Summary of Algebra

Author: Jacky567

Qiuzhen College, Tsinghua University
2026 Summer

Contents

Chapter 1

Group Theory

1.1 Conjugation

Def 1.1.1. Conjugation is an action of G on itself given by

$$(g, h) \mapsto ghg^{-1}.$$

The stabilizer of $g \in G$ is called the centralizer of g:

$$Z(g) = \{h \in G | gh = hg\}.$$

The orbit of $g \in G$ is called the conjugacy class of g:

$$C(g) = \{hgh^{-1} | h \in G\}.$$

The center of G consists of all elements that commute with every element in G:

$$Z = \{g | gh = hg \text{ for all } h \in G\}$$

Prop 1.1.1. *(1)* $g \in Z(g), Z \subset Z(g)$.

(2) $g \in Z$ *iff* $Z(g) = G$, i.e. $C(g) = \{g\}$.

Prop 1.1.2 (class equation)**.**

$$|G| = \sum_{conj.\ class\ C} |C|$$

Def 1.1.2. Consider the conjugation acts on subgroup H of G, the stabilizer of H is called the normalizer of H:

$$N(H) = \{g | gHg^{-1} = H\}.$$

Prop 1.1.3. *Let* $N = N(H)$ *be the normalizer of* H.

(1) $H \triangleleft N$

(2) $H \triangleleft G$ *iff* $N = G$.

1.2 Sylow theorems

Def 1.2.1. A group whose order is positive powers of a prime p is called p-group.

Prop 1.2.1. *The center of a* p*-group is not trivial.*

Proof. Let $C_1, \cdots, C_k$ be all conjugacy classes of G and $C_1 = \{e\}$.
Then $|C_i| = p^{t_i}$ for some $t_i > 0$ and $i \geqslant 2$ since $|C_i| > 1, |C_i||G|$.
By class equation, $|G| = \sum |C_i| = 1 + pt$ for some $t \in \mathbb{Z}$, contradiction! □

Prop 1.2.2. *The group of order p^2 is abelian.*

Proof. Suppose G is not abelian.
Then $|Z(G)| = p$, take $g \notin Z(G)$.
Since $Z(G) \subset Z(g)$ and $g \in Z(g)$.
So $|Z(g)| = p^2$, *i.e.* $Z(g) = G$.
Therefore $g \in Z(G)$, contradiction! □

Coro 1.2.1. *A group of order p^2 is either C_{p^2} or $C_p \times C_p$.*

Def 1.2.2. Let $|G| = n$ and $n = p^e m$, a subgroup H of G of order p^e is called Sylow p-subgroup.

Thm 1.2.1 (Sylow first theorem)**.** *Sylow p-subgroup always exists.*

Thm 1.2.2 (Sylow second theorem)**.** *(1) Sylow p-subgroups are conjugate subgroups*

(2) Every p-subgroup of G is contained in a Sylow p-subgroup.

Thm 1.2.3 (Sylow third theorem)**.** *Let s be the number of Sylow p-subgroups, then $s|m$ and $s \equiv 1 \pmod{p}$.*

Exam 1.2.1. *Let G be a group of order 12 and s, t be the number of Sylow 2-subgroups, Sylow 3-subgroups resp.*
Then $s = 1$ or 3 and $t = 1$ or 4.
If $s = t = 1$, let H, K be the Sylow 2-subgroup and Sylow 3-subgroup resp.
Then they are both normal.
So $H \cap K = \{1\}$ and $|H||K| = |G|$.
Thus $G = H \times K \cong C_2 \times C_2 \times C_3$ or $C_4 \times C_3$.
If $s = 1, t = 4$, let $H, K_1, \cdots, K_4$ be the Sylow 2-subgroup and Sylow 3-subgroups resp.
Then $|H \cup K_1 \cup \cdots \cup K_4| = 1 + 3 + 2 + 2 + 2 + 2 = 12$.
So all elements in G is contained in one of $H, K_1, \ldots, K_4$.
Notice that there is an action of G on $\{K_1, \ldots, K_4\}$ given by conjugation, it then induce a homeomorphism $f : G \to S_4$.
And since the normalizer N_i of K_i must be of order $12/4 = 3$.
Therefore for $k_i \in K_i$, $f(k_i)$ is a 3-cycle of $\{1, 2, 3, 4\}\backslash\{i\}$.
And for $h \in H$, $f(h)$ does not fix any elements, i.e. *f is injective.*
Thus $G < S_4$ and is of order 12, i.e. *$G \cong A_4$.*
If $s = 3, t = 1$, let H, K be a Sylow 2-subgroup and the Sylow 3-subgroup.
Then H is not normal and K is normal.
If $H \cong C_4$, let $H = \langle h \rangle, K = \langle k \rangle$.
So $khk^{-1} \notin H$ and $hkh^{-1} \in K$.
Thus $hk = k^2 h$, i.e. *$G \cong \langle h, k | h^4, k^3, hkh^{-1}k \rangle$.*
If $H \cong C_2 \times C_2$, let $H = \langle h_1, h_2 \rangle, K = \langle k \rangle$.
So $h_1 k h_1^{-1}, h_2 k h_2^{-1}, (h_1 h_2) k (h_1 h_2)^{-1} \in K$ and not all of $h_1, h_2, h_1 h_2$ commute with k.
Thus WLOG, $h_1 k = k h_1, h_2 k = k^2 h_2$, i.e. *$G \cong D_6$.*
If $s = 3, t = 4$, there are at least $1 + 3 + 3 + 3 + 2 + 2 + 2 + 2 = 18$ different elements in G, which is impossible.
In conclusion G is isomorphic to one of $C_4 \times C_3, C_2 \times C_2 \times C_3, A_4, D_6$ or $\langle a, b | a^4, b^3, aba^{-1}b \rangle$.

Chapter 2

Galois Theory

2.1 Field extension

Def 2.1.1. An extension of a field F is a field containing F as a subfield. The dimension of an extension E as a F-vector field is called degree of E over F, denoted by $[E : F]$. An extension is called finite extension if its degree is finite.

An F-homomorphism between two extensions E, E' of F is a homomorphism $\varphi : E \to E'$ such that $\varphi(F) = F$. An F-isomorphism is a bijective F-homomorphism.

Remark 2.1.1. F-homomorphism is always injective since its kernel must be an ideal and an ideal of a field must be trivial.

Prop 2.1.1. *Suppose fields $L \supset E \supset F$, then L/F is finite iff L/E and E/F are finite. Moreover,*

$$[L : F] = [L : E][E : F].$$

Proof. Let $(l_i), (e_j)$ be the basis of L/E and E/F, then $(l_i e_j)$ is the basis of L/F. □

Prop 2.1.2. *Let f be a monic irreducible polynomial of degree m and x be its root, then*

$$F[x] = F[X]/(f(X))$$

is a field of degree m over F.

Proof. We can easily find the inverse of an element by Bézout lemma. □

Def 2.1.2. An extension E of F is said to be simple if $E = F(\alpha)$ for some $\alpha \in E$. And in this case, such an α is called a primitive element of E.

Def 2.1.3. Let E be an extension of F and α be an element of E, consider an homomorphism

$$\varphi : F[X] \to E, f(X) \mapsto f(\alpha),$$

there are two cases:

(1) $\ker(\varphi) = 0$, that is, α is not a root for any non-trivial polynomial over F. So we say α is transcendental over F.

(2) $\ker(\varphi) \neq (0)$, take $f(X) \in \ker(\varphi)$, then $f(\alpha) = 0$. So we say α is algebraic over F. The polynomial $f \in F[X]$ such that $f(\alpha) = 0$ forms a principal ideal in $F[X]$, we call the generator the minimal polynomial of α over F. It is monic and irreducible.

Def 2.1.4. An extension E of F is said to be algebraic if every element of E is algebraic over F, otherwise it is said to be transcendental.

Prop 2.1.3. *An extension E of F is finite iff it is algebraic and finitely generated over F.*

Prop 2.1.4. *Consider fields $L \supset E \supset F$, L is algebraic over F iff L is algebraic over E and E is algebraic over F.*

Def 2.1.5. A polynomial is said to be split in $F[X]$ if it is a product of degree one polynomials in $F[X]$.

Prop 2.1.5. *For a field Ω, TFAE:*

(1) All nontrivial polynomial in $\Omega[X]$ is split in $\Omega[X]$.

(2) All nontrivial polynomial in $\Omega[X]$ has at least one root in Ω.

(3) The irreducible polynomial in $\Omega[X]$ is of degree 1

(4) Ω has no nontrivial finite extension.

Such field Ω is called algebraically closed field, and the algebraic closure of a field is its algebraically closed algebraic extension.

Prop 2.1.6. *Let Ω be an integral domain containing F as a subring, then*

$$\bar{F} = \{\alpha \in \Omega | \alpha \text{ algebraic over } F\}$$

is a field, which is called algebraic closure of F in Ω.

Moreover, if Ω is an algebraically closed field, then the algebraic closure of F in Ω is the algebraic closure of F.

2.2 Splitting fields

Prop 2.2.1. *Let $F(\alpha)$ be a simple extension and Ω be another extension of F.*

(1) Suppose α is transcendental over F, then for F-homomorphism $\varphi : F(\alpha) \to \Omega$, $\varphi(\alpha)$ is transcendental over Ω, so that there is an 1-1 correspondence

$$\{F\text{-homomorphisms } F(\alpha) \to \Omega\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } F\}.$$

(2) Suppose α is algebraic over F and let f be its minimal polynomial, then for F-homomorphism $\varphi : F[\alpha] \to \Omega$, $\varphi(\alpha)$ is a root of f in Ω, so that there is an 1-1 correspondence

$$\{F\text{-homomorphisms } F[\alpha] \to \Omega\} \leftrightarrow \{\text{roots of } f \text{ in } \Omega\}.$$

Def 2.2.1. Let $f \in F[X]$ be an polynomial, a field E containing F is said to split f if f splits in $E[X]$. If E split f and is generated by the roots of f, then we call E the splitting field of f.

Prop 2.2.2. *Let E_f be the splitting field of $f \in F[X]$, then*

$$[E_f : F] \leqslant (\deg f)!$$

Proof. Split a root of f each time and the degree of f decrease. □

Prop 2.2.3. *Let E be the extension of F generated by some roots of $f \in F[X]$ in E and Ω an extension of F splitting f, then the number of F-homomorphism $\varphi : E \to \Omega$ is at most $[E : F]$, and equals $[E : F]$ if the irreducible factors of f has distinct roots in Ω.*

Proof. Let $E = F[\alpha_1, \dots, \alpha_n]$ where $f(\alpha_i) = 0$.
Take $E_k = F[\alpha_1, \dots, \alpha_k]$ and f_k is the minimal polynomial of α_{k+1} in E_k.
By proposition 2.2.1, the number of E_k-homomorphism $E_k[\alpha_{k+1}] \to \Omega$ equals to the number of roots of f_k in Ω. □

Coro 2.2.1. *Any two splitting field of f are F-isomorphic.*

Proof. By proposition 2.2.3, there exists F-homomorphism $E_1 \to E_2$ and $E_2 \to E_1$.
Notice that F-homomorphism must be injective.
So $[E_1 : F] \leqslant [E_2 : F]$ and $[E_2 : F] \leqslant [E_1 : F]$. □

Coro 2.2.2. *Suppose E and L are extensions of F and E is finite over F, then the number of F-homomorphism $E \to L$ is at most $[E : F]$.*

Proof. Let $E = F[\alpha_1, \dots, \alpha_n]$ and f is the product of the minimal polynomials of $\alpha_1, \dots, \alpha_n$.
Take a extension Ω of L that splits f.
By proposition 2.2.3, the number of F-homomorphism $E \to L \hookrightarrow \Omega$ is at most $[E : F]$. □

2.3 Separable polynomial and perfect field

Prop 2.3.1. *The gcd of two polynomial in F is also the gcd of them in the extension field. In particular, distinct irreducible polynomials in $F[X]$ do not acquire a common root in any extension of F.*

Proof. By Bézout lemma. □

Def 2.3.1. Let $f \in F[X]$ and f splits into linear factors

$$f(X) = a \prod_{i=1}^{r} (X - \alpha_i)^{m_i}$$

in $E[X]$ for some extension E of F. We say α_i is a root of f of multiplicity m_i in E. α_i is called a multiple root of f if $m_i > 1$ and is called a simple root otherwise.

Lemma 2.3.1. *A root of f is multiple iff it is also a root of f'.*

Proof. Let $f = (x - \alpha)^m g$ where g is also a polynomial.
Then $f'(x) = m(x - \alpha)^{m-1} g + (x - \alpha)^m g'$.
So $m > 1$ iff $f'(\alpha) = 0$. □

Prop 2.3.2. *Let f be an irreducible polynomial, TFAE:*

(1) f has a multiple root.

(2) $\gcd(f, f') \neq 1$.

(3) F has nonzero characteristic p and f is a polynomial of X^p.

(4) all roots of f are multiple.

Proof. (1) ⇒ (2): By lemma 2.3.1.
(2) ⇒ (3): Since f is irreducible and $\gcd(f, f') \neq 1$.
So $f' = 0$ and by expands the polynomial, we can complete the proof.
(3) ⇒ (4): Let $f(X) = g(X^p)$ where g is an polynomial and $g(X) = \prod (X - \beta_i)^{m_i}$.
Then $\beta_i = \alpha_i^p$ for some α_i and we obtain that

$$f(X) = \prod (X^p - \alpha_i^p)^{m_i} = \prod (X - \alpha_i)^{pm_i}.$$

(4) ⇒ (1): Trivial. □

Def 2.3.2. A polynomial is separable if it only have simple roots.

Def 2.3.3. A field F is perfect if it has characteristic zero or it has characteristic p and every every element of F is a p-th power.

Prop 2.3.3. *A field F is perfect iff every irreducible polynomial $f \in F[X]$ is separable.*

Proof. Suppose f is not separable.
By proposition 2.3.2, $f(X) = a_n X^{pn} + \cdots + a_1 X^p + a_0$.
And let $a_n = b_n^p$ with $b_n \in F$.
Then $f(X) = (b_n X^n)^p + \cdots + (b_1 X)^p + b_0^p = (b_n X^n + \cdots + b_1 X + b_0)^p$ is not irreducible. □

2.4 Galois extension

Def 2.4.1. An F-isomorphism $E \to E$ is called an F-automorphism of E. All F-automorphisms of E forms the automorphism group $\mathrm{Aut}(E/F)$.

Prop 2.4.1. *Let E be a splitting field of a separable polynomial f in $F[X]$, then $|\mathrm{Aut}(E/F)| = [E : F]$.*

Proof. By proposition 2.2.3, numbers of F-homomorphisms $E \to E$ is exactly $[E : F]$.
And since F-homomorphism is injective.
So F-homomorphism $E \to E$ must be F-isomorphism. □

Def 2.4.2. Let $G < \mathrm{Aut}(E/F)$, we set

$$E^G = \{\alpha \in E | \sigma\alpha = \alpha \text{ for all } \sigma \in G\}.$$

It is a subfield of E, called the fixed field of G.

Thm 2.4.1 (Artin)**.** *Let $G < \mathrm{Aut}(E/F)$ be a finite group, then*

$$[E : E^G] \leqslant |G|.$$

Proof. Let $G = \{\sigma_1, \ldots, \sigma_m\}$ and $\{\alpha_1, \ldots, \alpha_n\} \subset E$ with $n > m$.
We want to show that $\{\alpha_1, \ldots, \alpha_n\}$ must be linearly dependent with coefficient in E^G.
Consider equations

$$\begin{cases} \sigma_1(\alpha_1)X_1 + \cdots + \sigma_1(\alpha_n)X_n = 0 \\ \sigma_2(\alpha_1)X_1 + \cdots + \sigma_2(\alpha_n)X_n = 0 \\ \cdots \\ \sigma_m(\alpha_1)X_1 + \cdots + \sigma_m(\alpha_n)X_n = 0 \end{cases}$$

with $X_1, \ldots, X_n \in E$.
Then nontrivial solution of the equation always exists since $m < n$.
Take $c_i = \sigma_1(X_i) + \cdots + \sigma_m(X_i)$.
So we obtain that

$$\alpha_1 c_1 + \cdots + \alpha_n c_n = \sum_{i=1}^{n}\sum_{j=1}^{m} = \alpha_i \sigma_j(X_i) = \sum_{j=1}^{m}\sum_{i=1}^{n} \sigma_j(\alpha_i)X_i = 0$$

$$\sigma_j(c_i) = \sum_{k=1}^{m} \sigma_j\sigma_k(X_i) = \sum_{k=1}^{m} \sigma_k(X_i) = c_i.$$

Hence $c_i \in E^G$ and this complete the proof. □

Coro 2.4.1. *Let $G < \mathrm{Aut}(E/F)$ be a finite group, then*

$$G = \mathrm{Aut}(E/E^G).$$

Proof. Notice that $G \subset \mathrm{Aut}(E/E^G)$.
By theorem 2.4.1 and corollary 2.2.2, $[E : E^G] \leqslant |G| \leqslant \left|\mathrm{Aut}(E/E^G)\right| \leqslant [E : E^G]$. □

Def 2.4.3. An algebraic extension E/F is separable if the minimal polynomial of every element of E is separable, otherwise, it is inseparable.

A normal extension E/F is an algebraic extension such that the minimal polynomial of every element of E splits in $E[X]$.

Moreover, An extension E/F is Galois if it is finite, separable and normal. In this case, we call $\mathrm{Aut}(E/F)$ the Galois group of E over F, denoted by $\mathrm{Gal}(E/F)$.

Thm 2.4.2. *TFAE:*

(1) E is the splitting field of a separable polynomial $f \in F[X]$.

(2) E is finite over F and $F = E^{\mathrm{Aut}(E/F)}$.

(3) $F = E^G$ for some finite group $G < \mathrm{Aut}(E)$.

(4) E is Galois over F.

Proof. (1) ⇒ (2): Let $M = E^{\mathrm{Aut}(E/F)} \supset F$.
By proposition 2.2.3 and corollary 2.4.1, $[E : F] = |\mathrm{Aut}(E/F)| = |\mathrm{Aut}(E/M)| = [E : M]$.
So $M = F$.
(2) ⇒ (3): Trivial.
(3) ⇒ (4): Let $G = \{\sigma_1, \ldots, \sigma_n\}$.
Take $\alpha \in E$, Let $\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\} = \{\alpha_1, \ldots, \alpha_m\}$ where $\alpha_i \neq \alpha_j$.
Consider polynomial $f(x) = (x - \alpha_1) \ldots (x - \alpha_m)$.
Notice that $\sigma_k(\alpha_i) - \sigma_k(\alpha_j) = \sigma_k(\alpha_i - \alpha_j) \neq 0$.
So $\sigma_k(f(x)) = f(\sigma_k(x))$ for any k, *i.e.* $f \in F[X]$.
Therefore minimal polynomial of α must be separable and split in $E[X]$.
Hence E is finite, separable and normal extension over F.
(4) ⇒ (1): Let $E = F[\alpha_1, \ldots, \alpha_n]$ and f_i be the minimal polynomial of α_i over F.
Set f to be the product of all distinct f_i.
Then E is the splitting field of f since f_i split in $E[X]$.
And f is separable since f_i are separable and distinct f_i has no common roots. □

Coro 2.4.2 (Artin theorem)**.** *Let $G < \mathrm{Aut}(E)$ be a finite group and $F = E^G$, then E is a Galois extension of F with Galois group G, and $[E : F] = |G|$.*

Proof. By corollary 2.4.1 and proposition 2.2.3, $G = \mathrm{Gal}(E/F)$ and $[E : F] = |G|$. □

Coro 2.4.3. *Let $E \supset M \supset F$, if E is Galois over F, then it is Galois over M.*

Proof. Let E be the splitting field of a separable polynomial $f \in F[X]$.
Then E is the splitting field of f as an polynomial in $M[X]$. □

2.5 Fundamental theorem of Galois theory

Def 2.5.1. A subextension of E/F is an extension M/F with $M \subset E$.

Thm 2.5.1 (fundamental theorem of Galois theory)**.** *Let E be a Galois extension over F with Galois group G, then the map $H \mapsto E^H$ is a bijection from the set of subgroups of G to the set os subextensions of E/F with inverse $M \mapsto \mathrm{Gal}(E/M)$. Moreover,*

(1) $H_1 \supset H_2$ iff $E^{H_1} \subset E^{H_2}$.

(2) When $H_1 \supset H_2$, $|H_1|/|H_2| = [E^{H_2} : E^{H_1}]$.

(3) $\sigma H \sigma^{-1} \leftrightarrow \sigma M$

(4) H is normal in G iff E^H is Galois over F and in each case $\mathrm{Gal}(E^H/F) \cong G/H$.

Proof. By Artin theorem and theorem 2.4.2, $\mathrm{Gal}(E/E^H) = H$ and $M = E^{\mathrm{Gal}(E/M)}$.
So $H \mapsto E^H$ and $M \mapsto \mathrm{Gal}(E/M)$ are bijection and inverse of each other.

(1) By definition of fixed field, $H_1 \supset H_2 \Rightarrow E^{H_1} \subset E^{H_2}$.
Conversely, every E^{H_2}-automorphism of E fixed E^{H_1}.
So $H_1 = \mathrm{Gal}(E/E^{H_1}) \supset \mathrm{Gal}(E/E^{H_2}) = H_2$.

(2) $[E^{H_2} : E^{H_1}] = \frac{[E:E^{H_1}]}{[E:E^{H_2}]} = \frac{|H_1|}{|H_2|}$.

(3)
$$\begin{aligned} E^{\sigma H \sigma^{-1}} &= \{\alpha \in E | \sigma h \sigma^{-1}(\alpha) = \alpha \text{ for all } h \in H\} \\ &= \{\alpha \in E | h(\sigma^{-1}\alpha) = \sigma^{-1}\alpha \text{ for all } h \in H\} = \sigma E^H \end{aligned}$$

(4) $\Rightarrow$: By (3), $\sigma M = M$ for any $\sigma \in G$.
Consider homomorphism $\varphi : G \to \mathrm{Aut}(M/F), \sigma \mapsto \sigma\big|_M$.
Then $\ker \varphi = H$ and $\mathrm{im}\, \varphi = G/H$.
So $M^{G/H} = F$, by theorem 2.4.2, M is Galois over F.
Moreover, by Artin theorem, $\mathrm{Gal}(M/F) = \mathrm{Gal}(M/M^{G/H}) \cong G/H$.
$\Leftarrow$: For $\alpha \in M$, $\sigma(\alpha)$ is a root of its minimal polynomial over F for any $\sigma \in G$.
So $\sigma(\alpha) \in M$ since M is a normal extension.
Hence $\sigma H \sigma^{-1} = H$, *i.e.* H is normal.

□

Prop 2.5.1. *Suppose E and L are extensions of F contained in some common field, if E/F is Galois, then EL/L and $E/E \cap L$ are Galois and the map*

$$\mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E \cap L) : \sigma \mapsto \sigma\big|_E$$

is an isomorphism.

Proof. Let E be the splitting field of separable polynomial $f \in F[X]$.
Then EL is the splitting field of f as a polynomial over L.
So EL/L is Galois.
And since $\sigma \in \mathrm{Gal}(EL/L)$ fixes L and maps roots of f to roots of f.
Therefore $\sigma\big|_E$ maps E to E and fixes $E \cap L$.

Conversely, given $\sigma_0 \in \mathrm{Gal}(E/E\cap L)$, $\sigma \in \mathrm{Gal}(EL/L)$ such that $\sigma_0 = \sigma\big|_E$ satisfies that

$$\sigma(el) = \sigma(e)\sigma(l) = \sigma_0(e)l,$$

where $e \in E$ and $l \in L$.

Hence the restriction map is an isomorphism. □

Coro 2.5.1. *In last proposition, suppose L is finite over F, then*

$$[EL : F] = \frac{[E : F][L : F]}{[E \cap L : F]}.$$

Proof.

$$[EL : F] = [EL : L][L : F] = |\mathrm{Gal}(EL/L)|[L : F] = |\mathrm{Gal}(E/E\cap L)|[L : F] = \frac{[E : F][L : F]}{[E \cap L : F]}$$

□

Prop 2.5.2. *Suppose E_1 and E_2 are Galois extensions of F contained in some common field, then E_1E_2 and $E_1 \cap E_2$ are Galois over F, and the map*

$$\mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F) : \sigma \mapsto \left(\sigma\big|_{E_1}, \sigma\big|_{E_2}\right)$$

is an isomorphism of $\mathrm{Gal}(E_1E_2/F)$ onto the subgroup

$$H = \left\{(\sigma_1, \sigma_2)\middle|\, \sigma_1\big|_{E_1\cap E_2} = \sigma_2\big|_{E_1\cap E_2}\right\}.$$

Proof. Let E_1, E_2 be the splitting field of separable polynomial $f_1, f_2 \in F[X]$ resp.

Then E_1E_2 is the splitting field of $\mathrm{lcm}(f_1, f_2)$ and $E_1 \cap E_2$ is the splitting field of $\gcd(f_1, f_2)$.

So both of them are Galois.

The rest part of the proposition is trivial. □

Exam 2.5.1. *We try to find all subextension of $\mathbb{Q}[\zeta]/\mathbb{Q}$ and their correspondence subgroup of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ where $\zeta = e^{\frac{2}{7}\pi i}$.*

The minimal polynomial of ζ is $x^6 + \cdots + x + 1 = 0$ and its roots are $\zeta, \zeta^2, \ldots, \zeta^6$.

So $\mathbb{Q}[\zeta]$ is Galois over $\mathbb{Q}$ and its Galois group is $(\mathbb{Z}/7\mathbb{Z})^\times = \mathbb{Z}/6\mathbb{Z}$.

Let $\sigma \in G = \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ such that $\sigma\zeta = \zeta^3$.

Then σ is a generator of G.

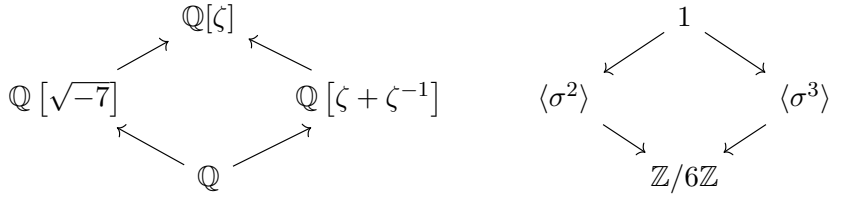
There are two nontrivial subgroup of G: $H_1 = \langle\sigma^2\rangle$ and $H_2 = \langle\sigma^3\rangle$.

For H_1, notice that $\alpha = \sigma + \sigma^2 + \sigma^4$ is fixed by σ^2 and $(\alpha - \sigma\alpha)^2 = -7$.

So $\mathbb{Q}[\zeta]^{H_1} \supset \mathbb{Q}\left[\sqrt{-7}\right] \neq \mathbb{Q}$, i.e. $\mathbb{Q}[\zeta]^{H_1} = \mathbb{Q}\left[\sqrt{-7}\right]$ since G/H_1 has no nontrivial subgroup.

For H_2, notice that $\beta = \sigma + \sigma^{-1}$ is fixed by σ^3.

So similarly, $\mathbb{Q}[\zeta]^{H_2} = \mathbb{Q}[\beta]$.



2.6 Galois group of polynomial

Def 2.6.1. Let $f \in F[X]$ be a separable polynomial, then its splitting field F_f is Galois over F and we called $\mathrm{Gal}(F_f/F)$ the Galois group G_f of f.

Remark 2.6.1. Since F_f is generated by the roots of f, G_f consists of some permutations of roots of f.

Def 2.6.2. Consider a monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = \prod_{i=1}^{n}(x - \alpha_i).$$

Set

$$\Delta(f) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j), D(f) = \Delta(f)^2 = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

Here $D(f)$ is called the discriminant of f, it is nonzero iff f is separable.

Prop 2.6.1. *Let $f \in F[X]$ be a separable polynomial and $\sigma \in G_f$, then*

(1) $\sigma\Delta(f) = \mathrm{sign}(\sigma)\Delta(f)$.

(2) $\sigma D(f) = D(f)$

Proof. By definition. □

Coro 2.6.1. *Let $f \in F[X]$ be a separable polynomial, then*

(1) The discriminant $D(f) \in F$.

(2) Assume $\mathrm{char}(F) \neq 2$, *then $F_f^{A_n \cap G_f} = F[\Delta(f)]$, that is, $G_f \subset A_n$ iff $\Delta(f) \in F$.*

Proof. (1) By the proposition.

(2) By the proposition, $\sigma \in G_f$ fixes $\Delta(f)$ iff $\sigma \in A_n$.
So $\mathrm{Aut}(F_f/F[\Delta(f)]) = A_n \cap G_f$.

□

Prop 2.6.2. *Let $f \in F[X]$ be a separable polynomial, then f is irreducible iff G_f permutes the roots of f transitively.*

Proof. $\Rightarrow$: Let α, β be two roots of f.
Then f is the minimal polynomial of α, β.
So $F[\alpha] \to F[\beta] : \alpha \mapsto \beta$ is an F-isomorphism.
Hence $F[\alpha] \to F[\beta] \hookrightarrow F_f$ can extend to an F-isomorphism $F_f \to F_f$ that maps α to β.
$\Leftarrow$: Suppose f is reducible.
Then there are two roots α, β of f such that their minimal polynomial are different.
So there exists no element $\sigma \in G$ such that $\sigma(\alpha) = \beta$, contradiction! □

Remark 2.6.2. When f is irreducible, n divides $|G_f|$ since $[F[\alpha] : F] = n$.

Exam 2.6.1. *Let f be a separable polynomial of degree 2, notice that $A_2 = \{1\}$.*
So f is irreducible iff $D(f)$ is not a square iff $G_f = S_2$.

Exam 2.6.2. *Let f be a separable irreducible polynomial of degree 3.*
Since $G_f < S_3$ and $A_3 \cong C_3$.
So there are only two cases: $G_f = C_3$ or S_3, according as $D(f)$ is a square in F or not.

Exam 2.6.3. *Let f be a separable irreducible polynomial of degree 4 with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.*
Consider a normal subgroup of S_4

$$V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

And take

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4, \beta = \alpha_1\alpha_3 + \alpha_2\alpha_4, \gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

So we can easily check that V is the subgroup of S_4 that fixes α, β and γ.
Therefore $F[\alpha, \beta, \gamma]$ is Galois over F with Galois group $V \cap G_f$.
Let $M = F[\alpha, \beta, \gamma]$ and $g(x) = (x-\alpha)(x-\beta)(x-\gamma)$, which is the resolvent cubic of f.
Then $g \in F[X]$ and M is the splitting field of g.
Notice that G_f is transitive subgroup of S_4 and $4 \big| |G_f|$.
So there are only five cases:

G	$\lvert G_f \cap V\rvert$	$\lvert G_f/(G_f \cap V)\rvert$
S_4	4	6
A_4	4	3
V	4	1
D_4	4	2
C_4	2	2

By investigate g, we can deduce $\mathrm{Gal}(M/F) \cong G_f/(G_f \cap V)$.
So we only need to consider the case that $|\mathrm{Gal}(M/F)| = 2$.
Notice that C_2 is not transitive subgroup of $G_f \cap V$.
Hence we can determine whether $G_f = D_4$ or C_4 by f is irreducible or not in $M[X]$.

Prop 2.6.3. *Let f be a separable polynomial and suppose orbits of G_f acting on the roots of f have $m_1, \ldots, m_r$ elements resp., then f factors as $f = f_1 \cdots f_r$ with f_i irreducible of degree m_i.*

Proof. WLOG, we assume f is monic and let $\alpha_1, \ldots, \alpha_{m_1}$ be the first orbit of G_f.
Then $f_1 = (x-\alpha_1)\cdots(x-\alpha_{m_1})$ is a polynomial in $F[X]$ and its splitting field M_1 corresponds to the subgroup of G_f fixing $\alpha_1, \ldots, \alpha_{m_1}$.
So $\mathrm{Gal}(M_1/F)$ isomorphic to image of the restriction $G_f \to \mathrm{Sym}\{\alpha_1, \ldots, \alpha_{m_1}\}$.
Hence it is transitive, *i.e.* f_1 is irreducible and similarly we can construct f_i. □

Thm 2.6.1 (Dedekind)**.** *Let $f(x) \in \mathbb{Z}[X]$ be a monic polynomial of degree m and let p be a prime number such that $\bar{f}$ in $F_p[X]$ is simple. Suppose $\bar{f} = f_1 \ldots f_r$ with f_i irreducible of degree m_i in $F_p[X]$, then G_f contains an element σ_p that has a cycle decomposition $\sigma_1 \ldots \sigma_r$ with σ_i of length m_i.*

Sketch of proof. Let $\alpha_1, \ldots, \alpha_m$ be the roots of f and P be a maximal ideal of $A = \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$ such that $P \cap \mathbb{Z} = p\mathbb{Z}$.
Then $A/P = F_p[\bar{\alpha}_1, \ldots, \bar{\alpha}_m]$ is the splitting field $E_{\bar{f}}$ of $\bar{f}$.
Consider $D_P = \{\sigma \in G_f | \sigma(P) = P\}$.
So the homomorphism $\phi : D_P \to G_{\bar{f}}, \sigma \mapsto \bar{\sigma}$ is injective.
Moreover, $\prod_{\sigma \in D_p}(X - \bar{\sigma}(\bar{a}))$ lies in $F_p[X]$, *i.e.* $|D_p| \geqslant [E_{\bar{f}} : F_p]$.
Therefore ϕ is bijective.
Notice that $G_{\bar{f}}$ is a cyclic group (see next section).
By proposition 2.6.3, take σ_p such that $\bar{\sigma}_p$ is generator of $G_{\bar{f}}$ and this complete the proof. □

Exam 2.6.4. *Consider $f(X) = X^5 - X - 1$.*
Then $f(x) \equiv (x^2 + x + 1)(x^3 + x^2 + 1) \pmod 2$ and $f \bmod 3$ is irreducible.
So WLOG, we assume G_f contains permutations $(a\ b)(c\ d\ e)$ and $(1\ 2\ 3\ 4\ 5)$.
Notice that $((a\ b)(c\ d\ e))^3 = (a\ b)$.
Hence $G_f = S_5$.

