Introduction to Algebraic Number Theory (M2 2008–09)

Jan Nekovář

References: (1) Course of R. Schoof (see the brochure), especially the examples.

(2) J. Neukirch – Algebraic Number Theory (§ I.1–8, 10, 11, II.1–4, 7, 8, 9, III.2)

(3) J.W.C. Cassels, A. Fröhlich – Algebraic Number Theory (§ I.1–I.7, II.1–II.12, III, V.1)

(4) J.-P. Serre, Corps locaux (§ I.1–I.8)

Basic object of study: number fields (fields $K \supset \mathbb{Q}$ s.t. $[K:\mathbb{Q}] < \infty$) and their rings of integers $\mathcal{O}_K = \{\alpha \in K \mid \alpha$ is integral over $\mathbb{Z}\}$ ("α is an algebraic integer")

Recall: $A \subset B$ rings (commutative, with 1). We say that $b \in B$ is integral over A if $\exists$ monic polynomial $f \in A[x]$ s.t. $f(b) = 0$ ($b^n + a_1 b^{n-1} + \cdots + a_n = 0$, $a_i \in A$)

Ex: $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$

$K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$

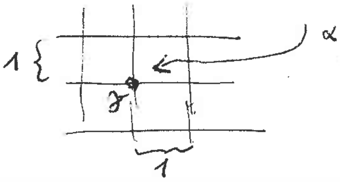
$K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z} + \frac{1+\sqrt{-3}}{2}\mathbb{Z}$

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$

$K = \mathbb{Q}(\zeta_n)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n] = \mathbb{Z} + \mathbb{Z}\zeta_n + \cdots + \mathbb{Z}\zeta_n^{\varphi(n)-1}$ $\quad (\zeta_n = e^{2\pi i/n})$

Prop. $\mathbb{Z}[i]$ is a euclidean domain w.r.t. the norm $N(\alpha) = \alpha\bar{\alpha}$ ($\alpha \in \mathbb{Z}[i]$):
$N(\alpha) \in \mathbb{N}$; $N(\alpha) = 0 \iff \alpha = 0$; $\forall \alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ $\exists \gamma \in \mathbb{Z}[i]$ $N(\alpha - \gamma\beta) < N(\beta)$

Pf. Take γ = the closest elt. of $\mathbb{Z}[i] \subset \mathbb{C}$ to $\alpha\beta^{-1} \in \mathbb{Q}(i) \subset \mathbb{C}$:



then $N(\alpha\beta^{-1} - \gamma) = |\alpha\beta^{-1} - \gamma|^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$

$\Rightarrow N(\alpha - \beta\gamma) < N(\beta)$.

Cor. $\mathbb{Z}[i]$ is a PID ($\Rightarrow$ UFD).

PID = principal ideal domain
UFD = unique factorisation domain

Prop. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD ($\Rightarrow$ is not a PID).

Pf. $\alpha = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ $(a, b \in \mathbb{Z})$; $N(\alpha) := \alpha\bar{\alpha} = a^2 + 5b^2$

$N(\alpha\beta) = N(\alpha)N(\beta)$

$\alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)}$

$\alpha \in \mathbb{Z}[\sqrt{-5}]^\times$ ($\iff \alpha^{-1} \in \mathbb{Z}[\sqrt{-5}]$) $\iff N(\alpha) \in \mathbb{Z}^\times = \{\pm 1\} \iff \alpha = \pm 1$

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

irreducible elements of $\mathbb{Z}[\sqrt{-5}]$

(if $1+\sqrt{-5} = \alpha\beta$, $\alpha, \beta \notin \mathbb{Z}[\sqrt{-5}]^\times$
$\Rightarrow 6 = N(\alpha)N(\beta)$
$\Rightarrow N(\alpha) = 2$, $N(\beta) = 3$ impossible)

Theorem.

Each $\mathcal{O}_K$ is a Dedekind ring: each non-zero ideal $I \subset \mathcal{O}_K$ has unique factorisation as $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, $\mathfrak{p}_i \subset \mathcal{O}_K$ distinct prime ideals (non-zero) ($a_i \geq 1$, $r \geq 0$)

this applies, in particular, to principal ideals

$(\alpha) = \alpha \mathcal{O}_K \qquad (\alpha \in \mathcal{O}_K,\ \alpha \neq 0).$

Ex: $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

$(2) = \mathfrak{p}^2$, $\quad \mathfrak{p} = (2, 1+\sqrt{-5})$

$(3) = \mathfrak{q}\mathfrak{q}'$, $\quad \mathfrak{q} = (3, 1+\sqrt{-5})$, $\mathfrak{q}' = (3, 1-\sqrt{-5})$

$(1+\sqrt{-5}) = \mathfrak{p}\mathfrak{q}$, $\quad (1-\sqrt{-5}) = \mathfrak{p}\mathfrak{q}'$

$\mathfrak{q}^2 = (-2+\sqrt{-5})$, $\mathfrak{q}'^2 = (2+\sqrt{-5})$

$$(6) = \mathfrak{p}^2\mathfrak{q}\mathfrak{q}' = \mathfrak{p}^2 \cdot \mathfrak{q}\mathfrak{q}' = \mathfrak{p}\mathfrak{q} \cdot \mathfrak{p}\mathfrak{q}'$$

"Arithmetic" part of the course: given a number field K,

- determine explicitly $\mathcal{O}_K$ $(= \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$, $n = [K:\mathbb{Q}])$
- determine $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid \alpha^{-1} \in \mathcal{O}_K\}$ (finitely gen. abelian gp)
- determine $Cl(\mathcal{O}_K) = \mathrm{Pic}(\mathcal{O}_K)$ = ideals / principal ideals (finite abelian group)

~~determine~~

Ex: $K = \mathbb{Q}$: $\mathcal{O}_K = \mathbb{Z}$, $\mathbb{Z}^\times = \{\pm 1\}$, $Cl(\mathbb{Z}) = \{1\}$

$K = \mathbb{Q}(i)$: $\mathcal{O}_K = \mathbb{Z}[i]$, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, $Cl(\mathbb{Z}[i]) = \{1\}$

$K = \mathbb{Q}(\sqrt{-5})$: $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$, $Cl(\mathbb{Z}[\sqrt{-5}]) \simeq \mathbb{Z}/2\mathbb{Z}$

- determine how a prime number p decomposes in $\mathcal{O}_K$:

$(p) = p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, $\quad \mathfrak{p}_i$ distinct prime ideals

($\Longleftrightarrow$ description of the Dedekind zeta function $\zeta_K(s)$ of K)

Ex: $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$:

$\alpha = a + bi \in \mathbb{Z}[i] \Rightarrow N(\alpha) = a^2 + b^2 \equiv 0, 1, 2 \pmod 4$

$N(\alpha\beta) = N(\alpha)N(\beta)$

- $p \equiv 3 \pmod 4$: p is irreducible in $\mathbb{Z}[i]$ $\quad$ ($N(p) = p^2$, $N(\alpha) \neq p \Rightarrow p \neq \alpha\beta$)
- $p = 2$: $2 = (1+i)^2 \cdot (-i)$
- $p \equiv 1 \pmod 4$: if $a \pmod p$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$ (cyclic of order $p-1$)

$\Rightarrow b := a^{\frac{p-1}{4}} \in \mathbb{Z}$ satisfies $p \mid (b^2+1) = (b+i)(b-i)$

As $p \nmid b \pm i$ in $\mathbb{Z}[i]$, p is not irreducible

$\Rightarrow p = \alpha\bar{\alpha}$, $\alpha = u + vi \in \mathbb{Z}[i]$, $u^2 + v^2 = p$.

Ex: $K=\mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K=\mathbb{Z}[\sqrt{-5}]$: $(2)=(2,1+\sqrt{-5})^2$, $(5)=(\sqrt{-5})^2$

$p\neq 2,5$: (p) is a prime ideal $\iff \left(\frac{-5}{p}\right)=-1 \iff p\equiv 11,13,17,19 \pmod{20}$

$(p)=\mathfrak{p}\mathfrak{p}' \iff \left(\frac{-5}{p}\right)=1 \iff p\equiv 1,3,7,9 \pmod{20}$

"Algebraic" part of the course: theory of Dedekind rings

Def. A noetherian integral domain A is a Dedekind ring if

$\iff \begin{cases} A \text{ is normal (each elt. of } \mathrm{Frac}(A) \text{ integral over } A \text{ lies in } A) \\ \text{and } \dim(A)\leq 1 \text{ (each non-zero prime ideal of } A \text{ is maximal).} \end{cases}$

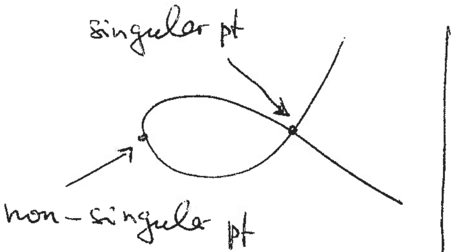
Fact: this is equivalent to:

$\dim(A)\leq 1$ and A is non-singular

Morally: A = the ring of functions on a non-singular geometric object of dim ≤ 1.

Fact: non-singularity is a local property (to be checked at each point)

$\Downarrow$



Local characterisation of Dedekind rings:

a noetherian domain A is a Dedekind ring $\iff \forall$ non-zero prime ideal $\mathfrak{p}\subset A$ the local ring $A_{\mathfrak{p}}$ is a PID ($\iff$ is a DVR)

("discrete valuation ring")

Ex. k field, $\underbrace{A=k[z]}_{\text{ring of functions on the affine line (defined over } k)}$ is a Dedekind ring (in fact, a PID)

Local study of Dedekind rings $\iff$ discrete valuations

In the geometric context, they correspond to points on non-singular projective curves (defined over k).

Over $k=\mathbb{C}$, such curves arise as compact Riemann surfaces.

Galois theory

let L/K be a field extension; set
$G = \mathrm{Aut}(L/K) := \{$ field automorphisms $\sigma : L \to L$ s.t. $\forall x \in K$ $\sigma(x) = x\}$
$(\Longrightarrow \quad K \subset L^G \subset L)$.

<u>Classical Galois theory</u>: if $[L:K] < \infty$, then:

(1) L/K is a (finite) Galois extension (with Galois group $\mathrm{Gal}(L/K) = G$)

$$\Updownarrow$$

$$K = L^G \Longleftrightarrow |G| = [L:K]$$

$$\Updownarrow$$

L/K is normal and separable.

(2) If this is the case, then there is a natural bijection

$$\left\{\begin{array}{c}\text{fields } E \\ K \subset E \subset L\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{subgroups} \\ H \subset G\end{array}\right\}$$

$$E \longmapsto \mathrm{Aut}(L/E) = \mathrm{Gal}(L/E)$$

$$L^H \longleftarrow H,$$

and E/K is a Galois extension $\Longleftrightarrow H \triangleleft G$ $(\Longrightarrow \mathrm{Gal}(E/K) = G/H)$

<u>Ex</u>: (1) $q = p^r$, $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a Galois extension

$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is <u>cyclic of order n</u>, generated by the (arithmetic) <u>Frobenius</u> over $\mathbb{F}_q$: $\sigma_q : x \longmapsto x^q$

(2) <u>If (char $(K) \nmid n$)</u>, set $\mu_n = \mu_n(\overline{K}) = \{x \in \overline{K} \mid x^n = 1\}$ (cyclic of order n)

($\overline{K}$ = a fixed algebraic closure of K)

there is a natural injective morphism of groups (the "<u>cyclotomic character</u>")

$$\chi_{n,K} : \mathrm{Gal}(K(\mu_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad \forall \zeta \in \mu_n \quad \sigma(\zeta) = \zeta^a$$

$$\sigma \longmapsto a$$

For $K = \mathbb{Q}$, $\chi_{n,\mathbb{Q}}$ is an <u>isomorphism</u>.

(3) <u>Kummer theory</u>: assume char $(K) \nmid n$, $\mu_n \subset K$. For any $a_1, \dots, a_r \in K^\times$, let $\Delta \subset K^\times/K^{\times n}$ be the subgroup generated by the images of $a_1, \dots, a_r$. Then $L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$ is a Galois extension of K (independent of the choice of the n-th roots) and the pairing

$$\mathrm{Gal}(L/K) \times \Delta \longrightarrow \mu_n$$

$$\sigma, a \longmapsto \sigma(\sqrt[n]{a})/\sqrt[n]{a}$$

(indep. of the choice of $\sqrt[n]{a}$) gives rise to an <u>isomorphism</u> of abelian groups $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Hom}_{Ab}(\Delta, \mu_n)$.

Infinite Galois theory

Let L/K be an algebraic field extension (possibly with $[L:K]=\infty$).
Set, as before, $G = Aut(L/K)$.

Theorem: (1) It is equivalent:

$L = \bigcup K'$, $K \subset K' \subset L$, $[K':K] < \infty$, K'/K Galois extension

$$\Updownarrow$$

$K = L^G \iff L/K$ is normal and separable.

(2) If this is the case, we say that L/K is a Galois extension (with Galois group $Gal(L/K) = G$). The fields K' from (1) then form a directed set(*) w.r.t. inclusions. The restriction maps

$$Aut(L/K) \xrightarrow{res_{L|K''}} \underbrace{Aut(K''/K)}_{Gal(K''/K)} \xrightarrow{res_{K''|K'}} \underbrace{Aut(K'/K)}_{Gal(K'/K)} \qquad (K \subset K' \subset K'' \subset L)$$

give rise to a morphism of ~~rings~~ groups

$$G = Aut(L/K) \longrightarrow \underbrace{\varprojlim_{K'} Gal(K'/K)}_{\text{compatible systems of elts of } Gal(K'/K) \text{ (via } res_{K''|K'})},$$

which is bijective.

(3) G has a natural topology, whose basis of open sets is given by $(res_{L|K'})^{-1}(\text{element of } \underbrace{Gal(K'/K)}_{\text{finite}})$

finite $\Rightarrow$ these (open) sets are also closed.

Equivalently, we take $G \xrightarrow{\sim} \underbrace{\varprojlim_{K'} Gal(K'/K)}_{\substack{\text{induced topology} \\ \text{of a closed subset} \\ \text{(compact Hausdorff)}}} \subset \underbrace{\prod_{K'} \underbrace{Gal(K'/K)}_{\substack{\text{finite set with} \\ \text{discrete topology}}}}_{\text{product topology (compact Hausdorff)}}$

"pro-finite topology on G"

(4) There is a canonical bijection

$$\left\{\begin{matrix}\text{fields } E \\ K \subset E \subset L\end{matrix}\right\} \longleftrightarrow \left\{\text{closed subgroups } H \subset G\right\}$$

$$E \longmapsto Aut(L/E) = Gal(L/E)$$

$$L^H \longleftarrow\!\shortmid H$$

(5) $[E:K] < \infty$

$$\Updownarrow$$

H is an open subgroup of G

(*) A non-empty partially ordered set $(I, <)$ is directed if $\forall i, j \in I \;\; \exists k \in I \;\; i < k$ and $j < k$

__Ex__: (1) Let $p_1, p_2, \dots,$ be an infinite set of __distinct prime numbers__, $L_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$,

$$\mathbb{Q} \subset L_1 \subset L_2 \subset \cdots \subset L := \bigcup_{n\geq 1} L_n = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots)$$

By Kummer theory, we have

$$\begin{array}{ccc} \mathrm{Gal}(L_{n+1}/\mathbb{Q}) & \xrightarrow{\sim} & \{\pm 1\}^{n+1} \\ \downarrow \mathrm{res}_{L_{n+1}|L_n} & & \downarrow \text{projection on the first } n \text{ factors} \\ \mathrm{Gal}(L_n/\mathbb{Q}) & \xrightarrow{\sim} & \{\pm 1\}^n \end{array}$$

$$\Rightarrow G = \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n \mathrm{Gal}(L_n/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n \{\pm 1\}^n = \prod_{n=1}^{\infty} \{\pm 1\}$$

(with the product topology: basis of open sets are $\emptyset$ and the sets ~~containing~~ $A \times \prod_{n>m} \{\pm 1\}$, for any $A \subset \prod_{n=1}^{m} \{\pm 1\}$ $(m \geq 1)$)

__Subfields $\mathbb{Q} \subset E \subset L$ with $[E:\mathbb{Q}] = 2$:__ $E = \mathbb{Q}(\sqrt{a_I})$,

$\emptyset \neq I \subset \{1, 2, \dots\}$ finite, $a_I = \prod_{i \in I} p_i$

$$H = \mathrm{Gal}(L/E) = \left\{ (\varepsilon_n)_{n\geq 1} \;\middle|\; \varepsilon_n = \pm 1, \prod_{i \in I} \varepsilon_i = 1 \right\} \subset G$$

is an open and closed subgroup of index $(G:H) = 2$.

$H \triangleleft G$ and $G/H \xrightarrow{\sim} \mathrm{Gal}(E/\mathbb{Q})$.

(!) __Warning__: $\exists$ __non-closed__ subgroups H' of G of index 2

($\Rightarrow$ the quotient topology on $G/H' \simeq \{\pm 1\}$ is __not__ Hausdorff)

__Proof__: G is a vector space over $\mathbb{F}_2$; $\exists$ $\mathbb{F}_2$-linear form $\alpha: G \longrightarrow \mathbb{F}_2$ which is non-zero on each factor $\{\pm 1\}$ of $G = \prod_{n=1}^{\infty} \{\pm 1\}$. Then $H' = \mathrm{Ker}(\alpha)$ satisfies (!)

__Ex__: (2) For each prime number p, the projective limit of

$$\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots$$

is the ring of __p-adic integers__

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{x = (x_n) \mid x_n \in \mathbb{Z}/p^n\mathbb{Z},\; x_{n+1} \equiv x_n \pmod{p^n}\}.$$

Its basis of open sets ($\Rightarrow$ closed) ~~those~~ is $\{x \in \mathbb{Z}_p \mid x_n \in A\}$ for fixed $n \geq 1$ and $A \subset \mathbb{Z}/p^n\mathbb{Z}$.

$\mathbb{Z}_p$ is compact and Hausdorff.

$\mathbb{Z}_p \ni x = \cdots b_n \cdots b_2 b_1 b_0$ $\quad b_i \in \{0, 1, \dots, p-1\}$ $\quad x = \sum_{i=0}^{\infty} b_i p^i$

$x = \cdots 2 \cdots 222 = -1 \in \mathbb{Z}_3$

(3) $\quad Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = (\mathbb{Z}/n\mathbb{Z})\sigma_q \quad , \quad \sigma_q(x) = x^q$

$\overline{\mathbb{F}_q} = \bigcup_{n\geq 1} \mathbb{F}_{q^n} \quad , \quad \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n} \Longleftrightarrow m \mid n$

$$\Downarrow$$

$$\begin{tikzcd} Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \arrow[r, "\sim"] \arrow[d, "res"] & (\mathbb{Z}/n\mathbb{Z})\sigma_q \arrow[d, "can"] & a \pmod n \arrow[d, mapsto] \\ Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) \arrow[r, equal] & (\mathbb{Z}/m\mathbb{Z})\sigma_q & a \pmod m \end{tikzcd}$$

$$Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \varprojlim_n Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \underbrace{\left(\varprojlim_n \mathbb{Z}/n\mathbb{Z}\right)}_{\hat{\mathbb{Z}}} \sigma_q$$

("pro-finite completion of $\mathbb{Z}$")

<u>Chinese remainder theorem:</u>

$n = p_1^{a_1} \cdots p_r^{a_r}$ (p_i distinct primes) $\Rightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}$

$$\Longrightarrow \quad \hat{\mathbb{Z}} \xrightarrow{\sim} \prod_{p \text{ prime}} \mathbb{Z}_p$$

$\left\{ \begin{array}{l} \cancel{\text{closed}}\ \text{open subgroups of} \\ \hat{\mathbb{Z}}\cdot\sigma_q \end{array} \right\} = \{(n\hat{\mathbb{Z}})\sigma_q\} \longleftrightarrow \left\{ \begin{array}{l} \text{fields } \mathbb{F}_{q^n} \\ \underbrace{\mathbb{F}_q \subset \mathbb{F}_{q^n}}_{\text{finite}} \subset \overline{\mathbb{F}_q} \end{array} \right\}$

---

(4) $\quad \mu_n = \mu_n(\mathbb{C}) = \{\sqrt[n]{1}\}$;

$$\begin{tikzcd} Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) \arrow[r, "\chi_n", "\sim"'] \arrow[d, "res"] & (\mathbb{Z}/n\mathbb{Z})^\times \arrow[d, "can"] & a \pmod n \arrow[d, mapsto] \\ Gal(\mathbb{Q}(\mu_m)/\mathbb{Q}) \arrow[r, "\chi_m", "\sim"'] & (\mathbb{Z}/m\mathbb{Z})^\times & a \pmod m \end{tikzcd}$$

$m \mid n$

$\mathbb{Q}(\mu_m) \subset \mathbb{Q}(\mu_n)$

$$\sigma(\zeta) = \zeta^{\chi_n(\sigma)} \qquad \forall \zeta \in \mu_n$$

$\mu_\infty = \bigcup_{n\geq 1} \mu_n \qquad Gal(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times \xrightarrow{\sim} \prod_{p \text{ prime}} \mathbb{Z}_p^\times$

p prime

$\mu_{p^\infty} = \bigcup_{n\geq 1} \mu_{p^n} \qquad Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times \quad (= \mathbb{Z}_p \setminus p\mathbb{Z}_p)$

---

(5) $\quad K^{sep} = \{x \in \overline{K} \mid x \text{ separable over } K\} \subset \overline{K} \qquad \overline{K}$ = a fixed algebraic closure of K

(the separable closure of K in $\overline{K}$)

$G_K = Gal(K^{sep}/K) \quad (= Aut(\overline{K}/K))$ – the absolute Galois group of K

<u>above</u>:

$$\begin{array}{ccc} G_{\mathbb{F}_q} & \xrightarrow{\sim} & \hat{\mathbb{Z}} \\ \cup\!\!\!\!\!\!\;\; \psi & & \psi \\ \sigma_q^a & \longleftrightarrow & a \end{array}$$

Valuations – examples

Algebraic number fields
Compact Riemann surfaces
Non-singular algebraic curves

$\Big\}$ very closely related

Ex: (1) $f \in \mathbb{C}(z)^\times$: $f = c\prod_{j=1}^{r}(z-z_j)^{m_j}$, $c \in \mathbb{C}^\times$, $z_j \in \mathbb{C}$ distinct, $r \geq 0$

z = variable

$z - z_j$ = a local parameter at z_j (coordinate)

$m_j = \mathrm{ord}_{z_j}(f) \in \mathbb{Z}$ (= order of zero of f at z_j if $m_j \geq 0$)

$f = \frac{g}{h}$, $g, h \in \mathbb{C}[z]$, $\deg(f) := \deg(g) - \deg(h) = \sum m_j$.

$$\boxed{\sum_{x \in \mathbb{C}} \mathrm{ord}_x(f) = \sum_j m_j = \deg(f)}$$

compactification: $\mathbb{C} \subset \mathbb{C} \cup \{\infty\}$ ("the Riemann sphere") $= \mathbb{P}^1(\mathbb{C})$ projective line over $\mathbb{C}$

local parameter at ∞ is $w = \frac{1}{z}$

$$f = c\prod_j\left(\frac{1}{w} - z_j\right)^{m_j} = c\, w^{-\sum m_j}\underbrace{\prod_j (1 - z_j w)^{m_j}}_{=1}$$ at $w = 0$ ($\Leftrightarrow z = \infty$)

$$\mathrm{ord}_\infty(f) = -\sum_j m_j = -\deg(f)$$

$$\boxed{\sum_{x \in \mathbb{P}^1(\mathbb{C})} \mathrm{ord}_x(f) = 0}$$

(2) $a \in \mathbb{Q}^\times$: $a = \pm\prod_{j=1}^{r} p_j^{m_j}$, p_j distinct prime numbers, $r \geq 0$

$m_j = \mathrm{ord}_{p_j}(a) \in \mathbb{Z}$

$$\boxed{\sum_{p \text{ prime}} \mathrm{ord}_p(a)\log(p) = \log|a|}$$

$\log = \log_e = \ln$

$$\boxed{\underbrace{|a|}_{\|a\|_\infty} \cdot \prod_{p \text{ prime}} \underbrace{p^{-\mathrm{ord}_p(a)}}_{\|a\|_p} = 1}$$

$a \longmapsto \|a\|_v$ valuations

$\cap$

$\mathbb{Q}^\times$

(3) $f \in k[z]^\times$: $\quad f = c \prod_{j=1}^{r} P_j^{m_j}$, $c \in k^\times$, P_j distinct monic irreducible polynomials (non-constant)

k field, z variable

$m_j = \mathrm{ord}_{P_j}(f) \in \mathbb{Z}$

$$\sum_P \mathrm{ord}_P(f)\deg(P) + \underbrace{(-\deg(f))}_{\mathrm{ord}_\infty(f)(\deg(\infty))} = 0 \qquad (\deg(\infty) = 1)$$

Fix $0 < \rho < 1$; define $\quad \|f\|_P := \rho^{\mathrm{ord}_P(f)\deg(P)}$, $\quad \|f\|_\infty := \rho^{\mathrm{ord}_\infty(f)(\deg(\infty))}$

$$\Rightarrow \quad \boxed{\|f\|_\infty \prod_P \|f\|_P = 1}$$

Goal: a unified treatment of (1)–(3)

$\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, $\{$prime numbers$\} \cup \{\infty\}$

$\{P \in k[z] \mid$ non-const. monic irreducible$\} \cup \{\infty\}$

ring A (PID)	$\mathbb{C}[z]$	$\mathbb{Z}$	$k[z]$
normalised irreducible elements	$z-x$ $(x \in \mathbb{C})$	p	P
$\mathrm{Max}(A) = \left\{\begin{matrix}\text{maximal ideals} \\ m \subset A\end{matrix}\right\}$	$(z-x)$	(p)	(P)
residue fields $k(m) = A/m$	$\mathbb{C}$	$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$	$k[z]/(P)$ field of degree $\deg(P)$ over k

$\mathrm{Max}(A) \longleftrightarrow$ (closed) points of a certain geometric object attached to A ("Spec(A)")

We must "compactify" it by adding "∞".

Ex: $A = k[z] = \{$regular functions on the affine line over $k\}$

$\mathrm{Frac}(A) = k(z) = \{$rational functions —— " ——$\}$

Algebraic terminology

A – ring (commutative, with 1), $I \subset A$ ideal

- A is a <u>domain</u> $\iff$ $A \neq 0$ and $[xy = 0$ in $A \Rightarrow x = 0$ or $y = 0]$
- $A^\times = \{x \in A \mid \exists y \in A \;\; xy = 1\}$ multiplicative group of units of A
- if $\alpha : A \longrightarrow A'$ is a ring homomorphism, then $\mathrm{Ker}(\alpha) = \alpha^{-1}(0)$ is an ideal of A (and each I arises in this way) and $A/\mathrm{Ker}(\alpha) \xrightarrow{\sim} \mathrm{Im}(\alpha)$
- I is <u>finitely generated</u> $\iff \exists a_1, \dots, a_n \in A$ $\;I = (a_1, \dots, a_n) = \{\sum_{i=1}^n a_i x_i \mid x_i \in A\}$
- I is <u>principal</u> if $I = (a) = aA$ for some $a \in A$
- A is <u>noetherian</u> $\iff$ each I is finitely generated
  $\iff$ each non-empty set of ideals has a maximal elt.
- $\sqrt{I} := \{x \in A \mid \exists n \geq 1 \;\; x^n \in I\}$ (the <u>radical</u> of I); it is also an ideal
- A is <u>reduced</u> if $\sqrt{(0)} = (0)$. $\quad$ [$\sqrt{(0)} = \{x \in A \mid \exists n \geq 1 \;\; x^n = 0\}$ is the <u>nilradical</u> of A]
- $I = \sqrt{I} \iff A/I$ is reduced
- A is a <u>PID</u> (principal ideal domain) $\iff$ A is a domain & each ideal is principal
- $a \mid b$ ("a divides b") $\iff \exists c \in A \;\; ac = b$ $\quad (a, b \in A)$
- $a \in A$ is <u>irreducible</u> $\iff [bc = a \Rightarrow b \in A^\times$ or $c \in A^\times$ $\quad (b, c \in A)]$
  $(a \neq 0,\; a \notin A^\times)$
- I is a <u>prime ideal</u> $\iff A/I$ is a domain $\iff [ab \in I \Rightarrow a \in I$ or $b \in I]$
  $\Uparrow$
- I is a <u>maximal ideal</u> $\iff A/I$ is a field $\iff A = (1)$ is the only ideal $\supsetneq I$
- $I \neq A \Rightarrow \exists$ maximal ideal $\supset I$
- $a \in A \smallsetminus A^\times \Rightarrow \exists$ maximal ideal $\ni a$ (take $I = (a)$ in)
- I, J ideals $\Rightarrow$ $I + J = \{x + y \mid x \in I, y \in J\}$
  $IJ = \{\sum_{i=1}^N x_i y_i \mid x_i \in I, y_i \in J, N \geq 0\}$ are ideals
- A domain $\Rightarrow [a \mid b \iff (a) \supseteq (b)]$ $\quad (a, b \in A)$
- $S \subset A$ is a <u>multiplicative subset</u> if $1 \in S$ and $[s, t \in S \Rightarrow st \in S]$;
  the <u>localisation of A at S</u> is the ring
  $S^{-1}A\;(= A_S) = \{\frac{a}{s} \mid a \in A, s \in S\}/\sim \;\;\Big|\;\; \frac{a}{s} \sim \frac{a'}{s'} \iff \exists s'' \in S \;\; s''(s'a - sa') = 0$
  $i_S : A \longrightarrow S^{-1}A$, $a \longmapsto \frac{a}{1}$ $\quad$, $i_S(s) \in (S^{-1}A)^\times \;\; \forall s \in S \;\Big|\; \mathrm{Ker}(i_S) = \{a \in A \mid \exists s \in S \;\; sa = 0\}$
- A domain $\Rightarrow (A \smallsetminus \{0\})^{-1}A = \mathrm{Frac}(A)$ is the <u>fraction field of A</u>
  $\Rightarrow$ if $0 \notin S$, $S^{-1}A = \{\frac{a}{s} \in \mathrm{Frac}(A) \mid s \in S, a \in A\} \subset \mathrm{Frac}(A)$
- $f \in A \Rightarrow \{f^n \mid n \geq 0\}$ is multiplicative, $A[1/f] := \{f^n \mid n \geq 0\}^{-1}A$

- A domain; a <u>fractional ideal of A</u> $:=$ subset $\alpha^{-1} I \subset \mathrm{Frac}(A)$, $\alpha \in A \smallsetminus \{0\}$, $(0) \neq I \subset A$ ideal
- $\{\text{ideals of } S^{-1}A\} = \{S^{-1}I \mid I \subset A \text{ ideal}\}$
- $\{\text{prime ideals of } S^{-1}A\} = \{S^{-1}I \mid I \subset A \text{ prime ideal s.t. } I \cap S = \emptyset\}$
- $\mathfrak{p} \subset A$ prime ideal $\Rightarrow$ $A \smallsetminus \mathfrak{p} \subset A$ is a multiplicative subset;
  $A_\mathfrak{p} := (A \smallsetminus \mathfrak{p})^{-1} A$ — the <u>localisation of A at $\mathfrak{p}$</u>
- (0) is a prime ideal $\Leftrightarrow$ A is a domain $\Rightarrow$ $A_{(0)} = \mathrm{Frac}(A)$

<u>Local rings</u>

<u>Def</u>: $(A, \mathfrak{m})$ is a <u>local ring</u> $\Leftrightarrow$ $\mathfrak{m}$ is the <u>unique maximal ideal of A</u>

($\Leftrightarrow$ $\mathfrak{m} \subset A$ is a maximal ideal & $A \smallsetminus \mathfrak{m} = A^\times$)

<u>Ex</u>: $\mathfrak{p} \subset A$ prime ideal $\Rightarrow$ $\{\text{prime ideals of } A_\mathfrak{p}\} = \{\underbrace{(A \smallsetminus \mathfrak{p})^{-1} I}_{I A_\mathfrak{p}} \mid I \subseteq \mathfrak{p} \text{ prime ideal of } A\}$

$\Rightarrow$ $(A_\mathfrak{p}, \mathfrak{p}A_\mathfrak{p})$ is a local ring.

<u>Ex</u>:

B	$\mathbb{Z}$	$\mathbb{C}[z] = \{\text{regular functions on } \mathbb{C}\}$
$\mathrm{Frac}(B)$	$\mathbb{Q}$	$\mathbb{C}(z) = \{\text{rational functions on } \mathbb{C}\}$
$\mathfrak{p} \subset B$ max. ideal	$\mathfrak{p} = (p)$, p prime	$\mathfrak{p} = (z - x)$, $x \in \mathbb{C}$
$A = B_\mathfrak{p}$	$\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$	$\mathbb{C}[z]_{(z-x)} = \{\frac{g}{h} \mid g, h \in \mathbb{C}[z], \underbrace{z - x \nmid h}_{h(x) \neq 0}\}$ $= \{\text{rational functions on } \mathbb{C} \text{ defined at } x\}$
$\mathfrak{m} = \mathfrak{p}B_\mathfrak{p}$	$p\mathbb{Z}_{(p)}$	$(z-x)\mathbb{C}[z]_{(z-x)} = \{\text{—''—} \mid f(x) = 0\}$
$\mathfrak{m} = \pi A$	$\pi = p$	$\pi = z - x$
$A^\times = A \smallsetminus \mathfrak{m}$	$\{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid a, p \nmid b\}$	$\{f \in \mathbb{C}(z) \mid f, \frac{1}{f} \text{ are defined at } x\}$ $= \{\frac{g}{h} \mid g, h \in \mathbb{C}[z], g(x), h(x) \neq 0\}$
$y \in \mathrm{Frac}(B)^\times$, $y = \pi^n u$, $u \in A^\times$, $n = \mathrm{ord}_\pi(y) \in \mathbb{Z}$	$y = p^n \frac{a}{b}$, $p \nmid a, p \nmid b$	$y = (z-x)^n \frac{g(z)}{h(z)}$, $g(x), h(x) \neq 0$

$yA = \pi^n A$ $\qquad A \smallsetminus \{0\} = \coprod_{n \geq 0} \pi^n A^\times$, $\qquad \mathrm{Frac}(A)^\times = \mathrm{Frac}(B)^\times = \coprod_{n \in \mathbb{Z}} \pi^n A^\times$

Discrete valuation rings (DVR)

Def. A DVR is a PID A with a unique non-zero prime ideal m.

