K) \cong S_n$.

Proof. write $f(x) = (x - x_1) \cdots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n \in K[x]$. Clearly, L is a splitting field of f over $K \rightsquigarrow L/K$ is Galois and $\operatorname{Gal}(L/K) \hookrightarrow S_n$.

Now, for $\sigma \in S_n$, σ can be regarded as an element in $\operatorname{Gal}(L/K)$:

$$\begin{aligned} \sigma : L &\to L \\ x_i &\mapsto x_{\sigma(i)} \end{aligned}$$

Since $\{\, \sigma(x_1), \ldots, \sigma(x_n) \,\} = \{\, x_1, \ldots, x_n \,\} \rightsquigarrow \sigma(s_i) = s_i \quad \forall\, i \rightsquigarrow \sigma\big|_K = \operatorname{Id}_K \rightsquigarrow \sigma \in \operatorname{Gal}(L/K)$. □

Coro 5.9.1. $L^{S_n} = K = F(s_1, \ldots, s_n)$.
$L^{S_n} = \{\, f(x_1, \ldots, x_n) \in L \mid f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n) \quad \forall\, \sigma \in S_n \,\}$ is all symmetric poly.

Coro 5.9.2. For any finite group G, by Cayley thm, $G \hookrightarrow S_n$ for some n. so $\operatorname{Gal}(L/L^G) \cong G$.

Now we prove the Main theorem:

Proof. Let $L = K(z_1, \ldots, z_n)$. Since $t_1, \ldots, t_n$ are the symmetric poly. w.r.t. $z_1, \ldots, z_n$, $L = F(z_1, \ldots, z_n)$.

Let $F(s_1, \ldots, s_n)$ and $F(x_1, \ldots, x_n)$ be given as in lemma 14.

since $t_1, \ldots, t_n$ are variables, $\exists\ \tau : F[t_1, \ldots, t_n] \twoheadrightarrow F[s_1, \ldots, s_n]$ with $\tau : t_i \mapsto s_i$. Also, Since $x_1, \ldots, x_n$ are variables, $\exists\ \sigma : F[x_1, \ldots, x_n] \twoheadrightarrow F[z_1, \ldots, z_n]$ with $\sigma : x_i \mapsto z_i$.

now, $\sigma \circ \tau(t_i) = \sigma(s_i) = \sigma\left(\sum x_{j_1} \cdots x_{j_i}\right) = \left(\sum z_{j_1} \cdots z_{j_i}\right) = t_i \implies \sigma \circ \tau = \operatorname{Id} \implies \tau$ is 1-1 and thus an isom. So there exists an extension $\tau' : F(t_1, \ldots, t_n) \xrightarrow{\sim} F(s_1, \ldots, s_n)$. Note $\bar{\tau}' : f(x) \mapsto g(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$.

Let $F(z_1, \ldots, z_n)$ be a splitting field of f over $F(t_1, \ldots, t_n)$ and $F(x_1, \ldots, x_n)$ be a splitting field of g over $F(s_1, \ldots, s_n)$ where $g = \bar{\tau}'(f)$. There exists $\sigma' : F(z_1, \ldots, z_n) \xrightarrow{\sim} F(x_1, \ldots, x_n)$ with $\sigma'\big|_{F(t_1, \ldots, t_n)} = \tau'$. So $\operatorname{Gal}(L/K) \cong S_n$ by lemma 14. □

Remark 32.

- Since S_n is transitive, f is irr.
- $\operatorname{char} F = 0 \rightsquigarrow f$ is separable.

5.10 Calculation of Galois groups

Let $f(x)$ be separable in $K[x]$ and $L = K(\alpha_1, \ldots, \alpha_n)$ be a splitting field of f over K. The goal is to find $\mathrm{Gal}(L/K)$ which is in S_n.

Define $\theta \triangleq y_1\alpha_1 + \cdots + y_n\alpha_n$. For each $\sigma \in S_n$, define $\sigma_y(\theta) \triangleq y_{\sigma(1)}\alpha_1 + \cdots + y_{\sigma(n)}\alpha_n$ and $\sigma_\alpha(\theta) = y_1\alpha_{\sigma(1)} + \cdots + y_n\alpha_{\sigma(n)}$. It is easy to see that $\sigma_y^{-1} = \sigma_\alpha$.

In $L(x, y_1, \ldots, y_n)$, we consider $F(x, \boldsymbol{y}) = \prod_{\sigma\in S_n} (x - \sigma_y(\theta)) = \prod_{\sigma^{-1}\in S_n} (x - \sigma_\alpha(\theta)) = \prod_{\sigma\in S_n} (x - \sigma_\alpha(\theta))$.
Since each coefficient of F is a symmetric polynomial of $\alpha_1, \ldots, \alpha_n$, by the fundamental theorem of symmetric polynomials, these symmetric polynomials are polynomials of the elementary symmetric polynomials. Thus $F(x, y) \in K[x, y_1, \ldots, y_n]$.

Decompose F into irreducible factors in $K[x, y_1, \ldots, y_n]$, say $F = F_1F_2\cdots F_r$. Notice that for any $\sigma \in S_n$, $F = \sigma_y F = \sigma_y F_1 \cdot \sigma_y F_2 \cdots \sigma_y F_r$. And each F_i is map to some F_j, thus σ induces a permutation of $F_1, F_2, \ldots, F_r$.

For convenience, assume $(x - \theta) \mid F_1$. We have the following lemma:

Lemma 15.

$$Q \triangleq \{\, \sigma : \sigma_y F_1 = F_1 \,\} = \{\, \sigma : \sigma_y(x - \theta) \mid F_1 \,\}$$

Proof. "$\subseteq$": Since $x - \theta \mid F_1$, so $\sigma_y(x - \theta) \mid \sigma_y F_1 = F_1$.

"$\supseteq$": $\sigma_y(x - \theta) = x - \sigma_y(\theta) \mid \sigma_y(F_1)$, so $\sigma_y(F_1)$ and F_1 has a common factor. Since F is separable, $\sigma_y(F_1) = F_1$. $\square$

Prop 5.10.1. $\mathrm{Gal}(L/K) = Q$.

Proof. "$\subseteq$": For each $\sigma \in \mathrm{Gal}(L/K) \hookrightarrow S_n$, extend σ to

$$\begin{aligned} \tilde{\sigma} : L(y_1, \ldots, y_n) &\to L(y_1, \ldots, y_n) \\ \alpha \in L &\mapsto \sigma(\alpha) \\ y_i &\mapsto y_i \end{aligned}$$

The automorphism fixes $K(y_1, \ldots, y_n)$, so $\tilde{\sigma}(\theta) = \sigma_\alpha(\theta)$ and θ share the same minimal polynomial over $K(y_1, \ldots, y_n)$. By Gauss's lemma, F_1 is irreducible in $K[y_1, \ldots, y_n][x] \implies F_1$ is irreducible in $K(y_1, \ldots, y_n)[x]$, thus $F_1 = m_{\theta, K(y_1,\ldots,y_n)} = m_{\sigma_\alpha(\theta), K(y_1,\ldots,y_n)}$, which implies $(x - \sigma_\alpha(\theta)) \mid F_1$. So $\sigma_y^{-1} F_1 = F_1 \implies \sigma^{-1} \in Q \implies \sigma \in Q$.

"$\supseteq$": For any $\sigma \in Q$, $F_1 = m_{\theta, K(y_1,\ldots,y_n)} = m_{\sigma_\alpha^{-1}(\theta), K(y_1,\ldots,y_n)}$, so there exists $\tau \in \mathrm{Aut}(L(\boldsymbol{y})/K(\boldsymbol{y}))$ satisfying $\tau(\theta) = \sigma_\alpha^{-1}(\theta) = \sigma_y(\theta)$. Since L/K normal, $\tau(L) = L$ and thus $\tau\big|_L \in \mathrm{Gal}(L/K)$ with $\tau\big|_L(\alpha_i) = \alpha_{\sigma^{-1}(i)}$, which implies that $\sigma^{-1} \in \mathrm{Gal}(L/K) \implies \sigma \in \mathrm{Gal}(L/K)$. $\square$

Theorem 66. Let $f(x)$ be monic, separable, in $\mathbb{Z}[x]$. Assume $p \nmid D = \prod_{i<j}(\alpha_i - \alpha_j)^2$, then the Galois group of $\bar{f}(x)$ in $\mathbb{F}_p[x]$ is a subgroup of the Galois group of $f(x)$.

Proof. Since f is separable, $D \neq 0$. The discriminant could be calculate by $D = (-1)^{n(n+1)/2}R(f, f')$ which only depends on the coefficients, so $\bar{D} \neq 0$ in $\mathbb{F}_p$ since $p \nmid D$. Thus f separable.

As above, let $F = F_1F_2\cdots F_r$ in $\mathbb{Z}[x, \boldsymbol{y}]$. Assume $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then $\bar{f}(x) = x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0$. Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be their roots, respectively. Define $\theta_p \triangleq y_1\beta_1 + \cdots + y_n\beta_n$. Since the coefficients of F are symmetric polynomials of $\alpha_1, \ldots, \alpha_n$, which only depends on the coefficients of f, and so is $F_p(x, y) = \prod_{\sigma\in S_n}(x - \sigma_y(\theta_p))$, we know that $F_p(x, y) = \bar{F}(x, y)$.

Now $\bar{F} = \bar{F}_1\bar{F}_2\cdots\bar{F}_r = (G_{1,1}\cdots G_{1,q_1})(G_{2,1}\cdots G_{2,q_2})\cdots(G_{r,1}\cdots G_{r,q_r})$

The Galois group of $\bar{f}$ is

$$\{\,\sigma \in S_n : \sigma_y G_{1,j} = G_{1,j},\, \forall\, j\,\} \subseteq \{\,\sigma \in S_n : \sigma_y \bar{F}_1 = \bar{F}_1\,\} = \{\,\sigma \in S_n : \sigma_y F_1 = F_1\,\}$$

Where the equality holds because $\sigma_y \bar{F}_1 = \bar{F}_1 \iff (x - \sigma_y(\theta_p)) \mid \bar{F}_1 \iff (x - \sigma_y(\theta)) \mid F_1 \iff \sigma_y F_1 = F_1$. Thus the galois group of $\bar{f}$ is a subgroup of f. $\square$

Fact 5.10.1.

- Every finite extension of $\mathbb{F}_p$ is cyclic, so the Galois group of $\bar{f}(x)$ in $\mathbb{F}_p[x]$ is cyclic.
- If $\bar{f}$ is irreducible, then the Galois group of $\bar{f}$ is transitive on its roots, thus the only possibililty is a cycle of length $n = \deg \bar{f}$ in S_n.
- If $\bar{f} = \bar{f}_1 \cdots \bar{f}_r$, with each $\bar{f}_i$ irreducible. Let the Galois group be $\langle\sigma\rangle$, then σ should be transitive on the roots of each $\bar{f}_i$. The only possibility of σ is a permutation composited by cycles of length $\deg \bar{f}_1, \ldots, \deg \bar{f}_r$. That is, $\sigma = (\alpha_{1,1}\ \ldots\ \alpha_{1,m_1}) \cdots (\alpha_{r,1}\ \ldots\ \alpha_{r,m_r})$ where $m_i \triangleq \deg \bar{f}_i$.

5.11 Transcendental extensions

Def 97. Let L/K be an extension and $S \subset L$.

- S is algebraically dependent over K if for some $n \in \mathbb{N}$, exists $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ satisfied $f(a_1, \dots, a_n) = 0$ for some distinct $a_1, \dots, a_n \in S$.
- S is algebraically independent over K if S is not algebraically dependent.
- S is called a transcendence base for L/K if S is algebraically independent and $L/K(S)$ is algebraic.

Theorem 67. Any two transcendence bases for L/K have the same cardinality.

Proof. Pick any transcendence base $S = \{s_1, \dots, s_n\}$ for L/K. Let T be another transcendence base for L/K. First we deal with the case which S is finite.

We claim that $\exists\, t_1 \in T$ such that t_1 is algebraically independent over $K(s_2, \dots, s_n)$.

