Algebraic Number Theory

Jingming Cui

1 Algebraic integers

Definition 1.1. A finite extension of $\mathbb{Q}$ is called **algebraic number field**.

Let K be an algebraic number field. Two fundamental questions arise:

1. How to define the ring of integers in K?
2. How to generalize the unique factorization theorem?

Definition 1.2. K algebraic number field. An element $\alpha \in K$ is called **integral** over $\mathbb{Z}$ if its minimal polynomial has coefficients in $\mathbb{Z}$.

Proposition 1.1. $\alpha \in K$ is integral over $\mathbb{Z}$ iff there exists $f(x) \in \mathbb{Z}[X]$ monic such that $f(\alpha) = 0$.

Proof. $\Longrightarrow$: clear.

$\Longleftarrow$: Suppose that $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ and $f(X) = \prod_{i=1}^r f_i(X)^{m_i}$ be factorization in $\mathbb{Q}[X]$ with all the leading coefficients 1. Then from Gauss Lemma $f_i(X) \in \mathbb{Z}[X]$, of $f(X)$ being irreducible. Since $f(\alpha) = 0$, there exists i such that $f_i(\alpha) = 0$. $\square$

Proposition 1.2. An element $\alpha \in K$ is integral over $\mathbb{Z}$ iff $\mathbb{Z}[\alpha]$ is finitely generated $\mathbb{Z}$-module.

Proof. $\Longrightarrow$: Suppose that α is integral over $\mathbb{Z}$, then α satisfies an equation

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathbb{Z}$$

Thus $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \cdots, \alpha^{n-1}$.

$\Longleftarrow$: If $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module. Let $\beta_1, \cdots, \beta_n$ be a set of generators of $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$. Consider the map $\alpha\cdot\colon \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]$. It is a homomorphism of $\mathbb{Z}$-module with respect to the basis $\beta_1, \cdots, \beta_n$, it has associated matrix $A \in \mathcal{M}_{n\times n}(\mathbb{Z})$. Let $f(X) = \det(X \cdot \mathrm{Id}_n - A) \in \mathbb{Z}[X]$ with leading coefficient 1, then $f(\alpha) = 0$. By Hamilton–Cayley Theorem, α is integral over $\mathbb{Z}$. $\square$

Corollary 1.1. Suppose that α, β integral over $\mathbb{Z}$, then $\alpha+\beta$, $\alpha\beta$ are both integral over $\mathbb{Z}$. In particular, all the integral element in K form a subring of K, denoted $\mathcal{O}_K$.

Proof. It is clear that $\alpha+\beta, \alpha\beta \in \mathbb{Z}[\alpha,\beta]$. By assumption $\mathbb{Z}[\alpha], \mathbb{Z}[\beta]$ is finitely generated $\mathbb{Z}$-module. Let $\alpha_1, \cdots, \alpha_r$ be a set of generators for $\mathbb{Z}[\alpha]$, $\beta_1, \cdots, \beta_s$ be a set of generators for $\mathbb{Z}[\beta]$. Then $\{\alpha_i\beta_j\}_{\substack{1\le i\le r\\ 1\le j\le s}}$ forms a set of generators of $\mathbb{Z}[\alpha,\beta]$. As $\mathbb{Z}$ is noetherian, the submodule $\mathbb{Z}[\alpha+\beta], \mathbb{Z}[\alpha\beta] \subset \mathbb{Z}[\alpha,\beta]$ are both finitely generated as $\mathbb{Z}$-module. By the previous assumption $\alpha+\beta$, $\alpha\beta$ are both integral over $\mathbb{Z}$. $\square$

Proposition 1.3. Let K be algebraic number field. Then $\mathcal{O}_K$ is a lattice in K, i.e., $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$ and $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} = K$. Moreover it contains all the subrings of K which is finitely generated as $\mathbb{Z}$-module.

Proof. 1) We show that $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} = K$. For $\alpha \in K$, it satisfies an equation:

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathbb{Q}$$

Take $c \in \mathbb{Z}$ such that $c \cdot a_i \in \mathbb{Z}$, $i = 1, \cdots, n$. Then $c^n(\alpha^n + a_1\alpha^{n-1} + \cdots + a_n) = 0$, so $(c\alpha)^n + (ca_1)(c\alpha)^{n-1} + \cdots + c^{n-1}(ca_n) = 0$. As $ca_i \in \mathbb{Z}$, $i = 1, \cdots, n$ and $c \in \mathbb{Z}$, we obtain that $c\alpha$ is integral over $\mathbb{Z}$. It follows that $c\alpha \in \mathcal{O}_K$, so $\alpha \in \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}$, and so $K \subset \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}$. On the other hand, since $\mathcal{O}_K \subset K$ and $\mathbb{Q} \subset K$, $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \subset K$. Therefore $K = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}$.

2) We show that $\mathcal{O}_K$ is finitely generate as $\mathbb{Z}$-module. If this holds, as $\mathcal{O}_K \subset K$ is torsion-free, it will be a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$. By 1) there exists $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_K$ which forms a basis of K over $\mathbb{Q}$.

   Let Λ be the $\mathbb{Z}$-module generated by $\alpha_1, \cdots, \alpha_n$, then Λ is a lattice in K and $\Lambda \subset \mathcal{O}_K$. Consider the bilinear form $\langle\cdot,\cdot\rangle\colon K \times K \to \mathbb{Q}$ defined by $\langle\alpha,\beta\rangle \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta)$. It is non-degenerate as $K/\mathbb{Q}$ is separable. For a lattice $L \subset K \cong \mathbb{Q}^n$, define $L^\vee = \{\alpha \in K \mid \langle\alpha, x\rangle \in \mathbb{Z}, \forall x \in L\}$. It is easy to verify that $L^\vee$ is still a lattice in K. So $\Lambda^\vee \subset \mathcal{O}_K^\vee$. Notice that $\mathcal{O}_K^\vee = \{\alpha \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x) \in \mathbb{Z}, \forall x \in \mathcal{O}_K\} \supset \mathcal{O}_K$ ($\alpha \in \mathcal{O}_K, x \in \mathcal{O}_K$ implies that $\alpha x \in \mathcal{O}_K$, so $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha x)$, the $(n-1)$-degree coefficient belongs to $\mathbb{Z}$. Thus $\mathcal{O}_K \subset \Lambda^\vee$. As $\mathbb{Z}$ is noetherian and $\Lambda^\vee$ is a lattice, we obtain that $\mathcal{O}_K$ is finitely generated.

3) Let $A \subset K$ be a subring and it is finitely generated as a $\mathbb{Z}$-module. We claim that any element of A is integral over $\mathbb{Z}$, which implies that $A \subset \mathcal{O}_K$. Indeed, let $\beta_1, \cdots, \beta_r$ be generators of A over $\mathbb{Z}$. Consider the homomorphism of $\mathbb{Z}$-modules $\alpha\cdot\colon A \to A$. Its associated matrix lies in $\mathrm{M}_{n\times n}(\mathbb{Z})$. Same argument as before shows that α is integral.

$\square$

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

(finite generation is necessary, see $\mathbb{Z} \subset \mathbb{Z}[1/p]$, $\mathbb{Z}[1/p]$ is not finitely generated $\mathbb{Z}$-module.)

This leads to a natural question: can we provide an abstract characterization of the ring of integers $\mathcal{O}_K$?

2 Dedekind domain

All the rings in this section are noetherian integral domain.

Definition 2.1. Let A be a subring of B. An element $\beta \in B$ is **integral** over A if there exists $f(x) \in A[X]$ with leading coefficient 1 such that $f(\beta) = 0$. This condition is also equivalent to $A[\beta]$ is finitely generated as A-module.

Proposition 2.1. For $\beta_1, \beta_2 \in B$. Suppose that β_1, β_2 are integral over A, then $\beta_1 + \beta_2$, $\beta_1\beta_2$ are integral over A. Hence all the elements of B which are integral over A form a subring of B, called the **integral closure** of A in B.

Example 2.1. $K/\mathbb{Q}$ finite, then $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

Definition 2.2. A ring A is called **integrally closed** if its integral closure in $\mathrm{Frac}(A)$ is A itself.

Definition 2.3. A **Dedekind domain** is a noetherian integral domain, which is integrally closed and of Krull dimension 1. (All the nonzero prime ideals are maximal).

Remark 2.1. Geometrically, A is an algebra over k, $k = \bar{k}$, $\mathrm{char}(k) = 0$, then A is of Krull dimension 1 iff A is the ring of regular functions on an affine algebraic curve. It is integrally closed iff the algebraic curve is smooth.

Example 2.2. Let $A = \mathbb{C}[[t^2, t^3]]$, then $\mathrm{Frac}(A) = \mathbb{C}((t))$, and the integral closure of A in $\mathrm{Frac}(A)$ is $\mathbb{C}[[t]]$.

Indeed, let $x = t^2$, $y = t^3$, then $y/x = t$ and x, y satisfy $y^2 = x^3$, so $(y/x)^2 = x$, and it follows that $t^2 = x$. Thus t is integral over A, $\mathbb{C}[[t]]$ is contained in the integral closure of $\mathbb{C}[[t^2, t^3]]$. But $\mathbb{C}[[t]]$ is a PID, hence already integrally closed. Consequently $\mathbb{C}[[t]]$ is the integral closure of A in $\mathbb{C}((t))$.

Geometrically, consider the algebraic curve $y^2 = x^3$ in $\mathbb{C}^2$. A is the completed local ring of the curve at 0. The introduction of $t = y/x$ is the blow-up at 0 of the curve.

Theorem 2.1. Let K be an algebraic number field, then $\mathcal{O}_K$ is a Dedekind domain.

Proposition 2.2. A PID is a Dedekind domain. In particular, $\mathbb{Z}$ and $k[T]$ (k a field), are Dedekind domains.

Proof. A PID is a noetherian integral domain. Moreover, a non-zero prime ideal in it is maximal. So it only suffices to show that it is integrally closed. Fix $x = a/b \in \mathrm{Frac}(A)$ with $(a, b) = 1$. If it is integral over A, then

$$\left(\frac{a}{b}\right)^n + c_1\left(\frac{a}{b}\right)^{n-1} + \cdots + c_n = 0$$

for some $c_1, \cdots, c_n \in A \iff a^n + c_1a^{n-1}b + c_2a^{n-2}b^2 + \cdots + c_nb^n = 0 \iff a^n = -b(c_1a^{n-1} + c_2a^{n-2}b + \cdots + c_nb^{n-1})$. By the unique factorization theorem of PID, a, b have common factor, contradiction to the assumption. $\square$

From the proof, a UFD is integral closed.

Theorem 2.2. Let A be a Dedekind domain with $\mathrm{Frac}(A) = K$. Let L be a finite separable extension of K. Let B be the integral closure of A in L, then B is a Dedekind domain.

$\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, Theorem 2.2 + Proposition 2.2 $\Longrightarrow$ Theorem 2.1.

Proof. 1) B is integral domain because $B \subset L$, L is a field.

2) B is noetherian.

Proposition 2.3. Same assumption as in Theorem 2.2, then B is finitely generated A-module and $B \otimes_A K = L$. Moreover, B contains all the subrings of L which is finitely generated as A-module.

If the proposition holds, B is finitely generated A-module implies that B is finitely generated A-algebra. Hence by Hilbert basis theorem, B is noetherian.

Proof of Proposition. 1) $B \otimes_A K = L$. Fix $x \in L$, it satisfies $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_1, \cdots, a_n \in K$. Let $c \in A$ be such that $ca_1, \cdots, ca_n \in A$, then $c^n(x^n + a_1x^{n-1} + \cdots + a_n) = 0$. It follows that $(cx)^n + (a_1c)(cx)^{n-1} + \cdots + (a_nc) \cdot c^{n-1} = 0$, so $cx \in B$, and so $B \otimes_A K = L$.

2) Let $\beta_1, \cdots, \beta_n$ (where $n = [L : K]$) be elements of B which forms a basis of L over K. Let $\Lambda = \sum_{i=1}^n A\beta_i$ be a finitely generated A-module. Consider the non-degenerate bilinear form $\langle \cdot, \cdot \rangle \colon L \times L \to K$, $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$. For a A-module contained in L, let $M^\vee = \{x \in L \mid \langle x, M \rangle \subset A\}$. Clearly $\Lambda^\vee \supset B^\vee$. and $\Lambda^\vee$ is

generated by dual basis $\beta_1^\vee, \cdots, \beta_n^\vee$ of $\beta_1, \cdots, \beta_n$ where $\langle \beta_i, \beta_j^\vee \rangle = \delta_{ij}$. Moreover $B^\vee = \{x \in L \mid \langle x, B\rangle \subset A\} = \{x \in L \mid \mathrm{Tr}_{L/K}(xb) \in A, \forall b \in B\} \supset B$. It contains B because $\mathrm{Tr}_{L/K}(xb) \in A$ for any $x \in B$. So $\Lambda^\vee \supset B^\vee \supset B$. Because A is noetherian and $\Lambda^\vee$ is a finitely generated A-module, $B \subset \Lambda^\vee$ is also finitely generated as A-module.

□

3) B is integrally closed.

Proposition 2.4. Let $A \subset B \subset C$ be inclusions of noetherian integral domain. Suppose that B is integral over A, and C is integral over B, then C is integral over A.

4) $\dim(B) = 1$.

Lemma 2.1 (Going down)**.** Let A be a subring of B. Suppose that B is integral over A. Let $\mathfrak{p} \subset \mathfrak{q} \subset B$ be prime ideals such that $\mathfrak{p} \cap A = \mathfrak{q} \cap A$, then $\mathfrak{p} = \mathfrak{q}$.

Assuming the lemma holds, suppose that $\dim(B) \neq 1$, then there exists prime ideals $0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{q} \subsetneq B$. Apply the lemma, get $0 \subsetneq \mathfrak{p} \cap A \subsetneq \mathfrak{q} \cap A \subsetneq A$, contradicts to $\dim(A) = 1$.

□

Example 2.3. 1) PID is Dedekind ring.

2) $\mathcal{O}_L \subset L$ finite.

Example 2.4. Let d be an odd square-free integer. Let $K = \mathbb{Q}(\sqrt{d})$. Let $x = a + b\sqrt{d} \in K$, $a, b \in \mathbb{Q}$. Then $x \in \mathcal{O}_K$ iff

$$\begin{cases} \mathrm{Tr}_{K/\mathbb{Q}}(x) = 2a \in \mathbb{Z}, \\ \mathrm{Nm}_{K/\mathbb{Q}}(x) = a^2 - b^2 d \in \mathbb{Z}. \end{cases}$$

$2a \in \mathbb{Z}$ iff $a \in \frac{1}{2}\mathbb{Z}$. If $a = \frac{2k+1}{2}$, then $b = \frac{2k'+1}{2}$ and $d \equiv 1 \pmod 4$ for $\mathrm{Nm}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. This implies that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & d \equiv 3 \pmod 4, \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4. \end{cases}$$

Example 2.5. Consider factorization in $\mathcal{O}_K$. $K = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{5}$. We can define the condition of irreducible, and factorization into irreducible elements. Note that $6 = 2 \cdot 3 = (1 + \sqrt{5})(1 - \sqrt{5})$. Verify that $2, 3, 1 + \sqrt{5}, 1 - \sqrt{5}$ are all irreducible. Suppose that $2 = (a + b\sqrt{5})(c + d\sqrt{5})$ where $a, b, c, d \in \mathbb{Z}$. It follows that $4 = (a^2 - 5b^2)(c^2 - 5d^2)$, so $b = d = 0$, $a^2c^2 = 4$. Thus $ac = \pm 2$, one deduce that $a = \pm 2, c = \pm 1$ or $a = \pm 1, c = \pm 2$. For irreducible $x, y \in \mathcal{O}_K$, there exists common divisors. It is the ideal generated by x, y in $\mathcal{O}_K$. Back to Example, consider $(2, 1+\sqrt{5})$, $(2, 1-\sqrt{5})$, $(3, 1+\sqrt{5})$, $(3, 1-\sqrt{5})$. Verify that they're both all maximal ideals, hence prime.

3 Localization and completion

We consider local properties of Dedekind ring.

Let p be a prime number, define

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, (a,b) = 1, p \nmid b \right\} = \mathbb{Z}\left[\frac{1}{\ell}, \ell \neq p \text{ prime}\right]$$

One can verify that the ideals of $\mathbb{Z}_{(p)}$ are all of the form $p^n\mathbb{Z}_{(p)}$, $n \in \mathbb{N}$. In fact, any $x \in \mathbb{Z}_{(p)}$ can be uniquely written as $x = p^n(a/b)$ where a, b coprime to p and $n \geq 0$. Then a/b is invertible in $\mathbb{Z}_{(p)}$, so we have $(x) = (p^n)$.

Define a function $\mathrm{val}_p \colon \mathbb{Z}_{(p)} \to \mathbb{Z} \cup \{\infty\}$ extend $\mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ by $x = p^n(a/b) \mapsto n$ and $0 \mapsto \infty$. It satisfies the property:

1) $\mathrm{val}_p(xy) = \mathrm{val}_p(x) + \mathrm{val}_p(y)$,

2) $\mathrm{val}_p(x+y) \geq \min\{\mathrm{val}_p(x), \mathrm{val}_p(y)\}$,

3) $\mathrm{val}_p(x) = \infty \iff x = 0$.

val_p is called **p-adic valuation**.

Therefore, we can define a norm $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ as $|x|_p = p^{-\mathrm{val}_p(x)}$, then it satisfies

1) $|x \cdot y|_p = |x|_p|y|_p$,

2) $|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$,

3) $|x|_p \geq 0$, and $|x|_p = 0 \iff x = 0$.

This norm is called **p-adic norm**.

Define $d_p : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}_{\geq 0}$ as $d_p(x,y) = |x-y|_p$, then

1) $d_p(x,y) \leq d_p(x,z) + d_p(z,y)$, $\forall z \in \mathbb{Q}$,

2) $d_p(x,y) \geq 0$, and $d_p(x,y) = 0 \iff x = y$.

So d_p defines a metric on $\mathbb{Q}$ (also on $\mathbb{Z}$ and $\mathbb{Z}_{(p)}$).

Remark 3.1. The definition above has arithmetic significance.

$$d_p(x,y) \le p^{-n} \iff |x-y|_p \le p^{-n} \iff \mathrm{val}_p(x-y) \ge n \iff x \equiv y \pmod{p^n} \quad (\text{if } x, y \in \mathbb{Z}).$$

That is, the higher the congruence between x and y, the closer are x and y.

Recall that to solve a Diophantine equation

$$\begin{cases} f_1(x_1, \cdots, x_n) = 0, \\ \cdots \\ f_m(x_1, \cdots, x_n) = 0, \end{cases} \qquad \text{where } f_i(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n].$$

We can solve it mod p^r, i.e., find $(a_1, \cdots, a_n) \in (\mathbb{Z}/p^r\mathbb{Z})^n$ such that $f_i(a_1, \cdots, a_n) \equiv 0 \pmod{p^r}$ holds for all $1 \le i \le m$. The solution becomes ever closer to the actual p-adic solution when $r \to +\infty$.

Notice that $\mathbb{Q}$ (resp. $\mathbb{Z}$, $\mathbb{Z}_{(p)}$) is not complete with respect to d_p. Let $\mathbb{Q}_p$ (resp. $\mathbb{Z}_p$) be the completion of $\mathbb{Q}$ (resp. $\mathbb{Z}$) with respect to d_p. (For a metric space (X, d), can always make it complete by means of Cauchy sequence. More precisely, a sequence $\{x_n\}_{n\in\mathbb{N}}$ in X is called a Cauchy sequence if $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$ such that $d(x_m, x_n) < \varepsilon$, $\forall m, n > N$. Two Cauchy sequences $\{x_n\}$, $\{y_n\}$ are equivalent iff $\lim_{n\to\infty} d(x_n, y_n) = 0$. Let $\widehat{X}$ be a set of the equivalence class of Cauchy sequences, then d extends to $\widehat{X}$ and $(\widehat{X}, d)$ is complete.)

Proposition 3.1. We have

$$\mathbb{Z}_p = \left\{ \sum_{n=0}^{+\infty} a_n p^n \mid a_n \in \{0, 1, \cdots, p-1\}, \forall n \in \mathbb{N} \cup \{0\} \right\}$$

and

$$\mathbb{Q}_p = \left\{ p^m \sum_{n=0}^{+\infty} a_n p^n \mid m \in \mathbb{Z}, a_n \in \{0, 1, \cdots, p-1\}, \forall n \in \mathbb{N} \cup \{0\} \right\}.$$

Proof. Let $\{x_n\}$ be a Cauchy sequence with respect to d_p. For arbitrary fixed $m \ge 1$, there exists N such that $d_p(x_n, x_{n'}) = |x_n - x_{n'}|_p \le p^{-m}$ holds for all $n, n' \ge N$. That is, $v_p(x_n - x_{n'}) \ge m$, $x_n \equiv x_{n'} \pmod{p^m}$. Take $0 \le y_m < p^m$ such that $y_m \equiv \lim_{n\to+\infty} \pi_m(x_n) \pmod{p^m}$. From definition $y_m \equiv y_{m-1} \pmod{p^{m-1}}$. Since $0 \le y_1 < p$, there exists unique $a_0 \in \{0, 1, \cdots, p-1\}$ such that $y_1 = a_0$. Since $0 \le y_2 < p^2$ and $y_2 \equiv y_1 = a_0 \pmod p$, it follows that $p \mid (y_2 - a_0)$ and $0 \le (y_2 - a_0)/p < p$, so there exists a unique $a_1 \in \{0, 1, \cdots, p-1\}$. such that $y_2 = a_0 + a_1 p$. By repeating the process, one can find a sequence $\{a_n\}$ such that $y_m = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1}$ holds for all m. Now we claim that $\{y_m\}$ is a Cauchy sequence which is equivalent to $\{x_n\}$. Indeed, since $y_n - y_m = a_m p^m + a_{m+1} p^{m+1} + \cdots + a_{n-1} p^{n-1}$, we have $p^m \mid (y_n - y_m)$, so

$|y_n - y_m|_p \leq p^{-m}$. For arbitrary $\varepsilon > 0$, one can choose m with $p^{-m} < \varepsilon$, then for every $n, n' \geq m$ we have $|y_n - y_{n'}|_p \leq p^{-m} < \varepsilon$. That is, $\{y_m\}$ is a Cauchy sequence in $\mathbb{Z}$, and then define a element in $\mathbb{Z}_p$, denoted as $\sum_{n=0}^{+\infty} a_n p^n$. Fix m, we have $x_n \equiv y_m \pmod{p^m}$ holds for n sufficiently large, so $|x_n - y_m|_p \leq p^{-m}$. Given $\varepsilon > 0$, we can choose m with $p^{-m} < \varepsilon$, and for n sufficiently large $|x_n - y_m|_p < \varepsilon$. Hence every element in $\mathbb{Z}_p$ can be written as $\sum_{n=0}^{+\infty} a_n p^n$.

Assume that $\sum_{n=0}^{+\infty} a_n p^n = \sum_{n=0}^{+\infty} b_n p^n$ in $\mathbb{Z}_p$. Fix $m \geq 1$, there exists N_0 such that $\left|\sum_{n=0}^{N-1} (a_n - b_n) p^n\right| \leq p^{-m}$ for all $N \geq N_0$. That is $\sum_{n=0}^{N-1} a_n p^n \equiv \sum_{n=0}^{N-1} b_n p^n \pmod{p^m}$, then $\sum_{n=0}^{m-1} a_n p^n \equiv \sum_{n=0}^{m-1} b_n p^n \pmod{p^m}$. Note that $\sum_{n=0}^{m-1} a_n p^n, \sum_{n=0}^{m-1} b_n p^n < p^m$, it follows that $\sum_{n=0}^{m-1} a_n p^n = \sum_{n=0}^{m-1} b_n p^n$ holds for every m. Consequently $a_n = b_n$ for all n.

Fix $x \in \mathbb{Q}$ and write $x = p^n(a/b)$, $a, b \in \mathbb{Z}$ coprime to p. We prove that $1/b$ can be expanded p-adically. Since $p \nmid b$, b is invertible in $\mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$. Then for every $r \geq 1$, there exists a unique c_r such that $0 \leq c_r < p^r$ and $bc_r \equiv 1 \pmod{p^r}$. Since $bc_{r+1} \equiv 1 \pmod{p^{r+1}}$, we have $bc_{r+1} \equiv 1 \pmod{p^r}$, so $c_{r+1} \equiv c_r \pmod{p^r}$. Therefore $|c_{r+1} - c_r| \leq p^{-r}$, $\{c_r\}$ is a Cauchy sequence, and converges to c in $\mathbb{Z}_p$. Note that $bc_r \equiv 1 \pmod{p^r}$ for all r, $|bc_r - 1|_p \leq p^{-r}$ for all r, so $bc = 1$. Thus $c = 1/b \in \mathbb{Z}_p$, $1/b = \sum_{n=0}^{+\infty} a_n p^n$ where $a_n \in \{0, 1, \cdots, p-1\}$. Moreover $\{a_n\}$ is essentially periodic sequence. So $\mathbb{Q}_p \supset \mathbb{Q} = \left\{\pm p^m \sum_{n=0}^{+\infty} a_n p^n \mid a_n \in \{0, 1, \cdots, p-1\}, \forall n \in \mathbb{N}, \text{and } \{a_n\} \text{ is essentially periodic}\right\}$.

Let $\{x_n\}$ be a Cauchy sequence in $\mathbb{Q}$, then there exists N such that $|x_n - x_{n'}|_p \leq 1$ for all $n, n' \geq N$. Thus $|x_n - x_N|_p \leq 1$, i.e., $v_p(x_n - x_N) \geq 0$, so $v_p(x_n) \geq \min\{v_p(x_N), 0\}$. Let $m = \min\{v_p(x_N), 0\} \in \mathbb{Z}$, it follows that $v_p(x_n) \geq m$ for all $n \geq N$, so $v_p(p^{-m}x_n) \geq 0$, i.e., $y_n \in \mathbb{Z}_{(p)}$. Set $y_n = p^{-m}x_n$, we have $x_n = p^m y_n$ where $y_n \in \mathbb{Z}_{(p)}$ for all $n \geq N$. Note that $|y_n - y_{n'}|_p = |p^{-m}(x_n - x_{n'})|_p = p^m |x_n - x_{n'}|_p \to 0$ since $|x_n - x_{n'}|_p \to 0$, $\{y_n\}$ is a Cauchy sequence. Thus $\{y_n\} \to y \in \mathbb{Z}_p$ for some y. Therefore $x = p^m y = p^m \sum_{n=0}^{+\infty} a_n p^n$, where $a_n \in \{0, 1, \cdots, p-1\}$. For the converse, given $x = p^m \sum_{n=0}^{+\infty} a_n p^n$ and consider $s_r = p^m \sum_{n=0}^{r} a_n p^n \in \mathbb{Q}$, since $|s_{r'} - s_r|_p \leq p^{-(m+r+1)}$, $\{s_r\}$ is a Cauchy sequence, and so $p^m \sum_{n=0}^{+\infty} a_n p^n \in \mathbb{Q}_p$. We finish the proof. $\square$

Remark 3.2. For a Cauchy sequence $\{x_n\}_{n=1}^{+\infty}$, the proof shows that we can find unique $0 \leq y_n \leq p^n$, $y_{n+1} \equiv y_n \pmod{p^n}$ for all n such that $\{y_n\}_{n=1}^{+\infty}$ forms a Cauchy sequence which is equivalent to $\{x_n\}_{n=1}^{+\infty}$. It also implies that

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n = \left\{(x_1, x_2, \cdots) \in \prod_{n \in \mathbb{N}} \mathbb{Z}/p^n \mid x_{n+1} \equiv x_n \pmod{p^n}, \forall n \in \mathbb{N}\right\},$$

which gives an algebraic expansion for $\mathbb{Z}_p$. In general, let A be a noetherian integral domain,

$I \subset A$ an ideal, can define the I-adic completion of A as $\widehat{A}_I = \varprojlim A/I^n$.

Let A be a ring. $S \subset A$ is called a multiplicative subset if $1 \in S$ and S is closed under multiplication. Define a relation on $A \times S$: $(a, s) \sim (b, t)$ iff there exists $u \in S$ such that $u(at - bs) = 0$.

One verifies that

1) $(a, s) \sim (a, s)$;

2) $(a, s) \sim (b, t)$ iff $(b, t) \sim (a, s)$;

3) $(a_1, s_1) \sim (a_2, s_2)$, $(a_2, s_2) \sim (a_3, s_3)$ implies $(a_1, s_1) \sim (a_3, s_3)$.

Define $S^{-1}A$ as the set of equivalence class in $A \times S$, equipped with

1) $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$

2) $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

get the ring of fraction of A with S.

Example 3.1. 1) Take $f \in A$, $f \neq 0$. Let $S = \{f^n\}_{n=0}^{+\infty}$, then $S^{-1}A = \left\{ \frac{a}{f^n} \mid a \in A, n \in \mathbb{N} \cup \{0\} \right\} \subset \mathrm{Frac}(A)$, denoted as A_f.

In case that $A = \mathbb{C}[x_1, \cdots, x_n]$, then $A_f = \left\{ \frac{g(x_1,\cdots,x_n)}{f(x_1,\cdots,x_n)^m} \mid g \in \mathbb{C}[x_1, \cdots, x_n], m \in \mathbb{N} \cup \{0\} \right\}$, the ring of rational functions on $\mathbb{C}^n$ which has poles along $V(f) = \{(x_1, \cdots, x_n) \in \mathbb{C}^n \mid f(x_1, \cdots, x_n) = 0\}$.

2) Let $\mathfrak{p} \subset A$ be a nonzero prime ideal. $S = A \setminus \mathfrak{p}$ is a multiplicative subset. Let $A_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}A$, call it the localization of A at $\mathfrak{p}$.

Proposition 3.2. Let A be a ring and $S \subset A$ be multiplicative set. Then

1) the ideals in $S^{-1}A$ are all of the form $S^{-1}\mathfrak{a}$, $\mathfrak{a} \subset A$ an ideal.

2) the prime ideals in $S^{-1}A$ are in bijection with the prime ideals in A which is disjoint from S.

Corollary 3.1. Let $\mathfrak{p} \subset A$ be a prime ideal, then the prime ideals in $A_{\mathfrak{p}}$ are in bijection with the prime ideals contained $\mathfrak{p}$. In particular it has unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.

Extension to A-module M. Define a relation on $M \times S$, $(m, s) \sim (n, t)$ iff $u(mt - ns) = 0$ for some $u \in S$. Similarly can verify that it is an equivalence relation. Define $S^{-1}M$ as the set of equivalence class in $M \times S$, equipped with

1) $\frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st}$ $m, n \in M$, for arbitrary $s, t \in S$.

2) $\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$, for arbitrary $a \in A$, $m \in M$, $s, t \in S$.

Get an $S^{-1}A$-module $S^{-1}M$, called the localization of M with respect to S.

Proposition 3.3. Let A be a ring. $S \subset A$ is a multiplicative set.

1) For an exact sequence $M_1 \to M_2 \to M_3$ of A-module, the induced sequence $S^{-1}M_1 \to S^{-1}M_2 \to S^{-1}M_3$ is exact.

2) Let M be an A-module, then $M \otimes_A S^{-1}A = S^{-1}M$. In particular $S^{-1}A$ is a flat A-module.

3) For A-modules M, N, we have $S^{-1}M \otimes_{S^{-1}A} S^{-1}N = S^{-1}(M \otimes_A N)$.

Proposition 3.4 (Local-Global Properties)**.** Let M be a A-module, TFAE:

1) $M = 0$

2) $M_{\mathfrak{p}} = 0$ for any prime ideal $\mathfrak{p} \subset A$

3) $M_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{m} \subset A$.

Proposition 3.5. Let A be a noetherian integral domain, then $A = \bigcap_{\mathfrak{p} \text{ prime}} A_{\mathfrak{p}}$ inside $\mathrm{Frac}(A)$.

Lemma 3.1 (Nakayama)**.** Let A be a local ring, noetherian integral domain. Let M be a finitely generated A-module. Suppose $M = \mathfrak{m}M$, then $M = 0$.

Corollary 3.2. Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated A-module. Suppose it has a submodule N such that $M = N + \mathfrak{m}M$, then $M = N$.

Corollary 3.3. Same hypothesis as in Corollary 3.2. Suppose that the image of $x_1, \cdots, x_r \in M$ in $M/\mathfrak{m}M$ form a basis of this vector space, then $x_1, \cdots, x_r$ generates M.

Let G be a topological abelian group, i.e., it is equipped with a topology such that $G \times G \xrightarrow{+} G$ and the inverse $G \to G$ are both continuous with respect to this topology.

For $a \in G$, let $T_a \colon G \to G$ defined by $x \mapsto x + a$ be the translation by a, then T_a is a homeomorphism. Indeed, T_a has a inverse T_{-a}, clearly T_a is the composition of $x \mapsto (x, a)$ and $(x, a) \mapsto x + a$, so is continuous, and similarly T_{-a} is continuous. So the topology of G is determined by the topology around $0 \in G$.

Proposition 3.6. If $\{0\}$ is closed in G, then G is Hausdorff.

Proof. Recall that a topology space X is Hausdorff iff $\Delta_X = \{(x, x) \mid x \in X\} \subset X \times X$ is closed. Notice that Δ_X is the preimage of $\{0\}$ for the map

$$f\colon G \times G \longrightarrow G, \quad (x, y) \longmapsto x - y$$

As f is continuous, if $\{0\}$ is closed, then Δ_X is closed as well. $\square$

Proposition 3.7. Let H be the intersection of all the open neighborhoods of $0 \in G$, then

1) H is a subgroup of G.

2) H is the closure of $\{0\}$.

3) G/H is Hausdorff.

4) $H = 0$ iff $\{0\}$ is closed iff G is Hausdorff.

Proof. 1) Need to show that H is closed under addition and taking inverse. For $i\colon G \to G$ defined by $x \mapsto -x$, it is a homeomorphism, so $i^{-1}(U)$ remains open. Thus

$$i^{-1}(H) = i^{-1}\left(\bigcap_{0 \in U \text{ open}} U\right) = \bigcap_{0 \in U \text{ open}} i^{-1}(U) = \bigcap_{0 \in V \text{ open}} V = H.$$

For $\mu\colon G \times G \to G$ defined by $(x, y) \mapsto x + y$, we have

$$\mu^{-1}(H) = \mu^{-1}\left(\bigcap_{0 \in U \text{ open}} U\right) = \bigcap_{0 \in U \text{ open}} \mu^{-1}(U).$$

Since $\mu^{-1}(U)$ is open in $G \times G$, it contains $H \times H$, so $\mu^{-1}(H) \supset H \times H$, i.e., $H \supset \mu(H \times H)$. Therefore H is closed under addition. Consequently, H is a subgroup of G.

2) $x \in H$ iff x lies in any open neighborhood U of 0, iff $0 \in x - U$ for every open neighborhood U of 0, iff every neighborhood of x contains 0, iff $x \in \overline{\{0\}}$.

3) Recall that a subset in G/H is closed iff its image under natural projection $G \to G/H$. By 2), $0_H \in G/H$ is closed. By Proposition 3.6, G/H is Hausdorff.

4) If $H = \{0\}$, we have $\overline{\{0\}} = \{0\}$ from 2), so $\{0\}$ is closed. If $\{0\}$ is closed, G is Hausdorff from Proposition 3.6. If G is Hausdorff, for any $x \in G$, $x \neq 0$, there exists $U_x \ni x$, $V \ni 0$ such that $U_x \cap V = \emptyset$. It follows that $x \notin H$, so $H = \{0\}$.

$\square$

Assume that $0 \in G$ has a countable fundamental system of open neighborhood, we can define the completion $\widehat{G}$ using Cauchy sequence. By definition, a sequence $\{x_n\}$ in G is a Cauchy sequence iff for any open neighborhood U of 0, there exists $N \in \mathbb{N}$ such that $x_n - x_m \in U$ for all $n, m \geq N$. Two Cauchy sequences $\{x_n\}, \{y_n\}$ are equivalent iff $\lim_{n\to\infty}(x_n - y_n) = 0$. Then $\widehat{G}$ is defined as the set of equivalence class of Cauchy sequences.

Remark 3.3. The natural map $i\colon G \to \widehat{G}$ defined by $x \mapsto (x, x, \cdots)$ is not automatically injective. In fact, $\mathrm{Ker}(i) = \bigcap_{0\in U \text{ open}} U = H$. So i is injective iff $H = \{0\}$ iff G is Hausdorff.

Proposition 3.8. The morphism $i\colon G \to \widehat{G}$ is injective iff G is Hausdorff.

In the following, suppose $0 \in G$ has a fundamental system of open neighborhood consisting of subgroups, i.e., there exists a sequence $G = G_0 > G_1 > G_2 > \cdots$ such that $U < G$ is open iff U contains G_n for some n.

Example 3.2. The p-adic topology for $\mathbb{Z}$ is given by the sequence $\mathbb{Z} \supset p\mathbb{Z} \supset p^2\mathbb{Z} \supset \cdots$.

Proposition 3.9. In the above situation, all the groups G_n are open and closed at the same time. G is totally disconnected if it is Hausdorff.

Proof. G_n is open by definition. Since G_n is a subgroup of G, G admits a coset decomposition, i.e., $G = G_n \cup \bigcup_{x\notin G_n}(x + G_n)$ is disjoint union. So $G_n = G \setminus \bigcup_{x\notin G_n}(x + G_n)$ is closed.

A topological space is totally disconnected iff its connected components are single points. It only need to show the connected component containing 0 is $\{0\}$. Let C_0 be the connected component containing 0. It follows that $C_0 \subset G_n$ for all n, otherwise $C_0 = (C_0 \cap G_n) \cup (C_0 \cap (G \setminus G_n))$ implies that C_0 is not connected. Thus $C_0 \subset \bigcap_{n=0}^{\infty} G_n$. If G is Hausdorff, $\subset \bigcap_{n=0}^{\infty} G_n = \{0\}$, so $C_0 = \{0\}$. □

For such topology abelian group G, its completion $\widehat{G}$ is constructed with Cauchy sequence. Notice that for a Cauchy sequence $\{x_n\}$ in G, let $\pi_n\colon G \to G/G_n$, $\varinjlim_{n\to\infty} \pi_m(x_n) = \pi_m(x_N)$ for some $N \gg 0$. As explained in the construction of $\mathbb{Z}_p$ we have

$$\widehat{G} = \varprojlim G/G_n = \left\{(x_1, x_2, \cdots) \in \prod_{n\in\mathbb{N}} G/G_n \mid x_{n+1} \bmod G_n = x_n, \forall n \in \mathbb{N}\right\}.$$

It is equipped with a topology which is generated by translations of open sets of the form

$$\widehat{G_n} = \left\{(0, \cdots, 0, x_n, x_{n+1}, \cdots) \in \prod_{n\in\mathbb{N}} G/G_n \mid x_{n+1} \bmod G_n = x_n, \forall n \in \mathbb{N}\right\}$$

Proposition 3.10. Suppose that $|G/G_n| < +\infty$ for all $n \in \mathbb{N}$, then $\widehat{G}$ is a compact topological space.