2.7 Finite field

Lemma 2.7.1. *Let G be a finite abelian group, if G has at most m elements of order dividing m for each divisor m of $|G|$, show that G is cyclic.*

Proof. Suppose G is not cyclic, take $g, h \in G$ of order p, q resp., where p, q are prime.
Then $p \neq q$, otherwise, there are at least $2p-2$ elements of order p, contradiction!
Assume $g^s \neq h^t$ for any $p \nmid s$ and $q \nmid t$, otherwise g, h are both some power of g^s.
So gh is an element of order pq.
Hence there are at least $p+q+pq-2$ elements of order dividing pq, contradiction! □

Prop 2.7.1. *Let F be a field, then every finite subgroup of $F^\times$ is cyclic.*

Proof. In $F^\times$, an element of order dividing m is a root of polynomial $x^m - 1$.
So there are at most m elements of order dividing m.
By the lemma, the finite subgroup of $F^\times$ must be cyclic. □

Coro 2.7.1. *Every extension of finite fields is simple.*

Proof. Let α be the generator of $E^\times$, then $E = F[\alpha]$. □

Prop 2.7.2. *For each power $q = p^n$ of p, there exists a unique field F_q with q elements, which is the splitting field of $X^q - X$ over F_p. Moreover, F_q is Galois over F_p with cyclic Galois group generated by the Frobenius automorphism $\sigma(a) = a^p$.*

Proof. By proposition 2.7.1, for $a \in F_q^\times$, $a^{q-1} = 1$, *i.e.* $a^q = a$.
So F_q are all roots of $f(X) = X^q - X$.
On the other hand, $f'(x) = qx^{q-1} - 1 = -1$.
So f has q distinct roots.
Notice that if $a^q = a, b^q = b$, then $(ab)^q = ab, (a+b)^q = a^q + b^q = a + b$.
Therefore all the roots of f forms a field, that is F_q.
Moreover, $F_q^{\langle\sigma\rangle} = \{a | a^p = a\} = F_p$.
Hence $\mathrm{Gal}(F_q/F_p) = \langle\sigma\rangle$. □

Coro 2.7.2. *F_q contains exactly one field with p^m elements with $m|n$.*

Proof. Corresponds to $\langle\sigma^m\rangle \subset \mathrm{Gal}(F_q/F_p)$. □

Coro 2.7.3. *Let $f \in F_p[x]$ be a monic irreducible polynomial of degree d, then $f | X^{p^d} - X$ and so its splitting field contains in F_{p^d}.*

Proof. Every root of f contained in a field of degree d over F_p, more precisely, F_{p^d}.
So some roots of $X^{p^d} - X$ are also roots of f, *i.e.* $f | X^{p^d} - X$. □

Coro 2.7.4. *F_p has an algebraic closure F.*

Proof. Take $n_i = i!$.
Then $n_i | n_{i+1}$ and so $F_{p^{n_1}} \subset F_{p^{n_2}} \subset F_{p^{n_3}} \subset \cdots$.
Let $F = \bigcup F_{p^{n_i}}$.
Then every polynomial in $F_p[X]$ splits in F, *i.e.* F is an algebraic closure of F_p. □

2.8 Applications of Galois theory

2.8.1 Primitive element theorem

Thm 2.8.1. *Let $E = F[\alpha_1, \dots, \alpha_r]$ and assume $\alpha_2, \dots, \alpha_r$ are separable over F, then there exists a $\gamma \in E$ such that $E = F[\gamma]$.*

Proof. We only need to prove for $r = 2$.
Let $E = F[\alpha, \beta]$ and f, g be minimal polynomials of α, β resp.
Let L be a splitting field of fg, $\alpha_1, \dots, \alpha_s$ be the roots of f and $\beta_1, \dots, \beta_t$ be the roots of g.
Then $\alpha_i + x\beta_j = \alpha + x\beta$ has exactly one solution for $j \neq 1$.
Take $c \in F$ such that $\alpha_i + c\beta_j \neq \alpha + x\beta$ and $\gamma = \alpha + c\beta$.
We claim that $F[\alpha, \beta] = F[\gamma]$.
Consider polynomial $g(X)$ and $f(\gamma - cX)$.
Since $\alpha_i + c\beta_j \neq \gamma$.
So $g(X)$ and $f(\gamma - cX)$ have only one common root β in L, *i.e.* $gcd(g(X), f(\gamma - cX)) = x - \beta$.
Hence $x - \beta \in F[\gamma][X]$, *i.e.* $\alpha, \beta \in F[\gamma]$. □

Prop 2.8.1. *Let $E = F[\gamma]$, then there are only finitely many subextension of E over F.*

Proof. Let M be a subextension of E and f be the minimal polynomial of γ over M.
Consider the subextension M' of M generated by the coefficient of f.
Then minimal polynomial of γ over M' is also f, *i.e.* $[E : M'] = \deg f = [E : M]$.
So $M = M'$ is generated by the coefficient of f.
Let g be the minimal polynomial of γ over F.
Then in $E[X]$, $g | f$.
Hence there are only finitely many different M. □

2.8.2 cyclotomic extension

Prop 2.8.2. *Suppose* $\mathrm{char}(F) \nmid n$ *and let E be the splitting field of $X^n - 1$.*

(1) There exists a primitive n-th root of 1 in E.

(2) If ζ is a primitive n-th root of 1 in E, then $E = F[\zeta]$.

(3) For $\sigma \in \mathrm{Gal}(E/F)$, there exists $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sigma\zeta = \zeta^i$ for all n-th root ζ of 1.

Proof. (1) $f'(x) = nx^{n-1}$ has only one root zero.
So f is separable and its roots form a finite subgroup of $E^\times$.
By proposition 2.7.1, this subgroup is cyclic, *i.e.* the generator is a primitive n-th root.

(2) $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ are distinct and are all roots of f.
So they are all the roots of f, *i.e.* $E = F[\zeta]$.

(3) σ is a permutation of roots of f.
So $\sigma\zeta = \zeta^i$ for some $\gcd(i, n) = 1$, *i.e.* $i \in (\mathbb{Z}/n\mathbb{Z})^\times$.

□

Def 2.8.1. The n-th cyclotomic polynomial is given by

$$\Phi_n = \prod (X - \zeta) \qquad \text{(product over the primitive } n\text{-th roots of 1)}$$

Prop 2.8.3. $\deg(\Phi_n) = \varphi(n), X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Lemma 2.8.1. *Suppose* $\mathrm{char}(F) \nmid n$ *and let* ζ *be a primitive* n*-th root of* 1*, TFAE:*

(1) The n*-th cyclotomic polynomial* Φ_n *is irreducible*

(2) The degree $[F[\zeta] : F] = \varphi(n)$

(3) The homomorphism $\mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ *is an isomorphism.*

Proof. (1) $\Rightarrow$ (2): The minimal polynomial of ζ is Φ_n.
So $[F[\zeta] : F] = \deg \Phi_n = \varphi(n)$.
(2) $\Rightarrow$ (3): This homomorphism is injective and $|\mathrm{Gal}(F[\zeta]/F)| = [F[\zeta] : F] = |(\mathbb{Z}/n\mathbb{Z})^\times|$.
So this homomorphism is an isomorphism.
(3) $\Rightarrow$ (1): $[F[\zeta] : F] = |\mathrm{Gal}(F[\zeta]/F)| = |(\mathbb{Z}/n\mathbb{Z})^\times| = \deg(\Phi(n))$.
And since the minimal polynomial of ζ is Φ_n.
So Φ_n is irreducible. □

Thm 2.8.2. Φ_n *is irreducible in* $\mathbb{Q}[X]$.

Proof. Let $\sigma_p \in \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ with $p \nmid n$ such that $\sigma_p(\zeta) \equiv \zeta^p \pmod P$ (see theorem 2.6.1).
Then $\sigma_p(\zeta) = \zeta^p$, *i.e.* $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times, \sigma_p \mapsto [p]$.
So the homomorphism is isomorphism. □

2.8.3 Cyclic extensions

Def 2.8.2. An extension E of F is cycliccyclic extension if it is Galois with cyclic Galois group.

Thm 2.8.3 (Dedekind)**.** *Let* F *be a field and* G *be a group, every finite set* $\{\chi_1, \dots, \chi_m\}$ *of group homomorphism* $G \to F^\times$ *is linearly independent over* F*.*

Proof. We prove it by induction.
When $m = 1$, trivial.
Assume the statement is true for $m - 1$.
Suppose $a_1\chi_1 + \cdots + a_m\chi_m = 0$ with $a_m \in F$ and $a_2 \neq 0$.
Take g such that $\chi_1(g) \neq \chi_2(g)$.
Then $a_1\chi_1(g)\chi_1(x) + \cdots + a_m\chi_m(g)\chi_m(x) = 0 = a_1\chi_1(g)\chi_1(x) + \cdots + a_m\chi_1(g)\chi_m(x)$.
So $a_2(\chi_2(g) - \chi_1(g))\chi_2(x) + \cdots + a_m(\chi_m(g) - \chi_1(g))\chi_m(x) = 0$ with $a_2(\chi_2 - \chi_1(g)) \neq 0$.
By induction assumption, contradiction! □

Prop 2.8.4. *Let* F *be a field containing a primitive* n*-th root of* 1 *and* $E = F[\alpha]$ *such that* $\alpha^n \in F$ *and no smaller power of* α *is in* F*. Then* E *is Galois over* F *with cyclic Galois group of order* n*. Conversely, if* E *is a cyclic extension of* F *of degree* n*, then* $E = F[\alpha]$ *for some* α *with* $\alpha^n \in F$*.*

Proof. Let ζ be the primitive n-th root of 1.
Then the roots of $X^n - a$ are $\zeta^i\alpha$.
So E is Galois over F and for $\sigma \in \mathrm{Gal}(E/F)$, $\sigma\alpha = \zeta^i\alpha$ for some i.
Therefore $\phi : \mathrm{Gal}(E/F) \to \mathbb{Z}/n\mathbb{Z}, \sigma \mapsto i$ is an injective homomorphism.
Suppose ϕ is not surjective.
Then $\mathrm{im}\,\phi \cong \mathbb{Z}/d\mathbb{Z}$ for some $d|n$.
So $\sigma\alpha^d = (\sigma\alpha)^d = \alpha^d$ for any $\sigma \in \mathrm{Gal}(E/F)$.
But $\alpha^d \notin F$ for $d < n$, contradiction!
Hence $\mathrm{Gal}(E/F) \cong \mathbb{Z}/n\mathbb{Z}$.
Conversely, let σ be the generator.
Since $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are group homomorphism $F^\times \to F^\times$.
So $\sum \zeta^i\sigma^i \neq 0$.
Take $\alpha = \sum \zeta^i\sigma^i(\gamma) \neq 0$.
Then $\sigma\alpha = \zeta^{-1}\alpha$, *i.e.* $E = F[\alpha]$ with $\alpha^n \in F$. □

2.8.4 Solvability of polynomial equations

Def 2.8.3. We say $f(X) = 0$ is solvable in radicals if its solutions can be obtained by the algebraic operations of addition, subtraction, multiplication, division and the extraction of mth roots, or, more precisely, if there exists a tower of fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_m$$

such that $F_i = F_{i-1}[\alpha_i]$ with $\alpha_i^{m_i} \in F_{i-1}$ and F_m contains the splitting field of f.

Lemma 2.8.2. *Let f be separable and F' be an extension of F, then* $\mathrm{Gal}(F'_f/F') < \mathrm{Gal}(F_f/F)$.

Proof. Let $F'_f = F'[\alpha_1, \ldots, \alpha_m]$.
Then $F_f = F[\alpha_1, \ldots, \alpha_m]$.
Since every element of $\mathrm{Gal}(F'_f/F')$ permutes α_i.
So $\mathrm{Gal}(F'_f/F')$ acts on F_f and the map $\sigma \mapsto \sigma\big|_{F_f}$ is an injection $\mathrm{Gal}(F'_f/F') \to \mathrm{Gal}(F_f/F)$. □

Thm 2.8.4. *Suppose* $\mathrm{char}(F) = 0$*, then f is solvable in radicals iff its Galois group is solvable.*

Proof. $\Leftarrow$: Take $F' = F[\zeta]$ where ζ is a primitive n-th root of 1 with sufficiently large n.
By the lemma, $G_0 = \mathrm{Gal}(F'_f/F')$ is solvable.
So there exists $G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{1\}$ such that G_i/G_{i+1} is cyclic.
By proposition 2.8.4, f is solvable in radicals.
$\Rightarrow$: Take $F_0, \ldots, F_m$ and $\alpha_1, \ldots, \alpha_m$ by definition.
Let Ω be a field Galois over F containing F_m and primitive n-th root ζ with large n.
Take $G = \mathrm{Gal}(\Omega/F)$ and the Galois closure $\tilde{E}$ of $F_m[\zeta]$ in Ω.
Then $\tilde{E} = \cup_{\sigma \in G} \sigma F_m[\zeta]$ and is generated by $\zeta, \alpha_1, \ldots, \alpha_m, \sigma\alpha_1, \ldots, \sigma\alpha_m, \ldots$
So we get a tower of fields

$$F_m \subset F_m[\zeta] \subset F_m[\zeta, \alpha_1] \subset \cdots \subset \tilde{E}.$$

By proposition 2.8.4, each step of the tower is a cyclic extension.
Hence $\mathrm{Gal}(\tilde{E}/F)$ is solvable, *i.e.* $\mathrm{Gal}(F_m/F) = \mathrm{Gal}(\tilde{E}/F)/\mathrm{Gal}(\tilde{E}/F_m)$ is solvable. □

Chapter 3

Commutative Algebra

3.1 Ring and ideals

Def 3.1.1. A ring A with exactly one maximal ideal $\mathfrak{m}$ is called a local ring and the field $k = A/\mathfrak{m}$ is called the residue field of A.

Prop 3.1.1. *(1) Let A be a ring and $\mathfrak{m} \neq (1)$ an ideal of A such that $x \in A\backslash\mathfrak{m}$ is a unit in A, then A is a local ring and $\mathfrak{m}$ is its maximal ideal.*

(2) Let A be a ring and $\mathfrak{m}$ a maximal ideal of A, such that every element of $1 + \mathfrak{m}$ is a unit in A, then A is a local ring.

Proof. (1) Let I be an ideal of A.

If $I \cap A\backslash\mathfrak{m} \neq 0$, then I contains a unit, *i.e.* $I = A$.

So $\mathfrak{m}$ is the only maximal ideal of A.

(2) Let I be an ideal of A.

Since $\mathfrak{m}$ is maximal.

So $I + \mathfrak{m} = \mathfrak{m}$ or (1), *i.e.* $I \subset \mathfrak{m}$ or $I \cap (1 + \mathfrak{m}) \neq \varnothing$.

Hence $\mathfrak{m}$ is the only maximal ideal of A.

□

Def 3.1.2. The set $\mathfrak{N}$ of all nilpotent elements is an ideal called nilradical.

Prop 3.1.2. *The nilradical is the intersection of all the prime ideals of A.*

Proof. For $r \in \mathfrak{N}$, let $r^n = 0$.
Then $r \cdot r^{n-1} = 0 \in \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal.
So $r \in \mathfrak{p}$, *i.e.* $\mathfrak{N}$ contains in the intersection of all the prime ideals of A.
On the other hand, let $a \notin \mathfrak{N}$ and S be the set of all ideals $\mathfrak{a}$ such that $f^n \notin \mathfrak{a}$ for any n.
By Zorn lemma, S has a maximal element $\mathfrak{p}$.
Take $x, y \notin \mathfrak{p}$, there exists $f^m \in \mathfrak{p} + (x)$ and $f^n \in \mathfrak{p} + (y)$.
So $f^{m+n} \in \mathfrak{p} + (xy)$, *i.e.* $xy \notin \mathfrak{p}$.
Hence $\mathfrak{p}$ is prime and $f \notin \mathfrak{p}$. □

Def 3.1.3. The Jacobson radical $\mathfrak{R}$ of A is the intersection of all the maximal ideals of A.

Prop 3.1.3. *$x \in \mathfrak{R}$ iff $1 - xy$ is a unit in A for all $y \in A$.*

Proof. $\Rightarrow$: Suppose $1-xy$ is not a unit.
Then $(1-xy) \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.
But notice that $\mathfrak{m} + (x) = (1 - xy + xy) = (1)$.
So $x \notin \mathfrak{m}$, contradiction!
$\Leftarrow$: Suppose there exists a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$.
Then $\mathfrak{m} + (x) = (1)$, *i.e.* there exists $t \in \mathfrak{m}, y \in A$ such that $t + xy = 1$.
So $t = 1 - xy \in \mathfrak{m}$ is not a unit, contradiction! □

Def 3.1.4. We say two ideal $\mathfrak{a}, \mathfrak{b}$ are coprime if $\mathfrak{a} + \mathfrak{b} = (1)$.

Prop 3.1.4. *Let A be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of A, define a homomorphism*

$$\phi : A \to \prod(A/\mathfrak{a}_i), x \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$$

(1) If $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime whenever $i \neq j$, then $\prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$.

(2) ϕ is surjective iff $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime whenever $i \neq j$.

(3) ϕ is injective iff $\bigcap \mathfrak{a}_i = (0)$.

Proof. (1) We prove this by induction.

When $n = 2$, $(\mathfrak{a}_1 \cap \mathfrak{a}_2)(\mathfrak{a}_1 + \mathfrak{a}_2) = (\mathfrak{a}_1 \cap \mathfrak{a}_2)\mathfrak{a}_1 + (\mathfrak{a}_1 \cap \mathfrak{a}_2)\mathfrak{a}_2 \subset \mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2$.

So $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$.

Assume the statement is true for $n = k - 1$.

When $n = k$, let $\mathfrak{b} = \mathfrak{a}_2 \cdots \mathfrak{a}_n$.

Let $x_i + y_i = 1$ for $x_i \in \mathfrak{a}_1$ and $y_i \in \mathfrak{a}_i$ with $2 \leqslant i \leqslant n$, then

$$\prod_{i=2}^{n} y_i = \prod_{i=2}^{n}(1 - x_i) \equiv 1 \pmod{\mathfrak{a}_1}.$$

So $\mathfrak{a}_1 + \mathfrak{b} = (1)$, *i.e.* $\prod \mathfrak{a}_i = \mathfrak{a}_1\mathfrak{b} = \mathfrak{a}_1 \cap \mathfrak{b} = \bigcap \mathfrak{a}_i$.

(2) $\Rightarrow$: $\phi_j(\mathfrak{a}_i) = A/\mathfrak{a}_j$.

So $\mathfrak{a}_i + \mathfrak{a}_j = (1)$.

$\Leftarrow$: By the proof of (1), $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ is coprime.

So there exists $x \in A$ such that $x \in 1 + \mathfrak{a}_1$ and $x \in \mathfrak{a}_i$ for $2 \leqslant i \leqslant n$.

Hence $\phi(x) = (1, 0, \ldots, 0)$ and so ϕ is surjective.

(3) $\ker \phi = \bigcap \mathfrak{a}_i$.

□

Prop 3.1.5. *(1) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup \mathfrak{p}_i$, then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.*

(2) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals and $\mathfrak{p}$ be a prime ideal containing $\bigcap \mathfrak{a}_i$, then $\mathfrak{p} \supset \mathfrak{a}_i$ for some i. Moreover, if $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof. (1) Suppose $\mathfrak{a} \nsubseteq \mathfrak{p}_i$ for any i.

We prove that $\mathfrak{a} \nsubseteq \bigcup \mathfrak{p}_i$, which gives us the contradiction, by induction.

When $n = 1$, trivial.

Assume the statment is true for $n = k - 1$.

When $n = k$, by induction assumption, there exists $x_i \in \mathfrak{a}$ such that $x_i \notin \mathfrak{p}_j$ for $j \neq i$.

We assume $x_i \in \mathfrak{p}_i$ otherwise we are done.

Take $y = \sum x_1 \cdots x_{i-1}x_{i+1} \cdots x_n$.

Then $y \in \mathfrak{a}$, $y \equiv x_1 \cdots x_{i-1}x_{i+1} \cdots x_n \pmod{\mathfrak{p}_i}$.

So $y \notin \bigcup \mathfrak{p}_i$.

(2) Suppose $\mathfrak{a}_i \nsubseteq \mathfrak{p}$ for any i, let $x_i \in \mathfrak{a}_i \backslash \mathfrak{p}$.

Then $\prod x_i \in \prod \mathfrak{a}_i \subset \bigcap \mathfrak{a}_i \subset \mathfrak{p}$.

But $\prod x_i \notin \mathfrak{p}$, contradiction!

Moreover, if $\mathfrak{p} = \bigcap \mathfrak{a}_i$, $\mathfrak{a}_i \subset \mathfrak{p} = \bigcap \mathfrak{a}_i \subset \mathfrak{a}_i$, *i.e.* $\mathfrak{p} = \mathfrak{a}_i$.

□

Def 3.1.5. The ideal quotient of two ideals $\mathfrak{a}, \mathfrak{b}$ is $(\mathfrak{a} : \mathfrak{b}) = \{x \in A | x\mathfrak{b} \subset \mathfrak{a}\}$. In particular, $(0 : \mathfrak{b})$ is called the annihilator of ideal $\mathfrak{b}$, denoted by $\mathrm{Ann}(\mathfrak{b})$

Prop 3.1.6. *(1)* $\mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$

(2) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$.

(3) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$.

(4) $(\bigcap \mathfrak{a}_i : \mathfrak{b}) = \bigcap (\mathfrak{a}_i : \mathfrak{b})$.

(5) $(\mathfrak{a} : \sum \mathfrak{b}_i) = \bigcap (\mathfrak{a} : \mathfrak{b}_i)$.

Def 3.1.6. The radical of an ideal $\mathfrak{a}$ is

$$r(\mathfrak{a}) = \{x \in A | x^n \in \mathfrak{a} \text{ for some } n > 0\}.$$

Prop 3.1.7. *(1)* $r(\mathfrak{a}) \supset \mathfrak{a}$.

(2) $r(r(\mathfrak{a})) = r(\mathfrak{a})$.

(3) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.

(4) $r(\mathfrak{a}) = (1)$ *iff* $a = (1)$.

(5) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.

(6) If $\mathfrak{p}$ *is prime,* $r(\mathfrak{p}^n) = \mathfrak{p}$ *for all* $n > 0$.

Prop 3.1.8. *The radical of an ideal* $\mathfrak{a}$ *is the intersection of the prime ideals which contain* $\mathfrak{a}$.

Proof. Notice that $r(\mathfrak{a}) = \pi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$ where $\pi : A \to A/\mathfrak{a}$ is the quotient map.
Apply proposition 3.1.2 on $A/\mathfrak{a}$ □

Prop 3.1.9. *If* $r(\mathfrak{a})$ *and* $r(\mathfrak{b})$ *are coprime, then* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are coprime.*

Proof. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b})) = r(1) = (1)$.
So $\mathfrak{a} + \mathfrak{b} = (1)$. □

Def 3.1.7. Let $f : A \to B$ be a ring homomorphism and $\mathfrak{a}$ be an ideal in A, we define the extension ideal $\mathfrak{a}^e$ of $\mathfrak{a}$ to be the ideal $f(\mathfrak{a})B$ generated by $f(\mathfrak{a})$.
Let $\mathfrak{b}$ be an ideal of B, $f^{-1}(\mathfrak{b})$ is called the contraction ideal $\mathfrak{b}^c$ of $\mathfrak{b}$.

Prop 3.1.10. *If* $\mathfrak{b}$ *is prime, then* $\mathfrak{b}^c$ *is prime.*

Prop 3.1.11. *(1)* $\mathfrak{a} \subset \mathfrak{a}^{ec}, \mathfrak{b} \supset \mathfrak{b}^{ce}$.

(2) $\mathfrak{b}^c = \mathfrak{b}^{cec}, \mathfrak{a}^e = \mathfrak{a}^{ece}$.

(3) If C is the set of contracted ideals in A and if E is the set of extended ideals in B, then $C = \{\mathfrak{a}|\mathfrak{a}^{ec} = \mathfrak{a}\}, E = \{\mathfrak{b}|\mathfrak{b}^{ce} = \mathfrak{b}\}$ and $\mathfrak{a} \mapsto \mathfrak{a}^e$ is a bijection $C \to E$, whose inverse is $\mathfrak{b} \mapsto \mathfrak{b}^c$.

Proof. (1) $\mathfrak{a} \subset f^{-1}(f(\mathfrak{a})) \subset f^{-1}(f(\mathfrak{a})B) = \mathfrak{a}^{ec}$.

$\mathfrak{b}^{ce} = f(f^{-1}(\mathfrak{b}))B \subset \mathfrak{b}B = \mathfrak{b}$.

(2) $\mathfrak{b}^c \subset (\mathfrak{b}^{ce})^c$ and $\mathfrak{b}^c \supset (\mathfrak{b}^{ce})^c$.

$\mathfrak{a}^e \subset (\mathfrak{a}^{ec})^e$ and $\mathfrak{a}^e \supset (\mathfrak{a}^e)^{ce}$.

(3) For $\mathfrak{a}$ such that $\mathfrak{a}^{ec} = \mathfrak{a}$, $\mathfrak{a} = (\mathfrak{a}^e)^c \in C$.

For $\mathfrak{b}$ such that $\mathfrak{b}^{ce} = \mathfrak{b}$, $\mathfrak{b} = (\mathfrak{b}^c)^e \in C$.

□

Prop 3.1.12. *If $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals of A and $\mathfrak{b}_1, \mathfrak{b}_2$ are ideals of B, then*

$$\begin{array}{ll} (\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e, & (\mathfrak{b}_1 + \mathfrak{b}_2)^c \supset \mathfrak{b}_1^c + \mathfrak{b}_2^c, \\ (\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subset \mathfrak{a}_1^e \cap \mathfrak{a}_2^e, & (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c, \\ (\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e, & (\mathfrak{b}_1\mathfrak{b}_2)^c \supset \mathfrak{b}_1^c\mathfrak{b}_2^c, \\ (\mathfrak{a}_1 : \mathfrak{a}_2)^e \subset (\mathfrak{a}_1^e : \mathfrak{a}_2^e), & (\mathfrak{b}_1 : \mathfrak{b}_2)^c = (\mathfrak{b}_1^c : \mathfrak{b}_2^c), \\ r(\mathfrak{a})^e \subset r(\mathfrak{a}^e) & r(\mathfrak{b})^c = r(\mathfrak{b}^c) \end{array}$$

3.2 Module

Prop 3.2.1. *(1) Let $L \supset M \supset N$ be A-modules, then $(L/N)/(M/N) \cong L/M$.*

(2) Let M_1, M_2 be submodules of M, then $(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$.

Proof. (1) Consider $\phi : L/N \to L/M, x + N \mapsto x + M$.

Then ϕ is surjective and $\ker \phi = M/N$, *i.e.* $(L/N)/(M/N) \cong L/M$.

(2) Consider $\phi : M_2 \hookrightarrow (M_1 + M_2) \to (M_1 + M_2)/M_1, x \mapsto x + M_1$.

Then ϕ is surjective and $\ker \phi = M_1 \cap M_2$, *i.e.* $M_2/(M_1 \cap M_2) \cong (M_1 + M_2)/M_1$.

□

Def 3.2.1. Let N, P be submodules of M, we define the ideal $(N : P) = \{a \in A|aP \subset N\}$. In particular, $(0 : M)$ is called the annihilator of module M, denoted by $\mathrm{Ann}(M)$.

An A-module is faithful if $\mathrm{Ann}(M) = 0$.

Prop 3.2.2. *(1)* $\mathrm{Ann}(M + N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$.

(2) $(N : P) = \mathrm{Ann}((N + P)/N)$.

Prop 3.2.3. *Let M be a finitely generated A-module, $\mathfrak{a}$ be an ideal of A and ϕ be an A-module endomorphism of M such that $\phi(M) \subset \mathfrak{a}M$, then ϕ satisfies an equation of the form*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

where $a_i \in \mathfrak{a}$.

Proof. Let $x_1, \dots, x_n$ be the generators of M and $\phi(x_i) = \sum a_{ij}x_j$.
Then $\sum(\delta_{ij}\phi - a_{ij})x_j = 0$.
By multiplying on the left by the adjoint matrix of $(\delta_{ij}\phi - a_{ij})$, $\det(\delta_{ij}\phi - a_{ij})x_j = 0$.
So $\delta(\delta_{ij}\phi - a_{ij}) = 0$, which is a polynomial of ϕ with coefficient in $\mathfrak{a}$. □

Coro 3.2.1. *Let M be a finitely generated A-module and $\mathfrak{a}$ be an ideal of A such that $\mathfrak{a}M = M$, then there exists $x \equiv 1 \pmod{\mathfrak{a}}$ such that $xM = 0$.*

Proof. Take $\phi = \mathrm{Id}$ and let $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$.
Then $(1 + a_1 + \cdots + a_n)M = 0$ and $1 + a_1 + \cdots + a_n \equiv 1 \pmod{\mathfrak{a}}$. □

Prop 3.2.4 (Nakayama)**.** *Let M be a finitely generated A-module and $\mathfrak{a}$ be an ideal of A contained in the Jacobson radical $\mathfrak{R}$ of A, if $\mathfrak{a}M = M$ then $M = 0$.*

Proof. By corollary 3.2.1, take $x \equiv 1 \pmod{\mathfrak{a}}$ such that $xM = 0$.
By proposition 3.1.3, x is a unit in A, let $xy = 1$.
So $M = yxM = 0$. □

Coro 3.2.2. *Let M be a finitely generated A-module, N be a submodule of M and $\mathfrak{a} \subset \mathfrak{R}$ be an ideal, if $M = \mathfrak{a}M + N$, then $M = N$.*

Proof. Since $\mathfrak{a}(M/N) = \mathfrak{a}M/(\mathfrak{a}M \cap N) = (\mathfrak{a}M + N)/N$.
So by Nakayama lemma on M/N, $M = N$. □

Prop 3.2.5. *Let A be a local ring and x_i be the elements of M whose image in $M/\mathfrak{m}M$ form a basis of this vector space. Then the x_i generate M.*

Proof. Let N be the submodule of M generated by x_i.
Then $N \to M \to M/\mathfrak{m}M$ maps onto $M/\mathfrak{m}M$.
So $N + \mathfrak{m}M = M$.
By corollary 3.2.2, $M = N$. □

Prop 3.2.6. *(1) The sequence*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$$

is exact iff for all A-modules N, the sequence

$$0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$$

is exact.

(2) The sequence

$$0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$$

is exact iff for all A-modules N, the sequence

$$0 \to \mathrm{Hom}(M, N') \xrightarrow{\bar{u}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M, N'')$$

is exact.

Proof. All four parts of this proposition are similar, we prove the first one for example.
Take $f, g \in \mathrm{Hom}(M'', N)$ with $\bar{v}(f) = \bar{v}(g)$.
Then $\bar{v}(f) = v \circ f, \bar{v}(g) = v \circ g$.
And since v is surjective.
So $f = g$, *i.e.* $\bar{v}$ is injective.
Take $h \in \mathrm{Hom}(M, N)$ such that $\bar{u}(h) = u \circ h = 0$.
Then $\ker v = \mathrm{im}\, u \subset \ker h$.
So $h : M \to M/\ker h \to N$ factor through $M/\ker v \cong M''$.
Hence $h = v \circ k = \bar{v}(k)$ for some $k \in \mathrm{Hom}(M'', N)$. □

Prop 3.2.7. *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow[u']{} & N & \xrightarrow[v']{} & N'' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of A-modules and homomorphisms, with the rows exact, then there exists an exact sequence

$$0 \to \ker(f') \xrightarrow{\bar{u}} \ker(f) \xrightarrow{\bar{v}} \ker(f'') \xrightarrow{d} \operatorname{coker}(f') \xrightarrow{\bar{u}'} \operatorname{coker}(f) \xrightarrow{\bar{v}'} \operatorname{coker}(f'') \to 0$$

where $\bar{u}, \bar{v}$ are restrictions of u, v and $\bar{u}', \bar{v}'$ are induced by u', v'.

Def 3.2.2. The tensor product of modules M, N is the unique A-module $M \otimes N$ with an A-bilinear map $g : M \times N \to M \otimes N$ satisfying the following universal property:

Given any A-module P with A-bilinear map $f : M \times N \to P$, there exists a unique A-linear map $f' : T \to P$ such that $f = g \circ f'$.

Prop 3.2.8. *Let M, N, P be A-modules, then there exist unique isomorphisms*

(1) $M \otimes N \to N \otimes M$

(2) $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$

(3) $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$

(4) $A \otimes M \to M$

Proof. Use the universal property. □

Def 3.2.3. Let $f : A \to B$ be an homomorphism and N be a B-module, then N has an A-module structure with $a \cdot m = f(a)m$. This A-module is said to be obtained from N by restriction of scalars. In particular, B has an A-module structure.

Let M be an A-module, then $M_B = B \otimes_A M$ has a B-module structure with $b \cdot (b' \otimes x) = bb' \otimes x$. The B-module M_B is said to be obtained from M by extension of scalars.

Prop 3.2.9. $\operatorname{Hom}(M \otimes N, P) \cong \operatorname{Hom}(M, \operatorname{Hom}(N, P))$.

Prop 3.2.10. *Let*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

be an exact sequence of A-modules and homomorphisms and N be any A-module, then the sequence

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0$$

is exact.

Proof. Take any A-module P.

By proposition 3.2.6, the following sequence is exact:

$$0 \to \operatorname{Hom}(M'', \operatorname{Hom}(N, P)) \xrightarrow{\bar{g}} \operatorname{Hom}(M, \operatorname{Hom}(N, P)) \xrightarrow{\bar{f}} \operatorname{Hom}(M', \operatorname{Hom}(N, P)).$$

So by proposition 3.2.9 and proposition 3.2.6, we complete the proof. □

3.3 Rings and modules of fractions

Def 3.3.1. A multiplicatively closed subset of A is a subset S of A such that $1 \in S$ and S is closed under multiplication. We define an equivalence relation on $A \times S$ such that $(a, s) \sim (b, t)$ iff $(at - bs)u = 0$ for some $u \in S$. The set of equivalence classes $S^{-1}A$ is a ring called the ring of fractions of A w.r.t. S.

There is a natural homomorphism $f : A \to S^{-1}A, x \mapsto \frac{x}{1}$, it has the universal property:

Prop 3.3.1. *Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$, then there exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = f \circ h$.*

Proof. Take $h(\frac{a}{s}) = g(a)g^{-1}(s)$.
For $\frac{b}{t} = \frac{a}{s}$, let $(at - bs)u = 0$ for $u \in S$.
Then $g(a)g(t) - g(b)g(s) = 0 \cdot g^{-1}(u) = 0$.
So $h(\frac{a}{s}) = g(a)g^{-1}(s) = g(b)g^{-1}(t) = h(\frac{b}{t})$, *i.e.* h is well-defined. □

Def 3.3.2. Define an equivalence relation on $M \times S$ such that $(m, s) \sim (m', s')$ iff $t(s'm - sm') = 0$ for some $t \in S$. The set of equivalence classes $S^{-1}M$ is an $S^{-1}A$-module called the module of fractions of M w.r.t. S.

Similarly, there is a natural A-module homomorphism $f : M \to S^{-1}M, m \mapsto \frac{m}{1}$ and it has the universal property:

Prop 3.3.2. *Let N be a $S^{-1}A$-module and $f : M \to N$ be an A-module homomorphism, then there exists a unique $S^{-1}A$-module homomorphism $h : S^{-1}M \to N$ such that $g = f \circ h$.*

Proof. Take $h(\frac{m}{s}) = \frac{1}{s}g(m)$.
For $\frac{m'}{s'} = \frac{m}{s}$, let $t(s'm - sm') = 0$ for $t \in S$.
Then $s'g(m) - sg(m') = \frac{0}{t} = 0$.
So $h(\frac{m}{s}) = \frac{1}{s}g(m) = \frac{1}{s'}g(m') = h(\frac{m'}{s'})$, *i.e.* h is well-defined. □

Prop 3.3.3. *The operation S^{-1} is exact,* i.e. *if the sequence*

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact, then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

is exact.

Proof. $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$.
So $\operatorname{im} S^{-1}f \subset \ker S^{-1}g$.
On the other hand, take $\frac{m}{s} \in \ker S^{-1}g$.
Then $S^{-1}g(\frac{m}{s}) = \frac{g(m)}{s} = 0$, *i.e.* $tg(m) = 0$ for some $t \in S$.
So $g(tm) = 0$, *i.e.* $tm \in \ker g = \operatorname{im} f$, take $m' \in f^{-1}(tm)$.
Therefore $S^{-1}f(\frac{m'}{st}) = \frac{tm}{st} = \frac{m}{s}$.
Hence $\ker(S^{-1}g) = \operatorname{im}(S^{-1}f)$. □

Coro 3.3.1. *(1)* $S^{-1}(N + P) = S^{-1}(N) + S^{-1}(P)$

(2) $S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$.

(3) $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$ *as $S^{-1}A$-modules.*

Proof. (3): apply S^{-1} to the exact sequence $0 \to N \to M \to M/N \to 0$. □

Prop 3.3.4. $S^{-1}M \cong S^{-1}A \otimes_A M$.

Proof. By universal property of tensor, there is a map

$$f : S^{-1}A \otimes_A M \to S^{-1}M, \frac{a}{s} \otimes m \mapsto \frac{am}{s}$$

On the other hand, by universal property of module of fractions, there is a map

$$g : S^{-1}M \to S^{-1}A \otimes_A M, \frac{m}{s} \mapsto \frac{1}{s} \otimes m.$$

Hence $S^{-1}M \cong S^{-1}A \otimes_A M$. □

Coro 3.3.2. $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N)$.

Proof.

$$\begin{aligned} S^{-1}(M \otimes_A N) &= S^{-1}A \otimes_A M \otimes_A N \\ &= S^{-1}A \otimes_A M \otimes_{S^{-1}A} S^{-1}A \otimes_A N \\ &= S^{-1}M \otimes_{S^{-1}A} S^{-1}N \end{aligned}$$

□

Def 3.3.3. Let $\mathfrak{p}$ be a prime ideal of A, then $S = A - \mathfrak{p}$ is multiplicatively closed and the ring of fraction $A_\mathfrak{p} = S^{-1}A$ is called localization at $\mathfrak{p}$.

Prop 3.3.5. *$A_\mathfrak{p}$ is a local ring.*

Proof. For $a \notin \mathfrak{p}$, $\frac{a}{s}$ is a unit with inverse $\frac{s}{a}$.
By proposition 3.1.1, A is a local ring with maximal ideal $\mathfrak{m} = \left\{\frac{p}{s} \middle| p \in \mathfrak{p}\right\}$. □

Def 3.3.4. A property P of a ring A (or of an A-module M) is said to be a local property if A (or M) has P iff $A_\mathfrak{p}$ (or $M_\mathfrak{p}$) has P for every prime ideal $\mathfrak{p}$ of A.

Prop 3.3.6. *TFAE:*

(1) $M = 0$.

(2) $M_\mathfrak{p} = 0$ *for all prime ideal* $\mathfrak{p}$ *of* A.