Proof. If not, then all elements of T is algebraically dependent over $K(s_2, \dots, s_n)$. This implies $K(s_2, \dots, s_n)(T)/K(s_2, \dots, s_n)$ is algebraic. And $L/K(T)$ is algebraic implies $L/K(T)(s_2, \dots, s_n)$ is algebraic. Then $L/K(s_2, \dots, s_n)$ is algebraic, which is a contradiction (s_1 is not). $\square$

By the claim, $\{ t_1, s_2, \dots, s_n \}$ is algebraic indepedent. Also, there exists $f \neq 0$ in $K[x_1, \dots, x_{n+1}]$ such that $f(t_1, s_1, \dots, s_n) = 0$ since t_1 is algebraic over $K(s_1, \dots, s_n)$. Since $\{ s_1, \dots, s_n \}$ and $\{ t_1, s_2, \dots, s_n \}$ are both algebraically indepedent, t_1, s_1 must occur in $f \implies s_1$ is algebraic over $K(t_1, s_2, \dots, s_n)$. Then $K(t_1, s_1, \dots, s_n)/K(t_1, s_2, \dots, s_n)$ is algebraic. Since $L/K(t_1, s_1, \dots, s_n)$ is algebraic, $L/K(t_1, s_2, \dots, s_n)$ is algebraic.

Repeating this process, we get find $t_1, \dots, t_n \in T$ s.t. $L/K(t_1, \dots, t_n)$ is algebraic. But T is a transcendence base, so we must have $T = \{ t_1, \dots, t_n \}$.

Now assume S is infinite. For another transcendence base T, we have $|T| = \infty$. For $s \in S$, s is algebraic over $K(T)$, and in fact is over $K(T_s)$ such that T_s is finite, since algebraic relation involves. Let $m_{s,K(T)} \in K(T_s)[x]$ for some finite set $T_s \subset T$. We claim that $\bigcup\limits_{s \in S} T_s = T$.

Proof. Let $U = \bigcup\limits_{s \in S} T_s$. Clearly $U \subseteq T$. And by def, $K(U)(S)/K(U)$ is algebraic. Also, $L/K(U)(S)$ is algebraic. So $L/K(U)$ is algebraic $\implies T = U$ since T is a transcendence base. $\square$

By well ordering principle, we can well-order S and denote its 1st element by s_1. Let

$$\begin{cases} T'_{s_1} = T_{s_1} \\ T'_s = T_s \setminus \bigcup_{l<s} T_l \end{cases} \qquad \implies \qquad \{ T'_s \}_{s \in S} \text{ are mutually disjoint}$$

For all T'_s, choose a fixed ordering of the elements in T'_s, says $t_{s,1}, \dots, t_{s,k_s}$. Define an injection $\varphi : \bigcup\limits_{s \in S} T'_s \to S \times \mathbb{N}$ with $\varphi : t_{s,i} \mapsto (s, i)$. So $|T| = \left| \bigcup\limits_{s \in S} T_s \right| \leq |S \times \mathbb{N}| = |S||\mathbb{N}| = |S|$ since $|S| = \infty$. $\square$

Def 98. Let S be a transcendence base of L/K, then we use $\operatorname{tr\,deg}_K L$ to denote $|S|$.

Remark 33. If S_1, S_2 are two transcendence base for L/K, then it is **not necessarily true** that $K(S_1) = K(S_2)$.

Def 99. L/K is called purely transcendental if exists a transcendental base S such that $L = K(S)$.

Theorem 68 (Lüroth's theorem)**.** If L is purely transcendental of degree 1 over K, then any proper intermediate field E is also purely transcendental of degree 1.

Lemma 16. Let $L = K(t)$ with t being transcendental over K and $u = f(t)/g(t) \in L \setminus K$ with $\gcd(f(t), g(t)) = 1$. Assume $n = \max(\deg f, \deg g)$, then $L/K(u)$ is algebraic and $[L : K(u)] = n$.

Proof. Write
$$f(t) = a_n t^n + \cdots + a_1 t + a_0, \quad g(t) = b_n t^n + \cdots + b_1 t + b_0$$
(note that either $a_n \neq 0$ or $b_n \neq 0$) Let $F(x) = f(x) - ug(x) = (a_n - ub_n)x^n + \cdots + (a_1 - ub_1)x + (a_0 - ub_0)$. Since $a_n - ub_n \neq 0$, $F(x) \neq 0$ and $\deg F(x) > 0$. By def. of u, we have $F(t) = 0 \implies t$ is algebraic over $K(u)$ and $[K(t) : K(u)] \leq n$. Now we prove that $F(x)$ is irreducible over $K(u)$. By Gauss's lemma, it suffices to show that $F(x)$ is irreducible in $K[u][x] = K[u, x]$. Assume that $F(x) = p(u, x)q(u, x)$ with $\deg_u p = 1$ and $q \in K[x]$. Since $F(x) = f(x) - ug(x)$, we have $q \mid f, q \mid g \implies q \mid \gcd(f, g) = 1 \implies q \in K$. So $[K(t) : K(u)] = n$. □

Now we prove the Lüroth's theorem:

Proof. For $v \in E \setminus K$, by lemma 16, t is algebraic over $K(v) \rightsquigarrow t$ is algebraic over E.

Let $m(x) = m_{t,E}$, then there exists $\beta(t) \in K(t)$ s.t. $\beta(t)m(x) = a_n(t)x^n + \cdots + a_1(t)x + a_0(t)$ is primitive in $K[t][x] = K[t, x]$. Let $F(t, x) = \beta(t)m(x)$.

Since t is not algebraic over K, there exists some $u = \frac{a_i(t)}{a_n(t)} \notin K$. Write $u = \frac{f(t)}{g(t)}$ with $\gcd(f, g) = 1$. (Note that $u \in E$)

By lemma 16, $[K(t) : K(u)] = r \geq n$. Now we show that $r \leq n$, then $r = n \implies E = K(u)$.

Let $l = f(t)g(x) - g(t)f(x)$, which is skew-symmetric in t and x. Notice that $g(t)^{-1}l \in E[x]$ and has t as a zero. So $m(x) \mid g(t)^{-1}l$ in $E[x] \implies \beta(t)m(x) \mid \beta(t)g(t)^{-1}l$. Since $\beta(t)g(t)^{-1} \in K[t]$, $F(t, x) \mid l$ in $K(t)[x]$. Since $F(t, x)$ is primitive in $K[t][x]$, $F(t, x) \mid l$ in $K[t][x]$.

Say $l = Fq$ for some $q(t, x) \in K[t][x]$. Note that $\deg_t l \leq r, \deg_t F \geq r \rightsquigarrow \deg_t l = \deg_t F = r, \deg_t q = 0$. So $q \in K[x] \rightsquigarrow q$ is primitive in $K[t][x]$. By Gauss's lemma, F, q are primitive, then l is also primitive in $K[t][x]$. Since l is skew-symmetric in t and x, l is also primitive in $K[x][t]$. But $q \in K[x]$ and $q \mid l$, we have $q \in K$. Hence $n = \deg_x F = \deg_x l = \deg_t l = \deg_t F \geq r$. □

5.12 Hilbert theorem 90 and Normal basis

Let $L = K(\alpha)$ with $f = m_{\alpha,K} = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ being separable. We have known that exists exactly n monomorphisms $\sigma_i :: L \to \overline{K}$ fixing K, and $\{\, \sigma_1(\alpha), \ldots, \sigma_n(\alpha) \,\}$ consists of all roots of f. So

$$\begin{aligned} x^n + a_{n-1}x^{n-1} + \cdots + a_0 &= (x - \sigma_1(\alpha)) \cdots (x - \sigma_n(\alpha)) \\ &\implies -a_{n-1} = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha) \text{ and } (-1)^n a_0 = \sigma_1(\alpha) \cdots \sigma_n(\alpha) \end{aligned}$$

Consider the K-linear transformation:

$$\begin{aligned} T_\alpha : K(\alpha) &\to K(\alpha) \\ v &\mapsto \alpha v \end{aligned}$$

Then

$$[T_\alpha]_\gamma = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}, \quad \text{where } \gamma = \{\, 1, \alpha, \alpha^2, \dots, \alpha^{n-1} \,\}$$

And $\mathrm{Tr}(T_\alpha) = -a_{n-1}, \det(T_\alpha) = (-1)^n a_0$.

Def 100. Let L/K be a Galois extension with $G = \mathrm{Gal}(L/K)$. for all $\alpha \in L$, define

$$N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \qquad N_{L/K} :: L^\times \to K^\times \text{ is multiplicative}$$
$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) \qquad \mathrm{Tr}_{L/K} :: L \to K \text{ is additive}$$

Theorem 69 (Hilbert theorem 90)**.** Let L/K is cyclic and $G = \langle \sigma \rangle$ with $\mathrm{ord}(\sigma) = n$, then

1. $\alpha \in L^\times$ and $N_{L/K}(\alpha) = 1 \iff \exists\, \beta \in L^\times, \alpha = \beta/\sigma(\beta)$.
2. $\alpha \in L$ and $\mathrm{Tr}_{L/K}(\alpha) = 0 \iff \exists\, \beta \in L, \alpha = \beta - \sigma(\beta)$.

Proof.

1. "$\Leftarrow$": $N_{L/K}(\alpha) = \prod_{k=0}^{n-1} \sigma^k(\beta/\sigma(\beta)) = 1$.

   "$\Rightarrow$": Since automorphisms are linearly independent, exists $c \in L$ such that

   $$0 \neq \beta = \mathrm{Id}(c) + \alpha\sigma(c) + \alpha\sigma(\alpha)\sigma^2(c) + \cdots + \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(c)$$

   Since $\alpha\sigma(\alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)) = N_{L/K}(\alpha) = 1$, it is easy to check that $\alpha\sigma(\beta) = \beta$.
2. "$\Leftarrow$": $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{L/K}(\beta - \sigma(\beta)) = \sum \big(\sigma^k(\beta) - \sigma^{k+1}(\beta)\big) = 0$.

   "$\Rightarrow$": Choose c such that $\beta_1 = c + \sigma(c) + \cdots + \sigma^{n-1}(c) \neq 0$, so $\sigma(\beta_1) = \beta_1$. Let

   $$\beta_2 = \alpha\sigma(c) + (\alpha + \sigma(\alpha))\sigma^2(c) + \cdots + \big(\alpha + \sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha)\big)\sigma^{n-1}(c)$$

   Then

   $$\beta_2 - \sigma(\beta_2) = \alpha\sigma(c) + \alpha\sigma^2(c) + \cdots + \alpha\sigma^{n-1}(c) + \alpha c = \alpha\beta_1.$$

   So let $\beta \triangleq \beta_2/\beta_1$, we obtain $\beta_2/\beta_1 - \sigma(\beta_2/\beta_1) = (\beta_2 - \sigma(\beta_2))/\beta_1 = \alpha$. □

Coro 5.12.1. Let $\mathrm{char}\, K = p$ and $[L : K] = p$, then L/K is Galois and cyclic $\iff$ $L = K(\alpha)$ where α is a root of $x^p - x - a$.

Proof. "$\Rightarrow$": Let $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ with $\mathrm{ord}(\sigma) = p$. Then $\mathrm{Tr}_{L/K}(1) = p = 0$. By theorem 69, exists α satisfied $1 = \sigma(\alpha) - \alpha$. So $\alpha \notin K$. Then we have $1 < [K(\alpha) : K] \bigm| [L : K] = p$, so $[K(\alpha) : K] = p \implies K(\alpha) = L$.

Notice that $\sigma^k(\alpha) = \alpha + k$. Since $\sigma^k(\alpha)$ iterates through all roots of $m_{\alpha,K}$ and $\sigma^k(\alpha) = \alpha + k$, $\alpha, \alpha+1, \dots, \alpha+p-1$ are all the roots of $m_{\alpha,K}$. We claim that $m_{\alpha,K} = x^p - x - a$ where $a \triangleq \alpha^p - \alpha$. Since $\sigma(a) = \sigma(\alpha)^p - \alpha = \alpha^p + p - \alpha = a$, a is fixed by all automorphisms, so $a \in K$. Moreover, $m_{\alpha,K}(\alpha + k) = \alpha^p + k^p - \alpha - k - a = 0$, thus the proof is completed.