Proof. Define two continuous $\alpha_n\colon \prod_{n\in\mathbb{N}} G/G_n \to G/G_n$ by $(x_m)_{m=1}^{+\infty} \mapsto x_n$ and $\beta_n\colon \prod_{n\in\mathbb{N}} G/G_n \to G/G_n$ by $(x_m)_{n=1}^{+\infty} \mapsto x_{n+1} \bmod G_n$ (note that it is the composition of $\prod_{n\in\mathbb{N}} G/G_n \to G/G_{n+1}$ and natural map $G/G_{n+1} \to G/G_n$), where $\prod_{n\in\mathbb{N}} G/G_n$ is equipped with the product topology. Since $|G/G_n| < +\infty$, it is Hausdorff, so Δ_{G/G_n} is closed, and so $(\alpha_n, \beta_n)^{-1}(\Delta_{G/G_n})$ is closed. Hence $\widehat{G} = \bigcap_{n\in\mathbb{N}} (\alpha_n, \beta_n)^{-1}(\Delta_{G/G_n})$ is closed in $\prod_{n\in\mathbb{N}} G/G_n$. By assumption, G/G_n is finite, hence compact. By Tychonoff Theorem, $\prod_{n\in\mathbb{N}} G/G_n$ is compact, so $\widehat{G}$ is compact as $\widehat{G}$ is closed in $\prod_{n\in\mathbb{N}} G/G_n$. $\square$

Example 3.3. $\mathbb{Z}_p$ is compact as $|\mathbb{Z}/p^n| = p^n < +\infty$.

Question: Is completion an exact functor?

Definition 3.1. 1) A projective system is a sequence of abelian groups $\{A_n\}_{n\in\mathbb{N}}$ equipped with translation morphism $\pi_n\colon A_{n+1} \to A_n$. Its projective limit is defined as

$$\varprojlim_n A_n = \left\{ (x_1, x_2, \cdots) \in \prod_{n\in\mathbb{N}} A_n \mid \pi_n(x_{n+1}) = x_n, \forall n \in \mathbb{N} \right\}$$

equipped with topology generated by translation of open sets of the form

$$\left\{ (0, \cdots, 0, x_n, x_{n+1}, \cdots) \in \prod_{n\in\mathbb{N}} \pi_n(x_{n+1}) = x_n, \forall n \in \mathbb{N} \right\}$$

2) The projective system $\{A_n\}_{n\in\mathbb{N}}$ is said to satisfy the Mittag-Leffler condition if π_n is surjective for $n \gg 0$.

3) Given projective systems $\{A_n\}, \{B_n\}, \{C_n\}$, if we have commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{n+1} & \longrightarrow & B_{n+1} & \longrightarrow & C_{n+1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0 \end{array}$$

for all n, we say that there is an exact sequence of projective system

$$0 \longrightarrow \{A_n\} \longrightarrow \{B_n\} \longrightarrow \{C_n\} \longrightarrow 0$$

Is it true that the sequence

$$0 \longrightarrow \varprojlim_n A_n \longrightarrow \varprojlim_n B_n \longrightarrow \varprojlim_n C_n \longrightarrow 0$$

is exact?

Theorem 3.1. Suppose that we have an exat sequence of projective systems

$$0 \longrightarrow \{A_n\} \longrightarrow \{B_n\} \longrightarrow \{C_n\} \longrightarrow 0 \ ,$$

then the sequence

$$0 \longrightarrow \varprojlim_n A_n \longrightarrow \varprojlim_n B_n \longrightarrow \varprojlim_n C_n$$

is always exact. If $\{A_n\}$ satisfies Mittag-Leffler condition, the sequence

$$0 \longrightarrow \varprojlim_n A_n \longrightarrow \varprojlim_n B_n \longrightarrow \varprojlim_n C_n \longrightarrow 0$$

is exact.

Proof. Let $A = \prod_{n\in\mathbb{N}} A_n$, define $d^A\colon A \to A$ defined by $(x_n)_n \mapsto (x_n - \pi_n(x_{n+1}))_n$ where $\pi_n\colon A_{n+1} \to A_n$ is the translation map, then $\varprojlim_n A_n = \mathrm{Ker}(d^A)$. Similarly we can define $(B, d^B), (C, d^C)$. By assumption, we have commutative diagram with exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{n+1} & \longrightarrow & B_{n+1} & \longrightarrow & C_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi_n^A} & & \downarrow{\scriptstyle \pi_n^B} & & \downarrow{\scriptstyle \pi_n^C} & & \\ 0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0 \end{array}$$

so we obtain commutative diagram of exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

By snake lemma, get the long exact sequence

$$0 \longrightarrow \mathrm{Ker}(d^A) \longrightarrow \mathrm{Ker}(d^B) \longrightarrow \mathrm{Ker}(d^C) \longrightarrow \mathrm{Coker}(d^A) \longrightarrow \mathrm{Coker}(d^B) \longrightarrow \mathrm{Coker}(d^C) \longrightarrow 0 \ .$$

By $\varprojlim_n A_n = \mathrm{Ker}(d^A)$ get the first exact sequence.

For the second assertion, as $\varprojlim_n A_n = \varprojlim_{n\geq n_0} A_n$, can assume that $\pi_n^A\colon A_{n+1} \to A_n$ is always surjective, then $d^A\colon A \to A$ defined by $(x_n) \mapsto (x_n - \pi_n(x_{n+1}))$ is surjective: For $(a_n) \in A = \prod_{n\in\mathbb{N}} A_n$, the equation $x_n - \pi_n(x_{n+1}) = a_n$ can be solved as π_n is surjective. Thus $\mathrm{Coker}(d^A) = \{0\}$, the second assertion holds. $\square$

Corollary 3.4. Let G be a topological abelian group with topology defined by a sequence of subgroups $\{G_n\}_{n\in\mathbb{N}}$. Suppose that we have exact sequence

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$$

and G', G'' are equipped with topology induced from G (defined by $\{G' \cap G_n\}$ and $\{\pi(G_n)\}$ respectively), then the sequence

$$0 \longrightarrow \widehat{G'} \longrightarrow \widehat{G} \longrightarrow \widehat{G''} \longrightarrow 0$$

is exact.

Proof. We have $(G' + G_n)/G_n \cong G'/(G' \cap G_n)$. On the other hand, $(G/G_n)/((G' + G_n)/G_n) \cong G/(G' + G_n)$, so $G/(G' + G_n) \cong (G/G')/\pi(G_n) = G''/\pi(G_n)$. Clearly $\mathrm{Ker}(G/G_n \to G/(G' + G_n)) = (G' + G_n)/G_n = \mathrm{Im}(G'/(G' \cap G_n) \to G/G_n)$. Hence we have short exact sequence

$$0 \longrightarrow G'/(G' \cap G_n) \longrightarrow G/G_n \longrightarrow G''/\pi(G_n) \longrightarrow 0\ .$$

Note that $G'/(G' \cap G_{n+1}) \to G'/(G' \cap G_n)$ is always surjective, $\{G'/(G' \cap G_n)\}$ satisfies the Mittag-Leffler condition. By Theorem 3.1 we finish the proof. $\square$

Corollary 3.5. Let G be a topological abelian group with topology defined by a sequence of subgroup $\{G_n\}_{n\in\mathbb{N}}$, then $\widehat{G}/\widehat{G_n} \cong G/G_n$. In particular $\widehat{\widehat{G}} = \widehat{G}$ and $\widehat{G}$ is Hausdorff.

Proof. Fix n and consider the exact sequence

$$0 \longrightarrow G_n \longrightarrow G \longrightarrow G/G_n \longrightarrow 0\ .$$

Equip G_n and G/G_n with the induced topology, then for arbitrary $m > n$,

$$0 \longrightarrow G_n/G_m \longrightarrow G/G_m \longrightarrow G/G_n \longrightarrow 0$$

is exact. By Theorem 3.1, get

$$\begin{tikzcd}
0 \arrow[r] & \varprojlim_m G_n/G_m \arrow[r] \arrow[d, equal] & \varprojlim_m G/G_m \arrow[r] \arrow[d, equal] & \varprojlim_m G/G_n \arrow[r] & 0 \\
& \widehat{G_n} & \widehat{G} & &
\end{tikzcd}$$

we obtain $\widehat{G}/\widehat{G_n} \cong G/G_n$.

From definition $\widehat{\widehat{G}} = \varprojlim_n \left(\widehat{G}/\widehat{G_n}\right) = \varprojlim_n (G/G_n) = \widehat{G}$. $\square$

Definition 3.2. Let A be a commutative ring, $\mathfrak{a} \subset A$ be an ideal, M be an A-module. $\widehat{A} = \varprojlim_n A/\mathfrak{a}^n$ is called $\mathfrak{a}$-adic completion of A. It is a topological ring. $\widehat{M} = \varprojlim_n M/\mathfrak{a}^n M$ is called $\mathfrak{a}$-adic completion of M. It is naturally an $\widehat{A}$-module.

Question

1) Is $\widehat{M} = M \otimes_A \widehat{A}$? What is $M \to \widehat{A}$?

2) Is $\widehat{A}$ a flat A-algebra?

3) If A is noetherian, does $\widehat{A}$ remain noetherian?

For 2), given an exact sequence of A-module

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0 \ ,$$

is the sequence

$$0 \longrightarrow M_1 \otimes_A \widehat{A} \longrightarrow M \otimes_A \widehat{A} \longrightarrow M_2 \otimes_A \widehat{A} \longrightarrow 0$$

exact?

Natural question: Does the $\mathfrak{a}$-adic topology on M induced the $\mathfrak{a}$-adic topology on M_1? That is, $\{\mathfrak{a}^n M \cap M'\} \sim \{\mathfrak{a}^m M'\}$? This is equivalent to for arbitrary $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $\mathfrak{a}^m M' \subset \mathfrak{a}^n M \cap M'$; and for arbitrary $m \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that $\mathfrak{a}^n M \cap M' \subset \mathfrak{a}^m M'$.

Definition 3.3. A filtration of M by A-modules

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots$$

is called $\mathfrak{a}$-filtration if $\mathfrak{a} M_n \subset M_{n+1}$ for all $n \in \mathbb{N}$. It is called a stable $\mathfrak{a}$-filtration if $\mathfrak{a} M_n = M_{n+1}$ for all $n \gg 0$.

Remark 3.4. $\{\mathfrak{a}^n M\}$ is a stable $\mathfrak{a}$-filtration.

Lemma 3.2. All the stable $\mathfrak{a}$-filtration on M defines the same topology on M.

Proof. Only need to show they define the same topology as $\{\mathfrak{a}^n M\}$. Let $\{M_n\}$ be a stable $\mathfrak{a}$-filtration, then $\mathfrak{a}^n M = \mathfrak{a}^n M_0 \subset M_n$ by definition. So the topology defined by $\{\mathfrak{a}^n M\}$ is coarser than by $\{M_n\}$. On the other hand, there exists n_0 such that $\mathfrak{a}^n M \supset \mathfrak{a}^n M_m = M_{n+m}$ for all $n \geq n_0$. Therefore the topology defined by $\{M_n\}$ is no coarser than that by $\{\mathfrak{a}^n M\}$. The two topology are equivalent. $\square$

Definition 3.4. 1) Let $A^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$, $\mathfrak{a}^0 = A$, with the ring structure $x_n \cdot x_m = x_n x_m \in \mathfrak{a}^{n+m}$ for $x_n \in \mathfrak{a}^n$ and $x_m \in \mathfrak{a}^m$. This makes A^* a graded ring, with $\mathfrak{a}^n$ being the degree n component of A^*.

2) For a $\mathfrak{a}$-filtration $\{M_n\}$ of M, defined $M^* = \bigoplus_{n=0}^{\infty} M_n$. It is equipped with a A^*-module structure by $x_i \cdot m_j = x_i m_j \in M_{i+j}$ for any $x_i \in \mathfrak{a}^i$ and $m_j \in M_j$. Then M^* is a graded A^*-module with M_n being the degree n component of M^*.

Geometrically, let $X = \operatorname{Spec} A$ and $Z = V(\mathfrak{a}) \subset X$. The blow-up along Z is $\operatorname{Bl}_Z X = \operatorname{Proj} A^*$.

Lemma 3.3. If A is noetherian, $\mathfrak{a} \subset A$ is an ideal, then A^* is noetherian.

Proof. By assumption, $\mathfrak{a}$ is finitely generated, let $x_1, \cdots, x_n$ be a set of generators. Define $A[X_1, \cdots, X_n] \to A^* = A \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \cdots$ by $X_1^{a_1} \cdots X_n^{a_n} \mapsto x_1^{a_1} \cdots x_n^{a_n} \in \mathfrak{a}^n$. It is a morphism of graded algebra and it is surjective. By Hilbert Basis Theorem, $A[X_1, \cdots, X_n]$ is noetherian. So $A^* = A[x_1, \cdots, x_n]$ is noetherian since the quotient ring of a noetherian ring is also noetherian. □

Lemma 3.4. Let A be a noetherian ring, M a finitely generated A-module. Let $\{M_n\}$ be a $\mathfrak{a}$-filtration, then the following conditions are equivalent:

1) $\{M_n\}$ is a stable $\mathfrak{a}$-filtration.

2) M^* is a finitely generated A^*-module.

Proof. First assume that $\{M_n\}$ is stable, there exists N_0 such that $M_{n+1} = \mathfrak{a}M_n$ for all $n \geq n_0$. So for arbitrary $m \geq n_0$ we have $M_m = \mathfrak{a}^{m-n_0} M_{n_0}$. We claim that $A^*(M_0 \oplus M_1 \oplus \cdots \oplus M_{n_0}) = M^*$. Clearly $A^*(M_0 \oplus M_1 \oplus \cdots \oplus M_{n_0}) \subset M^*$, given $x \in M^*$ homogeneous, on the other hand note that $M_0 \oplus M_1 \oplus \cdots \oplus M_{n_0} \subset A^*(M_0 \oplus M_1 \oplus \cdots \oplus M_{n_0}$ and $M_m = \mathfrak{a}^{m-n_0} M_{n_0} \subset A^* M_{n_0}$ for $m > n_0$, we then obtain $A^*(M_0 \oplus M_1 \oplus \cdots \oplus M_{n_0}) \supset M^*$. Since M is finitely generated and A is noetherian, $M_0, \cdots, M_{n_0}$ as submodule of M is also finitely generated, it follows that $M_0 \oplus \cdots \oplus M_{n_0}$ is finitely generated as A^*-module, hence M^* is finitely generated A^*-module.

Now assume that M^* is finitely generated as A^*-module, we can choose homogeneous $x_1, \cdots, x_s$ which generates M^*. Let $n_i = \deg x_i$ for $1 \leq i \leq s$ and let $r = \max\{n_1, \cdots, n_s\}$, we prove that $M_n = \mathfrak{a}M_{n-1}$ for $n \geq r+1$. From definition $M_n \supset \mathfrak{a}M_{n-1}$. For the converse, we have $M_n \subset \sum \mathfrak{a}^{n-n_i} M_{n_i} = \sum \mathfrak{a} \cdot \mathfrak{a}^{n-n_i-1} M_{n_i} \subset \sum \mathfrak{a}M_{n-1} = \mathfrak{a}M_{n-1}$. We finish the proof. □

Theorem 3.2 (Artin–Rees Lemma)**.** Let A be a noetherian, $\mathfrak{a} \subset A$ be an ideal, M finitely generated A-module. Let $\{M_n\}$ be a stable filtration. Let N be a A-submodule of M, then the induced filtration $\{M_n \cap N\}$ is a stable $\mathfrak{a}$-filtration. In particular, the topology on N is induced from the $\mathfrak{a}$-adic topology on M is equivalent to the $\mathfrak{a}$-adic topology on N.

Proof. $\{M_n \cap N\}$ is an $\mathfrak{a}$-filtration: $\mathfrak{a}(M_n \cap N) \subset \mathfrak{a}M_n \cap \mathfrak{a}N \subset M_{n+1} \cap N$. Let $N^* = \bigoplus_{n=0}^{\infty}(M_n \cap N)$. It is an A^*-submodule of M^*. Since $\{M_n\}$ is a stable $\mathfrak{a}$-filtration, M^* is a finitely generated A^*-module by Lemma 3.4. As A^* is noetherian, N^* is finitely generated A^*-module. By Lemma 3.4, $\{M_n \cap N\}$ is a stable $\mathfrak{a}$-filtration. □

Taking $M_n = \mathfrak{a}^n M$ we obtain what is usually known as the Artin–Rees Lemma:

Corollary 3.6. There exists an integer k such that

$$(\mathfrak{a}^n M) \cap M' = \mathfrak{a}^{n-k} \left((\mathfrak{a}^k M) \cap M' \right)$$

for all $n \geq k$.

Corollary 3.7. Let A be a noetherian ring, $\mathfrak{a} \subset A$ be an ideal, let M be a finitely generated A-module, then for any exact sequence

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$$

we have the exact sequence of $\mathfrak{a}$-adic completion

$$0 \longrightarrow \widehat{M_1} \longrightarrow \widehat{M} \longrightarrow \widehat{M_2} \longrightarrow 0 \ .$$

Proof. If we equip M_1 and M_2 with the topology induced from the $\mathfrak{a}$-adic topology of M, we get an exact sequence

$$0 \longrightarrow \widehat{M_1}' \longrightarrow \widehat{M} \longrightarrow \widehat{M_2}' \longrightarrow 0$$

from the proof of Corollary 3.4. By Artin–Rees Theorem, the induced topology are exactly the $\mathfrak{a}$-adic topology. So the exact sequence is exactly what we want. $\square$

Question: $\widehat{M} = M \otimes_A \widehat{A}$?

For every n we have natural projection $\widehat{A} \to A/\mathfrak{a}^n$, by tensoring M we obtain $\widehat{A} \otimes_A M \to (A/\mathfrak{a}^n) \otimes_A M \cong M/\mathfrak{a}^n M$. Thanks to the universal property of inverse limit, we obtain $\widehat{A} \otimes_A M \to \varprojlim_n M/\mathfrak{a}^n M = \widehat{M}$.

Proposition 3.11. Let A be a commutative united ring, $\mathfrak{a} \subset A$ an ideal. Let M be a finitely generated A-module, then the morphism $\widehat{A} \otimes_A M \to \widehat{M}$ is necessarily surjective. If A is noetherian, it is an isomorphism.

Proof. By assumption, there exists a surjective A-module morphism $\phi \colon F = A^r \twoheadrightarrow M$. It is clear that $\widehat{F} = \varprojlim_n F/\mathfrak{a}^n F = \varprojlim_n (A/\mathfrak{a}^n)^r \cong \left(\varprojlim_n A/\mathfrak{a}^n \right)^r = \widehat{A}^r = F \otimes_A \widehat{A}$ since limit commutes with limit in a category. Let $N = \operatorname{Ker}(\phi)$, we get an exact sequence

$$0 \longrightarrow N \longrightarrow F \longrightarrow M \longrightarrow 0 \ .$$

Tensoring $\widehat{A}$ get exact sequence

$$\begin{tikzcd}
 & N \otimes_A \widehat{A} \arrow[r] \arrow[d] & F \otimes_A \widehat{A} \arrow[r] \arrow[d, "\wr" description, phantom] & M \otimes_A \widehat{A} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \widehat{N} \arrow[r] & \widehat{F} \arrow[r] & \widehat{M} \arrow[r] & 0
\end{tikzcd}$$

where $\widehat{M}$ and $\widehat{N}$ are the completion of M and N with respect to the topology induced from F. The exactness of the bottom row is from Corollary 3.7. Since $\widehat{\phi}\colon \widehat{F} \to \widehat{M}$ is surjective and $\beta\colon F \otimes_A \widehat{A} \to \widehat{F}$ is an isomorphism, $\gamma\colon M \otimes_A \widehat{A} \to \widehat{M}$ must be surjective. If A is noetherian, N is finitely generated. the induced topology in N is the $\mathfrak{a}$-adic topology by Artin–Rees Lemma. The first assertion applies to $\alpha\colon \widehat{A} \otimes_A N \to \widehat{N}$ (note that $N \subset F$ is finitely generated), hence α is surjective. Diagram chasing show that $\mathrm{Ker}(\gamma) = 0$. So γ is an isomorphism. $\square$

Corollary 3.8. If A is noetherian, then $\widehat{A}$ is a flat A-algebra.

Proof. For exact sequence of finitely generated A-module

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0\ ,$$

we get the exact sequence of $\mathfrak{a}$-adic completion

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{M_1} & \longrightarrow & \widehat{M} & \longrightarrow & \widehat{M_2} & \longrightarrow & 0 \\ & & \wr\| & & \wr\| & & \wr\| & & \\ 0 & \longrightarrow & M_1 \otimes_A \widehat{A} & \longrightarrow & M \otimes_A \widehat{A} & \longrightarrow & M \otimes_A \widehat{A} & \longrightarrow & 0 \end{array}$$

Note that flatness can be checked on the inclusion $\mathfrak{a} \hookrightarrow A$ for any ideal $\mathfrak{a}$ of A, and $\mathfrak{a}$ must be finitely generated since A is noetherian. Hence $\widehat{A}$ is a flat A-algebra. $\square$

Question: If A is noetherian, is $\widehat{A}$ noetherian?

Proposition 3.12. Let A be a noetherian ring, $\mathfrak{a} \subset A$ be an ideal, $\widehat{A}$ is the $\mathfrak{a}$-adic completion of A, then

1) $\widehat{\mathfrak{a}} = \widehat{A}\mathfrak{a}$;
2) $\widehat{\mathfrak{a}}^n = \widehat{\mathfrak{a}^n}$;
3) $\widehat{\mathfrak{a}}^n/\widehat{\mathfrak{a}}^{n+1} = \mathfrak{a}^n/\mathfrak{a}^{n+1}$, so $\bigoplus_{n=0}^{\infty} \widehat{\mathfrak{a}}^n/\widehat{\mathfrak{a}}^{n+1} = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1}$;
4) $\mathfrak{a}$ is contained in the Jacobson radical of $\widehat{A}$.

Proof. 1) By assumption, $\mathfrak{a}$ is finitely generated. By Proposition 3.11, $\widehat{A} \otimes_A \mathfrak{a} \to \widehat{\mathfrak{a}}$ is an isomorphism. Its image is $\widehat{A}\mathfrak{a}$. So $\widehat{A} \otimes_A \mathfrak{a} \cong \widehat{A}\mathfrak{a} = \widehat{\mathfrak{a}}$.

2) $(\widehat{\mathfrak{a}})^n = \left(\widehat{A}\mathfrak{a}\right)^n = \widehat{A}\mathfrak{a}^n = \widehat{\mathfrak{a}^n}$ since $\mathfrak{a}^n$ is also an ideal.

3) We have already seen $\widehat{A}/\widehat{\mathfrak{a}^n} = \widehat{A}/\widehat{\mathfrak{a}}^n = A/\mathfrak{a}^n$. So $\widehat{\mathfrak{a}}^n/\widehat{\mathfrak{a}}^{n+1} = \mathrm{Ker}\left(\widehat{A}/\widehat{\mathfrak{a}^{n+1}} \to \widehat{A}/\widehat{\mathfrak{a}^n}\right) = \mathrm{Ker}\left(A/\mathfrak{a}^{n+1} \to A/\mathfrak{a}^n\right) = \mathfrak{a}^n/\mathfrak{a}^{n+1}$.

4) $x \in \mathfrak{a}$ implies that $x^n \in \widehat{\mathfrak{a}}^n$, so $x^n = 0$ in $\widehat{A}/\widehat{\mathfrak{a}}^n$, and so $(1-x)(1+x+\cdots+x^{n-1}) = 1 - x^n = 1$ in $\widehat{A}/\widehat{\mathfrak{a}}^n$. Note that $1+x+\cdots+x^{m-1} \equiv 1+x+\cdots+x^{n-1} \pmod{\widehat{\mathfrak{a}}^n}$, we have $1+x+x^2+\cdots \in \varprojlim_n \widehat{A}/\widehat{\mathfrak{a}}^n = \widehat{A}$ admits inverse $1-x$ in $\widehat{A}$, and so x lies in Jacobson radical of $\widehat{A}$.

$\square$

Corollary 3.9. Let A be a noetherian ring. $\mathfrak{m} \subset A$ a maximal ideal, then $\widehat{\mathfrak{m}}$ is the maximal ideal of $\widehat{A}$.

Proof. By the assumption $\widehat{A}/\widehat{\mathfrak{m}} \cong A/\mathfrak{m}$, get $\widehat{\mathfrak{m}}$ is the maximal ideal of $\widehat{A}$. By 4) in Proposition 3.12, $\widehat{\mathfrak{m}}$ is contained in the Jacobson radical of $\widehat{A}$, so must be the unique maximal ideal of $\widehat{A}$. $\square$

Definition 3.5. 1) Let A be a commutative unitary ring, $\mathfrak{a} \subset A$ be an ideal. Define $\mathrm{Gr}_{\mathfrak{a}}(A) = A/\mathfrak{a} \oplus \mathfrak{a}/\mathfrak{a}^2 \oplus \mathfrak{a}^2/\mathfrak{a}^3 \oplus \cdots$.

2) Let M be an A-module, $\{M_n\}$ is a $\mathfrak{a}$-filtration. Define $\mathrm{Gr}(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$. So we can define a $\mathrm{Gr}_{\mathfrak{a}}(A)$-module structure on $\mathrm{Gr}(M)$.

Geometrically, let $X = \operatorname{Spec} A$ and $Z = V(\mathfrak{a}) \subset X$, the normal cone is defined by $C_{Z/X} = \operatorname{Spec}_Z \left(\bigoplus_{n \geq 0} \mathfrak{a}^n/\mathfrak{a}^{n+1} \right)$. In particular, if x is a closed point, then $C_{x/X} = \operatorname{Spec}\left(\mathrm{Gr}_{\mathfrak{m}_x}(A)\right)$, which is the tangent cone of X at x. Here $\mathfrak{m}_x \subset \mathcal{O}_{X,x}$ is the maximal ideal of the local ring at x.

Proposition 3.13. Let A be a noetherian ring, $\mathfrak{a} \subset A$ an ideal, then

1) $\mathrm{Gr}_{\mathfrak{a}}(A)$ is noetherian;

2) If M is finitely generated A-module, $\{M_n\}$ is a stable $\mathfrak{a}$-filtration, then $\mathrm{Gr}(M)$ is finitely generated $\mathrm{Gr}_{\mathfrak{a}}(A)$-module;

3) $\mathrm{Gr}_{\mathfrak{a}}(A) = \mathrm{Gr}_{\widehat{\mathfrak{a}}}\left(\widehat{A}\right)$.

$$\begin{tikzcd}
(A, \mathfrak{a}) \arrow[dr] & & \left(\widehat{A}, \widehat{\mathfrak{a}}\right) \arrow[dl] \\
& \mathrm{Gr}_{\mathfrak{a}}(A) \arrow[d, equal] & \\
& \mathrm{Gr}_{\widehat{\mathfrak{a}}}\left(\widehat{A}\right) &
\end{tikzcd}$$

Proof. 1) A is noetherian, $\mathfrak{a}$ is finitely generated, let $x_1, \cdots, x_n$ be a set of generators for $\mathfrak{a}$. Consider the morphism $(A/\mathfrak{a})[X_1, \cdots, X_n] \to \mathrm{Gr}_{\mathfrak{a}}(A) = A/\mathfrak{a} \oplus \mathfrak{a}/\mathfrak{a}^2 \oplus \mathfrak{a}^2/\mathfrak{a}^3 \oplus \cdots$ defined by $X_i \mapsto x_i$, it is surjective. So $\mathrm{Gr}_{\mathfrak{a}}(A)$ is a finitely generated $A/\mathfrak{a}$-algebra. Since A is noetherian, so is $A/\mathfrak{a}$. By Hilbert Basis Theorem $\mathrm{Gr}_{\mathfrak{a}}(A)$ is noetherian.

2) By assumption, $\{M_n\}$ is a stable $\mathfrak{a}$-filtration, so there exists $n_0 \in \mathbb{N}$ such that $M_{n+n_0} = \mathfrak{a}^n M_{n_0}$. So $\bigoplus_{n=n_0}^{+\infty} M_n/M_{n+1}$ is generated by M_{n_0}/M_{n_0+1} over $\mathrm{Gr}_{\mathfrak{a}}(A)$. For $n = 0, \cdots, n_0 - 1$, $M_n \subset M$ is finitely generated, so M_n/M_{n+1} is a finitely generated $A/\mathfrak{a}$-module ($M_n/\mathfrak{a}M_n \twoheadrightarrow M_n/M_{n+1}$ and $M_n/\mathfrak{a}M_n$ is generated by image of generators of M_n as A-module). $\mathrm{Gr}(M) = \bigoplus_{n=0}^{n_0-1} M_n/M_{n+1} \oplus \bigoplus_{n \geq n_0} M_n/M_{n+1}$ is finitely generated as $\mathrm{Gr}_{\mathfrak{a}}(A)$-module.

3) Consequence of $\widehat{\mathfrak{a}}^n/\widehat{\mathfrak{a}}^{n+1} = \mathfrak{a}^n/\mathfrak{a}^{n+1}$.

□

Lemma 3.5. Let $\phi\colon A \to B$ be a morphism between filtered abelian groups (i.e., $\phi(A_n) \subset B_n$ for all n), let $\mathrm{Gr}(\phi)\colon \mathrm{Gr}(A) = \bigoplus_{n=1}^{+\infty} A_n/A_{n+1} \to \mathrm{Gr}(B)$ be the induced morphism and $\widehat{\phi}\colon \widehat{A} = \varprojlim_n A/A_n \to \widehat{B}$ be the induced morphisms, then

1) If $\mathrm{Gr}(\phi)$ is injective, then $\widehat{\phi}$ is injective;

2) If $\mathrm{Gr}(\phi)$ is surjective, then $\widehat{\phi}$ is surjective.

Proof. We have the commutative diagram of exact sequence

$$\begin{tikzcd}
0 \arrow[r] & A_n/A_{n+1} \arrow[r] \arrow[d, "\mathrm{Gr}_n(\phi)"] & A/A_{n+1} \arrow[r] \arrow[d, "\phi_{n+1}"] & A/A_n \arrow[r] \arrow[d, "\phi_n"] & 0 \\
0 \arrow[r] & B_n/B_{n+1} \arrow[r] & B/B_{n+1} \arrow[r] & B/B_n \arrow[r] & 0
\end{tikzcd}$$

If $\mathrm{Gr}(\phi)$ is injective, we show by induction ϕ_n are all injective. In general by the Snake Lemma,

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(\mathrm{Gr}_n(\phi)) \arrow[r] & \mathrm{Ker}(\phi_{n+1}) \arrow[r] & \mathrm{Ker}(\phi_n) \arrow[dll, out=0, in=180] & \\
& \mathrm{Coker}(\mathrm{Gr}_n(\phi)) \arrow[r] & \mathrm{Coker}(\phi_{n+1}) \arrow[r] & \mathrm{Coker}(\phi_n) \arrow[r] & 0
\end{tikzcd}$$

If ϕ_n is injective, then ϕ_{n+1} is injective. Since $A_1 = A$ and $B_1 = B$, $\phi_1\colon 0 \to 0$ is injective, so all ϕ_n are injective, i.e., $0 \to A/A_n \to B/B_n$. Since $\varprojlim$ is left exact, we get $0 \to \varprojlim A/A_n \xrightarrow{\widehat{\phi}} \varinjlim B/B_n$.

If $\mathrm{Gr}(\phi)$ is surjective, similarly we can show that $\phi_n\colon A/A_n \to B/B_n \to 0$ is surjective. Moreover, by the above exact sequence we get $\mathrm{Ker}(\phi_{n+1}) \twoheadrightarrow \mathrm{Ker}(\phi_n)$. The projective system $\{\mathrm{Ker}(\phi_n)\}$ satisfies Mittag-Leffler condition. For the exact sequence

$$0 \longrightarrow \{\mathrm{Ker}(\phi_n)\} \longrightarrow \{A/A_n\} \longrightarrow \{B/B_n\} \longrightarrow 0$$

we get the exact sequence

$$0 \longrightarrow \varprojlim_n \operatorname{Ker}(\phi_n) \longrightarrow \widehat{A} \xrightarrow{\widehat{\phi}} \widehat{B} \longrightarrow 0$$

In particular, $\widehat{\phi}$ is surjective. $\square$

Proposition 3.14. Let A be a commutative unitary ring, $\mathfrak{a} \subset A$ ideal. Suppose that $A = \widehat{A}$. Let M be an A-module equipped with an $\mathfrak{a}$-filtration $\{M_n\}$. Suppose that $\bigcap_{n=0}^{+\infty} M_n = \{0\}$. Suppose that $\mathrm{Gr}(M)$ is finitely generated $\mathrm{Gr}_{\mathfrak{a}}(A)$-module, then M is finitely generated as A-module.

Proof. Let ξ_i be a set of generators for $\mathrm{Gr}(M) = \bigoplus_{n=0}^{+\infty} M_n/M_{n+1}$. Without loss of generality, we can suppose that ξ_i are all homogeneous, say of degree n_i. Let x_i be a lift of ξ_i in M_{n_i}. For $n \in \mathbb{N}$, let $A[-n]$ be the graded ring with

$$A[-n]_i = \begin{cases} A & \text{if } i \leq n, \\ \mathfrak{a}^{i-n} & \text{if } i \geq n+1. \end{cases}$$

Then $\mathrm{Gr}(A[-n]) = 0 \oplus \cdots 0 \oplus A/\mathfrak{a} \oplus \mathfrak{a}/\mathfrak{a}^2 \oplus \cdots = \mathrm{Gr}_{\mathfrak{a}}(A)[-n]$. Let $F = \bigoplus_{i\in I} A[-n_i]$ with filtration $F_j = \bigoplus_{i\in I} A[-n_i]_j$. Since $A[-n_i] \cong A$, F is free finitely generated A-module. Define $\phi \colon F \to M$ defined by $1[-n_i] \mapsto x_i$, then ϕ is a morphism of filtered A-module. Indeed, it only suffices to check at every component $A[-n_i]$, if $j \leq n_i$, we have $A[-n_i]_j = A$, it follows that $\phi(A[-n_i]_j) = Ax_i \subset M_{n_i} \subset M_j$; if $j \geq n_i + 1$, $A[-n_i]_j = \mathfrak{a}^{j-n_i}$, which implies that $\phi(A[-n_i]_j) = \mathfrak{a}^{j-n_i}x_i \subset \mathfrak{a}^{j-n_i}M_{n_i} \subset M_j$. Now $\mathrm{Gr}(F) = \bigoplus_{i\in I} \mathrm{Gr}_{\mathfrak{a}}(A)[-n_i]$, by assumption, $\mathrm{Gr}(\phi)$ is surjective. By Lemma 3.5, $\widehat{\phi}$ is surjective, i.e., $\widehat{F} \xrightarrow{\widehat{\phi}} \widehat{M} \to 0$. Note that $\widehat{A[-n]} = \varprojlim_j A/A[-n]_j = \varprojlim_m A/\mathfrak{a}^m = \widehat{A}$ and completion commutes with finite direct sum, we obtain $\widehat{F} \cong F$. Moreover $\bigcap_{n=0}^{|\infty} M_n = \{0\}$ implies that $M \hookrightarrow \widehat{M}$ is injective. Hence we have the commutative diagram

$$\begin{tikzcd} F \arrow[r, "\phi"] \arrow[d, equal] & M \arrow[d, "i"] \\ \widehat{F} \arrow[r, "\widehat{\phi}"] & \widehat{M} \end{tikzcd}$$

Since $\widehat{\phi}$ is surjective, and i is surjective, ϕ must be surjecctive. Hence M, as the quotient module of finitely generated module F, is finitely generated A-module. $\square$

Corollary 3.10. Same hypotheses as in Proposition 3.14, but suppose that $\mathrm{Gr}(M)$ is a noetherian $\mathrm{Gr}_{\mathfrak{a}}(A)$-module, then M is a noetherian A-module.

Proof. Let N be a sub-A-module of M, then $\mathfrak{a}(N \cap M_n) \subset \mathfrak{a}N \cap \mathfrak{a}M_n \subset N \cap M_{n+1}$, the $\mathfrak{a}$-filtration $\{M_n\}$ on M induces the $\mathfrak{a}$-filtration $\{N \cap M_n\}_n$ on M. If $\{M_n\}$ satisfies the Hausdorff condition, so does $\{N \cap M_n\}_n$. By assumption, $\mathrm{Gr}(M)$ is noetherian $\mathrm{Gr}_{\mathfrak{a}}(A)$-module. So $\mathrm{Gr}(N) \subset \mathrm{Gr}(M)$ is finitely generated. By Proposition 3.14 N is finitely generated as A-module. Thus M is noetherian A-module. $\square$

Corollary 3.11. Let A be a noetherian ring, $\mathfrak{a} \subset A$ an ideal, then $\widehat{A}$ is noetherian.

Proof. Need to show that $\widehat{A}$ is noetherian as $\widehat{A}$-module. Note that $\widehat{A}$ is complete and Hausdorff. Since A is noetherian, $\mathrm{Gr}_{\mathfrak{a}}(A)$ is noetherian ring by Proposition 3.13 (a), i.e., $\mathrm{Gr}_{\mathfrak{a}}(A)$ is noetherian as $\mathrm{Gr}_{\mathfrak{a}}(A)$-module. Moreover, Proposition 3.13 gives $\mathrm{Gr}_{\widehat{\mathfrak{a}}}\left(\widehat{A}\right) = \mathrm{Gr}_{\mathfrak{a}}(A)$. By Corollary 3.10, $\widehat{A}$ is noetherian as $\widehat{A}$-module. $\square$

Note that $M \to \widehat{M}$ has kernel $\bigcap_{n=0}^{+\infty} \mathfrak{a}^n M$.

Theorem 3.3 (Krull)**.** Let A be a noetherian ring, $\mathfrak{a} \subset A$ an ideal, M is finitely generated A-module, $\widehat{M} = \varprojlim_n M/\mathfrak{a}^n M$, then $\mathrm{Ker}\left(M \to \widehat{M}\right) = \bigcap_{n=0}^{+\infty} \mathfrak{a}^n M$ is equal to

$$\{m \in M \mid \exists \alpha \in \mathfrak{a} \text{ such that } (1+\alpha)m = 0\}.$$

Proof. Let $N = \bigcap_{n=0}^{+\infty} \mathfrak{a}^n M$, it is a sub-$A$-module of M. Note that $N \cap \mathfrak{a}^n M = N$, the topology induced from M on N is trivial, i.e., $\mathcal{U} = \{\emptyset, N\}$. On the other hand, N has $\mathfrak{a}$-adic topology. By assumption, we can apply Artin–Rees Lemma, to conclude that the two topology are equivalent, i.e., the $\mathfrak{a}$-adic topology on N is trivial. Hence $\mathfrak{a}N \subset N$ open, forces $\mathfrak{a}N = N$. Consider the identity map $N \to N = \mathfrak{a}N$. N is submodule of M, M is finitely generated A-module, A is noetherian, we obtain N is finitely generated A-module. Assume that $x_1, \cdots, x_r$ are generators of N, since $N = \mathfrak{a}N$, for every i we have $x_i = \sum_{j=1}^{r} a_{ij} x_j$, where $a_{ij} \in \mathfrak{a}$. Write

$$\left(\mathrm{Id} - (a_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}\right) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0.$$

By multiplying $\mathrm{adj}\left(\mathrm{Id} - (a_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}\right)$, we have $\det\left(\mathrm{Id} - (a_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}\right) x_i = 0$ for all i. It follows that $\det\left(\mathrm{Id} - (a_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}\right) N = 0$, get the existence of $\alpha \in \mathfrak{a}$ such that $(1+\alpha)N = 0$. Therefore $\bigcap_{n=0}^{+\infty} \mathfrak{a}^n M = N \subset \{m \in M \mid \exists \alpha \in \mathfrak{a} \text{ such that } (1+\alpha)m = 0\}$.