(3) $M_\mathfrak{m} = 0$ *for all maximal ideal* $\mathfrak{m}$ *of* A.

Proof. (1) ⇒ (2) ⇒ (3) is trivial.
(3) ⇒ (1): Suppose $M \neq 0$, let $x \neq 0 \in A$.
Then $\mathrm{Ann}(x) \neq (1)$, take $\mathfrak{m} \supset \mathrm{Ann}(x)$.
So $\frac{x}{1} \in A_\mathfrak{m}$ is nonzero, otherwise $xs = 0$ for some $s \notin \mathfrak{m}$, *i.e.* $s \in \mathrm{Ann}(x)$, contradiction! □

Prop 3.3.7. *Let $f : M \to N$ be an A-module homomorphism, TFAE:*

(1) f is injective

(2) $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for all prime ideal $\mathfrak{p}$ of A.

(3) $f_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is injective for all maximal ideal $\mathfrak{m}$ of A.

Similarly with "injective" replaced by "surjective" throughout.

Proof. (1) $\Rightarrow$ (2): $0 \to M \to N$ is exact.
So by proposition 3.3.3, $0 \to M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is exact.
(2) $\Rightarrow$ (3): Trivial.
(3) $\Rightarrow$ (1): Suppose f is not injective, let $m \neq 0 \in M$ such that $f(m) = 0$.
Then $\mathrm{Ann}(m) \neq (1)$, take $\mathfrak{m} \supset \mathrm{Ann}(m)$.
So $\frac{m}{1} \in M_{\mathfrak{m}}$ is nonzero while $f_{\mathfrak{m}}(\frac{m}{1}) = \frac{0}{1} = 0$, contradiction! □

Prop 3.3.8. *Consider the homomorphism $f : A \to S^{-1}A$, let C be the set of contracted ideals.*

(1) Every ideal in $S^{-1}A$ is an extended ideal.

(2) If $\mathfrak{a}$ is an ideal in A, then $\mathfrak{a}^{ec} = \bigcup_{s\in S}(\mathfrak{a} : (s))$ and so $\mathfrak{a}^e = (1)$ iff $\mathfrak{a}$ meets S.

(3) $\mathfrak{a} \in C$ iff no element of S is a zero-divisor in $A/\mathfrak{a}$.

(4) The prime ideals of $S^{-1}A$ are in one-to-one correspondence ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) with the prime ideals of A which don't meet S.

Proof. (1) Let $\mathfrak{b}$ be an ideal of $S^{-1}A$ and take $\frac{x}{s} \in \mathfrak{b}$.
Then $\frac{x}{1} \in \mathfrak{b}$, *i.e.* $x \in \mathfrak{b}^c$.
So $\frac{x}{s} = \frac{x}{1} \cdot \frac{1}{s} \in \mathfrak{b}^c(S^{-1}A) = \mathfrak{b}^{ce}$, *i.e.* $\mathfrak{b} \subset \mathfrak{b}^{ce} \subset \mathfrak{b}$.

(2) Take $a \in \mathfrak{a}$.
Then for $b \in f^{-1}\left(\frac{a}{1}\right)$, $(a-b)s = 0$ for some $s \in S$.
So $b \in (\mathfrak{a} : (s))$, *i.e.* $\mathfrak{a}^{ec} \subset \bigcup_{s\in S}(\mathfrak{a} : (s))$.
On the other hand, take $b \in (\mathfrak{a} : (s))$ and let $bs = a \in \mathfrak{a}$.
Then $f(b) = \frac{b}{1} = \frac{a}{s} \in \mathfrak{a}(S^{-1}A) = \mathfrak{a}^e$, *i.e.* $(\mathfrak{a} : (s)) \subset \mathfrak{a}^{ec}$.

(3) In $A/\mathfrak{a}$, $(\mathfrak{a} : (s)) + \mathfrak{a} = \mathrm{Ann}_{A/\mathfrak{a}}(s + \mathfrak{a})$.
So $\mathfrak{a} = \mathfrak{a}^{ec}$ iff $\mathrm{Ann}_{A/\mathfrak{a}}(s + \mathfrak{a}) = (0) + \mathfrak{a}$, *i.e.* s is not zero divisor in $A/\mathfrak{a}$ for all $s \in S$.

(4) Take a prime ideal $\mathfrak{p}$ of A which don't meet S and $\frac{x}{s}, \frac{y}{t} \in S^{-1}A \backslash S^{-1}\mathfrak{p}$.
Then $x, y \notin \mathfrak{p}$, suppose $\frac{xy}{st} \in S^{-1}\mathfrak{p}$, let $\frac{xy}{st} = \frac{p}{u}$.
So $(pst - xyu)v = 0$ for some $v \in S$, *i.e.* $xyuv = pstv \in \mathfrak{p}$, contradiction!
Conversely, take an ideal $S^{-1}\mathfrak{a}$ which is prime in $S^{-1}A$ and $x, y \in A \backslash \mathfrak{a}$.
Then $\frac{x}{1}, \frac{y}{1} \notin S^{-1}\mathfrak{p}$, *i.e.* $\frac{xy}{1} \notin S^{-1}\mathfrak{p}$.
So $xy \notin \mathfrak{p}$.

□

Coro 3.3.3. *The operation S^{-1} commutes with formation of finite sum, products, intersections and radicals.*

Proof. By proposition 3.1.12, S^{-1} commutes with finite sum and products.
By corollary 3.3.1, S^{-1} commutes with intersections.
By proposition 3.1.12, $S^{-1}r(\mathfrak{a}) \subset r(S^{-1}\mathfrak{a})$.
Take $\frac{a}{s} \in r(S^{-1}\mathfrak{a})$ with $\left(\frac{a}{s}\right)^n = \frac{b}{t}$.
Then $(at)^n = bt^{n-1}s^n \in \mathfrak{a}$, *i.e.* $at \in r(\mathfrak{a})$.
So $\frac{a}{s} = \frac{at}{st} \in S^{-1}r(\mathfrak{a})$. □

Coro 3.3.4. *Let $\mathfrak{N}$ be the nilradical of A, then $S^{-1}\mathfrak{N}$ is the nilradical of $S^{-1}A$.*

Coro 3.3.5. *The prime ideals of the local ring $A_\mathfrak{p}$ are in one-to-one correspondence with the prime ideals of A contained in $\mathfrak{p}$.*

Prop 3.3.9. *Let M be a finitely generated A-module and S be a multiplicatively closed subset of A, then $S^{-1}(\mathrm{Ann}(M)) = \mathrm{Ann}(S^{-1}M)$.*

Proof. If this is true for M, N, then

$$\begin{aligned} S^{-1}(\mathrm{Ann}(M+N)) &= S^{-1}(\mathrm{Ann}(M) \cap \mathrm{Ann}(N)) = S^{-1}\,\mathrm{Ann}(M) \cap S^{-1}\,\mathrm{Ann}(N) \\ &= \mathrm{Ann}(S^{-1}M) \cap \mathrm{Ann}(S^{-1}N) = \mathrm{Ann}(S^{-1}(M+N)) \end{aligned}$$

So it suffices to prove for M generated by one element m.
Consider the homomorphism $\phi : A \to M, a \mapsto am$.
Then $\ker\phi = \mathrm{Ann}(M)$ and ϕ is surjective, *i.e.* $M \cong A/\,\mathrm{Ann}(M)$.
So $\mathrm{Ann}(S^{-1}M) = \mathrm{Ann}(S^{-1}A/S^{-1}\,\mathrm{Ann}(M)) = S^{-1}\,\mathrm{Ann}(M)$. □

Coro 3.3.6. *Let N, P be two submodules of an A-module M and if P is finitely generated, then $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$.*

Proof. By proposition 3.2.2, $(N : P) = \mathrm{Ann}((N+P)/P)$. □

Prop 3.3.10. *Let $f : A \to B$ be a ring homomorphism and $\mathfrak{p}$ be a prime ideal of A, if $\mathfrak{p}$ is a contraction then it is a contraction of a prime ideal.*

Proof. Let $S = f(A\backslash\mathfrak{p})$.
Then $\mathfrak{p}^e \cap S = \varnothing$, *i.e.* $S^{-1}\mathfrak{p}^e \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of $S^{-1}B$.
Let $\mathfrak{q}$ be the contraction of $\mathfrak{m}$ under $B \to S^{-1}B$.
So $\mathfrak{q} \supset \mathfrak{p}^e$ and $\mathfrak{q} \cap S = \varnothing$.
Hence $\mathfrak{q}^c = \mathfrak{p}$. □

3.4 integral dependence

Def 3.4.1. Let B be a ring and A be a subring of B. An element x of B is said to be integral over A if x is a root of a monic polynomial with coefficients in A.

Prop 3.4.1. *TFAE:*

(1) $x \in B$ is integral over A.

(2) $A[x]$ is a finitely generated A-module

(3) $A[x]$ is contained in a subring C of B such that C is a finitely generated A-module.

(4) There exists a faithful $A[x]$-module M which is finitely generated as an A-module.

Proof. (1) ⇒ (2): $A[x]$ can be generated by $1, x, \ldots, x^{n-1}$.
(2) ⇒ (3): $A[x] \subset A[x]$.
(3) ⇒ (4): C is a faithful $A[x]$-module.
(4) ⇒ (1): Consider $\phi : M \to M, m \mapsto xm$.
Then $\phi(M) \subset xM$.
By proposition 3.2.3, $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$.
And since M is faithful.
So $x^n + a_1x^{n-1} + \cdots + a_n = 0$, *i.e.* x is integral over A. □

Coro 3.4.1. *Let x_i be some elements of B that integral over A, then $A[x_1, \ldots, x_n]$ is a finitely-generated A-module.*

Coro 3.4.2. *The set C of elements that are integral over A is a subring of B containing A.*

Proof. For $x, y \in C$, $A[x, y]$ is finitely generated, *i.e.* $x + y, xy$ are integral over A. □

Def 3.4.2. Such ring C is called the integral closure of A in B. If $C = A$, then A is said to be integrally closed in B. If $C = B$, the ring B is said to be integral over A.

Coro 3.4.3. *Let $A \subset B \subset C$ be three rings such that B is integral over A and C is integral over B, then C is integral over A.*

Proof. For $x \in C$, let $x^n + b_1 x^{n-1} + \cdots + b_n = 0$.
Then $A[b_1, \ldots, b_n][x]$ is finitely generated over A.
So x is integral over A. □

Coro 3.4.4. *Let A be a subring of B and C be the integral closure of A in B, then C is integrally closed in B.*

Prop 3.4.2. *Let A be a subring of B such that B integral over A.*

(1) If $\mathfrak{b}$ is an ideal of B and $\mathfrak{a} = \mathfrak{b}^c = A \cap \mathfrak{b}$, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.

(2) If S is a multiplicatively closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.

Proof. (1) For $x \in B$, let $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_i \in A$.
Then $(x + \mathfrak{b})^n + (a_1 + \mathfrak{a})(x + \mathfrak{b})^{n-1} + \cdots + (a_n + \mathfrak{a}) = 0 + \mathfrak{b}$.

(2) For $x \in B$, let $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_i \in A$.
Then $\left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0$.

□

Prop 3.4.3. *Let $A \subset B$ be integral domains such that B integral over A, then B is a field iff A is a field.*

Proof. $\Rightarrow$: Since $x = \frac{1}{a}$ is an element in B for $a \in A$.
Let $x^n + a_1 x^{n-1} + \cdots + a_n = 0$.
Then $x + a_1 + a_2 a + \cdots + a_n a^{n-1} = 0$, *i.e.* $x \in A$.
$\Leftarrow$: For $x \in B$, let $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_n \neq 0$.
Then $\frac{1}{a_n} x^{n-1} + \frac{a_1}{a_n} x^{n-2} + \cdots + \frac{a_{n-1}}{a_n} + x^{-1} = 0$, *i.e.* $x^{-1} \in B$. □

Coro 3.4.5. *Let A be a subring of B such that B is integral over A, $\mathfrak{q}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{q} \cap A$, then $\mathfrak{q}$ is maximal iff $\mathfrak{p}$ is maximal.*

Coro 3.4.6. *Let A be a subring of B such that B is integral over A and $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of B such that $\mathfrak{q} \subset \mathfrak{q}', \mathfrak{q}^c = \mathfrak{q}'^c = \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. By proposition 3.4.2, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$.
Let $\mathfrak{m}$ be the extension of $\mathfrak{p}$ in $A_\mathfrak{p}$ and $\mathfrak{n}, \mathfrak{n}'$ be the extension of $\mathfrak{q}, \mathfrak{q}'$ in $B_\mathfrak{p}$ resp.
Then $\mathfrak{m}$ is maximal in $A_\mathfrak{p}$, *i.e.* $\mathfrak{n}, \mathfrak{n}'$ are maximal in $B_\mathfrak{p}$ and $\mathfrak{n} \subset \mathfrak{n}'$.
So $\mathfrak{n} = \mathfrak{n}'$ and $\mathfrak{q} = \mathfrak{q}'$ by proposition 3.3.8. □

Thm 3.4.1. *Let A be a subring of B such that B is integral over A and $\mathfrak{p}$ be a prime ideal of A, then there exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. Let $\mathfrak{n}$ be a maximal ideal of $B_\mathfrak{p}$.
Then $\mathfrak{m} = \mathfrak{n} \cap A_\mathfrak{p}$ is the only maximal ideal of $A_\mathfrak{p}$.
Take $\mathfrak{q}$ be the contraction of $\mathfrak{n}$ under $B \to B_\mathfrak{p}$.
So $\mathfrak{q} \cap A = \mathfrak{p}$. □

Thm 3.4.2 (going-up theorem)**.** *Let A be a subring of B such that B is integral over A, $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m\ (m < n)$ be a chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, then the chain $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.*

Proof. By proposition 3.4.2 we only need to consider the case that $m = 0, n = 1$, which can be deduced by theorem 3.4.1. □

Prop 3.4.4. *Let A be a subring of B, C be the integral closure of A in B and S be a multiplicatively closed subset of A, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. By proposition 3.4.2, $S^{-1}C$ is integral over $S^{-1}A$.
Conversely, suppose $\frac{b}{s} \in S^{-1}B$ is integral over $S^{-1}A$, let $\left(\frac{b}{s}\right)^n + \frac{a_1}{s_1}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s_n} = 0$.
Then by multiplying by $(ss_1 \cdots s_n)^n$, we obtain that $bs_1 \cdots s_n \in C$.
So $\frac{b}{s} = \frac{bs_1 \cdots s_n}{ss_1 \cdots s_n} \in S^{-1}C$. □

Def 3.4.3. An integrally closed integral domain is an integral domain which is integrally closed in its field of fractions.

Prop 3.4.5. *Let A be an integral domain, TFAE:*

(1) A is integrally closed

(2) $A_{\mathfrak{p}}$ is integrally closed for all prime ideal $\mathfrak{p}$.

(3) $A_{\mathfrak{m}}$ is integral ly closed for all maximal ideal $\mathfrak{m}$.

Proof. A localization of a field is itself.
So A is integrally closed iff the inclusion from A to its integral closure is surjective.
By proposition 3.3.7, surjective is a local property.
So by proposition 3.4.4, integrally closed is a local property. □

Def 3.4.4. Let A be a subring of B and $\mathfrak{a}$ be an ideal of A, then an element of B is said to be integral over $\mathfrak{a}$ if it is a root of a monic polynomial with coefficients in $\mathfrak{a}$. The integral closure of $\mathfrak{a}$ in B is the set of all elements of B which are integral over $\mathfrak{a}$.

Lemma 3.4.1. *Let C be the integral closure of A in B and $\mathfrak{a}^e$ denote the extension of $\mathfrak{a}$ in C, then the integral of $\mathfrak{a}$ in B is the radical of $\mathfrak{a}^e$.*

Proof. Since $\mathfrak{a}^e = \mathfrak{a}C$, take $x = \sum a_i x_i \in \mathfrak{a}^e$ with $a_i \in \mathfrak{a}, x_i \in C$.
Let $M = A[x_1, \ldots, x_k], \phi : M \to M, m \mapsto xm$.
Then $\phi M \subset \mathfrak{a}M$, let $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$, by proposition 3.2.3, with $a_i \in \mathfrak{a}$.
So $x^n + a_1\phi^{n-1} + \cdots + a_n = 0$, *i.e.* x is integral over $\mathfrak{a}$.
Conversely, for x integral over $\mathfrak{a}$, let $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathfrak{a}$.
Then $x^n = -a_1x^{n-1} - \cdots - a_n \in \mathfrak{a}C = \mathfrak{a}^e$.
So $x \in r(\mathfrak{a}^e)$. □

Prop 3.4.6. *Let $A \subset B$ be integral domains, A integrally closed and let $x \in B$ be integral over an ideal $\mathfrak{a}$ of A, then x is algebraic over the field of fractions K of A and if its minimal polynomial over K is $t^n + a_1t^{n-1} + \cdots + a_n$, then $a_1, \ldots, a_n \in r(\mathfrak{a})$.*

Proof. Let $f(t) = t^n + a_1t^{n-1} + \cdots + a_n$ with $a_i \in \mathfrak{a}$ such that $f(x) = 0$ and g be the minimal polynomial of x over K.
Then $g|f$, *i.e.* roots of g are integral over $\mathfrak{a}$.
So coefficients of g are integral over $\mathfrak{a}$, as they are polynomials of the roots.
And since A is integrally closed in K.
By the lemma, coefficients of g are contained in $r(\mathfrak{a})$. □

Thm 3.4.3 (Going-down theorem)**.** *Let $A \subset B$ be integral domains, A integrally closed and B integral over A. Let $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$ be a chain of prime ideals of A and let $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ $(m < n)$ be a chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, then the chain $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.*

Proof. By going-up theorem, it suffices to prove for $m = 1, n = 2$.
So we want to show that $\mathfrak{p}_2$ is the contraction of a prime ideal in $B_{\mathfrak{q}_1}$.
And by proposition 3.3.10, it suffices to prove that $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A = \mathfrak{p}_2$.
Take $\frac{x}{s} \in \mathfrak{p}_2 B_{\mathfrak{q}_1}$ with $x \in \mathfrak{p}_2 B, s \in B \backslash \mathfrak{q}_1$.
By lemma 3.4.1, x is integral over $\mathfrak{p}_2$.
Let $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ be its minimal polynomial over the field of fractions K of A.
By proposition 3.4.6, $a_i \in r(\mathfrak{p}_2) = \mathfrak{p}_2$.
Now suppose $\frac{x}{s} \in A$, *i.e.* $sa = x$ for some $a \in A$.
Then s is the root of irreducible polynomial $t^n + \frac{a_1}{a} t^{n-1} + \cdots + \frac{a_n}{a^n}$ in K.
Notice that s is integral over A and A is integrally closed in K.
By proposition 3.4.6, we obtain that $\frac{a_i}{a^i} \in A$ for all i.
Suppose $a \notin \mathfrak{p}_2$.
Then $\frac{a_i}{a^i} \in \mathfrak{p}_2$ for all i as $a_i \in \mathfrak{p}_2$ and $\mathfrak{p}_2$ is prime.
So s is integral over $\mathfrak{p}_2$, *i.e.* $s \in r(\mathfrak{p}_2^e) \subset r(\mathfrak{p}_1^e) \subset r(\mathfrak{q}_1) = \mathfrak{q}_1$, contradiction!
Hence $\frac{x}{s} = a \in \mathfrak{p}_2$. □

Chapter 4

Representation Theory

4.1 Representations of finite groups

Def 4.1.1. A representation of a finite group G on a finite-dimensional complex vector space V is a homomorphism $\rho : G \to \mathrm{GL}(V)$, and we say that such a map gives V a structure of G-module. The dimension of V is called the degreee of representation ρ.

A G-linear map between two representations V and W of G is a linear map $\varphi : V \to W$ such that $\rho_g^V \circ \varphi = \varphi \circ \rho_g^W$ for all $g \in G$.

A subrepresentation of a representation V is a subspace W of V which is invariant under G. A representation V is called irreducible if there is no non-trivial G-invariant subspace.

The direct sum, tensor product and dual representations are defined as those of vector space and with natural homomorphism from G.

Exam 4.1.1. *Let V be a vector space with basis $\{e_g\}_{g\in G}$, there is a representation $\rho : G \to V$ given by $\rho_g(e_h) = e_{gh}$. Such a representation is called the regular representation.*

Prop 4.1.1. *Let W be a subrepresentation of V, then there exists another subrepresentation W' of V such that $V = W \oplus W'$.*

Proof. Let $\langle\ ,\ \rangle$ be a Hermitian form on V, and take

$$\langle v, w\rangle_\rho = \sum_{g\in G} \langle \rho_g(v), \rho_g(w)\rangle.$$

Then $\langle\ ,\ \rangle_\rho$ is also a Hermitian form and $\langle v, w\rangle_\rho = \langle \rho_g(v), \rho_g(w)\rangle_\rho$ for all g.
For $v \in W^\perp, w \in W$ and $g \in G$, $\langle \rho_g(v), w\rangle = \langle v, \rho_{g^{-1}}(w)\rangle = 0$.
So $W^\perp$ is G-invariant, *i.e.* it is a subrepresentation of V.
Hence $V = W \oplus W^\perp$ as a representation. □

Remark 4.1.1. The trick of summing up the value of a map as the vector pass through its orbit under G-action is very useful in representation theory.

Coro 4.1.1. *Any representation is a direct sum of irreducible representations.*

Prop 4.1.2 (Schur lemma)**.** *Let V and W be two irreducible representations of G and $\varphi : V \to W$ is a G-linear map, then*

(1) φ is isomorphism or $\varphi = 0$.

(2) If $V = W$, then $\varphi = \lambda I$ for some $\lambda \in \mathbb{C}$.

Proof.

$\ker\varphi$ and $\operatorname{im}\varphi$ are subrepresentations of V and W resp.

So they must be trivial.

Since $\mathbb{C}$ is algebraically closed.

Let λ be an eigenvalue of φ.

Then $\varphi - \lambda I : V \to W$ is either isomorphism or zero by (1).

But $\varphi - \lambda I$ is degenerated.

So $\varphi = \lambda I$. □

Prop 4.1.3. *Let V be a representation of G, then there is a unique decomposition*

$$V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k},$$

where V_i are distinct irreducible representations.

4.2 Character theory

Def 4.2.1. The charater $\chi_V : G \to \mathbb{C}$ of a representation V is given by $\chi_V(g) = \operatorname{tr}(\rho_g)$.

Prop 4.2.1.

$$\chi_{V\oplus W} = \chi_V + \chi_W, \chi_{V\otimes W} = \chi_V\chi_W,$$

$$\chi_{V^*} = \bar{\chi}_V \text{ and } \chi_{\wedge^2 V}(g) = \frac{1}{2}\left(\chi_V(g)^2 - \chi_V(g^2)\right).$$

Exam 4.2.1. *Consider the regular representation ρ, then ρ_g are permutation matrix.*

So $\chi_R(1) = |G|$ and $\chi_R(g) = 0$.

Prop 4.2.2. *Let $V^G = \{v \in V | \rho_g(v) = v \text{ for all } G\}$ and take an endomorphism*

$$\varphi(v) = \frac{1}{|G|}\sum_{g\in G}\rho_g(v),$$

then φ is a G-linear projection from V onto V^G.

Proof.

$$\varphi(\rho_h(v)) = \frac{1}{|G|}\sum_{g\in G}\rho_g(\rho_h(v)) = \frac{1}{|G|}\sum_{g\in G}\rho_{gh}(v) = \varphi(v).$$

$$\rho_h(\varphi(v)) = \frac{1}{|G|}\sum_{g\in G}\rho_h(\rho_g(v)) = \frac{1}{|G|}\sum_{g\in G}\rho_{hg}(v) = \varphi(v).$$

$$\varphi(\varphi(v)) = \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G}\rho_g(\rho_h(v)) = \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G}\rho_{gh}(v) = \frac{1}{|G|}\sum_{g\in G}\varphi(v) = \varphi(v).$$

□

Coro 4.2.1.

$$\dim V^G = \operatorname{tr}(\varphi) = \frac{1}{|G|}\sum_{g\in G}\chi_V(g).$$

In particular, when V is irreducible, sum of all character is zero.

Coro 4.2.2. *Let* $\mathrm{Hom}_G(V,W)$ *be the vector space consists of all* G*-linear map* $V \to W$*, then*

$$\dim \mathrm{Hom}_G(V,W) = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_W(g).$$

In particular, when V *and* W *are irreducible,*

$$\frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_W(g) = \begin{cases}1 & \text{if } V\cong W\\ 0 & \text{if } V\ncong W\end{cases}$$

Proof. $\mathrm{Hom}(V,W)\cong V^*\otimes W$ and $\rho_g^{\mathrm{Hom}}(f)(v) = \rho_g^W\circ f\circ \rho_{g^{-1}}^V(v)$.
So $\mathrm{Hom}(V,W)^G = \mathrm{Hom}_G(V,W)$ and $\chi_{\mathrm{Hom}} = \bar{\chi}_V\chi_W$. □

Def 4.2.2. A function $\varphi: G\to\mathbb{C}$ is called class function if it is constant on the conjugacy classes of G. We denote the set of class function by $\mathbb{C}_{class}(G)$, which is a complex vector space, and define a Hermitian inner product on it by

$$(\alpha,\beta) = \frac{1}{|G|}\sum_{g\in G}\overline{\alpha(g)}\beta(g).$$

Thm 4.2.1. *Characters of the irreducible representations of* G *are orthonormal.*

Coro 4.2.3. *A representation* V *is irreducible iff* $(\chi_V,\chi_V)=1$.

Coro 4.2.4. *Any representation is determined by its character. Moreover, the multiplicity* a_i *of* V_i *in* V *is* (χ_{V_i},χ_V).

Coro 4.2.5. *Every irreducible representation* V *of* G *appears in the regular representation* $\dim V$ *times. In particular,* $|G|$ *is the sum of squares of dimension of all the irreducible representations.*

Proof. $(\chi_V,\chi_R) = \frac{1}{|G|}\chi_V(1)|G| = \chi_V(1) = \dim V$. □

Lemma 4.2.1. *Let* $\alpha: G\to\mathbb{C}$ *be any function on* G*, take* $\varphi_{\alpha,V} = \sum\alpha(g)\rho_g$*, then* $\varphi_{\alpha,V}$ *is a* G*-linear map for all representation* V *iff* α *is a class function.*

Proof. $\Rightarrow$: $\sum\alpha(g)\rho_h^{-1}\circ\rho_g\circ\rho_h = \rho_h^{-1}\circ\varphi_{\alpha,V}\circ\rho_h = \varphi_{\alpha,V} = \sum\alpha(g)\rho_g$.
So $\sum(\alpha(hgh^{-1})-\alpha(g))\rho_g = 0$.
Consider the regular representation ρ^R.
Then $\sum(\alpha(hgh^{-1})-\alpha(g))\rho_g^R(e_x) = \sum(\alpha(hgh^{-1})-\alpha(g))e_{gx} = 0$.
So $\alpha(hgh^{-1}) = \alpha(g)$ for any $g,h\in G$.
$\Leftarrow$: $\rho_h^{-1}\circ\varphi_{\alpha,V}\circ\rho_h(v) = \sum\alpha(g)\rho_{h^{-1}gh}(v) = \sum\alpha(hgh^{-1})\rho_g(v) = \sum\alpha(g)\rho_g(v) = \varphi_{\alpha,V}(v)$. □

Prop 4.2.3. *The number of irreducible representations of* G *is equal to the number of conjugacy class of* G*. Equivalently, their characters form an orthonormal basis for* $\mathbb{C}_{class}(G)$.

Proof. Suppose α is a class function and $(\alpha,\chi_V)=0$ for all irreducible representations V.
Then $\varphi_{\alpha,V}$ is G-linear, *i.e.* $\varphi_{\alpha,V} = \lambda I$ by Schur lemma.
So $\lambda = \frac{1}{n}\mathrm{tr}(\varphi_{\alpha,V}) = \frac{1}{n}\sum\alpha(g)\chi_V(g) = \frac{|G|}{n}\overline{(\alpha,\chi_{V^*})} = 0$.
Therefore $\varphi_{\alpha,V}=0$ for any representation V.
But for regular representation V, $\varphi(\alpha,V)(e_h) = \sum\alpha(g)e_{gh}$, contradiction! □

Coro 4.2.6. *Let* $\chi_1,\dots,\chi_n$ *be the character of all the irreducible representations, then*

$$\sum\overline{\chi_i(g)}\chi_i(g) = \frac{|G|}{c(g)}, \sum\overline{\chi_i(g)}\chi_i(h) = 0,$$

where g *is not conjugate to* h.

Proof. Let $\alpha : G \to \mathbb{C}$ maps G to 0 except on the conjugacy class C_g of g and $\alpha(C_g) = 1$.
Then $(\chi_i, \alpha) = \frac{|C_g|}{|G|}\overline{\chi_i(g)}$.
So $1 = \alpha(g) = \sum \frac{c(g)}{|G|}\overline{\chi_i(g)}\chi_i(g)$ and $0 = \alpha(h) = \sum \frac{c(g)}{|G|}\overline{\chi_i(g)}\chi_i(h)$. □

Exam 4.2.2. *Consider $G = C_n = \langle a|a^n\rangle$, it is abelian so there are n conjugacy classes.*
Let $\omega = e^{\frac{2\pi i}{n}}, \rho_j : G \to \mathbb{C}, a \mapsto \omega^j$.
Then ρ_j are all the irreducible representations of G and their characters are themselves.

C_n	1	a	$\cdots$	a^{n-1}
χ_0	1	1	$\cdots$	1
χ_1	1	ω	$\dots$	ω^{n-1}
χ_2	1	ω^2	$\dots$	ω^{2n-2}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_{n-1}	1	ω^{n-1}	$\dots$	$\omega^{(n-1)^2}$

Exam 4.2.3. *Consider $G = D_{2n} = \langle \tau, \phi|\tau^2, \phi^n, \tau\phi\tau\phi\rangle$, then $\{\phi^k, \phi^{-k}\}$ are some conjugacy classes.*
If $2|n$, $\phi^t\tau\phi^{-t} = \phi^{2t}\tau$, i.e. *$\{\phi^{2t}\tau\}, \{\phi^{2t+1}\tau\}$ are distinct conjugacy classes.*
We first consider the representation of degree 1, let $\rho(\phi) = a, \rho(\tau) = b$.
Then $b^2 = 1, a^n = 1, a^2b^2 = 1$, i.e. *$a, b \in \pm 1$ as $2|n$.*
So there are four different degree 1 representations.
Notice that D_n is the symmetric group of n-gon.
So let $\omega = e^{\frac{2\pi i}{n}}$, there are $\frac{n}{2} - 1$ natural degree 2 representations given by

$$\rho_j(\tau) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \rho_j(\phi) = \begin{bmatrix} \omega^j & 0 \\ 0 & \omega^{-j} \end{bmatrix}.$$

Their characters are $\chi_j(\phi^k) = \omega^{jk} + \omega^{-jk}, \chi_j(\phi^k\tau) = 0$.

D_{2n}	1	ϕ^k	τ	$\phi\tau$
$\chi_{1,1}$	1	1	1	1
$\chi_{1,-1}$	1	1	-1	-1
$\chi_{-1,1}$	1	$(-1)^k$	1	-1
$\chi_{-1,-1}$	1	$(-1)^k$	-1	1
χ_j	2	$\omega^{jk} + \omega^{-jk}$	0	0

If $2 \nmid n$, $\{\phi^t\tau\}$ is a conjugacy class and, similar to the above case, we have

D_{2n}	1	ϕ^k	τ
χ_0	1	1	1
$\chi_\pm$	1	1	-1
χ_j	2	$\omega^{jk} + \omega^{-jk}$	0

Exam 4.2.4. *Consider $G = S_3$, then 2-cycles and 3-cycles gives two conjugacy classes.*
Notice that there are two natural degree 1 representations $\rho_0(g) = 1$ and $\rho_\pm(g) = \mathrm{sgn}(g)$.
So the last representations is degree 2 and by column orthogonality, we have

S_3	1	(1 2)	(1 2 3)
χ_0	1	1	1
$\chi_\pm$	1	-1	1
χ_{st}	2	0	-1

Remark 4.2.1. The third representation can actually be writen down explicitly.
Consider a 3-dimensional vector space V spanned by e_1, e_2, e_3.
Then S_3 act on $\{e_1, e_2, e_3\}$ gives a representation ρ_{perm}.
And notice that the subspace spanned by $\{e_1 - e_2, e_2 - e_3\}$ is S_3-invariant.
So this gives a degree 2 representation ρ_{st}.
More explicitly, the representation is given by

$$\rho_{st}(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \rho_{st}(1\ 2) = \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix}, \rho_{st}(1\ 3) = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \rho_{st}(2\ 3) = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix},$$

$$\rho_{st}(1\ 2\ 3) = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \rho_{st}(1\ 3\ 2) = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}.$$

We can also construct this representation for S_n with $n > 3$ and it is always irreducible.
This is because $\rho_{st} \oplus \rho_0 = \rho_{perm}$ and χ_{perm} is counting the number of fix points, so

$$\begin{aligned} \sum_g \chi_{st}^2(g) &= \sum_g (\chi_{perm}(g) - 1)^2 \\ &= \sum_\sigma \sum_{i,j} \mathbf{1}_{\sigma(i)=i} \mathbf{1}_{\sigma(j)=j} - 2 \sum_\sigma \sum_i \mathbf{1}_{\sigma(i)=i} + n! \\ &= \sum_i (n-1)! + \sum_{i \neq j} (n-2)! - 2 \sum_i (n-1)! + n! \\ &= n! \end{aligned}$$

Hence $(\chi_{st}, \chi_{st}) = 1$.

Exam 4.2.5. *Consider $G = S_4$.*
Then there are four conjugacy classes: 2-cycles, 3-cycles, 4-cycles and two 2-cycles.
We already know three representations:

S_4	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_0	1	1	1	1	1
$\chi_\pm$	1	−1	1	−1	1
χ_{st}	3	1	0	−1	−1

Notice that $\rho_\pm \otimes \rho_{st}$ gives a different representation and it is obviously irreducible.
And the last representation can be determined by column orthogonality.

S_4	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_0	1	1	1	1	1
$\chi_\pm$	1	−1	1	−1	1
χ_{st}	3	1	0	−1	−1
$\chi_{\pm st}$	3	−1	0	1	−1
χ	2	0	−1	0	2

Exam 4.2.6. *Consider $G = A_4$.*
Then there are three conjugacy classes with representative elements $(1\ 2)(3\ 4), (1\ 2\ 3), (1\ 3\ 2)$.
We already know two representations ρ_0 and ρ_{st} of degree 1 and 3 resp.
So two representations left are both of degree 1, we set

S_4	1	(1 2)(3 4)	(1 2 3)	(1 3 2)
χ_0	1	1	1	1
χ_{st}	3	−1	0	0
χ_1	1	1	b	c
χ_2	1	1	$-1-b$	$-1-c$

By row orthogonality, we have $b + c = -1$.
And since χ_1, χ_2 *are of degree* 1.
So $|b| = |c| = |1 + b| = |1 + c| = 1$.
Hence $(b, c) = (\omega, \omega^2)$ *or* $(b, c) = (\omega^2, \omega)$ *where* $\omega = e^{\frac{2\pi i}{3}}$.

S_4	1	(1 2)(3 4)	(1 2 3)	(1 3 2)
χ_0	1	1	1	1
χ_{st}	3	-1	0	0
χ_1	1	1	ω	ω^2
χ_2	1	1	ω^2	ω

Exam 4.2.7. *Consider* $G = S_5$.

Then there are six conjugacy classes: 2*-cycles,* 3*-cycles,* 4*-cycles,* 5*-cycles, two* 2*-cycles and* 2*-cycle times* 3*-cycle.*

We already know four representations $\rho_0, \rho_\pm, \rho_{st}, \rho_{\pm st}$.