"$\Leftarrow$": Similarly, we know that all roots of $x^p - x - a$ are $\alpha, \alpha+1, \dots, \alpha+p-1$. Define $\sigma(\alpha) = \alpha+1$, then $\sigma^i(\alpha) = \alpha + i$, and thus $\mathrm{ord}(\sigma) = p$. Hence $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. □

Coro 5.12.2. If $x^2 + dy^2 = 1$ where $-d$ is not a square, then $L \triangleq \mathbb{Q}(\sqrt{-d})$ is a splitting field of $x^2 + d$ over $\mathbb{Q}$, so $N_{L/\mathbb{Q}}(a + b\sqrt{-d}) = a^2 + db^2$. Since $[L : \mathbb{Q}] = 2$, the galois group is obviously cyclic and in fact is $\langle\sigma\rangle$, where $\sigma = (a + b\sqrt{-d}) \mapsto (a - b\sqrt{-d})$. By theorem 69,

$$x^2 + dy^2 = 1 \iff \exists\, a + b\sqrt{-d} \quad \text{s.t.} \quad x + y\sqrt{-d} = \frac{a + b\sqrt{-d}}{a - b\sqrt{-d}} = \frac{(a^2 - db^2) + 2ab\sqrt{-d}}{a^2 + db^2}$$

Def 101. Let L/K be Galois and $\mathrm{Gal}(L/K) = \{\, \mathrm{Id} = \sigma_1, \dots, \sigma_n \,\}$. A basis for L/K of the form $\{\, \sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha) \,\}$ with $\alpha \in L$ is called a normal basis for L/K.

Lemma 17. $\alpha_1, \dots, \alpha_n \in L$ form a basis for L/K if and only if

$$\begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix} \neq 0$$

Proof. "$\Rightarrow$": If not, then the determinant is 0. Then

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n &= 0 \\ \sigma_1(\alpha_2)x_1 + \cdots + \sigma_n(\alpha_2)x_n &= 0 \\ \qquad\qquad \vdots & \;\;\vdots \\ \sigma_1(\alpha_n)x_1 + \cdots + \sigma_n(\alpha_n)x_n &= 0 \end{cases}$$

has a non-zero solution $\boldsymbol{c} = (c_1, \dots, c_n) \in L^n$. (i.e., $\sum c_j\sigma_j(\alpha_i) = 0$ for each i.) So $\left(\sum_j c_j\sigma_j\right)(\alpha_i) = 0$ for each α_i, but α_i is a basis, so $\sum_j c_j\sigma_j = 0$, then these automorphisms are linearly dependent, which leads to a contradiction.

"$\Rightarrow$": If not, then exists $\boldsymbol{0} \neq \boldsymbol{c} = (c_1, \dots, c_n)$ satisfied $\sum c_i\alpha_i = 0$. Then $\sum_i c_i\sigma_j(\alpha_i) = 0$ for each j. Thus the determinant is 0 which leads to a contradiction. $\square$

Lemma 18. Let $|K| = \infty$. Then $\sigma_1, \dots, \sigma_n$ are algebraically independent over L.

Proof. Let $f(x_1, \dots, x_n) \in L[x_1, \dots, x_n]$ such that $f(\sigma_1, \dots, \sigma_n) = 0$. Let $\{\, \alpha_1, \dots, \alpha_n \,\}$ be a basis for L/K. Then

$$0 = f(\sigma_1, \dots, \sigma_n)\left(\sum_{i=1}^n r_i\alpha_i\right) = f\left(r_1\sigma_1\left(\sum_{i=1}^n \alpha_i\right), \dots, r_n\sigma_n\left(\sum_{i=1}^n \alpha_i\right)\right)$$

So let

$$g(x_1, \dots, x_n) \triangleq f\left(\sum_i \sigma_1(\alpha_i)x_1, \dots, \sum_i \sigma_n(\alpha_i)x_n\right)$$

and write $g(x_1, \dots, x_n) = \sum_j g_j(x_1, \dots, x_n)\alpha_j$. Then $g_j(r_1, \dots, r_n) = 0, \forall\, \boldsymbol{r} \in K^n$. The only polynomial which has infinite zeros (without any relation) is the zero polynomial, thus $g_j = 0$ for each j.

Now, by lemma 17, $\det([\sigma_i(\alpha_j)]) \neq 0$. So it is possible to solve $\boldsymbol{x} = (x_i)$ satisfied $\boldsymbol{y} = (y_j) = \left(\sum_i \sigma_j(\alpha_i)x_i\right)$. Thus $g = 0 \implies f = 0$. $\square$

Theorem 70. Any Galois extension L/K has a normal basis.

Proof. Case 1: L/K is cyclic (so all finite field is included).
Let $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ with $\mathrm{ord}(\sigma) = n$. σ could be view as a linear transformation of L over K. Thus σ gives L a $K[x]$-module structure by $(f(x), \alpha) \mapsto f(\sigma)(\alpha)$.

Since $K[x]$ is a PID. By the structure theorem, we could write

$$L \cong K[x]/\langle d_1(x)\rangle \oplus \cdots \oplus K[x]/\langle d_s(x)\rangle \quad \text{with } d_i \mid d_{i+1}$$

Since $\mathrm{Id}, \sigma, \ldots, \sigma^{n-1}$ are linearly independent over K, $m_{\sigma,K}$ should have degree at least n, thus it is clear that $x^n - 1$ is the minimal polynomial of σ, thus $d_s(x) = x^n - 1$. But the characteristic polynomial of σ has degree at most n, thus $d_1(x)\cdots d_s(x) = x^n - 1$. So $L \cong K[x]/\langle x^n - 1\rangle$. Let $\alpha \in L$ such that $\mathrm{Ann}(\alpha) = \langle x^n - 1\rangle$, then $L = K[x]\alpha$. Hence $L = \langle \alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\rangle$.

Case 2: $|K| = \infty$. Let $\mathrm{Gal}(L/K) = \{\, \sigma_1, \ldots, \sigma_n \,\}$. Define $y_{i,j} = x_k$ so that $\sigma_i\sigma_j = \sigma_k$. Consider

$$f(x_1, \ldots, x_n) = \begin{vmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n,1} & y_{n,2} & \cdots & y_{n,n} \end{vmatrix}$$

This determinant is a non-zero polynomial in $x_1, x_2, \ldots, x_n$. Since if we fix σ_1, for each σ_i, exists unique j so that $\sigma_i\sigma_j = \sigma_1$. So the determinant has a x_1^n term and is not zero. Then $f(\sigma_1, \ldots, \sigma_n) \neq 0$ by lemma 18. Thus there exists $\alpha \in L$ s.t. $\det\big([\sigma_i\sigma_j(\alpha)]\big) = f(\sigma_1, \ldots, \sigma_n)(\alpha) \neq 0$. So by lemma 17, $\{\, \sigma_i(\alpha) \,\}$ is a basis. $\square$

6 Commutative Algebra

6.1 ED, PID and UFD

We shall consider R to be a integral domain below.

Def 102. A function $N : R \to \mathbb{N}$ with $N(0) = 0$ is called a norm on R.

Def 103. R is called a Euclidean domain if exists a norm N on R satisfy

$$\forall\, a, b \in R,\ \exists\, q, r \in R \text{ s.t. } a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

Eg 6.1.1.

- $\mathbb{Z}$ is a ED with $N(n) = |n|$.
- $K[x]$ is a ED with $N(f) = \deg f,\ \forall\, f \in K[x]$.

Def 104. A_d is defined to be the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{d})$ with $d \neq 1$ and d is square-free. That is,

$$A_d \triangleq \{\, \alpha \in \mathbb{Q}(\sqrt{d}) \mid \alpha \text{ is integral over } \mathbb{Z} \,\}$$

Theorem 71.

- If $d \equiv 1 \pmod 4$, then
$$A_d = \left\{a + b\frac{1+\sqrt{d}}{2} : a, b \in \mathbb{Z}\right\}$$
- Else, $d \equiv 2, 3 \pmod 4$, then
$$A_d = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\}$$

Theorem 72. A_d is a ED if $d = 2, 3, 5, -1, -2, -3, -7, -11$. Hence A_d is also PID and UFD.

Eg 6.1.2. A_{-5} is not a ED.

Proof. Consider $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Notice that $1 + \sqrt{-5}$ is irreducible, since if $1 + \sqrt{-5} = \alpha\beta$, then $6 = N(1 + \sqrt{-5}) = N(\alpha)N(\beta)$. But there is $a^2 + 5b^2 = 2$ or 3 has no integer solution. Also $1 + \sqrt{-5} \nmid 2, 3$. Since if $(1 + \sqrt{-5})\alpha = 2$, then $N(1 + \sqrt{-5})N(\alpha) = N(2)$, but $N(1 + \sqrt{-5}) = 6$. $\square$

6.1.1 A_{-1} and A_{-3}

First, α is a unit $\iff N(\alpha) = 1$. so we have:

- A_{-1}: $\pm 1, \pm \mathrm{i}$.
- A_{-3}: $\pm 1, \pm\omega, \pm\omega^2$.

If α is a prime in A_{-1} or A_{-3}, then $N(\alpha) = p$ or p^2 for some prime integer p.

Let $N(\alpha) = \alpha\bar{\alpha} = p_1 \cdots p_n$ in $\mathbb{Z}$

Def 105. If p is add and $a \not\equiv 0 \pmod p$, then

- If $x^2 \equiv a \pmod p$ is solvable, then define $\left(\frac{a}{p}\right) = 1$.
- Else $x^2 \equiv a \pmod p$ is not solvable and define $\left(\frac{a}{p}\right) = -1$.

Prop 6.1.1.

- $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

6.2 Primary decomposition

Def 106.

- The radical of an ideal I is defined by $\sqrt{I} = \{\, a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N} \,\}$.
- I is radical if $\sqrt{I} = I$.

Def 107. The **nilradical** is defined as $\sqrt{\langle 0 \rangle} \triangleq \{\, a \in R \mid a^n = 0 \text{ for some } n \in \mathbb{N} \,\}$. Elements in it are called nilpotent.

Prop 6.2.1. $\sqrt{\langle 0 \rangle} = \bigcap_{P \in \operatorname{Spec} R} P$, where $\operatorname{Spec} R$ is the set of prime ideals in R.

Proof. "$\subset$": Notice that $a^n = 0 \in P$ for any prime ideal P. By the definition of prime ideal, either $a \in P$ or $a^{n-1} \in P$. No matter which, eventually we would get $a \in P$.

"$\supset$": Let $\mathcal{S} \triangleq \{\, I : \text{ ideal in } R \mid a^n \notin I, \forall\, n \in \mathbb{N} \,\}$. By the routine argument of Zorn's lemma, exists maximal element Q in $\mathcal{S}$. We claim that $\mathcal{S}$ is a prime ideal.

For each $x, y \notin Q$, we have $Q + Rx \supsetneq Q$ and $Q + Ry \supsetneq Q$. By the maximality of Q, these two ideals are not in $\mathcal{S}$. So exists n, m such that $a^n \in Q + Rx$, $a^m \in Q + Ry$ which implies $a^{n+m} \in Q + Rxy$, so $Q + Rxy \notin \mathcal{S}$, thus $xy \notin Q$, hence Q is prime. $\square$

Coro 6.2.1.

$$\sqrt{I} = \bigcap_{\substack{P \supset I \\ P \in \operatorname{Spec} R}} P$$

Proof. Notice that $\operatorname{Spec} R/I = \{\, P \in \operatorname{Spec} R \mid R \subset I \,\}$. By the proposition above,

$$\sqrt{\langle \bar{0} \rangle} = \bigcap_{\bar{P} \in \operatorname{Spec} R/I} \bar{P} \implies \sqrt{I} = \bigcap_{\substack{P \supset I \\ P \in \operatorname{Spec} R}} P$$

$\square$

Def 108. An ideal q of R is called primary if $q \neq R$ and "$xy \in q$ and $x \notin q$" implies $y^n \in q$ for some $n \in \mathbb{N}$.

Prop 6.2.2.

- prime $\implies$ primary.
- $\sqrt{\text{primary}} \implies$ prime. Also, if q is primary, then $p = \sqrt{q}$ is the smallest prime ideal containing q, we say q is p-primary.

Proof. The first one is obvious.

If q is primary and $\sqrt{q} = p$. For any $xy \in p$ and $x \notin p$, there exists n so that $x^n y^n \in q$, and for this n, $x^n \notin q$. Thus $(y^n)^m \in q$ for some m, hence $y \in p$. We conclude that p is a prime ideal.

Finally, by corollary 6.2.1,

$$p = \sqrt{q} = \bigcap_{\substack{P \supset q \\ P \in \operatorname{Spec} R}} P \subset P, \quad \forall\, P \text{ prime },$$

thus p is indeed the smallest. $\square$

Eg 6.2.1. The primary ideals in $\mathbb{Z}$ are $\langle 0\rangle$ and $\langle p^m\rangle$ where p is a prime.