On the other hand, for $m \in M$ such that $(1+\alpha)m = 0$, $\alpha \in \mathfrak{a}$, then $m = (-\alpha)m = (-\alpha)^2 m = \cdots = (-\alpha)^n m$ implies that $m \in \bigcap_{n=0}^{+\infty} \mathfrak{a}^n M$. $\square$

Corollary 3.12. Let A be a noetherian integral domain, $\mathfrak{a} \subset A$ an ideal, $\bigcap_{n=0}^{+\infty} \mathfrak{a}^n = \{0\}$.

Proof. By Krull's Theorem, $\bigcap_{n=0}^{+\infty} \mathfrak{a}^n = \{m \in A \mid \exists \alpha \in \mathfrak{a} \text{ such that } (1+\alpha)m = 0\} = \{0\}$ as A is integral. $\square$

Corollary 3.13. Let A be a noetherian ring, $\mathfrak{a} \subset \mathrm{Jac}(A)$. Let M be a finitely generated A-module, then $\bigcap_{n=0}^{+\infty} \mathfrak{a}^n M = \{0\}$.

Proof. By Krull's Theorem, $\bigcap_{n=0}^{+\infty} \mathfrak{a}^n M = \{x \in M \mid \exists \alpha \in \mathfrak{a} \text{ such that } (1+\alpha)x = 0\}$. Since $\mathfrak{a} \subset \mathrm{Jac}(A)$, $1 + \alpha \in A^\times$, so $(1+\alpha)x = 0$ implies that $x = 0$. $\square$

Consequently, let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated A-module, then $\bigcap_{n=0}^{+\infty} \mathfrak{m}^n M = \{0\}$.

4 Localization of Dedekind ring

Let $K/\mathbb{Q}$ be finite extension, let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K, then $\mathcal{O}_K$ is a Dedekind ring, i.e., it is integrally closed of Krull dimension 1. Let $\mathfrak{p}$ be a non-zero prime ideal, let $\mathcal{O}_{K\mathfrak{p}}$ be its localization at $\mathfrak{p}$.

Proposition 4.1. Let A be a Dedekind ring, $\mathfrak{p} \subset A$ is non-zero prime ideal, then $A_\mathfrak{p}$ is a Dedekind local ring.

Proof. It is known that the prime ideals of $A_\mathfrak{p}$ is in bijection with the prime ideal of A contained in $\mathfrak{p}$. Since A is of Krull dim 1, so does $A_\mathfrak{p}$.

For the second assertion, we can show that $S^{-1}A$ is integrally closed for any multiplicative subset S. Let $x \in \mathrm{Frac}(A)$. Let $x \in \mathrm{Frac}(A)$ be integral over $S^{-1}A$, then it satisfies $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, $a_1, \cdots, a_n \in S^{-1}A$. Take $c \in S$ such that $ca_1, \cdots, ca_n \in A$. Multiply the equation by c^n, get $(cx)^n + a_1 c (cx)^{n-1} + a_2 c^2 (cx)^{n-2} + \cdots + a_n c c^{n-1} = 0$, which implies that cx is integral over A, so $cx \in A$, $x \in S^{-1}A$. $\square$

Then we conclude

Proposition 4.2. Let $K/\mathbb{Q}$ be finite extension, let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K, then $\mathcal{O}_{K\mathfrak{p}}$ is a noetherian integral domain, and it is integrally closed of Krull dimension 1.

Theorem 4.1. Let A be a noetherian integral domain, suppose that A has unique non-zero prime ideal, then A is integral closed iff A is a PID.

Corollary 4.1. Let $K/\mathbb{Q}$ be a finite extension, $\mathfrak{p} \subset \mathcal{O}_K$ a non-zero prime ideal, then $\mathcal{O}_{K\mathfrak{p}}$ is PID.

Definition 4.1. A principal ideal domain with unique non-zero prime ideal is called a **discrete valuation ring**.

Let A be a PID with unique non-zero prime ideal $\mathfrak{m}$, then $\mathfrak{m}$ is also maximal. Then $A \backslash \mathfrak{m} = A^{\times}$. Let $\mathfrak{m} = (\pi)$, consider the filtration $A \supset \mathfrak{m} = (\pi) \supset \mathfrak{m} = (\pi^2) \supset \cdots$. Since A is noetherian local ring, from Corollary 3.13 (taking $M = A$), $\bigcap_{n=0}^{+\infty} \mathfrak{m}^n = \{0\}$. For any $x \in A \setminus \{0\}$, there exists n such that $x \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. Thus $x = \pi^n u$, $u \in A \setminus \mathfrak{m}$. We can define $\mathrm{val}\colon A \to \mathbb{N} \cup \{\infty\}$ by $x = \pi^n u \mapsto n$. It satisfies

1) $\mathrm{val}(xy) = \mathrm{val}(x) + \mathrm{val}(y)$;

2) $\mathrm{val}(x+y) \geq \min\{\mathrm{val}(x), \mathrm{val}(y)\}$;

3) $\mathrm{val}(x) = \infty$ iff $x = 0$.

In fact, val can be extended to $K = \mathrm{Frac}(A) \to \mathbb{Z} \cup \{\infty\}$, $x = a/b = \pi^n u \mapsto n$, here $n \in \mathbb{Z}$ and $u \in A \setminus \mathfrak{m}$. It also satisfy the above three properties.

Definition 4.2. Let K be a field. Suppose that there exists $\mathrm{val}\colon K \to \mathbb{Z}$ satisfies 1), 2), 3), we call K a discrete valuation field, and val is a discrete valuation.

Proposition 4.3. Let A be a noetherian integral domain, it is a DVR iff there exists a discrete valuation $\mathrm{val}\colon K = \mathrm{Frac}(A) \to \mathbb{Z} \cup \{\infty\}$ such that $A = \{x \in K \mid \mathrm{val}(x) \geq 0\}$.

Example 4.1. Let $A = \mathbb{C}[[X,Y]]$ and $\mathfrak{m} = (X,Y)$. Consider the descending chain $A \supsetneq \mathfrak{m} \supsetneq \mathfrak{m}^2 \supsetneq \cdots$. Given $0 \neq f = \sum_{i,j \geq 0} a_{ij} X^i Y^j \in \mathbb{C}[[X,Y]]$, the set $\{i+j \mid a_{ij} \neq 0\}$ is not empty, let d be the minimal element of this set. Hence $f \in \mathfrak{m}^d \setminus \mathfrak{m}^{d+1}$, we have $\bigcap_{n=1}^{+\infty} \mathfrak{m}^n = \{0\}$. Thus for arbitrary $f \in A \setminus \{0\}$, let $\mathrm{val}(f) = \min\{i+j \mid a_{ij} \neq 0\}$. One can verify that val satisfies 1), 2), 3), but A is not a DVR. Indeed, (X,Y) is not principal ideal. Extend val to $\mathrm{val}\colon \mathbb{C}((x,y)) \to \mathbb{Z} \cup \{\infty\}$ as before, calculate $R = \{x \in \mathbb{C}((x,y)) \mid \mathrm{val}(x) \geq 0\}$. Choose $X/Y \in K$, we have $\mathrm{val}(X,Y) = 1 - 1 = 0$, but $X/Y \notin A = \mathbb{C}[[X,Y]]$. This implies that $A \subsetneq R$.

Proof of Theorem. We have show that PID must be integrally closed, it remains to prove the converse.

Let $\mathfrak{m}$ be the maximal ideal. For $x \in \mathfrak{m}$, $x \neq 0$, consider $A/(x)$. For $a \in A$, let $\overline{a}$ be its image in $A/(x)$, let $\mathrm{Ann}(\overline{a}) = \{b \in A \mid b\overline{a} = 0 \text{ in } A/(x)\} = \{b \in A \mid ba \in (x)\} = \{b \in A \mid x \mid ab\}$. It is an ideal of A, and it contains (x). Let $a_0 \in A$ such that $\mathfrak{q} = \mathrm{Ann}(\overline{a_0})$ is maximal under the inclusion relation.

Verify that $\mathfrak{q}$ is a prime ideal, then $\mathfrak{q} = \mathfrak{m}$. Suppose that there exists $b_1, b_2 \in A$ such that $b_1 b_2 \in \mathfrak{q}$ but $b_1 \notin \mathfrak{q}$, $b_2 \notin \mathfrak{q}$. Then $b_1 b_2 \overline{a_0} = 0$ implies that $b_2 \in \mathrm{Ann}\,(b_1 \overline{a_0})$. On the other hand for arbitrary $c \in \mathfrak{q}$, we have $c\overline{a_0} = 0$, so $c\,(b_1\overline{a_0}) = 0$. It follows that $\mathfrak{q} \subset \mathrm{Ann}\,(b_1\overline{a_0})$. So $\mathfrak{q} + (b_2) \subset \mathrm{Ann}\,(b_1\overline{a_0})$, contradiction to the maximality of $\mathfrak{q}$. That is, $\mathfrak{q}$ is a prime ideal. Moreover A has only one nonzero prime ideal, $\mathfrak{q} = \mathfrak{m}$.

Let $\pi = x/a_0$, if $b \in \mathfrak{q} = \mathrm{Ann}\,(\overline{a_0})$, there exists $c \in A$ such that $ba_0 = xc$, so $b = \pi c$. That is $b/\pi = c \in A$, $\pi^{-1}\mathfrak{q} \subset A$. We claim that $\pi^{-1}\mathfrak{q} = A$. Suppose not, then $\pi^{-1}\mathfrak{q} \subset \mathfrak{q}$ since A is local ring with maximal ideal $\mathfrak{m} = \mathfrak{q}$. From A is noetherian, $\mathfrak{q}$ is finitely generated A-module, π^{-1} is integral over A by a technic with Hamilton–Cayley Theorem. (More precisely, if M is finitely generated A-module, and $u \in \mathrm{Frac}(A)$ satisfies $uM \subset M$, then u is integral over A.) By assumption, A is integrally closed, so $\pi^{-1} \in A$, i.e., $a_0/x \in A$, $x \mid a_0$. But then $\mathrm{Ann}(\overline{a_0}) = \{b \in A \mid x \mid a_0 b\} = A$, contradiction to $\mathrm{Ann}(\overline{a_0}) = \mathfrak{q} \subsetneq A$. Therefore, $\pi^{-1}\mathfrak{q} = A$. We claim that $\mathfrak{q} = (\pi)$. For arbitrary $b \in \mathfrak{q}$, since $\pi^{-1}\mathfrak{q} \subset A$, $b = \pi \cdot (b/\pi) \in (\pi)$, so $\mathfrak{q} \subset (\pi)$. From $1 \in \pi^{-1}\mathfrak{q} = A$, there exists $q \in \mathfrak{q}$ such that $q = \pi$, so $(\pi) \subset \mathfrak{q}$. By Corollary 3.13 (taking $M = A$), $\bigcap_{n=0}^{+\infty} \mathfrak{m}^n = \{0\}$. Therefore, $x = \pi^n u$, where $u \in A \setminus \mathfrak{m} = A^\times$. For $I \subset A$, suppose that $I = (x_1, \cdots, x_r)$, let $x = \pi^{n_i} u_i$, $n_i \in \mathbb{N}$ and $u_i \in A^\times$. Let $n = \min\{n_1, \cdots, n_r\}$, then $I = (\pi^n)$, i.e., A is PID. $\square$

Corollary 4.2. Let A be a Dedekind ring, then $A_\mathfrak{p}$ is a PID (DVR) for any $\mathfrak{p} \subset A$ prime non-zero.

Definition 4.3. Let A be a noetherian integral domain of Krull dimension 1, let $\mathfrak{m}$ be a maximal ideal of A. A is said to be **regular** at $\mathfrak{m}$ if $\mathfrak{m}/\mathfrak{m}^2$ is of dimension 1 as $k = A/\mathfrak{m}$-vector space.

Why this definition? Let $C \subset \mathbb{C}^2$ be an algebraic curve defined by $f(x,y) = 0$, where $f(x,y)$ irreducible, let A be the coordinate ring on C, then $A = \mathbb{C}[x,y]/(f(x,y))$. By Hilbert's Nullstellensatz, all the maximal ideals of A are of the form $\mathfrak{m}_P = \{\varphi(x,y) \in A \mid \varphi(P) = 0\}$ where $P \in C$. By Taylor expansion, the cotangent space of C at P is $\mathfrak{m}_P/\mathfrak{m}_P^2$, the tangent space of C at P is $\left(\mathfrak{m}_P/\mathfrak{m}_P^2\right)^\vee$. Hence C is regular at P iff $\dim_\mathbb{C}\left(\mathfrak{m}_P/\mathfrak{m}_P^2\right) = 1$.

Proposition 4.4. Let A be a noetherian integral domain of Krull dimension 1, let $\mathfrak{m} \subset A$ be the maximal ideal, then A is regular at $\mathfrak{m}$ iff $A_\mathfrak{m}$ is PID iff $A_\mathfrak{m}$ is integrally closed.

Proof. First we prove: $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{m}A_\mathfrak{m}/\mathfrak{m}^2 A_\mathfrak{m}$ as $k = A/\mathfrak{m} = A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$-vector space. Indeed, note that we have short exact sequence

$$0 \longrightarrow \mathfrak{m}^2 \longrightarrow \mathfrak{m} \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow 0\ ,$$

by the exactness of localization we obtain

$$0 \longrightarrow \left(\mathfrak{m}^2\right)_{\mathfrak{m}} \longrightarrow \mathfrak{m}_{\mathfrak{m}} \longrightarrow \mathfrak{m}_{\mathfrak{m}}/\left(\mathfrak{m}^2\right)_{\mathfrak{m}} \longrightarrow 0\ ,$$

which implies that $(\mathfrak{m}/\mathfrak{m}^2)_{\mathfrak{m}} \cong \mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}}$. On the other hand we have $\mathfrak{m} \cdot \left(\mathfrak{m}/\mathfrak{m}^2\right) = 0$, for arbitrary $s \notin \mathfrak{m}$, its image in $k = A/\mathfrak{m}$ is invertible, so $\mathfrak{m}/\mathfrak{m}^2 \cong (\mathfrak{m}/\mathfrak{m}^2)_{\mathfrak{m}}$.

If $A_{\mathfrak{m}}$ is PID, let $\mathfrak{m}A_{\mathfrak{m}} = (\pi)$, then $\mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}} = (\pi)/(\pi^2)$ is generated by $\overline{\pi}$ over $k = A/\mathfrak{m}$. So $\dim_k\left(\mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}}\right) \leq 1$. Since $\pi \notin \mathfrak{m}^2A_{\mathfrak{m}}$, $\overline{\pi} \neq 0$, $\dim_k\left(\mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}}\right) = 1$. So A is regular at $\mathfrak{m}$.

Conversely, if A is regular at $\mathfrak{m}$, then $\mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}}$ is 1-dimensional as $A/\mathfrak{m}$-module. Since $A_{\mathfrak{m}}$ is a local ring, by Nakayama's Lemma, $\mathfrak{m}A_{\mathfrak{m}} = (\pi)$ for some $\pi \in \mathfrak{m}A_{\mathfrak{m}}$. Let $I \subset A_{\mathfrak{m}}$ be nonzero ideal. Consider $S = \{r \geq 0 \mid I \subset \mathfrak{m}^rA_{\mathfrak{m}} = (\pi^r)\}$. Since $I \subset A_{\mathfrak{m}} = \mathfrak{m}^0A_{\mathfrak{m}}$, S is not empty. $A_{\mathfrak{m}}$ is noetherian local ring, by Corollary 3.13, $\bigcap_{r\geq 0}\mathfrak{m}^rA_{\mathfrak{m}} = \{0\}$, so S admits an upper bound. Let t be the maximal element, we have $I \subset (\pi^t)$ but $I \not\subset (\pi^{t+1})$. Choose $x \in I \setminus (\pi^{t+1})$. However, $x \in I \subset (\pi^t)$, one can write $x = \pi^tu$ with $u \in A_{\mathfrak{m}}$. Since $u \notin (\pi)$, it is a unit. Hence $\pi^t = xu^{-1} \in I$, $(\pi^t) \subset I \subset (\pi^t)$, that is, $I = (\pi^t)$.

Clearly PID is UFD, hence integrally closed. From Theorem 4.1, noetherian domain with dimension 1 is integrally closed iff it is DVR. From DVR is PID, $A_{\mathfrak{m}}$ is PID iff it is integrally closed. □

Theorem 4.2. Let A be a noetherian integral domain, then A is a Dedekind ring iff $A_{\mathfrak{p}}$ is DVR at any non-zero prime ideal $\mathfrak{p} \subset A$.

5 Unique factorization theorem

Let A be a Dedekind domain.

Definition 5.1. 1) A fractional ideal of A is a finitely generated A-submodule of $K = \mathrm{Frac}(A)$.

2) Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of A, we define $\mathfrak{a} \cdot \mathfrak{b} = \{\text{finite sum of } a_ib_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$. It is a fractional ideal.

Proposition 5.1. The nonzero fractional ideals of A form a group under the above product, denoted I_K.

Corollary 5.1. Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of A. Suppose that $\mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$ for all $\mathfrak{p} \subset A$ prime, then $\mathfrak{a} = \mathfrak{b}$.

Proof. Let $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$, then $\mathfrak{c}_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}^{-1} = A_\mathfrak{p}$ implies that $\mathfrak{c} \subset \bigcap_\mathfrak{p} \mathfrak{c}_\mathfrak{p} = \bigcap_\mathfrak{p} A_\mathfrak{p} = A$ (note that A is integral domain). Thus $\mathfrak{c}_\mathfrak{p} = A_\mathfrak{p}$ for all $\mathfrak{p}$. Therefore $\mathfrak{c}$ is not contained in any maximal ideal of A. More precisely, if $\mathfrak{c} \subset \mathfrak{m}$, then $\mathfrak{c}_\mathfrak{m} = A_\mathfrak{m} \subset \mathfrak{m}A_\mathfrak{m}$, a contradiction. So $\mathfrak{c} = A$ and $\mathfrak{a} = \mathfrak{b}$. ☐

Proposition 5.2. Let $x \in K \setminus \{0\}$, then there exists only finitely many prime ideal $\mathfrak{p} \subset A$ such that $\mathrm{val}_\mathfrak{p}(x) \neq 0$.

Proof. Write $x \in K^\times$ as $x = a/b$ where $a, b \in A \setminus \{0\}$. Then $\{\mathfrak{p} \mid \mathrm{val}_\mathfrak{p}(x) \neq 0\} \subset \{\mathfrak{p} \mid \mathrm{val}_\mathfrak{p}(a) \neq 0\} \cup \{\mathfrak{p} \mid \mathrm{val}_\mathfrak{p}(b) \neq 0\}$. Only need to prove for $x \in A \setminus \{0\}$. Suppose that there are infinitely many prime ideals $\mathfrak{p}_n \subset A$, $n \in \mathbb{N}$ such that $\mathrm{val}_{\mathfrak{p}_n}(x) \neq 0$, then $\mathrm{val}_{\mathfrak{p}_n}(x) \geq 1$ implies that $x \in \mathfrak{p}_n$ for all $n \in \mathbb{N}$. So there exists descending chain

$$\mathfrak{p}_1 \supsetneq \mathfrak{p}_1 \cap \mathfrak{p}_2 \supsetneq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \supsetneq \cdots \supset (x).$$

Indeed, we want to show $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n \supsetneq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n \cap \mathfrak{p}_{n+1}$. since A is Dedekind domain, every nonzero prime ideal is maximal, so $\mathfrak{p}_i \not\subset \mathfrak{p}_{n+1}$. For every $i = 1, \cdots, n$ choose a_i such that $a_i \in \mathfrak{p}_i$ and $a_i \notin \mathfrak{p}_{n+1}$. Then $a_1 \cdots a_n \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ but $a_1 \cdots a_n \notin \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n \cap \mathfrak{p}_{n+1}$. Take inverse, we get

$$\mathfrak{p}_1^{-1} \subsetneq (\mathfrak{p}_1 \cap \mathfrak{p}_2)^{-1} \subsetneq (\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3)^{-1} \subsetneq \cdots \subsetneq (x^{-1}),$$

contradiction to the assumption that A is noetherian, ☐

Theorem 5.1. Let A be a Dedekind ring, then any fractional ideal can be factorized uniquely into product of prime ideals and their inverse.

Proof. Let $\mathfrak{a}$ be nonzero fractional ideal, there exists $d \in A \setminus \{0\}$ such that $d\mathfrak{a} \subset A$, it follows that $\mathfrak{a} = d^{-1}(d\mathfrak{a})$ where $d\mathfrak{a}$ is nonzero ideal of A. Note that $(d)^{-1}$ is the inverse of principal ideal (d), it is enough to prove the Theorem for $\mathfrak{a} \subset A$. Since A is noetherian, $\mathfrak{a}$ is generated by finitely many elements. If $\mathfrak{a}_\mathfrak{p} \neq A_\mathfrak{p}$ holds for some prime ideal $\mathfrak{p}$, we have $\mathfrak{a} \subset \mathfrak{p}$. In particular, if $x \in \mathfrak{a}$, then $x \in \mathfrak{p}$. However, for $x \in A \setminus \{0\}$, Proposition 5.2 says that there are only finitely many nonzero prime ideals $\mathfrak{p}$ satisfy $\mathfrak{p} \ni x$, so there are only finitely many nonzero prime ideals $\mathfrak{p}$ satisfy $\mathfrak{a}_\mathfrak{p} \neq A_\mathfrak{p}$, denoted as $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$. Let $\mathfrak{a} \subset A$ be nonzero ideal, since $A_{\mathfrak{p}_i}$ is DVR, there exists n_i such that $\mathfrak{a}_{\mathfrak{p}_i} = \mathfrak{p}_i^{n_i} A_{\mathfrak{p}_i}$. Define $\mathfrak{b} = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$, then $\mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$ holds for all prime ideals $\mathfrak{p}$. From Corollary 5.1 $\mathfrak{a} = \mathfrak{b}$.

For the uniqueness, assume that $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}} = \prod_\mathfrak{p} \mathfrak{p}^{m_\mathfrak{p}}$. For arbitrary nonzero prime ideal $\mathfrak{q}$, we have $\mathfrak{a}_\mathfrak{q} = \mathfrak{q}^{n_\mathfrak{q}} A_\mathfrak{q} = \mathfrak{q}^{m_\mathfrak{q}} A_\mathfrak{q}$. Since $A_\mathfrak{q}$ is DVR, $n_\mathfrak{q} = m_\mathfrak{q}$, which yields the uniqueness. $\square$

Definition 5.2. Let $P_K \subset I_K$ be the subgroup generated by (x), $x \in K^\times$. We call $\mathrm{Cl}_K = I_K/P_K$ the class group of K (or $\mathcal{O}_K$).

If $\mathrm{Cl}_K = \{e\}$, for arbitrary fractional ideal $\mathfrak{a}$, there exists $x \in K^\times$ such that $\mathfrak{a} = (x)$. That is, every fractional ideal is principal fractional ideal. In particular, every nonzero ideal $\mathfrak{a} \subset A$ is principal ideal, A is PID.

Theorem 5.2. Let K be a finite extension of $\mathbb{Q}$, then Cl_K, the class group of $\mathcal{O}_K$, is finite.

Lemma 5.1 (Chinese Remainder Theorem)**.** Let A be a Dedekind ring, $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be distinct non-zero prime ideals, $n_1, \cdots, n_r \in \mathbb{N}$, then there exists isomorphism

$$A/\prod_{i=1}^r \mathfrak{p}_i^{n_i} = \bigoplus_{i=1}^r A/\mathfrak{p}_i^{n_i}.$$

Proof. Consider the morphism of rings $A \xrightarrow{\phi} \prod_{i=1}^r A/\mathfrak{p}_i^{n_i}$ Verify that it is surjective by induction on r. $r = 1$ is obvious. In general, it is enough to show $A \xrightarrow{\phi'} A/\mathfrak{p}_1^{n_1} \times A/\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$ is surjective. Notice that $\mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r} = A$, we can find $x \in \mathfrak{p}_1^{n_1}$ and $y \in \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$ such that $x + y = 1$. This implies that $x \equiv 0 \pmod{\mathfrak{p}_1^{n_1}}$, $x \equiv 1 \pmod{\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}}$ and $y \equiv 1 \pmod{\mathfrak{p}_1^{n_1}}$, $y \equiv 0 \pmod{\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}}$. For any $a, b \in A$, to find $z \in A$ such that $z \equiv a \pmod{\mathfrak{p}_1^{n_1}}$, $z \equiv b \pmod{\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}}$. One can take $z = ay + bx$ to solve the equation. Clearly $\mathrm{Ker}(\phi) = \bigcap_{i=1}^r \mathfrak{p}_i^{n_i} = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$, we conclude the isomorphism. $\square$

Proposition 5.3. Let A be a Dedekind ring, $K = \mathrm{Frac}(A)$. Suppose that A has only finitely many nonzero prime ideals, then $\mathrm{Cl}_K = \{e\}$, i.e., A is a PID.

Proof. By Theorem 5.1, it is enough to show the prime ideals are principal. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be all the non-zero prime ideals. Since $A_{\mathfrak{p}_i}$ is DVR, $\mathfrak{p}_i A_{\mathfrak{p}_i} \supsetneq \mathfrak{p}_i^2 A_{\mathfrak{p}_i}$, which implies that $\mathfrak{p}_i \neq \mathfrak{p}_i^2$. Take $\pi_i \in A$ such that $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. By the Lemma 5.1 we can find $x_i \in A$ satisfying $x_i \equiv \pi_i \pmod{\mathfrak{p}_i^2}$ and $x_i \equiv 1 \pmod{\mathfrak{p}_j}$, $\forall j \in \{1, \cdots, r\} \setminus \{i\}$. So $\mathrm{val}_{\mathfrak{p}_i}(x_i) = 1$ and $\mathrm{val}_{\mathfrak{p}_j}(x_i) = 0$. Thus $(x_i) = \prod_{j=1}^r \mathfrak{p}_j^{v_{\mathfrak{p}_j}(x_i)} = \mathfrak{p}_i$. $\square$

6 Behaves of prime ideal under field extension

Let A be a Dedekind ring with $\mathrm{Frac}(A) = K$. Let L be a finite separable extension of K, B is the integral closure of A in L. For $\mathfrak{p} \subset A$ non-zero prime ideal, $\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$. Recall that the proof of Theorem 5.1 implies that $\mathfrak{P} \cap A = \mathfrak{p}$.

Definition 6.1. 1) $e_{\mathfrak{P}}$ is called the **ramification index** of L/K at $\mathfrak{P}$.

2) Since $\mathfrak{P} \cap A = \mathfrak{p}$, we have natural inclusion $A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}$. The residue field $k_{\mathfrak{P}} = B/\mathfrak{P}$ is an extension of $k_{\mathfrak{p}} = A/\mathfrak{p}$. The degree $f_{\mathfrak{P}} = [k_{\mathfrak{P}} : k_{\mathfrak{p}}]$ is called the **residue degree** of $\mathfrak{P}$.

3) If $e_{\mathfrak{P}} = 1$ and $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is separable we say that L/K is **unramified** at $\mathfrak{P}$. Otherwise call it **ramified**.

4) If $e_{\mathfrak{P}} = 1$ and $f_{\mathfrak{P}} = 1$ for all $\mathfrak{P}$ over $\mathfrak{p}$, we say that L/K is **split** at $\mathfrak{p}$.

5) If $\mathfrak{p} = \mathfrak{P}^{e_{\mathfrak{P}}}$ and $f_{\mathfrak{P}} = 1$, we say that L/K is **totally ramified** at $\mathfrak{p}$.

Proposition 6.1. Let $K \subset M \subset L$ be a tower of finite separable extension, let C be the integral closure of A in M, B be the integral closure A in L. For nonzero prime ideal $\mathfrak{P} \subset B$, let $\mathfrak{Q} = \mathfrak{P} \cap C$, then $e_{L/K,\mathfrak{P}} = e_{M/K,\mathfrak{Q}} \cdot e_{L/M,\mathfrak{P}}$ and $f_{L/K,\mathfrak{P}} = f_{M/K,\mathfrak{Q}} \cdot f_{L/M,\mathfrak{P}}$.

$$\begin{array}{ccccc} \mathfrak{P} & \subset & B & \subset & L \\ \Big| & & \Big| & & \Big| \\ \mathfrak{Q} & \subset & C & \subset & M \\ \Big| & & \Big| & & \Big| \\ \mathfrak{p} & \subset & A & \subset & K \end{array}$$

Proof. In a Dedekind ring, if $\mathfrak{p}B = \prod_{\mathfrak{P}'|\mathfrak{p}} \mathfrak{P}'^{e_{\mathfrak{P}'}}$, by localizing we obtain $\mathfrak{p}B_{\mathfrak{P}} = \mathfrak{P}^{e_{L/K,\mathfrak{P}}} B_{\mathfrak{P}}$. The ramification index is local. Since $\mathfrak{p}C_{\mathfrak{Q}} = \mathfrak{Q}^{e_{M/K,\mathfrak{Q}}} C_{\mathfrak{Q}}$, we have $\mathfrak{p}B_{\mathfrak{P}} = (\mathfrak{p}C_{\mathfrak{Q}})B_{\mathfrak{P}} = (\mathfrak{Q}^{e_{M/K,\mathfrak{Q}}} C_{\mathfrak{Q}})\, B_{\mathfrak{P}} = (\mathfrak{Q}B_{\mathfrak{P}})^{e_{M/K,\mathfrak{Q}}}$. From $\mathfrak{Q}B_{\mathfrak{P}} = \mathfrak{P}^{e_{L/M,\mathfrak{P}}} B_{\mathfrak{P}}$, we obtain $\mathfrak{p}B_{\mathfrak{P}} = (\mathfrak{P}^{e_{L/M,\mathfrak{P}}} B_{\mathfrak{P}})^{e_{M/K,\mathfrak{Q}}}$. That is, $\mathfrak{p}B_{\mathfrak{P}} = \mathfrak{P}^{e_{M/K,\mathfrak{Q}} e_{L/M,\mathfrak{P}}} B_{\mathfrak{P}}$. On the other hand $\mathfrak{p}B_{\mathfrak{P}} = \mathfrak{P}^{e_{L/K},\mathfrak{P}} B_{\mathfrak{P}}$. Hence $e_{L/K,\mathfrak{P}} = e_{M/K,\mathfrak{Q}} \cdot e_{L/M,\mathfrak{P}}$.

We have inclusion $k_{\mathfrak{p}} \subset k_{\mathfrak{Q}} \subset k_{\mathfrak{P}}$, so $f_{L/K,\mathfrak{P}} = f_{M/K,\mathfrak{Q}} \cdot f_{L/M,\mathfrak{P}}$. □

Proposition 6.2. B is finitely generated A-module and we have $B \otimes_A K = L$. In fact, B is a locally free A-module of rank $[L : K]$.

Proof. The first assertion has been shown.

For the second assertion, need to show that $B_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank $[L : K]$ for arbitrary $\mathfrak{p} \subset A$ prime non-zero. Since A is a Dedekind ring, $A_{\mathfrak{p}}$ is a PID and $B_{\mathfrak{p}} \subset L$ is a torsion-free finitely generated $A_{\mathfrak{p}}$-module. It follows that $B_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of finite rank. Moreover $B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K = (B \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} K \cong B \otimes_A K = L$. On the other hand if $B_{\mathfrak{p}} \cong A_{\mathfrak{p}}^{[L:K]}$, then $B_{\mathfrak{p}} \otimes A_{\mathfrak{p}} K \cong K^{[L:K]}$, which implies that $K^{[L:K]} \cong L$ as K-vector space. Thus $B_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank $[L : K]$. □

Proposition 6.3. For $\mathfrak{p} \subset A$ a non-zero prime ideal. Suppose that $\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$, then

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{p}} \cdot f_{\mathfrak{P}} = [L : K].$$

Proof. By the Chinese Remainder Theorem

$$B/\mathfrak{p}B = \bigoplus_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{c_{\mathfrak{P}}}.$$

Since $B_{\mathfrak{p}}$ is free $A_{\mathfrak{p}}$-module with rank $[L : K]$, we have $B_{\mathfrak{p}} \cong A_{\mathfrak{p}}^{[L:K]}$, it follows that $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \cong (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})^{[L:K]} \cong (A/\mathfrak{p})^{[L:K]}$. Thus $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ is $A/\mathfrak{p}$-vector space with dimension $[L : K]$. Note that $B/\mathfrak{p}B \cong B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$, $B/\mathfrak{p}B$ is $A/\mathfrak{p}$-vector space with dimension $[L : K]$. On the other hand, since B is Dedekind ring, $B_{\mathfrak{P}}$ is DVR, so $\mathfrak{P}B_{\mathfrak{P}} = (\pi)$ where π is a uniformizer. $B_{\mathfrak{P}}$ has filtration $B_{\mathfrak{P}} \supset \mathfrak{P}B_{\mathfrak{P}} \supset \mathfrak{P}^2 B_{\mathfrak{P}} \supset \cdots \supset \mathfrak{P}^{e_{\mathfrak{P}}} B_{\mathfrak{P}}$. Since $\mathfrak{P}^i B_{\mathfrak{P}} = (\pi^i)$, we have isomorphism $B/\mathfrak{P} \cong B_{\mathfrak{P}}/\mathfrak{P}B_{\mathfrak{P}} \cong \mathfrak{P}^i B_{\mathfrak{P}}/\mathfrak{P}^{i-1}B_{\mathfrak{P}}$. From $[B/\mathfrak{P} : A/\mathfrak{p}] = f_{\mathfrak{P}}$, we have $\dim_{A/\mathfrak{p}} (B/\mathfrak{P}^{e_{\mathfrak{P}}}) = \dim_{A/\mathfrak{p}} (B_{\mathfrak{P}}/\mathfrak{P}^{e_{\mathfrak{P}}} B_{\mathfrak{P}}) = \sum_{i=1}^{e_{\mathfrak{P}}} \dim_{A/\mathfrak{p}} \left(\mathfrak{P}^i B_{\mathfrak{P}}/\mathfrak{P}^{i-1}B_{\mathfrak{P}}\right) = \sum_{i=1}^{e_{\mathfrak{P}}} \dim_{A/\mathfrak{p}}(B/\mathfrak{P}) = e_{\mathfrak{P}} f_{\mathfrak{P}}$, then we get

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{p}} \cdot f_{\mathfrak{P}} = [L : K].$$

□

Theorem 6.1 (Dedekind)**.** Suppose that $B = A[\alpha]$, let $f(X) \in A[X]$ be the minimal polynomial of α. For $\mathfrak{p} \subset A$ non-zero prime ideal, let $f(X) \bmod \mathfrak{p} = \prod_{i=1}^r \overline{f_i}(X)^{e_i}$ be the fractorization into irreducible polynomials with leading coefficient 1, here $\overline{f_i}(X) \in (A/\mathfrak{p})[X] = k[X]$. Let $f_i(X) \in A[X]$ be a lifting of $\overline{f_i}(X)$ with leading coefficient 1. Let $\mathfrak{P}_i = \mathfrak{p}B + f_i(\alpha)B$, then $\mathfrak{P}_i$ is maximal and $\mathfrak{p}B = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ and $f_{\mathfrak{P}_i} = \deg\left(\overline{f_i}(X)\right)$.

Proof. By assumption, $B = A[\alpha] = A[X]/(f(X))$, $B/\mathfrak{p}B = (A/\mathfrak{p})[X]/\left(\overline{f}(X)\right) = k_{\mathfrak{p}}[X]/\left(\prod_{i=1}^r \overline{f_i}(X)^{e_i}\right) = \prod_{i=1}^r k_{\mathfrak{p}}[X]/\left(\overline{f_i}(X)\right)^{e_i}$. Calculate,

$$B/\mathfrak{P}_i = B/\left(\mathfrak{p}B + f_i(\alpha)B\right) = (B/\mathfrak{p}B)/\left((\mathfrak{p}B + f_i(\alpha)B)/\mathfrak{p}B\right) = \left((A/\mathfrak{p})[X]/\left(\overline{f}(X)\right)\right)/\left(\overline{f_i}(X)\right) = k_{\mathfrak{p}}[X]/\left(\overline{f_i}(X)\right)$$

is a field since $\overline{f_i}(X)$ is irreducible in $k_{\mathfrak{p}}[X]$. So $\mathfrak{P}_i \subset B$ is a maximal ideal and $f_{\mathfrak{P}_i} = [B/\mathfrak{P} : A/\mathfrak{p}] = [k_{\mathfrak{p}}[X]/\left(\overline{f_i}(X)\right) : k_{\mathfrak{p}}] = \deg\left(\overline{f_i}(X)\right)$. From $\mathfrak{p}B \subset \mathfrak{P}_i$, we have $\mathfrak{p} \subset \mathfrak{P}_i \cap A$. However A is a Dedekind ring, $\mathfrak{p} = \mathfrak{P}_i \cap A$. We have

$$\prod_{i=1}^{r} \mathfrak{P}_i^{e_i} = \prod_{i=1}^{r} (\mathfrak{p}B + f_i(\alpha)B)^{e_i} \subset \mathfrak{p}B + \prod_{i=1}^{r} f_i(\alpha)^{e_i} \cdot B.$$

Let $\overline{\alpha}$ be the image of α in $B/\mathfrak{p}B$. Since $\prod_{i=1}^{r} f_i(\alpha)^{e_i} \bmod \mathfrak{p}B \equiv \prod_{i=1}^{r} \overline{f_i}\left(\overline{\alpha}\right)^{e_i} \equiv f\left(\overline{\alpha}\right) \bmod \mathfrak{p} = 0 \bmod \mathfrak{p}$ (note that in $B/\mathfrak{p}B \cong k_{\mathfrak{p}}[X]/\left(\overline{f}(X)\right)$, $\overline{\alpha}$ is precisely the image of X), $\prod_{i=1}^{r} f_i(\alpha)^{e_i} \cdot B \subset \mathfrak{p}B$, we have surjection $B/\prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \twoheadrightarrow B/\mathfrak{p}B$. Both sides are $k_{\mathfrak{p}}$-vector space. Compare their dimension, $\dim_{k_{\mathfrak{p}}}(B/\mathfrak{p}B) = [L : K] = \deg(f) = \sum_{i=1}^{r} e_i \deg\left(\overline{f_i}\right)$, we have $f_{\mathfrak{P}_i} = \deg\left(\overline{f_i}(X)\right)$. On the other hand, the Chinese Remainder Theorem gives $B/\prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \cong \bigoplus_{i=1}^{r} B/\mathfrak{P}_i^{e_i}$. Thus $\dim_{k_{\mathfrak{p}}}\left(B/\prod_{i=1}^{r} \mathfrak{P}_i^{e_i}\right) = \sum_{i=1}^{r} \dim_{k_{\mathfrak{p}}}(B/\mathfrak{P}_i^{e_i}) = \sum_{i=1}^{r} e_i f_{\mathfrak{P}_i} = \sum_{i=1}^{e_i} \deg\left(\overline{f_i}\right)$. We have isomorphism $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}^{e_i}$. $\square$

Example 6.1. $K = \mathbb{Q}\left(\sqrt{-1}\right)$, $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-1}\right]$. The minimal polynomial of $\sqrt{-1}$ is $f(X) = X^2 + 1$. For p prime, $\overline{f}(X) = X^2 + 1 \bmod p$.