$\Longrightarrow$ (A, m) is a local ring

$\overset{PID}{\Longrightarrow}$ $m = \pi A$ $(\pi \neq 0)$, π irreducible $\overset{UFD}{\Longrightarrow}$ fractional ideals of A are $\pi^n A$, $n \in \mathbb{Z}$

$$A \smallsetminus \{0\} = \coprod_{n \geq 0} \pi^n A^\times, \quad \mathrm{Frac}(A)^\times = \coprod_{n \in \mathbb{Z}} \pi^n A^\times$$

π (a uniformiser of A) is unique up to $A^\times$

Ex: (1) $A = \mathbb{Z}_{(p)}$, $\pi = p$ | (2) $A = \mathbb{C}[z]_{(z-x)}$, $\pi = z - x$

(3) $A = \mathbb{Z}_p$, $\pi = p$ | (4) $A = \mathbb{C}[[z]] = \{\sum_{n \geq 0} a_n z^n \mid a_n \in \mathbb{C}\}$, $\pi = z$

A defines a function (surjective)

$$v = \mathrm{ord}_A = \mathrm{ord}_\pi : \mathrm{Frac}(A) \longrightarrow \mathbb{Z} \cup \{\infty\}$$
$$\begin{cases} 0 \longmapsto \infty \\ \pi^n u \longmapsto n \end{cases} \qquad (u \in A^\times, n \in \mathbb{Z})$$

satisfying

(0) $v(x) = \infty \iff x = 0$

(1) $v(xy) = v(x) + v(y)$ $\qquad x, y \in \mathrm{Frac}(A)$

(2) $v(x+y) \geq \min(v(x), v(y))$

Discrete valuations

Def. A discrete valuation (additive, normalised) on a field K is a surjective function $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ satisfying (0), (1), (2).

Then: $A := \{x \in K \mid v(x) \geq 0\}$ is a DVR with maximal ideal $m = \{x \in A \mid v(x) \geq 1\}$ $(= \pi A$, for any $\pi \in K$ s.t. $v(\pi) = 1)$ and fraction field $\mathrm{Frac}(A) = K$.

Ex: $K = \mathbb{Q}$, $v = \mathrm{ord}_p$ (p prime) $\Longrightarrow$ $A = \mathbb{Z}_{(p)}$

Exercise. Let A be a DVR.

(1) If $x, y \in A$ and $v(x) \neq v(y)$, then $v(x+y) = \min(v(x), v(y))$.

(2) If $x_1, \ldots, x_n \in A$, $n \geq 2$, $x_1 + \cdots + x_n = 0$, then $\exists\, i \neq j$ s.t. $v(x_i) = v(x_j) = \min_{1 \leq k \leq n} v(x_k)$.

(3) Fractional ideals of A are $\pi^n A$ $(n \in \mathbb{Z}$, $v(\pi) = 1)$

$\forall a \in A \smallsetminus \{0\}$ $aA = \pi^n A$, $n = v(a)$

DVR's in geometry

Data:

- $k = \bar{k}$ algebraically closed field
- $f \in k[x,y]$ non-constant irreducible polynomial $\Big\} \Rightarrow$ irreducible

affine plane curve $C: f(x,y) = 0$.

Points of C: $K \supset k$ field, $C(K) := \{ \binom{x_0}{y_0} \in K^2 \mid f(x_0, y_0) = 0 \}$

Regular functions on C: elements of the ring $k[C] = k[x,y]/(f)$ ($k[C]$ is a domain, since f is irreducible). For $g \in k[x,y]$ denote by $\bar{g}$ its image in $k[C]$. If $P = \binom{x_0}{y_0} \in C(k)$, then $g(P)$ depends only on $\bar{g}$ (if $\bar{g} = \bar{h}$, then $g = h + ff_1 \overset{f(P)=0}{\Longrightarrow} g(P) = h(P)$); denote it by $\bar{g}(P)$. The evaluation map

$$ev_P: k[C] \longrightarrow k, \quad \bar{g} \longmapsto \bar{g}(P)$$

is a surjective morphism of k-algebras. Its kernel is equal to $\mathrm{Ker}(ev_P) = m_P = (\bar{x} - x_0, \bar{y} - y_0)$. As $k[C]/m_P \simeq k$, the ideal $m_P \subset k[C]$ is maximal.

Fact (special case of Hilbert's Nullstellensatz): the map

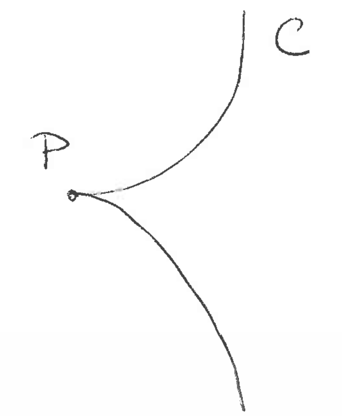
$$\begin{array}{ccc} C(k) & \longrightarrow & \{\text{maximal ideals of } k[C]\} \\ \Psi & & \Psi \\ P & \longmapsto & m_P \end{array}$$

is bijective.

Def. $P = \binom{x_0}{y_0} \in C(k)$ is a smooth point of C if

$$\frac{\partial f}{\partial x}(P) \neq 0 \quad \text{or} \quad \frac{\partial f}{\partial y}(P) \neq 0.$$

Ex: $P = \binom{0}{0}$ is not a smooth point of $C: y^2 - x^3 = 0$, but all the points of $C(k) \setminus \{P\}$ are smooth:



Def. The field of rational functions on C is $k(C) := \mathrm{Frac}(k[C])$.
If $f = \frac{\bar{g}}{\bar{h}} \in k(C)$ $\quad$ $(\bar{g}, \bar{h} \in k[C])$ and $\bar{h}(P) \neq 0$ $(P \in C(k))$, then f is defined at P (and $f(P) := \frac{\bar{g}(P)}{\bar{h}(P)} \in k$ is its value)

Theorem. Let $P = \binom{x_0}{y_0} \in C(k)$. Then:

(1) $A = k[C]_{m_P} = \{ f \in k(C) \mid f \text{ is defined at } P \}$

(2) If P is a smooth point of C, then A is a DVR. More precisely, if $\frac{\partial f}{\partial x}(P) \neq 0$ (resp., $\frac{\partial f}{\partial y}(P) \neq 0$), then $\overline{y} - y_0$ (resp., $\overline{x} - x_0$) is a uniformiser of A.

(3) If A is a DVR, then P is a smooth point of C.

Rmks: • "locally" around P, the geometry of C depends only on $k[C]_{m_P}$

• $\exists$ a similar thm for curves $\subset k^n$ over an arbitrary field k; in that case (2) holds always, (3) holds if k is perfect.

Proof. (1) this follows from the definitions ($\overline{h}(P) \neq 0 \Leftrightarrow \overline{h} \notin m_P$).

Replacing x, y by $x - x_0$, $y - y_0$, we can assume that $P = \binom{0}{0}$; then $m_P = (\overline{x}, \overline{y})$.

(3) If $A = k[C]_{(\overline{x}, \overline{y})}$ is a DVR with uniformiser $\pi \in A$, then $\pi A = \overline{x} A + \overline{y} A$, hence $v(\overline{x}), v(\overline{y}) \geq 1$ (with at least one equality). Say, $v(\overline{y}) = 1$. As $\pi A / \pi^2 A \simeq A/\pi = k$, $\exists\, \lambda \in k$ such that $v(\overline{x} - \lambda \overline{y}) \geq 2$, hence $\overline{x} - \lambda \overline{y} \in m_P^2 A \Longrightarrow$

$\exists\, h \in k[x,y]$ s.t. $h(0,0) \neq 0$ and $(\overline{x} - \lambda \overline{y}) \overline{h} \in m_P^2 = (\overline{x}, \overline{y})^2 k[C]$, hence $\exists\, g \in k[x,y]$ s.t. $(x - \lambda y) h - fg \in (x,y)^2 k[x,y] = (x^2, xy, y^2) k[x,y]$.

Taking $\frac{\partial}{\partial x}\Big|_{(0,0)}$, we get $0 \neq h(0,0) = g(0,0) \frac{\partial f}{\partial x}(0,0) \Rightarrow \frac{\partial f}{\partial x}(P) \neq 0$, so P is a smooth pt of C.

(2) A is a (noetherian) local domain with maximal ideal $m = (\overline{x}, \overline{y}) A$.

Lemma A (noetherian) local domain whose maximal ideal is principal is a DVR.

Pf. Exercise.

Assume $a := \frac{\partial f}{\partial x}(0,0) \neq 0$. We must show that $m = \overline{y} A$ (and then apply Lemma).

Write $f = ax + by + g(x,y)$, where $g \in (x^2, xy, y^2)\,k[x,y]$.

$\overline{f} = 0 \Longrightarrow \overline{x} = -a^{-1}(b\overline{y} + g(\overline{x},\overline{y})) \Longrightarrow \overline{x}A \subseteq (\overline{y}, \overline{x}^2)A$.

Set $N = mA/\overline{y}A = (\overline{x},\overline{y})A/\overline{y}A$. $\Downarrow$ Then

$N \supseteq \overline{x}N = (\overline{x}^2, \overline{x}\overline{y}, \overline{y})A/\overline{y}A = (\overline{x}^2, \overline{y})A/\overline{y}A \supseteq (\overline{x},\overline{y})A/\overline{y}A = N$,

so $N = \overline{x}N \underset{\overline{x}\in m}{\Longrightarrow} N = 0 \Longrightarrow mA = \overline{y}A$, as required.

<u>Nakayama Lemma</u>: Let B be a ring (commutative, with 1), $J \subset B$ an ideal s.t. $1 + J \subset B^\times$, N finitely generated B-module s.t. $JN = N$. Then $N = 0$.

(e.g., (B, J) = local ring).

<u>Pf.</u> $N = \sum_{i=1}^{r} Bn_i \underset{\#}{=} JN \Longrightarrow \exists\, b_{ij} \in J$ $\quad n_i = \sum_{j=1}^{r} b_{ij} n_j$

$$\underset{\substack{\cap \\ M_r(J)}}{(1_r - (b_{ij}))} \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in \underbrace{N \oplus \cdots \oplus N}_{r\text{-times}}$$

$$\Rightarrow \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \underbrace{\operatorname{adj}(1_r - (b_{ij}))(1_r - (b_{ij}))}_{\underbrace{\det(1_r - (b_{ij}))}_{\in 1 + J \subset B^\times} \cdot 1_r} \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} \Longrightarrow n_1 = \cdots = n_r = 0.$$

Integrality, finiteness, normalisation

$\boxed{\text{All rings are commutative, with } 1}$

Def. (1) Let $u: A \longrightarrow B$ be a morphism of rings.
B is finite over A $\Longleftrightarrow$ B is a finitely generated A-module (via u)

(2) An A-module M is faithful if the map $A \longrightarrow \mathrm{End}(M)$ is injective
$a \longmapsto (m \mapsto am)$

(3) The normalisation of A in a ring $B \supset A$ is $\{b \in B \mid b \text{ is integral over } A\}$

(4) A domain A is integrally closed ($=$ normal) if
$A =$ the normalisation of A in $\mathrm{Frac}(A)$.

(5) $B \supset A$ is integral over A if each $b \in B$ is integral over A.

Prop. Let $A \subset B$ be rings, $b \in B$. It is equivalent:
(1) b is integral over A $\Longleftrightarrow$ (2) $A[b] \subset B$ is a fin. generated A-module $\Longleftrightarrow$
$\Longleftrightarrow$ (3) $\exists$ faithful $A[b]$-module M which is ——— " ———

(Of course, $A[b] =$ the subring of B generated by A and b).

Proof: (1) $\Rightarrow$ (2) $b^n + a_1 b^{n-1} + \dots + a_n = 0$ $(a_i \in A) \Longrightarrow b^n \in \underbrace{Ab^{n-1} + \dots + Ab + A\cdot 1}_{N}$
By induction, $\forall m \geq n$ $b^m \in N \Longrightarrow A[b] = N$.
(2) $\Rightarrow$ (3) is automatic $(M = A[b])$
(3) $\Rightarrow$ (1) $M = \sum_{i=1}^{r} A m_i$, $b m_i = \sum_{j=1}^{r} a_{ji} m_j$ $(a_{ji} \in A)$
As in the proof of Nakayama's Lemma we get that the monic polynomial
$f(x) := \det(x \cdot 1_r - (a_{ji})) \in A[x]$ satisfies $f(b) m_i = 0$ $\forall i = 1, \dots, r$
$\Rightarrow f(b) m = 0$ $\forall m \in M \Longrightarrow f(b) = 0$ (as M is a faithful $A[b]$-module).

Corollary. Let $A \subset B \subset C$ be rings.
(1) The normalisation of A in B is a ring (containing A).
(2) If B is integral over A and C is integral over $B \Rightarrow C$ is integral over A.

Pf. (1) If $b, b' \in B$ are integral over A, $b^m \in Ab^{m-1} + \dots + Ab + A$
$b'^n \in Ab'^{n-1} + \dots + Ab' + A$
$\Longrightarrow N := \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} A b^i b'^j \subset B$ is an finitely generated over A $A[b, b']$-submodule
$\overset{\text{Prop.}}{\Longrightarrow}$ each element of $A[b, b']$ is integral over A.

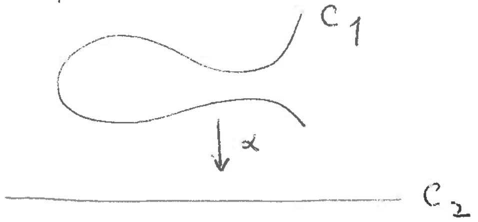
(2) $\forall c \in C$ $\cancel{\quad}$ $c^n + b_1 c^{n-1} + \dots + b_n = 0$, $b_i \in B$ ($\Rightarrow b_i$ integral over A)
$\forall m \geq n$ $c^m \in \underbrace{\sum_{i=0}^{n-1} A[b_1, \dots, b_n] c^i}_{M \text{ - fin. gen. over } A, \text{ by } (1)} \Longrightarrow A[c] = M$ $\Big\}$ $\overset{\text{Prop.}}{\Longrightarrow}$ c integral over A.

<u>Geometry</u>: any morphism of irreducible plane curves
$\alpha: C_1 \longrightarrow C_2$ (i.e., a polynomial map which sends $C_1(k)$ to $C_2(k)$)
defines a morphism of k-algebras

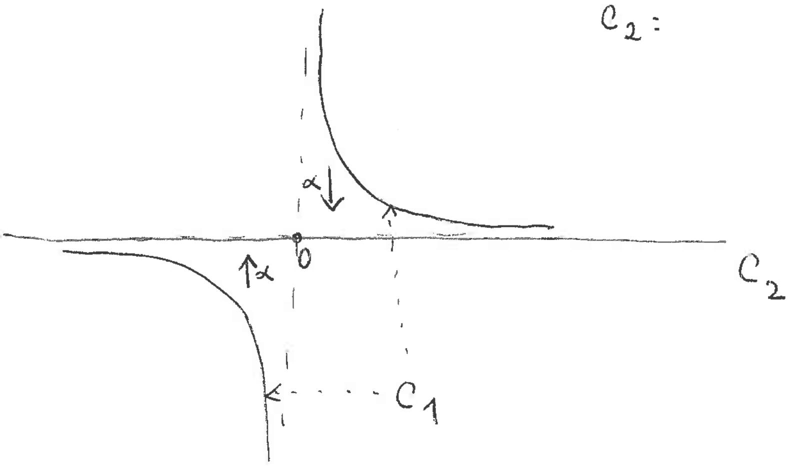
$$\begin{aligned} \alpha^*: k[C_2] &\longrightarrow k[C_1] \\ g &\longmapsto g\circ\alpha \end{aligned}$$

(and vice versa).

For <u>example</u>, if $C_1: f(x,y)=0$,
$C_2: y=0$ is the x-axis
and $\alpha: C_1 \longrightarrow C_2$, $\alpha(x,y)=(x,0)$ is the vertical projection,
then $\alpha^*: k[C_2]=k[x,y]/(y)=k[x] \longrightarrow k[C_1]=k[x,y]/(f)$
maps $x \longmapsto \bar{x}$

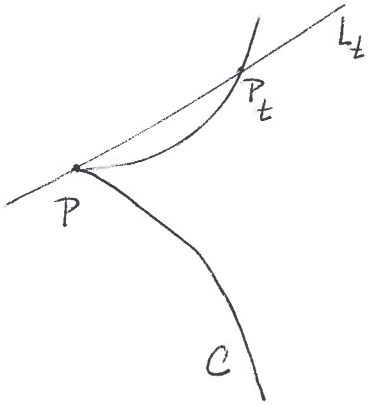


<u>Geometric example 1</u>: $C_1: xy-1=0$, $C_2: y=0$, $\alpha(x,y)=(x,0)$ is the vertical projection



- the morphism $\alpha^*: k[C_2]=k[x] \hookrightarrow k[C_1]=k[x,y]/(xy-1) \simeq k[x,\frac{1}{x}]$ is injective, but <u>not finite</u>: $k[x,\frac{1}{x}] = \sum_{n=1}^{\infty} \left(\frac{1}{x}\right)^n k[x]$
- $\bar{y}=\frac{1}{x} \in k[C_1]$ is <u>not integral</u> over $k[C_2]$
- α is <u>not finite in the geometric sense</u>: for $k=\mathbb{C}$,
  α^{-1}(a bounded neighbourhood of 0 in $C_2(\mathbb{C})$) is <u>not bounded</u> in $C_1(\mathbb{C})$

Geometric example 2 : $C : y^2 - x^3 = 0$ (over $k = \overline{k}$)



$k[C] = k[x,y]/(y^2 - x^3)$; $P = \begin{pmatrix}0\\0\end{pmatrix} \in C(k)$ is not a smooth point

For each $t \in k$, the line $L_t : y - tx = 0$ intersects C at P (with multiplicity 2) and at $P_t = \begin{pmatrix}t^2\\t^3\end{pmatrix}$. The map $t \longmapsto P_t$ is polynomial, hence comes from a morphism of curves

$\alpha : C_1$ (= line with coordinate t) $\longrightarrow C$.

The corresponding morphism between the rings of functions is given by

$$\alpha^* : k[C] = k[x,y]/(y^2 - x^3) \longrightarrow k[C_1] = k[t]$$
$$\overline{x} \longmapsto t^2$$
$$\overline{y} \longmapsto t^3$$

$\mathrm{Ker}(\alpha^*) = 0$, $\mathrm{Im}(\alpha^*) = k[t^2, t^3] = k + t^2 k[t] \subsetneq k[t]$. ($\exists$ algebraic map $t \mapsto \frac{\overline{y}}{\overline{x}}$ inverse to $\alpha : C_1(k) \setminus \{0\} \longrightarrow C(k) \setminus \{P\}$)

- the map α is a "desingularisation" of C
- α^* makes $k[C_1]$ into a normalisation of $k[C]$: $\frac{\overline{y}}{\overline{x}} \in \mathrm{Frac}(k[C])$ is integral over $k[C]$, $\frac{\overline{y}}{\overline{x}} \notin k[C]$

$\left(\left(\frac{\overline{y}}{\overline{x}}\right)^2 - \overline{x} = 0 \right)$ $\qquad \frac{\overline{y}}{\overline{x}} \downarrow t \in k[t]$

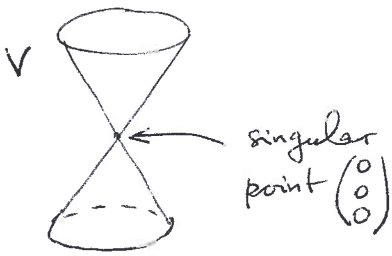
This is a special case of the following:

Facts : • in dim = 1, normality $\Longleftrightarrow$ non-singularity

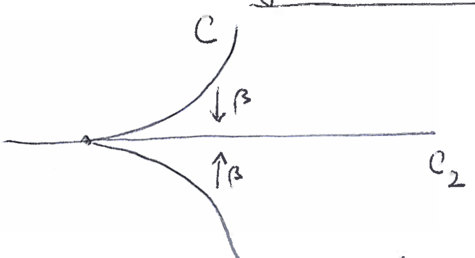
• in dim > 1, normality $\Longrightarrow$ codim (singular points) ≥ 2

Ex : $k = \overline{k}$, $\mathrm{char}(k) \neq 2$, the cone $V : x^2 + y^2 - z^2 = 0$ has dim = 2.

$k[V] = k[x,y,z]/(x^2+y^2-z^2)$ is a normal domain of dim = 2



Back to geometric example 2 : $C_2 : y = 0$ the x-axis



$\beta : C \longrightarrow C_2$ vertical projection (of degree 2)

$C_1 \xrightarrow{\alpha} C \xrightarrow{\beta} C_2$ correspond to

$$k[C_2] = k[x] \overset{\beta^*}{\hookrightarrow} \underbrace{k[C]}_{\text{free } k[C_2]\text{-module of rk}=2} = k[x,y]/(y^2 - x^3) \simeq k[t^2, t^3] \overset{\alpha^*}{\hookrightarrow} k[t] \overset{\shortparallel}{\;} k[C_1]$$

Arithmetic analogue : $\mathbb{Z} \hookrightarrow \mathbb{Z}[2i] = \mathbb{Z}[y]/(y^2+4) \hookrightarrow \mathbb{Z}[i]$ (normalisation of $k[C]$ / normalisation of $\mathbb{Z}[2i]$)

Dedekind rings

Recall: a *fractional ideal* in a domain A is a non-zero A-submodule $I \subset K = \mathrm{Frac}(A)$ s.t. $\exists\, a \in A \setminus \{0\}$ $\underbrace{aI \subset A}_{\text{ideal } J \text{ of } A}$ $(\Leftrightarrow I = a^{-1}J)$.

For $\alpha \in K^\times$, $(\alpha) := \alpha A$ is a *principal* fractional ideal.

Exercise: I, J fractional ideals of $A \Rightarrow$ so are $I+J$, IJ, $\{x \in K \mid xI \subset J\}$, $I^{-1} = \{x \in K \mid xI \subset A\}$.

Def. A fractional ideal I is *invertible* $\Leftrightarrow \exists$ fractional ideal J s.t. $IJ = A$ $(\Leftrightarrow II^{-1} = A)$.

Ex: $I = (\alpha)$ principal $\Rightarrow I^{-1} = (\alpha^{-1}) \Rightarrow II^{-1} = (1) = A \Rightarrow I$ invertible

---

Def. The (Krull) *dimension* of a ring A is

$$\dim(A) = \sup\{n \geq 0 \mid \exists \text{ prime ideals } I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_n \subset A\}$$

Morally, V algebraic variety of $\dim = d$ over $k \Rightarrow \dim k[V] = d$.

Ex: (1) A is a field $\Leftrightarrow A$ is a domain of $\dim(A) = 0$

(2) A is a PID $\Rightarrow$ if $(0) \neq I \subset A$ is a prime ideal, then $I = (\pi)$, π irreducible $\Rightarrow \dim(A) \leq 1$.

(3) A is a DVR $\Rightarrow \dim(A) = 1$.

(4) If A is a domain, then:
[$\dim(A) \leq 1 \Leftrightarrow$ a non-zero prime ideal is maximal]

(5) k field $\Rightarrow \dim k[T_1, \ldots, T_n] \geq n$ $\quad [(0) \subset (T_1) \subset \cdots \subset (T_1, \ldots, T_n)]$
(in fact, $= n$)

Prop. Let (A, m) be a local domain which is not a field. The following are equivalent:

(1) A is a DVR.

(2) A is a PID.

(3) A is noetherian and m is principal.

(4) Every fractional ideal of A is invertible.

(4') m is invertible.

(5) A is noetherian, normal and $\dim(A) = 1$.

Pf. $(1) \Rightarrow (2) \Rightarrow (3)$, $(1) \Rightarrow (4) \Rightarrow (4')$ are automatic.

$\left\{\begin{matrix} (4) \Rightarrow (2) \\ (4') \Rightarrow (3) \end{matrix}\right\}$ follow from the following Lemma (for $I = m$)

Lemma. A fractional ideal I of a local domain (A, m) is invertible $\Leftrightarrow I$ is principal.

Pf of Lemma: "$\Leftarrow$" is automatic.

"$\Rightarrow$" If $II^{-1}=A$, then $\exists\, x_j \in I$, $y_j \in I^{-1}$, $\sum_{j=1}^{r} x_j y_j = 1 \Rightarrow \exists j$ $x_j y_j \in A \setminus m = A^\times$; hence $(x_j)(y_j) = A$. We have $(x_j) \subset I$. If $(x_j) \subsetneq I$, then $A = (x_j)(y_j) \subsetneq I(y_j) \subset A$ – contradiction; thus $(x_j) = I$.

---

(3) $\Rightarrow$ (1): $m = (\pi)$, π irreducible. If $a \in m \setminus \{0\}$, then $\pi \mid a$.
Nakayama's lemma for $N = \bigcap_{n \geq 1} \pi^n A$ implies that $N = 0$, hence $\exists\, n \geq 1$ $\pi^n \mid a$, $\pi^{n+1} \nmid a$: $a \in \pi^n A^\times$. Thus $A = \{0\} \cup \coprod_{n \geq 0} \pi^n A^\times \Rightarrow (1)$.

(1) $\Rightarrow$ (5): A DVR $\Rightarrow$ A noetherian, $\dim(A) = 1$.
If $x \in \mathrm{Frac}(A) \setminus A$, then $v(x) < 0$. If $x^n + a_1 x^{n-1} + \dots + a_n = 0$, $a_i \in A$, then $1 = \underbrace{-(a_1 x^{-1} + \dots + a_n x^{-n})}_{y}$ and $v(y) > 0$ – contradiction; thus A is normal.

(5) $\Rightarrow$ (4'): We must show that $mm^{-1} \overset{?}{=} A$

Step 1. I fractional ideal $\underset{A \text{ noeth.}}{\Rightarrow}$ I is an A-module of finite type

$\Downarrow$

$E(I) = A$ $\underset{A \text{ normal}}{\Longleftarrow}$ $E(I) := \{x \in \mathrm{Frac}(A) \mid xI \subset I\}$ is integral over A

Step 2. $A \subset m^{-1} \Rightarrow m \subset mm^{-1} \subset A \Rightarrow mm^{-1} = \begin{cases} m \\ A \end{cases}$.
If $mm^{-1} = m$, then $m^{-1} \subset E(m) = A$.
So we must show that $A \overset{?}{\subsetneq} m^{-1}$

Step 3. The set of ideals $\{(0) \neq I \subset A \mid A \subsetneq I^{-1}\}$ is non-empty ($I = (a)$, $a \in m \setminus \{0\}$)
$\underset{}{\overset{A \text{ noeth.}}{\Longrightarrow}}$ $\exists$ maximal element I of this set.
We must show that I is a prime ideal ($\underset{\dim(A)=1}{\overset{I \neq (0)}{\Longrightarrow}}$ $I = m \Rightarrow A \subsetneq m^{-1}$)

Step 4. Assume $x, y \in A$, $xy \in I$, $x \notin I$. We must show that $y \overset{?}{\in} I$ ($\Rightarrow I$ prime ideal)
$x \notin I \Rightarrow (x) + I \supsetneq I \overset{\text{maximality}}{\Longrightarrow} ((x)+I)^{-1} = A$
$\forall z \in I^{-1}$ $\quad zy((x)+I) \subset I^{-1}I + yI^{-1}I \subset A \Rightarrow zy \in ((x)+I)^{-1} = A$
$\Rightarrow z((y)+I) \subset A \underset{I^{-1} \supsetneq A}{\Longrightarrow} ((y)+I)^{-1} \neq A \overset{\text{maximality}}{\Longrightarrow} (y)+I = I \Rightarrow y \in I$.

Theorem – Definition. A Dedekind ring is a domain A satisfying the following equivalent conditions.

(1) A is noetherian, normal and $\dim(A) \leq 1$ [A = field is allowed]

(2) A is noetherian and for each non-zero prime ideal $\mathfrak{p} \subset A$, $A_\mathfrak{p}$ is a DVR.

(3) All fractional ideals of A are invertible.

Pf. (1) $\Rightarrow$ (2): Let $(0) \neq \mathfrak{p} \subset A$ be a prime ideal ($\Rightarrow \dim(A_\mathfrak{p}) \geq 1$)
A satisfies (1) $\Rightarrow$ $A_\mathfrak{p}$ satisfies (1) $\overset{\text{Prop.}}{\Longrightarrow}$ $A_\mathfrak{p}$ is a DVR.

(3) $\Rightarrow$ (2): Let $(0) \neq \mathfrak{p} \subset A$ be a prime ideal ($\Rightarrow \dim(A_\mathfrak{p}) \geq 1$)
A satisfies (3) $\Rightarrow$ $A_\mathfrak{p}$ satisfies (3) $\overset{\text{Prop.}}{\Longrightarrow}$ $A_\mathfrak{p}$ is a DVR.

(2) $\Rightarrow$ (3): given a fractional ideal I of A, $\forall\, (0) \neq \mathfrak{p} \subset A$ prime ideal
$IA_\mathfrak{p}$ is a fractional ideal of $\underset{\text{DVR}}{A_\mathfrak{p}}$ $\Rightarrow (II^{-1})A_\mathfrak{p} = (IA_\mathfrak{p})(IA_\mathfrak{p})^{-1} = A_\mathfrak{p}$

$\Rightarrow$ $II^{-1} \not\subset \mathfrak{p}$ for each maximal ideal $\mathfrak{p} \subset A$ $\Rightarrow$ $II^{-1} = A$.

(3) $\Rightarrow$ (1): $(0) \neq I \subset A$ ideal $\Rightarrow II^{-1} = A \Rightarrow \exists\, a_j \in I,\ b_j \in I^{-1},\ \sum_{j=1}^{r} a_j b_j = 1$

$\forall x \in I \quad x = \sum_{j=1}^{r} a_j(b_j x) \in \sum_{j=1}^{r} A a_j \Rightarrow I = (a_1, \dots, a_r)$ is finitely gen. $\Rightarrow$ A is noetherian

If $x \in \mathrm{Frac}(A)$ is integral over A, then $B = A[x] \supset A$ is a fractional ideal and a ring; thus $BB = B$ and
$B = BA \overset{(3)}{=} BBB^{-1} = BB^{-1} \overset{(3)}{=} A \Rightarrow A$ is normal

Let $(0) \neq I$ be a prime ideal, $\mathfrak{m} \supseteq I$ a maximal ideal

$(I\mathfrak{m}^{-1})\mathfrak{m} = I \Rightarrow \begin{cases} I\mathfrak{m}^{-1} \subset I \\ \text{or} \\ \mathfrak{m} \subset I \Rightarrow I = \mathfrak{m} \text{ is maximal} \end{cases}$

If $I\mathfrak{m}^{-1} \subset I \overset{(3)}{\Longrightarrow} \mathfrak{m}^{-1} = I^{-1}I\mathfrak{m}^{-1} \subset I^{-1}I = A \overset{(3)}{\Longrightarrow} A \subset \mathfrak{m}$ – contradiction

$\Rightarrow$ I maximal ideal $\Downarrow$ $\dim(A) \leq 1$

Ex: (1) any PID is a Dedekind ring

(2) $A = k[C]$ ———— " ————, $k = \bar{k}$, C irreducible plane curve whose all points are smooth

---

Corollary / Definition. The fractional ideals of a Dedekind ring A form a group $I(A)$ with respect to multiplication. The principal fractional ideals form a subgroup $P(A) \subset I(A)$. The quotient group $I(A)/P(A) = Cl(A) = \mathrm{Pic}(A)$ is the ideal class group of A. (= the Picard group of A) There is an exact sequence

$$1 \longrightarrow A^\times \longrightarrow \mathrm{Frac}(A)^\times \longrightarrow I(A) \longrightarrow \mathrm{Pic}(A) \longrightarrow 1$$
$$\alpha \longmapsto (\alpha)$$

Remarks on invertible ideals

A = integral domain, I, J fractional ideals of A

Def. I is equivalent to J (notation: $I \sim J$) if $\exists\, \alpha \in \mathrm{Frac}(A)^\times$ $\alpha I = J$

Prop. $I \sim J \iff I$ and J are isomorphic as A-modules

(in particular, I is principal $\iff I \sim (1) = A \iff I$ is free (of rk $=1$) over A)

Pf. An isomorphism of A-modules $f: I \xrightarrow{\sim} J$ extends to an isomorphism of $\mathrm{Frac}(A)$-vector spaces $f \otimes \mathrm{id}: I \otimes_A \mathrm{Frac}(A) = \mathrm{Frac}(A) \xrightarrow{\sim} J \otimes_A \mathrm{Frac}(A) = \mathrm{Frac}(A)$, which must be given by multiplication by some $\alpha \in \mathrm{Frac}(A)^\times$, hence $\alpha I = J$. The converse is obvious.

Prop. Let $S \subset A$ be a multiplicative subset s.t. $0 \notin S$ ($\Rightarrow S^{-1}A \neq 0$).