Proof. If $q = \langle a\rangle$ is primary, then $\sqrt{q} = \langle p\rangle$ is prime, and $p^n \in \langle a\rangle$. So $ab = p^n$ which implies $a = p^m$ for some m. $\square$

Def 109. An ideal I is said to be **irreducible** if $I = q_1 \cap q_2 \implies I = q_1 \vee I = q_2$.

Def 110. Define $(I : x) = \{\, a \in R \mid ax \in I \,\}$.

Theorem 73. In a Noetherian ring R, every irreducible ideal I is primary.

Proof. Let $xy \in I$ and $x \notin I$. Consider $(I : y) \subseteq (I : y^2) \subseteq \cdots$. Since R is Noetherian, exists n such that $(I : y^n) = (I : y^m)$ for any $m \geq n$.

We claim that $I = (I + Ry^n) \cap (I + Rx)$.

- "$\subset$": Obvious.
- "$\supset$": For any $b \in (I + ry^n) \cap (I + Rx)$, write $b = a_1 + r_1 y^n = a_2 + r_2 x$. Then $r_1 y^{n+1} = a_2 y - a_1 y + r_2 xy \in I$ since $a_1, a_2, xy \in I$. So $r_1 \in (I : y^{n+1}) = (I : y_n) \implies r_1 y^n \in I$. Thus $b = a_1 + r_1 y^n \in I$.

Now by the fact that I is irreducible and $I \neq I + Rx$ since $x \notin I$, thus $I = I + Ry^n \implies y^n \in I$. $\square$

Theorem 74. In a Noetherian ring R, every ideal is a finite intersection of irreducible ideals.

Proof. If not, let $\mathcal{I} \triangleq \{\, I :\ \text{ideal in } R \mid I \text{ is not a finite intersection of irreducible ideals} \,\}$ and $\mathcal{I}$ is not an empty set. Since R is Noetherian, the set has a maximal element I_0. Then I_0 is not irreducible (or else it is an intersection of itself, which is irreducible). Write $I_0 = I_1 \cap I_2$, with $I_1, I_2 \neq I_0$. Then $I_1, I_2 \notin \mathcal{I}$, so these two ideals could be written as a finite intersection of irreducible ideals, implying that I_0 could also be written as a finite intersection of irreducible ideals, which is an contradiction. $\square$

Prop 6.2.3. Let q be a p-primary ideal and $x \in R$.

1. If $x \in q$, then $(q : x) = R$.

   Proof. In this case $1 \in (q : x)$, thus $(q : x) = R$. $\square$

2. If $x \notin q$, then $(q : x)$ is p-primary.

   Proof. For any $y \in (q : x)$, $xy \in q$ but $x \notin q$, thus $y^n \in q \implies y \in p$. Hence

   $$q \subset (q : x) \subset p \implies p = \sqrt{q} \subset \sqrt{(q : x)} \subset \sqrt{p} = p$$

   and thus $(q : x)$ is p-primary.

   For any y, z with $yz \in (q : x)$ but $y \notin (q : x)$, which is equivalent to $xyz \in q$ but $xy \notin q$. Since q primary, $z^n \in q \subset (q : x)$. $\square$

3. If $x \notin p$, then $(q : x) = q$.

Proof.

$$\begin{cases} y \in (q : x) \\ x \notin p \end{cases} \implies \begin{cases} xy \in (q : x) \\ x^n \notin q, \ \forall\, n \in \mathbb{N} \end{cases} \implies y \in q$$

$\square$

Prop 6.2.4. If each q_i are p-primary, then $q \triangleq \cap_{i=1}^n q_i$ is p-primary.

Proof. We check that $\sqrt{q} = \bigcap_{i=1}^n \sqrt{q_i} = \bigcap_{i=1}^n p = p$.

Also, if $xy \in q$ with $x \notin q$, then $x \notin q_k$ for some k. But $xy \in q_k$, thus $y^n \in q_k$. Since $\sqrt{q} = q_k$, $(y^n)^{m'} = y^m \in p \subset q$, thus q is p-primary. $\square$

Def 111. A **primary decomposition** of $I = q_1 \cap \cdots \cap q_n$ is **minimal** if $\sqrt{q_1}, \ldots, \sqrt{q_n}$ are distinct and $q_i \not\supseteq \bigcap_{j \neq i} q_j$.

A minimal primary decomposition of an ideal always exists in Noetherian ring since by theorem 74, the ideal could be written as a finite intersection of irreducible ideals, and then by theorem 73, these ideals are primary. Now If $\sqrt{q_i} = \sqrt{q_j}$ happen in these ideal, we could remove these two ideals and add $q' = \sqrt{q_i} \cap \sqrt{q_j}$. By proposition 6.2.4, q' is also primary. And if $q_i \subseteq \bigcap_{j \neq i} q_j$, we could simply remove q_i.

Theorem 75 (Uniqueness of primary decomposition)**.** Let $I = \cap_{i=1}^n q_i$ be a minimal decomposition of I. If $p_i = \sqrt{q_i}$, $\forall\, i$, then we have

$$\{\, p_i \,\} = \left\{ \sqrt{(I : x)} \;\middle|\; x \in R \wedge \sqrt{(I : x)} \in \operatorname{Spec} R \right\}$$

which is independent of the decomposition.

Proof. "$\supset$": Let $x \in R \setminus I$, then $(I : x) = \left(\bigcap_{i=1}^n q_i : x \right) = \bigcap_{i=1}^n (q_i : x)$. By proposition 6.2.3, we have $\sqrt{(I : x)} = \bigcap \sqrt{(q_i : x)} = \bigcap_{x \notin q_i} p_i$.

Now, we have the following observation. "If $p \in \operatorname{Spec} R$ with $p = \bigcap_{i=1}^n J_i$, then $p = J_j$ for some j." If not, then $J_i \not\subset p$ for all i, so we could pick $x_i \in J_i \setminus p$. But then $x_1 x_2 \cdots x_n \in \cap J_i \in p$ since J_i are ideals, which leads to a contradiction since p is prime.

So if $\sqrt{(I : x)}$ is a prime, then it is equal to some p_i.

"$\subset$": By assumption, $q_i \not\subseteq \bigcap_{j \neq i} q_j$ for each i, thus we could pick $x \in \bigcap_{j \neq i} q_j \setminus q_i$, then $\sqrt{(I : x)} = \bigcap_j \sqrt{(q_j : x)} = \sqrt{(q_i : x)} = p_i$. $\square$

Def 112. If $\{\, p_i \,\}$ is the unique prime ideals from the minimal primary decomposition of I.

- $\{\, p_i \,\}$ is said to be associated with I or to belong to I.
- The minimal elements in $\{\, p_i \,\}$ are called isolated primes.
- The other are called embedded primes.

Eg 6.2.2. Let $R = k[x, y]$ and $I = \langle x^2, xy \rangle$. If $P_1 = \langle x \rangle, P_2 = \langle x, y \rangle$, then $I = P_1 \cap P_2^2$. P_1 is isolated, while P_2 is embedded.

6.3 The equivalence of algebra and geometry

In the following, k will be an algebraically closed field.

Def 113. The category of affine algebraic sets $\mathcal{G}$, which its objects and morphisms are defined as following.

objects: The objects are affine algebraic sets in k^n.

An **affine algebraic set** is the common zero set of $\{F_i\}_{i\in\Lambda} \subset k[x_1, \dots, x_n]$ in k^n. We denote it by $V = \mathcal{V}(\{ F_i \}_{i\in\Lambda}) \subset k^n$. (In fact, $I = \langle F_i : i \in \Lambda\rangle$ is Noetherian, so $I = \langle F_1, \dots, F_n\rangle$ and $V = \mathcal{V}(I)$.)

morphisms: The morphisms are the polynomial map from k^n to k^m.

A **polynomial map** is a mapping as following:

$$\begin{aligned} k^n &\longrightarrow k^m \\ \alpha &\longmapsto (F_1(\alpha), \dots, F_m(\alpha)) \end{aligned}$$

where each F_i is a polynomial in $K[x_1, \dots, x_n]$.

Given two affine algebraic sets $V \subset k^n$ and $W \subset k^m$, if a map $F : V \to W$ is the restriction of a polynomial map from k^n to k^m, then F is a morphism from V to W.

Moreover, if $F : V \to W$ and $G : W \to V$ satisfy $F \circ G = \mathrm{Id}$ and $G \circ F = \mathrm{Id}$, then we say $V \cong W$.

Def 114. The category of finitely generated reduced k-algebra $\mathcal{A}$, which its objects and morphisms are defined as following.

objects: The objects are the reduced finitely generated k-algebra R.

A finitely generated k-algebra R is reduced if R has no non-zero nilpotent elements.

morphisms: The morphisms are the k-algebra homomorphisms.

Eg 6.3.1. It is easy to see that $\mathcal{V}(0) = k^n$ and $\mathcal{V}(1) = \varnothing$.

6.3.1 One-one correspondence between affine algebraic sets and radical ideals

Def 115. Define $\mathcal{I}(V) = \{ f \in k[x_1, \dots, x_n] \mid f(\alpha) = 0, \forall\, \alpha \in V \}$.

The one-one correspondence is given by

$$\begin{aligned} \{\text{affine algebraic sets in } \mathbb{A}_k^n\} &\longleftrightarrow \{\text{ radical ideals in } k[x_1, \dots, x_n]\} \\ V &\longmapsto \mathcal{I}(V) \\ \mathcal{V}(I) &\longleftarrow\!\shortmid\; I \end{aligned}$$

Prop 6.3.1.

- $\sqrt{\mathcal{I}(V)} = \mathcal{I}(V)$.

  Proof. For all $f^n \in \mathcal{I}(V)$, $f^n(\alpha) = 0, \forall\, \alpha \in V \implies f(\alpha) = 0, \forall\, \alpha \in V$. Thus $f \in \mathcal{I}(V)$. □

- If V is an affine set, then $\mathcal{V}(\mathcal{I}(V)) = V$.

  Proof. "$\supset$": $\forall\, \alpha \in V$, $f \in \mathcal{I}(V)$, $f(\alpha) = 0 \implies \alpha \in \mathcal{V}(\mathcal{I}(V))$.
  "$\subset$": Since V is an affine set, $V = \mathcal{V}(I)$, then $I \subset \mathcal{I}(V)$, so $\mathcal{V}(\mathcal{I}(V)) \subset \mathcal{V}(I) = V$. □

Lemma 19. Given $T/S/R$, a tower of rings. If R is Noetherian, T/S is a module finite and T/R is a ring finite, then S/R is a ring finite.

Proof. Let $T = R[a_1, \dots, a_n] = S\omega_1 + \cdots + S\omega_m$. Then $a_i = \sum_j r_{i,k}\omega_k$ for some $r_{i,k}$ and $\omega_{i,j} = \sum t_{i,j,k}w_k$ for some $t_{i,j,k}$.

Let $S' = R\big[\{ r_{i,k} \}, \{ t_{i,j,k} \}\big] \subseteq S$, which is Noetherian by the Hilbert basis theorem (R Notherian $\implies R[x]$ Notherian). Thus $T = S'\omega_1 + \cdots + S'\omega_m$ is a Noetherian S'-module by the fact that finitely generated module over a Noetherian ring is a Noetherian module.

Since $S \subset T$, S is a finitely generated S' submodule, so $S = S'v_1 + \cdots + S'v_r = R\big[\{ r_{i,k} \}, \{ t_{i,j,k} \}, \{ v_i \}\big]$. $\square$

Lemma 20. If $S = k(z_1, \dots, z_p)$, $p > 0$ with each z_i transcendental, then S/k is not ring finite.

Proof. If not, say $S = k[f_1, \dots, f_n]$ with $f_i = g_i/h_i$, $g_i, h_i \in k[z_1, \dots, z_p]$. Then for any irreducible polynomial p such that $p \nmid h_i$ for each h_i (This polynomial exists since for each h_i there are only finite degree 1 factors). Then $1/p \notin k[f_1, \dots, f_n]$ by checking the divisibility of the denominator under addition and multiplication, which leads to a contradiction. $\square$

Lemma 21. If A/k is an extension of fields and ring finite, then A/k is algebraic.