If $p = 2$, $X^2 + 1 \equiv 0 \bmod 2$ has root 1 with multiplicity 2, i.e., $X^2 + 1 \equiv (X+1)^2 \bmod 2$. From Dedekind Theorem $2\mathbb{Z}\left[\sqrt{-1}\right] = \mathfrak{P}^2$, where $\mathfrak{P}_2 = 2\mathcal{O}_K + \left(1+\sqrt{-1}\right)\mathcal{O}_K = \left(1+\sqrt{-1}\right)$. Then $2 = \left(1+\sqrt{-1}\right)^2 = \mathfrak{P}^2$ implies that $K/\mathbb{Q}$ ramified at $\mathfrak{P}$ with $e_{\mathfrak{P}} = 2$. $X^2 + 1 \equiv 0 \bmod p$ has multiple roots iff $\Delta = -4 \equiv 0 \bmod p$, i.e., $p = 2$, so only ramified over 2.

Now consider case $p \neq 2$. If $p \equiv 1 \bmod 4$, then $X^2 + 1 = (X-a)(X+a) \equiv \bmod p$, where $a \in \mathbb{F}_p$ satisfies $a^2 \equiv -1 \bmod p$. So $p\mathbb{Z}\left[\sqrt{-1}\right] = \mathfrak{P}_1\mathfrak{P}_2$. That is $K/\mathbb{Q}$ splits at 2. If $p \equiv 3 \bmod 4$, $X^2 + 1$ is irreducible in $\mathbb{F}_p[X]$, $p\mathbb{Z}\left[\sqrt{-1}\right]$ is a prime ideal.

7 Galois action

Suppose that L/K is a finite Galois extension with Galois group $\mathrm{Gal}(L/K) = G$. For $\mathfrak{P}$ lying over $\mathfrak{p}$, $\sigma(\mathfrak{P})$ remains a prime ideal, $\forall \sigma \in G$ and $\sigma(\mathfrak{P}) \cap A = \sigma(\mathfrak{P} \cap A) = \sigma(\mathfrak{p}) = \mathfrak{p}$. So G acts on the set $\{\mathfrak{P} \subset B \mid \mathfrak{P} \mid \mathfrak{p}\}$.

Proposition 7.1. The action of G on the set of prime ideals on B lying over $\mathfrak{p}$ is transitive. Consequently, all the ramification index $e_{\mathfrak{P}}$ (resp. residue degree $f_{\mathfrak{P}}$) takes the same value $e_{\mathfrak{p}}$ (resp. $f_{\mathfrak{p}}$) and we have $[L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$ where $g_{\mathfrak{p}}$ is the number of prime ideals over $\mathfrak{p}$.

Proof. Suppose that the action is not transitive, then there exists $\mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}$ such that $\mathfrak{P}' \neq \sigma(\mathfrak{P})$ for all $\sigma \in G$. By the Chinese Remainder Theorem we can find $x \in B$ such that $x \in \mathfrak{P}'$ but

$x \notin \sigma(\mathfrak{P})$ for all $\sigma \in G$. (More precisely, one can choose $x \equiv 0 \pmod{\mathfrak{P}'}$ and $x \equiv 1 \pmod{\sigma(\mathfrak{P})}$.) Then $\mathrm{N}_{L/K}(x) = \prod_{\sigma\in G} \sigma(x) \in \mathfrak{P}'$. On the other hand $x \in B$, so x is integral over A, and so $\sigma(x)$ is integral over A since σ fix A. For arbitrary $\tau \in G$, $\tau\left(\mathrm{N}_{L/K}(x)\right) = \prod_{\sigma\in G} \tau\sigma(x) = \prod_{\sigma\in G}\sigma(x) = \mathrm{N}_{L/K}(x)$, which implies that $\mathrm{N}_{L/K}(x) \in K$. Note that A is Dedekind ring, so is integrally closed, $\mathrm{N}_{L/K}(x) \in A$. Hence $\mathrm{N}_{L/K}(x) \in \mathfrak{P}' \cap A = \mathfrak{p} \subset \mathfrak{P}$. As $\mathfrak{P}$ is prime, there must exists $\sigma \in G$ such that $\sigma(x) \in \mathfrak{P}$. Contradiction!

Applying the Galois action to $\mathfrak{p}B = \prod_{i=1}^{g_\mathfrak{p}} \mathfrak{P}_i^{e_i}$ get $e_i = e_j$. If $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$, then σ induces a field isomorphism $B/\mathfrak{P}_i \to B/\mathfrak{P}_j$ defined by $x + \mathfrak{P}_i \mapsto \sigma(x) + \mathfrak{P}_j$. Since σ fixes A, the induced isomorphism fixes $A/\mathfrak{p}$. Thus $f_i = [k_{\mathfrak{P}_i} : k_\mathfrak{p}] = [k_{\mathfrak{P}_j} : k_\mathfrak{p}] = f_j$ for all i, j. So $[L : K] = \sum_{i=1}^{g_\mathfrak{p}} e_i f_i = \sum_{i=1}^{g_\mathfrak{p}} e_\mathfrak{p} f_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$. $\square$

For $\mathfrak{P} \mid \mathfrak{p}$ define $D_\mathfrak{P} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ called the **decomposition group**. Note that $D_\mathfrak{P}$ acts on $k_\mathfrak{P} = B/\mathfrak{P}$ and it keeps $k_\mathfrak{p} = A/\mathfrak{p}$ invariant. We get group homomorphism $D_\mathfrak{P} \to \mathrm{Aut}_{k_\mathfrak{p}}(k_\mathfrak{P})$.

Proposition 7.2. Suppose that $k_\mathfrak{P}$ is separable over $k_\mathfrak{p}$, then it is Galois, and the morphism $D_\mathfrak{P} \to \mathrm{Aut}_{k_\mathfrak{p}}(k_\mathfrak{P})$ is surjective.

Proof. Need to show that $k_\mathfrak{P}/k_\mathfrak{p}$ is normal. Let $x \in B$ and $\overline{x} = x + \mathfrak{P} \in k_\mathfrak{P}$. Consider $f(X) = \prod_{\sigma\in G}(X - \sigma(x))$. The coefficients of $f(X)$ are elementary symmetric polynomials of $\sigma(x)$, so they belongs to $L^G = K$. On the other hand $x \in B$ integral over A, since A is integrally closed, $f(X) \in A[X]$. Mod $\mathfrak{P}$, get $(X - \overline{x}) \prod_{\substack{\sigma\in G \\ \sigma\neq e}} \left(X - \overline{\sigma(x)}\right) \in k_\mathfrak{p}[X]$. That is, $f(X)$ splits into linear factors over the field $k_\mathfrak{P}$. So every $k_\mathfrak{p}$-conjugate of $\overline{x} \in k_\mathfrak{P}$ still lies in $k_\mathfrak{P}$. Therefore $k_\mathfrak{P}/k_\mathfrak{p}$ is normal.

For the second assertion, since $k_\mathfrak{P}/k_\mathfrak{p}$ is finite separable, we can find $\overline{\alpha} \in k_\mathfrak{P}$ such that $k_\mathfrak{P} = k_\mathfrak{p}[\overline{\alpha}]$ thanks to the Primitive Element Theorem. The the Galois action on $k_\mathfrak{P}$ is reflected by its action on $\overline{\alpha}$. To show that $D_\mathfrak{P} \to \mathrm{Aut}_{k_\mathfrak{p}}(k_\mathfrak{P})$ is surjective, need to show that the Galois conjugate of $\overline{\alpha}$ are of the form $\sigma(\overline{\alpha})$, $\sigma \in D_\mathfrak{P}$. Take $\alpha \in B$ such that $\alpha \equiv \overline{\alpha} \pmod{\mathfrak{P}}$ and $\alpha \equiv 0 \pmod{\sigma^{-1}(\mathfrak{P})}$ for all $\sigma \in G \setminus D_\mathfrak{P}$ by the Chinese Remainder Theorem. It is a lifting of $\overline{\alpha}$ and $\sigma(\alpha) \in \mathfrak{P}$ for all $\sigma \in G \setminus D_\mathfrak{P} \iff \overline{\sigma(\alpha)} = 0$ in $k_\mathfrak{P}$ for all $\sigma \in G \setminus D_\mathfrak{P}$. The polynomial $\prod_{\sigma\in G}(X - \sigma(\alpha)) \in A[X]$. Mod $\mathfrak{P}$, get $X^N \prod_{\sigma\in D_\mathfrak{P}} \left(X - \overline{\sigma(\alpha)}\right) \in k_\mathfrak{p}[X]$ where $N = |G| - |D_\mathfrak{P}|$, so $\prod_{\sigma\in D_\mathfrak{P}} \left(X - \overline{\sigma(\alpha)}\right) \in k_\mathfrak{p}[X]$. Now since $k_\mathfrak{P}/k_\mathfrak{p}$ is Galois arbitrary $\tau \in \mathrm{Aut}_{k_\mathfrak{p}}(k_\mathfrak{P})$ will send $\overline{\alpha}$ to some conjugate $\tau(\overline{\alpha})$. So there exist $\sigma \in D_\mathfrak{P}$ such that $\tau(\overline{\alpha}) = \overline{\sigma(\alpha)}$, we obtain $\tau = \sigma$. $\square$

Let $I_\mathfrak{P} = \mathrm{Ker}\left(D_\mathfrak{P} \to \mathrm{Aut}_{k_\mathfrak{p}}(k_\mathfrak{P})\right)$ called the **inertia subgroup**. If $k_\mathfrak{P}/k_\mathfrak{p}$ is Galois, then

$\mathrm{Aut}_{k_\mathfrak{p}}(k_\mathfrak{P}) = \mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p})$, by Proposition 7.2 get the exact sequence

$$1 \longrightarrow I_\mathfrak{P} \longrightarrow D_\mathfrak{P} \longrightarrow \mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p}) \longrightarrow 1 \ .$$

Since G acts on $\mathfrak{P} \subset B \mid \mathfrak{P} \mid \mathfrak{p}\}$ transitively, and $D_\mathfrak{P}$ is the stabilizer of $\mathfrak{P}$, we have $g_\mathfrak{p} = |\operatorname{Orb}(\mathfrak{P})| = [G : D_\mathfrak{P}]$. From $|G| = [L : K]$, we have $D_\mathfrak{P} = [L : K]/g_\mathfrak{p}$. $[L : K] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$ implies that $|D_\mathfrak{P}| = e_\mathfrak{p} f_\mathfrak{p}$. $|\mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p})| = [k_\mathfrak{P} : k_\mathfrak{p}] = f_\mathfrak{p}$. From the short exact sequence get $|I_\mathfrak{P}| = e_\mathfrak{p}$. The order of the inertia group is exactly the ramification index.

For K a number field (finite extension of $\mathbb{Q}$) or finite separable extension of $\mathbb{F}_p(X)$, the residue field $k_\mathfrak{p}$ is a finite field. For case $K/\mathbb{Q}$ finite, choose nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. Then there exists some prime p such that $\mathfrak{p} \cap \mathbb{Z} = (p)$, which induces injection $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$. But $\mathcal{O}_K$ is finitely generated $\mathbb{Z}$-module with rank $[K : \mathbb{Q}]$, then $\mathcal{O}_K/\mathfrak{p}$ is finite dimension $\mathbb{Z}/p\mathbb{Z}$-vector space. That is, $\mathcal{O}_K/\mathfrak{p}$ is a finite field. For case $K/\mathbb{F}_p(X)$ finite separable, let A be the integral closure of $\mathbb{F}_p[X]$ in K, choose nonzero prime ideal $\mathfrak{p} \subset A$. Then there exists some prime p such that $\mathfrak{p} \cap \mathbb{F}_p[X] = (h(X))$ where $h(X) \in \mathbb{F}_p[X]$ is irreducible. $\mathbb{F}_p[X]/(h(X))$ is a finite field. Then $A/\mathfrak{p}$ is finite extension of $\mathbb{F}_p[X]/(h(X))$, so is finite field.

Now let K be a number field or finite separable extension of $\mathbb{F}_p(X)$. Suppose that $k_\mathfrak{p} = \mathbb{F}_q$, since $[k_\mathfrak{P} : k_\mathfrak{p}] = f_\mathfrak{p}$, we have $k_\mathfrak{P} = \mathbb{F}_{q^{f_\mathfrak{p}}}$. $k_\mathfrak{P}/k_\mathfrak{p}$ must be Galois, and $\mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p})$ is generated by the Frobenius $\varphi \colon k_\mathfrak{P} \to k_\mathfrak{P}$ defined by $\alpha \mapsto \alpha^q$. Thanks to Proposition 7.2, let $\mathrm{Fr}_\mathfrak{P}$ be a lifting of φ in $D_\mathfrak{P}$, i.e., $\mathrm{Fr}_\mathfrak{P}(\alpha) \equiv \alpha^q \bmod \mathfrak{P}$, $\forall \alpha \in B$ called it a Frobenius at $\mathfrak{P}$.

$$1 \longrightarrow I_\mathfrak{P} \longrightarrow D_\mathfrak{P} \longrightarrow \mathrm{Gal}_{k_\mathfrak{p}}(k_\mathfrak{P}) \longrightarrow 1$$

$$\mathrm{Fr}_\mathfrak{P} \longmapsto \varphi$$

In case that $e_\mathfrak{p} = 1$, $I_\mathfrak{P} = \{e\}$, we have isomorphism $D_\mathfrak{P} \cong \mathrm{Gal}(k_\mathfrak{P}/k_\mathfrak{p})$, the lifting is unique.

If $e_\mathfrak{p} = 1$, $\mathrm{Fr}_\mathfrak{P} \in D_\mathfrak{P}$ is unique. From Proposition 7.1, for arbitrary $\mathfrak{P}'$ there exists $\tau(\mathfrak{P}) = \mathfrak{P}'$. Now we claim $D_{\mathfrak{P}'} = \tau D_\mathfrak{P} \tau^{-1}$ and $\mathrm{Fr}_{\mathfrak{P}'} = \tau \,\mathrm{Fr}_\mathfrak{P}\, \tau^{-1}$. Indeed, for $\gamma \in G$, $\gamma \in D_{\mathfrak{P}'}$ iff $\gamma(\mathfrak{P}') = \mathfrak{P}'$ iff $\gamma\tau(\mathfrak{P}) = \tau(\mathfrak{P})$ iff $\tau^{-1}\gamma\tau(\mathfrak{P}) = \mathfrak{P}$ iff $\gamma \in \tau D_\mathfrak{P} \tau^{-1}$. Thus $D_{\mathfrak{P}'} = \tau D_\mathfrak{P} \tau^{-1}$. Since $\mathrm{Fr}_\mathfrak{P} \in D_\mathfrak{P}$, we have $\tau \,\mathrm{Fr}_\mathfrak{P}\, \tau^{-1} \in D_{\mathfrak{P}'}$. Given any $x \in B$ and let $y = \tau^{-1}(x)$. From $\mathrm{Fr}_\mathfrak{P}(y) \equiv y^q \pmod{\mathfrak{P}}$, we have $\tau \,\mathrm{Fr}_\mathfrak{P}\, \tau^{-1}(x) = \tau \,\mathrm{Fr}_\mathfrak{P}(y) \equiv \tau(y^q)$ (mod $\tau(\mathfrak{P})$, i.e., $\tau \,\mathrm{Fr}_\mathfrak{P}\, \tau^{-1}(x) \equiv x^q \pmod{\mathfrak{P}'}$. Thanks to the uniqueness of lift, $\mathrm{Fr}_{\mathfrak{P}'} = \tau \,\mathrm{Fr}_\mathfrak{P}\, \tau^{-1}$. The conjugacy class of $\mathrm{Fr}_\mathfrak{P}$ in G depends only on $\mathfrak{p}$.

8 Completion

Let A be a Dedekind ring, $\mathfrak{p} \subset A$ be a nonzero prime ideal, $L/K = \mathrm{Frac}(A)$ finite separable extension. $B \subset L$ be the integral closure of A in L. Suppose that $\mathfrak{p}B = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$. Let $\widehat{A_\mathfrak{p}} = \varprojlim_n A/\mathfrak{p}^n$ be the completion of A with respect to $\mathfrak{p}$. Let $K_\mathfrak{p} = \mathrm{Frac}\left(\widehat{A_\mathfrak{p}}\right)$, then $K_\mathfrak{p}$ is the completion of K with respect to $\mathfrak{p}$. Similarly for $\widehat{B_\mathfrak{P}}$, $L_\mathfrak{P}$. $B_\mathfrak{P} = B \otimes_A A_\mathfrak{p}$ is a finite $A_\mathfrak{p}$-module of rank $[L:K]$. Therefore

$$B \otimes_A \widehat{A_\mathfrak{p}} = B \otimes_A \left(\varprojlim_n A/\mathfrak{p}^n\right) = \varprojlim_n B/\mathfrak{p}^n B = \varprojlim_n B/\prod_{i=1}^r \mathfrak{P}_i^{ne_i} = \varprojlim_n \prod_{i=1}^r B/\mathfrak{P}_i^{ne_i} = \prod_{i=1}^r \varprojlim_n B/\mathfrak{P}_i^{ne_i} = \prod_{i=1}^r \widehat{B_{\mathfrak{P}_i}}.$$

Hence

$$L \otimes_K K_\mathfrak{p} = (B \otimes_A K) \otimes_K K_\mathfrak{p} = B \otimes_A K_\mathfrak{p} = \left(B \otimes_A \widehat{A_\mathfrak{p}}\right) \otimes_{\widehat{A_\mathfrak{p}}} K_\mathfrak{p} = \prod_{i=1}^r \widehat{B_{\mathfrak{P}_i}} \otimes_{\widehat{A_\mathfrak{p}}} K_\mathfrak{p}.$$

Let π (resp. ϖ) be uniformizer of $A_\mathfrak{p}$ (resp. $B_{\mathfrak{P}_i}$). from $\mathfrak{p}B_{\mathfrak{P}_i} = \mathfrak{P}_i^{e_i} B_{\mathfrak{P}_i}$, we have $\pi = u_i \varpi^{e_i}$ for some $u_i \in B_{\mathfrak{P}_i}^\times$. It follows that $\widehat{B_{\mathfrak{P}_i}} \otimes_{\widehat{A_\mathfrak{p}}} K_\mathfrak{p} = \widehat{B_{\mathfrak{P}_i}}[1/\pi] = \mathrm{Frac}\left(\widehat{B_{\mathfrak{P}_i}}\right) = L_{\mathfrak{P}_i}$. Hence

$$L \otimes_K K_\mathfrak{p} = \prod_{i=1}^r L_{\mathfrak{P}_i}$$

and

$$B \otimes_A \widehat{A_\mathfrak{p}} = \prod_{i=1}^r \widehat{B_{\mathfrak{P}_i}}.$$

Notice that $\widehat{A_\mathfrak{p}}$ and $\widehat{B_{\mathfrak{P}_i}}$ are DVR (Let R be DVR with maximal ideal $\mathfrak{m}$, then $\widehat{R} = \varprojlim_n R/\mathfrak{m}^n$ is also a DVR), in particular, they are Dedekind rings. Note that $\widehat{B_{\mathfrak{P}_i}}$ is integral closed in $L_{\mathfrak{P}_i}$. Since B is a finitely generated A-module, $B \otimes_A \widehat{A_\mathfrak{p}}$ is a finitely generated $\widehat{A_\mathfrak{p}}$-module. It follows that $\widehat{B_{\mathfrak{P}_i}}$, as a direct summand of $B \otimes_A \widehat{A_\mathfrak{p}}$, is finitely generated as $\widehat{A_\mathfrak{p}}$-module since $\widehat{A_\mathfrak{p}}$ is DVR so is noetherian. Thus $\widehat{B_{\mathfrak{P}_i}}$ is integral over $\widehat{A_\mathfrak{p}}$. Consequently the integral closure of $\widehat{A_\mathfrak{p}}$ in $L_{\mathfrak{P}_i}$ is precisely $\widehat{B_{\mathfrak{P}_i}}$.

$$\begin{array}{ccc} \widehat{B_{\mathfrak{P}_i}} & \subset & L_{\mathfrak{P}_i} \\ \Big| & & \Big| \\ \widehat{A_\mathfrak{p}} & \subset & K_\mathfrak{p} \end{array}$$

From $\mathfrak{p}B = \prod_{j=1}^r \mathfrak{P}_j^{e_j}$, we have $\mathfrak{p}B_{\mathfrak{P}_i} = \mathfrak{P}_i^{e_i} B_{\mathfrak{P}_i}$, it follows that $\mathfrak{p}\widehat{B_{\mathfrak{P}_i}} = \mathfrak{P}_i^{e_i}\widehat{B_{\mathfrak{P}_i}} = \left(\mathfrak{P}_i \widehat{B_{\mathfrak{P}_i}}\right)^{e_i}$. The ramification index is also e_i. Thanks to Proposition 3.12 1) and 3), $\widehat{A_\mathfrak{p}}/\mathfrak{p}\widehat{A_\mathfrak{p}} = \widehat{A_\mathfrak{p}}/\widehat{\mathfrak{p}} = A/\mathfrak{p}$. Similarly $\widehat{B_{\mathfrak{P}_i}}/\mathfrak{P}_i\widehat{B_{\mathfrak{P}_i}} = B/\mathfrak{P}_i$. This implies that $\left[\widehat{B_{\mathfrak{P}_i}}/\mathfrak{P}_i\widehat{B_{\mathfrak{P}_i}} : \widehat{A_\mathfrak{p}}/\mathfrak{p}\widehat{A_\mathfrak{p}}\right] = [B/\mathfrak{P}_i : A/\mathfrak{p}] = f_i$, the residue degree is also f_i. Using the method of the proof of Proposition 6.3, get $[L_{\mathfrak{P}_i} : K_\mathfrak{p}] = e_i f_i$.

Suppose L/K is Galois, $\mathrm{Gal}(L/K) = G$. Let $B \supset \mathfrak{P} \mid \mathfrak{p} \subset A$. Recall $D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$. $\sigma(\mathfrak{P}) = \mathfrak{P}$ implies that $\sigma(\mathfrak{P}^n) = \sigma(\mathfrak{P})^n = \mathfrak{P}^n$. So $D_{\mathfrak{P}}$ acts on $B/\mathfrak{P}^n$ for each n. These actions are compatible with natural projections $B/\mathfrak{P}^{n+1} \to B/\mathfrak{P}^n$, so it acts on $\widehat{B_{\mathfrak{P}}} = \varprojlim_n B/\mathfrak{P}^n$, and it keep $\widehat{A_{\mathfrak{p}}} = \varprojlim_n A/\mathfrak{p}^n$ invariant. Therefore $D_{\mathfrak{P}}$ acts on $L_{\mathfrak{P}}$, keeping $K_{\mathfrak{p}}$ invariant. Get morphism of groups: $D_{\mathfrak{P}} \to \mathrm{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}})$. Since $B_{\mathfrak{P}}$ is a DVR, from Corollary 3.13, $\mathrm{Ker}\left(B_{\mathfrak{P}} \to \widehat{B_{\mathfrak{P}}}\right) = \bigcap_{n\geq 0} \mathfrak{P}^n B_{\mathfrak{P}} = 0$, so $B_{\mathfrak{P}} \hookrightarrow \widehat{B_{\mathfrak{P}}}$, and so $L = \mathrm{Frac}\,(B_{\mathfrak{P}}) \subset \mathrm{Frac}\left(\widehat{B_{\mathfrak{P}}}\right) = L_{\mathfrak{P}}$. If $\sigma \in D_{\mathfrak{P}}$ acts trivially on $L_{\mathfrak{P}}$, then it acts trivially on L, $D_{\mathfrak{P}} \hookrightarrow \mathrm{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}})$. On the other hand $|D_{\mathfrak{P}}| = e_{\mathfrak{p}} f_{\mathfrak{p}} = |\mathrm{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}})|$, $D_{\mathfrak{P}} = \mathrm{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}})$. Moreover $|\mathrm{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}})| = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ implies that $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois, so $\mathrm{Aut}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}}) = \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \longrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \longrightarrow 1 \; .$$

Let $L_{\mathfrak{P}}^0 = L_{\mathfrak{P}}^{I_{\mathfrak{P}}}$. Since $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois, and $I_{\mathfrak{P}} \lhd \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, then $\mathrm{Gal}\left(L_{\mathfrak{P}}/L_{\mathfrak{P}}^0\right) = I_{\mathfrak{P}}$ by the Galois correspondence, $\mathrm{Gal}(L_{\mathfrak{P}}^0/K_{\mathfrak{p}}) = \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})/I_{\mathfrak{P}} = \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$.

Let $\mathcal{O}_0$ be the ring of integers of $L_{\mathfrak{P}}^0$, $\mathfrak{P}_0 = \mathfrak{P}\widehat{B_{\mathfrak{P}}} \cap \mathcal{O}_0$, and $k_0 = \mathcal{O}_0/\mathfrak{P}_0$ be the residue field, clearly we have $k_{\mathfrak{p}} \subset k_0 \subset k_{\mathfrak{P}}$. Since $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is separable, $k_{\mathfrak{P}}/k_0$ is separable, so there exists $\overline{\alpha} \in k_{\mathfrak{P}}$ such that $k_{\mathfrak{P}} = k_0\,(\overline{\alpha})$. Choose $\alpha \in \widehat{B_{\mathfrak{P}}}$ be a lift of $\overline{\alpha}$. Define $f(X) = \prod_{\sigma\in I_{\mathfrak{P}}}(X - \sigma(\alpha)) \in \mathcal{O}_0[X]$, mod $\mathfrak{P}\widehat{B_{\mathfrak{P}}}$, get $\overline{f}(X) = \prod_{\sigma\in I_{\mathfrak{P}}}\left(X - \overline{\sigma(\alpha)}\right) = (X - \overline{\alpha})^{|I_{\mathfrak{P}}|} \in k_0[X]$ since every $\sigma \in I_{\mathfrak{P}}$ fix $k_{\mathfrak{P}}$. So the minimal polynomial of $\overline{\alpha}$ over k_0 must divide $\overline{f}(X)$. However, $k_{\mathfrak{P}}/k_0$ is separable, the minimal polynomial admits no multiple roots, so must be $X - \overline{\alpha}$. That is, $\overline{\alpha} \in k_0$. We obtain $k_{\mathfrak{P}} = k_0$. Now $f_{\mathfrak{p}} = [k_{\mathfrak{P}} : k_0][k_0 : k_{\mathfrak{p}}]$ implies that $f_{L_{\mathfrak{P}}^0/K_{\mathfrak{p}},\mathfrak{P}_0} = [k_0 : k_{\mathfrak{p}}] = f_{\mathfrak{p}}$. On the other hand $[L_{\mathfrak{P}}^0 : K_{\mathfrak{p}}] = |\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})| = f_{\mathfrak{p}}$. Since $[L_{\mathfrak{P}}^0 : K_{\mathfrak{p}}] = e_{L_{\mathfrak{P}}^0/K_{\mathfrak{p}},\mathfrak{P}_0} f_{L_{\mathfrak{P}}^0/K_{\mathfrak{p}},\mathfrak{P}_0}$, we have $e_{L_{\mathfrak{P}}^0/K_{\mathfrak{p}},\mathfrak{P}_0} = 1$, so $L_{\mathfrak{P}}^0/K_{\mathfrak{p}}$ is unramified. $[L_{\mathfrak{P}} : L_{\mathfrak{P}}^0] = e_{L_{\mathfrak{P}}/L_{\mathfrak{P}}^0,\mathfrak{P}\widehat{B_{\mathfrak{P}}}} f_{L_{\mathfrak{P}}/L_{\mathfrak{P}}^0,\mathfrak{P}\widehat{B_{\mathfrak{P}}}}$. From $[L_{\mathfrak{P}} : L_{\mathfrak{P}}^0] = e_{\mathfrak{p}}$ and $f_{L_{\mathfrak{P}}/L_{\mathfrak{P}}^0,\mathfrak{P}\widehat{B_{\mathfrak{P}}}} = [k_{\mathfrak{P}} : k_0] = 1$, get $e_{L_{\mathfrak{P}}/L_{\mathfrak{P}}^0,\mathfrak{P}\widehat{B_{\mathfrak{P}}}} = e_{\mathfrak{p}}$. Therefore $L_{\mathfrak{P}}/L_{\mathfrak{P}}^0$ is totally ramified.

Theorem 8.1. Let A be a complete DVR with fraction field K, let $\mathfrak{p}$ be the uniqueness maximal ideal of A. Let k be the residue field. Let $f(X) \in A[X]$ be a united polynomial such that $f(X)$ modulo $\mathfrak{p}$ is irreducible and separable, then $L = K[X]/(f(X))$ is an unramified extension of K and all the unramified extension of K arise in this way. Consequently there exists a bijection between the finite unramified extension of K and the finite separable extension of k.

Proof. First we show $f(X)$ is irreducible in $K[X]$, which implies that $L = K[X]/(f(X))$ is a field. Assume conversely, $f(X) = g(X)h(X)$ in $K[X]$. In K^{sp}, the roots of $g(X)$ and $h(X)$ are roots of $f(X)$, so integral over A. The coefficients of $g(X)$ and $h(X)$ are elementary symmetric polynomials of these roots, so integral over A. Note that A is integrally closed in K, we obtain

$g(X), h(X) \in A[X]$. Mod $\mathfrak{p}$, get $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$, contradicts to $\overline{f}(X)$ irreducible in $A/\mathfrak{p}[X]$. Thus $f(X)$ is irreducible in $K[X]$, L is a field with $[L : K] = \deg(f)$.

Let $B = A[X]/(f(X))$. Verify that it is a DVR, then it must be the integral closure of A in L. Since $B/\mathfrak{p}B = A/\mathfrak{p}[X]/\left(\overline{f}(X)\right)$ is a field. $\mathfrak{p}B$ is a maximal ideal of B. $\mathfrak{p}B$ is the unique prime ideal of B lying over $\mathfrak{p}$, so $\mathfrak{p}B$ is unique maximal ideal of B. Moreover, as $\mathfrak{p}$ is principal, $\mathfrak{p}B$ is principal as well. B is finitely generated A-module, and A is noetherian, so B is noetherian domain since $B \subset L$. Let $\overline{X}$ be X modulo $f(X)$, then $B = A\left[\overline{X}\right]$, which implies that B is integral over A. If $\mathfrak{q} \subset B$ is nonzero prime ideal, for $0 \neq b \in \mathfrak{q}$, we have $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ for some $a_1, \cdots, a_n \in A$. Take such a relation of minimal degree; then $a_n \neq 0$; otherwise, we can cancel a factor b to obtain an integrality relation of lower degree. It follows that $a_n = -b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) \in \mathfrak{q} \cap A = \mathfrak{p}$. Thus $\mathfrak{p}B \subset \mathfrak{q}$ implies that $\mathfrak{q} = \mathfrak{p}B$. That is, $\mathfrak{p}B$ is the unique nonzero prime ideal of B. Now B is a 1-dim noetherian local ring whose maximal ideal is principal, B is DVR.

Applying Dedekind Theorem, since $\overline{f}(X)$ is irreducible and separable, the extension B/A is unramified.

Conversely, let L be an unramified extension. Let B be the integral closure of A in L. Since A is complete DVR, $K = K_{\mathfrak{p}}$, so $L = L \otimes_K K_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}$. But L is a field, so there exists a unique $\mathfrak{P}$ lying over $\mathfrak{p}$. From $e_{\mathfrak{P}} = 1$ and $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is finite separable extension. Then $k_{\mathfrak{P}} = k_{\mathfrak{p}}\left[\overline{\alpha}\right]$ for some α in B. Moreover $[L : K] = e_{\mathfrak{P}} f_{\mathfrak{P}} = f_{\mathfrak{P}} = [k_{\mathfrak{P}} : k_{\mathfrak{p}}]$. Let $f(X)$ be the minimal polynomial of α in K, since α is integral over A, similarly we can prove $f(X) \in A[X]$. $\overline{f}(X) = f(X)$ mod $\mathfrak{p}$ satisfies $\overline{f}\left(\overline{\alpha}\right) = 0$. Since $\deg\left(\overline{f}(X)\right) = \deg(f(X)) = [K(\alpha) : K] \leq [L : K]$, and $\deg\left(\overline{\alpha}\right) = [k_{\mathfrak{P}} : k_{\mathfrak{p}}] = [L : K]$, we have $\deg\left(\overline{f}(X)\right) = [L : K]$ and $\overline{f}(X)$ is irreducible. Then $\overline{f}$ is irreducible and separable. Therefore $K[X]/(f(X))$ is unramified extension. On the other hand $K[X]/(f(X)) = K(\alpha) \subset L$ and $[K(\alpha) : K] = \deg(f(X)) = [L : K]$ gives $K(\alpha) = L$. We obtain $L = K[X]/(f(X))$.

We have a bijection between the finite unramified extension of K and the finite separable extension of k. Indeed,

$$\begin{aligned} \{\text{finite unramified extension of } K\} \quad &\longleftrightarrow \quad \{\text{finite separable extension of } k\}, \\ L/K \quad &\longleftrightarrow \quad k_{\mathfrak{P}}/k_{\mathfrak{p}}. \end{aligned}$$

□

Theorem 8.2. Let A be a complete DVR with fraction field K, let $\mathfrak{p}$ be the uniqueness maximal ideal of A. Let k be the residue class. Let $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$ be such that $a_i \in \mathfrak{p}(1 \leq i \leq n)$, and $a_n \in \mathfrak{p} \setminus \mathfrak{p}^2$. Such polynomials are called Eisenstein polynomial. Let $L = K[X]/(f(X))$, then L is totally ramified over K, and all the totally ramified extension of K arises in this way.

Proof. First prove $f(X)$ is irreducible in $K[X]$, then $L = K[X]/(f(X))$ is a field. Similar to the proof of Theorem 8.1, we factor $f(X) = g(X)h(X)$ in $A[X]$. Assume $g(X) = X^r + b_1X^{r-1} + \cdots + b_r$ and $h(X) = X^s + c_1X^{s-1} + \cdots + c_s$, where $r, s > 0$ and $r + s = n$. Mod $\mathfrak{p}$, get $\overline{g}(X)\overline{h}(X) = \overline{f}(X) = X^n$, so $\overline{g}(X) = X^r$ and $\overline{h}(X) = X^s$. Thus $b_r \in \mathfrak{p}$ and $c_s \in \mathfrak{p}$, which implies that $a_n = b_rc_s \in \mathfrak{p}^2$, a contradiction. So L is a field and $[L : K] = n$.

Let $B = A[X]/(f(X))$. Verify that it is DVR, then it is the integral closure of A in L. Similar to the proof of Theorem 8.1, let $x = X \bmod f(X)$, then $B = A[x]$ implies that B is integral over A. Let $\mathfrak{P} = \mathfrak{p}B + (x) \subset B$, then $B/\mathfrak{P} = A/\mathfrak{p}[X]/\left(\overline{f}(X), X\right) = k_{\mathfrak{p}}[X]/(X^n, X) = k_{\mathfrak{p}}$ implies that $\mathfrak{P}$ is maximal. Similar to the proof of Theorem 8.1, $\mathfrak{P}$ is the unique nonzero prime ideal of B. Moreover $\mathfrak{p}B = (a_n)$ and $a_n = (X^n + a_1X^{n-1} + \cdots + a_{n-1}X) \subset (X)$ in B. So $\mathfrak{P} = \mathfrak{p}B + (x) = (a_n) + (x) = (x)$ is principle in B. B is DVR.

Applying the Dedekind Theorem to B/A, as $\overline{f}(X) = X^n$, B is totally ramified over A.

Conversely, let L/K be a totally ramified extension, let B be the integral closure of A in L. Let $[L : K] = n$, then there exists a unique prime ideal $\mathfrak{P} \subset B$ lying over $\mathfrak{p}$, and $\mathfrak{p}B = \mathfrak{P}^n$, $B/\mathfrak{P} = A/\mathfrak{p}$. Let $\varpi \in B$ be a uniformizer, then $\pi = u\varpi^n$, $u \in B^\times$ is a uniformizer of A. Clearly $K \subset K(\varpi) \subset L$. Assume C be the integral closure of A in $K(\varpi)$, and let $\mathfrak{Q} = \mathfrak{P} \cap C$, then $\varpi \in \mathfrak{Q}$. It follows that $\varpi B = \mathfrak{P} \subset \mathfrak{Q}B$, so $\mathfrak{P} = \mathfrak{Q}B$. Since we have $\mathfrak{Q}B_{\mathfrak{P}} = \mathfrak{P}^{e_{L/K,\mathfrak{P}}}B_{\mathfrak{P}} = \mathfrak{P}B_{\mathfrak{P}}$, $e_{K(\varpi)/K,\mathfrak{Q}} = n$ thanks to Proposition 6.1. However $e_{K(\varpi)/K,\mathfrak{Q}} \leq [K(\varpi) : K]$, so $n = [L : K] \leq [K(\varpi) : K] \leq [L : K] = n$, get $K(\varpi) = L$. Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ be the minimal polynomial of ϖ over K. From $L = K(\varpi)$, $\deg(f) = n$. Moreover $\varpi \in B$ integral over A implies that $f(X) \in A[X]$. In B we have $\varpi^n + a_1\varpi^{n-1} + \cdots + a_n = 0$. Assume conversely there exists $a_i \notin \mathfrak{p}$, take i maximal such that $a_i \notin \mathfrak{p}$. Then $a_i\varpi^{n-1} \in \mathfrak{P}^{n-i} \setminus \mathfrak{P}^{n-i+1}$. However $a_i\varpi^{n-i} = -(\varpi^n + \cdots + a_{i-1}\varpi^{n-i+1} + a_{i+1}\varpi^{n-i-1} + \cdots + a_n) \in \mathfrak{P}^{n-i+1}$, a contradiction. Hence $a_1, \cdots, a_n \in \mathfrak{p}$. Now assume conversely $a_n \in \mathfrak{p}^2$, then $a_n \in \mathfrak{P}^{2n}$. But $\varpi^n = -(a_1\varpi^{n-1} + \cdots + a_n) \in \mathfrak{P}^{n+1}$, a contradiction since ϖ is uniformizer. We get $a_i \in \mathfrak{p}(1 \leq i \leq n)$ and $a_n \in \mathfrak{p} \setminus \mathfrak{p}^2$, $f(X)$ is a Eisenstein polynomial. Thus $B = A[\varpi]$, $L = K[\varpi] = K[X]/(f(X))$. $\square$

9 Discriminant

Suppose that $B = A[\alpha]$ for some $\alpha \in B$, let $f(X) \in A[X]$ be the minimal polynomial. By the Dedekind Theorem, the factorization of $\mathfrak{p}B$ is determined by the factorization of $f(X) \bmod \mathfrak{p} \in A/\mathfrak{p}[X]$. Thus there exists $\mathfrak{P} \mid \mathfrak{p}$ such that L/K is ramified iff $f(X) \bmod \mathfrak{p} = 0$ has multiple root.