(1) $(S^{-1}I)^{-1} = S^{-1}(I^{-1})$ is a fractional ideal of $S^{-1}A$

(2) I invertible $\Longrightarrow$ $S^{-1}I$ invertible (over $S^{-1}A$)

(3) I is invertible $\iff$ $\forall\, \mathfrak{p} \subset A$ prime ideal $I_\mathfrak{p}$ $(= IA_\mathfrak{p})$ is invertible over $A_\mathfrak{p}$
$\iff$ $\forall\, \mathfrak{m} \subset A$ maximal ideal $I_\mathfrak{m}$ — " — $A_\mathfrak{m}$.
$\iff$ — " — $I_\mathfrak{m}$ is principal.

Pf. (1) Exercise. (2) $IJ = A \Rightarrow (S^{-1}I)(S^{-1}J) = S^{-1}A$.

(3) Both "$\Rightarrow$" follow from (2). Assume I not invertible, $I \subset A$. Then $II^{-1} \subsetneq A \Rightarrow \exists\, \mathfrak{m} \subset A$ max. ideal $II^{-1} \subset \mathfrak{m} \Rightarrow I_\mathfrak{m}(I^{-1})_\mathfrak{m} \overset{(1)}{=} I_\mathfrak{m}(I_\mathfrak{m})^{-1} \subset \mathfrak{m}A_\mathfrak{m} \subsetneq A_\mathfrak{m}$
$\Rightarrow I_\mathfrak{m}$ is not invertible over $A_\mathfrak{m}$.

We already know that $I_\mathfrak{m}$ is invertible over $A_\mathfrak{m} \iff I_\mathfrak{m}$ is principal.

Ex: (1) $A = k[x,y]$, k field: which prime ideals I are invertible?

$I = (0)$ not a fractional ideal

$I = (f)$ ($f \in A$ non-const. irreducible) $I \sim (1) \Rightarrow I$ invertible

($k = \bar{k}$) $I = (x - x_0, y - y_0) = \mathfrak{m}_P$ (maximal ideal attached to $P = \binom{x_0}{y_0} \in k^2$)

$\mathfrak{m}_P^{-1} = A \Longrightarrow \mathfrak{m}_P \mathfrak{m}_P^{-1} = \mathfrak{m}_P \neq A$ $\quad \mathfrak{m}_P$ not invertible

[invertibility is a "codimension $=1$" phenomenon].

(2) Let $k = \bar{k}$. A prime ideal $\mathfrak{q} \subset k[x_1, \dots, x_n]$ defines an irreducible algebraic variety $V \subset k^n$ given by the equations $V: f(x_1, \dots, x_n) = 0$, $f \in \mathfrak{q}$. $(V = Z(\mathfrak{q}))$

Its ring of regular functions $k[V] = k[x_1, \dots, x_n]/\mathfrak{q}$ is a domain; the fraction field $k(V) = \mathrm{Frac}(k[V])$ is the field of rational functions on V.

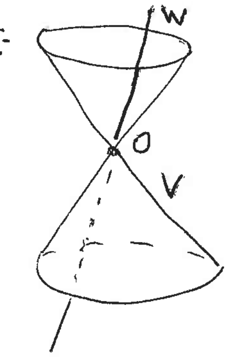
$\{$prime ideals $I \subset k[V]\} \overset{\text{bij.}}{\longleftrightarrow} \{$prime ideals $\mathfrak{p} \subset k[x_1, \dots, x_n]$, $\mathfrak{p} \supset \mathfrak{q}\} \ni \mathfrak{p}$

$I = \mathfrak{p}/\mathfrak{q} \longleftarrow \mathfrak{p}$ $\qquad \Updownarrow$ bijection

$\{$irreducible subvarieties $W \subset V\} \ni Z(\mathfrak{p})$

$k[W] = k[x_1, \dots, x_n]/\mathfrak{p} = k[V]/I$

Ex:



char$(k) \neq 2$, V = the cone: $x^2 + y^2 - z^2 = 0$

W = the line: $x = y - z = 0$

O = the point: $x = y = z = 0$

$A = k[V] = k[x,y,z]/(x^2+y^2-z^2) \supset I = (\bar{x}, \bar{y} - \bar{z}) \subset \mathfrak{m}_O = (\bar{x}, \bar{y}, \bar{z}) = \mathfrak{m}$

Fact: $I_\mathfrak{m} \subset A_\mathfrak{m}$ is not principal ($\Rightarrow O$ is a singular point of V)

Unique factorisation of ideals

Thm. Let A be a Dedekind ring ($\Longrightarrow \mathrm{Max}(A) = \{$non-zero prime ideals $\mathfrak{p} \subset A\}$).
Every non-zero ideal $I \subset A$ (resp., a fractional ideal I) admits a unique factorisation $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$, where $r \geq 0$, $\mathfrak{p}_i \in \mathrm{Max}(A)$ are distinct, and $n_i \geq 1$ (resp. $n_i \in \mathbb{Z}$).

Pf. Uniqueness: $\mathfrak{p} \neq \mathfrak{q} \in \mathrm{Max}(A) \Longrightarrow \mathfrak{p} + \mathfrak{q} = A \Longrightarrow \exists\, x \in \mathfrak{q} \cap (1 + \mathfrak{p}) \subset \mathfrak{q} \cap A_{\mathfrak{p}}^{\times}$

$\forall n \geq 0$ $\quad x^n A \subset \mathfrak{q}^n \subset A \Rightarrow A_{\mathfrak{p}} = x^n A_{\mathfrak{p}} \subset (\mathfrak{q}^n)_{\mathfrak{p}} = \mathfrak{q}^n A_{\mathfrak{p}} \subset A_{\mathfrak{p}} \Rightarrow \mathfrak{q}^n A_{\mathfrak{p}} = A_{\mathfrak{p}},\ \mathfrak{q}^{-n} A_{\mathfrak{p}} = (\mathfrak{q}^n A_{\mathfrak{p}})^{-1} = A_{\mathfrak{p}}$.

So, if $I = \prod_{\mathfrak{p} \in \mathrm{Max}(A)} \mathfrak{p}^{n(\mathfrak{p})}$ (finite product), then $I A_{\mathfrak{p}} = \mathfrak{p}^{n(\mathfrak{p})} A_{\mathfrak{p}} = (\mathfrak{p} A_{\mathfrak{p}})^{n(\mathfrak{p})}$

$\Rightarrow$ $n(\mathfrak{p})$ depends only on I and $\mathfrak{p}$.

Existence: enough for $(0) \neq I \subset A$. If $I = A$, take $r = 0$. If $I \subsetneq A$, $\exists\, \mathfrak{p}_1 \in \mathrm{Max}(A)$, $\mathfrak{p}_1 \supset I$
$\Rightarrow I = \mathfrak{p}_1 (\mathfrak{p}_1^{-1} I) = \mathfrak{p}_1 I_1$, $\quad I_1 = \mathfrak{p}_1^{-1} I \subset \mathfrak{p}_1^{-1}\mathfrak{p}_1 = A$. Apply the same procedure to I_1: get $I_1 = A$ or $I_1 = \mathfrak{p}_2 I_2$, so either $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, or $\exists$ infinite sequence of $\mathfrak{p}_i \in \mathrm{Max}(A)$ s.t. $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r I_r$, $\quad I_r \subset A \Rightarrow \mathfrak{p}_1 \supsetneq \mathfrak{p}_1\mathfrak{p}_2 \supsetneq \cdots \supset I$
$\Rightarrow \mathfrak{p}_1^{-1} \subsetneq \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \subsetneq \cdots \subset I^{-1}$ – impossible, as I^{-1} is a noetherian A-module.

Corollary (of proof). For each fractional ideal I and $\mathfrak{p} \in \mathrm{Max}(A)$, define $v_{\mathfrak{p}}(I) \in \mathbb{Z}$ by $I A_{\mathfrak{p}} = (\mathfrak{p} A_{\mathfrak{p}})^{v_{\mathfrak{p}}(I)}$. Then all but finitely many $v_{\mathfrak{p}}(I)$ are zero, and $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$. Clearly, $v_{\mathfrak{p}}(IJ) = v_{\mathfrak{p}}(I) + v_{\mathfrak{p}}(J)$.
For $\alpha \in \mathrm{Frac}(A)^{\times}$, set $v_{\mathfrak{p}}(\alpha) := v_{\mathfrak{p}}((\alpha))$.

Prop. For fractional ideals I, J of a Dedekind ring A define $I \mid J :=\ \exists$ non-zero ideal $I' \subset A$ s.t. $II' = J$. Then:

(1) $I \mid J \iff J \subset I \iff \forall \mathfrak{p} \in \mathrm{Max}(A)$ $\quad v_{\mathfrak{p}}(I) \leq v_{\mathfrak{p}}(J)$

(2) $v_{\mathfrak{p}}(I + J) = \min(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$ $\quad (\Longrightarrow I + J = \gcd(I, J))$

(3) $v_{\mathfrak{p}}(I \cap J) = \max(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$ $\quad (\Longrightarrow I \cap J = \mathrm{lcm}(I, J))$

(4) $\forall \mathfrak{p} \in \mathrm{Max}(A)$ $\quad \{0\} \cup \{\alpha \in \mathrm{Frac}(A)^{\times} \mid v_{\mathfrak{p}}(\alpha) \geq 0\} = A_{\mathfrak{p}}$

(5) $\bigcap_{\mathfrak{p} \in \mathrm{Max}(A)} A_{\mathfrak{p}} = A$, $\quad \bigcap_{\mathfrak{p}} I A_{\mathfrak{p}} = I$.

Pf. (1) $J \subset I \Rightarrow I^{-1} J \subset I^{-1} I = A \Rightarrow I(I^{-1}J) = J$; $\quad II' = J,\ I' \subset A \Rightarrow J \subset IA = I$.
So $I \mid J \iff I^{-1} J \subset A \Rightarrow \forall \mathfrak{p}$ $\quad v_{\mathfrak{p}}(I^{-1}J) \geq 0 \Rightarrow v_{\mathfrak{p}}(J) \geq v_{\mathfrak{p}}(I)$.
If $\forall \mathfrak{p}$ $\quad v_{\mathfrak{p}}(I) \leq v_{\mathfrak{p}}(J)$, then $I' = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(J) - v_{\mathfrak{p}}(I)} \subset A$ (the product is finite) and $II' = J$.

(2), (3) In the DVR $A_{\mathfrak{p}}$, $(\pi^m) + (\pi^n) = (\pi^{\min(m,n)})$, $\quad (\pi^m) \cap (\pi^n) = (\pi^{\max(m,n)})$
($\pi \in A_{\mathfrak{p}}$ uniformiser)

(4) Follows from the definition of $v_{\mathfrak{p}}$.

(5) "$\supset$" is clear. If $0 \neq \alpha \in \bigcap_{\mathfrak{p}} I A_{\mathfrak{p}}$, then $\forall \mathfrak{p}$ $\quad v_{\mathfrak{p}}(\alpha) \geq v_{\mathfrak{p}}(I) \Rightarrow (\alpha) = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)} \subset \underbrace{I}_{\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}} \Rightarrow \alpha \in I$.

Def. The <u>divisor group</u> of A is the free abelian group on $\mathrm{Max}(A)$:

$$\mathrm{Div}(A) = \bigoplus_{\mathfrak{p}\in \mathrm{Max}(A)} \mathbb{Z}\cdot[\mathfrak{p}].$$

Thm above can be reformulated by saying that the map

$$(v_{\mathfrak{p}}): \quad I(A) \xrightarrow{\sim} \mathrm{Div}(A), \qquad I \longmapsto \sum_{\mathfrak{p}} v_{\mathfrak{p}}(I)[\mathfrak{p}]$$

is an <u>isomorphism</u> of abelian groups (inverse: $\sum n_{\mathfrak{p}}[\mathfrak{p}] \mapsto \prod \mathfrak{p}^{n_{\mathfrak{p}}}$)

Prop. For a Dedekind ring A, it is equivalent:

$$\mathrm{Pic}(A)=0 \overset{(1)}{\iff} A \text{ is a PID} \overset{(2)}{\iff} A \text{ is a UFD}.$$

Pf. $\overset{(1)}{\iff}$ holds by definition; $\overset{(2)}{\implies}$ holds for any domain.

$\overset{(2)}{\impliedby}$: If A is a UFD, let $\mathfrak{p}\in \mathrm{Max}(A)$; fix $\alpha\in\mathfrak{p}\setminus\{0\}$. Then

$\mathfrak{p} \mid (\alpha) = (\pi_1)\cdots(\pi_r)$, where $\pi_i\in A$ are irreducible elements of A ($r\geq 1$, since $\alpha\notin A^\times$). Each (π_i) is a non-zero prime ideal

$\implies \exists i \quad \mathfrak{p} = (\pi_i)$, so $\mathfrak{p}$ is principal.

Chinese Remainder Theorem. (1) Let B be a ring, $I, J\subset B$ ideals such that $I+J=B$. Then $B/(I\cap J) \xrightarrow{\text{can}} B/I\times B/J$ is a ring isomorphism.

(2) If A is a Dedekind ring and $(0)\neq I, J\subset B$ ideals s.t. $\gcd(I,J)=(1)$, then

can: $A/IJ \xrightarrow{\sim} A/I\times A/J$ is a ring isomorphism.

In particular, if $\mathfrak{p}_i$ are distinct maximal ideals, then

$$A/\mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_r^{n_r} \xrightarrow{\sim} A/\mathfrak{p}_1^{n_1}\times\cdots\times A/\mathfrak{p}_r^{n_r}.$$

Pf: (1) $\alpha: B \longrightarrow B/I\times B/J$, $b \longmapsto (b \pmod I, b \pmod J)$ is a ring morphism, $\mathrm{Ker}(\alpha) = I\cap J$.

$I+J=B \implies \exists\, i\in I, j\in J \quad i+j=1 \implies \forall x,y\in B \quad (x \pmod I, y \pmod J) = \alpha(jx+iy) \implies \alpha$ is surjective.

(1) $\implies$ (2): $I\cap J = IJ$, since $\gcd(I,J)=(1)$.

Prop. Let A be a Dedekind ring an X an A-module of finite type.

(1) If X is torsion, then $X\simeq \bigoplus_{i=1}^{k} A/\mathfrak{p}_i^{n_i}$ ($\mathfrak{p}_i\in\mathrm{Max}(A)$, not necess. distinct)

(2) If X is torsion-free, then X is projective, $\exists$ ideals ($\neq 0$) $I_1,\dots,I_r\subset A$ s.t.

$$X\simeq \bigoplus_{i=1}^{r} I_i \simeq A^{r-1}\oplus(I_1\cdots I_r), \qquad \forall \mathfrak{p}\in\mathrm{Max}(A) \quad X_{\mathfrak{p}}\simeq A_{\mathfrak{p}}^{r} \text{ is free over } A_{\mathfrak{p}}.$$

(3) $X\simeq X_{\mathrm{tors}}\oplus(X/X_{\mathrm{tors}})$

Pf: Exercise.

Prop. Let A be a Dedekind ring, $\mathfrak{p}_1,\dots,\mathfrak{p}_r\in\mathrm{Max}(A)$, $n_1,\dots,n_r\in\mathbb{N}$. Given $x_1,\dots,x_r\in\mathrm{Frac}(A)$, $\exists\, x\in\mathrm{Frac}(A)$ $\forall i=1,\dots,r \quad v_{\mathfrak{p}}(x-x_i)\geq n_i$.

Pf: Exercise.

Discriminant, trace, norm

Polynomials: $f(T) = T^n + a_1 T^{n-1} + \dots + a_n = (T - x_1) \cdots (T - x_n)$

$\exists!$ polynomial $\mathrm{disc}(f) \in \mathbb{Z}[a_1, \dots, a_n]$ s.t. $\mathrm{disc}(f) = \prod_{1 \le i < j \le n} (x_i - x_j)^2$

Ex: $\mathrm{disc}(T^2 + aT + b) = a^2 - 4b$

Finite free algebras: $A \subset B$ rings s.t. B is a free A-module of rank n.

fix a basis $\omega_1, \dots, \omega_n$ of B over A: $B = \bigoplus_{i=1}^{n} A\omega_i$.

the regular representation of B over A

$$\begin{aligned} r : B &\longrightarrow \mathrm{End}_A(B) \xrightarrow{\sim} M_n(A) \\ b &\longmapsto (b' \mapsto bb') \end{aligned}$$

is an injective morphism of A-algebras

the characteristic polynomial of $b \in B$ (over A):

$$P_{B/A,b}(T) := \det(T \cdot I_n - r(b)) \in A[T] \quad (\text{monic})$$

Cayley–Hamilton: $P_{B/A,b}(r(b)) = 0 \in M_n(A)$

$$\left.\begin{aligned} P_{B/A,b}(r(b)) &= 0 \in M_n(A) \\ \shortparallel \quad & \\ r(P_{B/A,b}(b)) & \end{aligned}\right\} \underset{r \text{ injective}}{\Longrightarrow} \underline{P_{B/A,b}(b) = 0 \in B}$$

the trace of $b \in B$ (over A): $\mathrm{Tr}_{B/A}(b) := \mathrm{Tr}(r(b))$

norm $\qquad N_{B/A}(b) := \det(r(b))$

(everything is independent of the chosen basis $\{\omega_i\}$ of B/A)

Functoriality: $\forall$ ring morphism $\alpha : A \to A'$, set $B' = B \otimes_{A,\alpha} A'$.

then $r' : B' \longrightarrow \mathrm{End}_{A'}(B')$ satisfies: $\forall b \in B$ $\quad r'(b \otimes 1) = r(b) \otimes 1$.

Ex: $f(T) = T^n + a_1 T^{n-1} + \dots + a_n \in A[T]$, $\quad B = A[T]/(f) \ni \alpha = T \pmod{(f)}$

$B = \bigoplus_{i=0}^{n-1} A\alpha^i$, $\quad \alpha^n = -a_n - \dots - a_1 \alpha^{n-1}$, $\quad \alpha \cdot \alpha^i = \alpha^{i+1}$

In this basis,
$$r(\alpha) = \begin{pmatrix} 0 & 0 & & & -a_n \\ 1 & 0 & & 0 & \vdots \\ \vdots & 1 & & & \vdots \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}, \quad P_{B/A,\alpha}(T) = T^n + a_1 T^{n-1} + \dots + a_n = f(T)$$

Ex: $f(T) = T^n - c$ $(c \in A)$, $\quad B = A[T]/(f) \ni \alpha$ (as before), $\alpha^n = c$ $\quad (\alpha = \sqrt[n]{c})$

$B \ni b = u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}$ $(u_i \in A)$,
$$r(\alpha) = \begin{pmatrix} 0 & & & c \\ 1 & \ddots & 0 & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix}$$

$$r(b) = \begin{pmatrix} u_0 & cu_{n-1} & \cdots & cu_1 \\ u_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & cu_{n-1} \\ u_{n-1} & \cdots & u_1 & u_0 \end{pmatrix}$$

$\underline{n=2}$: $r(u_0 + u_1\sqrt{c}) = \begin{pmatrix} u_0 & cu_1 \\ u_1 & u_0 \end{pmatrix}$, $\quad \mathrm{Tr}_{B/A}(u_0 + u_1\sqrt{c}) = 2u_0$

$N_{B/A}(u_0 + u_1\sqrt{c}) = u_0^2 - cu_1^2$

(*) Separable field extensions: L/K separable, $[L:K]=n<\infty$

$\exists\ \alpha\in L$, $L=K(\alpha)$, $f(T)\in K[T]$ minimal polynomial of α over K

$\exists\ K'\supset K$ $\quad f(T)=\prod_{i=1}^{n}(T-\alpha_i)\in K'[T]$, $\alpha_1,\dots,\alpha_n\in K'$ distinct

there are n embeddings $\sigma_i : L\hookrightarrow K'$ over K $\quad(\sigma_i(\alpha)=\alpha_i,\ \sigma|_K=id)$

As $L\cong K[x]/(f)$, $\ \alpha\leftrightarrow x \pmod f$, we have an isomorphism of K'-algebras

$$\begin{array}{ccccccccc} L' = L\otimes_K K' & \simeq & K[x]/(f)\otimes_K K' & = K'[x]/(x-\alpha_1)\cdots(x-\alpha_n) & \xrightarrow{\sim} & \prod_{i=1}^{n} K'[x]/(x-\alpha_i) & \xrightarrow{\sim} & \prod_{i=1}^{n} K' \\ \alpha\otimes\lambda & \longmapsto & x\otimes\lambda & \longmapsto \lambda x & \longmapsto & (\lambda x)_i & \longmapsto & (\lambda\alpha_i)_i \\ b\otimes\lambda & & & \longmapsto & & & & (\lambda\sigma_i(b))_i \end{array}$$

$\forall\, b\in L$ $\quad P_{L/K,b}(T)=P_{L'/K',\,b\otimes 1}(T)=\prod_{i=1}^{n}P_{K'/K',\,\sigma_i(b)}(T)=\prod_{i=1}^{n}(T-\sigma_i(b))$

$\Longrightarrow\quad Tr_{L/K}(b)=\sum_{i=1}^{n}\sigma_i(b)$, $\quad N_{L/K}(b)=\prod_{i=1}^{n}\sigma_i(b)$

Discriminants: $\quad B=\bigoplus_{i=1}^{n}A\omega_i\quad$ as above

<u>Def</u>: $D(\omega_1,\dots,\omega_n):=\det\left(\left(Tr_{B/A}(\omega_i\omega_j)\right)_{1\le i,j\le n}\right)\in A$

(= determinant of the matrix of the symmetric A-bilinear form
$$\begin{array}{c} B\times B\longrightarrow A \\ b,b'\longmapsto Tr_{B/A}(bb') \end{array}$$
in the basis $\{\omega_i\}$)

<u>change of basis</u>: $\quad B=\bigoplus_{i=1}^{n}A\omega_i'$, $\quad M\in GL_n(A)$ change of basis matrix (from $\{\omega_i\}$ to $\{\omega_i'\}$)

$\Longrightarrow\quad \underline{D(\omega_1',\dots,\omega_n')=D(\omega_1,\dots,\omega_n)\det(M)^2}$, $\quad\det(M)\in A^\times$

<u>Special case</u>: $A=\mathbb{Z}$, $\quad B=\mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n$, $\quad\det(M)\in\mathbb{Z}^\times=\{\pm1\}$

$D(B/\mathbb{Z}):=D(\omega_1,\dots,\omega_n)\in\mathbb{Z}\quad$ <u>depends only on B</u>

In the case (*), if $L=\bigoplus_{i=1}^{n}K\omega_i$, then

$$\left(Tr_{L/K}(\omega_i\omega_j)\right)_{ij}=\left(\sum_{k=1}^{n}\sigma_k(\omega_i)\sigma_k(\omega_j)\right)_{ij}={}^tU\,U,\qquad U=\left(\sigma_i(\omega_j)\right)_{1\le i,j\le n}\in M_n(K')$$

$\Longrightarrow\quad D(\omega_1,\dots,\omega_n)=\det(U)^2$

$$\boxed{D(1,\alpha,\dots,\alpha^{n-1})=\det(U)^2=\prod_{i<j}(\alpha_i-\alpha_j)^2=\mathrm{disc}(f)\neq0}$$
(holds whenever $B=A[T]/(f(T))$, $\alpha=T \pmod f$, f monic)

$$U=\begin{pmatrix}1 & \alpha_1 & \cdots & \alpha_1^{n-1}\\ \vdots & \vdots & & \vdots\\ \vdots & \vdots & & \vdots\\ 1 & \alpha_n & \cdots & \alpha_n^{n-1}\end{pmatrix},\qquad \det(U)=\pm\prod_{i<j}(\alpha_i-\alpha_j)$$

Computing disc(f): $\quad f(T) = T^n + a_1 T^{n-1} + \dots + a_n$

(1) $s_k := \alpha_1^k + \dots + \alpha_n^k$; then $Tr_{L/K}(\alpha^i \alpha^j) = \alpha_1^{i+j} + \dots + \alpha_n^{i+j} = s_{i+j}$

$$disc(f) = \begin{vmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & & \vdots \\ \vdots & & & \vdots \\ s_{n-1} & \cdots & \cdots & s_{2n-2} \end{vmatrix}$$

Newton's recursive formulas: $s_0 = n$, $s_1 = \sigma_1$,

$s_2 - \sigma_1 s_1 + 2\sigma_2 = 0$

$s_3 - \sigma_1 s_2 + \sigma_2 s_1 - 3\sigma_3 = 0$ etc. $\quad (\sigma_i = (-1)^i a_i)$

---

(2) $f(T) = \prod_{i=1}^n (T - \alpha_i)$, $\quad f'(\alpha_i) = \prod_{\substack{j \neq i \\ 1 \le j \le n}} (\alpha_i - \alpha_j)$ $\quad$ (i fixed)

$$N_{L/K}(f'(\alpha)) = \prod_{i=1}^n f'(\alpha_i) = \prod_{\substack{j \neq i \\ 1 \le i,j \le n}} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} disc(f)$$

<u>Ex</u>: $f = T^2 + aT + b$, basis $1, \alpha$; $f'(\alpha) = 2\alpha + a$, $f(\alpha) = 0$

$$\left.\begin{aligned} f'(\alpha)\cdot 1 &= a\cdot 1 + 2\cdot\alpha \\ f'(\alpha)\cdot\alpha &= 2\alpha^2 + a\alpha = -2a\alpha - 2b + a\alpha = -2b\cdot 1 - a\cdot\alpha \end{aligned}\right\} \Rightarrow r(f'(\alpha)) = \begin{pmatrix} a & -2b \\ 2 & -a \end{pmatrix}$$

$$disc(T^2 + aT + b) = (-1)^{\binom{2}{2}} \begin{vmatrix} a & -2b \\ 2 & -a \end{vmatrix} = a^2 - 4b$$

<u>Exercise</u>: $\quad disc(T^n + aT + b) = ?$ $\quad (n > 2)$

<u>Proposition</u>. Let L/K be a finite field extension. It is equivalent:

(1) $Tr_{L/K} \equiv 0 \iff$ (2) $D(\omega_1, \dots, \omega_n) = 0$ for one ($\iff$ (2') for each) basis $\{\omega_i\}$ of L/K $\iff$ (3) L/K is not separable.

<u>Pf</u>: (1) $\Rightarrow$ (2) $\iff$ (2') is clear

(2') $\Rightarrow$ (3) $\quad L/K$ separable $\Rightarrow L = K(\alpha) = K[T]/(f)$, f separable,
$D(1, \alpha, \dots, \alpha^{n-1}) = disc(f) \neq 0$.

(3) $\Rightarrow$ (1) $\quad L/K$ not separable $\Rightarrow$ $char(K) = p > 0$, $\exists \alpha \in L$

$K \subset K(\alpha^p) \subsetneq K(\alpha) \subset L$. $\quad$ As $Tr_{C/A} = Tr_{B/A} \circ Tr_{C/B}$ $\quad (A \subset B \subset C)$,

we can replace K by $K(\alpha^p)$ and L by $K(\alpha)$, so that

$L = K(\alpha)$, $\alpha \notin K$, $\alpha^p = c \in K$. Then

$$Tr_{L/K}(u_0 + u_1\alpha + \dots + u_{p-1}\alpha^{p-1}) = Tr\begin{pmatrix} u_0 & & * \\ & \ddots & \\ * & & u_0 \end{pmatrix} = pu_0 = 0 \Rightarrow Tr_{L/K} \equiv 0.$$

$(\forall u_i \in K)$

Extensions of Dedekind rings

Theorem. Let A be a Dedekind ring, L a finite field extension of $K = \mathrm{Frac}(A)$, then the normalisation B of A in L is a Dedekind ring (and $\underbrace{\mathrm{Frac}(B) = L}_{\text{easy}}$).

Proof in a special case when the following finiteness condition holds:

(F) B is an A-module of finite type

[true if L/K is separable, or if A is a k-algebra of finite type, k = field]

$B \subset L \Rightarrow B$ is a domain. B = normalisation of $A \Rightarrow B$ is normal.

A noetherian, (F) $\Rightarrow$ each ideal $J \subset B$ is an A-module of finite type $\Rightarrow$ also a B-module of finite type; thus B is noetherian.

Let $(0) \neq P \subset B$ be a prime ideal. We must show that B/P is a field.

Claim: $A \cap P$ (a prime ideal of A) $\neq (0)$ ($\Rightarrow A/A\cap P$ is a field, since $\dim(A) \leq 1$).

Indeed, for any $b \in P \setminus \{0\}$, $a := N_{L/K}(b) \in K^\times$ is integral over A (being a product of elements integral over A), hence $a \in A \setminus \{0\}$. Moreover, the image of a in B/P is zero, hence $0 \neq a \in B \cap P \Rightarrow$ claim.

Thus B/P is a domain which is a vector space of finite dimension over the field $A/A\cap P \overset{\text{Lemma}}{\Longrightarrow} B/P$ is a field $\Rightarrow P \in \mathrm{Max}(B)$; $\Rightarrow \dim(B) \leq 1$.

Lemma. k field, $C \supset k$ domain, $\dim_k(C) < \infty \Rightarrow C$ is a field.

Pf: $\forall c \in C \setminus \{0\}$ the multiplication of $c : C \longrightarrow C$, $c' \longmapsto cc'$ is a k-linear injective map $\Rightarrow$ it is bijective, since $\dim_k(C) < \infty \Rightarrow c \in C^\times$.

Prop. If L/K is separable, then (F) holds.

Pf. Fix a basis $b_1, \dots, b_n$ of L/K s.t. $\forall i$ $b_i \in B$.

$\forall b \in B$ $bb_i \in B$, $\mathrm{Tr}_{L/K}(bb_i) = \sum_{\sigma : L \hookrightarrow K^{sep}} \underbrace{\sigma(bb_i)}_{\text{integral over } A} \in K$ is integral over A

$\Rightarrow \mathrm{Tr}_{L/K}(bb_i) \in A$

Let $\lambda_1, \dots, \lambda_n \in K$; then $\left[\sum_{j=1}^n \lambda_j b_j \in B \Rightarrow \forall i \ \sum_{j=1}^n \lambda_j \mathrm{Tr}_{L/K}(b_i b_j) \in A\right]$

L/K separable $\Rightarrow$ the matrix $M = (\mathrm{Tr}_{L/K}(b_i b_j)) \in M_n(A)$ has $\underbrace{\det(M)}_{d \in A} \neq 0$

So, $\sum_{j=1}^n \lambda_j b_j \in B \Rightarrow M\begin{pmatrix}\lambda_1\\ \vdots \\ \lambda_n\end{pmatrix} \in A^n \Rightarrow \underbrace{\mathrm{adj}(M)\,M}_{d \cdot I_n}\begin{pmatrix}\lambda_1\\ \vdots \\ \lambda_n\end{pmatrix} \in A^n \Rightarrow d\lambda_i \in A$ $\forall i$

$\Rightarrow B \subseteq \sum_{j=1}^n A \cdot d^{-1} b_j \overset{A \text{ noetherian}}{\Longrightarrow} B$ is an A-module of finite type.

Cor. For every number field K ($n = [K:\mathbb{Q}] < \infty$),

$O_K = \{\alpha \in K \mid \alpha \text{ integral over } \mathbb{Z}\}$ is a Dedekind ring.

(Moreover, $\mathbb{Q} \cdot O_K = K$ and $(O_K, +)$ is a finitely generated abelian group $\Rightarrow \exists\, \omega_1, \dots, \omega_n$ basis of $K/\mathbb{Q}$ ("an integral basis of K") s.t. $O_K = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$.

Cor. If L/K is separable and A is principal, then B is free (of rank $= [L:K]$) over A.

Pf: If $b_1, \ldots, b_n$ $(n = [L:K])$ is a basis of L/K s.t. $\forall i$ $b_i \in B$ (this can be achieved by replacing b_i by ab_i, for suitable $a \in A \setminus \{0\}$), then we have

$$\bigoplus_{i=1}^{n} A b_i \subset B \subset \bigoplus_{i=1}^{n} A\, d^{-1} b_i \qquad (d = D(b_1, \ldots, b_n) \in A \setminus \{0\})$$

Structure theory of finitely generated modules over ~~PID~~ PID's implies that B is free of rank n over A.

Special case: $A = \mathbb{Z}$, $K = \mathbb{Q}$, $n = [L:\mathbb{Q}] < \infty$, $B = \mathcal{O}_L$

$\Rightarrow \exists\, \omega_1, \ldots, \omega_n \in \mathcal{O}_L$ $\quad \mathcal{O}_L = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$ ($\{\omega_i\}$ is an <u>integral basis</u> of L)

Def: $D_L := D(\omega_1, \ldots, \omega_n) \in \mathbb{Z} \setminus \{0\}$ is independent of $\{\omega_i\}$; it is called the <u>discriminant</u> of L.

Ex: $L = \mathbb{Q}$, $n = 1$, $\omega_1 = \pm 1$, $D_{\mathbb{Q}} = 1$

Irreducibility

$A = $ domain, $K = \mathrm{Frac}(A)$

Prop. Assume A is a UFD. If $\alpha = \frac{a}{b} \in K$ ($a, b \in A$, $b \neq 0$, $\gcd(a,b) = 1$) is a root of $f(T) = \sum_{i=0}^{n} a_i T^i$ ($a_n \neq 0$), then $b \mid a_n$ and $a \mid a_0$.

Pf: Exercise.

Prop.-Def. Assume A is a UFD. (1) For $f(T) = \sum_{i=0}^{n} a_i T^i \in K[T] \smallsetminus \{0\}$ define the content of f as $\mathrm{cont}_A(f) = c^{-1} \gcd(ca_0, \dots, ca_n) \in K^\times$, for any $c \in A \smallsetminus \{0\}$ s.t. $cf \in A[T]$ (this does not depend on c).

(2) (Gauss Lemma) $\forall f, g \in K[T] \smallsetminus \{0\}$ $\quad \mathrm{cont}_A(fg) = \mathrm{cont}_A(f)\, \mathrm{cont}_A(g)$.

(3) If $f \in A[T] \smallsetminus \{0\}$ is reducible in $K[T]$, it is reducible in $A[T]$.