Proof. If A/k is transcendental and let $\{ z_1, \dots, z_t \}$ be a transcendental base. Then $A/k(z_1, \dots, z_t)$ is algebraic, thus a module finite. By lemma 19, $k(z_1, \dots, z_t)$ is ring finite, which contradict with lemma 20. $\square$

Theorem 76 (Weak form of Hilbert Nullstellensatz)**.**

$$I \subsetneq k[x_1, \dots, x_n] \implies v(I) \neq \varnothing$$

Proof. Since I proper, by lemma 7, exists a maximal ideal M such that $I \subseteq M$. Consider $K \triangleq k[x_1, \dots, x_n]/M = k[\bar{x}_1, \dots, \bar{x}_n]$. By proposition 5.1.8, K is a field, and by lemma 21, K/k is algebraic. Since k is already algebraically closed, $K = k$ and hence each $\bar{x}_i \in k$. Let $\alpha \triangleq (\bar{x}_1, \dots, \bar{x}_n) \in A^n_k$, then for any $f \in M$, $f(\alpha) = f(\bar{x}_1, \dots, \bar{x}_n) = \bar{f} = 0$, thus $\alpha \in \mathcal{V}(M) \subseteq \mathcal{V}(I)$. $\square$

Theorem 77 (Strong form of Hilbert Nullstellensatz)**.** $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$

Proof. "$\supset$": If $f^n \in I$, then $f(\alpha) = 0, \forall\, \alpha \in \mathcal{V}(I) \implies f^n(\alpha) = 0, \forall\, \alpha \in \mathcal{V}(I)$, thus $f^n \in \mathcal{I}(\mathcal{V}(I))$.

"$\subset$": If $\mathcal{I}(\mathcal{V}(I)) = 0$, then $I \subseteq \sqrt{I} \subseteq \mathcal{I}(\mathcal{V}(I)) = 0$, thus $I = 0$.

Otherwise, exists $0 \neq f \in \mathcal{I}(\mathcal{V}(I))$, Let $J = \langle I, ft - 1 \rangle \subset k[x_1, \dots, x_n, t]$. If $(a_1, \dots, a_n, t_0)$ is a zero of J, then $ft - 1 \in J \implies -1 = f(a_1, \dots, a_n)t_0 - 1 = 0$, which is a contradiction, so by theorem 76, $J = k[x_1, \dots, x_n, t]$.

Write $1 = \sum h_i f_i + s(ft - 1)$, where each $f_i \in I$ and $h_i, s \in k[x_1, \dots, x_n, t]$. This is a equation of variables, so if we set $t = 1/f$, the equation still holds. Now each h_i would be the form $\sum p_i/f^{k_i}$, so we could multiply each side by a suitable f^ρ and get $f^\rho = \sum c_i f_i$ with each $c_i \in k[x_1, \dots, x_n]$. This implies $f^\rho \in I$, thus $f \in \sqrt{I}$. $\square$

Def 116. Let $V \in \mathcal{G}$, the coordinate ring of V is $k[V] \triangleq k[x_1, \dots, x_n]/\mathcal{I}(V)$

6.3.2 Equivalence of $\mathcal{G}$ and $\mathcal{A}$

We define a functor F from $\mathcal{G}$ to $\mathcal{A}$ by

$$\begin{aligned} F: \quad \mathcal{G} &\longrightarrow \mathcal{A} \\ V &\longmapsto k[V] \end{aligned}$$

And For a polynomial map $f : V \to W$, define

$$\begin{aligned} F(f) = f^* : \quad k[W] &\longrightarrow k[V] \\ g &\longmapsto g \circ f \end{aligned}$$

Conversely, define a functor G by

$$\begin{aligned} G: \qquad \mathcal{A} &\longrightarrow \mathcal{G} \\ k[x_1, \ldots, x_n]/I &\longmapsto \mathcal{V}(I) \end{aligned}$$

Then if

$$\begin{aligned} \varphi: \quad k[\ldots]/I &\longrightarrow k[\ldots]/J \\ \bar{x}_i &\longmapsto \bar{f}_i \end{aligned}$$

Define

$$\begin{aligned} G(\varphi) = \psi: \qquad \mathcal{V}(J) &\longrightarrow \mathcal{V}(I) \\ \alpha = (a_1, \ldots, a_m) &\longmapsto (f_1(\alpha), \ldots, f_n(\alpha)) \end{aligned}$$

6.4 Gröbner basis

6.4.1 Division algorithm in $K[X_1, \dots, X_n]$

Eg 6.4.1. $I = \langle xy - 1, y^2 - 1\rangle \subseteq K[x, y]$, $f_1 = xy - 1$ an d $f_2 = y^2 - 1$ $G = \{ f_1, f_2 \}$. Does $f = x^2y + xy^2 + y^2 \in I$?

- Choose a lexicographic monomial ordering: $x > y$
- The multidegree $\partial(f) = (2, 1)$, $\partial(f_1) = (1, 1)$, $\partial(f_2) = (0, 2)$
- The leading term $\mathrm{LT}(f) = x^2y$, $\mathrm{LT}(f_1) = xy$, $\mathrm{LT}(f_2) = y^2$
- $\mathrm{LT}(f) = x\,\mathrm{LT}(f_1) \Rightarrow f = xf_1 + xy^2 + y^2 + x \Rightarrow f = \underset{h_1}{(x + y)}f_1 + \underset{h_2}{(1)}f_2 + \underset{\bar{f}^G}{(x + y + 1)}$ or $f = \underset{h_1}{x}\, f_1 + \underset{h_2}{(x + 1)}f_2 + \underset{\bar{f}^G}{(2x + 1)}$.

Note: Divisor h_1, h_2 and remainder $\bar{f}^G$ are not unique!!

Def 117. Fix a monomial ordering and let I be an ideal of $K[X_1, \dots, X_n]$. The ideal of leading terms in I is defined to be $\mathrm{LT}(I) = \langle\, \mathrm{LT}(f) \mid f \in I \,\rangle$.

Remark 34. Let $I = \langle f_1, \dots, f_n\rangle$. In general, $\langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_n)\rangle \subsetneq \mathrm{LT}(I)$.

Eg 6.4.2. Let $f_1 = xy^2 + y$, $f_2 = x^2y$. And, $xf_1 - yf_2 = xy \in \langle f_1, f_2\rangle$ but $xy \notin \langle xy^2, x^2y\rangle$.

Def 118. $G = \{ g_1, \dots, g_m \}$ is called a Gröbner basis of I if $I = \langle g_1, \dots, g_m\rangle$ and $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m)\rangle$.

Prop 6.4.1. Let $g_1, \dots, g_m \in I$, then $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m)\rangle \implies I = \langle g_1, \dots, g_m\rangle$.

Proof. $\forall\, f \in I$, do the division process. Then $f = \sum_{i=1}^{m} h_i g_i + r$, either $r = 0$ or $\underline{\bigstar = \text{no term of } r}$ $\underline{\text{is divisible by any of } \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m)}$. Assume $r \neq 0$, then $r = f - \sum_{i=1}^{m} h_i g_i \in I \Rightarrow \mathrm{LT}(r) \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m)\rangle$, which is a contradiction. Hence, $r = 0$ (i.e. $f \in \langle g_1, \dots, g_m\rangle$). $\square$

Theorem 78. Each ideal I has a Gröbner basis.

Proof. By Hilbert basis thm, $\mathrm{LT}(I) = \langle f_1, \dots, f_m\rangle$ for some f_i's. Write $f_i = \sum_{j=1}^{m_i} h_{ij}\,\mathrm{LT}(g_{ij})$ with $h_{ij} \in K[X_1, \dots, X_n]$, $g_{ij} \in I$. Then $\mathrm{LT}(I) = \langle\, \mathrm{LT}(g_{ij}) | i = 1, \dots, m,\ j = 1, \dots, m_i \,\rangle$. By prop 6.4.1, This is Gröbner basis. $\square$

Theorem 79. Let $G = \{ g_1, \dots, g_m \}$ be a Gröbner basis of I, then

- $\forall\, f \in K[X_1, \dots, X_n]$, $f = f_I + r$ where $f_I \in I, r = \bigstar$ are unique.

  Proof. By division algorithm, $f = f_I + \underset{\bigstar}{r} = f'_I + \underset{\bigstar}{r'}$, then $r \underset{\bigstar}{-} r' = f_I - f'_I$. But if $r - r' \neq 0$, then $\mathrm{LT}(r - r') \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m)\rangle$, which is a contradiction. Hence, $r - r' = 0 \Rightarrow f_I = f'_I$. $\square$

- $f \in I \iff r = 0$.

  Proof. Suppose $f \in I$, then $f = f_I + \underset{\bigstar}{r}$, and if $r \neq 0$, $\underset{\bigstar}{r} = f - f_I \in I$, which is a contradiction. Hence, $r = 0$. Conversly, if $r = 0$, $f = f_I \in I$. $\square$

6.4.2 Buchberger's algorithm

Def 119. Let $f, g \in K[x_1, \dots, x_n]$ and M be the monic least common multiple of $\mathrm{LT}(f)$ and $\mathrm{LT}(g)$. $S(f,g) = \frac{M}{\mathrm{LT}(f)} f - \frac{M}{\mathrm{LT}(g)} g$ is called an S-polynomial of f, g.

Let $I = \langle g_1, \dots, g_m \rangle$ and $G = \{ g_1, \dots, g_m \}$. A Gröner basis of I can be constructed by the following algorithm:

1. Initially let $G_0 \leftarrow G$.
2. Repeatly construct $G_{i+1} \leftarrow G_i \cup \left(\{ S(f,g) \mod G_i \,|\, f, g \in G_i \} \setminus \{ 0 \} \right)$, until once $G_{i+1} = G_i$, then G_i is a Gröbner basis of I.

Lemma 22. Let $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ with $a_1, \dots, a_m \in K$ satisfying $\partial(f_1) = \partial(f_2) = \cdots = \partial(f_m) = \alpha$ and $h = \sum_{i=1}^m a_i f_i$ with $\partial(h) < \alpha$. Then $h = \sum_{i=2}^m b_i S(f_{i-1}, f_i)$ for some $b_i \in K$.

Proof. Write $f_i = c_i f_i'$ with $c_i \in K$ and f_i' being monic of multidegree α. Note: $S(f_i, f_j) = f_i' - f_j'$ since all multidegree are equal. Then,

$$\begin{aligned} h &= \sum_{i=1}^m (a_i c_i f_i') \\ &= a_1 c_1 (f_1' - f_2') + (a_1 c_1 + a_2 c_2)(f_2' - f_3') + \cdots + (a_1 c_1 + \cdots + a_{m-1} c_{m-1})(f_{m-1}' - f_m') \\ &+ (a_1 c_1 + \cdots + a_m c_m) f_m' \\ &= \sum_{i=2}^m b_i S(f_{i-1}, f_i) + b_{m+1} f_m' \text{ with } b_i = \sum_{j=1}^{i-1} a_j c_j. \end{aligned}$$

Also, in this equality, f_m' is the only term that has multidegree α (other terms have multidegree less than α). So $b_{m+1} = 0$ must hold. Then, we have $h = \sum_{i=2}^m b_i S(f_{i-1}, f_i)$. ☐

Theorem 80 (Buchberger's criterion)**.** Assume $I = \langle g_1, \dots, g_m \rangle$, then $G = \{ g_1, \dots, g_m \}$ is a Gröbner basis of $I \iff S(g_i, g_j) \equiv 0 \pmod{G}$ for each i, j.

Proof.