Let $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$ be the root of $f(X)$ in K^{sp}, define

$$\Delta(f) = \prod_{1 \le i \ne j \le n} (\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2,$$

then $f(X) \bmod \mathfrak{p}$ has multiple root $\iff$ there exists $i \ne j$ such that $\alpha_i \equiv \alpha_j \pmod{\mathfrak{P}}$, $\mathfrak{P} \subset \mathcal{O}_{K^{\mathrm{sp}}}$ and $\mathfrak{P} \mid \mathfrak{p} \iff \Delta(f) \equiv 0 \pmod{\mathfrak{P}} \iff \Delta(f) \equiv 0 \pmod{\mathfrak{p}}$ (Since the discriminant can be expressed as a function of coefficients of $f(X)$ and $f(X) \in A[X]$, $\Delta(f) \in A$).

Note that

$$\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix}.$$

Moreover $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ is a basis of B as A-module. Let $\beta_1, \cdots, \beta_n$ be a basis of B as A-modules, let $\sigma_i \colon L \to K^{\mathrm{sp}}$, $i = 1, \cdots, n$ be all the K-embeddings. Since L/K is separable, there exactly exists n embeddings. Let

$$B_0 = \begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \cdots & \sigma_n(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix}.$$

Then there exists $g \in \mathrm{GL}_n(A)$ such that

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = g \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix},$$

which implies that $\det(g) \in A^\times$. So

$$\begin{pmatrix} \sigma_i(\beta_1) \\ \sigma_i(\beta_2) \\ \vdots \\ \sigma_i(\beta_n) \end{pmatrix} = g \begin{pmatrix} \sigma_i(1) \\ \sigma_i(\alpha) \\ \vdots \\ \sigma_i(\alpha^{n-1}) \end{pmatrix}.$$

Let

$$A_0 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix},$$

then $B_0 = gA_0$, so $\det(B_0) = \det(g) \cdot \det(A_0)$, so $(\det(B_0)^2) = (\det(A_0)^2) = (\Delta(f))$.

Consider

$$\begin{aligned} B_0 B_0^\top &= \begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \cdots & \sigma_n(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) & \cdots & \sigma_1(\beta_n) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) & \cdots & \sigma_n(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \sigma_n(\beta_2) & \cdots & \sigma_n(\beta_n) \end{pmatrix} \\ &= \left(\sum_{k=1}^n \sigma_k(\beta_i)\sigma_k(\beta_j) \right)_{i,j=1,\cdots,n} \\ &= \left(\sum_{k=1}^n \sigma_k(\beta_i\beta_j) \right)_{i,j=1,\cdots,n} \\ &= \left(\mathrm{Tr}_{L/K}(\beta_i\beta_j) \right)_{i,j=1,\cdots,n}. \end{aligned}$$

Hence $(\Delta(f)) = \det(B_0 B_0^\top) = \det \left(\mathrm{Tr}_{L/K}(\beta_i\beta_j) \right)_{i,j=1,\cdots,n}$. In general, given a basis $W = \{\beta_1, \cdots, \beta_n\}$ of L over K, define

$$\Delta_{L/K,W} = \det \left(\mathrm{Tr}_{L/K}(\beta_i\beta_j) \right)_{i,j=1,\cdots,n}.$$

Here $\Delta_{L/K,W}$ depends on the basis W. If W' is another basis of B over A, then $(\Delta_{L/K,W'}) = (\Delta_{L/K,W})$.

In general, B is a locally free A-module of rank $n = [L : K]$. For $\mathfrak{p} \subset A$ an ideal, then $B_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of rank $n = [L : K]$. Take a basis $\{\beta_1, \cdots, \beta_n\}$ of $B_\mathfrak{p}$ as $A_\mathfrak{p}$-module, define

$$\Delta_{L/K} = \det \left(\mathrm{Tr}_{L/K}(\beta_i\beta_j) \right)_{i,j=1,\cdots,n} \in A_\mathfrak{p}.$$

More intrinsically, consider the bilinear form

$$\langle\ ,\ \rangle : L \times L \longrightarrow K, \quad (x,y) \longmapsto \mathrm{Tr}_{L/K}(xy).$$

If $x, y \in B$, then $xy \in B$ integral over A, $\mathrm{Tr}_{L/K}(xy) \in K$ is also integral over A, which implies that $\mathrm{Tr}_{L/K}(xy) \in A$ since A is integrally closed in K. It restricts to non-degenerated bilinear form

$$\langle\ ,\ \rangle : B \times B \longrightarrow A.$$

Localized at $\mathfrak{p}$, get

$$\langle\ ,\ \rangle_{\mathfrak{p}} : B_{\mathfrak{p}} \times B_{\mathfrak{p}} \longrightarrow A_{\mathfrak{p}}.$$

Then $\det\left(\mathrm{Tr}_{L/K}(\beta_i\beta_j)\right)_{i,j=1,\cdots,n}$ is the discriminant of the bilinear form $\langle\ ,\ \rangle_{\mathfrak{p}}$.

Proposition–Definition 9.1. Let $d_{\mathfrak{p}} = \mathrm{val}_{\mathfrak{p}}(\Delta_{L/K,\mathfrak{p}})$, then $d_{\mathfrak{p}} \neq 0$ for only finitely many $\mathfrak{p} \subset A$. Hence the product

$$\Delta_{L/K} = \prod_{\mathfrak{p}\ \text{prime}} \mathfrak{p}^{d_{\mathfrak{p}}}$$

is well-defined, we call it the **discriminant** for L/K.

Proof. Let $\alpha_1, \cdots, \alpha_n \in B$ such that they form a basis of L/K, let $\Lambda = \bigoplus_{i=1}^n A\alpha_i \subset B$. Then $\Lambda_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ for all $\mathfrak{p} \subset A$ prime. Let $\beta_1, \cdots, \beta_n$ be a basis of $B_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$, then

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = g \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$$

for some $g \in \mathrm{GL}_n(K) \cap \mathcal{M}_n(A_{\mathfrak{p}})$. Let $\sigma_1, \cdots, \sigma_n : L \hookrightarrow K^{\mathrm{sp}}$, it follows that

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} = g \begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix}.$$

Let

$$A' = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}, \quad B' = \begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix},$$

get $\det(A'A'^{\top}) = \det(g)^2 \det(B'B'^{\top}) = \det(g)^2\Delta_{L/K,\mathfrak{p}}$. $g \in \mathcal{M}_n(A_\mathfrak{p})$ implies that $\det(g) \in A_\mathfrak{p}$. Since $\alpha_i \in B$ for all i, $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \in K$ integral over A, so $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \in A$, and so $\det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{i,j=1,\cdots,n} \in A$. Now $\mathrm{val}_\mathfrak{p}\left(\det(A'A'^{\top})\right) = 2\,\mathrm{val}_\mathfrak{p}(\det(g)) + \mathrm{val}_\mathfrak{p}\left(\Delta_{L/K,\mathfrak{p}}\right)$, it follows that $d_\mathfrak{p} \leq \mathrm{val}_\mathfrak{p}\left(\det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{i,j=1,\cdots,n}\right)$. On the other hand $\Delta_{L/K,\mathfrak{p}} \in A_\mathfrak{p}$ gives $d_\mathfrak{p} \geq 0$. Therefore

$$0 \leq d_\mathfrak{p} \leq \mathrm{val}_\mathfrak{p}\left(\det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{i,j=1,\cdots,n}\right).$$

Since A is Dedekind ring,

$$\left(\det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{i,j=1,\cdots,n}\right) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{val}_\mathfrak{p}\left(\det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{i,j=1,\cdots,n}\right)}.$$

There are finitely many $\mathfrak{p} \subset A$ such that $\mathrm{val}_\mathfrak{p}\left(\det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{i,j=1,\cdots,n}\right) \neq 0$. So $d_\mathfrak{p} \neq 0$ for finitely many $\mathfrak{p}$. $\Delta_{L/K}$ is finite product, so is well-defined. $\square$

10 Different

Recall that we have the non-degenerated bilinear form

$$\langle\ ,\ \rangle : B \times B \longrightarrow A, \quad (x, y) \longmapsto \mathrm{Tr}_{L/K}(xy).$$

Consider $B^\vee = \{x \in L \mid \langle x, y\rangle \in A, \forall y \in B\}$. We have $B^\vee \cong \mathrm{Hom}_A(B, A)$ defined by $x \mapsto \left(y \mapsto \mathrm{Tr}_{L/K}(xy)\right)$, since B is a finitely generated A-module, $B^\vee$ is also a finitely generated A-module. It is an A-module inside L, it is a fractional ideal of L. Moreover $B^\vee \supset B$.

Definition 10.1. Let $\delta_{L/K} = (B^\vee)^{-1} = \{z \in L \mid zB^\vee \subset B\} \subset B$, it is called the **different** of extension L/K.

Definition 10.2. Consider the group homomorphism $\mathrm{N}_{L/K}\colon I_L \to I_K$ such that $\mathrm{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f_\mathfrak{P}}$, where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ and $f_\mathfrak{P} = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ is residue degree. For general fractional ideal $\mathfrak{A} = \prod_\mathfrak{P} \mathfrak{P}^{n_\mathfrak{P}}$, let $\mathrm{N}_{L/K}(\mathfrak{A}) = \prod_\mathfrak{P} \mathrm{N}_{L/K}(\mathfrak{P})^{n_\mathfrak{P}} = \prod_\mathfrak{P}(\mathfrak{P} \cap \mathcal{O}_K)^{n_\mathfrak{P} f_\mathfrak{P}}$.

$$\begin{array}{ccccc} \delta_{L/K} & \subset & B & \subset & L \\ \Big| & & \Big| & & \Big| \\ \Delta_{L/K} & \subset & A & \subset & K \end{array}$$

Proposition 10.1. 1) Let $K \subset M \subset L$ be a tower of finite separable extension, then $\mathrm{N}_{L/K} = \mathrm{N}_{M/K} \circ \mathrm{N}_{L/M}$.

2) Let L/K be a finite Galois extension with $\mathrm{Gal}(L/K) = G$, then $\mathrm{N}_{L/K}(\mathfrak{P})\mathcal{O}_L = \prod_{\sigma\in G} \sigma(\mathfrak{P})$.

3) For $x \in L^\times$, then $\mathrm{N}_{L/K}((x)) = \big(\mathrm{N}_{L/K}(x)\big)$.

4) Let K be a finite extension of $\mathbb{Q}$, $\mathfrak{a} \subset \mathcal{O}_K$ be nonzero ideal, then $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|\mathbb{Z}$.

Proof. 1) Let $\mathfrak{P} \subset \mathcal{O}_L$ be a nonzero prime ideal, let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ and $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M$. Then $\mathrm{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f_{L/K,\mathfrak{P}}}$. On the other hand $\mathrm{N}_{M/K} \circ \mathrm{N}_{L/M}(\mathfrak{P}) = \mathrm{N}_{M/K}\left(\mathfrak{q}^{f_{L/M,\mathfrak{P}}}\right) = \mathrm{N}_{M/K}(\mathfrak{q})^{f_{L/M,\mathfrak{P}}} = \left(\mathfrak{p}^{f_{M/K,\mathfrak{q}}}\right)^{f_{L/M,\mathfrak{P}}}$. Hence $\mathrm{N}_{L/K}(\mathfrak{P}) = \mathrm{N}_{M/K} \circ \mathrm{N}_{L/M}(\mathfrak{P})$ since $f_{L/K,\mathfrak{P}} = f_{M/K,\mathfrak{q}} f_{L/M,\mathfrak{P}}$.

2) Let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Suppose that $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{P}_i^e$. Suppose that $\mathfrak{P}_1 = \mathfrak{P}$, then $r = |G/D_{\mathfrak{P}}|$. Therefore $\prod_{\sigma\in G} \sigma(\mathfrak{P}) = \prod_{i=1}^r \mathfrak{P}_i^{|D_{\mathfrak{P}}|} = \prod_{i=1}^r \mathfrak{P}_i^{ef} = (\prod_{i=1}^r \mathfrak{P}_i^e)^f = \mathfrak{p}^f\mathcal{O}_L$. Note that $\mathrm{N}_{L/K}(\mathfrak{P})\mathcal{O}_L = \mathfrak{p}^f\mathcal{O}_L$, we obtain $\mathrm{N}_{L/K}(\mathfrak{P})\mathcal{O}_L = \prod_{\sigma\in G}\sigma(\mathfrak{P})$.

3) For arbitrary $x \in L^\times$, we have

$$(x) = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(x)},$$

which implies that

$$\mathrm{N}_{L/K}((x)) = \prod_{\mathfrak{P}} \mathrm{N}_{L/K}(\mathfrak{P})^{v_{\mathfrak{P}}(x)} = \prod_{\mathfrak{p}} \mathfrak{p}^{\sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}} v_{\mathfrak{P}}(x)}.$$

Use the fact

$$v_{\mathfrak{p}}\left(\mathrm{N}_{L/K}(x)\right) = \sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}} v_{\mathfrak{P}}(x),$$

get

$$\big(N_{L/K}(x)\big) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathrm{N}_{L/K}(x))} = \prod_{\mathfrak{p}} \mathfrak{p}^{\sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}} v_{\mathfrak{P}}(x)}.$$

Consequently $\mathrm{N}_{L/K}((x)) = \big(\mathrm{N}_{L/K}(x)\big)$.

4) For distinct nonzero prime ideals $\mathfrak{p}_i, \mathfrak{p}_j \subset \mathcal{O}_K$, by the Chinese Remainder Theorem, $\mathcal{O}_K/\mathfrak{p}_i^{n_i}\mathfrak{p}_j^{n_j} = \mathcal{O}_K/\mathfrak{p}_i^{n_i} \times \mathcal{O}_K/\mathfrak{p}_j^{n_j}$, which implies that $\left|\mathcal{O}_K/\mathfrak{p}_i^{n_i}\mathfrak{p}_j^{n_j}\right| = |\mathcal{O}_K/\mathfrak{p}_i^{n_i}| \cdot \left|\mathcal{O}_K/\mathfrak{p}_j^{n_j}\right|$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime ideal, we have $\mathcal{O}_{K\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$. Consider the filtration $\mathcal{O}_{K\mathfrak{p}} \supset \mathfrak{p}\mathcal{O}_{K\mathfrak{p}} \supset \cdots \supset \mathfrak{p}^n\mathcal{O}_{K\mathfrak{p}}$, get $|\mathcal{O}_K/\mathfrak{p}^n| = \left|\mathcal{O}_{K\mathfrak{p}}/\mathfrak{p}^n\mathcal{O}_{K\mathfrak{p}}\right| = \prod_{i=1}^n \left|\mathfrak{p}^{i-1}\mathcal{O}_{K\mathfrak{p}}/\mathfrak{p}^i\mathcal{O}_{K\mathfrak{p}}\right| = \prod_{i=1}^n \left|\mathcal{O}_{K\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K\mathfrak{p}}\right| = |\mathcal{O}_K/\mathfrak{p}|^n$. Consequently, $\left|\mathcal{O}_K/\prod_{\mathfrak{p}}\mathfrak{p}^{n_{\mathfrak{p}}}\right| = \prod_{\mathfrak{p}} |\mathcal{O}_K/\mathfrak{p}|^{n_{\mathfrak{p}}}$. Enough to verify for $\mathfrak{a} = \mathfrak{p}$. Assume $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ and $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$, then $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p^f\mathbb{Z}$. So $|\mathcal{O}_K/\mathfrak{p}| = p^f\mathbb{Z} = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$.

□

Proposition 10.2. We have $\Delta_{L/K} = \mathrm{N}_{L/K}(\delta_{L/K})$.

Proof. Enough to verify that $\Delta_{L/K,\mathfrak{p}} = \mathrm{N}_{L/K}(\delta_{L/K,\mathfrak{p}})$ for arbitrary $\mathfrak{p} \subset A$ prime. Consider the bilinear form

$$\langle\ ,\ \rangle_{\mathfrak{p}} : B_{\mathfrak{p}} \times B_{\mathfrak{p}} \longrightarrow A_{\mathfrak{p}}$$

Let $\beta_1, \cdots, \beta_n$ be a set of basis $B_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$, let $\beta_1^*, \cdots, \beta_n^*$ be the dual basis of $\beta_1, \cdots, \beta_n$, i.e., $\langle \beta_i, \beta_j^* \rangle = \delta_{ij}$. So $B_{\mathfrak{p}}^\vee = A_{\mathfrak{p}}\beta_1^* + \cdots + A_{\mathfrak{p}}\beta_n^*$. Since B is a Dedekind domain, $B_{\mathfrak{p}}$ is PID. Thus $\delta_{L/K,\mathfrak{p}} = (\delta)$ for some $\delta \in B_{\mathfrak{p}}$. Moreover $\delta_{L/K,\mathfrak{p}} = \left(B_{\mathfrak{p}}^\vee\right)^{-1}$, $\delta B_{\mathfrak{p}}^\vee = B_{\mathfrak{p}}$, i.e., $B_{\mathfrak{p}} = A_{\mathfrak{p}}\delta\beta_1^* + \cdots + A_{\mathfrak{p}}\delta\beta_n^*$. Thus $\delta\beta_1^*, \cdots, \delta\beta_n^*$ is a basis of $B_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$. By definition,

$$\begin{aligned}
\Delta_{L/K,\mathfrak{p}} &= \Big(\det\left(\mathrm{Tr}_{L/K}(\beta_i\beta_j)\right)_{i,j=1,\cdots,n}\Big) \\
&= \left(\det\begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \cdots & \sigma_n(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix}\right) \cdot \left(\det\begin{pmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) & \cdots & \sigma_1(\beta_n) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) & \cdots & \sigma_2(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \sigma_n(\beta_2) & \cdots & \sigma_n(\beta_n) \end{pmatrix}\right) \\
&= \left(\det\begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \cdots & \sigma_n(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \cdots & \sigma_n(\beta_n) \end{pmatrix}\right) \cdot \left(\det\begin{pmatrix} \sigma_1(\delta\beta_1^*) & \sigma_1(\delta\beta_2^*) & \cdots & \sigma_1(\delta\beta_n^*) \\ \sigma_2(\delta\beta_1^*) & \sigma_2(\delta\beta_2^*) & \cdots & \sigma_2(\delta\beta_2^*) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\delta\beta_1^*) & \sigma_n(\delta\beta_2^*) & \cdots & \sigma_n(\delta\beta_n^*) \end{pmatrix}\right) \\
&= \Big(\det\left(\mathrm{Tr}_{L/K}(\beta_i\beta_j^*)\right)_{i,j=1,\cdots,n} \cdot \mathrm{N}_{L/K}(\delta)\Big) \\
&= \left(\mathrm{N}_{L/K}(\delta)\right) \\
&= \mathrm{N}_{L/K}((\delta)) \\
&= \mathrm{N}_{L/K}(\delta_{L/K,\mathfrak{p}}).
\end{aligned}$$

□

Lemma 10.1. Let L/K be a finite separable extension. Let $\mathfrak{a} \subset K$, $\mathfrak{b} \subset L$ be fractional ideals, then $\mathrm{Tr}_{L/K}(\mathfrak{b}) \subset \mathfrak{a} \iff \mathfrak{b} \subset \mathfrak{a}B \cdot \delta_{L/K}^{-1}$. Here $\mathrm{Tr}_{L/K}(\mathfrak{b}) := \{\mathrm{Tr}_{L/K}(x) \mid x \in \mathfrak{b}\} \subset K$.

Proof. $\mathrm{Tr}_{L/K}(\mathfrak{b}) \subset \mathfrak{a} \iff \mathfrak{a}^{-1}\,\mathrm{Tr}_{L/K}(\mathfrak{b}) \subset \mathcal{O}_K \iff \mathrm{Tr}_{L/K}(\mathfrak{a}^{-1}\mathfrak{b}) \subset \mathcal{O}_K \iff \mathfrak{a}^{-1}\mathfrak{b} \subset \mathcal{O}_K^\vee = \delta_{L/K}^{-1} \iff \mathfrak{b} \subset \mathfrak{a}B \cdot \delta_{L/K}^{-1}$. □

Proposition 10.3. Let $K \subset M \subset L$ be a tower of finite separable extension, then $\delta_{L/K} = \delta_{L/M} \cdot \delta_{M/K}$, $\Delta_{L/K} = \mathrm{N}_{M/K}(\Delta_{L/M}) \cdot \Delta_{M/K}^{[L:M]}$.

Proof. Let $\mathfrak{a} \subset K$ be arbitrary fractional ideal. Then by Lemma 10.1, $\mathfrak{a} \subset \delta_{L/K}^{-1} \iff \mathrm{Tr}_{L/K}(\mathfrak{a}) \subset \mathcal{O}_K \iff \mathrm{Tr}_{M/K}\left(\mathrm{Tr}_{L/M}(\mathfrak{a})\right) \subset \mathcal{O}_K \iff \mathrm{Tr}_{L/M}(\mathfrak{a}) \subset \delta_{M/K}^{-1} \iff \mathfrak{a} \subset \delta_{M/K}^{-1}\delta_{L/M}^{-1}$. So $\delta_{L/K} = \delta_{L/M} \cdot \delta_{M/K}$.

So

$$\begin{aligned}
\Delta_{L/K} &= \mathrm{N}_{L/K}(\delta_{L/K}) \\
&= \mathrm{N}_{L/K}(\delta_{M/K})\,\mathrm{N}_{L/K}(\delta_{L/M}) \\
&= \mathrm{N}_{M/K}\left(\mathrm{N}_{L/M}(\delta_{M/K})\right)\mathrm{N}_{M/K}\left(\mathrm{N}_{L/M}(\delta_{L/M})\right) \\
&= \mathrm{N}_{M/K}\left(\delta_{M/K}^{[L:M]}\right)\mathrm{N}_{M/K}(\Delta_{L/M}) \\
&= \mathrm{N}_{M/K}(\Delta_{L/M}) \cdot \Delta_{M/K}^{[L:M]}.
\end{aligned}$$

Here we prove, if $\mathfrak{c} \subset L$ be a fractional ideal, then $\mathrm{N}_{L/M}(\mathfrak{c}B) = \mathfrak{c}^{[L:M]}$, which implies that $\mathrm{N}_{L/M}(\delta_{M/K}) = \delta_{M/K}^{[L:M]}$. Write $\mathfrak{c} = \prod_{\mathfrak{q} \subset \mathcal{O}_M} \mathfrak{q}^{n_\mathfrak{q}}$, then

$$\mathfrak{q}B = \prod_{\mathfrak{q} \subset \mathcal{O}_M} (\mathfrak{q}B)^{n_\mathfrak{q}} = \prod_{\mathfrak{q} \subset \mathcal{O}_M} \prod_{\mathfrak{P} | \mathfrak{q}} \mathfrak{P}^{n_\mathfrak{q} e_\mathfrak{P}}.$$

It follows that

$$\mathrm{N}_{L/M}(\mathfrak{c}B) = \prod_{\mathfrak{q}} \prod_{\mathfrak{P}|\mathfrak{q}} \mathfrak{q}^{n_\mathfrak{q} e_\mathfrak{P} f_\mathfrak{P}} = \prod_{\mathfrak{q}} \mathfrak{q}^{n_\mathfrak{q} \sum_{\mathfrak{P}|\mathfrak{q}} e_\mathfrak{P} f_\mathfrak{P}} = \prod_{\mathfrak{q}} \mathfrak{q}^{n_\mathfrak{q}[L:M]} = \mathfrak{c}^{[L:M]}.$$

□

Proposition 10.4. Suppose that $B = A[\alpha]$ for some $\alpha \in B$, let $f(X) \in A[X]$ be the minimal polynomial, then $\delta_{L/K} = (f'(\alpha))$.

Proof. Since $B = A[\alpha]$, $1, \alpha, \cdots, \alpha^{n-1}$ is a basis of B over A, where $n = [L : K]$. We prove $B^\vee = (1/f'(\alpha))B$, in this case $\delta_{L/K} = (B^\vee)^{-1} = ((1/f'(\alpha))B)^{-1} = (f'(\alpha))$.

Let $f(X)$ be minimal polynomial of α, since L/K is separable, $f'(\alpha) \neq 0$. In $L[X]$ we write $f(X)/(X-\alpha) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$. Note that $f(X)/(X-\alpha) = X^{n-1} + (\alpha + a_{n-1})X^{n-2} + (\alpha^2 + a_{n-1}\alpha + a_{n-2})X^{n-3} + \cdots$, so $c_0, \cdots, c_{n-1} \in A[\alpha] = B$. Moreover $c_0, \cdots, c_{n-1}$ is also a basis of B over A. Let $\sigma_1, \cdots, \sigma_n$ be K-embeddings of L/K, and let $\alpha_i = \sigma_i(\alpha)$, then $f(X) = \prod_{i=1}^n (X - \alpha_i)$ and $f'(\alpha_i) = \prod_{r \neq i}(\alpha_i - \alpha_r)$. Apply σ_i to $f(X)/(X-\alpha) = \sum_{j=0}^{n-1} c_j X^j$, get $f(X)/(X-\alpha_i) = \sum_{j=0}^{n-1} \sigma_i(c_j)X^j$. Let

$$\ell_i(X) = \frac{f(X)}{(X-\alpha_i)f'(\alpha_i)} = \prod_{r \neq i} \frac{X - \alpha_r}{\alpha_i - \alpha_r}.$$

Now $f(X)/(X-\alpha_i) = \sum_{j=0}^{n-1} \sigma_i(c_j) X^j$, we have

$$\ell_i(X) = \frac{f(X)}{(X-\alpha_i)f'(\alpha_i)} = \sum_{j=0}^{n-1} \frac{\sigma_i(c_j)}{f'(\alpha_i)} X^j = \sum_{j=0}^{n-1} \sigma_i \left(\frac{c_j}{f'(\alpha)} \right) X^j.$$

Lagrange interpolation gives $X^m = \sum_{i=1}^{n} \alpha_i^m \ell_i(X)$. That is,

$$X^m = \sum_{i=1}^{n} \alpha_i^m \left(\sum_{j=0}^{n-1} \sigma_i \left(\frac{c_j}{f'(\alpha)} \right) X^j \right) = \sum_{j=0}^{n-1} \left(\sum_{i=1}^{n} \alpha_i^m \sigma_i \left(\frac{c_j}{f'(\alpha)} \right) \right) X^j.$$

Hence

$$\sum_{i=1}^{n} \alpha_i^m \sigma_i \left(\frac{c_j}{f'(\alpha)} \right) = \sum_{i=1}^{n} \sigma_i \left(\alpha^m \frac{c_j}{f'(\alpha)} \right) = \mathrm{Tr}_{L/K} \left(\alpha^m \frac{c_j}{f'(\alpha)} \right) = \delta_{mj}.$$

That is, $c_0/f'(\alpha), \cdots, c_{n-1}/f'(\alpha)$ is dual basis of $1, \alpha, \cdots, \alpha^{n-1}$. Consequently

$$B^\vee = A\frac{c_0}{f'(\alpha)} + \cdots + A\frac{c_{n-1}}{f'(\alpha)} = \frac{1}{f'(\alpha)} B.$$

□

Proposition 10.5. Let L/K be finite separable extension, let $\mathfrak{P} \subset B$ be a nonzero prime ideal, let $\mathfrak{p} = \mathfrak{P} \cap A$, then L/K is ramified at $\mathfrak{P}$ iff $\mathfrak{P} \mid \delta_{L/K}$. In this case $\mathfrak{p} \mid \Delta_{L/K}$.

Proof. Ramification is a local property, it depends only on the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Moreover if $\delta_{L/K} = \prod_{\mathfrak{Q} \subset B} \mathfrak{Q}^{d_{\mathfrak{Q}}}$, then $\delta_{L/K,\mathfrak{P}} = \mathfrak{P}^{d_{\mathfrak{P}}}$, $\mathfrak{P} \mid \delta_{L/K}$ iff $d_{\mathfrak{P}} > 0$, which is also local. So we prove under case $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Let $L_{\mathfrak{P}}^0$ be the maximal unramified extension of $K_{\mathfrak{p}}$ contained in $L_{\mathfrak{P}}$, then $L_{\mathfrak{P}}/L_{\mathfrak{P}}^0$ is totally ramified.

Now prove both $\mathcal{O}_{L_{\mathfrak{P}}}/\mathcal{O}_{L_{\mathfrak{P}}^0}$ and $\mathcal{O}_{L_{\mathfrak{P}}^0}/\mathcal{O}_{K_{\mathfrak{p}}}$ are generated by one element. Let $\mathfrak{q} \subset \mathcal{O}_{L_{\mathfrak{P}}^0}$ be the maximal ideal. Since $L_{\mathfrak{P}}^0$ is unramified, $(\mathcal{O}_{L_{\mathfrak{P}}^0}/\mathfrak{q})/(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}})$ is separable, so we can take $\alpha \in \mathcal{O}_{L_{\mathfrak{P}}^0}$ such that $\mathcal{O}_{L_{\mathfrak{P}}^0}/\mathfrak{q} = \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}(\overline{\alpha})$, where $\overline{\alpha} \in \mathcal{O}_{L_{\mathfrak{P}}^0}/\mathfrak{q}$. Let $g(X) \in \mathcal{O}_{K_{\mathfrak{p}}}[X]$ be the minimal polynomial of α over $K_{\mathfrak{p}}$, then $[\mathcal{O}_{L_{\mathfrak{P}}^0}/\mathfrak{q} : \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}] \le \deg(g(X))$. On the other hand $\deg(g(X)) \le [L_{\mathfrak{P}}^0 : K_{\mathfrak{p}}]$ since $K_{\mathfrak{p}}(\alpha) \subset L_{\mathfrak{P}}^0$. From $[\mathcal{O}_{L_{\mathfrak{P}}^0}/\mathfrak{q} : \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}] = [L_{\mathfrak{P}}^0 : K_{\mathfrak{p}}]$, we obtain $[K_{\mathfrak{p}}(\alpha) : K_{\mathfrak{p}}] = [L_{\mathfrak{P}}^0 : K_{\mathfrak{p}}]$, combine $K_{\mathfrak{p}}(\alpha) \subset L_{\mathfrak{P}}^0$ get $K_{\mathfrak{p}}(\alpha) = L_{\mathfrak{P}}^0$. Since $\mathcal{O}_{L_{\mathfrak{P}}^0}/\mathfrak{q} = \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}(\overline{\alpha})$, $1, \overline{\alpha}, \cdots, \overline{\alpha^{r-1}}$ generates $\mathcal{O}_{L_{\mathfrak{P}}^0}/\mathfrak{q}$ as $\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}$-vector space, where $r = [L_{\mathfrak{P}}^0 : K_{\mathfrak{p}}]$. It follows that $\mathcal{O}_{K_{\mathfrak{p}}}[\alpha] + \mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}\mathcal{O}_{L_{\mathfrak{P}}^0} = \mathcal{O}_{L_{\mathfrak{P}}^0}$. Nakayama Lemma gives $\mathcal{O}_{L_{\mathfrak{P}}^0} = \mathcal{O}_{K_{\mathfrak{p}}}[\alpha]$. Now consider totally ramified extension $L_{\mathfrak{P}}/L_{\mathfrak{P}}^0$. Let π be the uniformizer of $\mathcal{O}_{L_{\mathfrak{P}}}$, that is, $\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}} = (\pi)$. $L_{\mathfrak{P}}/L_{\mathfrak{P}}^0$ is totally ramified implies that $\mathfrak{q}\mathcal{O}_{L_{\mathfrak{P}}} = (\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}})^m = (\pi^m)$ where $m = [L_{\mathfrak{P}} : L_{\mathfrak{P}}^0]$ and $\mathcal{O}_{L_{\mathfrak{P}}^0}/\mathfrak{q} = \mathcal{O}_{L_{\mathfrak{P}}}/\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$. For arbitrary $x \in \mathcal{O}_{L_{\mathfrak{P}}}$, one can choose $a_0 \in \mathcal{O}_{L_{\mathfrak{P}}^0}$ such that $x - a_0 \in (\pi)$, i.e., there exists $x_1 \in \mathcal{O}_{L_{\mathfrak{P}}}$ such that $x - a_0 = \pi x_1$. Similarly, repeating this process, get $a_0, \cdots, a_{m-1} \in \mathcal{O}_{L^0_{\mathfrak{P}}}$ such that $x - \sum_{i=0}^{m-1} a_i \pi^i \in (\pi^m) = \mathfrak{q}\mathcal{O}_{L_{\mathfrak{P}}}$. Therefore $\mathcal{O}_{L_{\mathfrak{P}}} = \mathcal{O}_{L^0_{\mathfrak{P}}}[\pi] + \mathfrak{q}\mathcal{O}_{L_{\mathfrak{P}}}$, by Nakayama Lemma $\mathcal{O}_{L_{\mathfrak{P}}} = \mathcal{O}_{L^0_{\mathfrak{P}}}[\pi]$.

Apply Proposition 10.4. We have $\delta_{L^0_{\mathfrak{P}}/K_{\mathfrak{p}}} = (g'(\alpha))$. $\overline{g}(X) = g(X) \bmod \mathfrak{q}$ is the minimal polynomial of $\overline{\alpha}$ and $(\mathcal{O}_{L^0_{\mathfrak{P}}}/\mathfrak{q})/(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}})$ is separable implies that $\overline{g}'(\overline{\alpha}) \neq 0$. So $g'(\alpha) \notin \mathfrak{q}$, $g'(\alpha)$ is a unit in $\mathcal{O}_{L^0_{\mathfrak{P}}}$, $\delta_{L^0_{\mathfrak{P}}/K_{\mathfrak{p}}} = \mathcal{O}_{L^0_{\mathfrak{P}}}$. Let $h(X) \in \mathcal{O}_{L^0_{\mathfrak{P}}}[X]$ be the minimal polynomial of π over $L^0_{\mathfrak{P}}$, we have $\deg(h(X)) = m$. Write $h(X) = X^m + a_1 X^{m-1} + \cdots + a_{m-1}X + a_m$. Since $\mathcal{O}_{L_{\mathfrak{P}}} = \mathcal{O}_{L^0_{\mathfrak{P}}}[X]/(h(X))$, then $\mathcal{O}_{L_{\mathfrak{P}}}/\mathfrak{q}\mathcal{O}_{L_{\mathfrak{P}}} = \left(\mathcal{O}_{L^0_{\mathfrak{P}}}/\mathfrak{q}\right)[X]/\left(\overline{h}(X)\right)$. Note that $\mathcal{O}_{L_{\mathfrak{P}}}/\mathfrak{q}\mathcal{O}_{L_{\mathfrak{P}}} = \mathcal{O}_{L_{\mathfrak{P}}}/(\pi^m)$, we get $X^m \in \left(\overline{h}(X)\right)$, which forces $\overline{h}(X) = X^m$. Therefore $a_1, \cdots, a_m \in \mathfrak{q}$. For $m > 1$, $h'(\pi) = m\pi^{m-1} + (m-1)a_1\pi^{m-2} + \cdots + 2a_{m-2}\pi + a_{m-1} \in (\pi)$. $\delta_{L_{\mathfrak{P}}/L_{\mathfrak{P}^0}} = (h'(\pi))$ implies that $\mathfrak{P} \mid \delta_{L_{\mathfrak{P}}/L^0_{\mathfrak{P}}}$. Combine multiplicativity of different get the Proposition.

Moreover if $m = 1$, $L_{\mathfrak{P}} = L^0_{\mathfrak{P}}$, then $\delta_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = \delta_{L^0_{\mathfrak{P}}/K_{\mathfrak{p}}} = \mathcal{O}_{L^0_{\mathfrak{P}}}$, $\mathfrak{P} \nmid \delta$. $\square$

11 Dedekind zeta function

Let $K/\mathbb{Q}$ be a finite extension.

Recall that Riemann zeta function

$$\begin{aligned} \zeta(s) &= \sum_{n=1}^{+\infty} \frac{1}{n^s} \\ &= \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) \\ &= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \end{aligned}$$

converges absolutely for $\mathrm{Re}(s) > 1$. The **Dedekind zeta function** is defined by

$$\begin{aligned} \zeta_K(s) &= \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{\mathrm{N}(\mathfrak{a})^s} \\ &= \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ \mathfrak{p} \text{ prime}}} \left(1 + \frac{1}{\mathrm{N}(\mathfrak{p})^s} + \frac{1}{\mathrm{N}(\mathfrak{p})^{2s}} + \frac{1}{\mathrm{N}(\mathfrak{p})^{3s}} + \cdots\right) \\ &= \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ \mathfrak{p} \text{ prime}}} \frac{1}{1 - \mathrm{N}(\mathfrak{p})^{-s}} \end{aligned}$$

Here $\mathrm{N}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. By the Chinese Remainder Theorem $\mathrm{N}\left(\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}\right) = \mathrm{N}(\mathfrak{p}_1)^{n_1} \cdots \mathrm{N}(\mathfrak{p}_r)^{n_r}$.

Proposition 11.1. $\zeta_K(s)$ absolutely converges for $\mathrm{Re}(s) > 1$, hence it defines a holomorphic function on $\mathrm{Re}(s) > 1$.