S_5	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2 3 4 5)	(1 2)(3 4)	(1 2)(3 4 5)
χ_0	1	1	1	1	1	1	1
$\chi_\pm$	1	-1	1	-1	1	1	-1
χ_{st}	4	2	1	0	-1	0	-1
$\chi_{\pm st}$	4	-2	1	0	-1	0	1

Consider $\rho_{st} \otimes \rho_{st}$*, it can be divided into two subrepresentation* $\mathrm{Sym}^2 V$ *and* $\bigwedge^2 V$.
Their characters are $\chi_{\mathrm{Sym}^2}(g) = \frac{1}{2}(\chi_{st}(g)^2 + \chi_{st}(g^2)), \chi_{\wedge^2} = \frac{1}{2}(\chi_{st}(g)^2 - \chi_{st}(g^2))$*:*

S_5	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2 3 4 5)	(1 2)(3 4)	(1 2)(3 4 5)
χ_{Sym^2}	10	4	1	0	0	2	1
$\chi_{\wedge^2}$	6	0	0	0	1	-2	0

And we can easily check $(\chi_{\wedge^2}, \chi_{\wedge^2}) = 1, (\chi_{\mathrm{Sym}^2}, \chi_{\mathrm{Sym}^2}) = 3, (\chi_{\mathrm{Sym}^2}, \chi_0) = (\chi_{\mathrm{Sym}^2}, \chi_{st}) = 1$.
So $\rho_{\wedge^2}$ *is irreducible and* $\rho_{\mathrm{Sym}^2} = \rho_0 \oplus \rho_{st} \oplus \rho$ *where* ρ *is a degree* 5 *irreducible representation.*

S_5	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2 3 4 5)	(1 2)(3 4)	(1 2)(3 4 5)
χ_0	1	1	1	1	1	1	1
$\chi_\pm$	1	-1	1	-1	1	1	-1
χ_{st}	4	2	1	0	-1	0	-1
$\chi_{\pm st}$	4	-2	1	0	-1	0	1
χ	5	1	-1	-1	0	1	1
χ'	5	-1	-1	1	0	1	-1
$\chi_{\wedge^2}$	6	0	0	0	1	-2	0

Exam 4.2.8. *Consider* $G = A_5$*. Then there are four conjugacy classes with representative elements* $(1\ 2\ 3), (1\ 2)(3\ 4), (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4)$.

We already know two representations ρ_0 *and* ρ_{st}.

S_5	1	(1 2 3)	(1 2)(3 4)	(1 2 3 4 5)	(1 3 5 2 4)
χ_0	1	1	1	1	1
χ_{st}	4	1	0	-1	-1

Consider $\rho_{\mathrm{Sym}^2}, \rho_{\wedge^2}$.

S_5	1	(1 2 3)	(1 2)(3 4)	(1 2 3 4 5)	(1 3 5 2 4)
χ_{Sym^2}	10	1	2	0	0
$\chi_{\wedge^2}$	6	0	-2	1	1

Then we can compute that $(\chi_{\mathrm{Sym}^2}, \chi_{\mathrm{Sym}^2}) = 3, (\chi_{\mathrm{Sym}^2}, \chi_0) = (\chi_{\mathrm{Sym}^2}, \chi_{st}) = 1, (\chi_{\wedge^2}, \chi_{\wedge^2}) = 2$ *and* $\chi_{\wedge^2}$ *is orthogonal to* χ_0, χ_{st}.

So $\rho_{\mathrm{Sym}^2} = \rho_0 \oplus \rho_{st} \oplus \rho, \rho_{\wedge^2} = \rho_1 \oplus \rho^2$ *where* ρ, ρ_1, ρ_2 *are irreducible.*

And since $\deg^2 \rho_1 + \deg^2 \rho_2 = 60 - 1 - 16 - 25 = 18 = 9 + 9$.

We set

S_5	1	(1 2 3)	(1 2)(3 4)	(1 2 3 4 5)	(1 3 5 2 4)
χ_0	1	1	1	1	1
χ_{st}	4	1	0	-1	-1
χ	5	-1	1	0	0
χ_1	3	a	b	c	d
χ_2	3	$-a$	$-2-b$	$1-c$	$1-d$

By row orthogonality, $20a + 15b + 12c + 12d = -3, 20a = 12c + 12d - 12, 20a = 15b + 15$, $9 + 20a^2 + 15b^2 + 12c^2 + 12d^2 = 60$.

Hence $a = 0, b = -1, c = \frac{1+\sqrt{5}}{2}, d = \frac{1-\sqrt{5}}{2}$.

S_5	1	(1 2 3)	(1 2)(3 4)	(1 2 3 4 5)	(1 3 5 2 4)
χ_0	1	1	1	1	1
χ_{st}	4	1	0	-1	-1
χ	5	-1	1	0	0
χ_1	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_2	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

Remark 4.2.2. Notice that A_5 is the rotation symmetric group of dodecahedron, this naturally gives us a degree 3 representation. Explicitly, they are actually ρ_1 or ρ_2.

Prop 4.2.4. *Let* N *be a normal subgroup of* G *and* V *be a representation of* N*, we set* $\tilde{\rho} = \pi \circ \rho : G \to G/N \to \mathrm{GL}(V)$ *where* π *is the quotient map* $G \to G/N$*, then* $\tilde{\rho}$ *is irreducible iff* ρ *is irreducible.*

Proof. Since $\tilde{\rho}_g = \rho_{gN}$, we obtain that

$$\begin{aligned}(\tilde{\chi}, \tilde{\chi})_G &= \frac{1}{|G|} \sum_{g \in G} \overline{\tilde{\chi}(g)} \tilde{\chi}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi(gN)} \chi(gN) \\ &= \frac{1}{|G/N|} \sum_{g \in G/N} \overline{\chi(g)} \chi(g) \\ &= (\chi, \chi)_{G/N}\end{aligned}$$

□

Exam 4.2.9. *Consider* $G = S_4, N = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Then $G/N \cong S_3$*, this induce three irreducible representations*

S_4	1	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
$\tilde{\chi}_0$	1	1	1	1	1
$\tilde{\chi}_\pm$	1	-1	1	-1	1
$\tilde{\chi}_{st}$	2	0	-1	0	2

This can help us solve the character table more quickly.

4.3 Induced representation

Def 4.3.1. Let $H < G$ be a subgroup and V be a representation of G, then V restricts to a representation of H, denoted by $\mathrm{Res}^G_H V$. Let W be a subspace of V which is a representation of H, then the subspace $gW = \{\rho_g(w) | w \in W\}$ depends only on the left coset gH. We say V is induced by W if every element in V can be written uniquely as a sum of elements in such translates of W, *i.e.*

$$V = \bigoplus_{\sigma \in G/H} \sigma W.$$

In this case, we denote V by $\mathrm{Ind}^G_H W$.

Prop 4.3.1 (universal property of induced representation)**.** *Let W be a representation of H and U be a representation of G, suppose $V = \mathrm{Ind}\, W$, then any H-linear map $\varphi : W \to U$ extends uniquely to a G-linear map $\tilde{\varphi} : V \to U$, that is,*

$$\mathrm{Hom}_H(W, \mathrm{Res}\, U) = \mathrm{Hom}_G(\mathrm{Ind}\, W, U).$$

Proof. For $\sigma \in G/H, g \in \sigma H$ and $w \in W$, we define $\tilde{\varphi}(\rho^V_g(w)) = \rho^U_g(\varphi(w))$. □

Prop 4.3.2.

$$\chi_{\mathrm{Ind}\, W}(g) = \sum_{g\sigma = \sigma} \chi_W(\sigma^{-1} g \sigma).$$

Remark 4.3.1. The right side of the equation is well-defined since χ_W is a class function

Coro 4.3.1. *Let W be a representation of H and U be a representation of G, then*

$$(\chi_{\mathrm{Ind}\, W}, \chi_U)_G = (\chi_W, \chi_{\mathrm{Res}\, U})_H.$$

Proof. By corollary 4.2.2. □

Prop 4.3.3. *Let H, K be two subgroups of G, W be a representation of H and $V = \mathrm{Ind}^G_H W$. Choose a set of representatives S for $K\backslash G/H$, let $H_s = sHs^{-1} \cap K$ for $s \in S$. Set $\rho^s : H_s \to \mathrm{GL}(W), g \mapsto \rho^V_{s^{-1}gs}$, we denote this representation by W_s. Then the representation $\mathrm{Res}_K V$ is isomorphic to the direct sum of $\mathrm{Ind}^K_{H_s}(W_s)$ for $s \in S$.*

Proof. Let $V(s) = (KsH)W = \{\rho^V_x(w) | x \in KsH, w \in W\}$ for $s \in S$.
Then $V(s)$ is K-invariant, we claim that it is K-linear isomorphic to $\mathrm{Ind}^K_{H_s}(W_s)$.
For $k \in K$ such that $ksW = sW$, $s^{-1}ks \in H$, *i.e.* $k \in H_s$.
So $V(s) = \oplus_{\sigma \in K/H_s} \sigma(sW) = \mathrm{Ind}^K_{H_s}(sW)$.
And since sW is H_s-linear isomorphic to W_s by $W_s \to sW : w \mapsto \rho^V_s(w)$.
Hence $V(s) = \mathrm{Ind}^K_{H_s}(sW) = \mathrm{Ind}^K_{H_s}(W_s)$. □

4.4 The group algebra

Def 4.4.1. Let G a group, the group algebra $\mathbb{C}G$ is an algebra whose underlying vector space is spanned by $\{e_g\}_{g \in G}$, and the multiplication is defined by $e_g e_h = e_{gh}$.

Prop 4.4.1. *Let $\{V_i\}$ be the set of all irreducible representations of G, then $\mathbb{C}G \cong \bigoplus \mathrm{End}(V_i)$.*

Proof. A representation $G \to \mathrm{GL}(V_i)$ can be extended to a map $\mathbb{C}G \to \mathrm{End}(V_i)$ linearly.
So this gives us a map $\varphi : \mathbb{C}G \to \bigoplus \mathrm{End}(V_i)$.
Then φ is injective and $\dim \mathbb{C}G = |G| = \sum (\dim V_i)^2$. □

Prop 4.4.2 (Fourier inversion formula)**.** *Let* $(u_1, \dots, u_m) \in \bigoplus \mathrm{End}(V_i)$ *which corresponds to* $u = \sum u(g)e_g \in \mathbb{C}G$*, then*

$$u(g) = \frac{1}{|G|} \sum_{i=1}^{m} n_i \operatorname{tr}_{V_i} \left(\rho^i_{g^{-1}} u_i \right),$$

where $n_i = \dim V_i$*.*

Proof.

$$\begin{aligned}
\frac{1}{|G|} \sum_{i=1}^{m} n_i \operatorname{tr}_{V_i} \left(\rho^i_{g^{-1}} u_i \right) &= \frac{1}{|G|} \sum_{i=1}^{m} n_i \operatorname{tr}_{V_i} \left(\rho^i_{g^{-1}} \sum_{h \in G} u(h) \rho^i_h \right) \\
&= \frac{1}{|G|} \sum_{h \in G} u(h) \sum_{i=1}^{m} n_i \operatorname{tr}_{V_i} \left(\rho^i_{g^{-1}h} \right) \\
&= \frac{1}{|G|} \sum_{h \in G} u(h) \sum_{i=1}^{m} n_i \chi^i_{g^{-1}h} \\
&= \sum_{h \in G} u(h) \cdot \mathbf{1}_{g=h} = u(g)
\end{aligned}$$

□

Prop 4.4.3. *Let* V *be an irreducible representation of* G *of degree* n *and* $\tilde{\rho} : \mathbb{C}G \to \mathrm{End}(V)$ *be the corresponding map, then* $\tilde{\rho}$ *maps the center of* $\mathbb{C}G$ *to* $\{\lambda I | \lambda \in \mathbb{C}\}$*.*

More explicitly, let $u = \sum u(g)e_g \in Z(\mathbb{C}G)$*, then*

$$\lambda_i(u) = \frac{1}{n} \sum_{g \in G} u(g)\chi(g).$$

Proof. Since $u \in Z(\mathbb{C}G)$, *i.e.* $\sum u(g)e_g = e_h \cdot \sum u(g)e_g \cdot e_{h^{-1}} = \sum u(h^{-1}gh)e_g$.
So $\sum (u(h^{-1}gh) - u(g))e_g = 0$, *i.e.* u is a class function.
By lemma 4.2.1, $\tilde{\rho}(u)$ is a G-linear map.
By Schur lemma, $\tilde{\rho}(u) = \lambda(u)I$ for some $\lambda(u)$.
Moreover, $\lambda(u) = \frac{1}{n} \operatorname{tr}_V(\tilde{\rho}(u)) = \frac{1}{n} \sum u(g)\chi(g)$. □

Coro 4.4.1. $\mathbb{C}G \cong \bigoplus \mathrm{End}(W_i)$ *induces an isomorphism* $Z(\mathbb{C}G)$ *onto* $\mathbb{C}^m$ *where* m *is the number of conjugacy classes.*

Def 4.4.2. A complex number which is integral over $\mathbb{Z}$ is called algebraic integer.

Prop 4.4.4. *Let* V *be a representation of* G*, then* $\chi(g)$ *is an algebraic integer for all* $g \in G$*.*

Proof. $\chi(g) = \operatorname{tr}(\rho(g))$ and the eigenvalue of $\rho(g)$ are all roots of unity. □

Prop 4.4.5. *Let* $u = \sum u(g)e_g$ *be an element of* $Z(\mathbb{C}G)$ *such that* $u(g)$ *are all algebraic integers, then* u *is integral over* $\mathbb{Z}$*.*

Proof. Let $\{C_i\}$ be the set of conjugacy classes of G and $\Sigma_i = \sum_{g \in C_i} e_g$, take $g_i \in C_i$.
Then $\{\Sigma_i\}$ forms a basis of $Z(\mathbb{C}G)$ and $u = \sum u(g_i)\Sigma_i$.
So it suffices to show that Σ_i are integral over $\mathbb{Z}$.
Notice that $\Sigma_i\Sigma_j$ is a linear combination with integer coefficient of $\{\Sigma_k\}$.
So $\mathbb{Z}\Sigma_1 \oplus \cdots \oplus \mathbb{Z}\Sigma_m$ is a subring of $Z(\mathbb{C}G)$ and is finitely generated over $\mathbb{Z}$.
So Σ_i are integral over $\mathbb{Z}$. □

Coro 4.4.2. *Let* V *be an irreducible representation of* G *of degree* n *and* $u = \sum u(g)e_g$ *be an element of* $Z(\mathbb{C}G)$ *such that* $u(g)$ *are all algebraic integers, then* $\frac{1}{n} \sum u(g)\chi(g)$ *is an algebraic integer.*

Coro 4.4.3. *The degree of the irreducible representations of G divide the order of G.*

Proof. Let V be an irreducible representation of G of degree n.
Take $u = \sum \overline{\chi(g)} e_g$.
By proposition 4.4.4 and corollary 4.4.2, $\frac{1}{n} \sum \overline{\chi(g)} \chi(g) = \frac{|G|}{n}$ is an algebraic integer.
And since $\frac{|G|}{n} \in \mathbb{Q}$ and $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.
So $n \big| |G|$. □

Chapter 5

Lie Group and Lie Algebra

5.1 Basic concept

Def 5.1.1. A Lie group G is a group with a smooth manifold structure on it such that

$$G \times G \to G : (a, b) \mapsto ab,$$

$$G \to G : a \mapsto a^{-1}$$

are smooth maps. A Lie subgroup H of G is a subgroup of G with a Lie group structure such that the inclusion $H \to G$ is an immersion. A morphism between two Lie groups G and H is a smooth map $\rho : G \to H$ which is also a group homomorphism.

Lemma 5.1.1. *Any discrete normal subgroup of a connected Lie group G is in the center $Z(G)$.*

Proof. Take $g \in N$, then $hgh^{-1} \in N$ for all $h \in N$.
And since N is discrete.
So $\{hgh^{-1} | h \in H\} = \{g\}$, *i.e.* $g \in Z(G)$. □

Prop 5.1.1. *Let G be a Lie group, H be a connected manifold and $\varphi : H \to G$ a covering space map, take an element $\tilde{e}$ lying over the identity e of G then there is a unique Lie group structure on H such that e' is the identity, φ is a morphism of Lie groups and* $\ker \varphi \subset Z(H)$.

Proof. The multiplication $\times : G \times G \to G, (a, b) \mapsto ab$ can lift to a map $H \times H \to H$ with $(\tilde{e}, \tilde{e}) \mapsto \tilde{e}$ uniquely, which gives us the Lie group structure on H.
Moreover, $\ker \varphi$ is a discrete normal subgroup of H.
So by lemma, $\ker \varphi \subset Z(H)$. □

Def 5.1.2. We say such G and H are isogenous and call φ an isogeny.

Prop 5.1.2. *Let H be a Lie group and $\Gamma \subset Z(H)$ be a discrete subgroup of its center, then there is a unique Lie group structure on the quotient group $G = H/\Gamma$ such that the quotient map $H \to G$ is a Lie group morphism.*

Def 5.1.3.

$$L_g : G \to G, h \mapsto gh \qquad R_g : G \to G, h \mapsto hg,$$

$$\Phi_g : G \to G, h \mapsto ghg^{-1},$$

$$\mathrm{Ad}_g = (\mathrm{d}\Phi_g)_e : T_eG \to T_eG.$$

Here Ad_g gives a representation $\mathrm{Ad} : G \to \mathrm{GL}(T_eG)$, called the adjoint representation.
Moreover, we denote the differential of Ad_g at e by $\mathrm{ad} : T_eG \to \mathrm{End}(T_eG)$.

Prop 5.1.3. *Let $X, Y \in T_eG$, then*

$$\mathrm{ad}(X)(Y) = [X, Y] := \left(X^j \frac{\partial Y^i}{\partial x^j} - Y^j \frac{\partial X^i}{\partial x^j} \right) \frac{\partial}{\partial x^i}.$$

Here we call $[X, Y]$ the Lie bracket.

Prop 5.1.4. *Let G, H be two Lie groups and $\varphi : G \to H$ be a morphism, then*

$$\mathrm{d}\varphi_e \circ \mathrm{Ad}_g(X) = \mathrm{Ad}_{\varphi(g)} \circ \mathrm{d}\varphi_e(X),$$

$$\mathrm{d}\varphi_e \circ \mathrm{ad}(X)(Y) = \mathrm{ad}(\mathrm{d}\varphi_e(X))(\mathrm{d}\varphi_e(Y)).$$

Prop 5.1.5. *Lie bracket is skew-symmetric and satisfies the Jacobi identity:*

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0.$$

Def 5.1.4. A Lie algebra is a vector space together with a bilinear map $[\ ,\ ] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ that is skew-symmetric and satisfies the Jacobi identity. A Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is a subspace of $\mathfrak{g}$ that is closed under Lie bracket of $\mathfrak{g}$. A morphism between two Lie algebras $\mathfrak{g}, \mathfrak{h}$ over F is an F-linear map $f : \mathfrak{g} \to \mathfrak{h}$ such that $f[X, Y] = [fX, fY]$ for all $X, Y \in \mathfrak{g}$.

Remark 5.1.1. By the above discussion, the tangent space T_eG of a Lie group G is naturally a Lie algebra and a morphism of Lie group naturally induce a morphism of Lie algebra.

Exam 5.1.1. GL_n *and its Lie algebra is* $\mathfrak{gl}_n = M_n$.
SL_n *and its Lie algebra is* $\mathfrak{sl}_n = \{X \in M_n | \operatorname{tr} X = 0\}$.
$\mathrm{O}_{p,q}(\mathbb{R})$ *and its Lie algebra is* $\mathfrak{o}_{p,q}(\mathbb{R}) = \{X \in M_n(\mathbb{R}) | X^T I_{p,q} + I_{p,q} X = 0\}$.
$\mathrm{SO}_n(\mathbb{R})$ *and its Lie algebra is* $\mathfrak{so}_n(\mathbb{R}) = \{X \in M_n(\mathbb{R}) | X^T + X = 0\}$.
$\mathrm{U}_{p,q}(\mathbb{C})$ *and its Lie algebra is* $\mathfrak{u}_{p,q}(\mathbb{C}) = \{X \in M_n(\mathbb{C}) | X^* I_{p,q} + I_{p,q} X = 0\}$.
$\mathrm{SU}_n(\mathbb{C})$ *and its Lie algebra is* $\mathfrak{su}_n(\mathbb{C}) = \{X \in M_n(\mathbb{C}) | X^* + X = 0, \operatorname{tr} X = 0\}$.
Sp_{2n} *and its Lie algebra is* $\mathfrak{sp}_{2n} = \{X \in M_{2n} | \Omega X + X^T \Omega = 0\}$, *where Ω is the matrix of standard skew-symmetric matrix.*

Def 5.1.5. Let G be a Lie group, consider a morphism $\varphi : \mathbb{R} \to G$ such that

$$\mathrm{d}\varphi_t(X) = (L_{\varphi(t)})_*(X).$$

Then we defined the exponential map $\exp : \mathfrak{g} \to G, X \mapsto \varphi_X(1)$.

Prop 5.1.6. $\mathrm{d}\exp_0 : T_0\mathfrak{g} = \mathfrak{g} \to T_eG = \mathfrak{g}$ *is identity.*

Prop 5.1.7. *Let G, H be two Lie groups and $\varphi : G \to H$ be a morphism, then for $X \in \mathfrak{g}$,*

$$\varphi(\exp_G X) = \exp_H(\mathrm{d}\varphi_e(X)).$$

Coro 5.1.1. $x(\exp X)x^{-1} = \exp(Ad(x)(X)), \mathrm{Ad}(\exp X) = e^{\mathrm{ad}_X}$. *Here $e^{\cdot}$ is the exponential map of matrix.*

Prop 5.1.8. *Let H be a Lie subgroup of G and $i : H \hookrightarrow G$ is the inclusion, then*

$$\mathfrak{h} = \{X \in \mathfrak{g} | \exp_G(tX) \in i(H) \text{ for all } t \in \mathbb{R}\}.$$

Proof. Take $X \in \mathfrak{h}$, then $\exp_G(tX) = i(\exp_H(tX)) \in i(H)$.
Conversely, take $X \in \mathfrak{g}$ such that $\exp_G(tX) \in i(H)$ for all $t \in \mathbb{R}$.
We only prove this when H is an embedding Lie subgroup.
So $\gamma : \mathbb{R} \to H, t \mapsto \exp_G(tX)$ is smooth.
Hence $X = \gamma'(0) \in \mathfrak{h}$. □

Thm 5.1.1. *Let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{g}$, then there exists a unique connected Lie subgroup H of G with Lie algebra $\mathfrak{h}$. Moreover, H is generated by $\exp(\mathfrak{h})$.*

Thm 5.1.2 (Cartan closed subgroup)**.** *A closed subgroup of a Lie group G is an embedding Lie subgroup.*

Coro 5.1.2. *Let G, H be two Lie groups and $f : G \to H$ be a continuous group homomorphism, then f is analytic.*

Proof. Let Γ_f be the graph of f.
Then Γ_f is closed in $G \times H$, *i.e.* Γ_f is an embedding Lie subgroup of $G \times H$.
So $\Gamma_f \hookrightarrow G \times H \to G$ is bijective and analytic.
By inverse function theorem, $\Gamma_f \cong G$ as Lie group.
So $f : G \cong \Gamma_f \hookrightarrow G \times H \to H$ is analytic. □

Thm 5.1.3 (Baker-Comphell-Hausdorff-Dynkin)**.** *Denote $\exp(\mu(X, Y)) = \exp(X)\exp(Y)$, then $\mu(X, Y)$ is real analytic and*

$$\mu(X,Y) = X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}[X,[X,Y]] + \frac{1}{12}[Y,[Y,X]] + \dots$$

Thm 5.1.4 (Ado theorem)**.** *Any finite dimensional Lie algebra over a field of character 0 is a Lie subalgebra of certain $\mathfrak{gl}(V)$ for a finite dimensional vector space V.*

Coro 5.1.3 (Lie third theorem)**.** *Let $\mathfrak{g}$ be a finite dimensional real Lie algebra, then there exists a Lie group G with Lie algebra $\mathfrak{g}$. Moreover, we can choose G to be simply connected.*

Proof. By Ado theorem, there exists an inclusion $\mathfrak{g} \hookrightarrow \mathfrak{gl}_n$.
By theorem 5.1.1, there exists a Lie group $G \subset \mathrm{GL}_n$ with Lie algebra $\mathfrak{g}$.
Moreover, take the universal cover $\tilde{G}$ of G, its Lie algebra is also $\mathfrak{g}$. □

Prop 5.1.9. *Let G, H be two connected Lie group and $\varphi : G \to H$ be a homomorphism such that $\mathrm{d}\varphi : \mathfrak{g} \to \mathfrak{h}$, then φ is an isogeny.*

Proof. Let U be a neighborhood of e_G and it maps to a neighborhood of e_H diffeomorphically.
We claim that $\varphi^{-1}(V) = \bigsqcup_{g\in\Gamma} gU$, where $\Gamma = \varphi^{-1}(e_H)$.
For $x \in U, g \in \Gamma\backslash\{e_G\}$, $\varphi(gx) = \varphi(x)$ and $gx \neq x$.
So $gx \notin U$, *i.e.* $U \cap gU = \varnothing$.
And since $\varphi^{-1}(h)$ is a coset of Γ.
Therefore $\varphi^{-1}(V) = \bigsqcup_{g\in\Gamma} gU$ and each gU maps to V diffeomorphically.
Hence $\varphi : G \to H$ is an isogeny. □

Thm 5.1.5. *Let G, H be two connected Lie group, G is simply connected and $\rho : \mathfrak{g} \to \mathfrak{h}$ is a Lie algebra morphism, then there exists a unique $\varphi : G \to H$ such that $\mathrm{d}\varphi = \rho$.*

Proof. Let $\mathfrak{k}$ be the graph of ρ.
By theorem 5.1.1, there exists a Lie subgroup K of $G \times H$ with Lie algebra $\mathfrak{k}$.
So $\psi : K \hookrightarrow G \times H \to G$ induces a bijection $\mathfrak{k} \to \mathfrak{g}$.
By proposition 5.1.9, ψ is an isogen, *i.e.* ψ is isomorphism since G is simply connected.
Hence $\varphi : G \cong K \hookrightarrow G \times H \to H$ gives a map with $\mathrm{d}\varphi = \rho$. □

Coro 5.1.4. *Let G_1, G_2 be two simply connected Lie groups with $\mathfrak{g}_1 \cong \mathfrak{g}_2$, then $G_1 \cong G_2$.*

5.2 Solvable and nilponent Lie algebra

Def 5.2.1. A Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is called an ideal if $[x, y] \in \mathfrak{h}$ for every $x \in \mathfrak{h}, y \in \mathfrak{g}$.

The center of $\mathfrak{g}$ is $Z(\mathfrak{g}) = \{x | [x, y] = 0 \text{ for all } y \in \mathfrak{g}\}$. We say $\mathfrak{g}$ is abelian if $\mathfrak{g} = Z(\mathfrak{g})$.

Prop 5.2.1. *Let I, J be two ideals of $\mathfrak{g}$, then $I + J, [I, J]$ are ideals of $\mathfrak{g}$.*

Prop 5.2.2. *Let $\mathfrak{g}, \mathfrak{h}$ be two Lie algebras and $\varphi : \mathfrak{g} \to \mathfrak{h}$ be a morphism, then the kernel $\ker \varphi$ of φ is an ideal of $\mathfrak{g}$ and the image $\varphi(\mathfrak{g})$ is naturally isomorphic to $\mathfrak{g}/\ker \varphi$.*

Def 5.2.2. If $\mathfrak{g}$ is non-abelian and has no nontrivial ideals, then we called $\mathfrak{g}$ a simple Lie algebra.

Denote $D\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}], D_k\mathfrak{g} = [D_{k-1}\mathfrak{g}, \mathfrak{g}]$ and $D^k\mathfrak{g} = [D_{k-1}\mathfrak{g}, D_{k-1}\mathfrak{g}]$. $\mathfrak{g}$ is said to be nilpotent if $D_k\mathfrak{g} = 0$ for some k. We say $\mathfrak{g}$ is solvable if $D^k\mathfrak{g} = 0$ for some k. And $\mathfrak{g}$ is called semisimple Lie algebra if $\mathfrak{g}$ has no nontrivial solvable ideals.

Exam 5.2.1. *Let $t_n(F)$ be the set of upper triangular matrix and $n_n(F)$ be the set of strictly upper triangular matrix, then $D_n n_n(F) = 0, Dt_n(F) = n_n(F)$ and $[t_n(F), n_n(F)] = n_n(F)$.*

Then $t_n(F)$ is solvable but not nilpotent and $n_n(F)$ is nilpotent.

Prop 5.2.3. *Let $\mathfrak{g}$ be a Lie algebra, then it is solvable iff there exists a sequence of Lie algebras $\mathfrak{g} \supset \mathfrak{g}_1 \supset \cdots \supset \mathfrak{g}_l = 0$ such that $\mathfrak{g}_{i+1}$ is an ideal of $\mathfrak{g}_i$ and $\mathfrak{g}_i/\mathfrak{g}_{i+1}$ is abelian.*

Proof. $\Rightarrow$: take $\mathfrak{g}_i = D^k\mathfrak{g}$
$\Leftarrow$: Since $D(\mathfrak{g}_i/\mathfrak{g}_{i+1}) = 0$.
So $D\mathfrak{g}_i \subset \mathfrak{g}_{i+1}$.
Hence $D^k\mathfrak{g} \subset \mathfrak{g}_k$, *i.e.* $D^l\mathfrak{g} = 0$. □

Prop 5.2.4. *Let $\mathfrak{g}$ be a Lie algebra, then it is semisimple iff it has no nonzero abelian ideal.*

Proof. $\Rightarrow$: An abelian ideal is solvable.
$\Leftarrow$: For a solvable ideal I, let $D^k I = 0$ and $D^{k-1} I \neq 0$.
Then $D^{k-1} I$ is abelian. □

Prop 5.2.5. *Let $\mathfrak{h}$ be a Lie subalgebra of $\mathfrak{g}$, then $\mathfrak{g}$ is solvable iff $\mathfrak{h}$ and $\mathfrak{g}/\mathfrak{h}$ are solvable.*

Proof. $\Rightarrow$: $D^k\mathfrak{h} \subset D^k\mathfrak{g}, D(\mathfrak{g}/\mathfrak{h}) = (D\mathfrak{g})/\mathfrak{h}$.
$\Leftarrow$: Let $D^k(\mathfrak{g}/\mathfrak{h}) = 0$.
Then $D^k\mathfrak{g} \subset \mathfrak{h}$ is solvable. □

Prop 5.2.6. *Let I, J be two solvable ideals of $\mathfrak{g}$, then $I + J$ is also a solvable ideal.*

Proof. $(I + J)/I \cong J/(I \cap J)$ and $I, J, I \cap J$ are solvable. □

Prop 5.2.7. *Let H be a Lie subgroup of G, then $H \lhd G$ iff $\mathfrak{h}$ is an ideal of $\mathfrak{g}$.*

Proof. $\Rightarrow$: $\mathrm{Ad}_g\mathfrak{h} \subset \mathfrak{h}$ for all $g \in G$.
So $[x, \mathfrak{h}] = \mathrm{ad}_x(\mathfrak{h}) \subset \mathfrak{h}$ for all $x \in \mathfrak{g}$, *i.e.* $\mathfrak{h}$ is an ideal.
$\Leftarrow$: $\mathrm{Ad}(\exp x) = e^{ad_x}$ maps $\mathfrak{h}$ to $\mathfrak{h}$ for all $x \in \mathfrak{g}$.
And since $\exp \mathfrak{g}$ generates G.
So Ad_g maps $\mathfrak{h}$ to $\mathfrak{h}$ for all $g \in G$, *i.e.* $H \trianglelefteqslant G$. □

Prop 5.2.8. *A connected Lie group G is solvable iff $\mathfrak{g}$ is a solvable Lie algebra.*

Def 5.2.3. Let $I \subset \mathfrak{g}$ be a solvable ideal with maximal possible dimension, then I contains all solvable ideals of $\mathfrak{g}$, otherwise the ideal adding them up has bigger dimension. In this sense, we call I the maximal solvable ideal of $\mathfrak{g}$, denoted by $\mathrm{Rad}\,\mathfrak{g}$, called the radical of $\mathfrak{g}$.

Thm 5.2.1 (Levi theorem)**.** *Let $\mathfrak{g}$ be a Lie algebra over character zero field F, then there exists a Lie subalgebra $\mathfrak{h}$ such that $\mathfrak{h} \cong \mathfrak{g}/\operatorname{Rad}\mathfrak{g}$.*

Prop 5.2.9. *Let $\mathfrak{g}$ be a Lie algebra, then*

(1) If $\mathfrak{g}$ is nilpotent, then any Lie subgroup or quotient algebra of $\mathfrak{g}$ is nilpotent.

(2) $\mathfrak{g}/Z(\mathfrak{g})$ is nilpotent iff $\mathfrak{g}$ is nilpotent.

(3) If $\mathfrak{g}$ is nilpotent and nonzero, then $Z(\mathfrak{g}) \neq 0$.

Proof. (1) $D_k\mathfrak{h} \subset D_k\mathfrak{g}, D_k(\mathfrak{g}/\mathfrak{h}) = (D_k\mathfrak{g})/\mathfrak{h}$.

(2) Since $(D_k\mathfrak{g})/Z(\mathfrak{g}) = D_k(\mathfrak{g}/Z(\mathfrak{g})) = 0$ for some k .
So $D_k\mathfrak{g} \subset Z(\mathfrak{g})$ and $D_{k+1}\mathfrak{g} = [D_k\mathfrak{g}, \mathfrak{g}] \subset [Z(\mathfrak{g}), \mathfrak{g}] = 0$.

(3) Let $D_k\mathfrak{g} = 0$ and $D_{k-1}\mathfrak{g} \neq 0$.
Then $D_k = [D_{k-1}\mathfrak{g}, \mathfrak{g}] = 0$, *i.e.* $D_{k-1}\mathfrak{g} \subset Z(\mathfrak{g})$.

□

Def 5.2.4. Let $\mathfrak{g}$ be a Lie algebra, an element $x \in \mathfrak{g}$ is said to be ad-nilpotent if ad_x is a nilpotent endomorphism.