- Suppose G is a Gröbner basis of I. $S(g_i, g_j) \in I \Rightarrow S(g_i, g_j) = 0$ by thm 79.
- Converely, suppose $S(g_i, g_j) \equiv 0 \pmod{G} \forall\, i, j$. For $f \in I$, $f \underset{not\ division}{=} \sum_{i=1}^m h_i g_i$ for some $h_i \in K[x_1, \dots, x_n]$. Define $\alpha = \max\{\partial(h_1 g_1), \dots, \partial(h_m g_m)\}$. We have $\partial(f) \leq \alpha$ and we can select an expression $f = \sum_{i=1}^m h_i g_i$ for f s.t α is minimal.
- <u>Claim</u>: $\partial(f) = \alpha$
- (pf) Rewrite,

$$\begin{aligned} f &= \sum_{i=1}^m h_i g_i \\ &= \sum_{\partial(h_i g_i) = \alpha} h_i g_i + \sum_{\partial(h_i g_i) < \alpha} h_i g_i \qquad \text{(the first term} \neq 0 \text{ since } \alpha \text{ is minimal.)} \\ &= \sum_{\partial(h_i g_i) = \alpha} \mathrm{LT}(h_i) g_i + \sum_{\partial(h_i g_i) = \alpha} (h_i - \mathrm{LT}(h_i) g_i) + \sum_{\partial(h_i g_i) < \alpha} h_i g_i \end{aligned}$$

Let $\mathrm{LT}(h_i) = a_i h_i^0$ with h_i^0 being a monic monomial. Comparing the multidegree on both side, $\partial \left(\sum_{\partial(h_i g_i) = \alpha} a_i h_i^0 g_i \right) < \alpha$ By lemma 22, $\sum_{\partial(h_i g_i) = \alpha} (a_i h_i^0 g_i) = c_{12} S(h_{i_1}^0 g_{i_1}, h_{i_2}^0 g_{i_2}) + \dots$ (finite) where $\partial(h_{i_1}g_{i_1}) = \partial(h_{i_2}g_{i_2}) = \cdots = \alpha$. By def, if we set $\beta_{st} = M_{st}$ = the monic lcm of $\mathrm{LT}(g_{i_s}), \mathrm{LT}(g_{i_t})$, then

$$\begin{aligned}
S(h^0_{i_s}g_{i_s}, h^0_{i_t}g_{i_t}) &= \frac{X^\alpha}{\mathrm{LT}(h^0_{i_s}g_{i_s})}h^0_{i_s}g_{i_s} - \frac{X^\alpha}{\mathrm{LT}(h_{i_t}g_{i_t})}h^0_{i_t}g_{i_t} \\
&= X^{\alpha-\beta_{st}}\left(\frac{X^{\beta_{st}}}{\cancel{h^0_{i_s}}\,\mathrm{LT}(g_{i_s})}\cancel{h^0_{i_s}}g_{is} - \frac{X^{\beta_{st}}}{\cancel{h^0_{i_t}}\,\mathrm{LT}(g_{i_t})}\cancel{h^0_{i_t}}g_{i_t}\right) \\
&= X^{\alpha-\beta_{st}}S\left(g_{i_s}, g_{i_t}\right) \\
&= X^{\alpha-\beta_{st}}\sum_{j=1}^{m} l_j g_j \text{ (by division)}
\end{aligned}$$

- Then, $\partial(l_jg_j) < \beta_{st} \implies \partial(f) \geq \alpha$. Therefore, $\partial(f) = \alpha \implies \mathrm{LT}(f) = \sum_{\partial(h_ig_i)=\alpha} \mathrm{LT}(h_i)\,\mathrm{LT}(g_i)$ $\implies \mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m)\rangle$.

□

Theorem 81. The Buchberger's algorithm will terminate

Proof. .

- $\langle \mathrm{LT}(G_i)\rangle \subsetneq \langle \mathrm{LT}(G_{i+1})\rangle$ if $G_i \neq G_{i+1}$

$$G_i \neq G_{i+1} \implies \exists\, f, g \in G_i \text{ s.t. } S(f,g) \not\equiv 0 \pmod G \implies \mathrm{LT}(S(s,g)) \notin \langle \mathrm{LT}(G_i)\rangle$$

- $\langle \mathrm{LT}(G_0)\rangle \subsetneq \langle \mathrm{LT}(G_1)\rangle \subsetneq \cdots$ is not possible since $K[x_1, \dots, x_n]$ is a Noetherian ring. (Noetherian ACC condition).

□

6.5 Applications of Gröbner basis

Def 120. Let $I \subseteq K[x_1, \dots, x_n]$ and $x_1 > x_2 > \cdots > x_n$. $I_i \triangleq I \cap K[x_{i+1}, \dots, x_n]$ is called the i-th elimination ideal of I.

Theorem 82 (Elimination theorem)**.** Let $G = \{\, g_1, \dots, g_m \,\}$ be a Gröbner basis of $I \neq 0$ with ordering $x_1 > \cdots > x_n$. Then $G_i \triangleq G \cap K[x_{i+1}, \dots, x_n]$ is a Gröbner basis of I_i (i.e., $\langle \mathrm{LT}(G_i)\rangle = \mathrm{LT}(I_i)$).

Eg 6.5.1. Find $V = \mathcal{V}(x+y-z, x^2+y^2-z^3, x^3+y^3-z^5)$.
We compute a Gröbner basis of $I = \langle f_1, \dots, f_3\rangle$ with respect to the ordering $x > y > z$. The Gröbner basis is $\{\, x+y-z, 2y^2-2yz-z^3+z^2, 2z^5-3z^4+z^3 \,\}$.

Eg 6.5.2.

$$\begin{aligned} f:\quad \mathbb{A}^1 &\longrightarrow \mathbb{A}^3 \\ t &\longmapsto (t^4, t^3, t^2) \end{aligned}$$

We compute a Gröbner basis of $I = \langle t^4-x, t^3-y, t^2-z\rangle$ with respect to $t > x > y > z$. The Gröbner basis is $\{\, -t^2+z, ty-z^2, tz-y, x-z^2, y^2-z^3 \,\}$.

Eg 6.5.3.

$$\begin{aligned} f: \quad V = \mathcal{V}(x^3 - x^2z - y^z) &\longrightarrow \mathbb{A}^3 \\ (x, y, z) &\longmapsto (x^2z - y^2z, 2xyz, -z^3) \end{aligned}$$

The ideal is $\langle x^3 - x^2z - y^2z, u - x^2z + y^2z, v - 2xyz, w + z^3 \rangle$ has a Gröbner basis $\langle \dots, u^2 + v^2 - w^2 \rangle$.

Theorem 83. Let I, J be two ideals of $K[x_1, \dots, x_n]$, then $I \cap J = (t\tilde{I} + (1-t)\tilde{J}) \cap K[x_1, \dots, x_n]$.

Eg 6.5.4. $I = \langle y^2, x - yz \rangle$, $J = \langle x, z \rangle$. We shall find $I \cap J$.
$tI + (1-t)J = \langle tx - tyz, ty^2, (1-t)x, (1-t)z \rangle$ has a Gröbner basis $\{ f_1, f_2, f_3, f_4, xy, x - yz \}$, so $I \cap J = \langle xy, x - yz \rangle$.

Theorem 84. Let $L = \langle f_1, \dots, f_s \rangle \subsetneq K[x_1, \dots, x_n]$, then $f \in \sqrt{I} \iff \langle f_1, \dots, f_s, 1 - tf \rangle = K[x_1, \dots, x_n, t]$.

Eg 6.5.5. Let $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$, and we are to determine $f = y - x^2 + 1$ is in $\sqrt{I}$ or not.

Prop 6.5.1. An affine algebraic set V in $\mathbb{A}_k^n$ has a unique minimal decomposition. $V = V_1 \cap V_2 \cap \dots \cap V_m$ with V_i irreducible and $V_i \not\subset V_j$.

Theorem 85 (Decomposition)**.** Assume $\sqrt{I} = I$ and $I \subset J$, then $\mathcal{V}(I : J) = \overline{\mathcal{V}(I) \setminus \mathcal{V}(J)}$. and $\mathcal{V}(I) = \mathcal{V}(J) \cup \mathcal{V}(I : J)$.

Eg 6.5.6. Let $I = \langle xz - y^2, x^3 - yz \rangle$ and $V = \mathcal{V}(I)$.

Notice that $\langle xz - y^2, x^3 - yz \rangle \subseteq \langle x, y \rangle = J$, so $(I : J) = (I : \langle x \rangle) \cap (I : \langle y \rangle)$.

First we calculate $(I : x)$. Notice that we know how to calculate $I \cap \langle x \rangle$ now. After a calculation, $I \cap \langle x \rangle = \{ x^2z - xy^2, x^4 - xyz, x^3y - xz^2 \}$, so $(I : x) = \langle f_1/x, f_2/x, f_3/x \rangle = I + \langle x^2y - z^3 \rangle$. Simarly one could find that $(I : y) = (I : x)$, thus $(I : J) = (I : x)$.

Hence $V = \mathcal{V}(x, y) \cap \mathcal{V}(xz - y^2, x^3 - yz, x^2y - z^2)$.

Prop 6.5.2. In general, if $W \subseteq \mathbb{A}_k^n$ is an affine algebraic set defined by $x_i = f_i(t_1, \dots, t_m)$, then W is irreducible.

Prop 6.5.3. If $f : V \to W$ with $\overline{f(V)} = \mathcal{V}(\ker f^*)$, where $f^* : k[W] \to k[V]$.

6.6 Local Rings

From now on, R is a commutative ring with 1.

Def 121. R is called a local ring if it has a unique maximal ideal.

Prop 6.6.1.

(1) R is a local ring.

(2) The set of non-units forms an ideal.

(3) $\exists\, M \in \operatorname{Max} R$ s.t. $1+m$ is a unit $\forall\, m \in M$.

Proof.

(1) ⇒ (2): Let M be the unique maximal ideal of R. Then M couldn't contain any unit. For each non-unit x, $\langle x \rangle \neq R$ and is contained in a maximal ideal by lemma 7, thus $x \in M$. Hence $M = \{\text{ non-units }\}$.

(2) ⇒ (3): This ideal must be a maximal ideal M since it can't be extended. Now, $1 \notin M \rightsquigarrow 1+m \notin M$. So $1+m$ is a unit.

(3) ⇒ (1): If there exists another maximal ideal N, then $M+N=R$. Say $m \in M, n \in N$ s.t. $m+n=1$, then $n = 1-m$ is a unit $\implies N = R$, which is a contradiction.

□

Eg 6.6.1. $k[[x]]$ is a local ring with the unique maximal ideal $\langle x \rangle$.

Proof. For each $f = \sum a_n x^n \in k[[x]]$, one could see that f is an unit if and only if $a_n \neq 0$, and the leftovers form an ideal $\langle x \rangle$. □

Eg 6.6.2. Let $P \in \operatorname{Spec} R$. If $S = R \setminus P$, then S is a multiplicatively closed set with $1 \in S$ and $R_P \triangleq R_S$ is a local ring.

Proof. S is a multiplicatively closed set simply follow from the definition of prime ideal. One could then easily see that $P_P \triangleq \left\{ \frac{x}{s} \mid x \in P, s \in S \right\}$ contains all non-unit, thus R_P is local. □

Prop 6.6.2. The following sets are correspondent (k is algebraically closed):

(1) $\mathbb{A}_k^n$

(2) $\operatorname{Max} k[x_1, \ldots, x_n]$

(3) $\operatorname{Hom}_k(k[x_1, \ldots, x_n], k)$

Proof. (1) ⇒ (2): For any $(a_1, \ldots, a_n) \in \mathbb{A}_k^n$, $k[x_1, \ldots, x_n]/\langle x_1 - a_1, \ldots, x_n - a_n \rangle \cong k$ is a field, hence $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is a maximal ideal.

(2) ⇒ (1): Let $M \in \operatorname{Max} k[x_1, \ldots, x_n]$, by theorem 76, $\mathcal{V}(M) \neq \varnothing$, so exists $(a_1, \ldots, a_n) \in \mathcal{V}(M)$. Now $M = \sqrt{M} = \mathcal{I}(\mathcal{V}(M)) \subseteq \mathcal{I}((a_1, \ldots, a_n)) = \langle \ldots, x_i - a_i, \ldots \rangle$ which is maximal, We conclude that $(a_1, \ldots, a_n)$ is the only element in $\mathcal{V}(M)$ and $M = \langle \ldots, x_i - a_i, \ldots \rangle$.

(1) ⇒ (3): For each $(a_1, \ldots, a_n)$, define $\varphi \in \operatorname{Hom}_k(\cdots)$ by evaluation:

$$\begin{aligned} \varphi: \quad k[x_1, \ldots, x_n] &\longrightarrow k \\ x_i &\longmapsto a_i \end{aligned}$$

(3) ⇒ (1): Similarly, for each $\varphi \in \operatorname{Hom}_k(\cdots)$, recover $(a_1, \ldots, a_n)$ by $(\varphi(x_1), \ldots, \varphi(x_n))$. □

Remark 35. Inspired by the correspondence,

Def 122. A property of an R-module M is said to be a local property if

$$M \text{ has this property } \iff M_P \text{ (as an } R_P\text{-module) has this property } \forall\, P \in \operatorname{Spec} R$$

Prop 6.6.3. TFAE

(1) $M = 0$

(2) $M_P = 0 \quad \forall\, P \in \operatorname{Spec} R$

(3) $M_Q = 0 \quad \forall\, Q \in \operatorname{Max} R$

Proof. (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) are clear.