Proof. Take log of the product expansion,

$$\sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}} \log\left(\frac{1}{1-\mathrm{N}(\mathfrak{p})^{-s}}\right) = \sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}} \sum_{n=1}^{+\infty} \frac{1}{n\,\mathrm{N}(\mathfrak{p})^{ns}}.$$

It follows that

$$\sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}} \left|\log\left(\frac{1}{1-\mathrm{N}(\mathfrak{p})^{-s}}\right)\right| \leq \sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}} \sum_{n=1}^{+\infty} \frac{1}{n\,\mathrm{N}(\mathfrak{p})^{n\operatorname{Re}(s)}}.$$

For $\operatorname{Re}(s)>1$, $\mathrm{N}(\mathfrak{p}) = p^f \geq p$ thanks to Proposition 10.1, so

$$\sum_{\substack{\mathfrak{p}\subset\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}} \sum_{n=1}^{+\infty} \frac{1}{n\,\mathrm{N}(\mathfrak{p})^{n\operatorname{Re}(s)}} \leq \sum_{p\text{ prime}} \sum_{\mathfrak{p}|p} \sum_{n=1}^{+\infty} \frac{1}{np^{n\operatorname{Re}(s)}} \leq \sum_{p\text{ prime}} \sum_{n=1}^{+\infty} \frac{[K:\mathbb{Q}]}{np^{n\operatorname{Re}(s)}}$$

since $\#\{\mathfrak{p}:\mathfrak{p}\mid p\} \leq [K:\mathbb{Q}]$. Now

$$\begin{aligned}
[K:\mathbb{Q}] \sum_{p\text{ prime}} \sum_{n=1}^{+\infty} \frac{1}{np^{n\operatorname{Re}(s)}} &\leq [K:\mathbb{Q}] \sum_{p\text{ prime}} \sum_{n=1}^{+\infty} \frac{1}{p^{n\operatorname{Re}(s)}} \\
&\leq [K:\mathbb{Q}] \sum_{p\text{ prime}} \frac{p^{-\operatorname{Re}(s)}}{1-p^{-\operatorname{Re}(s)}} \\
&\leq [K:\mathbb{Q}] \frac{1}{1-2^{-\operatorname{Re}(s)}} \sum_{p\text{ prime}} \frac{1}{p^{\operatorname{Re}(s)}} \\
&\leq [K:\mathbb{Q}] \frac{1}{1-2^{-\operatorname{Re}(s)}} \sum_{m=1}^{+\infty} \frac{1}{m^{\operatorname{Re}(s)}}
\end{aligned}$$

converges as $\operatorname{Re}(s)>1$. ☐

Example 11.1. Consider the Gaussian integer ring $\mathbb{Z}\left[\sqrt{-1}\right] \subset K = \mathbb{Q}\left(\sqrt{-1}\right)$. Here $\mathbb{Z}\left[\sqrt{-1}\right]$ is a ED, hence a PID.

$$\zeta_K(s) = \sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \sum_{a\in\mathcal{O}_K/\mathcal{O}_K^\times} \frac{1}{\mathrm{N}((a))^s} = \frac{1}{4} \sum_{\substack{m,n=-\infty\\ (m,n)\neq(0,0)}}^{+\infty} \frac{1}{\mathrm{N}\left(\left(m+n\sqrt{-1}\right)\right)^s}$$

We prove: for $a = m+n\sqrt{-1} \in \mathbb{Z}\left[\sqrt{-1}\right]$, $(m,n)\neq(0,0)$, we have $\mathrm{N}((a)) = m^2+n^2$. From $\left(m+n\sqrt{-1}\right)\left(x+y\sqrt{-1}\right) = (mx-ny)+(my+nx)\sqrt{-1}$, (a) is generated by $a = m+n\sqrt{-1}$ and $a\sqrt{-1} = -n+m\sqrt{-1}$ as $\mathbb{Z}$-submodule. That is, when x,y run over all the integers, (a) corresponds to $(mx-ny, nx+my)$. The sublattice of $\mathbb{Z}\left[\sqrt{-1}\right]$ corresponding to (a) is generated by the column vectors of

$$\begin{pmatrix} m & -n \\ n & m \end{pmatrix}.$$

Therefore

$$\left|\mathbb{Z}\left[\sqrt{-1}\right]/(a)\right| = \left|\det\begin{pmatrix} m & -n \\ n & m \end{pmatrix}\right| = m^2+n^2.$$

Consequently

$$\zeta_K(s) = \frac{1}{4}\sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{+\infty} \frac{1}{(m^2+n^2)^s}.$$

On the other hand recall Example 6.1, $\sqrt{-1}$ has minimal polynomial X^2+1 with discriminant $\Delta=-4$, so the only ramified prime is 2. In $\mathbb{Z}\left[\sqrt{-1}\right]$, we have $(2) = \left(1+\sqrt{-1}\right)\left(1-\sqrt{-1}\right) = \left(1+\sqrt{-1}\right)^2$. For odd prime number p, p is unramified. p splits iff X^2+1 has a solution in $\mathbb{F}_p$, iff $\left(\frac{-1}{p}\right) = 1$, i.e., $p \equiv 1 \pmod 4$. In this case $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, $f=1$, $e=1$, $r=2$. It follows that $\mathrm{N}(\mathfrak{p}) = \mathrm{N}\left(\overline{\mathfrak{p}}\right) = p$. p inert iff $X^2+1=0$ has no solution in $\mathbb{F}_p$, iff $\left(\frac{-1}{p}\right) = -1$, i.e., $p \equiv 3 \bmod 4$. In this case (p) is prime ideal in $\mathbb{Z}\left[\sqrt{-1}\right]$, we have $f=2$, $e=1$, $r=1$, so $\mathrm{N}((p)) = p^2$. Consequently,

$$\begin{aligned}
\zeta_K(s) &= \prod_{\substack{\mathfrak{p}\subset\mathcal{O}_K \\ \mathfrak{p}\ \text{prime}}} \frac{1}{1-\mathrm{N}(\mathfrak{p})^{-s}} \\
&= \frac{1}{1-2^{-s}} \prod_{(p)=\mathfrak{p}\overline{\mathfrak{p}}} \frac{1}{(1-p^{-s})^2} \prod_{p\ \text{inert}} \frac{1}{1-p^{-2s}} \\
&= \frac{1}{1-2^{-s}} \prod_{(p)=\mathfrak{p}\overline{\mathfrak{p}}} \frac{1}{(1-p^{-s})^2} \prod_{p\ \text{inert}} \frac{1}{(1-p^{-s})(1+p^{-s})} \\
&= \zeta(s) \prod_{p\equiv 1 \bmod 4} \frac{1}{1-p^{-s}} \prod_{p\equiv 3 \bmod 4} \frac{1}{1+p^{-s}}.
\end{aligned}$$

We have $G = \mathrm{Gal}(K/\mathbb{Q}) = \{1,\sigma\}$, where $\sigma\left(\sqrt{-1}\right) = -\sqrt{-1}$. Let $\chi\colon G \to \{\pm 1\}$ defined by $\chi(1)=1$ and $\chi(\sigma)=-1$ be a character. For $p\neq 2$, p is unramified. If p splits, $\mathbb{Z}\left[\sqrt{-1}\right]/\mathfrak{p} = \mathbb{F}_p$, $x^p = x$ for every $x\in\mathbb{F}_p$, so $\mathrm{Fr}_{\mathfrak{p}} = 1$, get $\chi(\mathrm{Fr}_{\mathfrak{p}}) = 1$. We have

$$\frac{1}{1-\frac{\chi(\mathrm{Fr}_{\mathfrak{p}})}{p^s}} = \frac{1}{1-p^{-s}}.$$

If p inert, $\mathbb{Z}\left[\sqrt{-1}\right]/(p) = \mathbb{F}_{p^2}$, so $\mathrm{Fr}_p = \sigma$, which implies that $\chi(\mathrm{Fr}_p) = -1$.

$$\frac{1}{1-\frac{\chi(\mathrm{Fr}_p)}{p^s}} = \frac{1}{1+p^{-s}}.$$

Hence we obtain

$$\zeta_K(s) = \zeta(s)\prod_{p\neq 2}\frac{1}{1-\frac{\chi(\mathrm{Fr}_p)}{p^s}}.$$

Consider $\varphi\colon \mathbb{Z}/4 \to \{\pm 1\}$ be Dirichlet character modulo 4, defined by

$$\varphi(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 3 \bmod 4, \\ 0 & \text{if } n \equiv 0, 2 \bmod 4. \end{cases}$$

Then

$$\zeta_K(s) = \zeta(s) \prod_{p \neq 2} \frac{1}{1 - \frac{\varphi(p)}{p^s}} = \zeta(s) \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s}$$

as $\mathrm{Re}(s) > 1$.

12 Representations of finite group

Let G be a finite group, V is finite dimensional $\mathbb{C}$-vector space. A **representation** is a group homomorphism $\rho\colon G \to \mathrm{GL}(V)$ which satisfies $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ and $\rho(e) = \mathrm{Id}_V$. The **character** $\chi_\rho\colon G \to \mathbb{C}$ is defined by $g \mapsto \mathrm{Tr}(\rho(g))$. Equivalently, $\chi_\rho(g)$ is the sum of the eigenvalues of $\rho(g)$, counted with multiplicity. It is invariant under G-conjugacy. That is, it is a class function. Let $\mathbb{C}(G) = \{f\colon G \to \mathbb{C}\}$ be the vector space of functions on G of dimension $|G|$, define the inner product

$$\langle \varphi, \psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}.$$

Definition 12.1. Let $\rho\colon G \to \mathrm{GL}(V)$ be a representation. A linear subspace $W \subset V$ is called a **subrepresentation** of ρ if $\rho(g)W \subset W$ for all $g \in G$. ρ is called **irreducible** if it has no nontrivial subrepresentation.

Define $\mathbb{C}[G] = \left\{ \sum_{g \in G} a_g g \mid a_g \in \mathbb{C} \right\}$, which is called the **group algebra**. If $x = \sum_{g \in G} a_g g$ and $y = \sum_{h \in G} b_h h$, then $xy = \sum_{g,h \in G} a_g b_h (gh)$. This makes $\mathbb{C}[G]$ an algebra. For $x \in G$, define $L_x\colon \mathbb{C}[G] \to \mathbb{C}[G]$ by $y \mapsto xy$, then $G \to \mathrm{GL}(\mathbb{C}[G])$ given by $x \mapsto L_x$ is a representation, called the **left regular representation**. On the other hand, let $\rho\colon G \to \mathrm{GL}(V)$, then V becomes a $\mathbb{C}[G]$-module by $\left(\sum_{g \in G} a_g g \right) \cdot v = \sum_{g \in G} a_g \rho(g) v$. Consequently, the representation of G has $\mathbb{C}[G]$-module structure; and every $\mathbb{C}[G]$-module gives a representation of G.

Proposition 12.1. 1) Let $W \subset V$ be a subrepresentation, then there exists a subrepresentation W' of V such that $V = W \oplus W'$. In particular, any representation can be decomposed as direct sum of irreducible representations.

2) Let ρ, ρ' be irreducible representations, then

$$\langle \chi_\rho, \chi_{\rho'} \rangle_G = \begin{cases} 1 & \text{if } \rho = \rho', \\ 0 & \text{if } \rho \neq \rho'. \end{cases}$$

Thus $V = \bigoplus_{\rho' \in \mathrm{Irr}(G)} \rho^{\oplus \langle \chi_\rho, \chi_{\rho'} \rangle_G}$.

3) $\mathbb{C}[G] = \bigoplus_{\rho \in \mathrm{Irr}(G)} \rho^{\oplus \dim(\rho)}$.

For a subgroup $H < G$, a representation $\rho_H \colon H \to \mathrm{GL}(W)$, define the **induced representation** $\mathrm{Ind}_H^G \rho_H$ as $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$. Here $gh \otimes w = g \otimes \rho_H(h)w$ for $g \in G, h \in H$ and $w \in W$. The $\mathbb{C}[G]$-module action is given by $b \cdot (x \otimes w) = (bx) \otimes w$, where $b, x \in \mathbb{C}[G]$ and $w \in W$.

Theorem 12.1 (Frobenius reciprocity)**.** Let ρ be a representation of G, ρ_H a representation of H, then

$$\mathrm{Hom}_G\left(\mathrm{Ind}_H^G \rho_H, V_G\right) = \mathrm{Hom}_H(V_H, V_G),$$

which implies that

$$\left\langle \chi_{\mathrm{Ind}_H^G \rho_H}, \chi_\rho \right\rangle_G = \langle \chi_{\rho_H}, \chi_\rho \rangle_H .$$

13 Artin L-function

Let L/K be a finite Galois extension of Galois group G. For a representation $\rho\colon G \to \mathrm{GL}(V)$, where V is a finite dimensional $\mathbb{C}$-vector space, define the **Artin L-function** as

$$L(s, \rho, L/K) = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \det\left(\mathrm{Id} - \rho(\mathrm{Fr}_\mathfrak{p})\, \mathrm{N}(\mathfrak{p})^{-s}, V^{I_\mathfrak{p}}\right)^{-1}$$

Lemma 13.1. For a matrix $A \in \mathrm{M}_{n\times n}(\mathbb{C})$,

$$\log\det(\mathrm{Id} - At) = -\sum_{n=1}^{+\infty} \frac{\mathrm{Tr}(A^n)t^n}{n}.$$

Proof. Let $A \in \mathrm{M}_{n\times n}(\mathbb{C})$, since $\mathbb{C}$ is algebraically closed, there exists invertible matrix P such that $PAP^{-1} = T$ is an upper triangular matrix. Let $\lambda_1, \cdots, \lambda_m$ be the diagonal entries of T, they are precisely eigenvalues of A. Therefore,

$$\det(\mathrm{Id} - At) = \det(\mathrm{Id} - Tt) = \prod_{i=1}^{m}(1 - \lambda_i t),$$

$$\mathrm{Tr}(A^r) = \mathrm{Tr}(T^r) = \sum_{i=1}^{m} \lambda_i^r.$$

When $|t|$ sufficiently small, $|\lambda_i t| < 1$ for all i, so

$$\log\det(\mathrm{Id} - At) = \sum_{i=1}^{m} \log(1-\lambda_i t) = -\sum_{i=1}^{m}\sum_{n=1}^{\infty} \frac{\lambda_i^n t^n}{n} = -\sum_{n=1}^{+\infty}\sum_{i=1}^{m} \frac{\lambda_i^n t^n}{n} = -\sum_{n=1}^{\infty} \frac{\mathrm{Tr}(A^n)t^n}{n}.$$

□

Proposition 13.1. $L(s,\rho,L/K)$ is absolutely convergent for $\mathrm{Re}(s) > 1$.

Proof. Take log of the RHS, get

$$-\sum_{\mathfrak{p}\subset\mathcal{O}_K} \log\det\left(\mathrm{Id} - \rho(\mathrm{Fr}_{\mathfrak{p}})\,\mathrm{N}(\mathfrak{p})^{-s}, V^{I_{\mathfrak{p}}}\right) = \sum_{\mathfrak{p}\subset\mathcal{O}_K}\sum_{n=1}^{+\infty} \frac{\mathrm{Tr}\left(\rho\left(\mathrm{Fr}_{\mathfrak{p}}\right)^n, V^{I_{\mathfrak{p}}}\right)}{n\,\mathrm{N}(\mathfrak{p})^{ns}}.$$

From $d := \dim_{\mathbb{C}} V < +\infty$, $\rho(g)$ is of finite order, whose eigenvalues are all unity roots. Therefore

$$\mathrm{Tr}\left(\rho\left(\mathrm{Fr}_{\mathfrak{p}}\right)^n, V^{I_{\mathfrak{p}}}\right) \le \dim V^{I_{\mathfrak{p}}} \le \dim V = d.$$

Consequently,

$$\sum_{\mathfrak{p}\subset\mathcal{O}_K}\sum_{n=1}^{+\infty} \left|\frac{\mathrm{Tr}\left(\rho\left(\mathrm{Fr}_{\mathfrak{p}}\right)^n, V^{I_{\mathfrak{p}}}\right)}{n\,\mathrm{N}(\mathfrak{p})^{ns}}\right| \le d \sum_{\mathfrak{p}\subset\mathcal{O}_K}\sum_{n=1}^{+\infty} \frac{1}{n\,\mathrm{N}(\mathfrak{p})^{n\,\mathrm{Re}(s)}},$$

which converges as $\mathrm{Re}(s) > 1$. □

Theorem 13.1. Let L/K be a finite Galois extension of Galois group G, then

1) Let ρ_1, ρ_2 be representations of G, then

$$L(s, \rho_1 \oplus \rho_2, L/K) = L(s,\rho_1,L/K)L(s,\rho_2,L/K).$$

2) Let $H \triangleleft G$, $M = L^H$, let ρ be a representation of G/H, viewed as representation of G, then

$$L(s,\rho,L/K) = L(s,\rho,M/K).$$

3) Let $H < G$, let ρ_H be a representation of H, then

$$L\left(s, \mathrm{Ind}_H^G \rho_H, L/K\right) = L(s,\rho_H, L/M).$$

Proof. 1) Clearly $(V_1 \oplus V_2)^{I_{\mathfrak{p}}} = V_1^{I_{\mathfrak{p}}} \oplus V_2^{I_{\mathfrak{p}}}$. So $(\rho_1\oplus\rho_2)(\mathrm{Fr}_{\mathfrak{p}})|_{V_1^{I_{\mathfrak{p}}}\oplus V_2^{I_{\mathfrak{p}}}} = \rho_1(\mathrm{Fr}_{\mathfrak{p}})|_{V_1^{I_{\mathfrak{p}}}} \oplus \rho_2(\mathrm{Fr}_{\mathfrak{p}})|_{V_2^{I_{\mathfrak{p}}}}$. We can deduce

$$\det\left(\mathrm{Id} - (\rho_1\oplus\rho_2)(\mathrm{Fr}_{\mathfrak{p}})\,\mathrm{N}(\mathfrak{p})^{-s}, (V_1\oplus V_2)^{I_{\mathfrak{p}}}\right) = \det\left(\mathrm{Id} - \rho_1(\mathrm{Fr}_{\mathfrak{p}})\,\mathrm{N}(\mathfrak{p})^{-s}, V_1^{I_{\mathfrak{p}}}\right)\det\left(\mathrm{Id} - \rho_2(\mathrm{Fr}_{\mathfrak{p}})\,\mathrm{N}(\mathfrak{p})^{-s}, V_2^{I_{\mathfrak{p}}}\right).$$

Taking the product over all $\mathfrak{p} \subset \mathcal{O}_K$, we obtain

$$L(s, \rho_1 \oplus \rho_2, L/K) = L(s,\rho_1,L/K)L(s,\rho_2,L/K).$$

2) Take nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. Let $\mathfrak{P} \subset \mathcal{O}_L$ satisfy $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Let $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M$. Recall that $D_{\mathfrak{P}}(L/K) = \{g \in G : g\mathfrak{P} = \mathfrak{P}\}$, $I_{\mathfrak{P}} = \mathrm{Ker}\left(D_{\mathfrak{P}}(L/K) \to \mathrm{Aut}_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{P})\right)$, $D_{\mathfrak{q}}(M/K) = \{g \in \mathrm{Gal}(M/K) : g\mathfrak{q} = \mathfrak{q}\}$, $I_{\mathfrak{q}} = \mathrm{Ker}\left(D_{\mathfrak{q}}(M/K) \to \mathrm{Aut}_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_M/\mathfrak{q})\right)$. From $\mathrm{Gal}(M/K) = G/H$, $D_{\mathfrak{q}}$ and $I_{\mathfrak{q}}$ can be regraded as subgroup of G/H. $H \triangleleft G$ implies that M/K is Galois.

To begin with we prove $\pi(D_{\mathfrak{P}}(L/K)) = D_{\mathfrak{q}}(M/K)$, where $\pi\colon G \to G/H$ is natural projection. For arbitrary $g \in D_{\mathfrak{P}}(L/K)$, we have $g\mathfrak{P} = \mathfrak{P}$, so $\pi(g)\mathfrak{q} = g(\mathfrak{P} \cap \mathcal{O}_M) = g\mathfrak{P} \cap g\mathcal{O}_M = \mathfrak{P} \cap \mathcal{O}_M = \mathfrak{q}$. So $\pi(g) \in D_{\mathfrak{q}}(M/K)$. That is, $\pi(D_{\mathfrak{P}}(L/K)) \subset D_{\mathfrak{q}}(M/K)$. Now for arbitrary $\overline{g} \in D_{\mathfrak{q}}(M/K) \subset G/H$, one can choose a representative $g \in G$ such that $\pi(g) = \overline{g}$. Since $\overline{g}\mathfrak{q} = \mathfrak{q}$, we have $g\mathfrak{q} = \mathfrak{q}$. Moreover $g\mathfrak{P} \cap \mathcal{O}_M = g(\mathfrak{P} \cap \mathcal{O}_M) = g\mathfrak{q} = \mathfrak{q}$. Thanks to Proposition 7.1, there exists $h \in H$ such that $h(g\mathfrak{P}) = \mathfrak{P}$, which implies that $hg \in D_{\mathfrak{P}}(L/K)$. And $\pi(hg) = \pi(g) = \overline{g}$. This implies that $\pi(D_{\mathfrak{P}}(L/K)) \supset D_{\mathfrak{q}}(M/K)$. We conclude that $\pi(D_{\mathfrak{P}}(L/K)) = D_{\mathfrak{q}}(M/K)$.

Next we prove $\pi(I_{\mathfrak{P}}(L/K)) = I_{\mathfrak{q}}(M/K)$. For arbitrary $g \in I_{\mathfrak{P}}(L/K)$, we have $g(x) \equiv x \bmod \mathfrak{P}$, which is equivalent to $g(x) - x \in \mathfrak{P}$. Thus $g(x) - x \in \mathfrak{P} \cap \mathcal{O}_M = \mathfrak{q}$, $g(x) \equiv x \bmod \mathfrak{q}$. So $\pi(g) \in I_{\mathfrak{q}}(M/K)$, we obtain $\pi(I_{\mathfrak{P}}(L/K)) \subset I_{\mathfrak{q}}(M/K)$. Take $\overline{g} \in I_{\mathfrak{q}}(M/K)$, there exists $g \in D_{\mathfrak{P}}(L/K)$ such that $\pi(g) = \overline{g}$. $g \in D_{\mathfrak{P}}(L/K)$ and $\overline{g} \in I_{\mathfrak{q}}(M/K)$ implies that $g\mathfrak{P} = \mathfrak{P}$ implies that g induces $\widetilde{g} \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_M/\mathfrak{q}))$. Here $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_M/\mathfrak{q})$ is extension of finite fields, hence Galois. Thanks to Proposition 7.2, there exists $h \in H \cap D_{\mathfrak{P}}(L/K)$ such that $\widetilde{g}^{-1}$ is the image of h under $D_{\mathfrak{P}}(L/M) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_M/\mathfrak{q}))$. Hence hg acts trivially on $\mathcal{O}_L/\mathfrak{P}$, i.e., $hg \in I_{\mathfrak{P}}(L/K)$. On the other hand $\pi(hg) = \pi(g) = \overline{g}$. Thus we get $I_{\mathfrak{q}}(M/K) \subset \pi(I_{\mathfrak{P}}(L/K))$. Consequently $\pi(I_{\mathfrak{P}}(L/K)) = I_{\mathfrak{q}}(M/K)$.

Now clearly we have $\pi(\mathrm{Fr}_{\mathfrak{P}}(L/K)) = \mathrm{Fr}_{\mathfrak{q}}(M/K)$ and $V^{I_{\mathfrak{P}}(L/K)} = V^{I_{\mathfrak{q}}(M/K)}$. Moreover $\rho(\mathrm{Fr}_{\mathfrak{P}}(L/K)) = \rho(\mathrm{Fr}_{\mathfrak{q}}(M/K))$. We finish the proof.

□

Theorem 13.2 (Artin)**.** Let $K/\mathbb{Q}$ be a finite Galois extension of Galois group G, then

$$\zeta_K(s) = \prod_{\rho \in \mathrm{Irr}(G)} L(s, \rho, K/\mathbb{Q})^{\dim(\rho)} = \zeta(s) \prod_{\substack{\rho \in \mathrm{Irr}(G) \\ \rho \neq \mathrm{triv}}} L(s, \rho, K/\mathbb{Q})^{\dim(\rho)}$$

Proof.

$$\prod_{\rho \in \mathrm{Irr}(G)} L(s, \rho, K/\mathbb{Q})^{\dim(\rho)} = L(s, \mathrm{Ind}_{\{1\}}^{G} \mathrm{triv}, K/\mathbb{Q}) = L(s, \mathrm{triv}, K/\mathbb{Q}) = L(s, \mathrm{triv}, K/K) = \zeta_K(s).$$

□

Theorem 13.3 (Brauer)**.** Let G be a finite group, $\rho\colon G \to \mathrm{GL}(V)$ a representation, then there exists finitely many subgroups $H_i < G$ and characters $\chi_i\colon H_i \to \mathbb{C}^\times$, $i = 1, \cdots, r$ such that

$$\chi_\rho = \sum_{i=1}^{r} n_i \operatorname{Ind}_{H_i}^{G} \chi_i$$

for some $n_i \in \mathbb{Z}$.

Corollary 13.1. Let L/K be a finite Galois extension of Galois group G, with the above notations, let $M_i = L^{H_i}$, $L_i = L^{\mathrm{Ker}(\chi_i)}$, then

$$L(s, \rho, L/K) = \prod_{i=1}^{r} L(s, \chi_i, L_i/M_i)^{n_i}$$

Proof.

$$L(s, \rho, L/K) = \prod_{i=1}^{r} L(s, \operatorname{Ind}_H^G \chi_i, L/K)^{n_i} = \prod_{i=1}^{r} L(s, \chi_i, L/M_i)^{n_i} = \prod_{i=1}^{r} L(s, \chi_i, L_i/M_i)^{n_i}.$$

□

Theorem 13.4. Let L/K be a finite abelian extension of Galois group G, let $\chi\colon G \to \mathrm{U}(1)$ is a nontrivial character, then $L(s, \chi, L/K)$ extends to a holomorphic function on $\mathbb{C}$, which admits a functional equation.

Sketch of Proof. Through class field theory, every character $\chi\colon G \to \mathrm{U}(1)$ corresponds to a Hecke character of K. The Artin L-function $L(s, \chi, L/K)$ is equal to the corresponding Hecke L-function. Hecke L-function admits meromorphic continuation and functional equation. If χ is nontrivial, $L(s, \chi, L/K)$ is entire; if χ is trivial, we get Dedekind zeta function with simple pole $s = 1$. □

14 $\mathbb{A}_{\mathbb{Q}}$ and $\mathbb{A}_{\mathbb{Q}}^{\times}$

Recall $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n$. Then

$$\varprojlim_n \mathbb{Z}/n = \varprojlim_{n = p_1^{n_1} \cdots p_r^{n_r}} \mathbb{Z}/p_1^{n_1} \oplus \cdots \oplus \mathbb{Z}/p_r^{n_r} = \prod_{p \text{ prime}} \mathbb{Z}_p =: \widehat{\mathbb{Z}}.$$

Define

$$\mathbb{A}_{\mathbb{Q},f} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} = \left\{ (x_2, x_3, x_5, \cdots) \in \prod_{p \text{ prime}} \mathbb{Q}_p \mid x_p \in \mathbb{Z}_p \text{ for all but finitely many } p \right\}.$$

Indeed, since $\mathbb{Q} = (\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z}$, one get $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} = (\mathbb{Z} \setminus \{0\})^{-1}\widehat{\mathbb{Z}}$, so element in $\mathbb{A}_{\mathbb{Q},f}$ can be written as a/N, where $a = (a_p)_p \in \prod_p \mathbb{Z}_p$ and $N \in \mathbb{Z} \setminus \{0\}$. If $p \nmid N$, $N \in \mathbb{Z}_p^\times$, so $a_p/N \in \mathbb{Z}_p$. But such there are only finitely many p with $p \mid N$. On the other hand, given $x = (x_p)_p \in \prod_p \mathbb{Q}_p$ with $x_p \in \mathbb{Z}_p$ for all but finitely many p, we can choose $N = \prod_{x_p \notin \mathbb{Z}_p} p^{n_p}$. Then $Nx_p \in \mathbb{Z}_p$ for all p, which implies that $x = Nx/N \in \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{A}_{\mathbb{Q},f}$.

Let $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \mathbb{A}_{\mathbb{Q},f}$, call it the ring of **adèles** of $\mathbb{Q}$.

$$\mathbb{A}_{\mathbb{Q}} = \left\{ (x_\infty, x_2, x_3, x_5, \cdots) \in \mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Q}_p \mid x_p \in \mathbb{Z}_p \text{ for all but finitely many } p \right\}.$$

Let $|\mathbb{Q}| = \{\infty, 2, 3, 5, \cdots\}$, $\mathbb{A}_{\mathbb{Q}}$ has a basis of topology of the form

$$\prod_{\substack{v \in S \\ S \subset |\mathbb{Q}|, |S| < +\infty}} U_v \times \prod_{v \in |\mathbb{Q}| - S} \mathbb{Z}_p.$$

$(\mathbb{A}_{\mathbb{Q}}, +, \times)$ is a topological ring. Indeed, let $U_\infty \times \prod_{p \in S} U_v \times \prod_{p \notin S} \mathbb{Z}_p$ where $|S| < +\infty$, $0 \in U_\infty \subset \mathbb{R}$ open and $0 \in U_p \subset \mathbb{Q}_p$ open. Then there exists $0 \in V_\infty \subset \mathbb{R}$ such that $V_\infty + V_\infty \subset U_\infty$ and $0 \in V_p \subset \mathbb{Q}_p$ such that $V_p + V_p \subset U_p$ for all $p \in S$. Let $V = V_\infty \times \prod_{p \in S} V_p \times \prod_{p \notin S} \mathbb{Z}_p$, then V is a open neighborhood of 0 and $V + V \subset U$. Thus $+$ is continuous at 0. $-U$ is also open since $-U_\infty$ is open in $\mathbb{R}$ and $-U_p$ is open in $\mathbb{Q}_p$. Taking the additive inverse is continuous. Similarly multiplication is continuous.

Consider $\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}$ defined by $x \mapsto (x, x, \cdots)$. It is well-defined since if we can write $x = a/b$, $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, there are only finitely many p with $p \mid b$, i.e., there are only finitely many p with $x \notin \mathbb{Z}_p$.

Proposition 14.1 (Weak approximation)**.** $\mathbb{Q}$ is dense in $\mathbb{A}_{\mathbb{Q},f}$.

Proof. For $x = (x_\infty, x_2, x_3, x_5, \cdots) \in \mathbb{A}_{\mathbb{Q},f}$, let $S \subset |\mathbb{Q}|_f$ be finite set of places, let $U = \prod_{p \in S} U_p \times \prod_{p \notin S} \mathbb{Z}_p$. Need to find element in $(x + U) \cap \mathbb{Q}$. By definition, there are finitely many p with $x_p \notin \mathbb{Z}_p$. For such p, one can choose $n_p \geq 1$ such that $p^{n_p} x_p \in \mathbb{Z}_p$. Moreover choose $r_p \in \mathbb{Z}$ such that $r_p \equiv p^{n_p} x_p \bmod p^{n_p}\mathbb{Z}_p$. (More precisely, one can choose the n_p-th component of $p^{n_p} x_p$.) It follows that $x_p - \frac{r_p}{p^{n_p}} \in \mathbb{Z}_p$. Let $c = \sum_{x_p \notin \mathbb{Z}_p} \frac{r_p}{p^{n_p}} \in \mathbb{Q}$, then $x - c \in \widehat{\mathbb{Z}}$. This implies that $\mathbb{A}_{\mathbb{Q},f} = \mathbb{Q} + \widehat{\mathbb{Z}}$.

Therefore only need to prove $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$. That is, if we can find $m \in \mathbb{Z}$ such that $m \in (x - c) + U$, then $c + m \in (x + U) \cap \mathbb{Q}$. Let $x' = (x'_2, x'_3, \cdots) \in \prod_p \mathbb{Z}_p$. Need to find $m \in \mathbb{Z}$ such that $m - x'_p \in U_p$ for all $p \in S$ and $m - x'_p \in \mathbb{Z}_p$ for all $p \notin S$. Since $x'_p \in \mathbb{Z}_p$, for $m \in \mathbb{Z}$ we must have $m - x'_p \in \mathbb{Z}_p$. U_p is open neighborhood of 0, there exists $a_p \geq 1$ such that $p^{a_p}\mathbb{Z}_p \subset U_p$, then it suffices to find $m \in \mathbb{Z}$ such that $m - x'_p \in p^{a_p}\mathbb{Z}_p$ for all $p \in S$. One can choose $t_p \in \mathbb{Z}$ with $t_p \equiv x'_p \bmod p^{a_p}\mathbb{Z}_p$, so only need to find $m \in \mathbb{Z}$ such that $m \equiv t_p \bmod p^{a_p}$ for all $p \in S$. It is OK by the Chinese Remainder Theorem. $\square$

Proposition 14.2 (Strong approximation)**.** $\mathbb{Q}$ is discrete and cocompact (i.e., $\mathbb{Q}\backslash\mathbb{A}_{\mathbb{Q}}$ is compact) in $\mathbb{A}_{\mathbb{Q}}$.

Proof. Take $V = \left(-\frac{1}{2}, \frac{1}{2}\right) \times \prod_p \mathbb{Z}_p$. If $q \in \mathbb{Q} \cap V$, then $q \in \mathbb{Q} \cap \bigcap_p \mathbb{Z}_p = \mathbb{Z}$, which forces $q = 0$. Thus $\mathbb{Q}$ is discrete in $\mathbb{A}_{\mathbb{Q}}$.

For $x = (x_v)_{v \in |\mathbb{Q}|} \in \mathbb{A}_{\mathbb{Q}}$, there is only finitely many places where $x_p \notin \mathbb{Z}_p$, so there exists $c \in \mathbb{Q}$ such that $x - c \in \mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p$. This implies that

$$\mathbb{A}_{\mathbb{Q}} = \mathbb{Q} + \left(\mathbb{R} \times \prod_{p \text{ primes}} \mathbb{Z}_p\right),$$

so

$$\mathbb{Q}\backslash\mathbb{A}_{\mathbb{Q}} = \mathbb{Q}\backslash\mathbb{Q} + \left(\mathbb{R} \times \prod_{p \text{ primes}} \mathbb{Z}_p\right) = \left(\mathbb{Q} \cap \mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p\right) \backslash \left(\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p\right) = \mathbb{Z}\backslash \left(\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p\right).$$

Projection to the first component, get homomorphism $\mathbb{Z}\backslash\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p \to \mathbb{Z}\backslash\mathbb{R}$ with kernel $\prod_{p \text{ prime}} \mathbb{Z}_p$. One get continuous surjection $[0,1] \times \prod_{p \text{ prime}} \mathbb{Z}_p \to \mathbb{Z}\backslash\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p$. Note that it is restriction of $\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p \to \mathbb{Z}\backslash\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p$, so it is continuous. $[0,1]$ is bounded and closed then compact, $\prod_{p \text{ prime}} \mathbb{Z}_p$ is compact by Tychonoff Theorem. Therefore $\mathbb{Q}\backslash\mathbb{A}_{\mathbb{Q}} = \mathbb{Z}\backslash\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p$, as the continuous image of compact set, is compact. $\square$

Let $\mathbb{A}_{\mathbb{Q}}^\times$ be the group of invertible elements in $\mathbb{A}_{\mathbb{Q}}$, called the group of **idèles** of $\mathbb{Q}$. Explictly,

$$\begin{aligned} \mathbb{A}_{\mathbb{Q}}^\times &= \left\{(x_\infty, x_2, x_3, x_5, \cdots) \in \mathbb{R}^\times \times \prod_{p \text{ prime}} \mathbb{Q}_p^\times \mid x_p \in \mathbb{Z}_p, x_p^{-1} \in \mathbb{Z}_p \text{ for all but finitely many } p\right\} \\ &= \left\{(x_\infty, x_2, x_3, x_5, \cdots) \in \mathbb{R}^\times \times \prod_{p \text{ prime}} \mathbb{Q}_p^\times \mid x_p \in \mathbb{Z}_p^\times \text{ for all but finitely many } p\right\}. \end{aligned}$$

Attention: Consider $\mathbb{A}_{\mathbb{Q}}^\times$ with the induced topology from $\mathbb{A}_{\mathbb{Q}}$, then the inverse $\iota \colon \mathbb{A}_{\mathbb{Q}}^\times \to \mathbb{A}_{\mathbb{Q}}^\times$ defined by $x \mapsto x^{-1}$ is NOT continuous! Let p_n be the n-th prime number, define $x^{(n)} = \left(x_\infty^{(n)}, x_2^{(n)}, x_3^{(n)}, \cdots\right)$ by $x_\infty^{(n)} = 1$, $x_{p_n}^{(n)} = p_n$ and $x_q^{(n)} = 1$ for all primes $q \neq p_n$. Let $U_\infty \times \prod_{p \in S} U_p \times \prod_{p \notin S} \mathbb{Z}_p$ be a open neighborhood of 1, here $|S| < +\infty$, $1 \in U_\infty$ and $1 \in U_p$ for all $p \in S$. Then $p_n \notin S$ for n sufficiently large, one get $x^{(n)} \to 1$ under the topology of $\mathbb{A}_{\mathbb{Q}}$. However,

$\left(x^{(n)}\right)^{-1} \notin \mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p$ since its p_n-th component is p_n^{-1}. Note that $\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p$ is open neighborhood of 1. So $\left(x^{(n)}\right)^{-1} \not\to 1$.