Prop 5.2.10. *Let $\mathfrak{g}$ be a nilpotent Lie algebra, then element element of $\mathfrak{g}$ is ad-nilpotent.*

Proof. $(\operatorname{ad}_x y)^n = [x, [x, [\cdots, [x, y]\cdots]]] \in D_{n+1}\mathfrak{g}$. □

Thm 5.2.2 (Engel)**.** *$\mathfrak{g}$ is nilpotent iff every element of $\mathfrak{g}$ is ad-nilpotent.*

Thm 5.2.3. *Let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}(V)$, if every element of $\mathfrak{g}$ is a nilpotent operator, then there exists a nonzero $v \in V$ such that $x(v) = 0$ for all $x \in \mathfrak{g}$.*

Proof. We prove this by induction on $\dim\mathfrak{g}$.
When $\dim\mathfrak{g} = 1$, trivial.
Suppose we have proven for $\dim\mathfrak{g} = n - 1$.
When $\dim\mathfrak{g} = n$, since $x \in \mathfrak{g}$ is a nilpotent operator.
So ad_x is also nilpotent.
Let $\mathfrak{h}$ be a maximal subalgebra of $\mathfrak{g}$.
Then $\operatorname{ad}_x : \mathfrak{g}/\mathfrak{h} \to \mathfrak{g}/\mathfrak{h}$ is nilpotent.
Consider $\{\operatorname{ad}_x : \mathfrak{g}/\mathfrak{h} \to \mathfrak{g}/\mathfrak{h} | x \in \mathfrak{h}\} \subset \mathfrak{gl}(\mathfrak{g}/\mathfrak{h})$, which is a Lie subalgebra with dimension $< n$.
By induction assumption, there exists $y \in \mathfrak{g}/\mathfrak{h}$ such that $\operatorname{ad}_x y = 0 \in \mathfrak{g}/\mathfrak{h}$ for all $x \in \mathfrak{h}$.
So $\mathfrak{h}$ and y span a Lie subalgebra $\mathfrak{h}'$ of $\mathfrak{g}$ and $\dim\mathfrak{h}' = \dim\mathfrak{h} + 1$.
Therefore $\mathfrak{h}' = \mathfrak{g}$ and $\dim\mathfrak{h} = \dim\mathfrak{g} - 1$.
Consider $W = \{v | \mathfrak{h}v = 0\}$.
By induction assumption, W is nonzero.
And since for $x \in \mathfrak{h}, v \in W$, $xy(v) = yx(v) + [x, y](v) = \operatorname{ad}_x y(v) = 0$.
So $y(v) \in W$, *i.e.* y has a 0-eigenvector in W. □

Thm 5.2.4. *Let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}(V)$, if every element of $\mathfrak{g}$ is a nilpotent operator, then there exists flag $(0) = V_0 \subset V_1 \subset \cdots \subset V_n = V$ with $\dim V_i = i$ such that $xV_i \subset V_{i-1}$ for $x \in \mathfrak{g}$. In other word, there exists a basis of V such that the representative matrix of every $x \in \mathfrak{g}$ lies in $n_n(V)$.*

Proof. We prove this by induction on $\dim V$.
When $\dim V = 1$, trivial.
Suppose we have proven for $\dim V = n-1$.
When $\dim V = n$, by theorem 5.2.3, there exists v such that $x(v) = 0$ for every $x \in \mathfrak{g}$.
Let $W = V/\{cv | c \in F\}$.
By induction assumption, there exists a flag $W_0 \subset W_1 \subset \cdots \subset W_{n-1}$ such that $xW_i \subset W_{i-1}$.
Take $V_i = \pi^{-1}(W_{i-1})$ where $\pi : V \to W$. □

Proof of Engel theorem. $\mathrm{ad}_{\mathfrak{g}} \subset \mathfrak{gl}(\mathfrak{g})$ is a Lie subalgebra.
So $\mathrm{ad}_{\mathfrak{g}} \subset n_n(F)$ under a basis of $\mathfrak{gl}(\mathfrak{g})$.
Hence $\mathrm{ad}_{\mathfrak{g}} = \mathfrak{g}/Z(\mathfrak{g})$ is nilpotent. □

Thm 5.2.5 (Lie)**.** *Let F be a character zero algebraic closed field, V be a vector space over F and $\mathfrak{g} \subset \mathfrak{gl}(V)$ be solvable, then there exists $v \in V$ such that v is an eigenvector for any $x \in \mathfrak{g}$.*

Proof. We prove this by induction on $\dim \mathfrak{g}$.
When $\dim \mathfrak{g} = 1$, trivial.
Suppose we have proven for $\dim \mathfrak{g} = n-1$.
When $\dim \mathfrak{g} = n$, $\mathfrak{g}/D\mathfrak{g}$ is abelian and nontrivial.
So there is a ideal $\mathfrak{h}$ of $\mathfrak{g}$ with codimensional 1.
By induction assumption, there exists $v \in V$ such that v is an eigenvector for any $x \in \mathfrak{h}$.
Let $xv = \lambda(x)v$ with $\lambda(x) \in F$ and $W = \{w | xw = \lambda(x)w\}$.
Take $x \in \mathfrak{h}, y \in \mathfrak{g}\backslash\mathfrak{h}$ and $w \in W$, we want to show $xy(w) = \lambda(x)y(w)$.
Since $xy(w) = yx(w) + [x,y](w) = \lambda(x)y(w) + \lambda([x,y])w$.
So it suffices to show $\lambda([x,y]) = 0$.
Let $W_i = \mathrm{span}\{w, y(w), \ldots, y^{i-1}(w)\}$ and $W_m = W_{m+1} = \ldots$.
Then for $z \in \mathfrak{h}$, $z(y^i(w)) = yzy^{i-1}(w) + [z,y]y^{i-1}(w) \equiv \lambda(z)y^i w \pmod{W_i}$.
Therefore z preserves each W_i and $\mathrm{tr}_{W_n} z = n\lambda(z)$.
Take $z = [x,y] = xy - yx$, then $\mathrm{tr}_{W_n} z = 0$.
Hence $\lambda(z) = 0$. □

Coro 5.2.1. *Let F be a character zero algebraic closed field, V be a vector space over F and $\mathfrak{g} \subset \mathfrak{gl}(V)$ be solvable, then $\mathfrak{g}$ stabilizes certain flag on V. In other words, there exists a basis of V such that $\mathfrak{g} \subset t_n(F)$.*

Coro 5.2.2. *Let F be a character zero algebraic closed field and $\mathfrak{g}$ be a solvable Lie algebra over F, then there exists a chain of ideals $(0) = \mathfrak{g}_0 \subset \mathfrak{g}_1 \subset \cdots \subset \mathfrak{g}_n = \mathfrak{g}$ with $\dim \mathfrak{g}_i = i$.*

Proof. Consider $\mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ with image $\mathrm{ad}_{\mathfrak{g}} = \mathfrak{g}/Z(\mathfrak{g})$ is solvable.
Then the flag on $\mathfrak{g}$ is stabilized by the adjoint action. □

Coro 5.2.3. *Let F be a character zero algebraic closed field and $\mathfrak{g}$ be a solvable Lie algebra over F, if $x \in D\mathfrak{g}$, then $\mathrm{ad}_x : \mathfrak{g} \to \mathfrak{g}$ nilpotent and so $D\mathfrak{g}$ is nilpotent.*

Proof. $Dt_n(F) = n_n(F)$. □

We now let F be a field with character zero and V be a vector space on F.

Def 5.2.5. Let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}(V)$, then denote $B_V : \mathfrak{g} \times \mathfrak{g} \to F, (x,y) \mapsto \mathrm{tr}(xy)$.

Thm 5.2.6. *Let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}(V)$, then for any $i + j > 0$, $\mathfrak{g}$ is solvable iff $B_V(D^i\mathfrak{g}, D^j\mathfrak{g}) = 0$.*

Def 5.2.6. Let $\bar{F}$ be the algebraic closure of F, then an element $x \in \mathfrak{gl}_n(F)$ is called semisimple if it is diagonalizable over $\bar{F}$.

Prop 5.2.11. *Let $x, y \in \mathfrak{gl}(F)$ be semisimple and $xy = yx$, then $x + y$ is semisimple.*

Prop 5.2.12. *Let $x \in \mathrm{End}(V)$, then*

(1) There exist unique $x_s, x_n \in \mathrm{End}\, V$ such that $x = x_s + x_n$ where x_s is semisimple, x_n is nilpotent and $x_s x_n = x_n x_s$.

(2) There exists $p(T), q(T) \in F[T]$ with constant term 0 such that $x_s = p(x), x_n = q(x)$. In particular, x_s, x_n commute with any endomorphisms of V commuting with x.

(3) If $A \subset B \subset V$ are subspaces, $x(B) \subset A$, then $x_s(B), x_n(B) \subset A$

The decomposition $x = x_s + x_n$ is called the Jordan-Chevalley decomposition of x and x_s, x_n are called semisimple part and nilpotent part of x resp.

Proof. We first assume F is algebraically closed.

Let $f(T) = \prod (T - a_i)^{m_i}$ be the characteristic polynomial of x.

By Jordan decomposition, WLOG, we assume $x = \mathrm{diag}(J_1, \ldots, J_k)$ where J_i are Jordan block with eigenvalue λ_i.

Take polynomial $p(T)$ such that $p(T) \equiv a_i \pmod{(T - a_i)^{m_i}}, p(T) \equiv 0 \pmod{T}$ and $q(T) = T - p(T)$.

Then $p(J_i) = \lambda_i I$, *i.e.* $p(x) = x_s$ and $q(x) = x_n$.

We now assume F is not algebraic closed.

Let $x = x_s + x_n$ be the Jordan decomposition of x in $M_n(\bar{F})$.

Take a Galois extension K of F such that $x_s, x_n \in M_n(K)$.

Then for $\sigma \in \mathrm{Gal}(K/F)$, $x = \sigma(x) = \sigma(x_s) + \sigma(x_n)$.

And since Jordan decomposition is unique.

So $\sigma(x_s) = x_s, \sigma(x_n) = x_n$, *i.e.* $x_s, x_n \in F$. □

Lemma 5.2.1. *Let $A \subset B$ be two subspaces of $\mathfrak{gl}(V)$ and $M = \{x \in \mathfrak{gl}(V) | [x, B] \subset A\}$, if $x \in M$ and $\mathrm{tr}(xy) = 0$ for any $y \in M$, then x is nilpotent.*

Lemma 5.2.2. *Let $x, y, z \in \mathrm{End}(V)$, then $\mathrm{tr}([x, y]z) = \mathrm{tr}(x[y, z])$.*

Proof of Cartan criterion. $\Leftarrow$: We first assume $i = 0, j = 1$.

Let $M = \{x \in \mathfrak{gl}(V) | [x, \mathfrak{g}] \subset D\mathfrak{g}\}$.

For $x = [u, v] \in D\mathfrak{g}, y \in M$, $\mathrm{tr}(xy) = \mathrm{tr}(u[v, y]) = B_V(u, [v, y]) = 0$.

By lemma 5.2.1, x is nilpotent.

By Engel theorem, $D\mathfrak{g}$ is nilpotent, *i.e.* $\mathfrak{g}$ is solvable.

Now for general $i \leqslant j$, $B_V(D^{j+1}\mathfrak{g}, D^j\mathfrak{g}) = 0$.

So $D^j\mathfrak{g}$ is solvable, *i.e.* $\mathfrak{g}$ is solvable. □

Thm 5.2.7 (Intrinsic version of Cartan criterion)**.** *Let $B : \mathfrak{g} \times \mathfrak{g} \to F, (x, y) \mapsto \mathrm{tr}(\mathrm{ad}_x \mathrm{ad}_y)$, $\mathfrak{g}$ is solvable iff $B(\mathfrak{g}, D\mathfrak{g}) = 0$ iff $B(D^i\mathfrak{g}, D^j\mathfrak{g}) = 0$ with $i + j > 0$.*

We call this B the Killing form of $\mathfrak{g}$.

5.3 Semisimple Lie algebra

Def 5.3.1. Given a Lie algebra representation $\mathfrak{g} \to \mathfrak{gl}(V)$, a symmetric F-bilinear form $\beta : V \times V \to F$ is called associative if $\beta(x(v), w) + \beta(v, x(w)) = 0$.

Prop 5.3.1. *Let $\mathfrak{g} \subset \mathfrak{gl}(V)$, then B_V is symmetric, F-bilinear and associative.*

Proof. $B_V(\mathrm{ad}_x y, z) = \mathrm{tr}([x, y]z) = -\mathrm{tr}(y[x, z]) = -B_V(y, \mathrm{ad}_x z)$. □

Lemma 5.3.1. *Let $\beta : \mathfrak{g} \times \mathfrak{g} \to F$ be associative, $I \subset \mathfrak{g}$ be an ideal and $I^\perp = \{x \in \mathfrak{g} | \beta(I, x) = 0\}$ orthogonal complement of I w.r.t. β, then $I^\perp$ is also an ideal.*

Proof. Take $x \in I^\perp$ and $y, z \in \mathfrak{g}$, then $\beta([x, y], z) = \beta(x, [y, z]) = 0$.
So $[x, y] \in I^\perp$. □

Prop 5.3.2. *Let $\mathfrak{g}$ be a semisimple Lie subalgebra of $\mathfrak{gl}(V)$, then B_V is nondegenerate.*

Proof. Since $B_V : \mathfrak{g}^\perp \times \mathfrak{g}^\perp \to F$ is zero.
By Cartan criterion, $\mathfrak{g}^\perp$ is solvable.
So $\mathfrak{g}^\perp = 0$, *i.e.* B_V is nondegenerate. □

Coro 5.3.1. *Let $\mathfrak{g}$ be a semisimple Lie algebra, then B is nondegenerate.*

Thm 5.3.1 (Cartan criterion)**.** *Let $\mathfrak{g}$ be a Lie algebra, then $\mathfrak{g}$ is semisimple iff $B : \mathfrak{g} \times \mathfrak{g} \to F$ is nondegenerate.*

Proof. $\Leftarrow$: Let I be an abelian ideal of $\mathfrak{g}$.
Then for $x \in I, y \in \mathfrak{g}$, $\mathrm{ad}_x\mathrm{ad}_y \in I, (\mathrm{ad}_x\mathrm{ad}_y)^2 = 0$, *i.e.* $B(x, y) = 0$.
And since B is nondegenerate.
So $I = 0$. □

Lemma 5.3.2. *Let I be an ideal of $\mathfrak{g}$, then Killing form on $\mathfrak{g}$ restricts to the Killing form on I.*

Proof. Take a basis of I and extend it to a basis of $\mathfrak{g}$.
Then for $x \in I$, the representative matrix of ad_x is given by $\begin{bmatrix} A & B \\ 0 & 0 \end{bmatrix}$
So $\mathrm{tr}_{\mathfrak{g}}(\mathrm{ad}_x\mathrm{ad}_y) = \mathrm{tr}_I(\mathrm{ad}_x\mathrm{ad}_y)$. □

Prop 5.3.3. *Let $I \subset \mathfrak{g}$ be a semisimple ideal and $I^\perp$ be the orthogonal complement of I w.r.t. $B_{\mathfrak{g}}$, then $\mathfrak{g} = I \oplus I^\perp$ as vector space.*

Proof. By lemma 5.3.1, $I^\perp$ is an ideal.
And since $B_{\mathfrak{g}}\big|_{I \times I} = B_I$ is nondegenerate.
So $I \cap I^\perp = 0$, *i.e.* $\mathfrak{g} = I \oplus I^\perp$ as vector space. □

Prop 5.3.4. *Let I, J be two ideals of $\mathfrak{g}$, if $\mathfrak{g} = I \oplus J$ as vector space, then $\mathfrak{g} \cong I \times J$ as Lie algebra.*

Proof. For $x \in I, y \in J$, $[x, y] \in I \cap J = 0$. □

Thm 5.3.2. *Let $\mathfrak{g}$ be a semisimple Lie algebra, then $\mathfrak{g}$ has finitely many minimal nonzero ideals, let $I_1, \ldots, I_r$ be all minimal nonzero ideals of $\mathfrak{g}$, then*

(1) $I_1, \ldots, I_r$ are simple ideals.

(2) $\mathfrak{g} = I_1 \oplus \cdots \oplus I_r$ and $\mathfrak{g} \cong I_1 \times \cdots \times I_r$.

(3) Any nonzero ideal of $\mathfrak{g}$ is equal to direct sum of certain I_i so it is semisimple.

(4) Any quotient of $\mathfrak{g}$ be an ideal is still semisimple.

Proof. (1) By definition.

(2) By induction, there is a decomposition $\mathfrak{g} = I_1 \oplus \cdots \oplus I_t$ where $I_1, \ldots, I_t$ are minimal ideals.
Let I be another minimal ideal.
Then $[I, \mathfrak{g}] \subset I$ and $[I, \mathfrak{g}] \neq 0$ otherwise $Z(g) \neq 0$.
So $I = [I, \mathfrak{g}] = [I, I_1] \oplus \cdots \oplus [I, I_t]$ and $[I, I_i] \subset I \cap I_i$.
Hence $I = I_i$, *i.e.* $I_1, \ldots, I_t$ are all the minimal ideals.

(3) Take an ideal I of $\mathfrak{g}$.
Then $\mathfrak{g} = I \oplus I^{\perp}$.
So $I_i = [I_i, \mathfrak{g}] = [I_i, I] \oplus [I_i, I^{\perp}]$, *i.e.* $[I_i, I] = I_i$ or $[I_i, I^{\perp}] = I_i$.
Hence $I_i \subset I$ or $I_i \subset I^{\perp}$.

(4) $\mathfrak{g}/I \cong \prod_{I_i \subset I^{\perp}} I_i$.

□

Def 5.3.2. A representation of Lie algebra $\mathfrak{g}$ is a Lie algebraic morphism $\mathfrak{g} \to \mathfrak{gl}(V)$. We also call V a left $\mathfrak{g}$-module, which satisfies

(1) $(ax + by)v = a(xv) + b(yv)$.

(2) $x(av + bw) = a(xv) + b(xw)$.

(3) $[x, y]v = xyv - yxv$.

For two representations V, W of $\mathfrak{g}$, a morphism $\phi : V \to W$ is a morphism of left $\mathfrak{g}$-module. An irreducible representation of $\mathfrak{g}$ is a nonzero left $\mathfrak{g}$-module without nonzero proper submodule.

Thm 5.3.3 (Weyl)**.** *Let $\mathfrak{g}$ be a semisimple Lie algebra, any nonzero representation of $\mathfrak{g}$ is a direct sum of irreducible submodules.*

Prop 5.3.5. *Let $\mathfrak{g}$ be a semisimple Lie subalgebra of $\mathfrak{gl}(V)$, then for every $x \in \mathfrak{g}$, the semisimple part and nilpotent part of x in $\mathfrak{gl}(V)$ also lie in $\mathfrak{g}$.*

Def 5.3.3. Consider the Jordan decomposition $x = s + n$ in $\mathfrak{gl}(\mathfrak{g})$, then $s, n \in \mathfrak{g}$ so we call such $x = s + n$ the abstract Jordan decomposition of x in $\mathfrak{g}$.

Thm 5.3.4. *Let $\mathfrak{g}$ be a semisimple Lie algebra and $x = s+n$ be the abstract Jordan decomposition of $x \in \mathfrak{g}$, then for any Lie algebra representation $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$, the decomposition $\rho(x) = \rho(s) + \rho(n)$ is the Jordan decomposition of $\rho(x)$ in $\mathfrak{gl}(V)$.*

Proof. We first assume ρ is faithful.
Then by proposition 5.3.5, there exists $x = s' + n'$ such that $\rho(x) = \rho(s') + \rho(n')$ is Jordan decomposition and so $\mathrm{ad}_{s'}$ is semisimple and $\mathrm{ad}_{n'}$ is nilpotent.
Therefore $\mathrm{ad}_x = \mathrm{ad}_{s'} + \mathrm{ad}_{n'}$ is the Jordan decomposition of $\mathrm{ad}_x \in \mathfrak{gl}(\mathfrak{g})$.
Hence $s' = s, n' = n$.
Now for general ρ, consider $\rho \oplus \mathrm{ad} : \mathfrak{g} \hookrightarrow \mathfrak{gl}(V \oplus \mathfrak{g})$.
Then $(\rho \oplus \mathrm{ad})(x) = (\rho \oplus \mathrm{ad})(s) + (\rho \oplus \mathrm{ad})(n)$ is the Jordan decomposition.
So $\rho(x) = \rho(s) + \rho(n)$ is the Jordan decomposition. □

Def 5.3.4. Let $\mathfrak{g}$ be a semisimple Lie algebra and $x \in \mathfrak{g}$, then x is called semisimple element if x equals its semisimple part and x is called nilpotent element if x equals its nilpotent part.

We now assume F is algebraically closed field with character zero.

Lemma 5.3.3. *Let $\mathfrak{g}$ be a semisimple Lie algebra and $\mathfrak{h} \subset \mathfrak{g}$, if any element $x \in \mathfrak{h}$ is a semisimple element in $\mathfrak{g}$, then $\mathfrak{h}$ is abelian.*

Proof. Let $x \in \mathfrak{h}$, suppose $[x, y] = cy$ for some $y \in \mathfrak{h}$ with $c \neq 0$.
Then $\mathrm{ad}_y x = -cy$ and $(\mathrm{ad}_y)^2 x = 0$.
So $\mathrm{ad}_y : \langle x, y\rangle \to \langle x, y\rangle$ is not semisimple.
Hence $\mathrm{ad}_y : \mathfrak{g} \to \mathfrak{g}$ is not semisimple, contradiction! □

Def 5.3.5. Let $\mathfrak{g}$ be a semisimple Lie algebra, a Cartan subalgebra $\mathfrak{h}$ is a maximal subalgebra consisting of only semisimple elements.

Prop 5.3.6. *Notice that* $\{\mathrm{ad}_x | x \in \mathfrak{h}\}$ *can be diagonalized simultaneously, take basis* $(v_1, \ldots, v_n)$ *of* $\mathfrak{g}$ *such that* $\mathrm{ad}_x(v_i) = \lambda_i(x)v_i$. *For* $\lambda : \mathfrak{h} \to F$, *denote* $\mathfrak{g}^\lambda = \{v | \mathrm{ad}_x(v) = \lambda(x)v\}$. *Then*

$$\mathfrak{g} = \bigoplus_{\lambda \in \mathfrak{h}^*} \mathfrak{g}^\lambda, \ \{\lambda \in \mathfrak{h}^* | \mathfrak{g}^\lambda \neq (0)\} = \{\lambda_1, \ldots, \lambda_n\}$$

Proof. Let $\lambda \in \mathfrak{h}^*$ such that $\mathfrak{g}^\lambda \neq (0)$ and $v = \sum a_i v_i \in \mathfrak{g}^\lambda$.
Then $\lambda(x)v = \mathrm{ad}_x(v) = \sum a_i \lambda_i(x) v_i$.
So $a_i(\lambda_i(x) - \lambda(x)) = 0$ for all $x \in \mathfrak{g}$.
Hence $\lambda \in \{\lambda_1, \ldots, \lambda_n\}$ and $\mathfrak{g}^\lambda = \mathrm{span}\{v_i | \lambda_i = \lambda\}$. □

Def 5.3.6. Let $\mathfrak{g}$ be a semisimple Lie algebra and $\mathfrak{h} \subset \mathfrak{g}$ be a Cartan subalgebra, denote by $R = \{\lambda \in \mathfrak{h}^* | \lambda \neq 0, \mathfrak{g}^\lambda \neq (0)\}$, then the Cartan decomposition is

$$\mathfrak{g} = \mathfrak{g}^0 \oplus \left(\bigoplus_{\lambda \in R} \mathfrak{g}^\lambda \right)$$

Prop 5.3.7. *Take* $\alpha, \beta \in \mathfrak{h}^*$,

(1) $[\mathfrak{g}^\alpha, \mathfrak{g}^\beta] \subset \mathfrak{g}^{\alpha+\beta}$.

(2) If $x \in \mathfrak{g}^\alpha$, *then* $\mathrm{ad}_x : \mathfrak{g} \to \mathfrak{g}$ *is nilpotent.*

(3) If $\alpha + \beta \neq 0$, *then* $B_\mathfrak{g}(\mathfrak{g}^\alpha, \mathfrak{g}^\beta) = 0$.

Proof. (1) Take $x \in \mathfrak{g}^\alpha, y \in \mathfrak{g}^\beta$ and $z \in \mathfrak{h}$.
Then $\mathrm{ad}_z([x, y]) = [z, [x, y]] = [x, [z, y]] + [[z, x], y] = \beta(z)[x, y] + \alpha(z)[x, y]$.

(2) R is a finite set.
Then $(\mathrm{ad}_x)^k \mathfrak{g}^\beta \subset \mathfrak{g}^{k\alpha+\beta} = 0$ for sufficiently large k.

(3) For $x \in \mathfrak{g}^\alpha, y \in \mathfrak{g}^\beta$ and $\gamma \in R$, $\mathrm{ad}_x \mathrm{ad}_y \mathfrak{g}^\gamma \subset \mathfrak{g}^{\gamma+\alpha+\beta} \neq \mathfrak{g}^\gamma$.
So $B_\mathfrak{g}(\mathfrak{g}^\alpha, \mathfrak{g}^\beta) = 0$.

□

Prop 5.3.8. *Let* $\mathfrak{h}$ *be a Cartan subalgebra,* $\mathfrak{h} = \mathfrak{g}^0$.

Prop 5.3.9. *For* $\alpha \in \mathfrak{h}^*$, $B_\mathfrak{g} : \mathfrak{g}^\alpha \times \mathfrak{g}^{-\alpha} \to F$ *is nondegenerate. In particular,* $R = -R$.

Proof. For $x \in \mathfrak{g}^\alpha$, $B_\mathfrak{g}(x, \mathfrak{g}^\beta) = 0$ for all $\beta \neq -\alpha$.
So $B_\mathfrak{g}(x, \mathfrak{g}^{-\alpha}) \neq 0$. □

Prop 5.3.10. $\mathfrak{h}^* = \mathrm{span}_F(R)$.

Proof. Suppose there exists $x \in \mathfrak{h}$ such that $\alpha(x) = 0$ for all R.
Then $\mathrm{ad}_x(v) = \alpha(x)v = 0$ for all $v \in \mathfrak{g}^\alpha$.
So $[x, \mathfrak{g}] = 0$, contradiction! □

Def 5.3.7. For $\lambda \in \mathfrak{h}^*$, let $t_\lambda \in \mathfrak{h}$ be the unique element such that $\lambda = B(t_\lambda, \cdot)$.

Prop 5.3.11. *Take $\alpha \in R$,*

(1) For $x \in \mathfrak{g}^\alpha, y \in \mathfrak{g}^{-\alpha}$, $[x,y] = B(x,y)t_\alpha$.

(2) $[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}] = Ft_\alpha$.

(3) $\alpha(t_\alpha) = B(t_\alpha, t_\alpha) \neq 0$.

Proof. (1) For $z \in \mathfrak{h}$, $B(z,[x,y]) = B([z,x],y) = B(\alpha(z)x, y) = B(t_\lambda, z)B(x,y)$.
So $B(\mathfrak{h}, [x,y] - B(x,y)t_\lambda) = 0$.

(2) Since $B : \mathfrak{g}^\alpha \times \mathfrak{g}^{-\alpha} \to F$ is nondegenerate.
So by (1), $[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}] = Ft_\alpha$.

(3) Suppose $\alpha(t_\alpha) = 0$, take $x \in \mathfrak{g}^\alpha, y \in \mathfrak{g}^{-\alpha}$ such that $B(x,y) = 1$.
Then $[x,y] = t_\alpha, [t_\alpha, x] = \alpha(t_\alpha)x = 0$ and $[t_\alpha, y] = 0$.
Consider $S = \mathrm{span}\{x, y, t_\alpha\}$, which is a solvable subalgebra of $\mathfrak{g}$.
By Lie theorem, $\mathrm{ad}_S \subset \mathfrak{gl}(\mathfrak{g})$ consists of upper triangular matrices under some basis of $\mathfrak{g}$.
So $\mathrm{ad}_{t_\alpha} : \mathfrak{g} \to \mathfrak{g}$ is nilpotent.
But $t_\alpha \in \mathfrak{h}$ is semisimple, contradiction!

□

Prop 5.3.12. *Take $\alpha \in \mathfrak{h}^*, x \in \mathfrak{g}^\alpha$, there exists $y \in \mathfrak{g}^{-\alpha}$ such that* $\mathrm{span}\{x, y, [x,y]\} \cong \mathfrak{sl}_2(F)$ *with*

$$x \mapsto \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},\ y \mapsto \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},\ [x,y] \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

In particular, $[x,y] = \frac{2t_\alpha}{B(t_\alpha, t_\alpha)}$.

Proof. Take $y \in \mathfrak{g}^{-\alpha}$ such that $B(x,y) = \frac{2}{B(t_\alpha, t_\alpha)}$.
Then $[x,y] = B(x,y)t_\alpha = \frac{2t_\alpha}{B(t_\alpha,t_\alpha)}, [x,[x,y]] = \frac{2}{B(t_\alpha,t_\alpha)}\alpha(t_\alpha)x = 2x, [y,[x,y]] = -2y$.
So $\mathrm{span}\{x,y,[x,y]\} \cong \mathfrak{sl}_2(F)$. □

Def 5.3.8. Fro $\alpha \in R$, we denote $h_\alpha = \frac{2t_\alpha}{B(t_\alpha,t_\alpha)}$ and we call such (x, y, h_α) an $\mathfrak{sl}_2$ triple.

5.4 Representation theory of $\mathfrak{sl}_2(F)$

Def 5.4.1. Let $\mathfrak{g} = \mathfrak{sl}_2(F), x = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right], y = \left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right], h = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ and V be a representation of $\mathfrak{g}$. Notice that $h : V \to V$ is semisimple, $V = \bigoplus_{\lambda \in F} V_\lambda$ with $V_\lambda = \{v \in V | hv = \lambda v\}$. If $V_\lambda \neq 0$, we call λ a weight of $\mathfrak{h}$ in V and call V_λ a weight space.

Lemma 5.4.1. *Let $v \in V_\lambda$, then $xv \in V_{\lambda+2}, yv \in V_{\lambda-2}$.*

Proof. $hxv = [h,x]v + xhv = 2xv + \lambda xv = (\lambda + 2)xv$. □

Def 5.4.2. Let $\lambda \in F$ such that $V_\lambda(0)$ and $v \in V_\lambda$, if $xv = 0$, then we call v a maximal vector of weight λ.

Lemma 5.4.2. *Let $v_0 \in V_\lambda$ be a maximal vector, take $v_i = \frac{1}{i!}y^i v_0$, then*

$$hv_i = (\lambda - 2i)v_i, yv_i = (i+1)v_{i+1}, xv_i = (\lambda - i + 1)v_{i-1}.$$

Proof. Since $v_i \in V_{\lambda-2i}$.

So $hv_i = (\lambda - 2i)v_i, yv_i = (i+1)v_{i+1}$ and

$$\begin{aligned} xv_i &= \frac{1}{i}xyv_{i-1} = \frac{1}{i}([x,y]v_{i-1} + yxv_{i-1}) \\ &= \frac{1}{i}\left(hv_{i-1} + (\lambda - i + 2)yv_{i-2}\right) \\ &= \frac{1}{i}\left((\lambda - 2i + 2)v_{i-1} + (\lambda - i + 2)(i-1)v_{i-1}\right) \\ &= (\lambda - i + 1)v_{i-1} \end{aligned}$$

□

Thm 5.4.1. *Let V be an irreducible $\mathfrak{sl}_2(F)$-module, then*

(1) $V = \bigoplus V_\mu$ with $\mu = m, m-2, \ldots, 2-m, -m$ where $m+1 = \dim V$ and $\dim V_\mu = 1$.

(2) V has a unique maximal vector up to scalar, where weight is m called highest weight of V

(3) There exists exactly one irreducible $\mathfrak{sl}_2(F)$-module up to isomorphism for each dimension $m+1$.

Proof. Take a maximal vector $v_0 \in V_\lambda$ and m such that $v_m \neq 0$ and $v_{m+1} = 0$.

Then $xv_{m+1} = (\lambda - m)v_m$, *i.e.* $\lambda = m$ is an integer.

And $\operatorname{span}\{v_0, \ldots, v_m\} \subset V$ is an $\mathfrak{sl}_2(F)$-submodule, *i.e.* $V = \operatorname{span}\{v_0, \ldots, v_m\}$.

This proves (1)(2).

For (3), the uniqueness follows from the lemma.

And for existence, consider $\mathfrak{sl}_2(F) = \mathfrak{sl}_{m+1}(F)$ with

$$h \mapsto \begin{bmatrix} m & & & \\ & m-2 & & \\ & & \ddots & \\ & & & -m \end{bmatrix}, \; x \mapsto \begin{bmatrix} 0 & m & & & \\ & 0 & m-1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{bmatrix}, \; y \mapsto \begin{bmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 2 & \ddots & & \\ & & \ddots & 0 & \\ & & & m & 0 \end{bmatrix}$$

□

Coro 5.4.1. *Let V be any $\mathfrak{sl}_2(F)$-module, then the eigenvalue of $\mathfrak{h} : V \to V$ are all integers and multiplicities of n and $-n$ equal.*

Coro 5.4.2. *Let V be any $\mathfrak{sl}_2(F)$-module, then in any decomposition of V into direct sum of irreducible $\mathfrak{sl}_2(F)$-module, the number of summands is* $\dim V_0 + \dim V_1$.

Prop 5.4.1. *Let $\mathfrak{g}$ be a Lie algebra and V be a $\mathfrak{g}$-module, TFAE:*

(1) V is completely reducible.

(2) V is the sum of irreducible submodules.

(3) For all submodule $W \subset V$, there exists submodule W' of V, such that $V = W \oplus W'$.

Proof. (1) $\Rightarrow$ (2) and (3) $\Rightarrow$ (1) are trivial.

(2) $\Rightarrow$ (3): Suppose k is the maximal number where there exists irreducible submodule $W_1, \ldots, W_k$ such that $W \oplus W_1 \oplus \cdots \oplus W_k \subset V$.

If $W \oplus W_1 \oplus \cdots \oplus W_k = V$, we are done.

Otherwise, take irreducible submodule U of V such that $U \nsubseteq W \oplus W_1 \oplus \cdots \oplus W_k$.

So $U \cap (W \oplus W_1 \oplus \cdots \oplus W_k) = 0$.

Hence $W \oplus W_1 \oplus \cdots \oplus W_k \oplus U \subset V$, contradict with the maximality of k. □

Prop 5.4.2. *Take $\alpha \in R$,*

(1) $\dim \mathfrak{g}^\alpha = 1$.

(2) $R \cap F\alpha = \{\pm\alpha\}$

Proof. Let $M_\alpha = \sum_{c\in F} \mathfrak{g}^{c\alpha}, x \in \mathfrak{g}^\alpha$ and $y \in \mathfrak{g}^{-\alpha}$ such that $[x, y] = h_\alpha$.
Consider $S = \text{span}\{x, y, h_\alpha\}$.
Then $\mathfrak{g}$ is a S-module and M_α is an S-submodule of $\mathfrak{g}$.
For $x \in \mathfrak{g}^{c\alpha}$, $[h_\alpha, x] = 2cx$.
So $2c$ is weight for elements in $\mathfrak{g}^{c\alpha}$ w.r.t. h_α, *i.e.* $c \in \frac{1}{2}\mathbb{Z}$ if $\mathfrak{g}^{c\alpha} \neq 0$.
For any $z \in \ker(\alpha) \subset \mathfrak{h}$ and $x \in \mathfrak{g}^\alpha$, $[z, x] = \alpha(z)x = 0, [z, y] = 0, [z, h_\alpha] = 0$.
Therefore the adjoint action of S on $\ker(\alpha)$ is zero.
Notice that $\ker(\alpha)$ and S are S-submodules of M_α, which gives all weight 0 in M_α.
Thus the only even weights occuring in M_α are $0, \pm 2$, *i.e.* 2α is not in R.
Moreover, $\frac{1}{2}\alpha$ is not in R, *i.e.* 1 cannot appear as a weight for h_α.
Hence $M_\alpha = \ker(\alpha) \oplus S$. □

Def 5.4.3. Let $\mathfrak{g}$ be a semisimple Lie algebra and $\mathfrak{h} \subset \mathfrak{g}$ be a Cartan algebra, then $\alpha \in R$ is called the root in $\mathfrak{h}^*$.

Prop 5.4.3. *Take $\alpha, \beta \in R$,*

(1) $\beta(h_\alpha) \in \mathbb{Z}$ *and* $\beta - \beta(h_\alpha)\alpha \in R$.

(2) If $\beta \neq \pm\alpha$, let r, q be largest integers for which $\beta - r\alpha, \beta + q\alpha$ are roots, then all $\beta + i\alpha \in R$ for $-r \leqslant i \leqslant q$ and $\beta(h_\alpha) = r - q$

(3) $\mathfrak{g}$ *is generated by* $\mathfrak{g}^\alpha$ *as Lie algebra.*

Proof. (1) If $\beta = \pm\alpha$, then $\beta(h_\alpha) = \pm 2$ and $\beta - \beta(h_\alpha)\alpha = -\beta \in R$.
Now assume $\beta \notin F\alpha$, consider $K = \sum \mathfrak{g}^{\beta+i\alpha}$.
Then K is an S_α-module and the weight for elements of $\mathfrak{g}^{\beta+i\alpha}$ w.r.t. h_α is $\beta(h_\alpha) + 2i$.
So $\beta - \beta(h_\alpha)\alpha \in R$ and $\beta(h_\alpha) \in \mathbb{Z}$.

(2) There exists r, q such that $\beta + i\alpha$ with $-r \leqslant i \leqslant q$ are all roots of this form.
So $\beta(h_\alpha) - 2r, \beta(h_\alpha) + 2q$ are the lowest and highest weights.
Hence $(\beta(h_\alpha) - 2r) + (\beta(h_\alpha) + 2q) = 0$, *i.e.* $\beta(h_\alpha) = r - q$.

(3) $[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}] = Fh_\alpha = Ft_\alpha$.
And since R generates $\mathfrak{h}^*$.
So $\{t_\alpha\}$ generates $\mathfrak{h}$.

□

Def 5.4.4. For $\lambda, \mu \in \mathfrak{h}^*$, we define $(\lambda, \mu) = B(t_\lambda, t_\mu) = \lambda(t_\mu)$.

Prop 5.4.4. *(1)* $E_\mathbb{Q} = \text{span}_\mathbb{Q} R$ *is a $\mathbb{Q}$-structure of* $\mathfrak{h}^*$, i.e. $(\text{span}_\mathbb{Q} R) \otimes_\mathbb{Q} F \cong \mathfrak{h}^*$.

(2) $(\cdot, \cdot) : E_\mathbb{Q} \times E_\mathbb{Q} \to \mathbb{Q} \subset F$ *is positive definite.*

Proof. (1) Since $\mathrm{span}_F R = \mathfrak{h}^*$, we only need to prove $\dim_{\mathbb{Q}} \mathrm{span}_{\mathbb{Q}} R = \dim \mathfrak{h}^*$.

Take a subset $\{\alpha_1, \dots, \alpha_l\} \subset R$ which is an F-basis for $\mathfrak{h}^*$.

We only need to show for $\beta = \sum c_i \alpha_i \in R$, $c_i \in \mathbb{Q}$.

Since $(\beta, \alpha_j) = \sum c_i (\alpha_i, \alpha_j)$ and $[(\alpha_i, \alpha_j)]_{i,j}$ is nondegenerate.