(3) $\Rightarrow$ (1): If $M \neq 0$, let $x \in M$ such that $x \neq 0$, then $\operatorname{Ann}(x) \subsetneq R$ since $1 \notin \operatorname{Ann}(x)$. Let $\operatorname{Ann}(x) \subset Q \in \operatorname{Max} R$. By assumption, $M_Q = 0$ implies $\frac{x}{1} = \frac{0}{1}$. By the definition of equal in localization, $\exists\, r \notin Q$ such that $rx = 0$, thus $r \in \operatorname{Ann}(x)$ which leads to an contradiction. $\square$

Coro 6.6.1. Let $N \subseteq M$, TFAE (consider M/N)

(1) $N = M$

(2) $N_P = M_P \quad \forall\, P \in \operatorname{Spec} R$

(3) $N_Q = M_Q \quad \forall\, Q \in \operatorname{Max} R$

Prop 6.6.4. TFAE

(1) $0 \to M \xrightarrow{\phi} N \xrightarrow{\psi} L \to 0$ exact

(2) $0 \to M_P \xrightarrow{\phi_P} N_P \xrightarrow{\psi_P} L \to 0$ exact $\forall\, P \in \operatorname{Spec} R$

(3) $0 \to M_Q \xrightarrow{\phi_Q} N_Q \xrightarrow{\psi_Q} L \to 0$ exact $\forall\, Q \in \operatorname{Max} R$

Proof. (1) $\Rightarrow$ (2): By the fact that localization preserves exact sequence.

(2) $\Rightarrow$ (3): Obvious.

(3) $\Rightarrow$ (1): Let $K = \ker \phi$, then $0 \to K \to M \to N$ exact. Since we just proved (1) $\Rightarrow$ (3), $0 \to K_Q \to M_Q \to N_Q$ exact, but $K_Q = 0$, by proposition 6.6.3, $K = 0$.

We could prove the other half similarly by letting K to be the cokernel. $\square$

Def 123.

- Let $R \subseteq S$. $\bar{R} = \{\, x \in S \mid x \text{ is integral over } R \,\}$ is called the integral closure of R in S.
- R is integrally closed in S if $R = \bar{R}$.
- An integral domain R is called normal if R is integrally closed in its field of fractions.

Theorem 86. UFD is normal.

Proof. Let R be a UFD and K be its field of fractions. If $a \in K$ is integral over R and $a^n + r_1 a^{n-1} + \cdots + r_n = 0$. Write $a = u/s$ with $\gcd(u, s) = 1$. Then $u^n + r_1 s u^{n-1} + \cdots + r_n s^n = 0$. Now if s is a non-unit, says $p \mid s$ with p is a prime. Then $p \mid u$ obviously $\rightsquigarrow p \mid \gcd(u, s) = 1$, which is a contradiction. So s is a unit $\implies a \in R$. $\square$

Prop 6.6.5.

- Let S/R is an integral extension and $T \subset R$ be a m.c. set with $1 \in T$. Then S_T is also integral over R_T.

  Proof. Let $a/t \in S_T$ with $a^n + r_1 a^{n-1} + \cdots + r_n = 0$, then we have

  $$\left(\frac{a}{t}\right)^n + \frac{r_1}{t}\left(\frac{a}{t}\right)^{n-1} + \cdots + \frac{r_n}{t^n}\left(\frac{a}{t}\right)^n = 0$$

  Thus a/t is integral over R_T. □

- Let S/R be an arbitrary extension and $T \subset R$ be m.c. with $1 \in T$. Then $(\bar{R})_T = \overline{(R_T)}$ in S_T.

  Proof. By 1., $(\overline{R})_T$ is integral over R_T. If $a/t \in S_T$ is integral over R_T, say

  $$\left(\frac{a}{t}\right)^n + \frac{r_1}{t_1}\left(\frac{a}{t}\right)^n + \cdots + \frac{r_n}{t_n}\left(\frac{a}{t}\right)^n = 0$$

  If we let $v = t_1 t_2 \cdots t_n$, multiply the equation by $(tv)^n$, we get

  $$(va)^n + (r_1 t t_2 \cdots t_n)(va)^{n-1} + \cdots = 0 \implies va \in \overline{R}$$

  So $a/t = va/(vt) \in \overline{R}_T$. □

Prop 6.6.6. "Being normal" is a local property. TFAE

(1) R is normal

(2) R_P is normal $\forall\, P \in \operatorname{Spec} R$

(3) R_Q is normal $\forall\, Q \in \operatorname{Max} R$

Proof. The key is to realize that if K is the field of fraction of R, then K is also the field of fraction of any R_P. Then by lemma 6.6.4,

$$0 \to R \to \overline{R} \to 0 \iff 0 \to R_P \to (\overline{R})_P \to 0, \forall\, P$$

By the previous proposition, $(\overline{R})_P = \overline{R_P}$ in S_P, this proves all. □

Def 124. An R-module F is flat if the functor $- \otimes_R M$ is exact (i.e., it preserves exact sequence).

Prop 6.6.7. Given an homomorphism $R_1 \to R_2$. If M is a flat R_1-module, then $R_2 \otimes_{R_1} M$ is a flat R_2 module.

Proof. Notice that $N \otimes_{R_1} M \cong N \otimes_{R_2} (R_2 \otimes_{R_1} M)$, so

$$\begin{aligned} 0 \to N \to N' \text{ exact } &\implies 0 \to N \otimes_{R_1} M \to N' \otimes_{R_1} M \text{ exact} \\ &\implies 0 \to N \otimes_{R_2} (R_2 \otimes_{R_1} M) \to N' \otimes_{R_2} (R_2 \otimes_{R_1} M) \text{ exact} \end{aligned}$$

Which is to say that $R_2 \otimes_{R_1} M$ flat. □

Prop 6.6.8. TFAE

(1) M is a flat R-module

(2) M_P is a flat R-module $\forall\, P \in \operatorname{Spec} R$

(3) M_Q is a flat R-module $\forall\, Q \in \operatorname{Max} R$

Proof. (1) $\Rightarrow$ (2): By the previous proposition combined with the property of localization, $M_P \cong R_P \otimes_R M$ is a flat module.

(2) $\Rightarrow$ (3): Obvious.

(3) $\Rightarrow$ (1): If $0 \to N \to N'$ exact, then by prop 6.6.4, $0 \to N_Q \to N'_Q$ exact, so

$$0 \to N_Q \otimes_{R_Q} M_Q \to N'_Q \otimes_{R_Q} M_Q$$

is also exact. By the property of localization, $N_Q \otimes_{R_Q} M_Q \cong (N \otimes_R M)_Q$. Using prop 6.6.4, $0 \to N \otimes_R M \to N' \otimes_R M$ exact. $\square$

6.7 Krull dimension

Def 125.

- The Krull dimension of a topological space X is the supremum of the lengths n of all chains $X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$, where X_i are closed irreducible subset of X.
- The Krull dimension of a commutative ring R with 1 is the supremum of the lengths n of all chains $P_0 \subsetneq \cdots \subsetneq P_n$ where $P_i \in \operatorname{Spec} R$.

Prop 6.7.1. Let $R \subseteq S$ be two integral domains and S/R be integral. Then S is a field if and only if R is a field.

Proof. "$\Rightarrow$": For each $a \neq 0$ in R, $a^{-1} \in S$, so we could write

$$(a^{-1})^n + r_1(a^{-1})^{n-1} + \cdots + r_n = 0,\ \ r_i \in R$$

Which implies

$$a^{-1} = -(r_1 + \cdots + r_n a^{n-1}) \in R$$

"$\Leftarrow$": For each $a \neq 0$ is S, write

$$a^n + r_1 a^{n-1} + \cdots + r_n = 0,\ \ r_i \in R$$

Notice that we could assume $r_n \neq 0$, or else $a(a^{n-1} + r_1 a^{n-2} + \cdots + r_{n-1}) = 0$ and hence $a^{n-1} + r_1 a^{n-2} + \cdots + r_{n-1} = 0$ because R is an integral domain. Then

$$a^{-1} = -r_n^{-1}(a^{n-1} + r_1 a^{n-2} + \cdots + r_{n-2})$$

$\square$

Prop 6.7.2. Let S/R be integral.

1. If $q \in \operatorname{Spec} S$ and $p = q \cap R \in SpecR$, then $q \in \operatorname{Max} S \iff p \in \operatorname{Max} R$.

   Proof. It is easy to see that S/q is integral over R/p by the identification

$$\begin{aligned} R/p &\hookrightarrow S/p \\ r + p &\longmapsto r + q \end{aligned}$$

   So

$$q \in \operatorname{Max} S \iff S/q \text{ is a field } \iff R/p \text{ is a field } \iff p \in \operatorname{Max} R$$

$\square$

2. If $q, q' \in \operatorname{Spec} S$ with $q \subseteq q'$ and $q \cap R = p = q' \cap R$. Then $q = q'$.

   Proof. We know that $S_P \triangleq S_{R \setminus P}$ is integral over R_P. Since $q_P \subseteq q'_P$ and both $q_p \cap R_P$ and $q'_p \cap R_P$ equal P_P is maximal in R_P. Using 1., q_P, q'_P are maximal in S_P, but $q_P \subseteq q'_P \implies q_P = q'_P$. By corollary 6.6.1, $q = q'$. $\square$

Theorem 87 (Going-up theorem)**.** Let S/R be integral, then

- If $p \in \operatorname{Spec} R$, then $\exists\, q \in \operatorname{Spec} S$ such that $q \cap R = p$.
- If $p_1 \subset p_2$ in $\operatorname{Spec} R$ and $q_1 \in \operatorname{Spec} S$ with $q_1 \cap R = p_1$, then $\exists\, q_2 \in \operatorname{Spec} S$ with $q_1 \subset q_2$ and $q_2 \cap R = p_2$.

Theorem 88. If S/R is integral, then $\dim S = \dim R$.

Prop 6.7.3. Let S, R be integral domains and S/R be integral, assume R is normal with the field of fractions K. If $a \in S$ is integral over $I \subseteq R$, then $f = m_{\alpha,K} = x^n + r_1 x^{n-1} + \cdots + r_n$ with $r_i \in \sqrt{I}$.

Theorem 89 (Going-down theorem)**.** Let S, R be integral domains and S/R be integral, assume R is normal with the field of fractions K. If $p_1 \supset p_2$ in $\operatorname{Spec} R$ and $q_1 \in \operatorname{Spec} S$ with $q_1 \cap R = p_1$, then $\exists\, q_2 \in \operatorname{Spec} S$ such that $q_1 \supset q_2$ and $q_2 \cap R = p_2$.

Theorem 90. All maximal chain in $\operatorname{Spec} K[x_1, \ldots, x_n]$ have the same length n, and thus

$$\dim k[x_1, \ldots, x_n] = n.$$

6.8 Artinian rings and DVR

6.8.1 Artinian rings

Def 126. R is called an Artinian ring if one of the followings holds:

- any non-empty set of ideals has a minimal element.
- any descending chain of ideals is stationary (DCC).

Goal:

1. $R = \cong R_1 \times \cdots \times R_l$ where R_i is an Artinain local rings.
2. Artinian $\iff$ Noetherian $+ \dim = 0$.

Prop 6.8.1. Let R be an Artinian ring

(1) $I \subseteq R \rightsquigarrow R/I$ is also Artinian.

(2) If R is an integral domain, then R is a field.

Proof. $\forall \underset{\neq 0}{a} \in R, \langle a \rangle \supseteq \langle a^2 \rangle \supseteq \cdots$ is a descending chain of ideals $\implies \langle a^l \rangle = \langle a^{l+1} \rangle = \cdots$ for some $l \in \mathbb{N} \implies a^l = ba^{l+1} \implies a^l(1-ab) = 0 \implies ab = 1$ since $a^l \neq 0$. □

(3) $\operatorname{Spec} R = \operatorname{Max} R$. ($\implies \dim R = 0$)

Proof. $\forall p \in \operatorname{Spec} R, R/p$ is an integral domain $\rightsquigarrow R/p$ is a field $\rightsquigarrow p \in \operatorname{Max} R$. □

(4) $|\operatorname{Max} R| < \infty$.