Consider the embedding $\mathbb{A}_{\mathbb{Q}}^{\times} \hookrightarrow \mathbb{A}_{\mathbb{Q}} \times \mathbb{A}_{\mathbb{Q}}$ defined by $x \mapsto (x, x^{-1})$ for $\left(\mathbb{A}_{\mathbb{Q}}^{\times}, \times\right)$ to be a topological group, it is enough to take restriction of topology on $\mathbb{A}_{\mathbb{Q}} \times \mathbb{A}_{\mathbb{Q}}$ by the embedding ι. That is, $V \subset \mathbb{A}_{\mathbb{Q}}^{\times}$ open iff there exists open $W \subset \mathbb{A}_{\mathbb{Q}} \times \mathbb{A}_{\mathbb{Q}}$ such that $V = \iota^{-1}(W)$. Then one can get the topology of $\mathbb{A}_{\mathbb{Q}}^{\times}$ is generated by the set of open subsets of the form

$$U_\infty \times \prod_{p \in S} (1 + p^{a_p}\mathbb{Z}_p) \times \prod_{p \notin S} \mathbb{Z}_p^{\times},$$

$U_\infty \subset \mathbb{R}$ open containing 1. Indeed, recall that the basis of topology of $\mathbb{A}_{\mathbb{Q}}$ has the form $U_\infty \times \prod_{p \in S} U_p \times \prod_{p \notin S} \mathbb{Z}_p$. Let $W_1 \times W_2 = \left(U_\infty^{(1)} \times \prod_{p \in S_1} U_p^{(1)} \times \prod_{p \notin S_1} \mathbb{Z}_p\right) \times \left(U_\infty^{(2)} \times \prod_{p \in S_2} U_p^{(2)} \times \prod_{p \notin S_2} \mathbb{Z}_p\right)$ be an open neighborhood of $(1,1)$. If $\iota(x) = \left(x, x^{-1}\right) \in W_1 \times W_2$, then $x_p \in \mathbb{Z}_p^{\times}$ for $p \notin S = S_1 \cup S_2$. On the other hand, for $p \in S$, we have $x_p \in U_p^{(1)}$ and $x_p^{-1} \in U_p^{(2)}$ (if $p \notin S_1$, $U_p^{(1)} = \mathbb{Z}_p$; if $p \notin S_2$, $U_p^{(2)} = \mathbb{Z}_p$). Since $U_p^{(1)}, U_p^{(2)} \subset \mathbb{Q}_p$ open, there exists $a_p \geq 1$ such that $1 + p^{a_p}\mathbb{Z}_p \subset U_p^{(1)} \cap U_p^{(2)}$. We claim that $(1 + p^{a_p}\mathbb{Z}_p)^{-1} = 1 + p^{a_p}\mathbb{Z}_p$. For arbitrary $x_p \in \mathbb{Z}_p$, $1 + p^{a_p}x_p \equiv 1 \bmod p\mathbb{Z}_p$ since $a_p \geq 1$. Then $1 + p^{a_p}x_p \in \mathbb{Z}_p^{\times}$, $(1 + p^{a_p}x_p)^{-1} \in \mathbb{Z}_p^{\times} \subset \mathbb{Z}_p$. Moreover $(1 + p^{a_p}x_p)^{-1} - 1 = \frac{1-(1+p^{a_p}x_p)}{1+p^{a_p}x_p} = -p^{a_p}x_p(1 + p^{a_p}x_p)^{-1} \in p^{a_p}\mathbb{Z}_p$. One get $(1 + p^{a_p}x_p)^{-1} \in 1 + p^{a_p}\mathbb{Z}_p$. Therefore $(1 + p^{a_p}\mathbb{Z}_p)^{-1} \subset 1 + p^{a_p}\mathbb{Z}_p$. It then follows that $(1 + p^{a_p}\mathbb{Z}_p)^{-1} = 1 + p^{a_p}\mathbb{Z}_p$. Therefore $x_p \in 1 + p^{a_p}\mathbb{Z}_p \subset U_p^{(1)} \cap U_p^{(2)}$ implies that $x_p^{-1} \in U_p^{(1)} \cap U_p^{(2)}$. Also we can choose $U_\infty = U_\infty^{(1)} \cap \left\{x_\infty \in \mathbb{R}^{\times} \mid x_\infty^{-1} \in U_\infty^{(2)}\right\}$. Consequently, $U_\infty \times \prod_{p \in S}(1 + p^{a_p}\mathbb{Z}_p) \times \prod_{p \notin S} \mathbb{Z}_p^{\times} \subset \iota^{-1}(W_1 \times W_2)$. For the converse, given $U_\infty \times \prod_{p \in S}(1 + p^{a_p}\mathbb{Z}_p) \times \prod_{p \notin S} \mathbb{Z}_p^{\times}$, one can choose $W_1 = U_\infty \times \prod_{p \in S}(1 + p^{a_p}\mathbb{Z}_p) \times \prod_{p \notin S} \mathbb{Z}_p$ and $W_2 = \mathbb{R} \times \prod_{p \in S}(1 + p^{a_p}\mathbb{Z}_p) \times \prod_{p \notin S} \mathbb{Z}_p$ making $\iota^{-1}(W_1 \times W_2) = U_\infty \times \prod_{p \in S}(1 + p^{a_p}\mathbb{Z}_p) \times \prod_{p \notin S} \mathbb{Z}_p^{\times}$, so $U_\infty \times \prod_{p \in S}(1 + p^{a_p}\mathbb{Z}_p) \times \prod_{p \notin S} \mathbb{Z}_p^{\times}$ is precisely open. We conclude that the topology of $\mathbb{A}_{\mathbb{Q}}^{\times}$ is generated by the set of open subsets of the form

$$U_\infty \times \prod_{p \in S} (1 + p^{a_p}\mathbb{Z}_p) \times \prod_{p \notin S} \mathbb{Z}_p^{\times},$$

$U_\infty \subset \mathbb{R}$ open containing 1.

Consider $\mathbb{Q}^{\times} \hookrightarrow \mathbb{A}_{\mathbb{Q}}^{\times}$ defined by $x \mapsto (x, x, \cdots)$. Define $\|\cdot\|_{\mathbb{Q}} \colon \mathbb{A}_{\mathbb{Q}}^{\times} \to \mathbb{R}_+$ defined by $(x_v)_{v \in |\mathbb{Q}|} \mapsto |x_\infty| \times \prod_{p \text{ prime}} |x_p|_p$. Note that $x_p \in \mathbb{Z}_p^{\times}$ iff $|x_p|_p = 1$, it is well-defined. It is a group homomorphism.

Theorem 14.1 (Product formula)**.** For arbitrary $x \in \mathbb{Q}^{\times}$, $\|x\|_{\mathbb{Q}} = |x|_\infty \times \prod_{p \text{ prime}} |x|_p = 1$.

Proof. $\|\cdot\|_{\mathbb{Q}}$ is multiplicative, and number in $\mathbb{Q}^{\times}$ can be factored as product of prime numbers, it is enough to verify for $x = p$. $\|p\|_{\mathbb{Q}} = |p|_\infty \prod_{\ell \text{ prime}} |p|_\ell = p \times p^{-1} = 1$. $\square$

Let $\mathbb{A}_{\mathbb{Q}}^{\times,1} = \left\{x = (x_v) \in \mathbb{A}_{\mathbb{Q}}^{\times} \mid \|x\|_{\mathbb{Q}} = 1\right\} \leq \mathbb{A}_{\mathbb{Q}}^{\times}$, then $\mathbb{Q}^{\times} \hookrightarrow \mathbb{A}_{\mathbb{Q}}^{\times,1}$.

Proposition 14.3. $\mathbb{Q}^{\times}$ is discrete and cocompact in $\mathbb{A}_{\mathbb{Q}}^{\times,1}$.

Proof. Discrete only need to find U containing 1 in $\mathbb{A}_{\mathbb{Q}}^{\times,1}$ such that $U \cap \mathbb{Q}^{\times} = \{1\}$. Let $U_{\infty} = \left(\frac{1}{2}, \frac{3}{2}\right)$, set $U = \left(U_{\infty} \times \prod_{p \text{ prime}} \mathbb{Z}_p^{\times}\right) \cap \mathbb{A}_{\mathbb{Q}}^{\times,1}$. Assume that $x \in U \cap \mathbb{Q}^{\times}$, it follows that $x \in U_{\infty}$ and $x \in \mathbb{Z}_p^{\times}$. Write $x = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. If there exists prime $p \mid b$, then $x \notin \mathbb{Z}_p$, a contradiction. Thus $b = \pm 1$, which implies that $x \in \mathbb{Z}$. If there exists prime $p \mid x$, then $x \in p\mathbb{Z}_p$, contradicts to $x \in \mathbb{Z}_p^{\times}$. Thus $x = \pm 1$. Combine $x \in \left(\frac{1}{2}, \frac{3}{2}\right)$ get $x = 1$. Therefore $U \cap \mathbb{Q}^{\times} = \{1\}$. Indeed, above proof shows that $\mathbb{Q}^{\times}$ is discrete in $\mathbb{A}_{\mathbb{Q}}^{\times}$.

By definition, $x = (x_{\infty}, x_2, x_3, \cdots) \in \mathbb{A}_{\mathbb{Q}}^{\times,1}$, then $x_p \in \mathbb{Z}_p^{\times}$ for all but finitely many p. For finitely many p, there exists n_p such that $x_p \in p^{n_p}\mathbb{Z}_p^{\times}$. Take $c = \prod_{x_p \notin \mathbb{Z}_p^{\times}} p^{n_p} \in \mathbb{Q}^{\times}$, then $c^{-1}x_p \in \mathbb{Z}_p^{\times}$, $c^{-1}x \in \mathbb{R}^{\times} \times \prod_{p \text{ prime}} \mathbb{Z}_p^{\times}$. By the product formula, $\|c^{-1}x\|_{\mathbb{Q}} = \|c^{-1}\|_{\mathbb{Q}}\|x\|_{\mathbb{Q}} = 1 \cdot 1 = 1$. On the other hand, $c^{-1}x_p \in \mathbb{Z}_p^{\times}$ gives $\left|c^{-1}x_p\right|_p = 1$. Hence $\left|c^{-1}x_{\infty}\right|_{\infty} = 1$, that is, $c^{-1}x_{\infty} \in \{\pm 1\}$. This implies that

$$\mathbb{A}_{\mathbb{Q}}^{\times,1} = \mathbb{Q}^{\times} \times \left(\mathbb{R}^{\times} \times \prod_p \mathbb{Z}_p^{\times}\right) = \mathbb{Q}^{\times} \times \left(\{\pm 1\} \times \prod_{p \text{ prime}} \mathbb{Z}_p^{\times}\right).$$

Thus

$$\mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times,1} = \mathbb{Q}^{\times} \cap \left(\{\pm 1\} \times \prod_{p \text{ prime}} \mathbb{Z}_p^{\times}\right) \backslash \left(\{\pm 1\} \times \prod_{\text{prime}} \mathbb{Z}_p^{\times}\right) = \{\pm 1\} \backslash \left(\{\pm 1\} \times \prod_{\text{prime}} \mathbb{Z}_p^{\times}\right) = \prod_{p \text{ prime}} \mathbb{Z}_p^{\times}.$$

Let $\pi \colon \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ be natural projection, then $\mathbb{Z}_p^{\times} = \pi^{-1}(\mathbb{Z}/p\mathbb{Z})^{\times}$. Since $(\mathbb{Z}/p\mathbb{Z})^{\times} \subset \mathbb{Z}/p\mathbb{Z}$ is closed, $\mathbb{Z}_p^{\times} \subset \mathbb{Z}_p$ is closed. Recall Example 3.3, $\mathbb{Z}_p$ is compact. Therefore $\mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times,1}$ is compact by Tychonoff Theorem. □

Now let K be a finite extension of $\mathbb{Q}$, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

$$\varprojlim_{\mathfrak{a} \text{ ideal}} \mathcal{O}_K/\mathfrak{a} = \prod_{\mathfrak{p}} \widehat{\mathcal{O}_{K\mathfrak{p}}} = \prod_p \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathcal{O}_K.$$

Define

$$\mathbb{A}_{K,f} = \left(\prod_{\mathfrak{p}} \widehat{\mathcal{O}_{K\mathfrak{p}}}\right) \otimes_{\mathcal{O}_K} K = \left(\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathcal{O}_K\right) \otimes_{\mathcal{O}_K} K = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} K = \left(\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}\right) \otimes_{\mathbb{Q}} K = \mathbb{A}_{\mathbb{Q},f} \otimes_{\mathbb{Q}} K.$$

It follows that

$$\mathbb{A}_{K,f} = \left\{(x_{\mathfrak{p}})_{\mathfrak{p} \in |K|_f} \in \prod_{\mathfrak{p} \in |K|_f} K_{\mathfrak{p}} \mid x_{\mathfrak{p}} \in \widehat{\mathcal{O}_{K\mathfrak{p}}} \text{ for all but finitely many } \mathfrak{p}\right\}.$$

More precisely, since $K = (\mathcal{O}_K \setminus \{0\})^{-1}\mathcal{O}_K$, every $x \in \mathbb{A}_{K,f} = \left(\prod_{\mathfrak{p}} \widehat{\mathcal{O}_{K\mathfrak{p}}}\right) \otimes_{\mathcal{O}_K} K$ can be written as $x = \frac{a}{c}$, where $a = (a_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} \widehat{\mathcal{O}_{K\mathfrak{p}}}$ and $c \in \mathcal{O}_K \setminus \{0\}$. If $c \notin \mathfrak{p}$, then c is invertible in $\widehat{\mathcal{O}_{K\mathfrak{p}}}$, then $\frac{a_{\mathfrak{p}}}{c} \in \widehat{\mathcal{O}_{K\mathfrak{p}}}$. That is, $x_{\mathfrak{p}} \in \widehat{\mathcal{O}_{K\mathfrak{p}}}$ for all but finitely many $\mathfrak{p}$. For the converse, assume that $x = (x_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} K_{\mathfrak{p}}$ and $x_{\mathfrak{p}} \in \widehat{\mathcal{O}_{K\mathfrak{p}}}$ for all but finitely many $\mathfrak{p}$. For each $\mathfrak{p}$ with $x_{\mathfrak{p}} \notin \widehat{\mathcal{O}_{K\mathfrak{p}}}$, there exists $m_{\mathfrak{p}} \in \mathbb{Z}$ such that $x_{\mathfrak{p}} \in \mathfrak{p}^{-m_{\mathfrak{p}}}\widehat{\mathcal{O}_{K\mathfrak{p}}}$. Choose $0 \neq c \in \prod_{x_{\mathfrak{p}} \notin \widehat{\mathcal{O}_{K\mathfrak{p}}}} \mathfrak{p}^{m_{\mathfrak{p}}} \subset \mathcal{O}_K \subset \widehat{\mathcal{O}_{K\mathfrak{p}}}$, then $cx_{\mathfrak{p}} \in \widehat{\mathcal{O}_{K\mathfrak{p}}}$ for all $\mathfrak{p}$, one get $x = \frac{cx}{c} \in \left(\prod_{\mathfrak{p}} \widehat{\mathcal{O}_{K\mathfrak{p}}}\right) \otimes_{\mathcal{O}_K} K$.

Let $\mathbb{A}_{K,\infty} = \mathbb{A}_{\mathbb{Q},\infty} \otimes_{\mathbb{Q}} K = \mathbb{R} \otimes_{\mathbb{Q}} K$.

Proposition 14.4. Let $\tau_1, \cdots, \tau_r$ be all the real embeddings of K, $\tau_{r+1}, \overline{\tau_{r+1}}, \cdots, \tau_{r+s}, \overline{\tau_{r+s}}$ be all the complex embeddings of K, then $K \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{i=1}^{r} \mathbb{R} \times \prod_{j=1}^{s} \mathbb{C}$.

Proof. Since K is finite extension of $\mathbb{Q}$, then $\mathrm{char}(K) = 0$, there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. Let $f(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α, then $f(X) = f_1(X) \cdots f_r(X) f_{r+1}(X) \cdots f_{r+s}(X) \in \mathbb{R}[X]$. Here $f_i(X) = X - \tau_i(\alpha)$ for $1 \leq i \leq r$ and $f_{r+j}(X) = (X - \tau_{r+j}(\alpha))(X - \overline{\tau_{r+j}}(\alpha))$ for $1 \leq j \leq s$. It follows that

$$K \otimes_{\mathbb{Q}} \mathbb{R} = (\mathbb{Q}[X]/f(X)) \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}[X]/f(X) = \prod_{i=1}^{r} \mathbb{R}[X]/f_i(X) \times \prod_{j=1}^{s} \mathbb{R}[X]/f_{n+j}(X) = \prod_{i=1}^{r} \mathbb{R} \times \prod_{j=1}^{s} \mathbb{C}.$$

□

Define $\mathbb{A}_K = \mathbb{A}_{K,\infty} \times \mathbb{A}_{K,f}$, with topology generated by

$$\prod_{v|\infty} U_v \times \prod_{\substack{v \in S \\ |S| < +\infty}} U_v \times \prod_{v \in |K|_f - S} \widehat{\mathcal{O}_{Kv}}.$$

$(\mathbb{A}_K, +, \times)$ is a topological ring. Let $\mathbb{A}_K^{\times}$ be the group of invertible elements in $\mathbb{A}_K$, i.e.,

$$\begin{aligned}
\mathbb{A}_K^{\times} &= \left\{ (x_v)_{v \in |K|} \in \prod_{v \in |K|} K_{\mathfrak{p}}^{\times} \mid x_v \in \widehat{\mathcal{O}_{Kv}}, x_v^{-1} \in \widehat{\mathcal{O}_{Kv}} \text{ for all but finitely many } v \right\} \\
&= \left\{ (x_v)_{v \in |K|} \in \prod_{v \in |K|} K_{\mathfrak{p}}^{\times} \mid x_v \in \widehat{\mathcal{O}_{Kv}}^{\times} \text{ for all but finitely many } v \right\}
\end{aligned}$$

with topology generated by sets of the form

$$\prod_{v|\infty} U_v \times \prod_{\substack{v \in S \subset |K|_f \\ |S| < +\infty}} U_v \times \prod_{v \in |K|_f - S} \widehat{\mathcal{O}_{Kv}}^{\times}$$

where $U_v \ni 1$. Then $(\mathbb{A}_K^{\times}, \times)$ forms a topological ring.

Consider $K \hookrightarrow \mathbb{A}_K$ defined by $x \mapsto (x, x, \cdots)$.

Proposition 14.5 (Weak approximation)**.** *K is dense in $\mathbb{A}_{K,f}$.*

Proof. Let $\alpha_1, \cdots, \alpha_n$ be a basis of K as $\mathbb{Q}$-vector space, then $K = \mathbb{Q}\alpha_1 + \cdots + \mathbb{Q}\alpha_n$. It follows that $\mathbb{A}_{K,f} = \mathbb{A}_{\mathbb{Q},f} \otimes_{\mathbb{Q}} K = \mathbb{A}_{\mathbb{Q},f}^n$. Then $K \hookrightarrow \mathbb{A}_{K,f}$ can be identified as $\mathbb{Q}^n \hookrightarrow \mathbb{A}_{\mathbb{Q},f}^n$. Now use Proposition 14.1. $\square$

Proposition 14.6 (Strong approximation)**.** *K is discrete, cocompact in $\mathbb{A}_K$.*

Proof. $K \hookrightarrow \mathbb{A}_K$ can be identified as $\mathbb{Q}^n \hookrightarrow \mathbb{A}_{\mathbb{Q}}^n$. Moreover $\mathbb{Q}^n \backslash \mathbb{A}_{\mathbb{Q}}^n = (\mathbb{Q}\backslash\mathbb{A}_{\mathbb{Q}})^n$. Apply Proposition 14.2. $\square$

Consider $K^\times \hookrightarrow \mathbb{A}_K^\times$ defined by $x \mapsto (x, x, \cdots)$. Recall the proof of Proposition 14.4. For $v \in |K|$, define $|\cdot|_v \colon K^\times \to \mathbb{R}_+$ as

- $v \mid \infty$, corresponds to $\tau \colon K \hookrightarrow \mathbb{R}$, take $|x|_v = |\tau(x)|$;
- $v \mid \infty$, corresponds to $\tau \colon K \hookrightarrow \mathbb{C}$, take $|x|_v = |\tau(x)|^2$;
- $v \nmid \infty$, correspond to prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, take $|x|_v = q_v^{-\operatorname{val}_{\mathfrak{p}}(x)}$, $q_v = |\mathcal{O}_K/\mathfrak{p}|$. In particular, $x \in \widehat{\mathcal{O}_{K}}_v^\times$ iff $\operatorname{val}_{\mathfrak{p}}(x) = 0$ iff $|x|_v = 1$.

Define $\|\cdot\|_K \colon \mathbb{A}_K^\times \to \mathbb{R}_+$ by $(x_v)_{v\in|K|} \mapsto \prod_{v\in|K|} |x_v|_v$ and let $\mathbb{A}_K^{\times,1} = \{x \in \mathbb{A}_K^\times \mid \|x\|_K = 1\}$.

Theorem 14.2 (Product formula)**.** *For arbitrary $x \in K^\times$, $\|x\|_K = 1$. So $K^\times \hookrightarrow \mathbb{A}_K^{\times,1}$.*

Proof. Enough to prove it for $x \in \mathcal{O}_K \setminus \{0\}$. We have the equality

$$\prod_{v|\infty} |x|_v = \prod_{\tau\colon K\hookrightarrow\mathbb{R}} |\tau(x)| \cdot \prod_{\sigma\colon K\hookrightarrow\mathbb{C}/\sim} |\sigma(x)|^2 = \left|\operatorname{Nm}_{K/\mathbb{Q}}(x)\right| = |\mathcal{O}_K/x\mathcal{O}_K|.$$

On the other hand,

$$|\mathcal{O}_K/x\mathcal{O}_K| = \left|\prod_{\operatorname{val}_{\mathfrak{p}}(x)>0} \mathcal{O}_K/\mathfrak{p}^{\operatorname{val}_{\mathfrak{p}}(x)}\right| = \prod_{\mathfrak{p}} q_v^{\operatorname{val}_{\mathfrak{p}}(x)} = \prod_{v\nmid\infty} (|x|_v)^{-1}.$$

$\square$

Define

$$\mathbb{A}_K^\times \longrightarrow \mathbb{A}_{K,f}^\times \longrightarrow I_K, \quad (x_v)_{v\in|K|} \longmapsto (x_v)_{v\in|K|_f} \longrightarrow \prod_{\mathfrak{p}\text{ prime}} \mathfrak{p}^{\operatorname{val}_{\mathfrak{p}}(x_{\mathfrak{p}})}$$

a group homomorphism. For arbitrary $a \in K^\times$, the image of a is $\prod_{\mathfrak{p}} \mathfrak{p}^{-\operatorname{val}_{\mathfrak{p}}(a)} = a\mathcal{O}_K$. So the image of $K^\times$ in I_K is precisely P_K. Then

$$C_K \colon K^\times \backslash \mathbb{A}_K^{\times,1} \longrightarrow I_K/P_K = \operatorname{Cl}_K$$

is a group homomorphism. Furthermore it is surjective. Indeed, given $\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} + P_K \in I_K/P_K$, there are only finitely many $n_{\mathfrak{p}} \neq 0$. Choose $x_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times}$ such that $\mathrm{val}_{\mathfrak{p}}(x_{\mathfrak{p}}) = n_{\mathfrak{p}}$ for $n_{\mathfrak{p}} \neq 0$, and choose $x_{\mathfrak{p}} = 1$ for all $n_{\mathfrak{p}} = 0$. Now one can choose $(x_v)_{v|\infty}$ such that $\prod_{v|\infty} |x_v|_v = \left(\prod_{v\in|K|_f} |x_v|_v\right)^{-1}$. More precisely, choose one $v \mid \infty$ and let $x_w = 1$ for all $w \neq v$. If v correspond to $K \hookrightarrow \mathbb{R}$, let $x_v = \left(\prod_{v\in|K|_f} |x_v|_v\right)^{-1}$; if v corresponds to $K \hookrightarrow \mathbb{C}$, choose $x_v \in \mathbb{C}$ such that $|x_v|^2 = \left(\prod_{v\in|K|_f} |x_v|_v\right)^{-1}$. Consequently $x = (x_v)_{v\in|K|} \in \mathbb{A}_K^{\times,1}$ satisfies $C_K(K^\times x) = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} + P_K$. Then get short exact sequence

$$1 \longrightarrow \mathrm{Ker}(C_K) \longrightarrow K^\times \backslash \mathbb{A}_K^{\times,1} \xrightarrow{C_K} \mathrm{Cl}_K \longrightarrow 1$$

Let $\mathbb{A}_{K,\infty}^{\times,1} = \left\{x \in \mathbb{A}_{K,\infty}^{\times} \mid \prod_{v|\infty} |x_v|_v = 1\right\}$.

$$\mathrm{Ker}(C_K) = K^\times \backslash K^\times \left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}\right) = \mathcal{O}_K^\times \backslash \left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}\right).$$

Given $K^\times x \in \mathrm{Ker}(C_K)$, then there exists $a \in K^\times$ such that $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{val}_{\mathfrak{p}}(x_{\mathfrak{p}})} = a\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{val}_{\mathfrak{p}}(a)}$. Therefore $\mathrm{val}_{\mathfrak{p}}(x_{\mathfrak{p}}) = \mathrm{val}_{\mathfrak{p}}(a)$ for all $\mathfrak{p} \subset \mathcal{O}_K$, one get $a^{-1}x_{\mathfrak{p}} \in \widehat{\mathcal{O}_{K\mathfrak{p}}}^{\times}$. From $x \in \mathbb{A}_K^{\times,1}$ and $\|a\|_K = 1$, one get $\|a^{-1}x\|_K = 1$, then $\prod_{v|\infty} \left|a^{-1}x_v\right|_v = 1$. Therefore $a^{-1}x \in \mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}$, $x \in K^\times \left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}\right)$. On the other hand, if $x \in K^\times \left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}\right)$, there exists $a \in K^\times$ and $y \in \mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}$ with $x = ay$. It follows that $\mathrm{val}_{\mathfrak{p}}(x_{\mathfrak{p}}) = \mathrm{val}_{\mathfrak{p}}(a)$ for all $\mathfrak{p} \subset \mathcal{O}_K$ prime. Then $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{val}_{\mathfrak{p}}(x_{\mathfrak{p}})} = a\mathcal{O}_K \in P_K$ implies that $C_K(K^\times x) = 1$. We conclude that $\mathrm{Ker}(C_K) = K^\times \backslash K^\times \left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}\right)$. For the second, it suffices to show $K^\times \cap \left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}\right) = \mathcal{O}_K^\times$. Given $a \in K^\times \cap \left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}\right)$, then $a \in \widehat{\mathcal{O}_{K\mathfrak{p}}}$ for every prime $\mathfrak{p}$, so $\mathrm{val}_{\mathfrak{p}}(a) = 0$, $a\mathcal{O}_K = \mathcal{O}_K$. That is, $a \in \mathcal{O}_K^\times$. The converse is clear. Consequently we get exact sequence

$$1 \longrightarrow \mathcal{O}_K^\times \backslash \left(\mathbb{A}_{K,\infty}^{\times,1} \times \textstyle\prod_{v\in|K|_f} \widehat{\mathcal{O}_{Kv}}^{\times}\right) \longrightarrow K^\times \backslash \mathbb{A}_K^{\times,1} \xrightarrow{C_K} \mathrm{Cl}_K \longrightarrow 1$$

Theorem 14.3. $K^\times$ is discrete and cocompact in $\mathbb{A}_K^{\times,1}$.

Proof. Discrete: Since $\mathbb{A}_K^{\times,1}$ is a topological group, it is enough to find open neighborhood U of 1 in $\mathbb{A}_K^{\times,1}$ such that $U \cap K^\times = \{1\}$. For $v \mid \infty$, let U_v be a sufficient small open neighborhood of 1, for $v \nmid \infty$, let $U_v = \widehat{\mathcal{O}_{Kv}}$. For $x \in U \cap K^\times$, if $x \neq 1$, then $|x-1|_\infty$ is sufficiently close to 0 for $v \mid \infty$ and for $v \nmid \infty$ $x - 1 \in \widehat{\mathcal{O}_{Kv}}$ for $|x-1|_v = q_v^{-v(x-1)} \leq 1$. It follows that $\|x-1\|_K = \prod_{v\in|K|} |x-1|_v$ is sufficiently closed to 0, contradiction to the Product Formula.

Cocompact: Need to show that $K^\times \backslash \mathbb{A}_K^{\times,1}$ is compact. Idea: find a compact subset C in $\mathbb{A}_K^{\times,1}$ such that

$$C \longrightarrow \mathbb{A}_K^{\times,1} \longrightarrow K^\times \backslash \mathbb{A}_K^{\times,1}$$

is surjective. Since the continuous image of compact is also compact, we get $K^\times \backslash \mathbb{A}_K^{\times,1}$ is compact.

Lemma 14.1 (Minkowski)**.** There exists a constant $N = N(K)$ such that for any $x \in \mathbb{A}_K^\times$ such that $\|x\|_K > N$, there exists $y \in K^\times$ such that $|y|_v \le |x_v|_v$ for all $v \in |K|$.

Proof of Lemma. Since $\mathbb{A}_K$ is a locally compact topological group and it is abelian, there exists a Haar measure μ on $\mathbb{A}_K$. It descends to a Haar measure $K\backslash\mathbb{A}_K$, still denoted μ. Since $K\backslash\mathbb{A}_K$ is compact, the volume $\mu\left(K\backslash\mathbb{A}_K\right) < +\infty$. Let

$$C = \left\{ x \in \mathbb{A}_K \mid \text{for } v \mid \infty, |x_v|_v \le \frac{1}{4};\ \text{for } v \nmid \infty, |x_v|_v \le 1 \right\} \subset \mathbb{A}_K$$

compact, then $\mu(C) < +\infty$. Let $N = \mu(K\backslash\mathbb{A}_K)/\mu(C)$. For $x \in \mathbb{A}_K^\times$ such that $\|x\|_K > N$, then $\mu(xC) = \|x\|_K \mu(C) > \mu(K\backslash\mathbb{A}_K)$. The natural projection $xC \to K\backslash\mathbb{A}_K$ cannot be injective. Thus there exists $c_1, c_2 \in C$ such that $y \coloneqq c_1 x - c_2 x \in K^\times$. Then $|y|_v = |c_1 - c_2| \cdot |x|_v$. For v real, then $|y|_v \le (|c_1|_v + |c_2|_v) \cdot |x|_v \le \frac{2}{4}|x|_v < |x|_v$. For v complex, $|y|_v \le \left(\frac{1}{2} + \frac{1}{2}\right)^2 |x|_v = |x|_v$. For $v \nmid \infty$, then $|y|_v \le \max\{|c_1|_v, |c_2|_v\} \cdot |x_v|_v \le |x_v|_v$. y satisfies the condition. $\square$

Fix $x \in \mathbb{A}_K^\times$ such that $\|x\|_K > N(K)$, let

$$E = \{a \in \mathbb{A}_K \mid |a_v|_v \le |x_v|_v, \forall v \in |K|\},$$

then E is compact in $\mathbb{A}_K$. Indeed, for $v \mid \infty$, $\{a_v \mid |a_v|_v \le |x_v|_v\}$ is closed and bounded subset in $\mathbb{R}$ or $\mathbb{C}$, so compact; for $v \nmid \infty$, $\{a_v \mid |a_v|_v \le |x_v|_v\} = \varpi_v^{\mathrm{val}_v(x_v)}\widehat{\mathcal{O}_{K_v}}$ is also compact since $\widehat{\mathcal{O}_{K_v}}$ is compact. For $\alpha \in \mathbb{A}_K^{\times,1}$, we have $\|\alpha x\|_K = \|\alpha\|_K \cdot \|x\|_K = N(K)$. By Lemma 14.1, there exists $y \in K^\times$ such that $|y|_v \le |\alpha x|_v$ for all $v \in |K|$. This is equivalent to $|\alpha^{-1} y| \le |x|_v$, that is, $c_1 \coloneqq \alpha^{-1} y \in E$. Since $\alpha^{-1} \in \mathbb{A}_K^{\times,1}$, same argument implies existence of $y' \in K^\times$ such that $c_2 \coloneqq y'\alpha \in E$. By construction, $\alpha = y c_1^{-1} = {y'}^{-1} c_2$, so $yy' = c_1 c_2$. Let E' be the image of $E \times E$ under the multiplication map $\mathbb{A}_K \times \mathbb{A}_K \xrightarrow{\cdot} \mathbb{A}_K$, then E' is compact in $\mathbb{A}_K$ and $c_1 c_2 \in E'$. On the other hand $yy' \in K$. So $yy' = c_1 c_2 \in K \cap E'$. Since K is discrete in $\mathbb{A}_K$ and E' is compact, the intersection $K \cap E'$ is finite. Let $K^\times \cap E' = \{\gamma_1, \cdots, \gamma_N\}$, then $yy' = c_1 c_2 = \gamma_i$ for some i. By construction, $y'\alpha \in E$, $(y'\alpha)^{-1} = {y'}^{-1}\alpha^{-1} = (yy')^{-1} y \alpha^{-1} = \gamma_i^{-1} y \alpha^{-1} \in \gamma_i^{-1} E$. Consider the embedding $\iota \colon \mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$ defined by $x \mapsto \left(x, x^{-1}\right)$, $\mathbb{A}_K^\times$ is homeomorphism to $\iota(\mathbb{A}_K^\times)$. Let $C = \iota^{-1}\left(\bigcup_{i=1}^N (E \times \gamma_i^{-1} E)\right)$, then C is compact in $\mathbb{A}_K^\times$. The equation $y'\alpha \in E$ and $(y'\alpha)^{-1} \in \gamma_i^{-1} E$ says that $y'\alpha \in C$. We finish the proof. $\square$

Corollary 14.1 (Hermite–Minkowski)**.** Cl_K is finite.

Proof. Recall that $\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{K\,v}}^{\times} = \mathbb{A}_K^{\times,1} \cap \left(\mathbb{A}_{K,\infty}^{\times} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{K\,v}}^{\times}\right)$ is open in $\mathbb{A}_K^{\times,1}$. Let $q\colon \mathbb{A}_K^{\times,1} \to K^\times\backslash\mathbb{A}_K^{\times,1}$ be quotient mapping, if $U \subset \mathbb{A}_K^{\times,1}$ open, then $q^{-1}(q(U)) = \bigcup_{a\in K^\times} aU$ open, which implies that $q(U)$ is open. Therefore $\mathrm{Ker}(C_K) = q\left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{K\,v}}^{\times}\right)$ is open subgroup of $K^\times\backslash\mathbb{A}_K^{\times,1}$. One get $K^\times\backslash\mathbb{A}_K^{\times,1} = \bigcup_g g\,\mathrm{Ker}(C_K)$. Thanks to Theorem 14.3, take finite subcover, we obtain $\left(K^\times\backslash\mathbb{A}_K^{\times,1}\right)/\mathrm{Ker}(C_K) = \mathrm{Cl}_K$ finite. ☐

Corollary 14.2 (Dirichlet unit theorem)**.** Let μ_K be the roots of unity in K, then $\mu_K\backslash\mathcal{O}_K^\times$ is rank $(r+s-1)$ free abelian group. $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}$.

Proof. Open subgroup $\mathrm{Ker}(C_K)$ must be closed, from $K^\times\backslash\mathbb{A}_K^{\times,1}$ is compact, $\mathrm{Ker}(C_K)$ is compact. The projection $\mathbb{A}_{K,\infty}^{\times,1}\times\prod_{v\in|K|_f} \widehat{\mathcal{O}_{K\,v}}^{\times} \to \mathbb{A}_{K,\infty}^{\times,1}$ induces continuous surjection $\mathcal{O}_K^\times\backslash\left(\mathbb{A}_{K,\infty}^{\times,1} \times \prod_{v\in|K|_f} \widehat{\mathcal{O}_{K\,v}}^{\times}\right) \to \mathcal{O}_K^\times\backslash\mathbb{A}_{K,\infty}^{\times,1}$, it then follows that $\mathcal{O}_K^\times\backslash\mathbb{A}_{K,\infty}^{\times,1}$ is compact. Define $H = \left\{(t_v)_{v|\infty} \in \mathbb{R}^{r+s} \mid \sum_{v|\infty} t_v = 0\right\}$. Consider group homomorphism

$$\mathbb{A}_{K,\infty}^{\times,1} \longrightarrow H, \quad (x_v)_{v|\infty} \longmapsto (\log|x_v|_v)_{v|\infty}\,.$$

It is well-defined since $x \in \mathbb{A}_{K,\infty}^{\times,1}$ iff $\prod_{v|\infty}|x_v|_v = 1$ iff $\sum_{v|\infty}\log|x_v|_v = 0$. Moreover it is continuous surjective, given $(t_v)_{v|\infty} \in H$, then for v corresponding to $K \hookrightarrow \mathbb{R}$ let $x_v = \mathrm{e}^{t_v} \in \mathbb{R}^\times$ and for v corresponding to $K \hookrightarrow \mathbb{C}$ let $x_v = \mathrm{e}^{t_v/2} \in \mathbb{C}^\times$, we have $|x_v|_v = \mathrm{e}^{t_v}$ for all $v \mid \infty$, and its image is precisely $(t_v)_{v|\infty}$. Let $L\left(\mathcal{O}_K^\times\right) = \left\{(\log|u|_v)_{v|\infty} \mid u \in \mathcal{O}_K^\times\right\} \subset H$, so above surjection induces continuous surjection $\mathcal{O}_K^\times\backslash\mathbb{A}_{K,\infty}^{\times,1} \to L\left(\mathcal{O}_K^\times\right)\backslash H$, which implies that $L\left(\mathcal{O}_K^\times\right)\backslash H$ is compact.

Now prove $L\left(\mathcal{O}_K^\times\right)$ is discrete. For arbitrary $R > 0$, if $u \in \mathcal{O}_K^\times$ satisfy $|\log|u|_v| \le R$, then for arbitrary $\tau\colon K \hookrightarrow \mathbb{C}$ we have $|\tau(u)| \le \mathrm{e}^R$. The $\mathbb{Z}$-linear automorphism $\cdot u$ admits character polynomial $\prod_{\tau\colon K\hookrightarrow\mathbb{C}}(X - \tau(u)) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$. Hence $a_i = (-1)^i\sum_{\{\tau_1,\cdots,\tau_i\}\subset\{\tau\colon K\hookrightarrow\mathbb{C}\}} \tau_1(u)\cdots\tau_i(u)$, so $|a_i| \le \binom{n}{i}\mathrm{e}^{Ri}$. Note that $\#\mathbb{Z}\cap\left[-\binom{n}{i}\mathrm{e}^{Ri}, +\binom{n}{i}\mathrm{e}^{Ri}\right] < +\infty$, there are only finitely many such polynomial $X^n + a_1X^{n-1} + \cdots + a_n$. Fix $\tau_0\colon K \hookrightarrow \mathbb{C}$, since $\tau_0(u)$ is root of some polynomial $X^n + a_1X^{n-1} + \cdots + a_n$, so there only exists finitely many such $\tau_0(u)$, combine τ_0 injective there are finitely many $u \in \mathcal{O}_K^\times$ such that $|\log|u|_v| \le R$. Consequently $\#L\left(\mathcal{O}_K^\times\right) \cap \left\{(t_v)_{v|\infty} \in H \mid |t_v| \le 1 \text{ for all } v \mid \infty\right\} < +\infty$. If $F \coloneqq L\left(\mathcal{O}_K^\times\right) \cap \left\{(t_v)_{v|\infty} \in H \mid |t_v| \le 1 \text{ for all } v \mid \infty\right\} \ne \{0\}$, then $\left\{\max_{v|\infty}|t_v| \mid (t_v)_{v|\infty} \in F, (t_v)_{v|\infty} \ne 0\right\}$ admits minimal element, say $\delta > 0$. If $(t_v)_{v|\infty} \in L\left(\mathcal{O}_K^\times\right)$ and $|t_v| < \delta$, then $|t_v| < 1$, and so $(t_v)_{v|\infty} \in F$. Then get $\max_{v|\infty}|t_v| \ge \delta$, a contradiction. So $(t_v)_{v|\infty} = 0$. Thus $L\left(\mathcal{O}_K^\times\right) \cap$

$\left\{(t_v)_{v|\infty} \in H \mid |t_v| < \delta \text{ for all } v \mid \infty\right\} = \{0\}$. (If $F = \{0\}$ we just need to choose $\delta = 1$.) 0 is isolated point of $L\left(\mathcal{O}_K^\times\right)$. We obtain $L\left(\mathcal{O}_K^\times\right) \subset H$ is discrete subgroup.

Now H is $\mathbb{R}$-vector space of dimension $r+s-1$, $L\left(\mathcal{O}_K^\times\right) \subset H$ is discrete and cocompact, $L\left(\mathcal{O}_K^\times\right)$ is rank $r+s-1$ lattice in H.