So $\frac{2(\beta,\alpha_j)}{(\alpha_j,\alpha_j)} = \sum \frac{2(\alpha_i,\alpha_j)}{(\alpha_j,\alpha_j)} c_i$ has nontrivial solution.

And notice that for $\alpha, \beta \in R$ $\frac{2(\alpha,\beta)}{(\beta,\beta)} = \frac{2\alpha(t_\beta)}{B(t_\beta,\beta)} = \alpha(h_\beta) \in \mathbb{Z}$.

Hence $c_i \in \mathbb{Q}$.

(2) For $x, y \in \mathfrak{h}, z \in \mathfrak{g}^\alpha$, $\mathrm{ad}_x \mathrm{ad}_y z = \alpha(x)\alpha(y)z$.

So $B(x, y) = \mathrm{tr}(\mathrm{ad}_x \mathrm{ad}_y) = \sum_{\alpha \in R} \alpha(x)\alpha(y)$.

For $\lambda, \mu \in \mathfrak{h}^*$, $(\lambda, \mu) = \sum \alpha(t_\lambda)\alpha(t_\mu) = \sum (\alpha, \lambda)(\alpha, \mu)$.

Therefore for $\beta \in R$, $(\beta, \beta) = \sum (\alpha, \beta)^2$, *i.e.* $\frac{1}{(\beta,\beta)} = \sum \frac{(\alpha,\beta)^2}{(\beta,\beta)^2} \in \mathbb{Q}$.

Hence $(\alpha, \beta) \in \mathbb{Q}$, *i.e.* $(\lambda, \lambda) = \sum (\alpha, \lambda)^2 > 0$ for any $\gamma \in \mathfrak{h}^*$.

□

Thm 5.4.2. *Let $\mathfrak{g}$ be a semisimple Lie algebra and $\mathfrak{h}$ be a Cartan subalgebra, then $(\mathfrak{g}, \mathfrak{h})$ gives a pair $(R, E_{\mathbb{Q}})$ with positive definite bilinear map $E_{\mathbb{Q}} \times E_{\mathbb{Q}} \to \mathbb{Q}$ such that*

(1) $\mathrm{span}_{\mathbb{R}} R = E_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R}$.

(2) $\mathbb{R}\alpha \cap R = \{\pm\alpha\}$.

(3) If $\alpha, \beta \in R$, then $\beta - \frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha \in R$.

(4) For any α, β, $\frac{2(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$.

5.5 Root system and Dynkin diagram

We now let F be a character zero field.

Def 5.5.1. Let V be a vector space, a reflection of V with vector $\alpha \neq 0$ is an involution $V \to V$ sending α to $-\alpha$ and fixing a hyperplane, which is the kernel of $\alpha^\vee : V \to F$ and $\alpha^\vee(\alpha) = 2$. We denote the reflection by $s_{\alpha,\alpha^\vee} : V \to V, x \mapsto x - \alpha^\vee(x)\alpha$.

Lemma 5.5.1. *Let R be a finite set spanning V, for any $\alpha \in V$, there exists at most one reflection s with vector α, such that $s(R) \subset R$.*

Proof. Suppose there are two such reflections s, s', let $t = ss'$.

Then t acts as identity on $F\alpha$ and $V/F\alpha$.

So $(t-1)V \subset F\alpha$ and $(t-1)^2 V = 0$.

And since R is finite.

Therefore there exists $m \in \mathbb{Z}^+$ such that $t^m : R \to R$ is identity.

Hence $t^m - 1 = 0$, *i.e.* t is identity. □

Def 5.5.2. A subset R of V/F is called a root system if

(1) R is finite, $0 \notin R$ and $\mathrm{span}_F R = V$.

(2) For all $\alpha \in R$, there exists unique $\alpha^\vee : V \to F$ such that $\alpha^\vee(\alpha) = 2$ and $s_{\alpha,\alpha^\vee}(R) \subset R$.

(3) For all $\alpha, \beta \in R$, $s_\alpha(\beta) - \beta$ is an integral multiple of α.

We call α root, $\alpha^\vee$ coroots and $\dim V$ rank of R. Moreover, (V, R) is called reduced if for every $\alpha \in R$, $R \cap F\alpha = \{\pm\alpha\}$.

Exam 5.5.1. *Consider $\mathfrak{g} = \mathfrak{sl}_{n+1}(F)$ and $\mathfrak{h}$ consisting of all diagonal matrices in $\mathfrak{g}$.*
Then $\mathfrak{h}$ is a Cartan subalgebra.
Let $e^i \in \mathfrak{h}^*$ such that $e^i(A) = a_{ii}$.
So $R = \{\alpha_{ij} = e^i - e^j | i \neq j\}$ and $h_{\alpha_{ij}} = e_{ii} - e_{jj}$.
Therefore $s_{\alpha_{ij}} : \mathfrak{h}^* \to \mathfrak{h}^*, x \mapsto x - x(h_{\alpha_{ij}})\alpha_{ij}$ exchanging the i, j-th coordinates.
Hence $(\mathfrak{h}^*, R)$ is a reduced root system, called of type A_n.

Def 5.5.3. The automorphism group of root system R is $A(R) = \{g \in \mathrm{GL}(V) | g(R) = R\}$ and the Weyl group of R is $W(R) = \langle s_{\alpha,\alpha^\vee} | \alpha \in R\rangle$.

Lemma 5.5.2. *Let (V, R) be a root system and $(\cdot|\cdot) : V \times V \to F$ be a nondegenerate symmetric bilinear form invariant under $W(R)$, then any $\alpha \in R$ satisfies $(\alpha|\alpha) \neq 0$ and $\alpha^\vee = \left(\frac{2\alpha}{(\alpha|\alpha)}\middle|\cdot\right)$.*

Proof. Take $\alpha \in R$ and $x \in \ker \alpha^\vee$.
Then $s_\alpha(\alpha) = -\alpha, s_\alpha(x) = x - \alpha^\vee(x)\alpha = x$.
So $(\alpha|x) = (-\alpha|x) = 0$.
And since the reflection $x \mapsto x - \frac{2(\alpha|x)}{(\alpha|\alpha)}\alpha$ fixes $\ker(\alpha|\cdot) = \ker \alpha^\vee$ and maps α to $-\alpha$.
Hence $x - \frac{2(\alpha|x)}{(\alpha|\alpha)}\alpha = s_\alpha(x)$, *i.e.* $\alpha^\vee = \left(\frac{2\alpha}{(\alpha|\alpha)}\middle|\cdot\right)$. □

Prop 5.5.1. *Let $\mathfrak{g}$ be a semisimple Lie algebra and $\mathfrak{h}$ be a Cartan subalgebra, then $(\cdot, \cdot)$ is invariant under $W(R)$.*

Proof. Take $\alpha \in R$ and $\lambda, \mu \in \mathfrak{h}^*$, $s_\alpha(\lambda) = \lambda - \lambda(h_\alpha)\alpha$ and so

$$\begin{aligned}(s_\alpha(\lambda), s_\alpha(\mu)) - (\lambda, \mu) &= (\lambda - \lambda(h_\alpha)\alpha, \mu - \mu(h_\alpha)\alpha) - (\lambda, \mu)\\ &= -\lambda(h_\alpha)(\alpha, \mu) - \mu(h_\alpha)(\lambda, \alpha) + \lambda(h_\alpha)\mu(h_\alpha)(\alpha, \alpha)\\ &= -\lambda(h_\alpha)\mu(t_\alpha) - \mu(h_\alpha)\lambda(t_\alpha) + 2\lambda(h_\alpha)\mu(t_\alpha) = 0\end{aligned}$$

□

Lemma 5.5.3. *Let F' be an extension of F and (V, R) be a root system over F, then $(V_{F'}, R)$ is a root system over F'.*

Prop 5.5.2. *Let (V, R) be a root system and $V_\mathbb{Q} = \mathrm{span}_\mathbb{Q} R \subset V$, then*

(1) $V_\mathbb{Q}$ is a $\mathbb{Q}$-structure on V

(2) $R \subset V_\mathbb{Q}$ is a root system over $\mathbb{Q}$.

Now we only consider real root systems, and assume $(\cdot|\cdot)$ is a $W(R)$-invariant inner product.

Def 5.5.4. $\langle\beta, \alpha\rangle = \frac{2(\alpha|\beta)}{(\alpha|\alpha)} = \alpha^\vee(\beta)$.

Lemma 5.5.4. *Take $\alpha, \beta \in R$ and $\sigma \in A(R)$,*

(1) $\sigma s_\alpha \sigma^{-1} = s_{\sigma(\alpha)}$.

(2) $\langle\beta, \alpha\rangle = \langle\sigma(\beta), \sigma(\alpha)\rangle$.

Proof. (1) $\sigma s_\alpha \sigma^{-1}(x) = \sigma\left(\sigma^{-1}(x) - \alpha^\vee(\sigma^{-1}(x))\alpha\right) = x - (\sigma(\alpha))^\vee(x)\sigma(\alpha)$.
The last equality holds since $\alpha^\vee(\sigma^{-1}(\sigma(\alpha))) = 2$ and $\alpha^\vee(\sigma^{-1}(R)) = R$.

(2) By (1), $\langle\beta,\alpha\rangle = \alpha^\vee(\beta) = (\sigma\alpha)^\vee(\sigma\beta) = \langle\sigma(\beta),\sigma(\alpha)\rangle$.

□

Coro 5.5.1. *$W(R)$ is a normal subgroup of $A(R)$.*

Prop 5.5.3. *$R^\vee = \{\alpha^\vee | \alpha \in R\} \subset V^*$ is also a root system, with $s_{\alpha^\vee}(\lambda) = \lambda - \lambda(\alpha)\alpha^\vee$.*
We call $(V^*, R^\vee)$ the dual root system of R.

Remark 5.5.1. Consider $R' = \left\{ \frac{2\alpha}{(\alpha|\alpha)} \middle| \alpha \in R \right\} \subset V$, then (V, R') is also a root system and it is isomorphic to $(V^*, R^\vee)$ via $x \leftrightarrow (x|\cdot)$.

Def 5.5.5. Let (V, R) be a reduced root system, for $\alpha, \beta \in R$, write $\theta(\alpha,\beta) \in [0,\pi]$ such that $\cos\theta = \frac{(\alpha|\beta)}{\sqrt{(\alpha|\alpha)(\beta|\beta)}}$.

Prop 5.5.4. *For any $\alpha, \beta \in R$, $\theta(\alpha,\beta) \in \left\{0, \frac{\pi}{6}, \frac{\pi}{4}, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \frac{3\pi}{4}, \frac{5\pi}{6}, \pi\right\}$.*

Proof. $4\cos^\theta = \langle\alpha,\beta\rangle\langle\beta,\alpha\rangle \in \mathbb{Z}$.
When $4\cos^2\theta = 4$, $\beta = \pm\alpha$.
When $4\cos^2\theta = 0$, $\theta = \frac{\pi}{2}$ and $(\alpha|\beta) = \langle\alpha,\beta\rangle = \langle\beta,\alpha\rangle = 0$.
When $4\cos^2\theta = 1$, $\theta = \frac{\pi}{3}$ or $\frac{2\pi}{3}$, $(\alpha|\alpha) = (\beta|\beta)$ and $\langle\alpha,\beta\rangle = \langle\beta,\alpha\rangle = \pm 1$.
When $4\cos^2\theta = 2$, $\theta = \frac{\pi}{4}$ or $\frac{3\pi}{4}$, $\frac{(\beta|\beta)}{(\alpha|\alpha)} = 2$ or $\frac{1}{2}$ and $\{\langle\alpha,\beta\rangle, \langle\beta,\alpha\rangle\} = \pm\{1,2\}$.
When $4\cos^2\theta = 3$, $\theta = \frac{\pi}{6}$ or $\frac{5\pi}{6}$, $\frac{(\beta|\beta)}{(\alpha|\alpha)} = 3$ or $\frac{1}{3}$ and $\{\langle\lambda,\beta\rangle, \langle\beta,\alpha\rangle\} = \pm\{1,3\}$. □

Lemma 5.5.5. *Let $\alpha, \beta \in R$ with $\beta \notin F\alpha$, if $(\alpha|\beta) > 0$, then $\alpha - \beta \in R$; if $(\alpha|\beta) < 0$, then $\alpha + \beta \in R$.*

Proof. If $(\alpha|\beta) > 0$, then one of $\langle\alpha,\beta\rangle, \langle\beta,\alpha\rangle$ is 1.
WLOG, assume $\langle\beta,\alpha\rangle = 1$.
So $s_\alpha(\beta) = \beta - \alpha^\vee(\beta)\alpha = \beta - \alpha$. □

Prop 5.5.5. *Let $\alpha, \beta \in R$ with $\beta \notin F\alpha$ and r, q be the largest integers such that $\beta - r\alpha, \beta + q\alpha \in R$, then all $\beta + i\alpha \in R$ for $-r \leqslant i \leqslant q$ and $\langle\beta,\alpha\rangle = r - q$.*

Proof. Suppose $\beta + p\alpha \in R, \beta + (p+1)\alpha \notin R, \beta + (s-1)\alpha \notin R, \beta + s\alpha \in R$ and $-i \leqslant p < s \leqslant r$.
Then $\langle\alpha, \beta + p\alpha\rangle > 0, \langle\alpha, \beta + s\alpha\rangle < 0$.
So $(\alpha|\beta + p\alpha) \geqslant 0 \geqslant (\alpha|\beta + s\alpha)$, contradiction!
And since $s_\alpha(\beta + i\alpha) = \beta + i\alpha - \alpha^\vee(\beta + i\alpha)\alpha = \beta - i\alpha - \langle\beta,\alpha\rangle\alpha$.
So $q + \langle\beta,\alpha\rangle = r$, *i.e.* $\langle\beta,\alpha\rangle = r - q$. □

Coro 5.5.2. *Each string $\beta - r\alpha, \ldots, \beta + q\alpha$ has at most 4 vectors.*

Def 5.5.6. Let (V, R) be a root system, a subset $\Delta \subset R$ is called a base if

(1) Δ is a basis of V

(2) Each $\beta \in R$ can be written as $\beta = \sum_{\alpha\in\Delta} k_\alpha\alpha$ such that all $k_\alpha \geqslant 0$ or all $k_\alpha \leqslant 0$.

Fix a base, $\alpha \in \Delta$ is called simple root and $\sum k_\alpha$ is called the height of β, denoted by $\mathrm{ht}(\beta)$. If all $k_\alpha \geqslant 0$, then we call β positive, denoted by $\beta > 0$ and let $R^+ = \{\beta \in R | \beta > 0\}$ (and similar for $k_\alpha \leqslant 0$ case). Moreover, for $\lambda, \mu \in V$, we say $\lambda < \mu$ if $\mu - \lambda > 0$.

Lemma 5.5.6. *If Δ is a base, then $(\alpha|\beta) \leqslant 0$ for all $\alpha \neq \beta$ in Δ and $\alpha - \beta$ is not a root.*

Def 5.5.7. For $\gamma \in V$, define $R^+(\gamma) = \{\alpha \in R | \alpha^\vee(\gamma) > 0\}$. We call γ regular if $\gamma \notin \bigcup \ker\alpha^\vee$ and call γ singular otherwise. $\alpha \in R^+(\gamma)$ is called decomposable if $\alpha = \beta_1 + \beta_2$ for some $\beta_1, \beta_2 \in R^+(\gamma)$ and α is called indecomposable otherwise.

Thm 5.5.1. *Let $\gamma \in V$ be regular, then the set $\Delta(\gamma)$ of all indecomposable roots in $R^+(\gamma)$ is a base of R and every base of R is obtainable in this way.*

Proof. Suppose $\alpha \in R^+(\gamma)$ is not a $\mathbb{N}$-combination of $\Delta(\gamma)$ and $(\gamma|\alpha)$ is minimal.
Then $\alpha = \beta_1 + \beta_2$ for some $\beta_1, \beta_2 \in R^+(\gamma)$.
So $(\gamma|\beta_i) < (\gamma|\alpha)$ and β_1, β_2 are not $\mathbb{N}$-combinations of $\Delta(\gamma)$, contradiction!
For $\alpha \neq \beta \in \Delta(\gamma)$, suppose $(\alpha|\beta) > 0$.
Then $\alpha - \beta, \beta - \alpha \in R$.
WLOG, assume $\alpha - \beta \in R^+(\gamma)$, then $\alpha = (\alpha - \beta) + \beta$, contradiction!
Suppose $\sum s_\alpha \alpha = \sum t_\beta \beta$ with $s_\alpha, t_\beta \geqslant 0$.
Then $(\sum s_\alpha \alpha | \sum t_\beta \beta) = \sum s_\alpha t_\beta (\alpha|\beta) \leqslant 0$.
So $\sum s_\alpha \alpha = \sum t_\beta \beta = 0$, *i.e.* $0 = (\sum s_\alpha \alpha | \gamma) = \sum s_\alpha (\alpha|\gamma)$.
Thus $s_\alpha = t_\beta = 0$, contradiction!
Hence $\Delta(\gamma)$ is a base. □

Def 5.5.8. The connected components of $V \setminus \bigcup \ker \alpha^\vee$ are called Weyl chambers. Each regular $\gamma \in V$ belongs to a unique Weyl chamber denoted by $C(\gamma)$.

Prop 5.5.6. *The Weyl chambers and the bases have a one-to-one correspondence $C(\gamma) \leftrightarrow \Delta(\gamma)$.*

Proof. Suppose $\gamma, \gamma' \in V$ are regular with $\Delta(\gamma) = \Delta(\gamma')$.
Then $R^+(\gamma) = R^+(\gamma')$ and $R^-(\gamma) = R^-(\gamma')$.
So $(\gamma|\alpha)$ and $(\gamma'|\alpha)$ have same sign for any $\alpha \in R$.
Hence γ, γ' are in one Weyl chamber. □

Def 5.5.9. For $\Delta = \Delta(\gamma)$, we also write $c(\Delta) = c(\gamma)$, called the fundamental Weyl chamber relative to Δ. Explicitly,

$$C(\Delta) = \{\gamma \in V | (\gamma|\alpha) > 0 \text{ for all } \alpha \in \Delta\}$$

Prop 5.5.7. *Let $\gamma \in V$ be regular and $\sigma \in W(R)$, then $\sigma C(\gamma) = C(\sigma(\gamma)), \sigma\Delta(\gamma) = \Delta(\sigma(\gamma))$.*

Proof. Since $\sigma(Cr)$ is a connected component of $V \setminus \bigcup \ker \alpha^\vee$ and $\sigma\gamma \in \sigma C(\gamma)$.
So $\sigma C(\gamma) = C(\sigma(\gamma))$.
On the other hand, for $\alpha \in R^+(\gamma)$, $(\sigma(\gamma)|\sigma(\alpha)) = (\gamma|\alpha) > 0$, *i.e.* $\sigma(\alpha) \in R^+(\sigma(\gamma))$.
Hence $\sigma(R^+(\gamma)) = R^+(\sigma(\gamma))$ and $\sigma\Delta(\gamma) = \Delta(\sigma(\gamma))$. □

Lemma 5.5.7. *Let $\alpha \in \Delta$, then s_α permutes $R^+ \setminus \{a\}$.*

Proof. Let $\beta = \sum k_\gamma \gamma$ with $k_\gamma \in \mathbb{N}$.
Then there exists $\gamma \neq \alpha$ such that $k_\gamma > 0$.
So $s_\alpha(\beta) = \beta - \alpha^\vee(\beta)\alpha$ whose coefficient of γ is still $k_\gamma > 0$, *i.e.* $s_\alpha(\beta) \in R^+$. □

Coro 5.5.3. *Let $\delta = \frac{1}{2}\sum_{\beta \in R^+} \beta$, then for all $\alpha \in \Delta$, $s_\alpha(\delta) = \delta - \alpha$.*

Lemma 5.5.8. *Let $\alpha_1, \ldots, \alpha_t \in \Delta$ and write $\sigma_i = s_{\alpha_i}$, if $\sigma_1 \cdots \sigma_{t-1}(\alpha_t) \in R^-$, then there exists $1 \leqslant s < t$ such that $\sigma_1 \cdots \sigma_t = \sigma_1 \cdots \sigma_{s-1}\sigma_{s+1} \ldots \sigma_{t-1}$.*

Proof. Since $\sigma_1 \cdots \sigma_{t-1}(\alpha_t) < 0$ and $\alpha_t > 0$.
So there exists $s < t$ such that $\sigma_s \cdots \sigma_{t-1}(\alpha_t) < 0$ and $\sigma_{s+1} \cdots \sigma_{t-1}(\alpha_t) > 0$.
By lemma, $\sigma_{s+1} \cdots \sigma_{t-1}(\alpha_t) = \alpha_s$.
Hence $\sigma_s = s_{\sigma_{s+1} \cdots \sigma_{t-1}(\alpha_t)} = (\sigma_{s+1} \cdots \sigma_{t-1})\sigma_t(\sigma_{s+1} \cdots \sigma_{t-1})^{-1}$. □

Coro 5.5.4. *If $\sigma = \sigma_1 \ldots \sigma_t \in W(R)$ with $\sigma_i = s_{\alpha_i}$ reflection in simple roots α_i and t achieve minimum, then $\sigma(\alpha_t) < 0$.*

Thm 5.5.2. *Let (V, R) be a reduced root system and Δ be a base, then*

(1) The action of $W(R)$ on the sets of chambers and bases are compatible and transitive.

(2) For $\alpha \in R$, there exists $\sigma \in W(R)$ such that $\sigma(\alpha) \in \Delta$.

(3) $W(R) = \langle s_\alpha | \alpha \in \Delta \rangle$

(4) If $\sigma(\Delta) = \Delta$ with $\sigma \in W(R)$, then $\sigma = 1$.

Proof. Let $W' = \langle s_\alpha | \alpha \in \Delta \rangle$.
We first show (1)(2) for W'.

(1) Let $\delta = \frac{1}{2}\sum_{\alpha>0} \alpha$ and take $\sigma \in W'$ such that $(\sigma(\gamma)|\delta)$ is maximal.
Then for every $\alpha \in \Delta$, $(\sigma(\gamma)|\delta) \geqslant (s_\alpha\sigma(\gamma)|\delta) = (\sigma(\gamma)|s_\alpha(\delta)) = (\sigma(\gamma)|\delta - \alpha)$.
So $(\sigma(\gamma)|\alpha) \geqslant 0$, *i.e.* $\sigma(\gamma) \in C(\Delta)$.
Hence σ maps $C(\gamma)$ to $C(\Delta)$ and maps $\Delta(\gamma)$ to Δ.

(2) By (1), we only need to find a base of R containing α.
Take $\gamma \in \ker \alpha^\vee$ but $\gamma \notin \ker \beta^\vee$ for any $\beta \neq \alpha \in \Delta$.
Then there is some γ' near γ such that $(\gamma'|\alpha) = \varepsilon > 0$ and $|(\gamma'|\beta)| > \varepsilon$.
So $\alpha \in R^+(\gamma')$.
And suppose $\alpha = \beta_1 + \beta_2$ with $\beta_1, \beta_2 \in R^+(\gamma')$.
Then $0 < (\beta_i|\gamma) < (\alpha|\gamma)$, contradiction!
Hence $\alpha \in \Delta(r')$.

(3) For $\beta \in R$, there exists $\sigma \in W'$ such that $\alpha \in \sigma(\beta) \in \Delta$.
So $s_\alpha = s_{\sigma(\beta)} = \sigma s_\beta \sigma^{-1}$, *i.e.* $s_\beta = \sigma^{-1} s_\alpha \sigma \in W'$.
Hence $W(R) = W'$.

(4) By (3), $\sigma = \sigma_1 \dots \sigma_t$ with $\sigma_i = s_{\alpha_i}$ and $\alpha_i \in \Delta$.
Assume t is minimal, then $\alpha_t = \sigma(\alpha_t) < 0$, contradiction!

□

Def 5.5.10. Fix a base Δ, write $\sigma \in W(R)$ as $\sigma_1 \cdots \sigma_t$ with $\sigma_i = s_{\alpha_i}$, $\alpha_i \in \Delta$ and t minimal, then this expression is called reduced and $l(\sigma) = t$.

Def 5.5.11. Define $n(\sigma)$ to be the number of positive roots α for which $\sigma(\alpha) < 0$.

Lemma 5.5.9. *Let $\sigma \in W(R)$, then $l(\sigma) = n(\sigma)$.*

Proof. We prove this by induction on $l(\sigma)$.
When $l(\sigma) = 0$, $\sigma = \mathrm{Id}$ and $n(\sigma) = 0$.
Now assume we have proven for $l(\sigma) = t - 1$.
When $l(\sigma) = t$, let $\sigma = \sigma_1 \cdots \sigma_t$ be reduced.
Then $n(\sigma_1 \cdots \sigma_{t-1}) = t - 1$.
And since for $\alpha > 0$ and $\alpha \neq \alpha_t$, $\sigma_t(\alpha) > 0$.
So $\sigma_1 \cdots \sigma_t(\alpha) < 0$ iff $\sigma_1 \cdots \sigma_{t-1}(\sigma_t(\alpha)) < 0$ and $\sigma(\alpha_t) < 0$.
Hence $n(\sigma) = n(\sigma_1 \cdots \sigma_{t-1}) + 1 = t = l(\sigma)$. □

Lemma 5.5.10. *Let $\lambda, \mu \in \overline{C(\Delta)}$, suppose $\sigma \in W(R)$ such that $\sigma(\lambda) = \mu$, then $\lambda = \mu$ and $\sigma = \sigma_1 \cdots \sigma_t$ with $\sigma_i = s_{\alpha_i}$, $\alpha_i \in \Delta$ and $\lambda \in \ker \alpha_i^\vee$.*

Proof. Let $\sigma = \sigma_1 \cdots \sigma_t$ be reduced.
Then $\sigma(\alpha_t) < 0$ and so $0 \leqslant (\lambda|\alpha_t) = (\mu|\sigma(\alpha_t)) \leqslant 0$.
Therefore $\lambda_i^\vee(\lambda) = \frac{2(\alpha|\lambda)}{(\alpha|\alpha)} = 0$.
Hence $\sigma_t(\lambda) = \lambda$ and $\mu = \lambda_1 \dots \lambda_{t-1}(\lambda)$, the proof is done by induction. □

Def 5.5.12. Let (V, R) be a root system, if there exists $V_1, V_2 \subset V$ such that $V = V_1 \oplus V_2$ and $R \subset V_1 \cup V_2$, then $(V_1, V_1 \cap R)$ and $(V_2, V_2 \cap R)$ are root systems, denote $R_1 = V_1 \cap R, R_2 = V_2 \cap R$ and we say $(V, R) = (V_1, R_1) \oplus (V_2, R_2)$ is the direct sum of $(V_1, R_1), (V_2, R_2)$.
If $(V, R) = (V_1, R_1) \oplus (V_2, R_2)$, then we say (V, R) is reducible, otherwise it is irreducible.

Lemma 5.5.11. *R is irreducible iff Δ cannot be decomposed as $\Delta = \Delta_1 \sqcup \Delta_2$ such that $\langle \Delta_1, \Delta_2 \rangle = 0$.*

Proof. If R is reducible, let $R = R_1 \sqcup R_2$, $V_1 = \mathrm{span} R_1$ and $V_2 = \mathrm{span} R_2$.
Then $\langle R_1, R_2 \rangle = 0$.
Take $\Delta_1 = \Delta \cap R_1, \Delta_2 = \Delta \cap R_2$.
So $\Delta = \Delta_1 \sqcup \Delta_2$ and $\langle \Delta_1, \Delta_2 \rangle = 0$.
Conversely, let R_i be the set of roots that are W-conjugate to certain root in Δ_i.
Then $R = R_1 \cup R_2$.
For $\alpha, \beta \in R$ such that $\langle \alpha, \beta \rangle = 0$, $s_\alpha(\beta) = \beta$, *i.e.* $s_\alpha s_\beta = s_\beta s_\alpha$.
So we can write $\sigma \in W(R)$ as $\sigma = s_{\alpha_1} \cdots s_{\alpha_p} s_{\beta_1} \cdots s_{\beta_q}$ with $\alpha_i \in \Delta_1, \beta_j \in \Delta_2$.
Therefore for $\alpha \in \Delta_1$, $\sigma(\alpha) = s_{\alpha_1} \cdots s_{\alpha_p} \in \mathrm{span}\Delta_1$, *i.e.* $R_1 \subset \mathrm{span}\Delta_1$.
Hence $R_1 \cap R_2 = \varnothing$ and $\langle R_1, R_2 \rangle = 0$. □

Lemma 5.5.12. *Let R be a irreducible root system and Δ be a base, then there exists a unique root $\beta > 0$ with $\mathrm{ht}(\beta)$ maximal, moreover*

(1) For $\alpha \in \Delta$, $(\beta|\alpha) \geqslant 0$, in other words, $\beta \in \overline{C(\Delta)}$.

(2) $\beta = \sum k_\alpha \alpha$ with all $k_\alpha > 0$.

(3) For $\alpha \in R$, $\alpha < \beta$.

Such β is called the highest root.

(1) Suppose $(\beta|\alpha) < 0$ for some $\alpha \in \Delta$.
Then $\alpha + \beta \in R$ and $\mathrm{ht}(\alpha + \beta) = \mathrm{ht}(\beta) + 1 > \mathrm{ht}(\beta)$, contradiction!

(2) Let $\beta = \sum k_\alpha \alpha, \Delta_1 = \{\alpha \in \Delta | k_\alpha > 0\}$ and $\Delta_2 = \{\alpha \in \Delta | k_\alpha = 0\}$.
Then there exists $\alpha \in \Delta_2$ such that $\langle \alpha, \Delta_1 \rangle \neq 0$, otherwise R is reducible.
So $(\alpha|\beta) < 0$, contradiction!

(3) If $\alpha > \beta$, then $\mathrm{ht}(\alpha) = \mathrm{ht}(\beta) + \mathrm{ht}(\alpha - \beta) > \mathrm{ht}(\beta)$.
So β is maximal relative to $<$.
Suppose there is another β' that is maximal relative to $<$.
Then we can also prove (1) for β', let $\beta' = \sum k'_\alpha \alpha$ with $k'_\alpha > 0$.
Therefore $(\beta|\beta') = \sum k'_\alpha (\beta|\alpha) > 0$.
Hence $\beta - \beta' \in R$, *i.e.* $\beta > \beta'$ or $\beta' > \beta$, contradiction!

Prop 5.5.8. *An irreducible root system has one or two root length.*

Proof. Let $\alpha \in R$ and $V_1 = \text{span}W(R)\alpha$.
Then V_1 is stable under $W(R)$.
Since R is irreducible.
So $V_1 = V$, *i.e.* for $\alpha, \beta \in R$, there exists $\sigma \in W(R)$ such that $(\sigma(\alpha)|\beta) \neq 0$.
Therefore $\frac{(\alpha|\alpha)}{(\beta|\beta)} = \{1, 2, 3, \frac{1}{2}, \frac{1}{3}\}$.
Hence there are at most two root lengths. □

Def 5.5.13. If (V, R) has two lengths, we say they are long root and short root. If (V, R) has only one length, then they are all called long.

Prop 5.5.9. *Highest root is long.*

Proof. Let β be the highest root and $\alpha \in R$.
WLOG, we assume $\alpha \in \overline{C(\Delta)}$.
So $\beta - \alpha > 0$ and $(\gamma|\beta - \alpha) \geqslant 0$ for all $\gamma \in \overline{C(\Delta)}$.
Hence $(\beta|\beta - \alpha) \geqslant 0$ and $(\alpha|\beta - \alpha) \geqslant 0$, *i.e.* $(\beta|\beta) \geqslant (\alpha|\beta) \geqslant (\alpha|\alpha)$ □

Prop 5.5.10. *Let (V, R) be an irreducible root system with two root lengths and Δ be a base, then among all short roots, there exists a unique maximal one β, called the highest short root. Moreover, $(\beta|\alpha) \geqslant 0$ for $\alpha \in \Delta$ and $\beta = \sum k_\alpha \alpha$ with $k_\alpha > 0$.*

Prop 5.5.11. *Let (V, R) be a root system and Δ be a base, if $\Delta = \Delta_1 \sqcup \Delta_2$ with $\langle \Delta_1, \Delta_2 \rangle = (0)$, then Δ_i is a base for (V_i, R_i) with $V_i = \text{span}_{\mathbb{R}} \Delta_i$ and $R_i = W(R)\Delta_i$.*

Prop 5.5.12. *Let R be an irreducible root system, then roots with same length form a $W(R)$-orbit.*

Proof. Let $\|\alpha\| = \|\beta\|$ and WLOG, assume α is not orthogonal to β.
Then $\theta(\alpha, \beta) \in \{0, \frac{1}{3}\pi, \frac{2}{3}\pi, \pi\}$.
If $\theta(\alpha, \beta) = 0$ or π, then $\beta = \alpha$ or $\beta = s_\alpha(\alpha)$.
If $\theta(\alpha, \beta) = \frac{1}{3}\pi$, then $s_\beta s_\alpha s_\beta(\alpha) = s_\beta s_\alpha(\alpha - \beta) = s_\beta(-\alpha - \beta + \alpha) = \beta$.
If $\theta(\alpha, \beta) = \frac{2}{3}\pi$, then $s_\alpha s_\beta(\alpha) = s_\alpha(\alpha + \beta) = -\alpha + \beta + \alpha = \beta$. □

Def 5.5.14. Let $\Delta = \{\alpha_1, \ldots, \alpha_l\}$ be a base of (V, R), then the matrix $(\langle \alpha_i, \alpha_j \rangle)$ is called the Cartan matrix of R.

Prop 5.5.13. *Given (V, R, Δ) and (V', R', Δ') with $\Delta = \{\alpha_1, \ldots, \alpha_l\}, \Delta' = \{\alpha'_1, \ldots, \alpha'_l\}$, if $\langle \alpha_i, \alpha_j \rangle = \langle \alpha'_i, \alpha'_j \rangle$ for all i, j, then the bijection $\Delta \to \Delta', \alpha_i \mapsto \alpha'_i$ extends to a linear isomorphism $\phi : V \to V'$ such that $\phi(R) = R'$.*

Proof. $s_{\phi(\alpha)}(\phi(\beta)) = \phi(\beta) - \langle \phi(\beta), \phi(\alpha) \rangle \phi(\alpha) = \phi(\beta) - \langle \beta, \alpha \rangle \phi(\alpha) = \phi(s_\alpha(\beta))$.
So $W(R) \to W(R'), \sigma \mapsto \phi\sigma\phi^{-1}$ is a well-defined group isomorphism.
Moreover, for $\beta \in R$, there exists $\sigma \in W(R)$ such that $\beta = \sigma(\alpha)$ with $\alpha \in \Delta$.
Hence $\phi(\beta) = \phi\sigma\phi^{-1}(\phi(\alpha)) \in R'$. □

Def 5.5.15. The Coxeter graph of R w.r.t. Δ consisting of l vertices such that vertices i and j are connected by $\langle \alpha_i, \alpha_j \rangle \langle \alpha_j, \alpha_i \rangle$ undirected edges. And Dynkin diagram is the Coxeter graph with direction from large norm to small norm.

Exam 5.5.2. *Dynkin diagrams:*
A_l:
$B_l (l \geqslant 2)$:
$C_l (l \geqslant 3)$:
$D_l (l \geqslant 4)$:
E_6: , E_7: , E_8:
F_4: , G_2:

Def 5.5.16. Define a matrix S_Δ, called Schläfli matrix, whose diagonal elements are 2 and (i,j)-item is $-\sqrt{\langle\alpha_i,\alpha_j\rangle\langle\alpha_j,\alpha_i\rangle} = \frac{2(\alpha_i|\alpha_j)}{\|\alpha_i\|\|\alpha_j\|}$, then S_Δ is real symmetric matrix.