Pf of [(2) $\Rightarrow$ (3)]: if $f = gh$, $g, h \in K[T] \smallsetminus \{0\}$, let $b = \mathrm{cont}_A(g)$. Then $f = (b^{-1}g)(bh)$ and $b^{-1}g \in A[T]$ (by definition of cont_A),

$$\mathrm{cont}_A(bh) = b\, \mathrm{cont}_A(h) = \mathrm{cont}_A(g)\, \mathrm{cont}_A(h) \overset{(2)}{=} \mathrm{cont}_A(f) \in A \smallsetminus \{0\} \Rightarrow bh \in A[T].$$

Prop.-Def. Assume A is a Dedekind ring. (1) For $f(T) = \sum_{i=0}^{n} a_i T^i \in K[T] \smallsetminus \{0\}$, the content of f is the fractional ideal $\mathrm{ct}_A(f) := (a_0, \dots, a_n)$ of A.

(2) $\forall\ \mathfrak{p} \in \mathrm{Max}(A)$ $\quad \mathrm{ct}_A(f) A_\mathfrak{p} = (\mathrm{cont}_{A_\mathfrak{p}}(f))$

(3) $\forall f, g \in K[T] \smallsetminus \{0\}$ $\quad \mathrm{ct}_A(fg) = \mathrm{ct}_A(f)\, \mathrm{ct}_A(g)$

(4) If $f \in A[T] \smallsetminus \{0\}$ is reducible in $K[T]$ and monic, then f is reducible in $A[T]$.

Pf. (2): by definition. (3) follows from (2) and $\mathrm{cont}_{A_\mathfrak{p}}(fg) = \mathrm{cont}_{A_\mathfrak{p}}(f)\, \mathrm{cont}_{A_\mathfrak{p}}(g)$.

(4) If $f = gh$, $g, h \in K[T]$, we can replace g by λg, h by $\lambda^{-1} h$ and assume that g is monic $\Longrightarrow$ h monic. Then

$A = (1) \subseteq \mathrm{ct}_A(g), \mathrm{ct}_A(h)$ and $A = \mathrm{ct}_A(f) \overset{(3)}{=} \mathrm{ct}_A(g)\, \mathrm{ct}_A(h)$

$\Longrightarrow \mathrm{ct}_A(g) = \mathrm{ct}_A(h) = A \Longrightarrow g, h \in A[T]$.

Ex: $K = \mathbb{Q}(\sqrt{-5})$, $A = \mathbb{Z}[\sqrt{-5}]$

$$\underbrace{f(T) = 2T^2 + 2T + 3}_{\text{not monic}} = \frac{(2T + (1+\sqrt{-5}))(2T + (1-\sqrt{-5}))}{2}$$ is not reducible in $A[T]$

Eisenstein criterion of irreducibility: let $\mathfrak{p} \subset A$ be a prime ideal.
If $f(T) = \sum_{i=0}^{n} a_i T^i \in A[T]$ is monic $(a_n = 1)$, $\forall i<n$ $a_i \in \mathfrak{p}$, $a_0 \notin \mathfrak{p}^2$ ("f is an Eisenstein polynomial w.r.t. $\mathfrak{p}$"), then f is irreducible in $A[T]$.

Pf: If $f = gh$, $g = \sum b_i T^i$, $h = \sum c_j T^j$ non-constant
$\Rightarrow b_0 c_0 = a_0 \in \mathfrak{p} \Rightarrow b_0 \in \mathfrak{p}$ or $c_0 \in \mathfrak{p}$. Say, $b_0 \in \mathfrak{p} \Rightarrow c_0 \notin \mathfrak{p}$ (as $b_0 c_0 \notin \mathfrak{p}^2$). As f is monic, $\exists$ $k = \min\limits_{b_i \notin \mathfrak{p}} \{i \geq 0\} \leq \deg(g) < n$.
then $a_k = \underbrace{b_0 c_k + b_1 c_{k-1} + \dots + b_{k-1} c_1}_{\in \mathfrak{p}} + \underbrace{b_k c_0}_{\notin \mathfrak{p}} \Rightarrow a_k \notin \mathfrak{p}$ – contradiction.

Ex: (1) $A = \mathbb{Z}$, $T^n - 2$, $\mathfrak{p} = (2)$.
(2) $A = \mathbb{Z}$, $\frac{(1+T)^p - 1}{T} = T^{p-1} + \binom{p}{1} T^{p-2} + \dots + \binom{p}{p-1}$, $\mathfrak{p} = (p)$.

Minimal polynomial vs. characteristic polynomial

L/K finite field extension, $\alpha \in L$
$K \subset K(\alpha) \subset L$, $n = [K(\alpha):K]$, $m = [L:K(\alpha)]$
$\omega_1, \dots, \omega_m$ a basis of $L/K(\alpha) \Rightarrow \alpha^i \omega_j$ $(0 \leq i \leq n-1,\ 1 \leq j \leq m)$ is a basis of L/K

In this basis, $r: L \hookrightarrow \mathrm{End}_K(L) \simeq M_{mn}(K)$ satisfies

$$r(\alpha) = \begin{pmatrix} A & & 0 \\ & \ddots & \\ 0 & & A \end{pmatrix}, \text{ where } A = \begin{pmatrix} 0 & & & -a_n \\ 1 & & 0 & \vdots \\ & \ddots & & \vdots \\ 0 & & 1 & -a_1 \end{pmatrix} \in M_n(K)$$
(m times A)

$f(T) = T^n + a_1 T^{n-1} + \dots + a_n$ = minimal pol. of α over K

$\Rightarrow P_{L/K,\alpha}(T) = \det(T \cdot I_n - A)^m = f(T)^m$

Determining O_K

$[K:\mathbb{Q}] = n < \infty$ Goal: find $\omega_1, \dots, \omega_n \in K$ s.t. $O_K = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n$.

Prop. let A be a normal domain, $K = \mathrm{Frac}(A)$, $[L:K] < \infty$, $\beta \in L$. let $f \in K[T]$ be the (monic) minimal polynomial of α over K.

Then: (1) β is integral over $A \Leftrightarrow$ (2) $P_{L/K,\beta}(T) \in A[T] \Leftrightarrow$ (3) $f \in A[T]$.

Pf: As $P_{L/K,\beta} = f^{[L:K(\alpha)]}$, (3) $\Rightarrow$ (2) $\Rightarrow$ (1) holds.

(1) $\Rightarrow$ (3): $f(T) = \prod_{i=1}^{n} (T - \beta_i)$, $\beta_i \in K'$ (the splitting field of f over K)

β is integral over $A \Rightarrow$ each β_i is $\Rightarrow$ each coefficient of f is $\overset{(A \text{ normal})}{\Longrightarrow}$ (3)

Quadratic fields

Prop. let $[K:\mathbb{Q}] = 2$. then:

(1) $\exists!$ square-free $d \in \mathbb{Z} \setminus \{0,1\}$ such that $K = \mathbb{Q}(\sqrt{d})$.

(2) $$O_K = \mathbb{Z}[\alpha] = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\alpha, \quad \alpha = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4 \\ \sqrt{d} & d \equiv 2,3 \pmod 4 \end{cases}$$

(3) $$D_K = \mathrm{disc}(O_K/\mathbb{Z}) = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & d \equiv 2,3 \pmod 4 \end{cases}$$

Pf: (1) Easy exercise. | (2) $\Rightarrow$ (3) $D_K = \mathrm{disc}(\mathbb{Z}[\alpha]/\mathbb{Z}) = \mathrm{disc}(f)$,

$$f(T) = \text{minimal polynomial of } \alpha \text{ over } \mathbb{Q} = \begin{cases} T^2 - T + \frac{1-d}{4} \\ T^2 - d \end{cases} \Rightarrow D_K = \begin{cases} d \\ 4d. \end{cases}$$

(2) $\beta = u + v\sqrt{d} \in K$ $(u, v \in \mathbb{Q}) \Rightarrow P_{K/\mathbb{Q},\beta}(T) = T^2 - 2uT + (u^2 - dv^2)$

So $\beta \in O_K \Leftrightarrow 2u, u^2 - dv^2 \in \mathbb{Z}$

$$\Leftrightarrow \begin{cases} u \in \mathbb{Z}, dv^2 \in \mathbb{Z} \Leftrightarrow u, v \in \mathbb{Z} \quad (d \text{ square-free}) \\ u \in \mathbb{Z} + \frac{1}{2}, dv^2 \in \mathbb{Z} + \frac{1}{4} \Leftrightarrow u \in \mathbb{Z} + \frac{1}{2}, d(2v)^2 \in 4\mathbb{Z}+1 \Leftrightarrow u, v \in \mathbb{Z} + \frac{1}{2}, d \in 4\mathbb{Z}+1 \end{cases}$$

Prop. If $B' \supset B$ are rings free of rank n over $\mathbb{Z}$, then
$$D(B^\#/\mathbb{Z}) = D(B'/\mathbb{Z}) \cdot (B' : B^\#)^2$$

Pf: $\exists \mathbb{Z}$-bases $B' = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n \supset B^\# = \mathbb{Z}d_1\omega_1 + \dots + \mathbb{Z}d_n\omega_n$ $(d_i \in \mathbb{Z}_{>0})$

$D(B^\#/\mathbb{Z}) = D(d_1\omega_1, \dots, d_n\omega_n) = (d_1 \cdots d_n)^2 D(\omega_1, \dots, \omega_n) = (B' : B^\#)^2 D(B'/\mathbb{Z})$.

Cor: If $B \subset O_K$ is free of rank $n=[K:\mathbb{Q}]$ over $\mathbb{Z}$ and $D(B/\mathbb{Z})$ is square-free, then $B = O_K$ and $D_K = D(B/\mathbb{Z})$ is square-free.

Pf: $D(B/\mathbb{Z}) = D(O_K/\mathbb{Z})\,(O_K:B)^2$ square-free $\Rightarrow (O_K:B)=1$.

Ex: $K=\mathbb{Q}(\alpha)$, $f(\alpha)=0$, $f(T)=T^3-T+1$ (irred. $/\mathbb{Q}$)

$D(\mathbb{Z}[\alpha]/\mathbb{Z}) = \mathrm{disc}(f) = -4(-1)^3 - 27\cdot 1^2 = -23 \Rightarrow O_K = \mathbb{Z}[\alpha]$, $D_K = -23$

What to do if $p^2 \mid D(B/\mathbb{Z})$? (p prime)

Is there $x \in B$ s.t. $\frac{x}{p} \in O_K$, but $\frac{x}{p} \notin B$?

Prop. Given a prime number p and a subring $B \subset O_K$ of finite index ($\Longleftrightarrow$ B is free over $\mathbb{Z}$ of rank $=[K:\mathbb{Q}]$), let $\mathrm{Nil}(B/pB) \subset B/pB$ be the nil radical of B/pB ($=\sqrt{(0)}$ in B/pB) and $N \subset B$ the inverse image of $\mathrm{Nil}(B/pB)$ in B. Consider the ring morphism

$$m: B/pB \longrightarrow \mathrm{End}_{B/pB}(N/pN).$$
$$y \longmapsto (n \mapsto yn)$$

Then

$$\boxed{\mathrm{Ker}(m) = (B \cap pO_K)/pB}$$

Cor. (1) $\mathrm{Ker}(m) = 0 \Longleftrightarrow B \cap pO_K = pB \Longleftrightarrow p \nmid (O_K:B)$

(2) If $x \in B$, $m(x \,(\mathrm{mod}\, pB)) \neq 0 \Rightarrow \frac{x}{p} \in O_K$, $\frac{x}{p} \notin B$.

Pf of Prop: $pB \subset N \subset B \Rightarrow N$ $\mathbb{Z}$-module of finite type

"$\subseteq$": $x \in B$, $m(x\,(\mathrm{mod}\, pB)) = 0 \Rightarrow xN \subseteq pN \Rightarrow \frac{x}{p} N \subseteq N$ $\Big\} \Rightarrow \frac{x}{p} \in O_K$

"$\supseteq$": set $B' = \{x \in O_K \mid xN \subset N\} = \{x \in K \mid xN \subset N\}$, $B'' = O_K \cap p^{-1}B$

If $x \in B \cap pO_K$, then $\frac{x}{p} \in B'' \underset{\text{below}}{\overset{\text{Lemma}}{=\!=}} B' \Rightarrow xN \subset pN \Rightarrow m(x\,(\mathrm{mod}\, pB)) = 0$.

Lemma: $B' = B''$.

Pf. $x \in B' \overset{p \in N}{\Longrightarrow} px \in N \subset B \Rightarrow x \in B''$.

$x \in B'' \Rightarrow x \in O_K$, $px \in B$. Fix $y \in N$; $\exists m \geq 1$ $y^m \in pB \Rightarrow xy^m \in pxB \subset B$

$\Rightarrow \forall k \geq 1$ $y^m (xy^m)^k = x^k y^{m+mk} \in pB \Rightarrow \forall k = 0, \dots, n-1$ $x^k y^{mn} \in pB$

$x \in O_K$: $\underbrace{x^n + a_1 x^{n-1} + \dots + a_n = 0, \quad a_i \in \mathbb{Z} \subset B}_{\forall k \geq 0 \ x^k y^{mn} \in pB}$

$k = mn$: $(xy)^{mn} \in pB \Rightarrow xy \in N$. So $x \in B'$.

Ex: (Eisenstein case) $f(T) = T^n + a_1 T^{n-1} + \dots + a_n \in \mathbb{Z}[T]$
Eisenstein polynomial w.r.t. prime number p, $f(\alpha) = 0$,
$K = \mathbb{Q}(\alpha) = \mathbb{Q}[T]/(f) \supset B = \mathbb{Z}[\alpha] = \mathbb{Z}[T]/(f) = \mathbb{Z}[T]/f\mathbb{Z}[T]$

$B/pB = \mathbb{F}_p[T]/(\bar{f}) = \mathbb{F}_p[T]/(T^n)$ $\qquad \bar{a} = a \pmod p$

$\mathrm{Nil}(B/pB) = T \cdot (B/pB)$, $N = \{g \in \mathbb{Z}[T] \mid g(0) \equiv 0 \pmod p\} / f\mathbb{Z}[T]$

$= \underbrace{\mathbb{Z} \cdot p}_{\omega_1} \oplus \underbrace{\mathbb{Z} \cdot T}_{\omega_2} \oplus \dots \oplus \underbrace{\mathbb{Z} \cdot T^{n-1}}_{\omega_n} \quad (\mathrm{mod}\ f\mathbb{Z}[T])$

$N/pN = \mathbb{F}_p \cdot \omega_1 \oplus \dots \oplus \mathbb{F}_p \omega_n$

$m : B/pB = \mathbb{F}_p[T]/(T^n) \longrightarrow \mathrm{End}_{B/pB}(N/pN)$

Claim: $\mathrm{Ker}(m) = 0$ $\quad (\overset{\text{Prop.}}{\Longleftrightarrow} \quad \underline{p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])})$

Pf of Claim: $\mathrm{Ker}(m)$ is an ideal in $\mathbb{F}_p[T]/(T^n) \Rightarrow \mathrm{Ker}(m) = (T^i)$.
the ~~minimal~~ smallest non-zero ideal is (T^{n-1}), so it is enough to show that $r(T^{n-1}) \overset{?}{\neq} 0$. Let us compute the matrix of $r(T)$ in the basis $\{\omega_i\}$ (over $\mathbb{F}_p$):

$T\omega_1 = pT = p\omega_2 \equiv 0 \pmod p$
$T\omega_2 = T^2 = \omega_3, \dots, T\omega_{n-1} = T^{n-1} = \omega_n$
$T\omega_n = T^n = -a_n - a_{n-1}T - \dots - a_1 T^{n-1}$
$\equiv -(a_n/p)\omega_1 \pmod p$, $\qquad a_n/p \not\equiv 0 \pmod p$

So $r(T) = \underbrace{\begin{pmatrix} 0 & 0 & & & c \\ 0 & 0 & & & 0 \\ \vdots & 1 & & 0 & \vdots \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}}_{n} \in M_n(\mathbb{F}_p)$, $c \in \mathbb{F}_p$, $\underline{c \neq 0}$

$T^{n-1}\omega_2 = T\omega_n \neq 0$
$\Rightarrow r(T^{n-1}) \neq 0 \Rightarrow \mathrm{Ker}(m) = 0$.

Ex (see R. Schoof's course): $\underline{K = \mathbb{Q}(\sqrt[3]{17})}$

$B = \mathbb{Z}[\sqrt[3]{17}] \subset \mathcal{O}_K$; $f(T) = T^3 - 17$ $\Big\}$ $D(B/\mathbb{Z}) = \mathrm{disc}(f) = -3^3 \cdot 17^2$
$\mathrm{disc}(T^3 + aT + b) = -4a^3 - 27b^2$ $\qquad = D_K (\mathcal{O}_K : B)^2$
f is Eisenstein w.r.t. $17 \Rightarrow 17 \nmid (\mathcal{O}_K : B)$ $\Big\} \Rightarrow (\mathcal{O}_K : B) = \begin{cases} 1 \\ 3 \end{cases}$

$\underline{p=3}$: $B = \mathbb{Z}[T]/(T^3 - 17)$, $T \pmod f = \sqrt[3]{17}$; $B/3B = \mathbb{F}_3[T]/(T^3 + 1) = \mathbb{F}_3[T]/(T+1)^3$
$\mathrm{Nil}(B/3B) = (T+1) \cdot B/3B \Rightarrow N = 3B + \underbrace{(1 + \sqrt[3]{17})}_{\alpha} B$

$0 = (\alpha - 1)^3 - 17 = \alpha^3 - 3\alpha^2 + 3\alpha - 18$

$B = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\alpha \oplus \mathbb{Z}\cdot\alpha^2 \quad , \quad \alpha^3 \in 3B$

$N = 3B + \alpha B = \mathbb{Z}\cdot 3 \oplus \mathbb{Z}\cdot\alpha \oplus \mathbb{Z}\cdot\alpha^2 \qquad \alpha^3 \in 3N$

$m : \quad B/3B \longrightarrow \mathrm{End}_{B/3B}(N/3N)$

$x = a + b\alpha + c\alpha^2 \in B \qquad x\cdot 3 \equiv a\cdot 3 \pmod{3N}$

$x\cdot\alpha \equiv a\cdot\alpha + b\cdot\alpha^2 \pmod{3N}$

$x\cdot\alpha^2 \equiv a\cdot\alpha^2 \pmod{3N}$

$$m(x) = \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & b & a \end{pmatrix} \pmod 3 \quad \in M_3(\mathbb{F}_3)$$

$\mathrm{Ker}(m) = \mathbb{F}_3\cdot(\alpha^2 \pmod{3B}) \implies \alpha^2/3 \in O_K \quad , \alpha^2 \in B$

$\frac{\alpha^2}{3} = \frac{(1+\sqrt[3]{17})^2}{3} \qquad B \subsetneqq B' = B + \mathbb{Z}\beta \subset O_K \qquad (B' : B) = 3$

$(O_K : B) \mid 3 \implies \boxed{O_K = B' = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\alpha \oplus \mathbb{Z}(\alpha^2/3) \quad , \quad \alpha = 1 + \sqrt[3]{17}}$

$\left(\alpha^2/3 - \alpha = \frac{1 - \sqrt[3]{17} + (\sqrt[3]{17})^2}{3} =: \gamma \in O_K \right.$

$$\boxed{\begin{aligned} D_K &= D(B/\mathbb{Z})/3^2 \\ &= -3\cdot 17^2 \end{aligned}}$$

$P_{K/\mathbb{Q},\gamma}(T)$: $r(\gamma)$ in the basis $1, \sqrt[3]{17}, (\sqrt[3]{17})^2$ is

$$r(\gamma) = \begin{pmatrix} 1/3 & 17/3 & -17/3 \\ -1/3 & 1/3 & 17/3 \\ 1/3 & -1/3 & 1/3 \end{pmatrix}$$

$P_{K/\mathbb{Q},\gamma}(T) = \det(T\cdot I_3 - r(\gamma)) = T^3 - T^2 + 6T - 12$ (the minimal polynomial of γ over $\mathbb{Q}$)

$= (T - 1/3)^3 + \frac{17}{3}(T - \frac{1}{3}) - \frac{2^4\cdot 17}{27}$

$D(\mathbb{Z}[\gamma]/\mathbb{Z}) = -4\left(\frac{17}{3}\right)^3 - 27\left(-\frac{2^4\cdot 17}{27}\right)^2 = -\frac{17^2}{27}\big(\underbrace{4\cdot 17 + 2^8}_{4\cdot 3^4}\big) = -2^2\cdot 3\cdot 17^2$

Ex: Cyclotomic fields $\quad p$ prime number, $n \geq 1$, $p^n \neq 2$

$\xi = \xi_{p^n} = e^{2\pi i/p^n}$, $\alpha = \xi - 1$

$f(\xi) = 0$, $\quad f(T) = (T^{p^n}-1)/(T^{p^{n-1}}-1)$, $\quad f(1) = \frac{p^n}{p^{n-1}} = p$

$g(\alpha) = 0$, $\quad g(T) = f(1+T) = \frac{(1+T)^{p^n}-1}{(1+T)^{p^{n-1}}-1} \equiv \frac{T^{p^n}}{T^{p^{n-1}}} \equiv T^{p^n - p^{n-1}} \pmod{p\mathbb{Z}[T]}$

$g(0) = p$

$\Rightarrow$ g is Eisenstein w.r.t p $\Rightarrow$ f, g are irreducible over $\mathbb{Q}$,

$[\mathbb{Q}(\xi_{p^n}) : \mathbb{Q}] = \deg(f) = \varphi(p^n) = p^n - p^{n-1}$.

Discriminant:

$$\operatorname{disc}(f) = (-1)^{\binom{\deg(f)}{2}} N_{\mathbb{Q}(\xi)/\mathbb{Q}}(f'(\xi))$$

$$f'(\xi) = \frac{p^n \xi^{p^n-1}}{\xi^{p^{n-1}}-1} = \frac{p^n \xi^{-1}}{\xi^{p^{n-1}}-1}, \quad N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi) = \prod_{\substack{j=1 \\ p \nmid j}}^{p^n} \xi^j = 1$$

$\xi^{p^{n-1}} = \xi_p = e^{2\pi i/p}$

$$N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi_p - 1) = \underbrace{\left(N_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(\xi_p - 1)\right)}_{\prod_{j=1}^{p-1}(\xi_p^j - 1)}^{\overbrace{[\mathbb{Q}(\xi_{p^n}) : \mathbb{Q}(\xi_p)]}^{p^{n-1}}}$$

$$\prod_{j=1}^{p-1}(\xi_p^j - 1) = (-1)^{p-1} \left.\frac{T^p - 1}{T-1}\right|_{T=1} = (-1)^{p-1} p$$

$$\Rightarrow \quad \operatorname{disc}(g) = \operatorname{disc}(f) = (-1)^{\frac{\varphi(p^n)(\varphi(p^n)-1)}{2}} p^{n\varphi(p^n)} \Big/ (-1)^{\varphi(p^n)} p^{p^{n-1}}$$

$$= \pm p^{np^n - (n+1)p^{n-1}}$$

g Eisenstein at p $\Rightarrow$ $p \nmid (\mathcal{O}_{\mathbb{Q}(\xi)} : \mathbb{Z}[\xi - 1])$ $\quad \Rightarrow$

$$\boxed{\mathcal{O}_{\mathbb{Q}(\xi_{p^n})} = \mathbb{Z}[\xi_{p^n} - 1] = \mathbb{Z}[\xi_{p^n}]}$$

$$\boxed{D_{\mathbb{Q}(\xi_{p^n})} = \pm p^{np^n - (n+1)p^{n-1}}}$$

$n = 1$ $(p > 2)$: $\quad D_{\mathbb{Q}(\xi_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}$

$\mathcal{O}_{\mathbb{Q}(\xi_p)} = \mathbb{Z}[\xi_p]$

Decomposition of prime ideals

Prop.–Def. A Dedekind ring, $K = \mathrm{Frac}(A)$, $[L:K] < \infty$,
B = normalisation of A in L ($\Rightarrow B$ Dedekind). Assume:

(F) B is an A-module of finite type.

Then: $\forall \mathfrak{p} \in \mathrm{Max}(A)$

$$\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}, \quad P_i \in \mathrm{Max}(B) \text{ distinct}, \; e_i \geq 1$$

$\{P_1, \dots, P_r\} = \{P \in \mathrm{Max}(B) \mid P \cap A = \mathfrak{p}\}$

$$\sum_{i=1}^{r} e_i f_i = n = [L:K], \quad f_i = [B/P_i : A/\mathfrak{p}]$$

Terminology: $e_i = e(P_i/\mathfrak{p})$ = the ramification index of P_i over $\mathfrak{p}$
$f_i = f(P_i/\mathfrak{p})$ = the relative degree (= the inertia index) — " —

$P_i | \mathfrak{p}$
"P_i is above $\mathfrak{p}$"

P_i is unramified in $L/K \iff e_i = 1$ & B/P_i separable over $A/\mathfrak{p}$
$\mathfrak{p}$ —— " —— $\iff \forall i \; e_i = 1$ & — " —
$\mathfrak{p}$ is inert in $L/K \iff r = 1, \; e_1 = 1 \iff \mathfrak{p}B \in \mathrm{Max}(B)$
$\mathfrak{p}$ splits completely in $L/K \iff r = [L:K]$ ($\iff \forall i \; e_i = f_i = 1$).

Pf: $\mathfrak{p}B \subset B$ is a non-zero ideal $\Rightarrow \mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$,

$$B/\mathfrak{p}B = \prod_{i=1}^{r} B/P_i^{e_i}B.$$

Lemma: C ring, $m \in \mathrm{Max}(C) \Rightarrow \forall i \leq j \quad m^i/m^j \simeq m^i C_m / m^j C_m$
Pf: Exercise.

$\Rightarrow \quad B \supset P \supset P^2 \supset \cdots, \quad P^k/P^{k+1} \simeq (PB_P)^k/(PB_P)^{k+1}$
$\forall P \in \mathrm{Max}(B)$

$B/P \simeq B_P/PB_P$ as B_P = DVR

as $\underbrace{B/P}_{\text{field}}$-modules, so $\dim_{B/P} P^k/P^{k+1} = 1$
$\forall k \geq 0$.

For $P = P_i$, $P_i | \mathfrak{p}B \Rightarrow \mathfrak{p}B \subset P_i \Rightarrow \mathfrak{p} \subset \underbrace{A \cap P_i}_{\text{prime ideal of } A} \Rightarrow \mathfrak{p} = A \cap P_i$.

$\underbrace{A/\mathfrak{p}}_{\text{field}} \hookrightarrow \underbrace{B/P_i}_{\text{field, } A\text{-module of f.t.}} \Rightarrow f_i = [B/P_i : A/\mathfrak{p}] < \infty$

$\mathfrak{p}B \subset P_i^{e_i} \Rightarrow B/P_i^{e_i}$ is an $A/\mathfrak{p}$-module

$$\dim_{A/\mathfrak{p}} B/P_i^{e_i} = \sum_{k=0}^{e_i - 1} \dim_{A/\mathfrak{p}} P_i^k/P_i^{k+1} = \sum_{k=0}^{e_i-1} f_i = e_i f_i$$

$$\Rightarrow \quad \dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{i=1}^{r} e_i f_i .$$

On the other hand, $B/\mathfrak{p}B = B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$, $B_\mathfrak{p} = A_\mathfrak{p}B \subset L$

$B_\mathfrak{p}$ torsion-free $A_\mathfrak{p}$-module of f.t. $\Rightarrow$ free of $rk = t$

$$\Downarrow$$

$B_\mathfrak{p} \otimes_{A_\mathfrak{p}} K = L \Rightarrow t = [L:K] = n$

$$\sum e_i f_i = \dim_{\underbrace{A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}}_{A/\mathfrak{p}}} \underbrace{B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}}_{B/\mathfrak{p}B} = t$$

$\Rightarrow \sum e_i f_i = n$.

Index

Def. A Dedekind ring, $X \supset Y$ A-modules of fin. type s.t. X/Y is torsion. Then $X/Y \simeq \bigoplus_{i=1}^{r} A/I_i$, $I_i \subset A$ ideal ($\neq 0$). The index $(X:Y) = \prod_{i=1}^{r} I_i$ ($\neq 0$ ideal of A) depends only on X/Y.

Properties: (1) $X \supset Y \supset Z \Rightarrow (X:Z) = (X:Y)(Y:Z)$

(2) $\forall \mathfrak{p} \in Max(A)$ $(X:Y)A_\mathfrak{p} = (XA_\mathfrak{p} : YA_\mathfrak{p})$

(3) $X = A^n$, $Y = MA^n$, $M \in M_n(A) \cap GL_n(Frac(A)) \Rightarrow (A^n : MA^n) = (\det(M))$

Thm (Kummer–Dedekind) A Dedekind ring, $K = Frac(A)$, L/K finite separable extension, B = normalisation of A in L. Fix $\alpha \in B$ s.t. $L = K(\alpha)$ (it always exists). Then $B/A[\alpha]$ is a torsion A-module of finite type. Let $f \in A[T]$ be the minimal polynomial of α over K.

Then: for each $\mathfrak{p} \in Max(A)$ s.t. $\mathfrak{p} \nmid (B:A[\alpha])$, let

$$f(T) \equiv \overline{g}_1(T)^{e_1} \cdots \overline{g}_r(T)^{e_r} \pmod{\mathfrak{p}A[T]},$$

where $\overline{g}_i(T) \in (A/\mathfrak{p})[T]$ are distinct monic irreducible polynomials (non-const.) and $e_i \geq 1$. Each ideal

$$P_i = g_i(\alpha)B + \mathfrak{p}B \subset B \quad \text{(where } g_i \in A[T] \text{ is any}$$

polynomial s.t. $g_i \pmod{\mathfrak{p}A[T]} = \overline{g}_i$) depends only on $\overline{g}_i$, $P_i \in Max(B)$, $P_i \neq P_j$ for $i \neq j$, $[B/P_i : A/\mathfrak{p}] = \deg(\overline{g}_i)$ and

$$\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$$

Pf: As $\mathfrak{p} \nmid (B : A[\alpha])$, $A_\mathfrak{p}[\alpha] = A[\alpha]_\mathfrak{p} = B_\mathfrak{p}$ $(= BA_\mathfrak{p})$, so

$$\underbrace{B/\mathfrak{p}B} = B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}[\alpha] = A/\mathfrak{p}[\alpha] = A/\mathfrak{p}[T]/(\bar f)$$

$$= A/\mathfrak{p}[T]/\Big(\prod_{i=1}^r \bar g_i(T)^{e_i}\Big) \xrightarrow{\sim} \prod_{i=1}^r A/\mathfrak{p}[T]/(\bar g_i(T)^{e_i})$$

$$\cancel{\Big(\prod_j B/P_j^{e'_j} \text{ if } \mathfrak{p}B = \prod_j P_j^{e'_j}\Big)}$$

Define $P_i := \mathrm{Ker}\Big(B \longrightarrow B/\mathfrak{p}B \xrightarrow{\sim} \prod_{i=1}^r A/\mathfrak{p}[T]/(\bar g_i(T)^{e_i}) \longrightarrow \overbrace{A/\mathfrak{p}[T]/(\bar g_i(T))}^{\text{field}}\Big)$

surjective

$\Rightarrow$ $P_i \in \mathrm{Max}(B)$, $P_i \neq P_j$ for $i \neq j$, $\qquad \mathfrak{p}B \subset P_i \Rightarrow \underline{\mathfrak{p} = A \cap P_i}$

$[B/P_i : A/\mathfrak{p}] = \deg(\bar g_i)$

By definition, $P_i = \mathfrak{p}B + g_i(\alpha)A[\alpha] = \mathfrak{p}B + g_i(\alpha)B$

$\forall i$ $\quad P_i^{e_i} \subseteq \mathfrak{p}B + g_i(\alpha)^{e_i}B$

$$\Rightarrow \prod_{i=1}^r P_i^{e_i} \subseteq \mathfrak{p}B + \underbrace{\prod_{i=1}^r g_i(\alpha)^{e_i}}_{\equiv f(\alpha) \ (\mathrm{mod}\ \mathfrak{p}B),\ =0} B \subseteq \mathfrak{p}B \Rightarrow \mathfrak{p}B \mid P_1^{e_1}\cdots P_r^{e_r}$$

$$\Rightarrow \mathfrak{p}B = \prod_{i=1}^r P_i^{e'_i},\ e'_i \le e_i$$

But: $[L:K] = \dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{i=1}^r e_i \underbrace{\deg(\bar g_i)}_{[B/P_i : A/\mathfrak{p}]} \Rightarrow \forall i\ e'_i = e_i$

$\| \quad \sum_{i=1}^r e'_i [B/P_i : A/\mathfrak{p}]$

Ex: $K = \mathbb{Q}(\sqrt d)$, $d \in \mathbb{Z} \setminus \{0,1\}$ square-free, $\alpha = \sqrt d$, $f(T) = T^2 - d$

$(\mathcal{O}_K : \mathbb{Z}[\alpha]) = 1$ or 2. So:

$\forall p \neq 2$: $\left(\frac{d}{p}\right) = -1 \Rightarrow T^2 - d \ (\mathrm{mod}\ p) \in \mathbb{F}_p[T]$ irred. $\Rightarrow (p) \in \mathrm{Max}(\mathcal{O}_K)$

$\left(\frac{d}{p}\right) = 1 \Rightarrow T^2 - d \equiv (T-a)(T+a) \ (\mathrm{mod}\ p) \Rightarrow (p) = \mathfrak{p}\mathfrak{p}'$

$D_K = d$ or $4d$ $\qquad \mathfrak{p} = (\sqrt d - a, p)$, $\mathfrak{p}' = (\sqrt d + a, p)$

$p \mid d \Rightarrow T^2 - d \equiv T^2 \ (\mathrm{mod}\ p) \Rightarrow (p) = \mathfrak{p}^2$, $\mathfrak{p} = (\sqrt d, p)$

$\boxed{\text{What if } p \mid (\mathcal{O}_K : \mathbb{Z}[\alpha])\text{? Ex. in Schoof, p. 31}}$

In particular, $p \neq 2$ is ramified in $K/\mathbb{Q}$ $\Leftrightarrow$ $p \mid D_K$.