Proof. Consider the set $\left\{ \bigcap_{\text{finite}} \mathfrak{m} \,\middle|\, \mathfrak{m} \in \operatorname{Max} R \right\} \neq \emptyset$. So there exists a minimal element in this set (R is Artinian), say $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$. Now, for $\mathfrak{m} \in \operatorname{Max} R$, we have $\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$ since the latter is minimal $\implies \mathfrak{m} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k \rightsquigarrow \mathfrak{m} \supseteq \mathfrak{m}_i$ for some $i \rightsquigarrow \mathfrak{m} = \mathfrak{m}_i$. So $\operatorname{Max} R = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_k\}$. □

(5) $\exists\, n_1, \ldots, n_k \in \mathbb{N}$ s.t. $\langle 0 \rangle = \mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \overset{\star}{=} \mathfrak{m}_1^{n_1} \cap \mathfrak{m}_2^{n_2} \cap \cdots \cap \mathfrak{m}_k^{n_k}$.

Proof. $\star$: Recall I_i, I_j are coprime for $i \neq j \rightsquigarrow \prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$. And

$$\sqrt{\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j}} = \sqrt{\sqrt{\mathfrak{m}_i^{n_i}} + \sqrt{\mathfrak{m}_j^{n_j}}} = \sqrt{\mathfrak{m}_i + \mathfrak{m}_j} = \sqrt{R} = R \rightsquigarrow \mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j} = R.$$

Now, since R is Artinian, $\forall\, i, \exists\, n_i \in \mathbb{N}$ s.t. $\mathfrak{m}_i^{n_i} = \mathfrak{m}_i^{n_i+1} = \cdots$ Assume $\mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \neq 0$, consider the set $\mathcal{S} = \{ J \subseteq R \,|\, J\mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \neq 0 \}$ [3] and let J_0 be the minimal element of $\mathcal{S}$.

So there exists $x \in J_0$ s.t. $x\mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \neq 0$. We know that $\langle x \rangle \subseteq J_0 \rightsquigarrow J_0 = \langle x \rangle$. We also find that $x\mathfrak{m}_1^{n_1+1} \mathfrak{m}_2^{n_2+1} \cdots \mathfrak{m}_k^{n_k+1} = x\mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \neq 0$. This implies $x\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_k \in \mathcal{S}$. But $x\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_k \subseteq \langle x \rangle = J_0 \implies x\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_k = \langle x \rangle = xR$. Write

$$(\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_k) xR = xR \rightsquigarrow (\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_k) xR = xR \rightsquigarrow (\operatorname{Jac} R) xR = xR$$

By Nakayama's lemma, $xR = 0 \implies x = 0$, which is a contradiction. □

[3] this set is non-empty since $\mathfrak{m}_i$ in it.

(6) The nilradical $\mathfrak{n}_R$ of R is nilpotent.

Proof. By (3), $\mathfrak{n}_R = \operatorname{Jac} R$. Let $n = \max\{n_1, \dots, n_k\}$ in (5), then $\mathfrak{n}_R^n = (\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_k)^n = 0$. $\square$

<u>Goal 1:</u> $R \cong R_1 \times R_k$ where R_i is Artinian local ring.

Proof. By Chinese Remainder theorem,

$$R \cong R/\langle 0 \rangle = R/\mathfrak{m}_1^{n_1}\mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \cong R/\mathfrak{m}_1^{n_1} \times R/\mathfrak{m}_2^{n_2} \times \cdots \times R/\mathfrak{m}_k^{n_k}$$

Let $R_i = R/\mathfrak{m}_i^{n_i}$, then $\bar{\mathfrak{m}} \in \operatorname{Max} R_i$ if $\mathfrak{m} \in \operatorname{Max} R$ and $\mathfrak{m} \supset \mathfrak{m}_i^{n_i} \rightsquigarrow \mathfrak{m} = \mathfrak{m}_i$. So $\operatorname{Max} R_i = \{\, \bar{\mathfrak{m}_i} \,\} \implies R_i$ is a local ring. $\square$

Lemma 23. Let V be a K-vector space, TFAE

(1) $\dim_k V < \infty$

(2) V has DCC on subspaces.

(3) V has ACC on subspaces.

Proof. $\square$

<u>Observation:</u> If R is Northerian and $\dim R = 0$, then $\langle 0 \rangle = \bigcap_{i=1}^k q_i$ (primary decomposition) and $\sqrt{q_i} = \mathfrak{m}_i \in \operatorname{Max} R$.

Since $\mathfrak{m}_i$ is finitely generated, $\exists\, n_i$ s.t. $\mathfrak{m}_i^{n_i} \subseteq q_i$. Hence

$$\langle 0 \rangle \subseteq \mathfrak{m}_1^{n_1}\mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} = \mathfrak{m}_1^{n_1} \cap \mathfrak{m}_2^{n_2} \cap \cdots \cap \mathfrak{m}_k^{n_k} \subseteq q_1 \cap q_2 \cap \cdots \cap q_k = \langle 0 \rangle$$
$$\implies \mathfrak{m}_1^{n_1}\mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} = \langle 0 \rangle$$

<u>Goal 2:</u> In a ring R, let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be, not necessarily different, maximal ideals in R s.t. $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n = 0$. Then R is Artinian $\iff$ R is Noetherian.

Proof. We have a chain of ideals in R: $\mathfrak{m}_0 = R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n = 0$.

Let $M_i = \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_i$ as R-module. Notice that $\mathfrak{m}_i M_i = 0$, we can treat M_i as $R/\mathfrak{m}_i$-module. But $R/\mathfrak{m}_i$ is a field, so M_i can be regarded as a vector space. Hence,

$$M_i \text{ is Artinian } \iff M_i \text{ is Noetherian.}$$

By definition, $0 \to \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_i \to \mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_{i-1} \to M_i \to 0$ is exact in $\mathbf{Mod}_R$. By Ex1, $\square$

6.8.2 DVR (Discrete Valuation Ring)

Def 127.

(1) Let K be a field. A discrete valuation of K is $\nu : K^\times \twoheadrightarrow \mathbb{Z}$ ($\nu(0) = \infty$) s.t.

- $\nu(xy) = \nu(x) + \nu(y)$.
- $\nu(x \pm y) = \min\{\nu(x), \nu(y)\}$.

(2) The valuation ring of ν is $R = \{\, x \in K \mid \nu(x) \geq 0 \,\}$, called a DVR.

- $\mathfrak{m} = \{\, x \in R \mid \nu(x) > 0 \,\}$ is the unique maximal ideal in R since $\nu(x) = 0 \iff x$ is a unit.

- Let $t \in R$ with $\nu(t) = 1$, then $\mathfrak{m} = \langle t \rangle$.
- Let $I \subseteq \mathfrak{m}$ and define $m = \min\{\, l \in \mathbb{N} \mid x = t^l u \quad \forall\, x \in I \,\}$. Then $I = \langle t^m \rangle$.

Prop 6.8.2. R is a DVR $\iff$ R is 1-dimensional normal, Noetherian local domain.

Proof. □

6.8.3 Dedekind domains

Def 128. A Dedekind domain is a Noetherian normal domain of dim 1.

Def 129. Let R be an integral domain and $K = \mathrm{Frac}(R)$. A nonzero R-submodule I of K is called a fractional ideal of R if $\exists\, 0 \neq a \in R$ s.t. $aI \subset R$.

Eg 6.8.1. If $I = \langle f_1, \ldots, f_n \rangle_R$ with $f_i = \frac{a_i}{b_i} \in K$, then $a = b_1 b_2 \cdots b_n$ and $aI \subset R \implies I$ is fractional.

In general, if R is a Noetherian, then every fractional ideal I of R is finitely generated.

Def 130. A fractional ideal I of R is invertible if $\exists\, J$: a fractional ideal of R s.t. $IJ = R$.

Prop 6.8.3.

1. If I is invertible, then $J = I^{-1}$ is unique and equals $J = (R : I) \triangleq \{\, a \in K \mid aI \subset R \,\}$.

   Proof. □

2. If I is invertible, then$I$ is a finitely generated R-module.

   Proof. □

3. Let R be a local domain but not a field, $K = \mathrm{Frac}(R)$. Then R is a DVR $\iff$ every nonzero fractional ideal I of R is invertible.

   Proof. □

Theorem 91. Let R be an integral domain and $K = \mathrm{Frac}(R)$. TFAE

(a) R is a Dedekind domain.
(b) R is Noetherian and R_P is a DVR for all $P \in \mathrm{Spec}\, R$.
(c) Every nonzero fractional ideal of R is invertible.
(d) Every nonzero proper ideal of R can be written (uniquely) as a product of powers of prime ideals.

Proof.

(a)⇔(b):

- R is normal $\iff$ R_P is normal for all $P \in \mathrm{Spec}\, R$.
- $\dim R_P = 1 \quad \forall\, P \in \mathrm{Spec}\, R \iff h(P) = 1 \quad \forall\, 0 \neq P \in \mathrm{Spec}\, R \iff \dim R = 1$.

(b)⇔(c):

(a)$\Leftrightarrow$(b):

(a)(b)(c)$\Rightarrow$(d):

(d)$\Rightarrow$(c):

$\square$

7 Introduction to Homological Algebra

7.1 Projective, Injective and Flat modules

Def 131.

- $M \in \mathbf{Mod}_R$ is **projective** if $\operatorname{Hom}(M, \cdot)$ preserves the *right* exactness.
- $N \in \mathbf{Mod}_R$ is **injective** if $\operatorname{Hom}(\cdot, N)$ preserves the *right* exactness.
- $M \in \mathbf{Mod}_R$ is **flat** if $M \otimes \cdot$ preserves the *left* exactness.

Fact 7.1.1.

- M is projective $\iff$ $$\begin{tikzcd} & M \arrow[dl, "\exists \tilde{f}"'] \arrow[d, "f"] & \\ M_2 \arrow[r] & M_3 \arrow[r] & 0 \end{tikzcd}$$
- N is injective $\iff$ $$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r] \arrow[d, "g"'] & M_2 \arrow[dl, "\exists \tilde{g}"] \\ & N & \end{tikzcd}$$
- free $\implies$ projective: If $X = \{ x_i \mid i \in \Lambda \}$ and $f : x_i \mapsto a_i$. Then we can set $\tilde{f} : x_i \mapsto b_i$ for any b_i s.t. $\beta : b_i \mapsto a_i$.
$$\begin{tikzcd} & F(X) \arrow[dl, "\exists \tilde{f}"'] \arrow[d, "f"] & \\ M_2 \arrow[r, "\beta"] & M_3 \arrow[r] & 0 \end{tikzcd}$$
- free $\implies$ flat:
- If S is a m.c. set in R with $1 \in S$, then
$$0 \to M \to N \to L \to 0 \implies 0 \to M_S \to N_S \to L_S \to 0.$$
We know that $M_S \cong R_S \otimes_R M$. So R_S is a flat R-module. $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.
- $\forall\, M \in \mathbf{Mod}_R, \exists\, F$: free on X s.t. $F \to M \to 0$. This is obvious since we can choose X to be the generating set of M.

Ques: $\forall\, M \in \mathbf{Mod}_R$, does there exist $N \in \mathbf{Mod}_R$ is injective s.t. $0 \to M \to N$?

Theorem 92 (Boer's criterion)**.** N is injective $\iff \forall\, I \subset R$, $$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] \arrow[d, "f"'] & R \arrow[dl, dashed, "\exists h"] \\ & N & \end{tikzcd}$$

Proof. □

Def 132. M is **divisible** if $\forall\, x \in M, r \in R \setminus \{0\}$, there exists $y \in M$ such that $x = ry$, i.e. $rM = M \quad \forall\, r \in R \setminus \{0\}$.

Prop 7.1.1.

1. Every injective module N over an integral domain is divisible.

   Proof. □

2. Every divisible module N over an PID is injective.

Proof. □

Theorem 93. $\forall\, M \in \mathbf{Mod}_R$, $\exists\, N$ is injective s.t. $M \hookrightarrow N$.

Proof. 1. If $R = \mathbb{Z}$,

□

Prop 7.1.2. TFAE

1. M is projective.
2. $\forall \quad 0 \to M_1 \to M_2 \to M \to 0$ is split exact.
3. $\exists\, M'$ s.t. $M \oplus M' \cong F$: free.

Prop 7.1.3. TFAE

1. M is projective.
2. $\forall \quad 0 \to M_1 \to M_2 \to M \to 0$ is split exact.
3. $\exists\, M'$ s.t. $M \oplus M' \cong F$: free.

Prop 7.1.4. TFAE

1. M is injective.
2. $\forall \quad 0 \to M \to M_2 \to M_3 \to 0$ is split exact.

Prop 7.1.5. projective $\implies$ flat.

Index