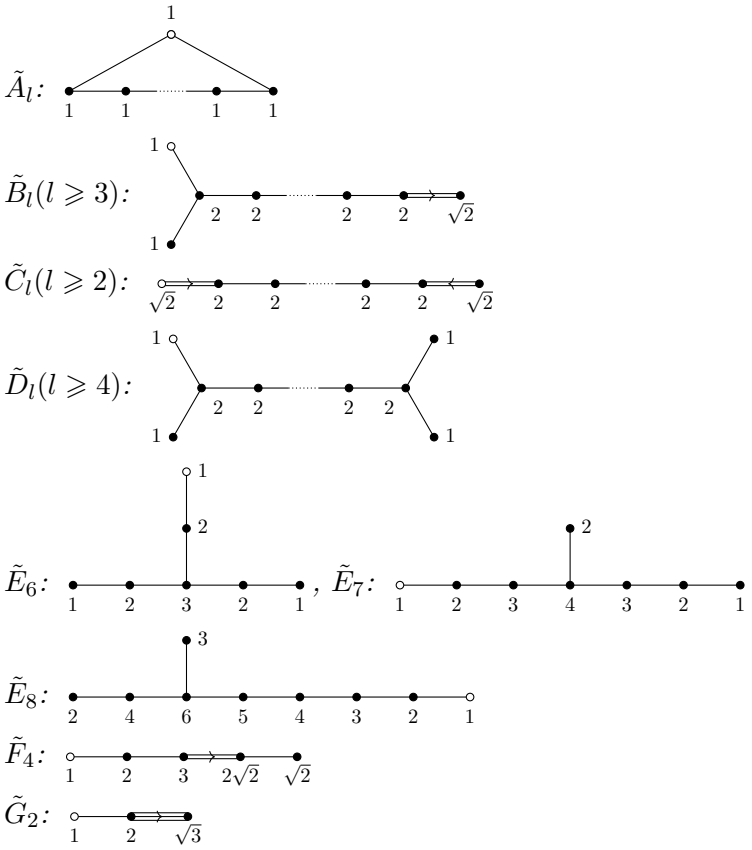
Remark 5.5.2. S_Δ is the intersection matrix for $2(\cdot|\cdot)$ w.r.t. $\left\{\frac{\alpha_i}{\|\alpha_i\|}\right\}$ and so S_Δ is positive definite.

Lemma 5.5.13. *Let S be a real symmetric matrix with $s_{ii} > 0, s_{ij} \leqslant 0$ for $i \neq j$, suppose S is positive definite, then by replacing $s_{ij} = s_{ji}$ by certain $s' \in (n_{ij}, 0]$, the resulting matrix S' is still positive definite.*

Prop 5.5.14. *Let G be a connected graph such that there are at most three edges between each pair of points and S_G be the associated matrix, suppose there exists $\lambda = (\lambda_1, \dots, \lambda_l) > 0$ such that $S_G\lambda = 0$, then for any $\mu \in \mathbb{R}^l$, $\mu^T S_G \mu \geqslant 0$ and the equality holds iff $\mu \in \mathbb{R}\lambda$.*

In other words, S_G is semi positive definite with rank $l-1$.

Exam 5.5.3. *Extended Dynkin graphs:*



Prop 5.5.15. *For graphs in example 5.5.2, S_G is positive definite.*

For graphs in example 5.5.3, S_G is semi-positive definite with $r(S_G) = |G| - 1$.

Thm 5.5.3. *A connected graph G with S_G positive definite must belong to example 5.5.2.*

Thm 5.5.4. *Let (V, R) be a reduced irreducible root system over $\mathbb{R}$ and Δ be a base, then its Dynkin diagram belongs to example 5.5.2.*

Exam 5.5.4. *Explicit description of root systems of type A to G:*

A_l: $V = \{\sum \lambda_i v_i | \sum \lambda_i = 0\}, R = \{v_i - v_j | i \neq j\}, \Delta = (v_1 - v_2, \dots, v_l - v_{l+1})$, highest root is $v_1 - v_{l+1}$ and $W(R) = S_{l+1}$.

$B_l(l \geqslant 2)$: $V = \mathbb{R}^l, R = \{\pm v_i, \pm v_i \pm v_j\}, \Delta = (v_1 - v_2, \dots, v_{l-1} - v_l, v_l)$, highest root is $v_1 + v_2$, highest short root v_1 and $W(R) \cong S_l \ltimes (\mathbb{Z}/2\mathbb{Z})^l$.

$C_l(l \geqslant 3)$: $V = \mathbb{R}^l, R = \{\pm 2v_i, \pm v_i \pm v_j\}, \Delta = (v_1 - v_2, \dots, v_{l-1} - v_l, 2v_l)$, highest root is $2v_1$, highest short root $v_1 + v_2$ and $W(R) \cong S_l \ltimes (\mathbb{Z}/2\mathbb{Z})^l$.

$D_l (l \geqslant 4)$: $V = \mathbb{R}^l, R = \{\pm v_i \pm v_j\}, \Delta = (v_1 - v_2, \ldots, v_{l-1} - v_l, v_{l-1} + v_l)$, *highest root is* $v_1 + v_2$ *and* $W(R) \cong S_l \ltimes (\mathbb{Z}/2\mathbb{Z})^{l-1}$.

E_8: $V = \mathbb{R}^8$,

$$R = \{\pm v_i \pm v_j\} \cup \left\{ \frac{1}{2} \sum (-1)^{\varepsilon_i} v_i \middle| \varepsilon \in \{0,1\}, 2 | \sum \varepsilon_i \right\},$$

$$\Delta = \left(\frac{1}{2}(v_1 + v_8 - v_2 \cdots - v_7), v_1 + v_2, v_1 - v_2, \ldots, v_7 - v_8 \right)$$

and the highest root is $v_7 + v_8$.

F_4: $V = \mathbb{R}^4$,

$$R = \{\alpha = \sum k_i v_i | k_i \in \frac{1}{2}\mathbb{Z}, k_i - k_j \in \mathbb{Z}, (\alpha|\alpha) = 1, (\alpha|\alpha) = 1 \text{ or } 2\},$$

$$\Delta = \left(v_2 - v_3, v_3 - v_4, v_4, \frac{1}{2}(v_1 - v_2 - v_3 - v_4) \right)$$

and the highest root is $v_1 - v_2$.

G_2: $V = (v_1 + v_2 + v_3)^\perp \subset \mathbb{R}^3$,

$$R = \{\alpha = \sum k_i v_i | k_i \in \mathbb{Z}, (\alpha|\alpha) = 2 \text{ or } 6\},$$

$$\Delta = (v_1 - v_2, -2v_1 + v_2 + v_3)$$

and the highest root is $2v_3 - v_1 - v_2$.

Prop 5.5.16. *$W(R)$ is normal in $A(R)$ and $A(R)/W(R) \cong \Gamma = \{\tau \in A(R) | \tau(\Delta) = \Delta\}$, which is the group of automorphisms of Dynkin diagrams.*

We now assume F is an algebraically closed field with character zero.

Def 5.5.17. A Lie algebra $\mathfrak{g}$ is called reductive if $\mathrm{Rad}(\mathfrak{g}) = Z(\mathfrak{g})$.

Prop 5.5.17. *Let $\mathfrak{g}$ be a Lie algebra, TFAE:*

(1) $\mathfrak{g}$ is reductive

(2) $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ is completely reducible (semisimple)

(3) $\mathfrak{g} \cong I \times \mathfrak{h}$ with I abelian and $\mathfrak{h}$ semisimple.

Proof. (3) $\Rightarrow$ (1): $\mathrm{Rad}(I \times \mathfrak{h}) = \mathrm{Rad}(I) \times \mathrm{Rad}(\mathfrak{h}) = I = Z(\mathfrak{g})$.
(1) $\Rightarrow$ (2): Since $Z(\mathfrak{g})$ is the kernel of ad.
So ad factor through $\mathfrak{g}/Z(\mathfrak{g}) \to \mathfrak{gl}(\mathfrak{g})$ and $\mathfrak{g}/Z(\mathfrak{g})$ is semisimple.
By Weyl theorem, $\mathfrak{g}$ is completely reducible as $\mathfrak{g}/Z(\mathfrak{g})$-module.
(2) $\Rightarrow$ (3): Let $\mathfrak{g} = \bigoplus I_i$ be a complete decomposition as $\mathfrak{g}$-module.
Then each I_i is an minimal ideal.
And since ideal of I_i is still ideal of $\mathfrak{g}$.
So $\dim I_i = 1$ or I_i is simple.
Hence $\mathfrak{g}$ is isomorphic to a product of simple Lie algebras and an abelian one. □

Prop 5.5.18. *Let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}(V)$, suppose V is irreducible as $\mathfrak{g}$-module, then $\mathfrak{g}$ is reductive with $\dim Z(\mathfrak{g}) \leqslant 1$. Moreover, if $\mathfrak{g} \subset \mathfrak{sl}(V)$, then $\mathfrak{g}$ is semisimple.*

Proof. Let $S = \mathrm{Rad}(\mathfrak{g})$.

Similar to the proof of Lie theorem, there is a basis $(v_1, \dots, v_n)$ of V such that $s \in S$ are upper-triangular matrices with all diagonal elements equal to $\lambda(s)$ under this basis.

And since for $s \in [S, \mathfrak{g}]$, $\mathrm{tr}(s) = 0$.

So for $s \in S$ and $x \in \mathfrak{g}$, $s(x(v)) = \lambda([s,x])v + \lambda(s)x(v) = \lambda(s)x(v)$.

Hence $S = Z(\mathfrak{g})$, *i.e.* $\mathfrak{g}$ is reductive and $\dim S \leqslant 1$.

Moreover, if $\mathfrak{g} \subset \mathfrak{sl}(V)$, then $\lambda(s) = 0$ for $s \in S$, *i.e.* $S = 0$. □

Prop 5.5.19. *For $\mathfrak{g} = \mathfrak{sl}_n(F), \mathfrak{so}_n(F), \mathfrak{sp}_{2n}(F)$, the corresponding $\mathfrak{g} \hookrightarrow \mathfrak{gl}(V)$ is irreducible. Moreover, they are semisimple.*

Proof. Let $\mathcal{A}$ be the associative subalgebra of $\mathfrak{gl}(V)$ generated by $\mathfrak{g}$ and 1.

If $\mathcal{A} = \mathfrak{gl}(V)$, then $\mathfrak{g} \hookrightarrow \mathfrak{gl}(V)$ is irreducible.

For $\mathfrak{g} = \mathfrak{sl}_n(F)$, $\mathfrak{gl}_n(F) = \mathfrak{sl}_n(F) \oplus F \cdot I = \mathcal{A}$.

For $\mathfrak{g} = \mathfrak{sp}_{2n}(F)$, let $x = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$, then

$$\begin{bmatrix} A^T & C^T \\ B^T & D^T \end{bmatrix} \begin{bmatrix} & I \\ -I & \end{bmatrix} + \begin{bmatrix} & I \\ -I & \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = 0.$$

So $A^T + D = 0, B = B^T, C = C^T$, in particular, $\mathfrak{sp}_{2n}(F) \subset \mathfrak{sl}_{2n}(F)$.

Therefore $\left[\begin{smallmatrix} E & \\ & -E \end{smallmatrix}\right] \in \mathfrak{g}, \left[\begin{smallmatrix} & E \\ E & \end{smallmatrix}\right] = \left[\begin{smallmatrix} & I \\ -I & \end{smallmatrix}\right]\left[\begin{smallmatrix} E & \\ & -E \end{smallmatrix}\right] \in \mathcal{A}, \left[\begin{smallmatrix} E & \\ & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & \\ & E \end{smallmatrix}\right] \in \mathcal{A}$ for any diagonal matrices E and so $e_{ii} \in \mathcal{A}$.

Moreover, $e_{ii} x e_{jj} \in \mathcal{A}$ for $x \in \mathfrak{g}$, *i.e.* $e_{ij} \in \mathcal{A}$ for any i, j.

For $\mathfrak{g} = \mathfrak{so}_{2n}(F)$, let $x = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$, then

$$\begin{bmatrix} A^T & C^T \\ B^T & D^T \end{bmatrix} \begin{bmatrix} & I \\ I & \end{bmatrix} + \begin{bmatrix} & I \\ I & \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = 0.$$

So $A^T + D = 0, B + B^T = 0, C + C^T = 0$, similar as $\mathfrak{sp}_{2n}$, $\mathfrak{g} \to \mathfrak{gl}(V)$ is irreducible.

For $\mathfrak{g} = \mathfrak{so}_{2n+1}(F)$, let

$$x = \begin{bmatrix} a & b_1 & b_2 \\ c_1 & m & n \\ c_2 & p & q \end{bmatrix},$$

then we have

$$\begin{bmatrix} a & c_1^T & c_2^T \\ b_1^T & m^T & p^T \\ b_2^T & n^T & q^T \end{bmatrix} \begin{bmatrix} 1 & & \\ & & I \\ & I & \end{bmatrix} + \begin{bmatrix} 1 & & \\ & & I \\ & I & \end{bmatrix} \begin{bmatrix} a & b_1 & b_2 \\ c_1 & m & n \\ c_2 & p & q \end{bmatrix} = 0.$$

So $a = 0, b_1 + c_2^T = 0, b_2 + c_1^T = 0, p + p^T = n + n^T = 0, q + m^T = 0$.

Similar as $\mathfrak{sp}_{2n}$, we can show that $e_{ij} \in \mathcal{A}$ for $i, j \geqslant 2$, and so

$$E_{ii} \begin{bmatrix} 0 & -1 & \cdots & -1 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix} = e_{i1}, \begin{bmatrix} 0 & -1 & \cdots & -1 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix} E_{jj} = -e_{1j} \in \mathcal{A}.$$

Moreover, $e_{1i} e_{i1} = e_{11} \in \mathcal{A}$. □

Prop 5.5.20. *The root system corresponding to $\mathfrak{sp}_{2n}(F)$ is of type C_n.*

Proof. Let $M_{ij} = e_{i,j} - e_{n+j,n+i}, P_{ij} = e_{i,n+j} + e_{j,n+i}, Q_{ij} = e_{n+i,j} + e_{n+j,i}$ with $1 \leqslant i, j \leqslant n$.

Then M_{ij}, P_{ij}, Q_{ij} is a basis of $\mathfrak{sp}_{2n}(F)$.

Let $\mathfrak{h} \subset \mathfrak{g}$ be the set of diagonal matrices.

Then elements in $\mathfrak{h}$ are all semisimple.

Suppose $\left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in \mathfrak{sp}_{2n}(F)$ commutes with $\left[\begin{smallmatrix} E & \\ & -E \end{smallmatrix}\right] \in \mathfrak{h}$, then

$$\begin{bmatrix} AE & -BE \\ CE & -DE \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} E & \\ & -E \end{bmatrix} = \begin{bmatrix} E & \\ & -E \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} EA & EB \\ -EC & -ED \end{bmatrix}.$$

So $AE = EA, DE = ED, EB = -BE, CE = -EC$, *i.e.* A, D are diagonal and $B = C = 0$.
Therefore $N_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{h}$, *i.e.* $\mathfrak{h}$ is a Cartan subalgebra.
Let $\mathfrak{h}^v = \text{span}\{\varepsilon_1, \dots, \varepsilon_n\}$ with $\varepsilon_i(M_{jj}) = \delta_{ij}$.
And since $[M_{kk}, M_{ij}] = (\varepsilon_i - \varepsilon_j)(M_{kk})M_{ij}$.
So $M_{ij} \in \mathfrak{g}^{\varepsilon_i - \varepsilon_j}$.
Similarly, $[M_{kk}, P_{ij}] = (\varepsilon_i + \varepsilon_j)(M_{kk})P_{ij}$, *i.e.* $P_{ij} \in \mathfrak{g}^{\varepsilon_i + \varepsilon_j}$.
And $[M_{kk}, Q_{ij}] = (-\varepsilon_i - \varepsilon_j)(M_{kk})Q_{ij}$, *i.e.* $Q_{ij} \in \mathfrak{g}^{-\varepsilon_i - \varepsilon_j}$.
Hence $R = \{\pm\varepsilon_i \pm \varepsilon_j, \pm 2\varepsilon_i\}$. □

Prop 5.5.21. *The root system corresponding to $\mathfrak{so}_{2n+1}(F)$ is of type B_n.*

Proof. We denote index from 0, let $B_i = e_{i,0} - e_{0,n+i}, C_i = e_{0,i} - e_{n+i,0}, M_{ij} = e_{i,j} - e_{n+j,n+i}$, $P_{ij} = e_{i,n+j} - e_{j,n+i}, Q_{ij} = e_{n+j,i} - e_{n+i,j}$.
Then $B_i, C_i, M_{ij}, P_{ij}, Q_{ij}$ is a basis of $\mathfrak{sp}_{2n}(F)$.
Let $\mathfrak{h} \subset \mathfrak{g}$ be the set of diagonal matrices.
Similar as above, we can verify that $\mathfrak{h}$ is a Cartan subalgebra.
Let $\mathfrak{h}^\vee = \text{span}\{\varepsilon_1, \dots, \varepsilon_n\}$ with $\varepsilon_i(M_{jj}) = \delta_{ij}$.
Then $B_i \in \mathfrak{g}^{\varepsilon_i}, C_i \in \mathfrak{g}^{-\varepsilon_i}, M_{ij} \in \mathfrak{g}^{\varepsilon_i - \varepsilon_j}, P_{ij} \in \mathfrak{g}^{\varepsilon_i + \varepsilon_j}, Q_{ij} \in \mathfrak{g}^{-\varepsilon_i - \varepsilon_j}$ with $i \neq j$.
So $R = \{\pm\varepsilon_i, \pm\varepsilon_i \pm \varepsilon_j\}$. □

Prop 5.5.22. *The root system corresponding to $\mathfrak{so}_{2n}(F)$ is of type D_n.*

Proof. Let $M_{ij} = e_{i,j} - e_{n+j,n+i}$,
$P_{ij} = e_{i,n+j} - e_{j,n+i}, Q_{ij} = e_{n+j,i} - e_{n+i,j}$.
Then $B_i, C_i, M_{ij}, P_{ij}, Q_{ij}$ is a basis of $\mathfrak{sp}_{2n}(F)$.
Let $\mathfrak{h} \subset \mathfrak{g}$ be the set of diagonal matrices.
Similar as above, we can verify that $\mathfrak{h}$ is a Cartan subalgebra.
Let $\mathfrak{h}^\vee = \text{span}\{\varepsilon_1, \dots, \varepsilon_n\}$ with $\varepsilon_i(M_{jj}) = \delta_{ij}$.
Then $M_{ij} \in \mathfrak{g}^{\varepsilon_i - \varepsilon_j}, P_{ij} \in \mathfrak{g}^{\varepsilon_i + \varepsilon_j}, Q_{ij} \in \mathfrak{g}^{-\varepsilon_i - \varepsilon_j}$ with $i \neq j$.
So $R = \{\pm\varepsilon_i \pm \varepsilon_j\}$. □

Prop 5.5.23. *Let $\mathfrak{g}$ be a simple Lie algebra and $\mathfrak{h}$ be a Cartan subalgebra, then $(\mathfrak{h}^\vee, R)$ is irreducible.*

Proof. Suppose $R = R_1 \sqcup R_2, \langle R_1, R_2 \rangle = 0$.
Then for $\alpha \in R_1, \beta \in R_2$, $(\alpha + \beta|\alpha) > 0, (\alpha + \beta|\beta) > 0$, *i.e.* $\alpha + \beta \notin R$.
So $[\mathfrak{g}^\alpha, \mathfrak{g}^\beta] = \mathfrak{g}^{\alpha+\beta} = 0$.
Let $\mathfrak{k}$ be the subalgebra of $\mathfrak{g}$ generated by $\mathfrak{g}^\alpha$ with $\alpha \in R_1$.
Then for $\beta \in R_2$, $[\mathfrak{k}, \mathfrak{g}^\beta] = 0$.
So $\mathfrak{k}$ is an ideal of $\mathfrak{g}$, contradiction! □

Thm 5.5.5. *Let $\mathfrak{g}, \mathfrak{g}'$ be two simple Lie algebra, $\mathfrak{h} \subset \mathfrak{g}, \mathfrak{h}' \subset \mathfrak{g}'$ be Cartan subalgebras and R, R' be the corresponding root systems. Suppose there exists linear isomorphism $\mathfrak{h} \to \mathfrak{h}'$ such that $R \to R'$ and $\alpha \mapsto \alpha'$. Take any base $\Delta \subset R$, let $\Delta' \subset R'$ be the corresponding base, for $\alpha \in \Delta, \alpha' \in \Delta'$, take generator $x_\alpha \in \mathfrak{g}^\alpha, x'_{\alpha'} \in (\mathfrak{g}')^{\alpha'}$, then there exists unique isomorphism $\mathfrak{g} \to \mathfrak{g}'$ compatible with $\mathfrak{h} \to \mathfrak{h}', x_\alpha \mapsto x'_{\alpha'}$.*

Chapter 6

Number Field

6.1 Number field and number ring

Def 6.1.1. A number field is a subfield of $\mathbb{C}$ having finite degree over $\mathbb{Q}$.

Lemma 6.1.1. *Let f be a monic polynomial over $\mathbb{Z}$, suppose $f = gh$ where g, h are monic polynomial over $\mathbb{Q}$, then $g, h \in \mathbb{Z}[x]$.*

Proof. Let m, n be the minimal integers such that $mg \in \mathbb{Z}[x]$ and $nh \in \mathbb{Z}[x]$.
Then for $p|mn$, $mg \cdot nh \equiv mnf = 0 \pmod{p}$.
But since $\mathbb{Z}_p[x]$ is an integer domain.
So $mg \equiv 0 \pmod{p}$ or $nh \equiv 0 \pmod{p}$, *i.e.* $\frac{m}{p}g$ or $\frac{n}{p}h$ is polynomial over $\mathbb{Z}$.
Hence $m = n = 1$. □

Thm 6.1.1. *Let α be an integer and f be the minimal polynomial of α over $\mathbb{Z}$, then f is irreducible over $\mathbb{Q}$.*

Proof. Notice that f is monic.
By lemma, f is irreducible over $\mathbb{Q}$. □

Coro 6.1.1. *Algebraic integers in $\mathbb{Q}$ are $\mathbb{Z}$.*

Coro 6.1.2. *Let m be a squarefree integer, then the set of algebraic integers in $\mathbb{Q}[\sqrt{m}]$ is*

$$\left\{a + b\sqrt{m} \middle| a, b \in \mathbb{Z}\right\} \text{ if } m \equiv 2 \text{ or } 3 \pmod{4}$$

$$\left\{\frac{a + b\sqrt{m}}{2} \middle| a, b \in \mathbb{Z}, 2|(a - b)\right\} \text{ if } m \equiv 1 \pmod{4}$$

Proof. Let $\alpha = r + s\sqrt{m}$ with $r, s \in \mathbb{Q}$ and $s \neq 0$.
Then the minimal polynomial of α in $\mathbb{Q}$ is $x^2 - 2rx + r^2 - s^2m$.
So α is algebraic integer iff $2r \in \mathbb{Z}, r^2 - s^2m \in \mathbb{Z}$.
Let $r = \frac{a}{2}, s = \frac{b}{2}$.
Then α is algebraic integer iff $4|a^2 - b^2m$.
If $m \equiv 2$ or $3 \pmod{4}$, $4|a^2 - b^2m$ iff $2|a, b$.
If $m \equiv 1 \pmod{4}$, $4|a^2 - b^2m$ iff $2|a - b$. □

Thm 6.1.2. *TFAE:*

(1) α is an algebraic integer.

(2) The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated.

(3) α is a member of some subring of $\mathbb{C}$ having a finitely generated additive group.

(4) $\alpha A \subset A$ for some finitely generated additive subgroup $A \subset \mathbb{C}$.

Coro 6.1.3. *If α and β are algebraic integers, then so are $\alpha+\beta$ and $\alpha\beta$.*

Def 6.1.2. We denote the set of algebraic integers by $\mathbb{A}$, and the subring $\mathbb{A} \cap K$ of K is called a number ring.

Def 6.1.3. Let K be a number field and $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$ where $n = [K : \mathbb{Q}]$, then for $\alpha \in K$, we set

$$T(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots \sigma_n(\alpha),$$

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) \ldots \sigma_n(\alpha),$$

which are called trace and norm resp.

Prop 6.1.1. *Let $\alpha, \beta \in K, r \in \mathbb{Q}$, then $T(\alpha+\beta) = T(\alpha)+T(\beta), N(\alpha\beta) = N(\alpha)N(\beta), T(r\alpha) = rT(\alpha)$ and $N(r\alpha) = r^n N(\alpha)$.*

Prop 6.1.2. *Let $\alpha \in K$ of degree d over $\mathbb{Q}$ and $[K : \mathbb{Q}] = n$, then*

$$T(\alpha) = \frac{n}{d} t(\alpha), N(\alpha) = (n(\alpha))^{\frac{n}{d}},$$

where $t(\alpha), n(\alpha)$ are the sum and product of d conjugates of α over $\mathbb{Q}$.

Thm 6.1.3. *Let $\alpha \in K$, $T(\alpha)$ and $N(\alpha)$ are rational. In particular, if α is an algebraic integer, then $T(\alpha)$ and $N(\alpha)$ are integers.*

Exam 6.1.1. *Consider $K = \mathbb{Q}[\sqrt{m}]$ and $\alpha = a + b\sqrt{m}$.*
Then $T(\alpha) = 2a, N(\alpha) = a^2 - mb^2$.

Def 6.1.4. Let $\alpha_1, \ldots, \alpha_n \in K$, we define the discriminant of $\alpha_1, \ldots, \alpha_n$ to be

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

Thm 6.1.4.

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(T(\alpha_i\alpha_j)).$$

Proof. $[\sigma_j(\alpha_i)][\sigma_i(\alpha_j)] = [\sum_k \sigma_k(\alpha_i\alpha_j)] = [T(\alpha_i\alpha_j)]$. □

Coro 6.1.4. $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$ *iff $\alpha_1, \ldots, \alpha_n$ are linearly dependent over $\mathbb{Q}$.*

Proof. $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(T(\alpha_i\alpha_j)) = 0$ iff row of $[T(\alpha_i\alpha_j)]$ are linearly dependent iff $\alpha_1, \ldots, \alpha_n$ are linearly dependent. □

Thm 6.1.5. *Let $K = \mathbb{Q}[\alpha]$ and $\alpha_1, \ldots, \alpha_n$ be the conjugations of α over $\mathbb{Q}$, then*

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leqslant r < s \leqslant n} (\alpha_r - \alpha_s)^2 = \pm N^K(f'(\alpha)),$$

where f be the minimal polynomial of α and the $+$ sign holds iff $n \equiv 0$ or $1 \pmod 4$.

Proof. Since $\sigma_i(\alpha^j) = (\sigma_i(\alpha))^j = \alpha_i^j$.
By the determinant of Vandermonde matrix, the first equality holds.
Moreover,

$$N^K(f'(\alpha)) = \prod_{r=1}^{n} f'(\alpha_r) = \prod_{r=1}^{n} \prod_{s \neq r} (\alpha_r - \alpha_s) = \pm \prod_{1 \leqslant r < s \leqslant n} (\alpha_r - \alpha_s)^2.$$

And the $+$ sign holds iff $4 | n(n-1)$, *i.e.* $n \equiv 0$ or $1 \pmod 4$. □

Exam 6.1.2. *Consider $K = \mathbb{Q}[\omega]$ with $\omega = e^{\frac{2\pi i}{p}}$.*
Then the minimal polynomial of ω is $f(x) = 1 + x + \cdots + x^{p-1} = \frac{x^p-1}{x-1}$.
So $f'(\omega) = \frac{p}{\omega(\omega-1)}$ and $N(f'(\omega)) = \frac{N(p)}{N(\omega)N(\omega-1)} = \frac{p^{p-1}}{p} = p^{p-2}$.
Now assume $\omega = e^{\frac{2\pi i}{m}}$ for arbitrary $m \in \mathbb{Z}$.
Let f be the minimal polynomial of ω and $x^m - 1 = f(x)g(x)$.
Then $f'(\omega) = \frac{m}{\omega g(\omega)}$ and $N(f'(\omega)) = \frac{m^{\varphi(m)}}{N(\omega g(\omega))}$.
So $\operatorname{disc}(\omega) | m^{\varphi(m)}$

Thm 6.1.6. *Let K be a number field of degree n over $\mathbb{Q}$, R be the ring of algebraic integers in K and $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K over $\mathbb{Q}$ containing in R, then every $\alpha \in R$ can be expressed in the form*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{\operatorname{disc}(\alpha_1, \ldots, \alpha_n)}$$

with all $m_j \in \mathbb{Z}$ and all m_j^2 divisible by $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$.

Proof. Let $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$.
Then $\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n)$.
By Cramer rule, $x_i = \frac{y_i}{\delta}$ where $\delta = \det(\sigma_i(\alpha_j))$ and y_i is obtained from δ by replacing the j column by the $\sigma_i(\alpha)$.
So y_i, δ are algebraic integers and $dx_i = \delta y_i \in \mathbb{Q}$.
Therefore $m_i = dx_i \in \mathbb{Z}$.
Moreover, $\frac{m_i^2}{d} = y_i^2 \in \mathbb{Q}$ is algebraic integers, *i.e.* $d | m_i^2$. □

Coro 6.1.5. *R is a free abelian group of rank n.*

Def 6.1.5. A set of algebraic integers $\{\beta_1, \ldots, \beta_n\}$ is called an integral basis for R if every $\alpha \in R$ can be uniquely represented by the linear combination of $\{\beta_1, \ldots, \beta_n\}$ over $\mathbb{Z}$.

Exam 6.1.3. *Consider $K = \mathbb{Q}[\sqrt{m}]$.*
Then an integral basis for R can be given by $\{1, \sqrt{m}\}$ when $m \equiv 2$ or $3 \pmod 4$ and $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$ when $m \equiv 1 \pmod 4$.

Lemma 6.1.2. *Let $\omega = e^{\frac{2\pi i}{m}}$, then $\mathbb{Z}[1-\omega] = \mathbb{Z}$ and $\operatorname{disc}(1-\omega) = \operatorname{disc}(\omega)$.*

Lemma 6.1.3. *Let $m = p^r, \omega = e^{\frac{2\pi i}{m}}$, then $\prod_{p \nmid k}(1-\omega^k) = p$.*

Proof. Let $f(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$.
Then $f(x) = \prod_{p \nmid k}(x - \omega^k)$.
So $f(1) = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}} = p$. □

Thm 6.1.7. *Let $m = p^r, \omega = e^{\frac{2\pi i}{m}}$, then $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$.*

Proof. Let $\alpha = \frac{m_1 + m_2(1-\omega) + \cdots + m_n(1-\omega)^{n-1}}{\operatorname{disc}(\omega)} \in R = \mathbb{A} \cap \mathbb{Q}[\omega]$.
Since $d = \operatorname{disc}(\omega) | m^{\varphi(m)}$.
So d is power of p.
Suppose there exists i such that $d \nmid m_i$, WLOG, assume $m_j = 0$ for $j < i$.
By lemma 6.1.3 $\frac{p}{(1-\omega)^n} \in \mathbb{Z}[\omega]$.
Therefore $\frac{\beta p}{(1-\omega)^i} \in R$, *i.e.* $\frac{m_i}{1-\omega} \in R$.
But $N(m_i) = m_i^n$ and $N(1-\omega) = p \nmid m_i^n$, contradiction! □

Thm 6.1.8. *Let $\{\beta_1, \ldots, \beta_n\}$ and $\{\gamma_1, \ldots, \gamma_n\}$ be two integral bases for $R = \mathbb{A} \cap K$, then $\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\gamma_1, \ldots, \gamma_n)$.*

Proof. Let $(\beta_1, \dots, \beta_n)^T = M(\gamma_1, \dots, \gamma_n)^T$.
Then $(\sigma_j(\beta_i)) = M(\sigma_j(\gamma_i))$.
So $\operatorname{disc}(\beta_1, \dots, \beta_n) = |M|^2 \operatorname{disc}(\gamma_1, \dots, \gamma_n)$.
Conversely, we also have $\operatorname{disc}(\beta_1, \dots, \beta_n) | \operatorname{disc}(\gamma_1, \dots, \gamma_n)$.
Hence $\operatorname{disc}(\beta_1, \dots, \beta_n) = \operatorname{disc}(\gamma_1, \dots, \gamma_n)$. □

Exam 6.1.4.

$$\operatorname{disc}\left(\mathbb{A} \cap \mathbb{Q}\left[\sqrt{m}\right]\right) = \begin{cases} \operatorname{disc}(\sqrt{m}) = 4m & m \equiv 2 \text{ or } 3 \pmod 4 \\ \operatorname{disc}(\frac{1+\sqrt{m}}{2}) = m & m \equiv 1 \pmod 4 \end{cases}$$

Thm 6.1.9. *Let K, L be two number fields, R, S, T be rings of algebraic integers in K, L, KL resp. and $d = \gcd(\operatorname{disc} R, \operatorname{disc} S)$, suppose $[KL : \mathbb{Q}] = mn$, then $T \subset \frac{1}{d} RS$.*
In particular, if $d = 1$, then $T = RS$.

Coro 6.1.6. *Let $K = \mathbb{Q}[\omega]$ with $\omega = e^{\frac{2\pi i}{m}}$ and $R = \mathbb{A} \cap K$, then $R = \mathbb{Z}[\omega]$.*

Proof. Let $m = m_1 m_2$ such that m_1, m_2 are coprime, $\omega_1 = \omega^{m_2}, \omega_2 = \omega^{m_1}$.
Then $\operatorname{disc}(\omega_1) | m_1^{\varphi(m_1)}, \operatorname{disc}(\omega_2) | m_2^{\varphi(m_2)}$.
So $\gcd(\operatorname{disc}(\omega_1), \operatorname{disc}(\omega_2)) = 1$.
By theorem 6.1.9, the proof is done. □

Thm 6.1.10. *Let $\alpha \in R$ of degree n over $\mathbb{Q}$, then there is an integral basis*

$$1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}},$$

where $d_i \in \mathbb{Z}$ such that $d_1 | d_2 | \cdots | d_{n-1}$ and f_i are monic polynomials over $\mathbb{Z}$ with $\deg f_i = i$.

Exam 6.1.5. *Consider $K = \mathbb{Q}\left[\sqrt[3]{m}\right]$ where $m = hk^2$ such that h and k are squarefree and coprime.*
Set $\alpha = \sqrt[3]{m}$, then an integral basis of R can be given by

$$\left\{1, \alpha, \frac{\alpha^2}{k}\right\} \text{ if } m \not\equiv \pm 1 \pmod 9,$$

$$\left\{1, \alpha, \frac{\alpha^2 \pm k^2 \alpha + k^2}{3k}\right\} \text{ if } m \equiv \pm 1 \pmod 9.$$

6.2 Prime decomposition in number rings

Def 6.2.1. A Dedekind domain is an integral domain R such that

(1) Every ideal is finitely generated.

(2) Every nonzero prime ideal is a maximal ideal.

(3) R is an integrally closed integral domain.

Thm 6.2.1. *Every number ring is a Dedekind domain.*

Proof. Since R is a free abelian group of rank n.
So every ideal is finitely generated.
Let I be a prime ideal, $\alpha \in I$ and $m = N^K(\alpha) = \alpha\beta$.
Then $\beta = \frac{m}{\alpha} \in K$ and β is an algebraic integer.
Therefore $m \in I$.
Notice that $|R/(m)| = m^n$.
So R/I is finite integral domain, *i.e.* R/I is a field.
Moreover, R is integrally closed in K since $\mathbb{A}$ is integrally closed in $\mathbb{C}$. □

Lemma 6.2.1. *In a Dedekind domain, every ideal contains a product of prime ideals.*

Proof. Suppose not, let I be a maximal member of such ideal and $r, s \in R\backslash I$ such that $rs \in I$.
Then $I + (r), I + (s)$ is larger than I, *i.e.* they contains a product of prime ideals.
So $(I + (r))(I + (s)) \subset I$ contains a product of prime ideals, contradiction! □

Lemma 6.2.2. *Let I be a proper ideal of Dedekind domain R with field of fractions K, then there is an element $\gamma \in K\backslash R$ such that $\gamma I \subset R$.*

Proof. By the lemma, let $a \in I, I \subset P$ and $P_1P_2 \cdots P_r \subset (a)$ with minimal r.
Suppose P does not contain any of P_i, take $a_i \in P_i\backslash P$.
Then $a_1a_2 \cdots a_r \in P$, *i.e.* $a_i \in P$ for some i, contradiction!
WLOG, assume $P_1 \subset P$, *i.e.* $P_1 = P$.
And since r is minimal.
Take $b \in P_2P_3 \cdots P_r\backslash(a)$ and $\gamma = \frac{b}{a}$.
Then $\gamma A \subset \frac{b}{a}P_1 \subset \frac{1}{a}P_2P_3 \cdots P_rP_1 = \frac{1}{a}(a) = R$. □

Thm 6.2.2. *Let I be an ideal of Dedekind domain R, then there exists an ideal J such that IJ is principal.*

Proof. Let $\alpha \in I$ and take $J = \{\beta \in R | \beta I \subset (\alpha)\}$.
Then $IJ \subset (\alpha)$, we claim that $IJ = (\alpha)$.
Let $A = \frac{1}{\alpha}IJ$, which is an ideal of R.
Suppose A is a proper ideal of R.
Then by lemma, there exists $\gamma \in K\backslash R$ such that $\gamma A \subset R$.
So $\gamma J \subset \gamma A \subset R$.
Moreover, for $\beta \in J$, $\gamma\beta I \subset \gamma\alpha A \subset \alpha R = (\alpha)$.
Therefore $\gamma J \subset J$.
By proposition 3.2.3, γ is a root of a polynomial over R, contradiction. □

Coro 6.2.1. *Let A, B be two ideals of Dedekind domain R, with $B \subset A$ and $A \neq R$, then there exists $\gamma \in K$ such that $\gamma B \subset R, \gamma B \nsubseteq A$.*

Proof. Let $BC = (\alpha)$.
Then $BC \nsubseteq \alpha A$, *i.e.* there exists $\beta \in C$ such that $\beta B \nsubseteq \alpha A$.
So take $\gamma = \frac{\beta}{\alpha}$. □

Def 6.2.2. We define an equivalence relation on the set of ideals of a ring R where $A \sim B$ iff $\alpha A = \beta B$ for some $\alpha, \beta \in R$. We call the equivalence class ideal class.