Exercise: what happens for $p = 2$?

Dedekind ζ-function

let $[K:\mathbb{Q}]<\infty$.

Def. The norm of a non-zero ideal $I\subset O_K$ is $N(I):=|O_K/I|$.

Prop. (1) $N(\prod_{i=1}^r P_i^{n_i}) = \prod_{i=1}^r N(P_i)^{n_i}$ $\quad$ ($P_i\in \mathrm{Max}(O_K)$ distinct, $n_i\geq 1$)
$(\Rightarrow N(IJ)=N(I)N(J))$.

(2) $\forall \alpha\in O_K\setminus\{0\}$ $\quad N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$.

Pf: (1) $O_K/\prod_i P_i^{n_i} \xrightarrow{\sim} \prod_i (O_K/P_i^{n_i})$ (Chinese Remainder Thm)

$O_K\supset P_i \supset \cdots \supset P_i^{n_i}$, $\quad P_i^k/P_i^{k+1}\simeq O_K/P_i \Rightarrow N(P_i^{n_i}) = \prod_{i=0}^{n_i-1} |P_i^k/P_i^{k+1}| = N(P_i)^{n_i}$

(2) $\exists\, \omega_1,\dots,\omega_n\in O_K$ ($[K:\mathbb{Q}]=n$) s.t. $O_K = \mathbb{Z}\omega_1\oplus\cdots\oplus\mathbb{Z}\omega_n$,
$\alpha O_K = d_1\omega_1\mathbb{Z}\oplus\cdots\oplus d_n\omega_n\mathbb{Z}$ as abelian groups ($d_i\geq 1$).
In the basis $\{\omega_i\}$, $r(\alpha)=A\in M_n(\mathbb{Z}) \Longrightarrow$
$N((\alpha)) = |O_K/\alpha O_K| = |\mathbb{Z}^n/A\mathbb{Z}^n| = |\det(A)| = |N_{K/\mathbb{Q}}(\alpha)|$.

Prop.-Def. The Dedekind zeta-function of K

$$\zeta_K(s) = \sum_{(0)\neq I\subset O_K} N(I)^{-s} = \prod_{P\in \mathrm{Max}(O_K)} (1-N(P)^{-s})^{-1}$$

is absolutely convergent for $\mathrm{Re}(s)>1$ (and $|\zeta_K(s)|\leq|\zeta(s)|^{[K:\mathbb{Q}]}$ then)

Pf: $\forall$ prime number p, $\quad \mathrm{Re}(s)>1$

$$\Big|\prod_{\substack{P|p\\ P\in\mathrm{Max}(O_K)}} (1-N(P)^{-s})^{-1}\Big| < |(1-p^{-s})|^{\#\{P|p\}} \leq |1-p^{-s}|^{[K:\mathbb{Q}]}$$

$(P_1,\dots,P_r|p,\quad N(P_i)=p^{f_i},\quad f_i\geq 1,\quad r\leq[K:\mathbb{Q}])$

$\zeta(s) = \prod_p (1-p^{-s})^{-1} = \prod_p (1+p^{-s}+p^{-2s}+\cdots) = \sum_{n=1}^\infty n^{-s}$ $\quad$ abs. conv. for $\mathrm{Re}(s)>1$

$\Rightarrow \zeta_K(s) = \prod_P (1-N(P)^{-s})^{-1} = \prod_P (1+N(P)^{-s}+N(P)^{-2s}+\cdots)^{-1} = \sum_{I\neq(0)} N(I)^{-s}$ — " —

Ex: $K=\mathbb{Q}(i)$: $\quad (2) = (1+i)^2$, $\quad N((1+i))=2$
$p\equiv 1 \pmod 4$ $\quad (p)=p\mathbb{Z}[i] = \pi\pi'$, $\quad N(\pi)=N(\pi')=p$
$p\equiv 3\pmod 4$ $\quad (p)=p\mathbb{Z}[i]\in \mathrm{Max}(\mathbb{Z}[i])$, $\quad N((p))=p^2$

$$\zeta_{\mathbb{Q}(i)}(s) = (1-2^{-s})^{-1}\prod_{p\equiv 1(4)}(1-p^{-s})^{-2}\prod_{p\equiv 3(4)}(1-p^{-2s})^{-1} = \zeta(s)\underbrace{\prod_{p\equiv 1(4)}(1-p^{-s})^{-1}\prod_{p\equiv 3(4)}(1+p^{-s})^{-1}}_{L(s)}$$

$L(s) = 1-3^{-s}+5^{-s}-7^{-s}+9^{-s}-\cdots$

$\mathrm{Res}_{s=1}\zeta(s)=1 \Longrightarrow \mathrm{Res}_{s=1}\zeta_{\mathbb{Q}(i)}(s) = 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots = \frac{\pi}{4}$

Special case (1): $K = \mathbb{Q}(\alpha)$, $\alpha \in O_K$, $f \in \mathbb{Z}[T]$ the minimal polynomial of α over $\mathbb{Q}$, p prime number s.t. $p \nmid \operatorname{disc}(f)$:

(a) $p \nmid \operatorname{disc}(f) = D(\mathbb{Z}[\alpha]/\mathbb{Z}) = D_K\,(O_K : \mathbb{Z}[\alpha])^2 \iff p \nmid D_K,\ p \nmid (O_K : \mathbb{Z}[\alpha])$

(b) $\bar{f} := f \pmod{p\mathbb{Z}[T]} \in \mathbb{F}_p[T]$ satisfies $\underbrace{\operatorname{disc}(\bar{f})}_{\operatorname{disc}(f) \pmod{p\mathbb{Z}}} \neq 0 \in \mathbb{F}_p$

$\Rightarrow \bar{f}$ is separable, $\bar{f} = \bar{g}_1 \cdots \bar{g}_r$, $\bar{g}_i \in \mathbb{F}_p[T]$ distinct monic irred. non-const

$\Longrightarrow$ $p O_K = P_1 \cdots P_r$, p is unramified in $K/\mathbb{Q}$.

Later on: p unramified in $K/\mathbb{Q} \iff p \nmid D_K$.

Special case (2): $K = \mathbb{Q}(\alpha)$, $\alpha \in O_K$, $f \in \mathbb{Z}[T]$ the min. pol. of α over $\mathbb{Q}$; assume f is an Eisenstein polynomial w.r.t. a prime number p:

(a) we know that $p \nmid (O_K : \mathbb{Z}[\alpha])$ in this case,

(b) $\bar{f} = T^n \in \mathbb{F}_p[T]$ $\quad (n = [K:\mathbb{Q}]) \Rightarrow pO_K = P^n$, p is totally ramified in $K/\mathbb{Q}$

$P = (p, \alpha)$

Both (1) and (2) hold true for L/K separable (with obvious modifications)

Cyclotomic fields

$m \geq 1$, $\zeta_m = e^{2\pi i/m}$, $\mu_m = \{\alpha \in \mathbb{C} \mid \alpha^m = 1\}$, $K_m = \mathbb{Q}(\zeta_m) = \mathbb{Q}(\mu_m)$

As $K_m = K_{m/2}$ if $m \equiv 2 \pmod 4$, we assume that $m \not\equiv 2 \pmod 4$

Prop. (1) $\chi_m : \operatorname{Gal}(K_m/\mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ $\quad (\zeta^{\chi_m(\sigma)} = \sigma(\zeta),\ \forall \zeta \in \mu_m)$ is an isomorphism $(\Longrightarrow [K_m : \mathbb{Q}] = \varphi(m))$.

(2) For a prime number p, write $m = m_0 p^n$ $(n \geq 0)$. Then $\mathbb{Q} \subset K_{m_0} \subset K_m = K_{m_0}(\zeta_{p^n})$, p is unramified in $K_{m_0}/\mathbb{Q}$ and each $P \mid p$ in K_{m_0} is totally ramified in K_m/K_{m_0}.

(3) If $p \nmid m$, let $f \geq 1$ be the minimal exponent s.t. $p^f \equiv 1 \pmod m$. Then $pO_{K_m} = P_1 \cdots P_g$, $fg = \varphi(m)$, $N(P_i) = p^f$ $\forall i$.

(4) $O_{K_m} = \mathbb{Z}[\zeta_m] = \bigoplus_{j=0}^{\varphi(m)-1} \mathbb{Z}\zeta_m^j$.

Pf: (3) Let $\Phi_m(T) = \prod_{\zeta \in \mu_m^0} (T - \zeta) = \prod_{d \mid m} \Phi_{m/d}(T)^{\mu(d)} \in \mathbb{Z}[T]$

$(\mu_m^0 = \{\alpha \in \mu_m \mid \forall d \mid m, d \neq m,\ \alpha^d \neq 1\})$. Then $\Phi_m(T) = \prod_{\substack{j=1 \\ (j,m)=1}}^{m} (T - \zeta_m^j)$, $\deg(\Phi_m) = \varphi(m)$, $\Phi_m(\zeta_m) = 0$.

χ_m is injective by definition $\Rightarrow$ $[K_m : \mathbb{Q}] \mid \varphi(m)$.

If $f \in \mathbb{Z}[T]$ is the minimal polynomial of ζ_m over $\mathbb{Q}$, then $f \mid \Phi_m \mid (T^m - 1)$. If p is a prime s.t. $\underline{p \nmid m}$, then $\gcd(T^m - 1, mT^{m-1}) = 1$ in $\mathbb{F}_p[T]$ $\Rightarrow$ $T^m - 1$, Φ_m, $f \pmod{p\mathbb{Z}[T]} \in \mathbb{F}_p[T]$ are separable

$\Rightarrow p \nmid \mathrm{disc}(f) \Rightarrow p \nmid D_{K_m}$, $p \nmid (\mathcal{O}_{K_m} : \mathbb{Z}[\zeta_m])$, p is unramified in $K_m/\mathbb{Q}$. (*)

Write $m = m_r = p_1^{n_1} \cdots p_r^{n_r}$ $(r \geq 1$, p_i distinct primes, $n_i \geq 1)$.

Induction on r shows:

(a) $K_{m_{r-1}} \subset K_{m_{r-1}}(\zeta_{p_r^{n_r}}) = K_{m_r}$ is obtained by adjoining the root $\zeta_{p_r^{n_r}} - 1$ of $\Phi_{p_r^{n_r}}(1+T)$, which is an <u>Eisenstein polynomial</u> w.r.t. any $P \mid p_r$ in $K_{m_{r-1}}$ (as $e(P/p_r) = 1$, by (*)), hence

$$[K_{m_r} : K_{m_{r-1}}] = \deg(\Phi_{p_r^{n_r}}) = \varphi(p_r^{n_r}) \Rightarrow [K_m : \mathbb{Q}] = \varphi(m), \ \chi_m \text{ isom.}$$

(b) $d_{\mathcal{O}_{K_{m_r}}/\mathcal{O}_{K_{m_{r-1}}}}$ divides $(\mathfrak{p}_r)^{\text{something}}$, $p \nmid (\mathcal{O}_{K_{m_r}} : \mathcal{O}_{K_{m_{r-1}}}[\zeta_{p_r^{n_r}}])$

$$\Rightarrow \mathcal{O}_{K_{m_r}} = \mathcal{O}_{K_{m_{r-1}}}[\zeta_{p_r^{n_r}}] \Longrightarrow \mathcal{O}_{K_m} = \mathbb{Z}[\zeta_{p_1^{n_1}}, \ldots, \zeta_{p_r^{n_r}}] = \mathbb{Z}[\zeta_m]$$

If $p \nmid m$, then $p \nmid m = \left.\dfrac{T^m - 1}{T - 1}\right|_{T=1} = \prod_{\zeta \in \mu_m \smallsetminus \{1\}} (1 - \zeta) \Rightarrow$ if $p\mathcal{O}_{K_m} = P_1 \cdots P_g$ in $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$, $\forall i$ the reduction map $\mu_m \longrightarrow (\mathcal{O}_{K_m}/P_i)^\times$ is injective $\Rightarrow m \mid N(P_i) - 1$.

As $K_m/\mathbb{Q}$ is a Galois extension, $\exists a \ \forall i \ N(P_i) = p^a$ (later), $ag = [K_m : \mathbb{Q}] = \varphi(m)$, $p^a \equiv 1 \pmod m \Rightarrow f \mid a$.

By definition, χ_m(the decomposition group of P_i) $\subset (\mathbb{Z}/m\mathbb{Z})^\times$ = the cyclic subgroup generated by $p \pmod m$, and its order is equal to a, hence $a = f$.

Decomposition group, inertia group

Assume: $A =$ Dedekind ring, $K = \mathrm{Frac}(A)$, L/K finite Galois extension, $B =$ normalisation of A in L. Set $G = \mathrm{Gal}(L/K)$.

Prop. (1) $\forall \sigma \in G$ $\sigma(B) = B$; (2) $B^G = A$; (3) $\forall \mathfrak{p} \in \mathrm{Max}(A)$ G acts transitively on $\{P \in \mathrm{Max}(B) \mid P \cap A = \mathfrak{p}\} = \{P | \mathfrak{p}\}$.

Pf: (1), (2) Exercise.
(3) If not, $\exists P, P' | \mathfrak{p}$ s.t. $\forall \sigma \in G$ ${}^\sigma P \neq P'$.
Approximation Thm $\Rightarrow$ $\exists b \in B$ $\forall \sigma \in G$ $\cancel{b} \equiv \begin{cases} 1 & (\mathrm{mod}\ {}^\sigma P) \\ 0 & (\mathrm{mod}\ {}^\sigma P') \end{cases}$

$$\Rightarrow N_{L/K}(b) = \prod_{\sigma \in G} \sigma(b) \equiv \begin{cases} 1 & (\mathrm{mod}\ P \cap A = \mathfrak{p}) \\ 0 & (\mathrm{mod}\ P' \cap A = \mathfrak{p}) \end{cases} \quad \text{contradiction.}$$

Def–Cor. For fixed $\mathfrak{p}$, the decomposition groups $D_P = \{\sigma \in G \mid {}^\sigma P = P\}$ of P $(P | \mathfrak{p})$ are conjugate in G.

Cor. $f = f(P/\mathfrak{p})$ (resp. $e = e(P/\mathfrak{p})$) depends only on $\mathfrak{p}$, hence
$\mathfrak{p} B = (P_1 \cdots P_g)^e$, $[B/P_i : A/\mathfrak{p}] = f$, $efg = n = [L:K] = |G|$
$\forall P | \mathfrak{p}$ $|G| = |D_P| \cdot \underbrace{|\text{orbit of } P|}_{g}$ $\Rightarrow$ $|D_P| = ef$.

Fix $P | \mathfrak{p}$ in B; set $D = D_P \subset G$. Then $\forall \sigma \in D$ ~~denote~~

$$\bar\sigma : \begin{array}{ccc} B/P & \longrightarrow & B/{}^\sigma P = B/P \\ b\ (\mathrm{mod}\ P) & \longmapsto & \sigma(b)\ (\mathrm{mod}\ P) \end{array}$$

is an element of $\mathrm{Aut}(\underbrace{k(P)}_{B/P} / \underbrace{k}_{A/\mathfrak{p}})$

Prop.–Def. (1) The extension $k(P)/k$ is normal. Denote by $k(P)_s/k$ its maximal separable subextension, $f_0 = [k(P)_s : k]$
($\Rightarrow$ $f = f_0 \times \begin{cases} 1 & \text{if } \mathrm{char}(k) = 0 \\ p^s & \text{if } \mathrm{char}(k) = p > 0 \end{cases}$).

(2) The homomorphism

$$\begin{array}{ccc} D & \longrightarrow & \mathrm{Aut}(k(P)/k) \xrightarrow{\sim} \mathrm{Gal}(k(P)_s/k) \\ \sigma & \longmapsto & \bar\sigma \end{array}$$

is surjective. Its kernel is the inertia group of P:
$I = I_P = \{\sigma \in D_P \mid \forall b\ (\mathrm{mod}\ P)\ \ \sigma(b) \equiv b\ (\mathrm{mod}\ P)\}$, $|I| = p^s e \left(= \frac{|D|}{f_0}\right)$

Pf: (1) $\forall \bar a \in k(P)$ fix $a \in B$ s.t. $\bar a = a\ (\mathrm{mod}\ P)$. Then $h(T) := \prod_{\sigma \in G} (T - \sigma(a)) \in A[T]$,
$h(a) = 0$ $\Rightarrow \bar h := h\ (\mathrm{mod}\ \mathfrak{p} A[T]) \in k[T]$ satisfies $\bar h(\bar a) = 0$
and each conjugate of $\bar a$ over k is a root of $\bar h$ $\Rightarrow$ is of the form $\sigma(a)\ (\mathrm{mod}\ P) \in k(P)$ (for some $\sigma \in G$). Thus $k(P)/k$ is normal.
(2) Fix $\bar a \in k(P)_s^\times$ s.t. $k(P)_s = k(\bar a)$. Approximation thm $\Rightarrow$ $\exists a \in B$ $a\ (\mathrm{mod}\ P) = \bar a$ and $\forall \sigma \in G \setminus D_P$ $a \in {}^\sigma P$ ($\Rightarrow \sigma^{-1}(a) \in P$). Set
$h(T) = \prod_{\sigma \in G} (T - \sigma(a)) \in A[T]$, $\bar h \in k[T]$ as above. Its $\neq 0$ roots are $\bar\sigma(\bar a)$, $\sigma \in D_P$
$\Rightarrow$ each conjugate of $\bar a$ is of the form $\bar\sigma(\bar a)$, $\sigma \in D_P$.

Fix $P \mid p$; $D := D_P \supset I_P = I$

<u>Cor</u>: Set $K_D = L^D \subset K_I = L^I$. The splitting behaviour of p in L/K is as follows:

$$K \xhookrightarrow{\;g\;} K_D \xhookrightarrow[\text{unramified}]{f_0} K_I \xhookrightarrow{\;p^s e\;} L$$

$$\begin{array}{lccccccc}
 & p & \underbrace{\qquad\qquad} & Q & \underbrace{\qquad\qquad} & R & \underbrace{\qquad\qquad} & P \\
e & & 1 & & 1 & & e & \\
f & & 1 & & f_0 & & p^s &
\end{array}$$

$$k = k(p) \;=\!=\!=\; k(Q) \xhookrightarrow[\text{Galois } D/I]{f_0} k(R) \xhookrightarrow[\text{purely insep.}]{p^s} k(P) \qquad \text{(residue fields)}$$

<u>Special case</u>: $k(P)/k$ <u>separable</u> ($\Longleftrightarrow$ Galois)

$$\underbrace{K \hookrightarrow \underbrace{K_D \underbrace{\xhookrightarrow[\text{unramified}]{}}_{D/I} K_I \underbrace{\xhookrightarrow[\text{totally ramified}]{}}_{\text{Galois group} = I} L}_{D}}_{G}$$

$$k = k(p) \;=\!=\!=\; k(Q) \underbrace{\xhookrightarrow[\text{Galois}]{f}}_{D/I} k(R) \;=\!=\!=\; k(P)$$

$I \trianglelefteq D$, $D/I \xrightarrow{\sim} \mathrm{Gal}(k(P)/k)$, $|I| = e$, $|D| = ef$

$I = \{1\} \Longleftrightarrow e = 1 \Longleftrightarrow D \xrightarrow{\sim} \mathrm{Gal}(k(P)/k) \Longleftrightarrow P$ <u>unramified in L/K</u>

$\Longleftrightarrow p$ ——— " ———

<u>Ex</u>: <u>Number fields case</u>: L/K finite Galois extension, $[L:\mathbb{Q}] < \infty$

If $p \subset O_K$ is <u>unramified in L/K</u> and $P \mid p$ $(P \subset O_L)$, then

$$G \supset D = D_P \xrightarrow{\sim} \mathrm{Gal}(k(P)/k(p)) = \mathrm{Gal}(\mathbb{F}_{\underset{N(p)^f}{N(P)}} / \mathbb{F}_{N(p)})$$

is cyclic of order f; it is generated by the (arithmetic) <u>Frobenius element</u> $\sigma = \mathrm{Fr}_{L/K}(P) = \left(\frac{L/K}{P}\right) \in D \subset G$, which is characterised by

$$\forall b \in O_L \qquad \sigma(b) \equiv b^{N(p)} \pmod{P}.$$

<u>Properties</u>: (1) $\forall \tau \in G \quad \left(\frac{L/K}{\tau(P)}\right) = \tau \left(\frac{L/K}{P}\right) \tau^{-1} \in D_{\tau(P)} = \tau D_P \tau^{-1}$

(2) $f = f(P \mid p)$ = the order of $\left(\frac{L/K}{P}\right)$.

Ex: Cyclotomic fields: $m \not\equiv 2 \pmod 4$, $K_m = \mathbb{Q}(\mu_m)$, $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$

$p \nmid m$ prime number $\Rightarrow$ p unramified in $K_m/\mathbb{Q}$

Fix $P \mid p$ in $\mathcal{O}_{K_m}$; as $G = \mathrm{Gal}(K_m/\mathbb{Q})$ is abelian, $D_p = D_P$ depends only on p.

Claim: $\chi_m : G \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ maps $\left(\frac{K_m/\mathbb{Q}}{p}\right) = \sigma$ to $p \pmod m$.

Pf: $\forall\, x \in \mathcal{O}_{K_m}$ $\quad \sigma(x) \equiv x^p \pmod P$

Taking $x = \zeta_m \in \mu_m$, we get $\zeta_m^{\chi_m(\sigma)} \equiv \zeta_m^p \pmod P \Rightarrow \chi_m(\sigma) = p$, since $\mu_m \longrightarrow (\mathcal{O}_{K_m}/P)^\times$ is injective.

Cor: $p\mathcal{O}_{K_m} = P_1 \cdots P_g$, $\quad fg = [K_m : \mathbb{Q}] = \varphi(m)$,

$f =$ order of $p \pmod m$ in $(\mathbb{Z}/m\mathbb{Z})^\times = \min.\ a \geq 1$ s.t. $p^a \equiv 1 \pmod m$

So: the splitting of $p \nmid m$ in $\mathbb{Q}(\mu_m)/\mathbb{Q}$ depends only on $p \pmod m$!

Ex: Quadratic reciprocity law: $q \neq 2$ prime number

$$\mathbb{Q} \subset \underbrace{\mathbb{Q}(\sqrt{\mathrm{disc}(f)})}_{\underbrace{\mathbb{Q}(\sqrt{q^*})}_{K}} \subset \underbrace{\mathbb{Q}(\zeta_q)}_{L} = \text{splitting field of } \quad f(T) = \frac{T^q - 1}{T-1}$$

$$q^* = (-1)^{\frac{q-1}{2}} q \qquad \mathrm{disc}(f) = (-1)^{\frac{q-1}{2}} q^{q-2}$$

splitting of $p \neq 2, q$ in $\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}$ depends only on $\left(\frac{q^*}{p}\right)$

———— " ———— $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ —— " —— on $p \pmod q$

$$\begin{array}{rccc} \chi_q : & \mathrm{Gal}(L/\mathbb{Q}) & \xrightarrow{\sim} & (\mathbb{Z}/q\mathbb{Z})^\times = \mathbb{F}_q^\times \\ & \cup & & \cup \\ & \mathrm{Gal}(L/K) & \xrightarrow{\sim} & \mathbb{F}_q^{\times 2} \end{array}$$

$$\Rightarrow \quad \begin{array}{ccc} \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2} \xleftarrow{\sim} \mathrm{Gal}(L/\mathbb{Q})/\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} & \{\pm 1\} \\ \Psi & \Psi \\ a\,\mathbb{F}_q^{\times 2} \longmapsto & \left(\frac{a}{q}\right) \end{array}$$

$\left(\frac{q^*}{p}\right) = 1 \Leftrightarrow p$ splits in $K/\mathbb{Q} \Leftrightarrow \left(\frac{K/\mathbb{Q}}{p}\right) = 1 \Leftrightarrow \left(\frac{L/\mathbb{Q}}{p}\right) \in \mathrm{Gal}(L/K)$

$\Leftrightarrow p \pmod q \in \mathbb{F}_q^{\times 2} \Leftrightarrow \left(\frac{p}{q}\right) = 1$

Characters

Def. G finite abelian group. A *character* of G is a morphism of groups $\chi : G \to U(1)$ $\quad (U(1) = \{z \in \mathbb{C}^\times \mid |z| = 1\})$. The characters of G form an abelian group $\widehat{G}$ $\quad ((\chi\chi')(g) = \chi(g)\chi'(g))$.

Ex: G cyclic of order n. For each generator $\sigma \in G$, the map
$$\widehat{G} \longrightarrow \mu_n(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1\}$$
$$\chi \longmapsto \chi(\sigma)$$
is an isomorphism of groups
($\Rightarrow \widehat{G}$ is also cyclic of order n)

Prop: (1) $\widehat{G_1 \oplus G_2} = \widehat{G_1} \oplus \widehat{G_2}$

(2) $\widehat{G}$ is non-canonically isomorphic to G

(3) The biduality map $\begin{aligned} G &\longrightarrow \widehat{\widehat{G}} \\ g &\longmapsto (\chi \mapsto \chi(g)) \end{aligned}$ is an isomorphism $\quad (g \in G, \chi \in \widehat{G})$

Pf: (1) Clear. (2),(3) Write $G \simeq \oplus$ cyclic gps & apply (1) (& Ex. above)

Functoriality: $\alpha : G \to H$ gp. morphism induces $\begin{aligned} \hat{\alpha} : \widehat{H} &\longrightarrow \widehat{G} \\ \psi &\longmapsto (g \mapsto \psi(\alpha(g))) \end{aligned}$ $\quad (\hat{\alpha}(\psi) = \psi \circ \alpha)$

Dirichlet characters

Def. Let $m \geq 1$. A *Dirichlet character* (mod m) is an element of $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$: $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to U(1)$. Its *conductor* f_χ is the smallest $f_\chi \mid m$ (w.r.t. divisibility) s.t. χ factors ~~through~~ as
$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\text{proj.}} \underbrace{(\mathbb{Z}/f_\chi\mathbb{Z})^\times \xrightarrow{\chi_{prim}} U(1)}$$
the *primitive character* associated to χ.

~~Ex~~ (if $f_\chi = m$, then $\chi = \chi_{prim}$ is primitive).

Ex: (1) If $\chi = 1$, then $f_\chi = 1$.

(2) $\forall$ prime $p \neq 2$, the Legendre symbol $\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ is primitive

Def. The *Dirichlet L-function* of $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to U(1)$ is
$$L(s, \chi) = \sum_{\substack{n \geq 1 \\ (n, f_\chi) = 1}} \frac{\chi_{prim}(n)}{n^s} = \prod_{p \nmid f_\chi} \left(1 - \frac{\chi_{prim}(p)}{p^s}\right)^{-1} \quad (= L(s, \chi_{prim}))$$
(abs. conv. for $\mathrm{Re}(s) > 1$)

Ex: $\chi = 1 \Rightarrow L(s, 1) = \zeta(s)$

Thm. $\forall m \geq 1$ $\quad \zeta_{\mathbb{Q}(\zeta_m)}(s) = \prod_{\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to U(1)} L(s,\chi)$

$\zeta_m = e^{2\pi i/m}$

[case $m=4$: $\quad \zeta_{\mathbb{Q}(i)}(s) = \zeta(s)\,(1^{-s} - 3^{-s} + 5^{-s} - 7^{-s} + \cdots)$]

"Pf" (only for the Euler factors at $p \nmid m$): if $p \nmid m$, then

$$p\,\mathcal{O}_{\mathbb{Q}(\zeta_m)} = P_1 \cdots P_g, \quad N(P_i) = p^f, \quad fg = \varphi(m), \quad f = \min.\ a \geq 1 \text{ s.t. } p^a \equiv 1 \ (m)$$

Lemma. G finite abelian group, $\sigma \in G \Rightarrow \prod_{\chi \in \widehat{G}} (1 - \chi(\sigma)T) = (1 - T^f)^{|G|/f}$

$f =$ the order of σ

Pf of Lemma: let $\langle\sigma\rangle \subset G$ be the subgp. generated by σ and $\langle\sigma\rangle^\perp = \{\chi \in \widehat{G} \mid \chi(\sigma) = 1\} \subset \widehat{G}$. Then the restriction $\widehat{G} \longrightarrow \widehat{\langle\sigma\rangle}$ is surjective, hence $\widehat{G}/\langle\sigma\rangle^\perp \xrightarrow{\sim} \widehat{\langle\sigma\rangle}$, which implies that

$$\prod_{\chi \in \widehat{G}} (1 - \chi(\sigma)T) = \prod_{\chi \in \widehat{\langle\sigma\rangle}} (1 - \chi(\sigma)T)^{|\widehat{G}|/|\widehat{\langle\sigma\rangle}|} = \prod_{j \in \mathbb{Z}/f\mathbb{Z}} (1 - \zeta_f^j T)^{|G|/f} = (1 - T^f)^{|G|/f}.$$

Apply Lemma to $G = (\mathbb{Z}/m\mathbb{Z})^\times$, $\sigma = p \pmod m$, $T = p^{-s}$:

$$\prod_{\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to U(1)} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{fs}}\right)^{\varphi(m)/f} = \prod_{j=1}^{g} \left(1 - \frac{1}{N(P_j)^s}\right)$$

Subfields of $\mathbb{Q}(\zeta_m)$

Let $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_m)$. Then $\chi_m : \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$

$$\widehat{\mathrm{Gal}(K/\mathbb{Q})} \xrightarrow{\sim} \{\psi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow U(1) \mid \psi(\underbrace{\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)}_{H}) = 1\} = H^\perp$$

Thm. $\zeta_K(s) = \prod_{\psi : \mathrm{Gal}(K/\mathbb{Q}) \to U(1)} L(s,\psi) = \prod_{\substack{\psi : (\mathbb{Z}/m\mathbb{Z})^\times \to U(1) \\ \psi|_H = 1}} L(s,\psi).$

Ex: $q \neq 2$ prime number, $K = \mathbb{Q}(\sqrt{q^*}) \subset \mathbb{Q}(\zeta_q)$ $\quad q^* = (-1)^{\frac{q-1}{2}} q$

$U(1) \xleftarrow{\psi} (\mathbb{Z}/q\mathbb{Z})^\times = \mathbb{F}_q^\times \supset \mathbb{F}_q^{\times 2} \simeq H$, $\quad \psi|_H = 1 \iff \psi = 1$ or $\psi = \left(\frac{\cdot}{q}\right) = \left(\frac{q^*}{\cdot}\right)$

$$\zeta_{\mathbb{Q}(\sqrt{q^*})}(s) = \zeta(s)\, L\left(s, \left(\frac{\cdot}{q}\right)\right)$$

"Pf": for $p \nmid m$, apply Lemma below to $G = (\mathbb{Z}/m\mathbb{Z})^\times \supset H$ as above, $\sigma = p \pmod m$ $\quad (\Longrightarrow p\,\mathcal{O}_K = P_1 \cdots P_g,\ N(P_i) = p^f,\ fg = [K:\mathbb{Q}] = |G/H|)$

Lemma: $G \supset H$ finite ab. gps, $\sigma \in G$, $pr : G \longrightarrow G/H$ the projection $\Longrightarrow$

$$\prod_{\substack{\chi \in \widehat{G} \\ \chi(H) = 1}} (1 - \chi(\sigma)T) = \prod_{\psi \in \widehat{G/H}} (1 - \psi(pr(\sigma))T) = (1 - T^f)^{|G/H|/\underbrace{\text{order of } pr(\sigma)}_{f}}$$

Valuations

Recall: $\forall\, a \in \mathbb{Q}^\times$ $\quad \|a\|_\infty \prod_{p \text{ prime}} \|a\|_p = 1$, $\quad \|a\|_\infty = |a|$, $\|p^n \frac{b}{c}\|_p = p^{-n}$ $\;(p \nmid b, c)$, $b, c \in \mathbb{Z}$

$\|\cdot\|_v$ are valuations (normalised) of $\mathbb{Q}$ $\quad (\|0\|_v = 0)$.

Def. A valuation of a field K is a map $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ s.t.

(I) $|x| = 0 \iff x = 0$

(II) $|xy| = |x|\,|y| \quad \forall x, y \in K$ $\Big\} \Rightarrow |\cdot| : K^\times \longrightarrow \mathbb{R}^\times_{>0}$ is a group morphism

(III) $\exists\, C > 0 \quad |x+y| \leq C \max(|x|, |y|)$ $\quad$ —"—

Ex: (0) trivial valuation: $\forall x \in K^\times \quad |x| = 1$ $\qquad (C=1)$

(1) usual $|x|$ on $K = \mathbb{C}$ $\qquad (C=2)$

(2) $K = \mathrm{Frac}(A)$, A Dedekind ring, $\mathfrak{p} \in \mathrm{Max}(A)$, $0 < \rho < 1$, $|x| = \rho^{v_{\mathfrak{p}}(x)}$ $\qquad (C=1)$

Prop. 1: (a) $\forall$ valuation $|\cdot|$ on K $\forall a \in \mathbb{R}_{>0}$ $\underbrace{|\cdot|^a \text{ is also a valuation on } K}_{\text{"valuations equivalent to } |\cdot| \text{"}}$

(b) Each valuation $|\cdot|$ is equivalent to one for which $C = 2$

(c) If $C=2$ for $|\cdot|$, then $\forall x, y \in K$ $\quad |x+y| \leq |x| + |y|$ (triangle inequality)

$\Rightarrow$ $\mathrm{dist}(x,y) := |x-y|$ is a metric on K.

Pf: (a), (b) trivial; (c) $C = 2 \overset{\text{induction}}{\Longrightarrow} \forall r \geq 1 \;\; \forall x_i \in K \;\; \left|\sum_{i=1}^{2^r} x_i\right| \leq 2^r \max |x_i|$

$\forall n \geq 1 \;\exists r\;\; 2^{r-1} < n \leq 2^r \Rightarrow \left|\sum_{i=1}^{n} x_i\right| \leq 2^r \max|x_i| \leq 2n \max|x_i| \Rightarrow |\underbrace{n \cdot 1_K}_{n}| \leq 2n$

$\forall x, y \in K \quad |x+y|^n = \left|\sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}\right| \leq 2(n+1) \max_{0 \leq j \leq n} \left(\left|\binom{n}{j}\right| |x|^j |y|^{n-j} \right) \leq$

$\leq 4(n+1) \max_{0 \leq j \leq n} \left(\binom{n}{j} |x|^j |y|^{n-j} \right) \leq 4(n+1)(|x|+|y|)^n \Longrightarrow |x+y| \leq \sqrt[n]{4(n+1)}\,(|x|+|y|)$

Let $n \to +\infty$ $\Rightarrow$ $|x+y| \leq |x| + |y|$.

Prop. 2: (a) the sets $\{x \in K \mid |x - x_0| < r\}$ $(x_0 \in K, r > 0)$ form a basis of a topology on K, which depends only on the equivalence class of $|\cdot|$.

(b) If $C = 2$, this is the topology defined by the metric $|x-y|$.

(c) K is a topological field (mult., add. $K \times K \to K$, inverse: $K^\times \to K^\times$ are cont.)

(d) Two valuations $|\cdot|_1, |\cdot|_2$ define the same topology $\iff$ they are equivalent.

Pf: (a), (b) trivial; (c) exercise; (d) for $z \in K$, $|z|_1 < 1 \iff \lim_{n \to +\infty} z^n = 0 \iff |z|_2 < 1$

For $x, y \in K^\times$ and $m, n \in \mathbb{Z}$, take $z = x^m y^n$: $\; m \log|x|_1 + n \log|y|_1 \gtrless 0 \iff$ idem for $|\cdot|_2$

$\Rightarrow \dfrac{\log|x|_1}{\log|y|_1} = \dfrac{\log|x|_2}{\log|y|_2} \Rightarrow |\cdot|_1, |\cdot|_2$ are equivalent.

Ex: $K = \mathbb{Q}$, $|\cdot| = \|\cdot\|_p \Rightarrow \lim_{n \to +\infty} p^n = 0$, basis of open sets: $a + p^n \mathbb{Z}_{(p)}$ $(a \in \mathbb{Q}, n \in \mathbb{Z})$

(Non-) archimedean valuations

<u>Def</u>. A valuation $|\cdot|$ on K is <u>non-archimedean</u> if (III) holds with $C=1$:
$\forall x,y\in K \quad |x+y|\leq \max(|x|,|y|)$ $\quad$ ($\Rightarrow$ all equivalent valuations are non-arch.)
Otherwise $|\cdot|$ is <u>archimedean</u>.

<u>Ex</u>: (1) $\forall \sigma: K\hookrightarrow \mathbb{C}$, $\quad x\mapsto |\sigma(x)|$ is an <u>archimedean</u> val. on K
(and all arch. val. on K are equivalent to $|\sigma(x)|$, for some $\sigma: K\hookrightarrow\mathbb{C}$).
(2) $|x| = \rho^{v_{\mathfrak{p}}(x)}$ on $K=\mathrm{Frac}(A)$ (A Dedekind, $\mathfrak{p}\in\mathrm{Max}(A)$) is <u>non-arch.</u>

<u>Prop 3.</u> Assume $|\cdot|$ is non-archimedean. (a) If $x,y\in K$, $|x|<|y| \Rightarrow |x+y|=|y|$
(b) $\underset{\sim}{\mathcal{O}} = \{x\in K \mid |x|\leq 1\}$ is a subring of K, $\mathfrak{m}=\{x\in K\mid |x|<1\}$ is a maximal ideal of $\mathcal{O}$
the <u>valuation ring</u> of $|\cdot|$, $\quad(\mathcal{O},\mathfrak{m})$ is a <u>local ring</u>; $k:=\mathcal{O}/\mathfrak{m}$ the <u>residue field</u> of $|\cdot|$,
(c) $\mathcal{O}$ is a DVR $\Leftrightarrow$ $\mathfrak{m}$ is a principal ideal. | $K=\mathrm{Frac}(\mathcal{O})$

<u>Pf</u>: (a) $|x|<|y| \;\; |y| = |(x+y)+(-x)| \leq \max(|x|,|x+y|) \Rightarrow |x+y|\geq |y|>|x| \Rightarrow |x+y|=|y|$.
(b) trivial; (c) exercise.

<u>Prop. 4</u>. A valuation $|\cdot|$ on K is non-archimedean $\Leftrightarrow$ $\forall n\in\mathbb{Z}\quad |\underbrace{n\cdot 1_K}_{n\in K}|\leq 1$

<u>Cor</u>: $\mathrm{char}(K)=p>0 \Rightarrow$ all val. on K are non-arch.

<u>Pf of Prop. 4</u>: ($\Rightarrow$) trivial; ($\Leftarrow$) we can assume that $C=2$; $\forall x,y\in K$

$$|x+y|^n = \Big|\sum_{j=0}^{n}\binom{n}{j}x^j y^{n-j}\Big| \leq \sum_{j=0}^{n}|x|^j|y|^{n-j}\leq (n+1)\max(|x|,|y|)^n \Rightarrow |x+y|\leq \sqrt[n]{n+1}\max(|x|,|y|)$$

letting $n\to+\infty$, $\quad |x+y|\leq\max(|x|,|y|)$.

$\boxed{\text{Cor: } \mathrm{char}(K)=p>0 \Rightarrow \text{any } |\cdot| \text{ on } K \text{ is non-arch. } (\mathbb{Z}\cdot 1_K=\mathbb{F}_p\cdot 1_K,\ \forall a\in\mathbb{F}_p^\times\ a^{p-1}=1 \Rightarrow |a|=1)}$

<u>Thm</u> (Ostrowski) A non-trivial valuation $|\cdot|$ on $\mathbb{Q}$ is equivalent to $\|\cdot\|_\infty$ or $\|\cdot\|_p$.

<u>Pf</u>. Again, we can assume that $C=2$. Let $a\in\mathbb{Z}_{>1}$. For any $b\in\mathbb{Z}_{>0}$,
$b=b_m a^m+\dots+b_0$, $\quad 0\leq b_j<a$, $\quad m\leq \log(b)/\log(a) \Rightarrow$

$$|b|\leq\sum_{i=0}^{m}|b_i||a|^i\leq (m+1)\underbrace{\max(|1|,\dots,|a-1|)}_{M}\max(1,|a|^m)\leq M\Big(1+\frac{\log(b)}{\log(a)}\Big)\max(1,|a|^{\log(b)/\log(a)})$$

Let $b=c^n$, $n\to+\infty \Rightarrow \forall c\in\mathbb{Z}_{>0}\quad |c|\leq\max(1,|a|^{\log(c)/\log(a)})$.

(case 1) $\exists c\in\mathbb{Z}\ |c|>1 \Rightarrow \forall a\in\mathbb{Z}_{>1}\ |a|>1 \overset{a\leftrightarrow c}{\Longrightarrow} |c|^{1/\log(c)}=|a|^{1/\log(a)} \Rightarrow |\cdot|$ is eq. to $\|\cdot\|_\infty$.
(case 2) $\forall c\in\mathbb{Z}\ |c|\leq 1 \Rightarrow |\cdot|$ non-trivial non-arch. $\Rightarrow I=\{a\in\mathbb{Z}\mid |a|<1\}$ is
a non-zero prime ideal of $\mathbb{Z} \Rightarrow I=p\mathbb{Z}$ (p prime) $\Rightarrow |\cdot|$ is eq. to $\|\cdot\|_p$.

<u>Exercise</u>. Let k be a field. Show that a non-trivial valuation on $k(t)$
which is trivial on k is equivalent to $\|\cdot\|_\infty$ or $\|\cdot\|_p$ from p. ... .

Prop. – Def. A valuation $|\cdot|$ on K is <u>discrete</u> if it is non-trivial and $|K^\times|$ is a $(\neq\{1\})$ discrete subgroup of $\mathbb{R}^\times_{>0}$. In this case $|\cdot|$ is non-archimedean, the valuation ring $\mathcal{O}$ of $|\cdot|$ is a DVR and $|\cdot| = \rho^{v(\cdot)}$ for some $0<\rho<1$, where $v: K^\times \twoheadrightarrow \mathbb{Z}$ is the normalised additive discrete valuation associated to $\mathcal{O}$.

Pf. $|K^\times| \subset \mathbb{R}^\times_{>0}$ is a discrete subgroup $\neq \{1\} \Rightarrow$ equal to $\rho^{\mathbb{Z}}$, $0<\rho<1$.
If $\mathrm{char}(K)>0 \Rightarrow |\cdot|$ is non-arch. If $\mathrm{char}(K)=0 \Rightarrow \mathbb{Q}\subset K$, $|\mathbb{Q}^\times| \subset |K^\times|$ is discrete $\overset{\text{Ostrowski}}{\Longrightarrow}$ $|\mathbb{Z}\cdot 1_K| = \|\mathbb{Z}\|_p^{\text{sth.}} \leq 1 \Rightarrow |\cdot|$ is non-arch.
If $|\pi| = \rho$, then $K^\times = \pi^{\mathbb{Z}}\mathcal{O}^\times \Rightarrow \mathcal{O}$ is a DVR, $|\pi^n u| = \rho^n = \rho^{v(\pi^n u)}$ $(u\in\mathcal{O}^\times)$.

Extensions of discrete valuations

<u>Assume</u>: A Dedekind ring, $K=\mathrm{Frac}(A)$, $[L:K]<\infty$, B = normalisation of A in L s.t. (F) B is an A-module of finite type.

Prop. – Def: (1) there are natural group morphisms $I(A) \underset{N}{\overset{i}{\rightleftarrows}} I(B)$ given by $i(I) = IB$, $N(J) = (B:J)$ (index of A-modules)
($N = N_{B/A}$ is the <u>relative norm</u>). ($J\subset B$, $I\subset A$ non-zero ideals)

(2) $\forall \mathfrak{p}\in\mathrm{Max}(A)$ $\quad N_{B/A}(J)_\mathfrak{p} = N_{B_\mathfrak{p}/A_\mathfrak{p}}(JA_\mathfrak{p})$ $\quad (B_\mathfrak{p} = BA_\mathfrak{p})$

(3) $\forall \beta\in B\smallsetminus\{0\}$ $\quad N((\beta)) = (N_{L/K}(\beta))$

(4) $\quad N(i(I)) = I^n$, $n=[L:K]$

(5) $\quad v_P(i(I)) = e(P|\mathfrak{p})\, v_\mathfrak{p}(I)$ $\quad (\mathfrak{p} = P\cap A,\ P\in\mathrm{Max}(B))$

(6) $\quad v_\mathfrak{p}(N(J)) = \sum_{P|\mathfrak{p}} f(P|\mathfrak{p})\, v_P(J)$ $\quad (\mathfrak{p}\in\mathrm{Max}(A))$

In particular, $N_{B/A}(P) = \mathfrak{p}^f$, $\mathfrak{p} = P\cap A$, $f = f(P|\mathfrak{p})$.

(7) $\forall \beta\in L^\times$ $\forall \mathfrak{p}\in\mathrm{Max}(A)$ $\quad v_\mathfrak{p}(N_{L/K}(\beta)) = \sum_{P|\mathfrak{p}} f(P|\mathfrak{p})\, v_P(\beta)$

Pf: (2) (1) i morphism } clear; (1) N morphism: as in the case $A=\mathbb{Z}$
(3) replace A by $A_\mathfrak{p}$; then — " — (as $B_\mathfrak{p}$ is free over $A_\mathfrak{p}$)
(4) $B/i(I)B \simeq (A/I)^n$; (5) $I = \mathfrak{q}\in\mathrm{Max}(A) \Rightarrow i(I) = Q_1^{e_1}\cdots Q_r^{e_r}$,
$v_P(i(I)) = \begin{cases} e_i & P=Q_i \\ 0 & P\notin\{Q_i\}\end{cases}$, $v_\mathfrak{p}(I) = \begin{cases} 1 & \mathfrak{p}=\mathfrak{q} \\ 0 & \mathfrak{p}\neq\mathfrak{q}.\end{cases}$

(6) $N_{B/A}(P) = \mathfrak{p}^f$: as in the case $A=\mathbb{Z}$; general case by multiplicativity
(7) combine (3), (6).

<u>Cor</u>: there are induced morphisms $\mathrm{Pic}(A) \underset{N}{\overset{i}{\rightleftarrows}} \mathrm{Pic}(B)$, $N\circ i = [L:K]$

Completions

Def. A field K is <u>complete</u> w.r.t. a <u>valuation $|\cdot|$</u> if it is a complete metric space w.r.t. $\mathrm{dist}(x,y) = |x-y|^a$ $\quad (a>0$ s.t. $|\cdot|^a$ has $C=2)$.

~~Prop.~~ **Def.** Let $(K_i, |\cdot|_i)$ $(i=1,2)$ be fields with a valuation. A <u>morphism of valued fields</u> $(K_1,|\cdot|_1) \longrightarrow (K_2,|\cdot|_2)$ is a field morphism $\sigma: K_1 \longrightarrow K_2$ s.t. $\forall x \in K_1$ $|\sigma(x)|_2 = |x|_1$ (we also say that $|\cdot|_2$ <u>extends</u> $|\cdot|_1$, if we view K_1 as a subfield of K_2 via σ).

Prop. – Def. A <u>completion</u> of K w.r.t. a valuation $|\cdot|$ is a morphism of valued fields $\imath: K \longrightarrow \widehat{K}$ s.t. $\widehat{K}$ is complete and $\imath(K)$ is dense in $\widehat{K}$. It exists and is universal ($\Rightarrow$ unique up to isomorphism): $\forall$

$$\begin{array}{ccc} K & \xrightarrow{\imath} & \widehat{K} \\ & \searrow^{\sigma} & \downarrow \exists! \tau \\ & & \underbrace{L}_{\text{complete}} \end{array} \qquad \tau \circ \imath = \sigma$$

(σ morphism of valued fields)

Pf: $\widehat{K}$ = the completion of the metric space K, $\mathrm{dist}(x,y) = |x-y|^a$:
$= \{\text{Cauchy sequences in } K\} / \{\text{sequences} \to 0\}$
this is a field with obvious operations and valuation $|\{a_n\}| = \lim\limits_{n\to+\infty} |a_n|$.

Ex: (1) $K = \mathbb{Q}$, $|\cdot| = \|\cdot\|_\infty \Rightarrow \widehat{K} = \mathbb{R}$.

(2) $|\cdot|$ non-arch $\Rightarrow$ $|\cdot|$ non-arch on $\widehat{K}$ and $|\widehat{K}^\times| = |K^\times|$
$(\forall y \in \widehat{K}^\times\ \exists x \in K\ \ |x-y| < |y| \Rightarrow |x| = \max(|x-y|, |y|) = |y|\ )$

<u>Special case (discrete valuations):</u> $K = \mathrm{Frac}(A)$, A DVR, $\pi \in A$ unif., $|\pi^n u| = \rho^n$ $\quad (u \in A^\times,\ n \in \mathbb{Z})$ $\quad 0<\rho<1$

Def: $\left.\begin{array}{l} \widehat{A} := \varprojlim\limits_n A/\pi^n A \\ \text{(the } \pi\text{-adic completion of } A) \end{array}\right\} \Rightarrow \widehat{A} = \left\{ \sum\limits_{n=0}^{\infty} a_n \pi^n \ \middle|\ a_n \in S \right\}$ $\quad S \subset A$ repr. of A/π

$\widehat{A}$ is a DVR, $\pi \in \widehat{A}$ unif., $\widehat{A}/\pi^n\widehat{A} = A/\pi^n A$

$\Rightarrow \widehat{\widehat{A}} = \widehat{A}$ $\quad$ ($\widehat{A}$ is a <u>complete</u> DVR).

$\widehat{K} = \mathrm{Frac}(\widehat{A}) = \widehat{A}[1/\pi]$, $|\cdot|$ extends to $\widehat{K}$ $\quad (|\pi^n u| = \rho^n,\ u \in \widehat{A}^\times, n \in \mathbb{Z})$

Topology on $\widehat{A}$ induced by $|\cdot|$ = π-adic topology
(= $\varprojlim$ topology, $A/\pi^n A$ discrete)

$\Rightarrow$ $\left.\begin{array}{l} A \text{ is dense in } \widehat{A} \\ K \text{ —— '' —— } \widehat{K} \end{array}\right\} \Rightarrow \widehat{K}$ = the completion of $(K, |\cdot|)$.

<u>Ex:</u> (1) $A = \mathbb{Z}_{(p)}$, $K = \mathbb{Q}$, $\pi = p$, $\rho = p^{-1}$, $|\cdot| = \|\cdot\|_p$, $\widehat{A} = \mathbb{Z}_p$, $\widehat{K} = \mathbb{Q}_p$

(2) $A = k[t]_{(t-a)}$, $K = k(t)$, $\pi = t-a$, $\widehat{A} = k[[t-a]] = \left\{ \sum\limits_{n=0}^{\infty} b_n (t-a)^n \ \middle|\ b_n \in k \right\}$
$a \in k$ field

A Dedekind ring ($\neq$ field), $\mathfrak{p} \in \mathrm{Max}(A)$, $K = \mathrm{Frac}(A)$, $0 < \rho < 1$

$|x| = \rho^{v_\mathfrak{p}(x)}$ is a discrete valuation on K

<u>$\mathfrak{p}$-adic completion of A</u>: $\hat{A}_\mathfrak{p} := \varprojlim_n A/\mathfrak{p}^n = \varprojlim_n A_\mathfrak{p}/\underbrace{(\mathfrak{p}A_\mathfrak{p})^n}_{\pi^n A_\mathfrak{p}}$

$\pi \in A_\mathfrak{p}$ uniformiser

$\hat{A}_\mathfrak{p}$ is a DVR with uniformiser π

$\hat{A}_\mathfrak{p}/\pi^n\hat{A}_\mathfrak{p} = A_\mathfrak{p}/\pi^n A_\mathfrak{p} = A/\mathfrak{p}^n$ $\Rightarrow |x| = \rho^{v_\mathfrak{p}(x)}$ defines a valuation on $\mathrm{Frac}(\hat{A}_\mathfrak{p})$

$\hat{A}_\mathfrak{p} = \{ \sum_{n=0}^{\infty} a_n \pi^n \mid a_n \in S \}$, for any set of representatives $S \subset A$ of $A/\mathfrak{p}$

the projective limit topology of $\hat{A}_\mathfrak{p}$ ($A/\mathfrak{p}^n$ has discrete topology)

has basis of open sets $a + \mathfrak{p}^n \hat{A}_\mathfrak{p} = \{ x \in \hat{A}_\mathfrak{p} \mid |x-a| \leq \rho^{n-1} \}$ $(n \geq 1)$

A is dense in $\hat{A}_\mathfrak{p}$

K —— " —— $K_\mathfrak{p} = \hat{K}_\mathfrak{p} = \mathrm{Frac}(\hat{A}_\mathfrak{p}) = \hat{A}_\mathfrak{p}[1/\pi] = \bigcup_{n\geq 1} \pi^{-n}\hat{A}_\mathfrak{p}$ (inductive limit topology)

$\Rightarrow$ $K_\mathfrak{p}$ = the completion of $(K, |\cdot|)$.

<u>Ex</u>: <u>$A = \mathbb{Z}$</u>, $\mathfrak{p} = (p)$: $\hat{A}_\mathfrak{p} = \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ p-adic integers

$K_\mathfrak{p} = \mathbb{Z}_p[1/p] = \mathbb{Q}_p$

<u>Ex</u>: <u>$A = \mathbb{Z}[i]$</u> : (1) $p \equiv 3 \pmod 4$, $\mathfrak{p} = p\mathbb{Z}[i]$

$K = \mathbb{Q}(i)$, $\mathbb{Z}[i]/p^n\mathbb{Z}[i] \cong \mathbb{Z}/p^n\mathbb{Z}[T]/(\underbrace{T^2+1}_{\text{irred.}})$

irred. over $\mathbb{Z}/p\mathbb{Z} \Rightarrow$ irred over each $\mathbb{Z}/p^n\mathbb{Z}$ $\Rightarrow$ over $\mathbb{Z}_p$ $\Rightarrow$ over $\mathbb{Q}_p$

$\hat{A}_\mathfrak{p} \simeq \mathbb{Z}_p[T]/(T^2+1)$, $K_\mathfrak{p} = \mathbb{Q}(i)_\mathfrak{p} \simeq \mathbb{Q}_p[T]/(T^2+1)$

$[K_\mathfrak{p} : \mathbb{Q}_p] = 2$

(2) $p \equiv 1 \pmod 4$, $p = \pi\bar{\pi}$, $\pi = a+bi$, $a^2+b^2 = p$, $\mathfrak{p} = (\pi)$, $\bar{\mathfrak{p}} = (\bar{\pi})$

~~$\mathbb{Z}[i]/\pi^n\mathbb{Z}[i] \simeq \mathbb{Z}/p^n\mathbb{Z}[T]/(T^2+1, T-u)$~~

$u \in \mathbb{Z}$, $u^2 \equiv -1 \pmod{p^n}$

$\mathbb{Z}[i]/p^n\mathbb{Z}[i] = \mathbb{Z}/p^n\mathbb{Z}[T]/(T^2+1) \xrightarrow{\sim} \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$

$T \mapsto u$

$T \mapsto -u$

$\wr\!\wr$ CRT

$\mathbb{Z}[i]/\pi^n\mathbb{Z}[i] \times \mathbb{Z}[i]/\bar{\pi}^n\mathbb{Z}[i]$

$\Rightarrow$ $\hat{A}_\mathfrak{p} \simeq \mathbb{Z}_p \simeq \hat{A}_{\bar{\mathfrak{p}}}$, $K_\mathfrak{p} \simeq \mathbb{Q}_p \simeq K_{\bar{\mathfrak{p}}}$

<u>Def</u>. A <u>local field</u> = a locally compact complete valued field

arch. • $\mathbb{R}$, $\mathbb{C}$

non-arch. char $= 0$ • $[K:\mathbb{Q}_p] < \infty$

non-arch. char $= p$ • $\mathbb{F}_q((t))$

valuation is discrete, residue field is finite

<u>Finite extensions</u>: A Dedekind, $K = \mathrm{Frac}(A)$, $[L:K] = n < \infty$, B = normalisation of A in L, (F) <u>B of finite type over A</u>

<u>Prop.</u> For $\mathfrak{p} \in \mathrm{Max}(A)$, let $\widehat{A}_\mathfrak{p} = \varprojlim_n \underbrace{A/\mathfrak{p}^n}_{A_\mathfrak{p}/(\mathfrak{p}A_\mathfrak{p})^n}$, $K_\mathfrak{p} = \widehat{K_\mathfrak{p}} = \mathrm{Frac}(\widehat{A}_\mathfrak{p})$

(idem $\widehat{B}_P$, $L_P = \widehat{L_P}$ for $P \in \mathrm{Max}(B)$) (1) there are natural isomorphisms of B-algebras (resp., L-algebras)

$$B \otimes_A \widehat{A}_\mathfrak{p} \xrightarrow{\sim} \prod_{P|\mathfrak{p}} \widehat{B}_P, \quad L \otimes_K K_\mathfrak{p} \xrightarrow{\sim} \prod_{P|\mathfrak{p}} L_P, \quad [L_P : K_\mathfrak{p}] = e(P/\mathfrak{p})\, f(P/\mathfrak{p})$$

(2) If L/K is a Galois extension, then $\forall P \in \mathrm{Max}(B)$ the (group) morphism

$\alpha : D_P = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma P = P\} \longrightarrow \mathrm{Aut}(\widehat{B}_P/\widehat{A}_\mathfrak{p}) \xrightarrow{\sim} \mathrm{Aut}(L_P/K_\mathfrak{p})$

is an isomorphism and $L_P/K_\mathfrak{p}$ is a Galois extension, hence

$D_P \xrightarrow{\sim} \mathrm{Gal}(L_P/K_\mathfrak{p})$.

<u>Pf</u>. (1) $\mathfrak{p}B = \prod_{P|\mathfrak{p}} P^{e_P}$ $\qquad f_P = [B/P : A/\mathfrak{p}]$

$B_\mathfrak{p} = BA_\mathfrak{p}$ is free over $A_\mathfrak{p}$ of $\mathrm{rk} = [L:K] = \sum_{P|\mathfrak{p}} e_P f_P$

$\forall n \geq 1$ $\quad B/\mathfrak{p}^n B = B \otimes_A A/\mathfrak{p}^n = B_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}/\mathfrak{p}^n A_\mathfrak{p} \xrightarrow{\sim} \prod_{P|\mathfrak{p}} \underbrace{B/P^{n e_P}}_{\text{free of } \mathrm{rk} = e_P f_P \text{ over } A/\mathfrak{p}^n}$ (Chinese R.T.)

$\Rightarrow$ $B \otimes_A \widehat{A}_\mathfrak{p} = B_\mathfrak{p} \otimes_{A_\mathfrak{p}} \widehat{A}_\mathfrak{p} \xrightarrow{\sim} \prod_{P|\mathfrak{p}} \underbrace{\widehat{B}_P}_{\text{free of } \mathrm{rk} = e_P f_P \text{ over } \widehat{A}_\mathfrak{p}}$. $\qquad A_\mathfrak{p}/(\mathfrak{p}A_\mathfrak{p})^n$

(2) If $\sigma \in \mathrm{Ker}(\alpha)$, then $\forall b \in B$ $\forall n \geq 1$ $\sigma(b) \equiv b \pmod{P^n} \Rightarrow \sigma(b) = b \Rightarrow \sigma = \mathrm{id}$

So α is injective, $e_P f_P = |D_P| \leq |\mathrm{Aut}(L_P/K_\mathfrak{p})| \leq [L_P : K_\mathfrak{p}] = e_P f_P \Rightarrow$ equalities $\Rightarrow$ result.

<u>Number fields case</u>

$n = [K:\mathbb{Q}] < \infty$ <u>Def</u>. A <u>place</u> of K = equivalence class of non-trivial valuations

<u>Normalised valuations</u>: (1) <u>non-archimedean</u>: $P \in \mathrm{Max}(O_K)$, $P|p$

$e = e(P|p)$, $f = f(P|p)$ $\qquad (N(P) = |O_K/P| = p^f)$

$\forall \beta \in K^\times$ $\qquad \|\beta\|_P := N(P)^{-v_P(\beta)} = p^{-f v_P(\beta)}$

$(\Rightarrow \forall \alpha \in \mathbb{Q}^\times$ $\quad \|\alpha\|_P = p^{-ef v_p(\alpha)} = \|\alpha\|_p^{ef})$

$$\prod_{P|p} \|\beta\|_P = (p^{-1})^{\overbrace{\sum_{P|p} f(P|p)\, v_P(\beta)}^{}} = \|N_{K/\mathbb{Q}}(\beta)\|_p$$
$$\qquad v_p(N_{K/\mathbb{Q}}(\beta))$$

(2) <u>archimedean</u>: $K = \mathbb{Q}(\alpha) \simeq \mathbb{Q}[T]/(f)$, $f \in \mathbb{Q}[T]$ monic irred., $f(\alpha) = 0$

$K \otimes_\mathbb{Q} \mathbb{R} \simeq \mathbb{R}[T]/(f) \simeq \underbrace{\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}}_{\prod_1^{r_1} \mathbb{R}[T]/(f_j) \times \prod_1^{r_2} \mathbb{R}[T]/(g_j)}$, $\quad f = \prod_{j=1}^{r_1} (\underbrace{T - \alpha_j}_{f_j}) \prod_{k=1}^{r_2} \underbrace{(T - \beta_j)(T - \overline{\beta_j})}_{g_j(T)}$, $\alpha_j \in \mathbb{R}$, $\beta_j \notin \mathbb{R}$

<u>Def</u>: $\underset{\sim}{w|\infty}$: element of $\mathrm{Hom}_\mathbb{Q}(K, \mathbb{C}) / \mathrm{Gal}(\mathbb{C}/\mathbb{R})$: each σ defines $\|x\|_w = |\sigma(x)|$

archimedean primes of K $\qquad \sigma$ $\qquad \|x\|_w = |\sigma(x)|^{[K_w:\mathbb{R}]}$

r_1 real primes of K : $\forall j = 1, \dots, r_1$; $\sigma_j : K = \mathbb{Q}(\alpha) \hookrightarrow \mathbb{R}$

$\alpha \longmapsto \alpha_j$

completion $K_{w_j} = \mathbb{R}$

$K \xrightarrow{\sigma_j} K_{w_j}$

$\Rightarrow$ prime w_j

$\|x\|_{w_j} = |\sigma_j(x)|$

r_2 complex primes of K : $\forall k = 1, \dots, r_2$: pair of embeddings

$\sigma_{r_1+k}, \overline{\sigma_{r_1+k}} : K = \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$

$\alpha \longmapsto \beta_k, \overline{\beta_k}$

$\Rightarrow$ prime w_{r_1+k}

$\|x\|_{w_{r_1+k}} = |\sigma_{r_1+k}(x)|^2 = |\overline{\sigma_{r_1+k}}(x)|^2$

completion $K \hookrightarrow K_{w_j} \xrightarrow{\sim} \mathbb{C}$ depends on the choice of β_k or $\overline{\beta_k}$

Again : $\forall \gamma \in K^\times$ $\prod_{w|\infty} \|\gamma\|_w = \prod_{\sigma : K \hookrightarrow \mathbb{C}} |\sigma(\gamma)| = |N_{K/\mathbb{Q}}(\gamma)|$

Prop : (1) A non-trivial valuation of K is equivalent to precisely one of $\|\cdot\|_p$ or $\|\cdot\|_w$.

(2) $\forall x \in K^\times$ $\prod_v \|x\|_v = 1$.

Pf : (2) L.H.S. $= \|y\|_\infty \prod_p \|y\|_p = 1$, $y = N_{K/\mathbb{Q}}(x) \in \mathbb{Q}^\times$.

(1) Ostrowski + ... (omitted).

Abstract definition of $\|\cdot\|_v$: $[K:\mathbb{Q}] < \infty$

(1) $P \in \mathrm{Max}(O_K)$: $B = O_K$, $\underbrace{\hat{B}_P}_{\text{complete DVR}} = \varprojlim_n \underbrace{B/P^n}_{\text{finite}}$ is compact, $K_P = \mathrm{Frac}(\hat{B}_P)$ is locally compact

$\pi \in \hat{B}_P$ unif.

$\exists$ measure μ on K_P s.t. • $\mu(\text{cpt}) < \infty$

• $\mu(x+U) = \mu(U)$ $\forall x \in K_P$

μ is unique up to $\mu \mapsto c\mu$, $c \in \mathbb{R}^\times_{>0}$.

So : $\forall a \in K_P^\times$ $U \longmapsto \mu(aU)$ is equal to $c\mu$, $c \in \mathbb{R}^\times_{>0}$

Fact : $c = \|a\|_P$ $\left(= \dfrac{\mu(aU)}{\mu(U)} \right.$ for any cpt open $U \subset K_P \Big)$

Pf : $a \in \hat{B}_P^\times$, $\underbrace{U = \hat{B}_P}$ $\Rightarrow aU = U \Rightarrow c = 1$

$a = \pi$, $U = \coprod_{x \in S} (x + \pi U)$ S = repr. of $\hat{B}_P/\pi = \mathbb{F}_{N(P)}$

$\Rightarrow \#S \cdot \mu(\pi U) = \mu(U)$ $= c = \dfrac{1}{\#S} = \dfrac{1}{N(P)}$.

(2) $v|\infty$: $K_v \simeq \begin{cases} \mathbb{R} \\ \mathbb{C} \end{cases}$, μ = Lebesgue measure on K_v, $\mu(aU)/\mu(U) = \|a\|_v$, $U \subset K_v$

Completions of a number field: $[K:\mathbb{Q}]<\infty$

- r_1 real completions $K_v \simeq \mathbb{R}$
- r_2 complex $K_v \simeq \mathbb{C}$

$$K\otimes_{\mathbb{Q}}\mathbb{R} \xrightarrow{\sim} \prod_{v|\infty} K_v \xrightarrow{\sim} \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$$

- p prime number $K\otimes_{\mathbb{Q}}\mathbb{Q}_p \xrightarrow{\sim} \prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$, $[K_{\mathfrak{p}}:\mathbb{Q}_p] = e(\mathfrak{p}|p)f(\mathfrak{p}|p)$

Ex: $K=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{Z}\setminus\{0,1\}$ square-free, $p\nmid 2d$

If $\underbrace{\left(\frac{d}{p}\right)=1}_{\exists\alpha_1\in\mathbb{Z},\ \alpha_1^2\equiv d \pmod p}$ $\Longrightarrow$ $p\mathcal{O}_K=\mathfrak{p}\bar{\mathfrak{p}}$, $\mathcal{O}_K/\mathfrak{p}\simeq\mathcal{O}_K/\bar{\mathfrak{p}}\simeq\mathbb{F}_p$ $e=f=1$ for $\mathfrak{p},\bar{\mathfrak{p}}$

$$\begin{tikzcd} K \arrow[r, hook, "\iota"] \arrow[rrr, bend right, "\bar{\iota}"'] & K_{\mathfrak{p}} \simeq \mathbb{Q}_p & \simeq & K_{\bar{\mathfrak{p}}} \end{tikzcd}$$

$\Longrightarrow$ $\iota(\sqrt{d})=\alpha\in\mathbb{Q}_p$, $\alpha^2=d$
$(\alpha\in\mathbb{Z}_p$, $\alpha^2\equiv d \pmod{p^n}\ \forall n)$

Hensel's Lemma (= Newton's method)

K field complete w.r.t. non-arch. valuation $|\cdot|$, $\mathcal{O}\subset K$ the valuation ring of $|\cdot|$, $f(X)\in\mathcal{O}[X]$. If $\alpha_0\in\mathcal{O}$ satisfies $|f(\alpha_0)|<|f'(\alpha_0)|^2$, then $\exists!$ $\alpha\in\mathcal{O}$ s.t. $f(\alpha)=0$, $|\alpha-\alpha_0|\le|f(\alpha_0)|/|f'(\alpha_0)|$.