Coro 6.2.2. *The ideal classes of Dedekind domain R forms a group, called ideal class group.*

Proof. The identity consisting principal ideal and by above theorem, the inverse always exists. □

Coro 6.2.3. *Let A, B, C be three ideals of Dedekind domain, if $AB = AC$, then $B = C$.*

Proof. Let $AJ = (\alpha)$.
Then $\alpha B = \alpha C$, *i.e.* $B = C$. □

Coro 6.2.4. *Let A, B be ideals of Dedekind domain, then $A|B$ iff $A \supset B$.*

Proof. $\Rightarrow$: Trivial.
$\Leftarrow$: Let $AJ = (\alpha)$, take $C = \frac{1}{\alpha}BJ$.
Since $BJ \subset AJ = (\alpha)$.
So C is an ideal of R and $AC = \frac{1}{\alpha}AJB = B$. □

Thm 6.2.3. *Every ideal of Dedekind domain R is uniquely representable as a product of prime ideals.*

Proof. Suppose not, let I be the maximal member of such ideals and $I \subset P$.
By corollary 6.2.4, $I = PJ$ for some ideal J containing I.
Suppose $I = J$.
Then $PI = RI$, *i.e.* $P = R$, contradiction.
So $I \subsetneqq J$.
But then J is a product of prime ideals, contradiction! □

Coro 6.2.5. *The ideals of a number ring factor uniquely into prime ideals.*

Exam 6.2.1. *Consider* $R = \mathbb{Z}\left[\sqrt{-5}\right]$.
Then $(2) = \left(2, 1+\sqrt{-5}\right)^2, (3) = \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right)$.

Thm 6.2.4. *Let I be an ideal of Dedekind domain R and $\alpha \in I$, then there exists $\beta \in I$ such that $I = (\alpha, \beta)$.*

Proof. Let $I = P_1^{n_1} \cdots P_r^{n_r}$.
Then $P_i^{n_i} | (\alpha)$ and let $Q_1, \ldots, Q_s$ be the other prime ideal dividing (α).
Take $\beta_i \in P_i^{n_i} \backslash P_i^{n_i+1}$ and β such that $\beta \equiv \beta_i \pmod{P_i^{n_i+1}}, \beta \equiv 1 \pmod{Q_i}$.
Such β exists by Chinese Remainder Theorem. □

Thm 6.2.5. *A Dedekind domain is a UFD iff it is a PID.*

Proof. $\Leftarrow$: Trivial $\Rightarrow$: Let I be an ideal of R and $\alpha \in I$.
Then $I | (\alpha)$.
Since α is a product of prime elements in R.
So I divides a product of principal prime ideals.
Hence I is a product of principal prime ideals, *i.e.* I is a principal ideal. □

From now on, we let $K \subset L$ be two number fields and $R = \mathbb{A} \cap K, S = \mathbb{A} \cap L$

Prop 6.2.1. *Let P be a prime of R, Q be a prime of S, then TFAE:*

(1) $Q | PS$.

(2) $Q \supset PS$.

(3) $Q \supset P$.

(4) $Q \cap R = P$.

(5) $Q \cap K = P$.

When these conditions hold, we say Q lies over P and P lies under Q

Proof. (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) and (4) $\Rightarrow$ (3) are trivial, (4) $\Leftrightarrow$ (5) since $Q \subset \mathbb{A}$.
(3) $\Rightarrow$ (4): Since P is maximal ideal of R.
So $Q \cap R = P$ or R.
But if $R \subset Q$, then $RS = S \subset Q$, this is impossible. □

Thm 6.2.6. *Every prime Q of S lies over a unique prime P of R and every prime P of R lies under at least one prime Q of S.*

Proof. Since Q is prime ideal.
So $P = Q \cap R$ is prime ideal.
And by theorem 3.4.1, P lies under at least one prime Q of S. □

Def 6.2.3. Let Q^e be the exact power of Q dividing PS, then e is called the ramification index of Q over P, denoted by $e(Q|P)$.

Exam 6.2.2. *Consider $R=\mathbb{Z}, S=\mathbb{Z}[i]$.*
Then the principal ideal $(1-i)$ in S lies over 2.
And since $2S=(1-i)^2$.
So $e((1-i)|2)=2$.
Moreover, consider $R=\mathbb{Z}, S=\mathbb{Z}[\omega]$ with $\omega=e^{\frac{2\pi i}{m}}, m=p^r$.
Then the principal ideal $(1-\omega)$ in S lies over p.
And we can check that $1+\omega+\cdots+\omega^t$ is a unit in S if t and m are coprime
So $p=u(1-\omega)^{\varphi(m)}$ where u is a unit by lemma 6.1.3.
Therefore $e((1-\omega)|p)=\varphi(m)=p^{r-1}(p-1)$.

Def 6.2.4. Consider the residue fields of P and Q, S/Q is an extension of finite degree f over R/P, then f is called the inertial degree of Q over P and is denoted by $f(Q|p)$.

Exam 6.2.3. *Consider $R=\mathbb{Z}, S=\mathbb{Z}[i], p=(2), Q=(1-i)$.*
Then $|S/Q|=|R/p|=2$.
So $f(Q|p)=1$.
And consider $p=(3), Q=(3)$, we have $|S/Q|=9$ and $|R/p|=3$.
Therefore $f(Q|p)=2$.

Prop 6.2.2. *Let $P\subset Q\subset U$ be the prime ideals in three number rings $R\subset S\subset T$, then $e(U|P)=e(U|Q)e(Q|P), f(U|P)=f(U|Q)f(Q|P)$.*

Thm 6.2.7. *Let n be the degree of L over K, I,J be the ideals of R and write $\|I\|$ to indicate the index $|R/I|$.*

(1) $\|IJ\|=\|I\|\|J\|$

(2) $\|IS\|=\|I\|^n$

(3) Let $\alpha\in R$, $\|(\alpha)\|=\left|N_{\mathbb{Q}}^K(\alpha)\right|$.

Thm 6.2.8. *Let n be the degree of L over K and let $Q_1,\dots,Q_r$ be the primes of S lying over a prime P of R. Denote by $e_1,\dots,e_r$ and $f_1,\dots,f_r$ the corresponding ramification indices and inertial degrees, then $\sum e_if_i=n$.*

We prove these two theorem simultaneously.

Proof of theorem 6.2.7(1). Suppose I and J are coprime.
By CRT, we have an isomorphism $R/IJ\to R/I\times R/J$.
So $\|IJ\|=\|I\|\|J\|$.
Now it suffices to check that $\|P^m\|=\|P\|^m$.
This is because $R/P\to P^k/P^{k+1}$ is a group isomorphism for all k.
Hence $\|P\|=\left|P^k/P^{k+1}\right|$. □

Proof of theorem 6.2.8, Special case. We assume $K=\mathbb{Q}$ and then $P=p\mathbb{Z}$ for some prime p.
Let $pS=\prod Q_i^{e_i}$.
So $p^n=\|pS\|=\prod\|Q_i\|^{e_i}=\prod p^{f_ie_i}$.
Hence $n=\sum f_ie_i$. □

Proof of theorem 6.2.7(2). By (1), it suffices to prove for prime ideal I.
Since S/IS is a vector space over field R/I.
Suppose $[\alpha_1], \dots, [\alpha_{n+1}] \in S/IS$ is linearly independent over R/I.
Then $\alpha_1, \dots, \alpha_{n+1}$ is linearly dependent over K and also over R.
Let $\beta_1\alpha_1 + \cdots + \beta_{n+1}\alpha_{n+1} = 0$ for $\beta_i \in R$.
By corollary 6.2.1, there exists $\gamma \in K$ such that $\gamma\beta_i \in R$ but not all $\gamma\beta_i$ contains in I.
So $\alpha_1, \dots, \alpha_{n+1}$ is linearly dependent over R/I, contradiction!
Therefore $\dim S/IS \leqslant n$.
On the other hand, let $I \cap \mathbb{Z} = p\mathbb{Z}$ and P_i are all prime ideals of R lying over p.
We set $n_i = \dim S/P_iS, e_i = e(P_i|p), f_i = f(P_i|p), m = [K : \mathbb{Q}]$.
Then $p^{mn} = \|pS\| = \prod \|P_iS\|^{e_i} = \prod \|P_i\|^{n_ie_i} = \prod p^{f_in_ie_i}$.
So $n\sum f_ie_i = mn = \sum f_in_ie_i$, *i.e.* $n = n_i$. □

Proof of theorem 6.2.8. Since $PS = \prod Q_i^{e_i}$.
So $\|P\|^n = \|PS\| = \prod \|Q_i\|^{e_i} = prod\|P\|^{f_ie_i}$.
Hence $n = \sum f_ie_i$. □

Proof of theorem 6.2.7(3). Extend K to a normal extension M of $\mathbb{Q}$ and let $T = \mathbb{A} \cap M$.
Then $\|\sigma(\alpha)T\| = \|\alpha T\|$.
So $|N|^{mn}, \|NT\| = \prod \|\sigma(\alpha)T\| = \|\alpha T\|^n = \|(\alpha)\|^{mn}$ where $m = [M : K]$ and $N = N_{\mathbb{Q}}^K(\alpha)$.
Hence $\left|N_{\mathbb{Q}}^K(\alpha)\right| = \|(\alpha)\|$. □

Exam 6.2.4. *Consider $R = \mathbb{Z}, S = \mathbb{Z}[\omega]$ with $\omega = e^{\frac{2\pi i}{m}}$ and $m = p^r$.*
Then $\|(1-\omega)\|^n = \|(1-\omega)^n\| = \|p\mathbb{Z}[\omega]\| = p^n$.
So $\|(1-\omega)\| = p$, i.e. *$(1-\omega)$ is a prime ideal.*
Consider $S = \mathbb{Z}[\alpha]$ with $\alpha = \sqrt[3]{2}$.
Then $2S = (\alpha)^3$, i.e. *(α) is a prime ideal and $f((\alpha)|2) = 1$.*
Since $5S = (5, \alpha+2)(5, \alpha^2+3\alpha-1)$.
We claim that $(5, \alpha^2+3\alpha-1)$ is prime ideal.
Notice that $\mathbb{Z}_5[x]/(x^2+3x-1)$ is a field and we can map it onto $S/(5, \alpha^2+3\alpha-1)$.
So $S/(5, \alpha^2+3\alpha-1)$ is $\mathbb{F}_{25}$.
Therefore $f((5, \alpha^2+3\alpha-1)|5) = 2$ and so $(5, \alpha+2)$ is a prime ideal with inertial index 1.
Consider α such that $\alpha^3 = \alpha + 1$.
Then $23S = (23, \alpha-10)^2(23, \alpha-3)$ and so $(23, \alpha-10), (23, \alpha-3)$ are prime ideals.

Thm 6.2.9. *Let L be a normal extension over K and Q, Q' be two prime ideals of S lying over P of R, then $\sigma(Q) = Q'$ for some $Q \in G = \mathrm{Gal}(L/K)$.*

Proof. Suppose $\sigma(Q) \neq Q'$ for all $\sigma \in G$.
Then by CRT, there exists $\alpha \in S$ such that $\alpha \equiv 0 \pmod{Q'}$ and $\alpha \equiv 1 \pmod{\sigma(Q)}$.
So $N_K^L(\alpha) \in R \cap Q' = P$.
And since $\sigma(\alpha) \notin Q$.
Therefore $N_K^L(\alpha) \notin Q$, contradiction! □

Coro 6.2.6. *Let L be a normal extension over K and Q, Q' be two prime ideals lying over P, then $e(Q|P) = e(Q'|P)$ and $f(Q|P) = f(Q'|P)$.*

Def 6.2.5. A prime ideal P of R is called ramified in S if $e(Q|P) > 1$ for some Q of S lying over P. Otherwise, it is called unramified. Moreover, if $PS = Q^n$ with $n = [L : K]$, then we say P is totally ramified in S.

Thm 6.2.10. *Let p be a prime in $\mathbb{Z}$ and suppose p is ramified in a number ring R, then $p|\operatorname{disc}(R)$.*

Coro 6.2.7. *Let $\alpha \in R$ such that $K = \mathbb{Q}[\alpha]$ and f be any monic polynomial over $\mathbb{Z}$ such that $f(\alpha) = 0$, if p is a prime such that $p \nmid N^K f'(\alpha)$, then p is unramified in K.*

Coro 6.2.8. *Only finitely many primes of $\mathbb{Z}$ are ramified in R.*

Coro 6.2.9. *Only finitely many primes of R are ramified in S.*

Prop 6.2.3. *If $p|m$, then $pR = (p, \sqrt{m})^2$.*

If m is odd, then

$$2R = \begin{cases} (2, 1+\sqrt{m})^2 & m \equiv 3 \pmod 4 \\ \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) & m \equiv 1 \pmod 8 \\ \text{prime} & m \equiv 5 \pmod 8 \end{cases}$$

If p is odd and $p \nmid m$, then

$$pR = \begin{cases} (p, n+\sqrt{m})\,(p, n-\sqrt{m}) & m \equiv n^2 \pmod p \\ \text{prime} & m \text{ is not a square mod } p \end{cases}$$

Proof. The case that pR is not prime are easy to check.

When $p = 2, m \equiv 5 \pmod 8$, Let $f(x) = x^2 - x + \frac{1-m}{4}$ and P be a prime ideal lying over p.

Then f has roots $\frac{1\pm\sqrt{m}}{2}$ in R, *i.e.* f has root in field R/P.

But since $(2x-1)^2 - m$ cannot be divided by 8.

So $f(x)$ has no root in field $\mathbb{F}_2$, *i.e.* $R/P \neq \mathbb{F}_2$.

Therefore $P = 2R$ and $f(P|2) = 2$.

Similarly, when p is odd and m is not a square mod p, let $f(x) = x^2 - m$. □

Prop 6.2.4. *Let $R = \mathbb{Z}[\omega]$ with $\omega = e^{\frac{2\pi i}{m}}$ and $m = p^k n$, then $pR = (Q_1 \dots Q_r)^e$ with $e = \varphi(p^k)$ and f is the order of p mod n.*

Coro 6.2.10. *If $p \nmid m$, then p splits into $\frac{\varphi(m)}{f}$ distinct prime ideal in $\mathbb{Z}[\omega]$, where f is the order of p mod m.*

Thm 6.2.11. *Let $L = K[\alpha]$ with $\alpha \in S$ of degree n over K, p be a prime that does not divide $|S/R[\alpha]|$ and prime ideal P of R lying over p. Consider the minimal polynomial g of α over K, it factors into monic irreducible factors in $(R/P)[x]$ in the form*

$$\bar{g} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}.$$

Then the prime decomposition of PS is given by

$$Q_1^{e_1} \cdots Q_r^{e_r},$$

where $Q_i = (P, g_i(\alpha))$

Exam 6.2.5. *Consider $K = \mathbb{Q}, L = \mathbb{Q}[\sqrt{m}]$.*

When $p = 2$ and $m \equiv 1 \pmod 4$, take $\alpha = \frac{1+\sqrt{m}}{2}$.

Then $S = R[\alpha]$ and so the result can be obtained by factoring $x^2 - x + \frac{1-m}{4}$ over $\mathbb{F}_2$.

In other case, take $\alpha = \sqrt{m}$.

Then $S = R[\alpha]$ and so the result can be obtained by factoring $x^2 - m$ over $\mathbb{F}_p$.

6.3 Galois theory applied to prime decomposition

We now assume that number field L is a normal extension over K of degree n and we denote its Galois group as G.

Def 6.3.1. Let Q be a prime ideal of S lying over P of R, we define the decomposition group $D(Q|P) = \{\sigma \in G | \sigma Q = Q\}$ and inertia group $E(Q|P) = \{\sigma \in G | \sigma(\alpha) \equiv \alpha \pmod{Q}, \alpha \in S\}$.

Let L_D, L_E be the fixed field of D and E resp, we call L_D the decomposition field and L_E the inertia field.

Thm 6.3.1. *Let $K, L, R, S, P, Q, G, D, E, r, e$ and f as above, then we have*

DEGREES	L	Q	*RAMIFICATION INDICES*	*INERTIAL DEGREES*
e			e	1
	L_E	Q_E		
f			1	f
	L_D	Q_D		
r			1	1
	K	P		

Coro 6.3.1. *Let $\bar{G}$ be the Galois group of S/Q over R/P, then there is a map from D onto $\bar{G}$ by $\sigma \to \bar{\sigma}$ with kernel E.*

Proof. Let $\varphi : D \to \bar{G}, \sigma \to \bar{\sigma}$.
Then $\ker \varphi = \{\sigma | \sigma(\alpha + Q) = \alpha + Q, \alpha \in S\} = E$.
So φ factor through injection $D/E \to \bar{G}$.
And since $|D/E| = [L_E : L_D] = f = |\bar{G}|$.
Hence φ is surjective. □

Coro 6.3.2. *Suppose D is a normal subgroup of G, then P splits into r distinct primes in L_D. If E is also normal in G, then each of them remains prime in L_E. Finally, each one becomes an e-th power in L.*

Proof. Normal subgroup of Galois group corresponds to Galois extension over K.
So by corollary 6.2.6, the proof is done. □

Exam 6.3.1. *Consider $R = \mathbb{Z}, S = \mathbb{Z}[omega]$ with $\omega = e^{\frac{2\pi i}{23}}$, $P = (2)$.*
By proposition 6.2.4, $e = 1, f = 11, r = 2$.
So the decomposition field is a extension of $\mathbb{Q}$ of degree 2, i.e. *it must be $\mathbb{Q}\left[\sqrt{-23}\right]$.*
And P is unramified, i.e. *the inertia field is all of $\mathbb{Q}[\omega]$.*
Consider $L = \mathbb{Q}\left[i, \sqrt{2}, \sqrt{5}\right]$ with Galois group $G = (\mathbb{Z}/2\mathbb{Z})^3$, and $P = (5)$.
Then 5 splits into two prime ideals in $\mathbb{Q}[i]$, is inert in $\mathbb{Q}\left[\sqrt{2}\right]$ and become a square in $\mathbb{Q}\left[\sqrt{5}\right]$.
So $r, e, f \geqslant 2$ and $ref = 8$, i.e. *$r = e = f = 2$.*
Hence $\mathbb{Q}[i]$ is the decomposition field and $\mathbb{Q}\left[i, \sqrt{2}\right]$ is the inertia field and $5S = (2+i)^2(2-i)^2$.

Thm 6.3.2. *(1) L_D is the largest intermediate field K' such that $e(P'|P) = f(P'|P) = 1$.*

(2) L_D is the smallest K' such that Q is the only prime ideal of S lying over P'.

(3) L_E is the largest K' such that $e(P'|P) = 1$.

(4) L_E is the largest K' such that Q is totally ramified over P'.

Def 6.3.2. A prime ideal P in K splits completely in an extension field L iff P splits into $[L:K]$ distinct primes.

Coro 6.3.3. *If D is a normal subgroup of G, then P splits completely in K' iff $K' \subset L_D$.*

Prop 6.3.1. *Let p be an odd prime and $q \neq p$ be any prim, fix a divisor d of $p-1$, then q is a d-th power mod p iff q splits completely in F_d, which is the unique subfield of $\mathbb{Q}[\omega]$ having degree d over $\mathbb{Q}$.*

Proof. Let $R = \mathbb{Z}[\omega]$.
By proposition 6.2.4, qR splits into r distinct prime where $f = \frac{p-1}{r}$ is the order of q.
So q is d-th power mod p iff $f \mid \frac{p-1}{d}$, *i.e.* $d|r$, $F_d \subset F_r$.
And since F_r is the decomposition field of q.
Hence q is d-th power iff q splits completely in F_d. □

Coro 6.3.4 (Gauss quadratic reciprocity law)**.** *For odd prime $p \neq q$, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.*

Proof. $\left(\frac{q}{p}\right) = 1$ iff q splits completely in $F_2 = \mathbb{Q}\left[\sqrt{(-1)^{\frac{p-1}{2}}p}\right]$.
So $\left(\frac{q}{p}\right) = 1$ iff $(-1)^{\frac{p-1}{2}}p$ is a square mod q, *i.e.* $\left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = 1$.
And since $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$.
Hence $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$. □

Thm 6.3.3. *Let L, M be two extension of K, if P is unramified in both L and M, then P is unramified in LM. If P splits completely in both L and M, then P splits completely in LM.*

Proof. Let P' be a prime ideal of LM lying over P, F be a normal extension of K containing LM and Q be a prime ideal of F lying over P'.
Then Q lies over P.
And since $Q \cap L, Q \cap M$ are unramified.
So $L, M \subset F_E$, *i.e.* $LM \subset F_E$.
Therefore $e(P'|P) = 1$ for all P' lying over P.
Hence P is unramified in LM.
Similarly, if P splits completely in both L and M, then P splits completely in LM. □

Coro 6.3.5. *Let L be an extension of K and P be a prime ideal of K, if P is unramified or splits completely in L, then the same is true in the normal closure M of L over K.*

Proof. If P is unramified(or splits completely) in L, then so it is in $\sigma(L)$. □

Thm 6.3.4. *Let P be a prime ideal of R which is unramified in S and Q of S lying over P, then there exists a unique $\phi \in D$ such that*

$$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q}.$$

Moreover, if G is abelian, then ϕ only depends on P and

$$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{PS}.$$

We denote $\phi = \phi(Q|P)$ and it is called Frobenius automorphism.

Proof. Since P is unramified, *i.e.* $e(Q|P) = 1$.
So $D(Q|P)$ is isomorphic to the Galois group of S/Q over R/P.
Notice that Galois group of S/Q over R/P is generated by a map $x \mapsto x^{\|P\|}$ on R/P.
Hence it corresponds to a map $\phi \in D$ with $\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q}$. □

Thm 6.3.5. *Let M be an intermediate field of $L \supset K$ with Galois group H, $T = M \cap \mathbb{A}$ and P be a prime ideal of R which is unramified in S, suppose that the set of right coset of H in G is partitioned into sets*

$$\{H\sigma_1, H\sigma_1\phi, \dots, H\sigma_1\phi^{m_1-1}\},$$

$$\vdots$$

$$\{H\sigma_r, H\sigma_r\phi, \dots, H\sigma_r\phi^{m_r-1}\}.$$

Then the splitting of P in M is given by $PT = Q_1 \cdots Q_r$, where $Q_i = (\sigma_i U) \cap T$ and U is a prime ideal of S lying over P. Moreover, $f(Q_i|P) = m_i$.

Proof. If $Q_i = Q_j$, then $\sigma_i U$ and $\sigma_j U$ are prime ideals of S lying over $Q_i = Q_j$.
So there exists $\tau \in H$ such that $\tau\sigma_i U = \sigma_j U$, *i.e.* $H\sigma_i = H\sigma_j$.
And since $\phi(\sigma_i U|Q_i) = \phi(\sigma_i U|P)^{f(Q_i|P)}$.
So $\phi(\sigma_i U|Q_i) = (\sigma_i\phi\sigma_i^{-1})^{f(Q_i|P)} = \sigma_i\phi^{f(Q_i|P)}\sigma_i^{-1}$, *i.e.* $\sigma_i\phi^{f(Q_i|P)}\sigma_i^{-1} \in H$.
Hence $m_i | f(Q_i|P)$, *i.e.* $m_i = f(Q_i|P)$. □

Thm 6.3.6. *Let p be a prime in $\mathbb{Z}$ such that $p|\operatorname{disc}(R)$, then p is ramified in R.*

6.4 The ideal class group and the unit group

Thm 6.4.1. *Let K be a number field and $R = \mathbb{A} \cap K$, then there is a positive real number λ depending on K such that every nonzero ideal I of R contains a nonzero element α with $\left|N_{\mathbb{Q}}^K(\alpha)\right| \leqslant \lambda\|I\|$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be an integral basis of R and take

$$\lambda = \prod_{i=1}^{n}\sum_{j=1}^{n}|\sigma_i\alpha_j|.$$

For any ideal I, let $m^n \leqslant \|I\| < (m+1)^n$ and consider $S = \{\sum m_j\alpha_j | m_j \in \mathbb{Z}, \cap[0, m]\}$.
Then there must exist two elements of S which are congruent mod I.
So their difference is contained in I, denote it by $\alpha = \sum m_j\alpha_j$ with $m_j \in \mathbb{Z} \cap [-m, m]$.
Hence we have

$$\left\|N_{\mathbb{Q}}^K(\alpha)\right\| = \prod_{i=1}^{n}\left|\sum_{j=1}^{n}m_j\sigma_i\alpha_j\right| \leqslant \prod_{i=1}^{n}m\sum_{j=1}^{n}|\sigma_i\alpha_j| \leqslant \lambda\|I\|.$$

□

Coro 6.4.1. *Every ideal class of R contains an ideal J with $\|J\| \leqslant \lambda$.*

Proof. Let C be an ideal class, take $I \in C^{-1}$ and $\alpha \in I$.
Then there exists $J \in C$ such that $IJ = (\alpha)$.
Hence $\|I\|\|J\| = \|(\alpha)\| = \left|N_{\mathbb{Q}}^K(\alpha)\right| \leqslant \lambda\|I\|$, *i.e.* $\|J\| \leqslant \lambda$. □

Coro 6.4.2. *There are only finitely many ideal classes in R.*

Exam 6.4.1. *Consider* $R = \mathbb{Z}\left[\sqrt{2}\right]$ *and* $\lambda = \left(1+\sqrt{2}\right)^2 \approx 5.8$.

Then for $\|J\| \leqslant \lambda$, *prime divisors of* $\|J\|$ *must lie over* $2, 3$ *or* 5.

And since $2R = \left(\sqrt{2}\right)^2$, $3R, 5R$ *are primes.*

So J *can only be one of* $R, \left(\sqrt{2}\right)$ *or* (2), i.e. *every ideal in* R *is principal.*

Consider $R = \mathbb{Z}\left[\sqrt{-5}\right]$ *and* $\lambda = \left(1+\sqrt{5}\right)^2 \approx 10.5$.

Then for $\|J\| \leqslant \lambda$, *prime divisors of* $\|J\|$ *must lie over* $2, 3, 5$ *or* 7.

And since $2R = \left(2, 1+\sqrt{-5}\right)^2, 3R = \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right), 5R = \left(\sqrt{-5}\right)^2$ *and* $7R = \left(7, 3+\sqrt{-5}\right)\left(7, 3-\sqrt{-5}\right)$.

For $\left(2, 1+\sqrt{-5}\right)$, *suppose it is a principal ideal* (α) *and* $\alpha = a + b\sqrt{-5}$.

Then $\left|N_{\mathbb{Q}}^K(\alpha)\right| = \|(\alpha)\| = 2$.

So $a^2 + 5b^2 = 2$, *impossible by mod* 5.

Thus $\left(2, 1+\sqrt{-5}\right)$ *is not principal.*

Notice that $N\left(1+\sqrt{-5}\right) = 6$, i.e. $\left(1+\sqrt{-5}\right) = P_1P_2$ *with* $\|P_1\| = 2, \|P_2\| = 3$.

So one of the prime ideal lying over 3 *is the inverse of* $P_1 = \left(2, 1+\sqrt{-5}\right)$, *and the other one is equivalent to* P_1.

Similarly, $\left(3+\sqrt{-5}\right) = Q_1Q_2$ *with* $\|Q_1\| = 2, \|Q_2\| = 7$.

Moreover, since the inverse of $\left(2, 1+\sqrt{-5}\right)$ *is itself.*

Hence the ideal class group of R *is isomorphic to* $\mathbb{Z}/2\mathbb{Z}$.

Def 6.4.1. Let $\sigma_1, \ldots, \sigma_r$ be the embedding of K in $\mathbb{R}$ and $\tau_1, \bar{\tau}_1, \ldots, \tau_s, \bar{\tau}_s$ be the remaining embeddings of K in $\mathbb{C}$.

Consider a map

$$K \to \mathbb{R}^n : (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \operatorname{Re}\tau_1(\alpha), \operatorname{Im}\tau_1(\alpha), \ldots, \mathbb{R}\tau_s(\alpha), \operatorname{Im}\tau_s(\alpha)),$$

which maps R onto an n-dimensional lattice, denoted by $\wedge_R$.

Prop 6.4.1. *A fundamental parallelotope for this lattice has volume*

$$\operatorname{vol}(\mathbb{R}^n/\wedge_R) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(R)|}.$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of R.

Then the volume of fundamental parallelotope is

$$\begin{aligned}
&\det(\sigma_1(\alpha_i), \ldots, \sigma_r(\alpha_i), \operatorname{Re}\tau_1(\alpha_i), \operatorname{Im}\tau_1(\alpha_i), \ldots, \mathbb{R}\tau_s(\alpha_i), \operatorname{Im}\tau_s(\alpha_i)) \\
&= \frac{1}{(2i)^s}\det(\sigma_1(\alpha_i), \ldots, \sigma_r(\alpha_i), \tau_1(\alpha_i), \bar{\tau}_1(\alpha_i), \ldots, \tau_s(\alpha_i), \bar{\tau}_s(\alpha_i)) \\
&= \frac{1}{(2i)^s}\sqrt{\operatorname{disc}(R)}
\end{aligned}$$

And since the volume must be a positive real number.

So $\operatorname{vol}(\mathbb{R}^n/\wedge_R) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(R)|}$. □

Coro 6.4.3. *The image of* K *is dense in* $\mathbb{R}^n$.

Def 6.4.2. For each point $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, we set

$$N(x) = x_1 \cdots x_r \left(x_{r+1}^2 + x_{r+2}^2\right) \cdots \left(x_{n-1}^2 + x_n^2\right).$$

Thm 6.4.2 (Minkowski)**.** *Every* n*-dimensional lattice* $\wedge$ *in* $\mathbb{R}^n$ *contains a nonzero point* x *with*

$$|N(x)| \leqslant \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \operatorname{vol}(\mathbb{R}^n/\wedge).$$

Coro 6.4.4. *Every nonzero ideal I in R contains a element x with*

$$\left|N_{\mathbb{Q}}^{K}(\alpha)\right| \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(R)|}\|I\|.$$

Coro 6.4.5. *Every ideal class of R contains an ideal J with*

$$\|J\| \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(R)|}.$$

Exam 6.4.2. *Consider $R = \mathbb{Z}\left[\sqrt{-5}\right]$, there exists $\|J\| \leqslant \frac{4\sqrt{5}}{\pi} \approx 2.8$.*

Consider $R = \mathbb{Z}[\omega]$ with $e^{\frac{2\pi i}{5}}$, there exists $\frac{15\sqrt{5}}{2\pi^2} \approx 1.7$.

Coro 6.4.6. *For $R \neq \mathbb{Z}$, $|\mathrm{disc}(R)| \geqslant \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2s} > 1$.*

Thm 6.4.3 (Dirichlet)**.** *Let U be the group of units in a number ring $R = \mathbb{A} \cap K$, let r and $2s$ denote the number of real and non-real embeddings of K in $\mathbb{C}$, then U is the direct product $W \times V$ where W is a finite cyclic group consisting of the root of 1 in K and V is a free abelian group of rank $r + s - 1$. In other words, V consists of products*

$$u_1^{k_1} \cdots u_{r+s-1}^{k_{r+s-1}}, k_i \in \mathbb{Z}$$

for some set of $r + s - 1$ units $u_1, \ldots, u_{r+s-1}$ and such a set is called a fundamental system of units in R. The exponents $k_1, \ldots, k_{r+s-1}$ are uniquely determined for a given member of V.

Exam 6.4.3. *For imaginary quadratic case, U only contains the root of 1.*

For real quadratic case, the root of 1 are just ± 1 and the free abelian part of U has rank 1, i.e. *$U = \{\pm u^k | k \in \mathbb{Z}\}$ for some unit u, called a fundamental unit in R.*

6.5 The distribution of ideals in a number ring

Def 6.5.1. For each real number $t \geqslant 0$, let $i(t)$ be the number of ideals I of R with $\|I\| \leqslant t$. And for each ideal class C, let $i_C(t)$ denote the number of ideals I in C with $\|I\| \leqslant t$.

Thm 6.5.1. *There exists a number κ depending on R but independent of C such that*

$$i_C(t) = \kappa t + \varepsilon_C(t),$$

where the "error" $\varepsilon_C(t)$ is $O\left(t^{1-\frac{1}{n}}\right)$.

Coro 6.5.1. *$i(t) = h\kappa t + \varepsilon(t)$ where h is the number of ideal classes in R and $\varepsilon(t)$ is $O\left(t^{1-\frac{1}{n}}\right)$.*

Def 6.5.2. Let U be the group of units in R, consider mapping

$$U \subset R - \{0\} \to \wedge_R - \{0\} \xrightarrow{\log} \mathbb{R}^{r+s}$$

where $\log(x_1, \ldots, x_n) = \left(\log|x_1|, \ldots, \log|x_r|, \log|x_{r+1} + x_{r+2}i|^2, \ldots, \log|x_{n-1} + x_n i|^2\right)$. It maps U onto a lattice $\wedge_U \subset H \subset \mathbb{R}^{r+s}$ where $H = \{x_1 + \cdots + x_{r+s} = 0\}$. Let $v_1, \ldots, v_{r+s-1}$ be the basis of $\wedge_U$, then the regulator of R is define as the determinant of $(r + s) \times (r + s)$ matrix having $v_1, \ldots, v_{r+s-1}$ in the first $r + s - 1$ rows and $(\frac{1}{n}, \ldots, \frac{2}{n})$ (r number of $\frac{1}{n}$ and s number of $\frac{2}{n}$) in the last row, denoted by $\mathrm{reg}(R)$.

Thm 6.5.2. *Let w be the number of roots of 1 in K, then*

$$\kappa = \frac{2^{r+s}\pi^s \mathrm{reg}(R)}{w\sqrt{\mathrm{disc}(R)}}$$

Prop 6.5.1.

$$\mathrm{reg}(R) = \frac{\mathrm{vol}(H/\wedge_U)}{\sqrt{r+s}},$$

and if $v_1, \ldots, v_{r+s-1}$ *is the basis of* $\wedge_U$*, then* $\mathrm{reg}(R)$ *is the absolute value of the determinant obtained by deleting any column from the matrix having rows* $v_1, \ldots, v_{r+s-1}$*.*

Exam 6.5.1. *Consider* $R = \mathbb{Q}[\sqrt{m}]$ *with* $m > 0$ *and let* u *be the fundamental unit in* R*.*
Then $r = 2, s = 0$ *and* $v_1 = \left(\log u, \log \frac{1}{u}\right)$*.*
So $\mathrm{reg}(R) = \log(u)$ *and* $\kappa = \frac{2\log(u)}{\sqrt{\mathrm{disc}(R)}}$*.*
Consider $R = \mathbb{Z}\left[\sqrt[3]{2}\right]$*.*
Then $r = 1, s = 1$*, let* u *be the fundamental unit in* R *and* $\rho e^{\pm i\theta}$ *be its conjugates.*
So $u = \rho^{-2}$ *and* $\mathrm{disc}(u) = -4\sin^2\theta\left(\rho^3 + \rho^{-3} - 2\cos\theta\right)^2 < 4\left(u^3 + u^{-3} + 6\right)$*.*
Therefore $u^3 > \frac{|\mathrm{disc}(R)|}{4} - 7 = 20$*.*
And take $\beta = \frac{1}{\alpha - 1} = \alpha^2 + \alpha + 1$*.*
Then $\beta < 3\sqrt[3]{4} < 20^{\frac{2}{3}} < u^2$*,* i.e. $\beta = u$*.*
Hence $\mathrm{reg}(R) = \log(u)$ *and* $\kappa = \frac{4\pi\log(u)}{2\sqrt{108}} = \frac{\pi\log(u)}{3\sqrt{3}}$

Index