Pf: $f(X+Y)=f(X)+\underbrace{f_1(X)}_{f'(X)}Y+\cdots+f_j(X)Y^j+\cdots$

$\delta=\dfrac{|f(\alpha_0)|}{|f'(\alpha_0)|^2}<1$

Take β_0 s.t. $f(\alpha_0)+f_1(\alpha_0)\beta_0=0$, $\alpha_1=\alpha_0+\beta_0$

$\Longrightarrow$ $|f(\alpha_1)|\le\max_{j\ge2}|f_j(\alpha_0)\beta_0^j|\le\max_{j\ge2}|\beta_0|^j\le|f(\alpha_0)|^2/|f_1(\alpha_0)|^2\le|f(\alpha_0)|\delta$

Similarly, $|f_1(\alpha_1)-f_1(\alpha_0)|<|f_1(\alpha_0)|$ $\Longrightarrow$ $|f_1(\alpha_1)|=|f_1(\alpha_0)|$

$|\alpha_1-\alpha_0|=|f(\alpha_0)|/|f_1(\alpha_0)|<1$

Repeating the same procedure with α_1, we get $\alpha_2=\alpha_1+\beta_1$ s.t.

$|\alpha_2-\alpha_1|\le|f(\alpha_1)|/|f_1(\alpha_1)|\le|f(\alpha_0)|^2/|f'(\alpha_0)|^3=|f(\alpha_0)|^{1/2}\delta^{3/2}$

$|f'(\alpha_2)|=|f'(\alpha_0)|$, $|f(\alpha_2)|\le|f(\alpha_1)|^2/|f'(\alpha_0)|^2\le|f(\alpha_0)|^4/|f'(\alpha_0)|^6=|f(\alpha_0)|\delta^3$

$|f(\alpha_3)|\le|f(\alpha_2)|^2/|f'(\alpha_0)|^2\le|f(\alpha_0)|\delta^7$

$|\alpha_{n+1}-\alpha_n|=|f(\alpha_n)|/|f'(\alpha_n)|\le|f(\alpha_0)|^{1/2}\delta^{2^n-1/2}$ $\Longrightarrow$ $|f(\alpha_n)|\le|f(\alpha_0)|\delta^{2^n-1}$

$\alpha_n\in\mathcal{O}$

$\Longrightarrow$ $\{\alpha_n\}$ is a Cauchy sequence $\Longrightarrow$ $\exists\,\alpha=\lim_{n\to\infty}\alpha_n\in\mathcal{O}$,

$f(\alpha)=\lim_{n\to\infty}f(\alpha_n)=0$.

Uniqueness: If $f(\alpha+\beta)=0$, $|\beta|\le|f(\alpha_0)|/|f'(\alpha_0)|<|f'(\alpha_0)|$

$|f'(\alpha)|=|f'(\alpha_0)|$

then $0=f'(\alpha)+f_2(\alpha)\beta+\cdots$

$\Longrightarrow$ $|f'(\alpha)|\le\max_{j\ge1}|\beta|^j$ – contradiction.

Ex: $(\pm3)^2\equiv2 \pmod 7$. If $x_n^2\equiv2\pmod{7^n}$, $x_{n+1}=x_n+7^ny$ $(n\ge1)$

$x_{n+1}^2\equiv x_n^2+7^n\cdot2x_ny\pmod{7^{n+1}}$; putting $y\equiv\dfrac{2-x_n^2}{7^n}\cdot(2x_n)^{-1}\pmod 7$

we get unique $x_{n+1}\equiv x_n\pmod{7^n}$ s.t. $x_{n+1}^2\equiv2\pmod{7^{n+1}}$.

$\Longrightarrow$ get two elements $\pm\alpha\in\mathbb{Z}_7$ s.t. $\alpha^2=2$.

Special case of Hensel's Lemma:

$A = \varprojlim_n A/\pi^n A$ complete DVR, $f(X) \in A[X]$, $c \geq 0$. If $\alpha_0 \in A$ satisfies $f(\alpha_0) \equiv 0 \pmod{\pi^{2c+1}}$, $f'(\alpha_0) \equiv 0 \pmod{\pi^c}$, $f'(\alpha_0) \not\equiv 0 \pmod{\pi^{c+1}}$, then $\exists!\ \alpha \in A$ s.t. $f(\alpha) = 0$, $\alpha \equiv \alpha_0 \pmod{\pi^{c+1}}$.

Unramified extensions

Given: $A = \varprojlim_n A/\pi^n A$ complete DVR, $K = \mathrm{Frac}(A)$, $k = A/\pi A$.

Prop: If L/K is a finite separable extension, then the normalisation B of A in L is a complete DVR. Let $\Pi \in B$ be a uniformiser, $k_L = B/\Pi B$ the residue field and $e = v_\Pi(\pi)$ the ramification index; then $[L:K] = ef$, $f = [k_L : k]$.

Pf: separability $\Rightarrow$ (F) $\Longrightarrow B = B \otimes_A \underbrace{\hat{A}_\pi}_{A} \xrightarrow{\sim} \prod_{P|\pi} \widehat{B_P}$

$B \subset L$ integral domain $\Rightarrow \exists!\ P|\pi$ in $B \Rightarrow \mathrm{Max}(B) = \{P\} \Rightarrow B$ DVR

$B \xrightarrow{\sim} \widehat{B}_P \Rightarrow B$ complete. Finally, (F) $\Rightarrow [L:K] = \sum_{P|\pi} e_P f_P = ef$.

Prop. The functor $L \longmapsto k_L$ gives rise to an equivalence of categories

$$\left\{\begin{matrix}\text{finite separable extensions of } K \\ \text{~~which are~~ unramified}\end{matrix}\right\} \xrightarrow{\approx} \left\{\begin{matrix}\text{finite separable} \\ \text{extensions of } k\end{matrix}\right\}$$

Cor. Fix a separable closure K^{sep} of K. Let $K^{ur} = \bigcup_{\substack{K \subset L \subset K^{sep} \\ L/K \text{ unramified},\ [L:K]<\infty}} L$.

Then every finite subextension of K^{ur}/K is unramified and $L \mapsto k_L$ induces an isomorphism $\mathrm{Gal}(K^{ur}/K) \xrightarrow{\sim} \mathrm{Gal}(k^{sep}/k)$

Special case: $[K:\mathbb{Q}_p] < \infty$, $k = \mathbb{F}_q$ $(q = p^r)$, $k^{sep} = \bar{k} = \bigcup_{p \nmid m} k(\mu_m)$

$$K^{ur} = \bigcup_{p \nmid m} K(\mu_m)$$

Pf of Prop: (α) ($\forall\ k'/k$ finite separable) ($\exists\ L/K$ unr. sep.) $k_L \simeq k'$:

Pf: $k' = k(\bar{\alpha})$; fix $g(T) \in A[T]$ monic s.t. $g \pmod{\pi A[T]} = \bar{g}$ = min. pol. of $\bar\alpha$ over k (irred. separable)

$\Rightarrow g$ irred. $/K$, separable. ~~Take~~ $L = \underset{= K(\alpha)}{K[T]/(g)} \supset B = A[T]/(g) \twoheadrightarrow \underbrace{k[T]/(\bar{g})}_{k_L} = k'$, $\alpha = T \pmod g$

(β) L, L' finite unram. sep. ext. of $K \Longrightarrow \underbrace{\mathrm{Hom}_K(L, L') \xrightarrow{\sim} \mathrm{Hom}_k(k_L, k_{L'})}$:
$\sigma \longmapsto \bar\sigma$

Pf: $\forall\ \rho \in \mathrm{Hom}_k(k_L, k_{L'})$ $k_L = k[T]/(\bar{g}) = k[\bar\alpha]$ $\bar\alpha = T \pmod{\bar g} \Rightarrow \bar{g}(\rho(\bar\alpha)) = 0$

Hensel's lemma $\Rightarrow \exists!\ \alpha' \in B' \subset L'$, $g(\alpha') = 0$, $\alpha' \pmod{\Pi'} = \rho(\bar\alpha)$

$\exists!\ \sigma: L = K(\alpha) \longrightarrow L'$, $\sigma(\alpha) = \alpha'$ $\Longrightarrow \bar\sigma = \rho$.

If $\bar\tau = \rho \Rightarrow \tau(\alpha) = \alpha' \Rightarrow \tau = \sigma$.

Structure of $A^\times$: $A = \varprojlim_n A/\pi^n A$ complete DVR, $A/\pi A = k$

$A = A_0 \supset A_1 \supset A_2 \supset \cdots$ $\qquad A_n = 1 + \pi^n A \qquad \forall n \geq 1$

$A_0/A_1 \xrightarrow{\sim} k^\times$, $\quad \forall n \geq 1 \quad A_n/A_{n+1} \xrightarrow{\sim} (k, +)$, as $(1+\pi^n x)(1+\pi^n y) \equiv 1 + \pi^n(x+y) \pmod{\pi^{n+1}A}$

__Cor__: If $m \geq 1$ is not divisible by $\mathrm{char}(k)$, then

$$\begin{array}{ccc} A_1 & \longrightarrow & A_1 \\ x & \longmapsto & x^m \end{array}$$ is an isomorphism, hence

$\mu_m(A) \xrightarrow{\sim} \mu_m(k)$ and $A^\times/A^{\times m} \xrightarrow{\sim} k^\times/k^{\times m}$.

__Ex__: $m = 2$, $A = \mathbb{Z}_p$: (a) __$p \neq 2$__ $\Rightarrow$ $\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2} \xrightarrow{\sim} \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \xrightarrow[\sim]{(\frac{\cdot}{p})} \{\pm 1\}$.

$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times \Rightarrow \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} = \{1, p, u, up\} \pmod{\mathbb{Q}_p^{\times 2}}$

3 quadratic ext. of $\mathbb{Q}_p$: $\underbrace{\mathbb{Q}_p(\sqrt{u})}_{\text{unram. over } \mathbb{Q}_p}$, $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{pu})$ $\quad\Big|\quad \left(\frac{u}{p}\right) = -1$, $u \in \mathbb{Z}_p^\times$

(b) __$p = 2$__: Hensel's lemma $\Rightarrow$ $\mathbb{Z}_2^{\times 2} = \{x \in \mathbb{Z}_2^\times \mid x \equiv y^2 \pmod 8\} = 1 + 8\mathbb{Z}_2$

$\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} \xrightarrow{\sim} (\mathbb{Z}/8\mathbb{Z})^\times \Rightarrow \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} = \{\pm 1, \pm 5, \pm 2, \pm 10\} \pmod{\mathbb{Q}_2^{\times 2}}$

$\Rightarrow$ 7 quadratic extensions of $\mathbb{Q}_2$; $\quad \mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified.

Geometric representation of $K \supset \mathcal{O}_K$ $\quad ([K:\mathbb{Q}]<\infty)$

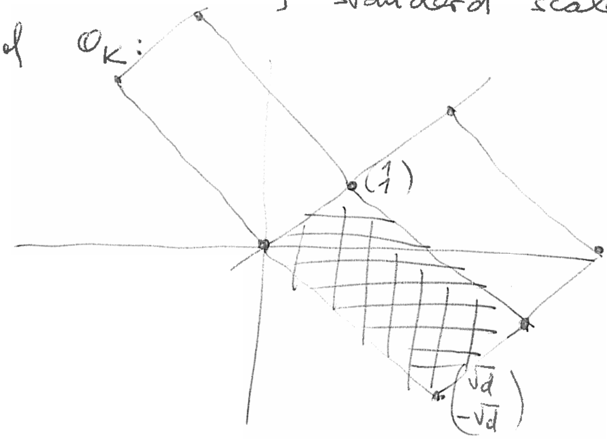
Ex: $K=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{Z}\setminus\{0,1\}$ square-free, $d\equiv 2,3 \pmod 4$

$\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\sqrt{d}$, $D_K=4d$

(1) $d>0$: $\sigma_1,\sigma_2: K\hookrightarrow\mathbb{R}$ $\quad \sigma_1(\sqrt{d})=\sqrt{d}$, $\sigma_2(\sqrt{d})=-\sqrt{d}$

$(\sigma_1,\sigma_2): K\hookrightarrow\mathbb{R}^2$ } standard scalar product

image of $\mathcal{O}_K$:



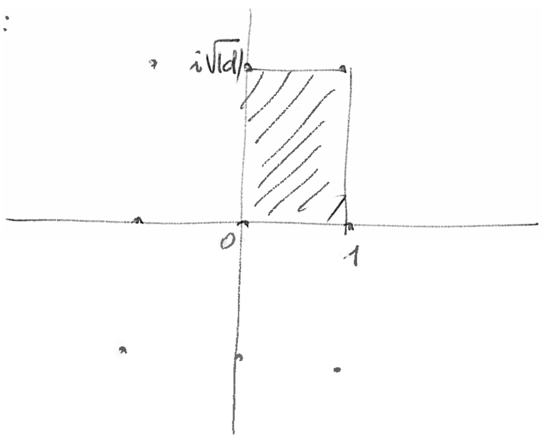
rectangular lattice of covolume

$\left\|\binom{1}{1}\right\|\cdot\left\|\binom{\sqrt{d}}{-\sqrt{d}}\right\| = 2\sqrt{d}=\sqrt{D_K}$

(2) $d<0$: $\sigma: K\hookrightarrow \underset{\sim}{\mathbb{C}}$, $\sqrt{d}\longmapsto i\sqrt{|d|}$

$2\cdot$ standard scalar product on $\mathbb{C}=\mathbb{R}\oplus\mathbb{R}i\simeq\mathbb{R}^2$

image of $\mathcal{O}_K$:



rectangular lattice of covolume

$\cancel{2}\cdot 1\cdot\sqrt{|d|}=\sqrt{|D_K|}$

General case: $K\hookrightarrow K_{\mathbb{R}}=K\otimes_{\mathbb{Q}}\mathbb{R}\xrightarrow{\sim}\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ $\qquad \dim_{\mathbb{R}}(K_{\mathbb{R}})=[K:\mathbb{Q}]$

canonical involution on $K_{\mathbb{R}}$: $\underbrace{}_{id^{r_1}}$ $\underbrace{}_{c^{r_2}}$ $\qquad c:\mathbb{C}\to\mathbb{C}$ cplx conj.

scalar product on $K_{\mathbb{R}}$: $\langle x,y\rangle=\mathrm{Tr}_{K_{\mathbb{R}}/\mathbb{R}}(x\bar{y})$ $\quad$ (sym., pos.-definite).

on each $\mathbb{R}$: $\mathrm{Tr}_{\mathbb{R}/\mathbb{R}}(xy)=xy$ $\quad$ usual scalar product

— " — $\mathbb{C}$: $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}\left((a+bi)\overline{(c+di)}\right)=2(ac+bd)=2\cdot$ usual scalar product

$\|x\|=\sqrt{\langle x,x\rangle}$

Above: $\sigma_1,\dots,\sigma_{r_1}: K\hookrightarrow\mathbb{R}$, $\quad \sigma_{r_1+j},\ \overline{\sigma}_{r_1+j}: K\hookrightarrow\mathbb{C}$ $\quad (1\le j\le r_2)$

$\{\sigma\}_{\sigma\in\Sigma}=(\sigma_1,\dots,\sigma_{r_1+r_2}): K\hookrightarrow\prod_{\sigma\in\Sigma}K_\sigma$ $\qquad \Sigma=\{\sigma_1,\dots,\sigma_{r_1+r_2}\}$

$\langle(x_\sigma),(y_\sigma)\rangle=\sum_{\sigma\in\Sigma}\mathrm{Tr}_{K_\sigma/\mathbb{R}}(x_\sigma\overline{y_\sigma})$

$\deg(\sigma_j)=[K_{\sigma_j}:\mathbb{R}] = \begin{cases}1 & j\le r_1\\ 2 & j>r_1\end{cases}$

Euclidean lattices: a Euclidean lattice is a free abelian group L of finite rank and a scalar product (symmetric, positive definite) $\langle , \rangle$ on $V = L \otimes_{\mathbb{Z}} \mathbb{R}$. The covolume of L is the volume (w.r.t. $\langle , \rangle$) of V/L. | Terminology: L is a lattice in V.

If $L = \bigoplus_{i=1}^{n} \mathbb{Z} v_i$, then $F = \prod_{i=1}^{n} [0,1) v_i \subset V$ is a fundamental domain of L in V ($V = \coprod_{u \in L} (u+F)$, disjoint union) and $\mathrm{covol}(L) = \mathrm{vol}(F)$.

Ex: (1) If $L = \bigoplus_{i=1}^{n} \mathbb{Z} v_i$, then $\mathrm{covol}(L)^2 = |\det((\langle v_i, v_j \rangle)_{1 \le i,j \le n})|$ (Gram

(2) If $V = \mathbb{R}^n$, $\langle , \rangle$ = standard scalar product $\Rightarrow \mathrm{covol}(L) = |\det(v_1 | \cdots | v_n)|$

Lemma. Let $L \subset V$ be a subgroup of a Euclidean space $(V, \langle , \rangle)$. Then:

(1) L is a lattice in $V \Longleftrightarrow$ (2) L is discrete ($\Leftrightarrow$ the top. induced on L is discrete) and cocompact ($\Leftrightarrow$ V/L is compact)

$\Longleftrightarrow$ (3) L contains a basis of V $\wedge$ ($\forall$ bounded $B \subset V$ $|L \cap B| < \infty$).

Pf: (1) $\Rightarrow$ (2): $L = \bigoplus_{i=1}^{n} \mathbb{Z} v_i \subset V = \bigoplus_{i=1}^{n} \mathbb{R} v_i$

$\forall v \in L$ $\quad L \cap (v + \underbrace{\prod_{i=1}^{n} (-1/2, 1/2) v_i}_{\text{open}}) = \{v\} \Longrightarrow L$ discrete

$\prod_{i=1}^{n} [0,1] v_i$ = compact $\xrightarrow[\text{cont.}]{\text{surj.}}$ V/L $\Longrightarrow V/L$ cpt.

(2) $\Rightarrow$ (3): $W := \mathbb{R}L \subset V$; cpt. $V/L \xrightarrow[\text{surj.}]{\text{cont.}} V/W$ cpt $\mathbb{R}$-v.s. $\Longrightarrow V/W = 0$, $W = V$.

$\forall B \subset V$ bounded $\overline{B}$ is cpt $\Longrightarrow$ $\overline{B} \cap L$ is cpt $\wedge$ discrete $\Longrightarrow$ finite

(3) $\Rightarrow$ (1): $\exists\, w_1, \ldots, w_n \in L$ $\mathbb{R}$-basis of V; $B := \prod_{i=1}^{n} [0,1] w_i \subset V$ bounded

$L = \bigcup_{\underbrace{x \in B \cap L}_{\text{finite}}} (x + (\underbrace{\bigoplus_{i=1}^{n} \mathbb{Z} w_i}_{L' \text{ lattice}})) \Longrightarrow m = (L : L') < \infty \Longrightarrow L' \subset L \subset \frac{1}{m} L' \Longrightarrow L \simeq \mathbb{Z}^n$, $\mathbb{R}L = V$.

Minkowski's Thm on convex bodies: let $L \subset V = L \otimes_{\mathbb{Z}} \mathbb{R}$ ($\dim_{\mathbb{R}} V = n$) be a lattice, $B \subset V$ a bounded symmetric ($x \in B \Rightarrow -x \in B$) convex ($x, y \in B$, $0 \le \lambda \le 1 \Rightarrow \lambda x + (1-\lambda) y \in B$) set s.t. $\mathrm{vol}(B) > 2^n \mathrm{covol}(L)$ (if B is closed, s.t. $\mathrm{vol}(B) \ge 2^n \mathrm{covol}(L)$). Then $\exists\, b \in (B \cap L) \setminus \{0\}$.

Pf: $\alpha : B \hookrightarrow V \twoheadrightarrow V/2L$. If $\mathrm{vol}(B) > 2^n \mathrm{covol}(L) = \mathrm{covol}(2L)$, then

$\exists\, x, y \in B$, $x \ne y$, $\alpha(x) = \alpha(y) \Longrightarrow x - y \in 2L$, $0 \ne \underset{L}{\underbrace{\tfrac{1}{2}(x-y)}} = \underbrace{\tfrac{1}{2}(x + (-y))}_{\in B} \in L \cap B$.

If B is closed and $\mathrm{vol}(B) = 2^n \mathrm{covol}(L)$,

$\forall m \ge 1$ $\exists$ $b_m \in (\underbrace{L \cap (1 + \tfrac{1}{m}) B}_{\text{finite set}}) \setminus \{0\} \Longrightarrow \exists\, b$ occuring ∞-many times

$\Longrightarrow b \ne 0$, $b \in L \cap \bigcap_{m \ge 1} (1 + \tfrac{1}{m}) B = L \cap (\text{closure of } B) = L \cap B$.

Prop.: $\mathcal{O}_K \subset K \hookrightarrow K_{\mathbb{R}} = \prod_{\sigma\in\Sigma} K_\sigma$ is a lattice of $\mathrm{covol}(\mathcal{O}_K) = |D_K|^{1/2}$

Pf: $\mathcal{O}_K$ contains a $\mathbb{Q}$-basis of $K \Rightarrow$ contains an $\mathbb{R}$-basis of $K_{\mathbb{R}}$

$\forall r>0 \quad B_r = \{x \in K_{\mathbb{R}} \mid \|x\| < r\} \subset K_{\mathbb{R}}$ is bounded, $\bigcup_{r>0} B_r = K_{\mathbb{R}}$

$\forall x \in \mathcal{O}_K \cap B_r \quad \mathrm{Tr}(x\bar{x}) < r^2 \Rightarrow \forall \sigma \in \Sigma \quad |\sigma(x)| < r$

$\Rightarrow \quad P_{K/\mathbb{Q},x}(T) = \prod_{\sigma: K \hookrightarrow \mathbb{C}} (T - \sigma(x)) \in \mathbb{Z}[T]$ has coeff. bounded in terms of r

$\Rightarrow \quad |\mathcal{O}_K \cap B_r| < \infty$. So $\mathcal{O}_K$ is a lattice.

If $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$, then $\mathrm{covol}(\mathcal{O}_K)^2 = \left|\det(\underbrace{\langle \omega_j, \omega_k\rangle}_{\mathrm{Tr}_{K/\mathbb{Q}}(\omega_j\omega_k)})\right| = |D_K|$.

Cor. $\forall\, (0) \neq I \subset \mathcal{O}_K$ ideal, $I \subset K_{\mathbb{R}}$ is a lattice of covolume
$\mathrm{covol}(I) = (\mathcal{O}_K : I)\, \mathrm{covol}(\mathcal{O}_K) = N(I)\, |D_K|^{1/2}$.

Prop. $\forall m \geq 1 \quad |\{ (0) \neq I \subset \mathcal{O}_K \mid N(I) \leq m\}| < \infty$.

Pf: If $N(I) = n \geq 1$, then $n \cdot (\mathcal{O}_K/I) = 0 \Rightarrow n\mathcal{O}_K \subset I \subset \mathcal{O}_K$; then I is determined by $\underbrace{I/n\mathcal{O}_K}_{\text{finitely many possibilities}} \subset \underbrace{\mathcal{O}_K/n\mathcal{O}_K}_{\text{finite}} \Rightarrow |\{I \subset \mathcal{O}_K \mid N(I) = n\}| < \infty$.

Thm. $\forall$ fractional ideal J of K $\exists$ ideal $I \subset \mathcal{O}_K$ equivalent to J^{-1} s.t.
$N(I) \leq \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2}$.

Cor: $|Cl(\mathcal{O}_K)| < \infty$.

Pf: we can assume $J \subset \mathcal{O}_K$. Fix $c = (c_\sigma \in \mathbb{R}_{>0}\ (\sigma\in\Sigma))$ s.t. $N(c) = \prod_{\sigma\in\Sigma} c_\sigma^{\deg(\sigma)} = \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2} N(J)$. The set $B = \{(x_\sigma) \in K_{\mathbb{R}} \mid \forall \sigma\in\Sigma \quad |x_\sigma| \leq c_\sigma\}$ is closed, symmetric, bounded, convex and $(n = [K:\mathbb{Q}])$

$$\mathrm{vol}(B) = \prod_{i=1}^{r_1} (2c_{\sigma_i}) \prod_{j=1}^{r_2} (2\pi c_{\sigma_{r_1+j}}^2) = 2^{r_1}(2\pi)^{r_2} N(c) = 2^n |D_K|^{1/2} N(J) = 2^n \mathrm{covol}(J)$$

$\Rightarrow \quad \exists\, \alpha \in B \cap J,\ \alpha \neq 0$. Then $(\alpha) \subset J$, $J \mid (\alpha)$, $|N_{K/\mathbb{Q}}(\alpha)| \leq N(c)$

$I := J^{-1}(\alpha) \subset \mathcal{O}_K$ is equivalent to J^{-1} and

$N(I) = N(J)^{-1} |N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2}$.

Improvement: for $r>0$, consider $B_r^! = \{(x_\sigma) \in K_{\mathbb{R}} \mid \sum_\sigma \deg(\sigma)|x_\sigma| \leq r\}$.

AG inequality: $\prod |x_\sigma|^{\deg(\sigma)} \leq \left(\sum_\sigma \deg(\sigma)|x_\sigma| / n\right)^n$

$\mathrm{vol}(B_r^!) = 2^{r_1}\pi^{r_2} r^n / n!$

Choosing r s.t. $\mathrm{vol}(B_r^!) = 2^n |D_K|^{1/2} N(J) \Rightarrow \exists\, \alpha \in B_r^! \cap J \setminus \{0\}$

s.t. $|N_{K/\mathbb{Q}}(\alpha)| \leq (r/n)^n = \frac{n!}{n^n} 2^{-r_1}\pi^{-r_2} \mathrm{vol}(B_r^!) = \underbrace{\boxed{\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_K|^{1/2}}}_{M_K \text{ Minkowski's const.}} N(J)$

Prop: $\forall J \quad \exists I \sim J^{-1}, I \subset \mathcal{O}_K,\ N(J) \leq M_K$.

Ex: $K=\mathbb{Q}(\sqrt{-5})$: $n=2,\ r_2=1,\ D_K=-20$, $M_K=\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|D_K|^{1/2}=\frac{4\sqrt5}{\pi}<\frac{9}{\pi}<3$

So: every ideal class contains an ideal $I\subset O_K$ s.t. $N(I)<3$.

$N(I)=1\iff I=(1)$.

$N(I)=2$: we must factorise $(2)=?$: $O_K=\mathbb{Z}[\sqrt{-5}]=\mathbb{Z}[T]/(T^2+5)$

$T^2+5\equiv(T-1)^2 \pmod 2 \Rightarrow (2)=\mathfrak{p}^2$, $\mathfrak{p}=(2,\sqrt{-5}-1)$, $N(\mathfrak{p})=2$.

Is $\mathfrak{p}\sim 1$? If $\mathfrak{p}=(x+\sqrt{-5}\,y)$ $(x,y\in\mathbb{Z})\Rightarrow 2=x^2+5y^2$ – impossible.

thus $\mathfrak{p}\not\sim 1$. As $\mathfrak{p}^2=(2)\sim 1$, the ideal class group is $Cl(O_K)\simeq\mathbb{Z}/2\mathbb{Z}$, generated by the class of $\mathfrak{p}$.

Application: solve $y^2+5=x^3$, $x,y\in\mathbb{Z}$:

As $y^2\equiv 0,1,4 \pmod 8$ and $x^3\equiv 0,1,3,5,7 \pmod 8 \Rightarrow 2|y,\ 2\nmid x$.

In $I(O_K)$, $(y+\sqrt{-5})(y-\sqrt{-5})=(x)^3$ If $5|y\Rightarrow 5|x^3$, $5^2\nmid x^3$ – impossible

$\Downarrow$ $5\nmid xy$

Claim: the ideals $(y+\sqrt{-5})$, $(y-\sqrt{-5})$ are relatively prime.

Pf: If $\mathfrak{q}\in Max(O_K)$ divides both $(y\pm\sqrt{-5})$, then $\mathfrak{q}|(2\sqrt{-5})$, $\mathfrak{q}|(2y)$

$N(\mathfrak{q})\mid \underbrace{\gcd(20,4y^2)}_{\text{in } \mathbb{Z}}=4 \Rightarrow \mathfrak{q}=\mathfrak{p}\Rightarrow \mathfrak{p}\mid\underbrace{(y+\sqrt{-5})-(\sqrt{-5}-1)}_{y+1}$

$\Rightarrow 2=N(\mathfrak{p})\mid(y+1)^2$ in $\mathbb{Z}$ – impossible (as $2|y$).

Unique factorisation into ideals $\Rightarrow (y+\sqrt{-5})=I^3$, $(y-\sqrt{-5})=\bar{I}^3$.

As $3\nmid|Cl(O_K)|$ and $I^3\sim 1\Rightarrow I\sim 1$, $I=(\alpha)$. $(\alpha\in O_K)$.

thus $(y+\sqrt{-5})=(\alpha^3)\Rightarrow \exists u\in O_K^\times=\{\pm1\}$ $y+\sqrt{-5}=u\alpha^3=(u\alpha)^3$

$u\alpha=a+b\sqrt{-5}$ $(a,b\in\mathbb{Z})$ $y+\sqrt{-5}=(a^3-15ab^2)+\sqrt{-5}\,\underbrace{(3a^2b-5b^3)}_{1}$

$\Rightarrow 1=b(3a^2-5b^2)$, $b=\pm1$, $3a^2-5=\pm1$, $3a^2=\begin{cases}4\\6\end{cases}$ – impossible.

So there are NO $x,y\in\mathbb{Z}$ s.t. $y^2+5=x^3$

Prop. $K\neq\mathbb{Q}\Rightarrow |D_K|>1\Rightarrow \exists\ p$ prime $|D_K$ ($\iff$ p ramifies in $K/\mathbb{Q}$).

Pf: $1\le M_K=\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|D_K|^{1/2}\Rightarrow |D_K|\ge\left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{n^n}{n!}\right)^2\ge\left(\frac{\pi}{4}\right)^n\left(\frac{n^n}{n!}\right)^2\ge\left(\frac{\pi}{4}\right)^n 2^{2n-4}=\frac{\pi^n}{4}>1$

induction: $n^n\ge 2^{n-1}\cdot n!$ (as $n=[K:\mathbb{Q}]\ge 2$)

Units in $\mathcal{O}_K$ $\quad ([K:\mathbb{Q}]<\infty)$

Prop. $\mathcal{O}_K^\times = \{\alpha\in\mathcal{O}_K \mid N_{K/\mathbb{Q}}(\alpha)\in\mathbb{Z}^\times=\{\pm1\}\}$.

Pf. $\subseteq$ $\quad \alpha,\beta\in\mathcal{O}_K \Rightarrow N_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\beta)\in\mathbb{Z}$

$\alpha\beta=1 \Rightarrow N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)=1$

$\supseteq$ Let $\alpha\in\mathcal{O}_K$, let $f(T)\in\mathbb{Z}[T]$ be the minimal pol. of α over $\mathbb{Q}$.
then $f(T)=(T-\alpha_1)\cdots(T-\alpha_n)$, $\alpha_1=\alpha$, $\alpha_j\in L=\mathbb{Q}(\alpha_1,\dots,\alpha_n)$.
We have $\alpha_j\in\mathcal{O}_L$ and $N(\alpha)/\alpha=\alpha_2\cdots\alpha_n\in\mathcal{O}_L\cap K=\mathcal{O}_K$.

Ex: $[K:\mathbb{Q}]=2$, $K=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{Z}\setminus\{0,1\}$ square-free

$$\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\beta,\quad \beta=\begin{cases}\sqrt{d} & d\equiv 2,3 \pmod 4\\ (1+\sqrt{d})/2 & d\equiv 1 \pmod 4\end{cases}$$

$$\beta' = \text{the conj. of } \beta = \begin{cases}-\sqrt{d}=-\beta\\ (1-\sqrt{d})/2=1-\beta\end{cases}$$

$$\mathcal{O}_K\ni\alpha=x-y\beta\quad(x,y\in\mathbb{Z}),\quad N_{K/\mathbb{Q}}(\alpha)=(x-y\beta)(x-y\beta')=\begin{cases}x^2-dy^2\\ x^2-xy+\frac{1-d}{4}y^2\end{cases}$$

(1) $d<0$:
($r_1=0, r_2=1$)

$$\begin{cases}x^2+|d|y^2=1: & |d|>1 \Rightarrow y=0,\ x=\pm1\\ & |d|=1 \Rightarrow \text{— " —},\quad x=0,\ y=\pm1\\ (2x-y)^2+|d|y^2=4: & |d|>3 \Rightarrow y=0,\ x=\pm1\\ d\equiv 1 \pmod 4 & |d|=3 \Rightarrow \text{— " —},\quad y=\pm1,\ 2x-y=\pm1\end{cases}$$

$$\mathcal{O}_K^\times=\begin{cases}\mu_4 & d=-1\\ \mu_6 & d=-3\\ \{\pm1\} & d\neq -1,-3\end{cases}$$

(2) $d>0$:
($r_1=2, r_2=0$)

$$\begin{cases}x^2-dy^2=\pm1\\ x^2-xy+\frac{1-d}{4}y^2=\pm1\end{cases}\ (x,y\in\mathbb{Z}_{>0}) \iff \begin{array}{l}\left|\frac{x}{y}-\sqrt{d}\right| \text{ is small}\\ \left|\frac{x}{y}-\frac{1+\sqrt{d}}{2}\right| \text{— " —}\end{array}$$

continued fraction of $\begin{cases}\sqrt{d}\\ \frac{1+\sqrt{d}}{2}\end{cases}$ $\rightsquigarrow$ solutions $x_n-y_n\beta=(\underbrace{x_1-y_1\beta}_{\varepsilon})^n$

$$\mathcal{O}_K^\times=\{\pm1\}\times\varepsilon^{\mathbb{Z}}$$

Ex: $d=5$: $\quad \varepsilon=\frac{1+\sqrt5}{2}$

$d=7$: $\quad \sqrt7=[2;\overline{1,1,1,4}]$, $\quad [2,1,1,1]=2+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{1}}}=\frac{8}{3}$

$\varepsilon=8+3\sqrt7$

Units in $\mathcal{O}_K$ (general case)

$K \subset K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{\sigma \in \Sigma} K_\sigma \xrightarrow[\text{homog. pol. } /\mathbb{R} \text{ of deg } = n = [K:\mathbb{Q}]]{N} \mathbb{R}$ $\qquad N((x_\sigma)) = \prod_{j=1}^{r_1} \sigma_j(x) \prod_{k=1}^{r_2} |\sigma_{r_1+k}(x)|^2$

$\forall \alpha \in K \qquad N(\alpha) = N_{K/\mathbb{Q}}(\alpha)$.

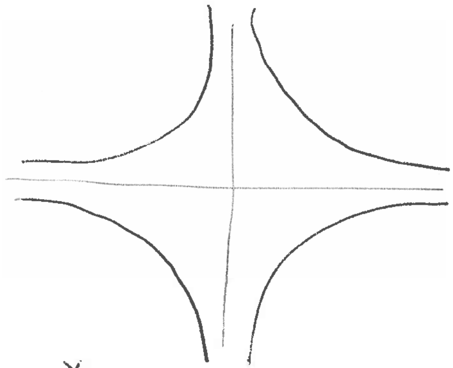
Units: $\mathcal{O}_K^\times = \mathcal{O}_K \; (= \text{lattice}) \cap \underbrace{\{x \in K_{\mathbb{R}} \mid |N(x)| = 1\}}_{\text{hypersurface } \{|N|=1\}}$

Ex: $K = \mathbb{Q}(\sqrt{d})$

$d < 0$: $|N| = 1$ compact

$\mathcal{O}_K \cap \{|N| = 1\} = \text{finite}$
discrete cpt

$d > 0$:



$\{|N| = 1\}$

Linearisation of $\{|N|=1\} \subset K_{\mathbb{R}}^\times$:

Group homomorphisms

$\log|N| : K_{\mathbb{R}}^\times \xrightarrow{\sim} \prod_{\sigma \in \Sigma} K_\sigma^\times \xrightarrow{\ell} \mathbb{R}^{r_1+r_2} \xrightarrow{\Sigma} \mathbb{R}$

$x = (x_\sigma) \longmapsto (\deg(\sigma) \log|x_\sigma|) \longmapsto \sum_{\sigma \in \Sigma} \deg(\sigma) \log|x_\sigma| = \log|N(x)|$

$\underbrace{H = \mathrm{Ker}(\Sigma)}_{\mathbb{R}\text{-v. sp. of}} \subset \mathbb{R}^{\Sigma} = \mathbb{R}^{r_1+r_2}$ $\quad \dim_{\mathbb{R}}(H) = r_1 + r_2 - 1$.

Prop. (1) $(\mathcal{O}_K \setminus \{0\}) \cap \mathrm{Ker}(\ell) = \mu(K) = \underbrace{(\mathcal{O}_K^\times)_{tors}}_{\text{finite}}$ (= roots of unity contained in K)

(2) $\ell(\mathcal{O}_K^\times)$ is a lattice in H.

Cor. (Dirichlet) $\quad \mathcal{O}_K^\times \simeq \mu(K) \times \mathbb{Z}^{r_1+r_2-1}$.

Pf: (1) If $\alpha \in \mathcal{O}_K$, $\ell(\alpha) = 0 \Rightarrow \forall \sigma : K \hookrightarrow \mathbb{C} \quad |\sigma(\alpha)| = 1$

$\Rightarrow \forall n \geq 1$ coeff. of $P_{K/\mathbb{Q}, \alpha^n}(T) = \prod_{\sigma : K \hookrightarrow \mathbb{C}} (T - \sigma(\alpha)^n) \in \mathbb{Z}[T]$

are bounded $\Rightarrow \{\alpha^n \mid n \geq 1\}$ is a finite set $\Rightarrow \alpha \in \mu(K)$.

As $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$, $|\mu(K)| < \infty$. Clearly, $\mu(K) \subset \mathrm{Ker}(\ell)$.

(2) $\alpha \in \mathcal{O}_K^\times \Rightarrow |N(\alpha)| = 1 \Rightarrow \ell(\alpha) \in H$.

$B \subset H$ bounded $\Rightarrow \ell^{-1}(B) \subset K_{\mathbb{R}}$ bounded $\Rightarrow |\mathcal{O}_K^\times \cap \ell^{-1}(B)| < \infty$

$\Rightarrow |\ell(\mathcal{O}_K^\times) \cap B| < \infty$. It remains to show that $H/\ell(\mathcal{O}_K^\times)$ is compact ($\Longleftrightarrow$ $\{|N| = 1\}/\mathcal{O}_K^\times$ is compact).

- Fix $c = (c_\sigma)_{\sigma\in\Sigma}$ s.t. $c_\sigma > 0$, $N(c) = \prod_\sigma c_\sigma^{\deg(\sigma)} = \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2} =: C$
- $\exists\, \alpha_1, \dots, \alpha_N \in \mathcal{O}_K \setminus \{0\}$ s.t. $\forall a \in \mathcal{O}_K \setminus \{0\}$ with $|N_{K/\mathbb{Q}}(a)| \le C$
  $\exists j \quad (a) = (\alpha_j) \quad (\Longleftrightarrow \quad a\alpha_j^{-1} \in \mathcal{O}_K^\times)$.
- $X := \{ (x_\sigma) \in K_\mathbb{R} \mid \forall \sigma \ \ |x_\sigma| \le c_\sigma \} \subset K_\mathbb{R}$ is compact
- Set $Y := \bigcup_{j=1}^{N} \alpha_j^{-1} X$ - also compact.

<u>Lemma</u>: $\{|N| = 1\} = \mathcal{O}_K^\times (\{|N|=1\} \cap Y)$ $\left(\Rightarrow \{|N|=1\}/\mathcal{O}_K^\times \text{ is cpt} \Rightarrow (2)\right)$.

<u>Pf</u>: Let $\beta \in \{|N| = 1\}$; then $\beta^{-1}X$ is cpt convex symmetric,
$\mathrm{vol}(\beta^{-1}X) = \mathrm{vol}(X) = 2^n \mathrm{covol}(\mathcal{O}_K) \Rightarrow \exists\ a \in \mathcal{O}_K \cap \beta^{-1}X$, $a \ne 0$.
$|N_{K/\mathbb{Q}}(a)| \le |N(\beta)|^{-1} C = C \Rightarrow \exists j\ \exists \varepsilon \in \mathcal{O}_K^\times \quad a = \alpha_j \varepsilon$
$\Rightarrow \quad \alpha_j \varepsilon = a = \beta^{-1} x$, $x \in X \Rightarrow \beta = \varepsilon^{-1}\alpha_j^{-1} x \in \mathcal{O}_K^\times (Y \cap \{|N|=1\})$.
$1 = |N(\beta)| = |N(\alpha_j^{-1}x)|$.

<u>Prop.</u> If $K \ne \mathbb{Q}$, then $|D_K| > 1$.

<u>Cor.</u> If $K \ne \mathbb{Q}$, then $\exists$ prime p which ramifies in $K/\mathbb{Q}$.

<u>Pf.</u> Minkowski's bound $\Rightarrow$ $M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_K|^{1/2} \ge 1$
$\Rightarrow |D_K| \ge \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2 \ge \left(\frac{\pi}{4}\right)^{n} 2^{2n-2} = \frac{\pi^n}{4} > 1$, as $n > 1$.
Induction: $n^n \ge 2^{n-1} n!$

Class field theory

$$\overbrace{\underbrace{K \subset K^{ab}}_{G_K^{ab} = G_K/[G_K, G_K]^{\text{closure}}} \subset \overline{K}}^{G_K}$$

K^{ab}/K maximal abelian extension

Toy model: the cyclotomic case

(1) Local case: $\mathbb{Q}_p^{ab} = \bigcup_{n \geq 1} \mathbb{Q}_p(\mu_n) =$

$$= \mathbb{Q}_p(\mu_{p^\infty}) \cdot \underbrace{\bigcup_{p \nmid m} \mathbb{Q}_p(\mu_m)}_{\mathbb{Q}_p^{ur}}, \qquad \mathbb{Q}_p^{ur} \cap \mathbb{Q}_p(\mu_{p^\infty}) = \mathbb{Q}_p$$

$$\mathbb{Q}_p \subset \mathbb{Q}_p^{ur} \subset \mathbb{Q}_p^{ur}(\mu_{p^\infty}) = \mathbb{Q}_p^{ab}$$

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p^{ur}) \arrow[r] \arrow[d, equal, "\text{inertia subgroup}"'] & \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \arrow[r] \arrow[dd, equal] & \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) \arrow[r] \arrow[d, "\wr"] & 1 \\
 & \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \arrow[d, "\wr"] & & \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \arrow[d, "\wr"] & \\
1 \arrow[r] & \mathbb{Z}_p^\times \arrow[r] \arrow[d, equal] & \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \arrow[r] & \hat{\mathbb{Z}} \cdot Fr_p \arrow[r] & 1 \\
1 \arrow[r] & \mathbb{Z}_p^\times \arrow[r] & \mathbb{Q}_p^\times \arrow[r, "v_p"] \arrow[u, hook] & \mathbb{Z} \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

(2) Global case: $\mathbb{Q}^{ab} = \bigcup_{n \geq 1} \mathbb{Q}(\mu_n)$, $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times \simeq \prod_p \mathbb{Z}_p^\times$

$p \nmid n$:

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$$
$$p \pmod n \longmapsto \left(\frac{\mathbb{Q}(\mu_n)/\mathbb{Q}}{p}\right).$$

Recall: $[K:\mathbb{Q}] < \infty$, L/K finite abelian extension

$\mathrm{Ram}(L/K)$ the set of places of K which ramify in L/K

($v \mid \infty$ lies in $\mathrm{Ram}(L/K) \iff K_v \simeq \mathbb{R}$ and $\exists\, w \mid v$ in L $L_w \simeq \mathbb{C}$)

If $\mathfrak{p} \notin \mathrm{Ram}(L/K)$, $P \mid \mathfrak{p}$ in $L \implies \left(\frac{L/K}{P}\right) \in \underbrace{\mathrm{Gal}(L/K)}_{\text{abelian}}$

depends only on $\mathfrak{p}$; call it $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Artin's symbol: for each fractional ideal $I \in I(\mathcal{O}_K)$ relatively prime to $\mathrm{Ram}(L/K)$, write $I = \prod_{\mathfrak{p} \notin \mathrm{Ram}(L/K)} \mathfrak{p}^{n(\mathfrak{p})}$ and define

$$\left(\frac{L/K}{I}\right) = \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}}\right)^{n(\mathfrak{p})} \in \mathrm{Gal}(L/K).$$

Analogue of $(\mathbb{Z}/n\mathbb{Z})^\times$: $[K:\mathbb{Q}]<\infty$

Data: $m = m_f m_\infty$, $(0)\neq m_f \subset O_K$ ideal, $m_\infty \subset \mathrm{Hom}(K,\mathbb{R}) = \{\sigma : K \hookrightarrow \mathbb{R}\}$

Def: $I_m = \{ I \in I(O_K) \text{ prime to } m_f \}$
$\cup$
P_m = subgroup generated by (α), $\alpha \in O_K$, $\alpha \equiv 1 \pmod{m_f}$
$\forall \sigma \in m_\infty \quad \sigma(\alpha) > 0$.

$Cl_m = I_m / P_m$

Ex: (1) $m=1$ ($m_f = (1)$, $m_\infty = \emptyset$): $I_m = I(O_K)$, $P_m = P(O_K)$, $Cl_m = Cl(O_K)$

(2) $K=\mathbb{Q}$, $m_f = (n)$, $m_\infty = \{\mathbb{Q} \hookrightarrow \mathbb{R}\}$

$I_m = \{ (ab^{-1}) \mid a,b \in \mathbb{Z}_{>0},\ (a,n)=(b,n)=1\}$

P_m = generated by $(c) \mid c \in \mathbb{Z}_{>0},\ c \equiv 1 \pmod n$

$$\begin{array}{ccc} Cl_m & \xrightarrow{\sim} & (\mathbb{Z}/n\mathbb{Z})^\times \\ \psi & & \psi \\ (ab^{-1}) & \longmapsto & (a \bmod n)(b \bmod n)^{-1} \end{array} \qquad (\simeq \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}))$$

(3) $K=\mathbb{Q}$, $m_f=(n)$, $m_\infty=\emptyset$ $\quad (n>2)$

I_m as above, P_m gen. by $(c) \mid c \in \mathbb{Z},\ c \equiv 1 \pmod n$
$\Longleftrightarrow$ by $(c) \mid c \in \mathbb{Z}_{>0},\ c \equiv \pm 1 \pmod n$

$Cl_m \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\} \qquad (\simeq \mathrm{Gal}(\mathbb{Q}(\mu_n)^+/\mathbb{Q}))$

$\mathbb{Q}(\mu_n)^+ = \mathbb{Q}(\mu_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Analogue of Dirichlet characters: $\chi : Cl_m \longrightarrow U(1)$

as in the classical case, χ has a conductor $f_\chi \mid m$ and it factors through $\chi: Cl_m \longrightarrow Cl_{f_\chi} \xrightarrow{\chi_{prim}} U(1)$

$$L(\chi,s) = L(\chi_{prim},s) = \sum_{\substack{(0)\neq I \subset O_K \\ (I,f_\chi)=(1)}} \chi_{prim}(I)\, N(I)^{-s} = \prod_{\substack{\mathfrak{p}\in Max(O_K) \\ \mathfrak{p} \nmid f_\chi}} (1-\chi_{prim}(\mathfrak{p})\, N(\mathfrak{p})^{-s})^{-1}$$

Artin's Reciprocity Law : $[L:K]<\infty$, $Gal(L/K)$ abelian

$\Longrightarrow$ (1) $\exists\, m \quad \forall \quad (\alpha) \in P_m \qquad \left(\frac{L/K}{(\alpha)}\right) = 1 \in Gal(L/K)$

(2) $\exists \quad H \subset Cl_m$ s.t. $\left(\frac{L/K}{\cdot}\right)$ induces an isomorphism $Cl_m/H \xrightarrow{\sim} Gal(L/K)$

(3) $\forall\, m \quad \forall\, H \subset Cl_m \quad \exists \ L/K$ as in (2)

$$\boxed{\text{Cor. } \quad \zeta_L(s) = \prod_{\substack{\chi \in \widehat{Cl_m} \\ \chi(H)=1}} L(\chi, s)}$$

Ray class fields: K_m/K abelian, $\left(\frac{K_m/K}{\cdot}\right) : Cl_m \xrightarrow{\sim} Gal(K_m/K)$

$Ram(K_m/K) = \{ v \mid m \}$

Ex: $m = 1$: $K_1 =$ Hilbert class field of K

= maximal abelian extension L/K s.t. $Ram(L/K) = \emptyset$.

$Gal(K_1/K) \xrightarrow{\sim} Cl(\mathcal{O}_K)$.

Ex: $K = \mathbb{Q}(\sqrt{-23})$ $\quad K_1 =$ splitting field of $T^3 - T + 1$

$K = \mathbb{Q}(\sqrt{-31})$ $\qquad T^3 + T + 1$

$(Cl(\mathcal{O}_K) \simeq \mathbb{Z}/3\mathbb{Z})$

Cor: $p \neq 23$ prime

$\exists\, x, y \in \mathbb{Z} \quad p = x^2 + 23y^2 \iff T^3 - T + 1 \equiv 0 \pmod p$ has 3 roots in $\mathbb{F}_p$.

Adèles ~~adèles~~

$[K:\mathbb{Q}]<\infty$, $\mathfrak{p}\in \mathrm{Max}(O_K)$ $\widehat{O}_{K,\mathfrak{p}} = \varprojlim_n O_K/\mathfrak{p}^n$, $K_\mathfrak{p} = \mathrm{Frac}(\widehat{O}_{K,\mathfrak{p}})$

Def: $K_\infty := K\otimes_\mathbb{Q} \mathbb{R} \xrightarrow{\sim} \prod_{v|\infty} K_v$

$$\underbrace{\mathbb{A}_{K,f}}_{\substack{\text{finite}\\ \text{adèles of } K}} := \{(x_\mathfrak{p})_{\mathfrak{p}\in\mathrm{Max}(O_K)} \mid x_\mathfrak{p}\in K_\mathfrak{p}\ ;\ \text{for almost all } \mathfrak{p} \quad x_\mathfrak{p}\in\widehat{O}_{K,\mathfrak{p}}\}$$

$$= \bigcup_{\substack{S\subset \mathrm{Max}(O_K)\\ |S|<\infty}} \underbrace{\Big(\prod_{\mathfrak{p}\in S} K_\mathfrak{p}\times\prod_{\mathfrak{p}\notin S}\widehat{O}_{K,\mathfrak{p}}\Big)}_{\text{product topology}} \Bigg\}\ \text{inductive } \varinjlim_S \text{ topology}$$

$$\underbrace{\mathbb{A}_K}_{\text{adèles of } K} = \underbrace{K_\infty\times\mathbb{A}_{K,f}}_{\text{product top.}} = \{(x_v)\mid x_v\in K_v\ ;\ \text{for almost all } v\nmid\infty \quad x_v\in\widehat{O}_{K,v}\}$$

$K \xhookrightarrow{\text{diag}} \mathbb{A}_K$, $x\longmapsto (x_v)$ $(x_v = x \ \forall v)$

Ex: $K=\mathbb{Q}$: $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \mathrm{Hom}_{Ab}(\mathbb{Q}/\mathbb{Z},\mathbb{Q}/\mathbb{Z})$

$$\mathbb{A}_{\mathbb{Q},f} = \widehat{\mathbb{Z}}\otimes_\mathbb{Z}\mathbb{Q} = \mathrm{Hom}_{Ab}(\mathbb{Q},\mathbb{Q}/\mathbb{Z})$$

approximation thm : $\mathbb{A}_\mathbb{Q} = \mathbb{Q} + (\mathbb{R}\times\widehat{\mathbb{Z}})$

as $\mathbb{Q}\cap(\mathbb{R}\times\widehat{\mathbb{Z}}) = \mathbb{Z} \Rightarrow \mathbb{A}_\mathbb{Q}/\mathbb{Q} \simeq (\mathbb{R}\times\widehat{\mathbb{Z}})/\mathrm{diag}(\mathbb{Z})\ (\xrightarrow{\sim} \varprojlim_n \mathbb{R}/n\mathbb{Z})$

In general: (1) $\mathbb{A}_K = K\otimes_\mathbb{Q}\mathbb{A}_\mathbb{Q}$; (0) $\mathbb{A}_K$ is a loc. cpt. topological ring
(2) K is discrete in $\mathbb{A}_K$; (3) $\mathbb{A}_K/K$ is compact and connected.

Idèles

$f_1,\dots,f_m\in O_K[T_1,\dots,T_n]$ define an affine algebraic variety $X\subset$ affine space of dim $=n$

$X(\mathbb{A}_K) = \{(x_1,\dots,x_n)\mid x_i\in\mathbb{A}_K,\ f_1,\dots,f_m(x_1,\dots,x_n)=0\}\subset \mathbb{A}_K^n$ has induced topology

Ex: idèles : $X=\mathbb{G}_m$ multiplicative group : $xy-1=0$

$$\begin{array}{l} \mathbb{G}_m(\mathbb{A}_K) = \{(x,y)\in\mathbb{A}_K^2\mid xy=1\} \\ \downarrow 2 \\ \mathbb{A}_K^\times = \{x=(x_v)\mid x_v\in K_v^\times\ ;\ \text{for almost all } v\nmid\infty \quad x_v\in\widehat{O}_{K,v}^\times\}\end{array}$$

topology induced by $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K^2$, $x\longmapsto(x,x^{-1})$ ($\Rightarrow$ inverse $x\mapsto x^{-1}$ is continuous)

Divisor map:
$$\mathbb{A}_K^\times \xrightarrow{\text{div}} I(O_K) \longrightarrow 0$$
$$(x_v)\longmapsto \prod_\mathfrak{p}\mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})}$$

$$\mathrm{Ker}(\mathrm{div}) = K_\infty^\times\times\underbrace{\prod_\mathfrak{p}\widehat{O}_{K,\mathfrak{p}}^\times}_{U} \Longrightarrow \mathbb{A}_K^\times/(K_\infty^\times\times U)K^\times \simeq \mathcal{C}\ell(O_K)$$

Idèle class group: $C_K = \mathbb{A}_K^\times / K^\times$

Ex: $K=\mathbb{Q}$: $\mathbb{Q}^\times \subset \mathbb{A}_\mathbb{Q}^\times \supset \mathbb{R}_{>0}^\times \times \hat{\mathbb{Z}}^\times$

$\mathbb{Q}^\times \cap (\mathbb{R}_{>0}^\times \times \hat{\mathbb{Z}}^\times) = \mathbb{Z}_{>0}^\times = \{1\}$

$Cl(\mathbb{Z}) = \{1\}$, $\quad \mathbb{R}^\times = \mathbb{R}_{>0}^\times \cdot \mathbb{Z}^\times \implies \mathbb{A}_\mathbb{Q}^\times = \mathbb{Q}^\times \cdot (\mathbb{R}_{>0}^\times \times \hat{\mathbb{Z}}^\times)$

$$\implies C_\mathbb{Q} = \mathbb{A}_\mathbb{Q}^\times / \mathbb{Q}^\times \simeq \underbrace{\mathbb{R}_{>0}^\times}_{\text{the connected component } C_\mathbb{Q}^0 \text{ of } C_\mathbb{Q} \text{ containing } 1} \times \hat{\mathbb{Z}}^\times$$

$$\implies \pi_0(C_\mathbb{Q}) = C_\mathbb{Q} / C_\mathbb{Q}^0 \xrightarrow{\sim} \hat{\mathbb{Z}}^\times = \mathrm{Gal}\Big(\bigcup_{n\geq 1} \mathbb{Q}(\mu_n)/\mathbb{Q}\Big) = \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}).$$

General case: $[K:\mathbb{Q}] < \infty$ $\qquad \exists$ reciprocity maps

$$\begin{tikzcd}
C_K \arrow[r, two heads] & \pi_0(C_K) \arrow[r, "\sim"] & \mathrm{Gal}(K^{ab}/K) \\
\mathbb{A}_K^\times \arrow[u, two heads] & & \\
K_v^\times \arrow[u, hook] \arrow[rr, hook] & & \mathrm{Gal}(K_v^{ab}/K_v) \arrow[uu, hook]
\end{tikzcd}$$

$\forall$ place v of K

Norm, discriminant - relative case

$A =$ Dedekind ring, $K = \mathrm{Frac}(A)$, $[L:K] < \infty$, $B =$ normalisation of A in L

Assume: (F) B is an A-module of finite type

Def: For a non-zero ideal $J \subset B$, set $N_{B/A}(J) = \underbrace{(B:J)}_{\text{index of } A\text{-modules of f.t.}} \subset A$

Properties: (1) $\forall P \in \mathrm{Max}(B)\ \forall n \geq 1$ $\quad N_{B/A}(P^n) = N_{B/A}(P)^n$, $N_{B/A}(P) = p^f$,

$p = P \cap A \in \mathrm{Max}(A)$, $f = f(P/p) = [B/P : A/p]$.

(2) $N_{B/A}(JJ') = N_{B/A}(J)\, N_{B/A}(J')$

(3) $\forall p \in \mathrm{Max}(A)$ $\quad (N_{B/A}(J))_p = \prod_{P|p} N_{B_p/A_p}(J_P)$

(4) $\forall \beta \in B \setminus \{0\}$ $\quad N_{B/A}((\beta)) = (N_{L/K}(\beta))$

(5) $\forall I \subset A$ non-zero ideal $\quad N_{B/A}(IB) = I^{[L:K]}$

Pf: (1) as in the case $A = \mathbb{Z}$; (2), (3) follow from (1)

(4) as in the case $A = \mathbb{Z}$, after localising at each $p \in \mathrm{Max}(A)$

~~We need to show~~ (5) enough for $I = p \in \mathrm{Max}(A)$: $pB = P_1^{e_1} \cdots P_r^{e_r}$,

$N_{B/A}(pB) = p^{\sum e_i f_i} = p^{[L:K]}$.

Def. Assume L/K separable ($\Rightarrow$ (F)). (1) $\forall p \in \mathrm{Max}(A)$

$B_p = BA_p$ is free of rk $= [L:K]$ over $A_p \Rightarrow \exists$ basis $\{w_i\}$ of B_p over A_p;

the local discriminant ideal $(0) \neq d_{B_p/A_p} = D(w_1, \dots, w_n) A_p \subset A_p$ does not depend on $\{w_i\}$ and is equal to A_p for almost all p

[if $A\alpha_1 \oplus \cdots \oplus A\alpha_n \subset B$, $\{\alpha_i\}$ basis of L/K, then
$d_{B_p/A_p} = A_p$ whenever $p \nmid D(\alpha_1, \dots, \alpha_n) \in A \setminus \{0\}$].

the global discriminant ideal $(0) \neq d_{B/A} \subset A$ is defined by

$\forall p \in \mathrm{Max}(A)$ $\quad (d_{B/A})_p = d_{B_p/A_p}$.

[if A is principal, choose $\{w_i\}$ s.t. $B = \bigoplus_{i=1}^{n} Aw_i$; then
$d_{B/A} = (D(w_1, \dots, w_n))$ is principal.]

---

(2) $B^* := \{ b \in L \mid \forall b' \in B\ \ \mathrm{Tr}_{L/K}(bb') \in A \}$ is a fractional ideal of B containing B. The different of B/A is the ideal (non-zero)
$\mathcal{D}_{B/A} = (B^*)^{-1} \subset B$.

We know: $\forall p \in \mathrm{Max}(A)$ $\quad B_p \subset (B^*)_p \subset d_{B_p/A_p}^{-1}(B_p)$

$\Rightarrow \quad \mathcal{D}_{B/A} \mid d_{B/A} \cdot B$

Ex: $A=\mathbb{Z}$, $B=\mathbb{Z}[i]$

$B^* = \{ x+iy \mid x,y\in\mathbb{Q},\ \forall a,b\in\mathbb{Z}\quad \underbrace{Tr_{\mathbb{Q}(i)/\mathbb{Q}}((x+iy)(a+bi))}_{2(ax-by)} \in \mathbb{Z}\} = \frac{1}{2}\mathbb{Z}[i]$

$\mathcal{D}_{\mathbb{Z}[i]/\mathbb{Z}} = 2\mathbb{Z}[i]$

Prop. Let L/K be separable. Then:

$[\mathfrak{p}\in Max(A)$ is unramified in $L/K \iff \mathfrak{p}\nmid d_{B/A}]$.

Cor. Let $[k:\mathbb{Q}]<\infty$. Then: [a prime number p is unramified in $L/\mathbb{Q} \iff p\nmid D_k$]

Pf. Lemma 1. Let F be a field, $C\supset F$ $\underset{(comm.)}{\text{a ring}}$ s.t. $\dim_F(C)<\infty$. Then

$Max(C)=\{m_1,\dots,m_r\}$ is finite and $\exists n\geq 1$ $(m_1\cdots m_r)^n=0$ (exercise).

$\left[\overset{(CRT)}{\Longrightarrow}\ C\simeq \prod_{m\in Max(C)} C/m^n,\quad \underbrace{Nil(C)}_{\sqrt{(0)}\text{ in } C} \simeq \prod_m m/m^n,\quad C^{red} = C/\sqrt{(0)} \simeq \prod_m \underbrace{C/m}_{\text{field}}\right]$

Lemma 2. In the situation of Lemma 1, it is equivalent:

(1) $T_{C/F}: C\times C \longrightarrow F$, $(x,y)\longmapsto Tr_{C/F}(xy)$ is a non-degenerate F-bilinear form.

(2) $C=C^{red} = \prod_{i=1}^r F_i$, F_i/F finite separable field extension.

Pf of Lemma 2: (2)$\Rightarrow$(1): $T_{C/F} = T_{\prod F_i/F} = \bigoplus \underbrace{T_{F_i/F}}_{\text{non-degenerate}}$ (F_i/F separable)

(1)$\Rightarrow$(2): $\forall x\in Nil(C)$ $Tr_{C/F}(x)=0 \Longrightarrow Nil(C)\subset$ kernel of $T_{C/F}=\{0\}$

$\Longrightarrow C=C^{red}=\prod_1^r F_i$, F_i field, $[F_i:F]<\infty$

$T_{C/F} = \bigoplus T_{F_i/F}$ non-deg. $\Longrightarrow F_i/F$ separable.

Pf of Prop: replace A by $A_\mathfrak{p}$ and B by $B_\mathfrak{p}=BA_\mathfrak{p}$; then

$B=\bigoplus_1^n Ab_i$ is free over A and $B/\mathfrak{p}B = \bigoplus_1^n (A/\mathfrak{p})\overline{b_i}$, $\overline{b_i}=b_i \pmod{\mathfrak{p}B}$

We have

$\mathfrak{p}\nmid d_{B/A} \iff \mathfrak{p}\nmid D(b_1,\dots,b_n) \iff D(\overline{b}_1,\dots,\overline{b}_n)\neq 0\in A/\mathfrak{p}$

$\iff T_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = \bigoplus_{i=1}^r T_{(B/P_i^{e_i})/(A/\mathfrak{p})}$ non-degenerate

$\iff \forall i$ $e_i=1$ & B/P_i is separable over $A/\mathfrak{p}$.

$(\mathfrak{p}B = P_1^{e_1}\cdots P_r^{e_r})$

Thm. If L/K is separable, then: (0) $\mathcal{D}_{B_P/A_\mathfrak{p}} = (\mathcal{D}_{B/A})_P$ $\forall P\in Max(B)$, $\mathfrak{p}=A\cap P$

(1) $d_{B/A} = N_{B/A}(\mathcal{D}_{B/A})$

(2) $P\in Max(B)$ is ramified in $B/A \iff P\mid \mathcal{D}_{B/A}$

(3) If $B=A[T]/(f)=A[\alpha]$ ($\alpha = T \pmod f$, f irred. over K)

then $\mathcal{D}_{B/A} = f'(\alpha)B$.

Pf: See [Serre] or [Cassels – Fröhlich].

(0) Exercise.

Pf: (1) $N_{B/A}(\mathcal{D}_{B/A}) = \underbrace{(B:(B^*)^{-1})}_{\text{index over } A} = (B^*:B)$

If B is A-free, $B = \bigoplus_{i=1}^{n} Ab_i$, then $(B^*:B) = (\det(\mathrm{Tr}_{L/K}(b_ib_j))) = d_{B/A}$.
In general replace A by A_p.

(2) later

(3) $$\frac{1}{f(T)} = \sum_{i=1}^{n} \frac{1}{f'(\alpha_i)(T-\alpha_i)} \Rightarrow \underbrace{\mathrm{Tr}_{L/K}\left(\frac{\alpha^j}{f'(\alpha)}\right)}_{\sum_{i=1}^{n} \frac{\alpha_i^j}{f'(\alpha_i)}} = \begin{cases} 0 & 0 \le j \le n-2 \\ 1 & j = n-1 \end{cases}$$

$$\Rightarrow \left(\bigoplus_{j=0}^{n-1} A\alpha^j\right)^* = \bigoplus_{j=0}^{n-1} A \frac{\alpha^j}{f'(\alpha)}$$

Prop. Let $A \subset B \subset C$, $K = \mathrm{Frac}(A) \subset L \subset M$, $[M:K] < \infty$, A = Dedekind, B (resp. C) normalisation of A in L (resp., in M), M/K separable

then: (1) $\mathcal{D}_{C/A} = \mathcal{D}_{C/B} \cdot i(\mathcal{D}_{B/A})$ $(i(I) = IC,\ I \subset B \text{ ideal})$

(2) $d_{C/A} = N_{B/A}(d_{C/B})\, d_{B/A}^{[M:L]}$

Pf. (1) let $z \in M$

$z \in \mathcal{D}_{C/A}^{-1} \Leftrightarrow \mathrm{Tr}_{M/K}(zC) \subseteq A \Leftrightarrow \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(zC)) \subset A$

$\Leftrightarrow \forall y \in B \quad \mathrm{Tr}_{L/K}(\underbrace{y\,\mathrm{Tr}_{M/L}(zC)}_{\mathrm{Tr}_{M/L}(yzC)}) \subset A \Leftrightarrow \mathrm{Tr}_{M/L}(zC) \subset \mathcal{D}_{B/A}^{-1}$

$\Leftrightarrow \mathrm{Tr}_{M/L}(z\mathcal{D}_{B/A}C) \subset B \Leftrightarrow z\mathcal{D}_{B/A}C \subset \mathcal{D}_{C/B}^{-1}$.

(2) $d_{C/A} = N_{C/A}(\mathcal{D}_{C/B} \cdot i(\mathcal{D}_{B/A})) = N_{B/A}(\underbrace{N_{C/B}(\mathcal{D}_{C/B})}_{d_{C/B}}) \underbrace{N_{B/A}(\underbrace{N_{C/B}(\mathcal{D}_{B/A}C)}_{\mathcal{D}_{B/A}^{[M:L]}})}_{d_{B/A}^{[M:L]}}$