Finally determine the kernel of $\mathcal{O}_K^\times \to H$ defined by $u \mapsto (\log |u|_v)_{v|\infty}$. For $u \in \mathcal{O}_K^\times$, $(\log |u|_v)_{v|\infty} = 0$ iff $|u|_v = 1$. For arbitrary m we have $|u^m|_v = 1$. Above proof shows that $\#\{u^m \mid m \geq 0\} < +\infty$. So there exists $m' > m \geq 0$ such that $u^{m'} = u^m$, $u \in \mu_K$, get $\mathrm{Ker} \subset \mu_K$. On the other hand for $u \in \mu_K$, there exists $N \geq 1$ such that $u^N = 1$. From $|u|_v^N = |u^N|_v = 1$ and $|u|_v > 0$ we have $|u|_v = 1$, so $\log |u|_v = 0$. That is, $u \in \mathrm{Ker}$, $\mu_K \subset \mathrm{Ker}$. We conclude $\mathrm{Ker}\left(\mathcal{O}_K^\times \to H\right) = \mu_K$. $\square$

We have short exact sequence

$$1 \longrightarrow \mu_K \longrightarrow \mathcal{O}_K^\times \longrightarrow L\left(\mathcal{O}_K^\times\right) \longrightarrow 0 \ ,$$

where $\mathcal{O}_K^\times \to L\left(\mathcal{O}_K^\times\right)$ is defined by $u \mapsto (\log |u|_v)_{v|\infty}$.

15 Integration on Adèles and Idèles

For $v \in |K|$,

- If $K_v = \mathbb{R}$, then $\mathrm{d}x_v$ be the Lebesgue measure on $\mathbb{R}$.
- If $K_v = \mathbb{C}$, we take the measure $|\mathrm{d}z \wedge \mathrm{d}\overline{z}| = 2\mathrm{d}x\mathrm{d}y$
- If $v \nmid \infty$, we take the Haar measure on K_v such that $\mathrm{d}x_v\left(\widehat{\mathcal{O}_{K_v}}\right) = 1$.

Lemma 15.1. For $a \in K_v^\times$, then $\mathrm{d}(ax_v)$ is still a Haar measure on K_v and $\mathrm{d}(ax_v) = |a|_v \mathrm{d}x_v$. Consequently $\frac{\mathrm{d}x_v}{|x_v|_v}$ defines a Haar measure on $K_v^\times$, and

$$\int_{\mathcal{O}_v^\times} \frac{\mathrm{d}x_v}{|x_v|_v} = 1 - q_v^{-1}, \quad q_v = |\mathcal{O}_K/\mathfrak{p}_v|$$

where $\widehat{\mathcal{O}_{K_v}} = \mathcal{O}_v$.

Proof. First consider v archimedean place. If $K_v = \mathbb{R}$, then $\mathrm{d}y = |a|\mathrm{d}x = |a|_v\mathrm{d}x$; if $K_v = \mathbb{C}$, then $\mathrm{d}(az) = 2\mathrm{d}(\mathrm{Re}(az))\mathrm{d}(\mathrm{Im}(az)) = |a|_{\mathbb{C}}^2\mathrm{d}x\mathrm{d}y = |a|_v\mathrm{d}z$.

Now let $v \nmid \infty$. First consider $a \in \mathcal{O}_K \setminus \{0\}$. Since both $\mathrm{d}(ax_v)$ and $\mathrm{d}x_v$ are Haar measure, we get $\mathrm{d}(ax_v) = c \cdot \mathrm{d}x_v$ for some $c \in \mathbb{R}$. Compute $\mathrm{d}(ax_v)(\mathcal{O}_v) = \mathrm{d}x_v(a\mathcal{O}_v) = \mathrm{d}x_v\left(\mathfrak{p}^{v(a)}\right)$. Note that $\mathcal{O}_v/\mathfrak{p}^{v(a)}$ is a finite group of cardinal $q_v^{v(a)}$ since $\mathfrak{p}^j/\mathfrak{p}^{j+1} = \mathcal{O}/\mathfrak{p}$, and

$$\mathcal{O}_v = \bigsqcup_{[a]\in\mathcal{O}_v/\mathfrak{p}^{v(a)}} a + \mathfrak{p}^{v(a)},$$

we get

$$1 = \mathrm{d}x_v(\mathcal{O}_v) = \sum_{[a]\in\mathcal{O}_v/\mathfrak{p}^{v(a)}} \mathrm{d}x_v\left(a + \mathfrak{p}^{v(a)}\right) = \left|\mathcal{O}_v/\mathfrak{p}^{v(a)}\right| \mathrm{d}x_v\left(\mathfrak{p}^{v(a)}\right) = q_v^{v(a)} \cdot \mathrm{d}x_v\left(\mathfrak{p}^{v(a)}\right),$$

which implies that

$$\mathrm{d}x_v\left(\mathfrak{p}^{v(a)}\right) = q_v^{-v(a)} = |a|_v.$$

Thus

$$c = \frac{\mathrm{d}(ax_v)(\mathcal{O}_v)}{\mathrm{d}x_v(\mathcal{O}_v)} = \frac{|a|_v}{1} = |a|_v.$$

Remark 15.1. In the proof, we get $\mathrm{d}x_v\left(\mathfrak{p}_v^n\right) = q_v^{-n}$.

Now from $\mathrm{d}x_v = \mathrm{d}\left(\pi_v^n \pi_v^{-n} x_v\right) = q_v^n \mathrm{d}\left(\pi_v^{-n} x_v\right)$ implies that $\mathrm{d}\left(\pi_v^{-n} x_v\right) = q_v^n \mathrm{d}x_v$. For the unit $u \in \mathcal{O}_v^\times$ we have $\mathrm{d}(ux_v) = \mathrm{d}x_v$. Thus for arbitrary $a \in K_v^\times$, by writing $a = u\pi_v^m$ where $u \in \mathcal{O}_v^\times$ and $m \in \mathbb{Z}$, we obtain $\mathrm{d}(ax_v) = |a|_v \mathrm{d}x_v$.

By the equation $\mathrm{d}(ax_v) = |a|_v \mathrm{d}x_v$, we get

$$\frac{\mathrm{d}(ax_v)}{|ax_v|_v} = \frac{|a|_v \mathrm{d}x_v}{|a|_v |x_v|_v} = \frac{\mathrm{d}x_v}{|x_v|_v}.$$

So $\frac{\mathrm{d}x_v}{|x_v|_v}$ is a Haar measure.

Now

$$\int_{\mathcal{O}_v^\times} \frac{\mathrm{d}x_v}{|x_v|_v} = \int_{\mathcal{O}_v^\times} \mathrm{d}x_v$$

since $|x_v|_v = 1$ holds for all $x_v \in \mathcal{O}_v^\times$. We have partition $\mathcal{O}_v = \mathcal{O}_v^\times \sqcup \mathfrak{p}$. So

$$1 = \int_{\mathcal{O}_v} \mathrm{d}x_v = \mathrm{d}x_v(\mathcal{O}_v) = \mathrm{d}x_v\left(\mathcal{O}_v^\times\right) + \mathrm{d}x_v(\mathfrak{p}) = \mathrm{d}x_v\left(\mathcal{O}_v^\times\right) + q_v^{-1},$$

which implies that

$$\int_{\mathcal{O}_v^\times} \mathrm{d}x_v = 1 - q_v^{-1}.$$

□

For $\mathbb{A}_K$, take the product measure $\mathrm{d}x$ of

- $K_v = \mathbb{R}$, $\mathrm{d}x$;
- $K_v = \mathbb{C}$, $2\mathrm{d}x\mathrm{d}y$;

- $v \nmid \infty$, Haar measure such that $\mathrm{d}x_v(\mathcal{O}_v) = 1$.

Proposition 15.1. Let $C \subset \mathbb{A}_K$ be compact subset, then $\mathrm{d}x(C) < +\infty$.

Proof. For every $x = (x_v)_v \in C$, there exists a neighborhood $U^{(x)} = \prod_v U_v^{(x)}$ where $U_v^{(x)} = \mathcal{O}_v$ for all but finitely many $v \nmid \infty$. Since C is compact, one can take finitely many $U^{(i)}$ with $C \subset \bigcup_{i=1}^m U^{(i)}$. Clearly for all but finitely many $v \nmid \infty$ we have $U_v^{(i)} = \mathcal{O}_v$ for every i, then $C_v \subset \mathcal{O}_v$ for all but finitely many $v \nmid \infty$. There exists compact open subset $C_v \subset K_v$ such that $C_v = \mathcal{O}_v$ for all that but finitely many $v \in |K|$ and $C \subset \prod_{v\in|K|} C_v$.

$$\mathrm{d}x(C) < \prod_{\substack{v\in S\\ |S|<+\infty}} \mathrm{d}x_v(C_v) \prod_{v\notin S} \mathrm{d}x_v(\mathcal{O}_v) = \prod_{\substack{v\in S\\ |S|<+\infty}} \mathrm{d}x_v(C_v) < +\infty.$$

□

On $\mathbb{A}_K^\times$, we take the product measure $\mathrm{d}^\times x$

- $v \mid \infty$, $\frac{\mathrm{d}x_v}{|x_v|}$
- $v \nmid \infty$, $\frac{1}{1-q_v^{-1}}\frac{\mathrm{d}x_v}{|x_v|}$

Then

$$\mathrm{vol}\left(\mathcal{O}_v^\times\right) = \int_{\mathcal{O}_v^\times} \frac{1}{1-q_v^{-1}}\frac{\mathrm{d}x_v}{|x_v|} = 1.$$

Proposition 15.2. For any compact open subset C of $\mathbb{A}_K^\times$, $\mathrm{d}^\times x(C) < +\infty$.

Theorem 15.1.

$$\int_{K\backslash\mathbb{A}_K} \mathrm{d}x = \left|\Delta_{K/\mathbb{Q}}\right|^{\frac{1}{2}}.$$

Proof.

$$\mathbb{A}_K = K + \left(\prod_{v|\infty} K_v \times \prod_{v\nmid\infty} \mathcal{O}_v\right)$$

implies that

$$\begin{aligned} K\backslash\mathbb{A}_K &= K\backslash K + \left(\prod_{v|\infty} K_v \times \prod_{v\nmid\infty} \mathcal{O}_v\right) \\ &= \left(K \cap \prod_{v|\infty} K_v \times \prod_{v\nmid\infty} \mathcal{O}_v\right) \backslash \left(\prod_{v|\infty} K_v \times \prod_{v\nmid\infty} \mathcal{O}_v\right) \\ &= \mathcal{O}_K\backslash\left(\prod_{v|\infty} K_v \times \prod_{v\nmid\infty} \mathcal{O}_v\right). \end{aligned}$$

The projection

$$K\backslash\mathbb{A}_K=\mathcal{O}_K\backslash\left(\prod_{v|\infty}K_v\times\prod_{v\nmid\infty}\mathcal{O}_v\right)\longrightarrow\mathcal{O}_K\backslash\prod_{v|\infty}K_v$$

has kernel $\mathcal{O}_K\backslash\left(\mathcal{O}_K\times\prod_{v\nmid\infty}\mathcal{O}_v\right)=\prod_{v\nmid\infty}\mathcal{O}_v$ (here $\mathcal{O}_K\subset\prod_{v|\infty}K_v$ as the image of diagonal embedding). Thus we get short exact sequence

$$0\longrightarrow\prod_{v\nmid\infty}\mathcal{O}_v\longrightarrow K\backslash\mathbb{A}_K\longrightarrow\mathcal{O}_K\backslash\prod_{v|\infty}K_v\longrightarrow 0\ ,$$

which implies that

$$\int_{K\backslash\mathbb{A}_K}\mathrm{d}x=\int_{\mathcal{O}_K\backslash\prod_{v|\infty}K_v}\int_{\prod_{v\nmid\infty}\mathcal{O}_v}\mathrm{d}x_f\mathrm{d}x_\infty=\int_{\mathcal{O}_K\backslash\prod_{v|\infty}K_v}\mathrm{d}x_\infty.$$

since

$$\int_{\prod_{v\nmid\infty}\mathcal{O}_v}\mathrm{d}x_f=\mathrm{vol}\left(\prod_{v\nmid\infty}\mathcal{O}_v\right)=1.$$

Suppose that K has r real embeddings $\sigma_1,\cdots,\sigma_r$ and s complex embeddings $\sigma_{r+1},\overline{\sigma_{r+1}},\cdots,\sigma_{r+s},\overline{\sigma_{r+s}}$. Then $\prod_{v|\infty}K_v=\mathbb{R}^r\times\mathbb{C}^s$. It is known that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]=r+2s=:n$. Let $\alpha_1,\cdots,\alpha_n$ be a set of basis of $\mathcal{O}_K$ over $\mathbb{Z}$. Let $v_i=(\sigma_1(\alpha_i),\cdots,\sigma_r(\alpha_i),\sigma_{r+1}(\alpha_i),\cdots,\sigma_{r+s}(\alpha_i))\in\prod_{v|\infty}K_v$, then $v_1,\cdots,v_n$ generates a lattice L in $\prod_{v|\infty}K_v=\mathbb{R}^r\times\mathbb{C}^s$, and

$$\int_{\mathcal{O}_K\backslash\prod_{v|\infty}K_v}\mathrm{d}x_\infty=\mathrm{vol}\left(L\backslash\mathbb{R}^r\times\mathbb{C}^s\right)=2^s\mathrm{d}x\left(L'\backslash\mathbb{R}^r\times\mathbb{R}^{2s}\right)$$

where L' is the image of $\mathcal{O}_K\hookrightarrow\mathbb{R}^r\times\mathbb{R}^{2s}$ given by

$$x\mapsto\left(\sigma_1(x),\cdots,\sigma_r(x),\frac{\sigma_{r+1}(x)+\overline{\sigma_{r+1}}(x)}{2},\frac{\sigma_{r+1}(x)-\overline{\sigma_{r+1}}(x)}{2},\cdots,\frac{\sigma_{r+s}(x)+\overline{\sigma_{r+s}}(x)}{2},\frac{\sigma_{r+s}(x)-\overline{\sigma_{r+s}}(x)}{2}\right).$$

Then

$$\int_{\mathcal{O}_K\backslash\prod_{v|\infty}K_v}\mathrm{d}x_\infty=2^s\cdot\begin{vmatrix}\sigma_1(\alpha_1)&\cdots&\sigma_1(\alpha_n)\\\vdots&\ddots&\vdots\\\sigma_r(\alpha_1)&\cdots&\sigma_r(\alpha_n)\\\frac{\sigma_{r+1}(\alpha_1)+\overline{\sigma_{r+1}}(\alpha_1)}{2}&\cdots&\frac{\sigma_{r+1}(\alpha_n)+\overline{\sigma_{r+1}}(\alpha_n)}{2}\\\frac{\sigma_{r+1}(\alpha_1)-\overline{\sigma_{r+1}}(\alpha_1)}{2}&\cdots&\frac{\sigma_{r+1}(\alpha_n)-\overline{\sigma_{r+1}}(\alpha_n)}{2}\\\vdots&\ddots&\vdots\\\frac{\sigma_{r+s}(\alpha_1)+\overline{\sigma_{r+s}}(\alpha_1)}{2}&\cdots&\frac{\sigma_{r+s}(\alpha_n)+\overline{\sigma_{r+s}}(\alpha_n)}{2}\\\frac{\sigma_{r+s}(\alpha_1)-\overline{\sigma_{r+s}}(\alpha_1)}{2}&\cdots&\frac{\sigma_{r+s}(\alpha_n)-\overline{\sigma_{r+s}}(\alpha_n)}{2}\end{vmatrix}=\begin{vmatrix}\sigma_1(\alpha_1)&\cdots&\sigma_1(\alpha_n)\\\vdots&\ddots&\vdots\\\sigma_r(\alpha_1)&\cdots&\sigma_r(\alpha_n)\\\sigma_{r+1}(\alpha_1)&\cdots&\sigma_{r+1}(\alpha_n)\\\overline{\sigma_{r+1}}(\alpha_1)&\cdots&\overline{\sigma_{r+1}}(\alpha_n)\\\vdots&\ddots&\vdots\\\sigma_{r+s}(\alpha_1)&\cdots&\sigma_{r+s}(\alpha_n)\\\overline{\sigma_{r+s}}(\alpha_1)&\cdots&\overline{\sigma_{r+s}}(\alpha_n)\end{vmatrix}=\left|\Delta_{K/\mathbb{Q}}\right|^{\frac{1}{2}}.$$

$\square$

Theorem 15.2.
$$\int_{K^\times\backslash\mathbb{A}_K^{\times,1}}\mathrm{d}^{\times,1}x=\frac{2^r(2\pi)^s h_K R_K}{|\mu_K|},$$
where h_K is the class number, R_K is regulator, and μ_K is roots of unity in $K^\times$.

Proof. We have split exact sequence

$$0\longrightarrow\mathbb{A}_K^{\times,1}\longrightarrow\mathbb{A}_K^\times\xrightarrow{\|\cdot\|_K}\mathbb{R}_+^\times\longrightarrow 0\ ,$$

where for arbitrary $r\in\mathbb{R}_+^\times$, define $(x_v)_{v\in|K|}$: fixing a place $v_0\mid\infty$, if v_0 corresponds to a real embedding, take $x_{v_0}=r$; if v_0 corresponds to a complex embedding, take $x_{v_0}=\sqrt{r}$, and for all $v\neq v_0$ take $x_v=1$. Thus we get $\mathbb{A}_K^\times=\mathbb{A}_K^{\times,1}\times\mathbb{R}_+^\times$, $\mathrm{d}^\times x=\mathrm{d}^{\times,1}x\times\frac{\mathrm{d}r}{r}$. We have exact sequence

$$1\longrightarrow\mathcal{O}_K^\times\backslash\left(\mathbb{A}_{K,\infty}^{\times,1}\times\textstyle\prod_{v\nmid\infty}\mathcal{O}_v^\times\right)\longrightarrow K^\times\backslash\mathbb{A}_K^{\times,1}\longrightarrow\mathrm{Cl}_K\longrightarrow 1\ ,$$

then

$$\int_{K^\times\backslash\mathbb{A}_K^{\times,1}}\mathrm{d}^{\times,1}x=h_K\cdot\int_{\mathcal{O}_K^\times\backslash(\mathbb{A}_{K,\infty}^{\times,1}\times\prod_{v\nmid\infty}\mathcal{O}_v^\times)}\mathrm{d}^{\times,1}x=h_K\cdot\int_{(\mathcal{O}_K^\times\backslash\mathbb{A}_{K,\infty}^{\times,1})\times\prod_{v\nmid\infty}\mathcal{O}_v^\times}\mathrm{d}^{\times,1}x=h_K\cdot\int_{\mathcal{O}_K^\times\backslash\mathbb{A}_{K,\infty}^{\times,1}}\mathrm{d}^{\times,1}x_\infty.$$

Here every element $a\in\mathcal{O}_K^\times$ satisfy $v_{\mathfrak{p}}(a)=0$ for every prime ideal $\mathfrak{p}\subseteq\mathcal{O}_K$, so $a\in\prod_{v\nmid\infty}\mathcal{O}_v^\times$, which implies that the fundamental domain of $\mathcal{O}_K^\times\backslash\left(\mathbb{A}_{K,\infty}^{\times,1}\times\prod_{v\nmid\infty}\mathcal{O}_v^\times\right)$ is $\left(\mathcal{O}_K^\times\backslash\mathbb{A}_{K,\infty}^{\times,1}\right)\times\prod_{v\nmid\infty}\mathcal{O}_v^\times$. By the unit theorem of Dirichlet, $\mathcal{O}_K^\times\cong\mu_K\times\mathbb{Z}^{r+s-1}$. Let $u_1,\cdots,u_{r+s-1}\in\mathcal{O}_K^\times$ be a set of generators for $\mathbb{Z}^{r+s-1}$. Note that

$$\mathbb{A}_{K,\infty}^{\times,1}=\left\{(x_v)_{v|\infty}\in\mathbb{R}^r\times\mathbb{C}^s\mid\prod_{v|\infty}|x_v|_v=1\right\}.$$

Consider

$$\varphi\colon\mathbb{A}_{K,\infty}^{\times,1}\longrightarrow H=\left\{(x_v)\in\prod_{v|\infty}\mathbb{R}\mid\sum_v x_v=0\right\}\subset\mathbb{R}^r\times\mathbb{R}^s$$

defined by

$$(x_v)_{v|\infty}\longmapsto(\log|x_v|_v)_{v|\infty}\,.$$

Then it is well-defined, surjective, and

$$\mathrm{Ker}(\varphi)=\prod_{K_v=\mathbb{R}}\{\pm1\}\times\prod_{K_v=\mathbb{C}}\mathrm{U}(1).$$

If $K_v=\mathbb{R}$, we have $\frac{\mathrm{d}x_v}{|x_v|_v}=\mathrm{d}\left(\log|x_v|_v\right)$; if $K_v=\mathbb{C}$, write $x_v=\rho\mathrm{e}^{\mathrm{i}\theta}$, it follows that $\frac{\mathrm{d}x_v}{|x_v|_v}=2\frac{\mathrm{d}\rho}{\rho}\mathrm{d}\theta=\mathrm{d}\left(\log|x_v|_v\right)\mathrm{d}\theta$. It follows that

$$\mathrm{d}^{\times,1}x_\infty=2^r(2\pi)^s\mathrm{d}x,$$

where $\mathrm{d}x$ is Lebesgue measure on H. However, $\varphi\left(\mathcal{O}_K^\times\right)$ is the lattice Λ in H generated by

$$w_i = (\log |u_i|_v)_{v|\infty}$$

and φ kills μ_K in $\mathcal{O}_K^\times$. We have

$$\int_{\mathcal{O}_K^\times \backslash \mathbb{A}_{K,\infty}^{\times,1}} \mathrm{d}^{\times,1} x_\infty = \frac{2^r (2\pi)^s}{|\mu_K|} \int_{\Lambda\backslash H} \mathrm{d}y.$$

Let $\vec{\delta} = \left(\frac{n_v}{n}\right)_{v|\infty}$, $n_\mathbb{R} = 1$, $n_\mathbb{C} = 2$, then $\vec{\delta}$ is a normal vector of H with norm 1. Then

$$\int_{\Lambda\backslash H} \mathrm{d}y = \left|\det\left(\vec{\delta}, w_1, \cdots, w_{r+s-1}\right)\right| =: R_K$$

called the regulator of K. $\square$

16 Functional equation of Riemann ζ-function

Recall the Riemann ζ-function

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}, \quad \mathrm{Re}(s) > 1.$$

Let

$$Z_\mathbb{Q}(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

Theorem 16.1 (Riemann)**.** The function $Z_\mathbb{Q}(s)$ can be extended to a meromorphic function on $\mathbb{C}$, with simple poles at $s = 0$ and $s = 1$, and it satisfies

$$Z_\mathbb{Q}(s) = Z_\mathbb{Q}(1-s).$$

Proof. Recall Euler Γ-function

$$\Gamma(s) = \int_0^{+\infty} \mathrm{e}^{-t} t^s \frac{\mathrm{d}t}{t}.$$

Take change of variable $t \to \pi n^2 t$,

$$\Gamma(s) = \int_0^{+\infty} \mathrm{e}^{-\pi n^2 t} (\pi n^2 t)^s \frac{\mathrm{d}t}{t} = \pi^s n^{2s} \int_0^{+\infty} \mathrm{e}^{-\pi n^2 t} t^s \frac{\mathrm{d}t}{t}.$$

Thus

$$\pi^{-s} \Gamma(s) \frac{1}{n^{2s}} = \int_0^{+\infty} \mathrm{e}^{-\pi n^2 t} t^s \frac{\mathrm{d}t}{t}.$$

Thus

$$\begin{aligned}
\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \int_0^{+\infty}\sum_{n=1}^{+\infty}\mathrm{e}^{-\pi n^2 t}t^{\frac{s}{2}}\frac{\mathrm{d}t}{t}\\
&= \frac{1}{2}\int_0^{+\infty}\left(\sum_{n\in\mathbb{Z}}\mathrm{e}^{-\pi n^2 t}-1\right)t^{\frac{s}{2}}\frac{\mathrm{d}t}{t}\\
&= \frac{1}{2}\left(\int_0^1+\int_1^{+\infty}\right)\left(\sum_{n\in\mathbb{Z}}\mathrm{e}^{-\pi n^2 t}-1\right)t^{\frac{s}{2}}\frac{\mathrm{d}t}{t}.
\end{aligned}$$

Let

$$\theta(t)=\sum_{n\in\mathbb{Z}}\mathrm{e}^{-\pi n^2 t},$$

then

$$\theta(t)=\sum_{n\in\mathbb{Z}}\mathrm{e}^{-\pi n^2 t}=\Theta\left(\mathrm{i}t\right).$$

From

$$\Theta\left(\frac{-1}{\mathrm{i}t}\right)=\Theta\left(\frac{\mathrm{i}}{t}\right)=\sqrt{t}\Theta(\mathrm{i}t),$$

we have

$$\theta\left(\frac{1}{t}\right)=\sqrt{t}\theta(t).$$

Therefore

$$\begin{aligned}
&\int_1^{+\infty}(\theta(t)-1)t^{\frac{s}{2}}\frac{\mathrm{d}t}{t}+\int_1^{+\infty}\left(\theta\left(\frac{1}{t}\right)-1\right)t^{-\frac{s}{2}}\frac{\mathrm{d}t}{t}\\
=&\int_1^{+\infty}(\theta(t)-1)t^{\frac{s}{2}}\frac{\mathrm{d}t}{t}+\int_1^{+\infty}(\theta(t)-1)t^{\frac{1-s}{2}}\frac{\mathrm{d}t}{t}+\int_1^{+\infty}t^{\frac{1-s}{2}}\frac{\mathrm{d}t}{t}-\int_1^{+\infty}t^{-\frac{s}{2}}\frac{\mathrm{d}t}{t}\\
=&\int_1^{+\infty}(\theta(t)-1)t^{\frac{s}{2}}\frac{\mathrm{d}t}{t}+\int_1^{+\infty}(\theta(t)-1)t^{\frac{1-s}{2}}\frac{\mathrm{d}t}{t}+\frac{2}{s-1}-\frac{2}{s}.
\end{aligned}$$

□

Jacobi theta function:

$$\Theta(\tau)=\sum_{n\in\mathbb{Z}}\mathrm{e}^{2\pi\mathrm{i}\tau},\quad \tau\in\mathfrak{h},$$

where $\mathfrak{h}=\{x+\mathrm{i}y \mid y>0\}$. It is holomorphic on $\mathfrak{h}$.

Theorem 16.2 (Jacobi)**.**

$$\Theta(z+2)=\Theta(\tau),$$
$$\Theta\left(\frac{-1}{\tau}\right)=\sqrt{\mathrm{i}\tau}\Theta(\tau).$$

This implies that $\Theta(\tau)$ is a modular form of weight $1/2$ for the subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

Corollary 16.1.

$$\theta\left(\frac{1}{t}\right) = \sqrt{t}\theta(t).$$

For $f(x) \in L^2(\mathbb{R}) \cap L^1(\mathbb{R})$, define Fourier transform on $\mathbb{R}^1$ by

$$\widehat{f}(\xi) = \int_{\mathbb{R}} f(x) \mathrm{e}^{2\pi \mathrm{i} \xi x} \mathrm{d}x.$$

It satisfies

1)

$$\frac{\mathrm{d}}{\mathrm{d}x} f(x) \xrightarrow{\text{Fourier}} 2\pi \mathrm{i} \xi f(\xi)$$

2)

$$2\pi \mathrm{i} f(x) \xrightarrow{\text{Fourier}} \frac{\mathrm{d}}{\mathrm{d}\xi} f(\xi)$$

Let $\mathcal{S}(\mathbb{R})$ be the Schwartz functions on $\mathbb{R}$, they satisfy

$$\lim_{|x| \to \infty} |x|^m \left| f^{(n)}(x) \right| = 0, \quad \forall n, m \in \mathbb{N}.$$

Then the Fourier transform restricts to

$$\mathcal{S}(\mathbb{R}) \longrightarrow \mathcal{S}(\mathbb{R}), \quad f \longmapsto \widehat{f}.$$

Theorem 16.3 (Poisson summation formula)**.** For any $f \in \mathcal{S}(\mathbb{R})$ we have

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(n).$$

Proof. Let

$$F(x) = \sum_{n \in \mathbb{Z}} f(x+n),$$

then $F(x)$ is a smooth function on $\mathbb{R}/\mathbb{Z} = S^1$. Consider the Fourier expansion of $F(x)$, its Fourier coefficient is

$$a_n = \int_0^1 F(x) \mathrm{e}^{-2\pi \mathrm{i} n x} \mathrm{d}x = \int_0^1 \sum_{n \in \mathbb{Z}} f(x+n) \mathrm{e}^{-2\pi \mathrm{i} n(x+n)} \mathrm{d}x = \int_{\mathbb{R}} f(x) \mathrm{e}^{-2\pi \mathrm{i} n x} \mathrm{d}x = \widehat{f}(n).$$

Thus

$$F(x) = \sum_{n\in\mathbb{Z}} a_n \mathrm{e}^{2\pi i n x} = \sum_{n\in\mathbb{Z}} \widehat{f}(n)\mathrm{e}^{2\pi i n x}.$$

Setting $x = 0$, get

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n).$$

$\square$

Lemma 16.1. Let $f(x) = \mathrm{e}^{-\pi x^2}$, then $f = \widehat{f}$.

Proof. $f(x)$ satisfies the equation

$$\frac{\mathrm{d}f}{\mathrm{d}x} = -2\pi x \cdot \mathrm{e}^{-\pi x^2} = -2\pi x \cdot f.$$

So its Fourier transform satisfies

$$2\pi \mathrm{i}\xi \cdot \widehat{f}(\xi) = -\mathrm{i}\frac{\mathrm{d}}{\mathrm{d}\xi}\widehat{f}(\xi),$$

i.e.,

$$\frac{\mathrm{d}}{\mathrm{d}\xi}\widehat{f}(\xi) = -2\pi\xi\widehat{f}(\xi).$$

Therefore

$$\widehat{f}(x) = Cf(x).$$

Compare

$$\widehat{f}(0) = \int_{\mathbb{R}} f(x)\mathrm{d}x = \int_{\mathbb{R}} \mathrm{e}^{-\pi x^2}\mathrm{d}x = 1.$$

So $C = 1$ and $\widehat{f}(x) = f(x)$. $\square$

Proof of Corollary 16.1. Let $f(x) = \mathrm{e}^{-\pi x^2}$ and $f^t(x) = f\left(x\sqrt{t}\right) = \mathrm{e}^{-\pi x^2 t}$.

$$\begin{aligned}
\widehat{f^t}(\xi) &= \int_{\mathbb{R}} f^t(x)\mathrm{e}^{2\pi \mathrm{i}\xi x}\mathrm{d}x \\
&= \int_{\mathbb{R}} f\left(x\sqrt{t}\right)\mathrm{e}^{2\pi \mathrm{i}\xi x}\mathrm{d}x \\
&= \int_{\mathbb{R}} f(x)\mathrm{e}^{2\pi \mathrm{i}\xi \frac{x}{\sqrt{t}}}\frac{\mathrm{d}x}{\sqrt{t}} \\
&= \frac{1}{\sqrt{t}}\widehat{f}\left(\frac{\xi}{\sqrt{t}}\right).
\end{aligned}$$

Thus

$$\theta(t) = \sum_{n\in\mathbb{Z}} \mathrm{e}^{-\pi n^2 t} = \sum_{n\in\mathbb{Z}} f^t(n) = \sum_{n\in\mathbb{Z}} \widehat{f^t}(n) = \sum_{n\in\mathbb{Z}} \frac{1}{\sqrt{t}}\mathrm{e}^{-\pi n^2/t} = \frac{1}{\sqrt{t}}\sum_{n\in\mathbb{Z}} \mathrm{e}^{-\pi n^2/t} = \frac{1}{\sqrt{t}}\theta\left(\frac{1}{t}\right).$$

$\square$

1)

$$Z_{\mathbb{Q}}(s) = \frac{1}{2}\int_0^{+\infty} (\theta(t)-1)t^{\frac{s}{2}}\frac{\mathrm{d}t}{t}$$

2) Poisson summation formula on $(\mathbb{R}, +)$.

17 Hecke L-function

Let $K/\mathbb{Q}$ be finite extension, a Hecke character is a continuous morphism $\chi\colon K^\times\backslash\mathbb{A}_K^\times \to \mathrm{U}(1)$, it is a generalization of Dirichlet character. Consider the restriction $\chi|_{K_v^\times} : K_v^\times \to \mathrm{U}(1)$,

1) If $K_v = \mathbb{R}$, $\chi|_{\mathbb{R}} : \mathbb{R} = \{\pm 1\} \times \mathbb{R}_+^\times \to \mathrm{U}(1)$, $x \mapsto (\mathrm{sgn}(x))^a \cdot |x|^{\mathrm{i}\theta}$, $a = 0, 1$, $\theta \in (0, 2\pi)$.
2) If $K_v = \mathbb{C}$, $\chi|_{\mathbb{C}} : \mathbb{C} = S^1 \times \mathbb{R}_+^\times \to \mathrm{U}(1)$, $x \mapsto \left(\frac{x}{|x|}\right)^n \cdot |x|^{\mathrm{i}\theta}$, $n \in \mathbb{Z}$.
3) If v finite, $\chi_v = \chi|_{K_v^\times} : K_v^\times = \langle\pi\rangle \times \mathcal{O}_{K_v}^\times \to \mathrm{U}(1)$ continuous. Let $1 \in U \subset \mathrm{U}(1)$ small enough, then there exists $U_v \subset \mathcal{O}_{K_v}^\times$ small enough (U_v can be take as $1 + \pi^N\mathcal{O}_v$), such that $\chi(U_v) \subset U$ and $\chi_v\left(1 + \pi^N\mathcal{O}_v\right)$ is a subgroup in U. For U small enough, it contains no subgroup of $\mathrm{U}(1)$. So $\chi_v\left(1 + \pi^N\mathcal{O}_v\right) = 1$ for $N \gg 0$. Let $f_{x,v} \in \mathbb{N} \cup \{0\}$ be the smallest number such that $1 + \mathfrak{p}^{f_{x,v}} \subset \mathrm{Ker}(\chi_v)$.

Recall that for $v \in |K|$, we take the additive measure

- If $K_v = \mathbb{R}$, then $\mathrm{d}x_v$ be the Lebesgue measure on $\mathbb{R}$.
- If $K_v = \mathbb{C}$, we take the measure $|\mathrm{d}z \wedge \mathrm{d}\overline{z}| = 2\mathrm{d}x\mathrm{d}y$
- If $v \nmid \infty$, we take the Haar measure on K_v such that $\mathrm{d}x_v\left(\mathcal{O}_v\right) = \left|\Delta_{K_v/\mathbb{Q}_p}\right|^{-\frac{1}{2}}$. This implies that $\mathrm{vol}\left(K\backslash\mathbb{A}_K\right) = 1$.

On $\mathbb{A}_K^\times$, we take the product measure $\mathrm{d}^\times x$

- If $v \mid \infty$, we take $\frac{\mathrm{d}x_v}{|x_v|_v}$, where $\mathrm{d}x_v$ is the above additive measure.
- If $v \nmid \infty$, we take $\mathrm{d}^\times x_v$ satisfying $\mathrm{vol}\left(\mathcal{O}_v^\times, \mathrm{d}^\times x_v\right) = 1$.

Definition 17.1. $\mathfrak{f}_x \coloneqq \prod_{v\in|K|_f} \mathfrak{p}^{f_{x,v}}$ called the **conductor** of χ.

Definition 17.2.

$$L(\chi, s) = \prod_{\substack{\mathfrak{p}\ \text{prime} \\ \mathfrak{p}\nmid\mathfrak{f}_x}} \frac{1}{1 - \frac{\chi_v(\pi_v)}{\mathrm{N}(\mathfrak{p})^s}}.$$

Example 17.1. Let $\chi_p\colon \mathbb{Q}_p^\times \to \mathrm{U}(1)$ be an unramified character ($f_{x,p} = 0$). Calculate

$$\int_{\mathbb{Q}_p^\times} \mathbf{1}_{\mathbb{Z}_p}(x)\chi_p(x)|x|_p^s \mathrm{d}^\times x_p = \int_{\mathbb{Z}_p\setminus\{0\}} \chi_p(x)|x|_p^s \mathrm{d}^\times x_p.$$

The character is unramified iff $\chi_p(\mathbb{Z}_p^\times) = 1$. $\mathbb{Z}_p \setminus \{0\} = \bigsqcup_{n=0}^{+\infty} p^n\mathbb{Z}_p^\times$, so

$$\begin{aligned}
\int_{\mathbb{Z}_p\setminus\{0\}} \chi_p(x)|x|_p^s \mathrm{d}^\times x_p |x|_p &= \sum_{n=0}^{+\infty} \int_{p^n\mathbb{Z}_p^\times} \chi_p(x)|x|_p^s \mathrm{d}^\times x_p \\
&= \sum_{n=0}^{+\infty} \int_{\mathbb{Z}_p^\times} \chi_p(p^n x)|p^n x|_p^s \mathrm{d}^\times x_p \\
&= \sum_{n=0}^{+\infty} \int_{\mathbb{Z}_p^\times} \chi_p(p)^n p^{-ns} \mathrm{d}^\times x_p \\
&= \left(\sum_{n=0}^{+\infty} \chi_p(p)^n p^{-ns}\right) \int_{\mathbb{Z}_p^\times} \mathrm{d}^\times x_p \\
&= \frac{1}{1 - \frac{\chi_p(p)}{p^s}}.
\end{aligned}$$

Definition 17.3. For $v \in |K|_f$, let ϕ_v be a locally constant function on K_v with compact support. Let $\chi_v\colon K_v^\times \to \mathrm{U}(1)$ be a continuous morphism, we define the **local zeta integral**

$$Z_v(\phi_v, \chi_v, s) = \int_{K_v^\times} \phi_v(x)\chi_v(x)|x|_v^s \mathrm{d}^\times x_v.$$

Let $\phi = \bigotimes_{v\in|K|_f} \phi_v$ such that $\phi_v = \mathbf{1}_{\mathcal{O}_{K_v}}$ for all but finitely many $v \in |K|_f$, define

$$Z(\phi, \chi, s) = \int_{\mathbb{A}_K^\times} \phi(x)\chi(x)\|x\|_K^s \mathrm{d}^\times x.$$

By definition

$$Z(\phi, \chi, s) = \prod_v \int_{K_v^\times} \phi_v(x)\chi_v(x)|x|_v^s \mathrm{d}^\times x_v = \prod_v Z(\phi_v, \chi_v, s).$$

If $f_v = \mathbf{1}_{\mathcal{O}_v}$, χ_v is unramified, then similar to Example 17.1 we have

$$Z_v(\mathbf{1}_{\mathcal{O}_v}, \chi_v, s) = \frac{1}{1 - \frac{\chi_v(\pi_v)}{\mathrm{N}(\mathfrak{p})^s}}.$$

From Proposition 10.1, if $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then $\mathrm{N}(\mathfrak{p}) = p^f \geq p$, it follows that

$$\left|1 - \frac{\chi_v(\pi_v)}{\mathrm{N}(\mathfrak{p})^s}\right| \geq 1 - \left|\frac{\chi_v(\pi_v)}{\mathrm{N}(\mathfrak{p})^s}\right| \geq 1 - \frac{1}{p^{\mathrm{Re}(s)}},$$

which implies that

$$\left|\frac{1}{1 - \frac{\chi_v(\pi_v)}{\mathrm{N}(\mathfrak{p})^s}}\right| \leq \frac{1}{1 - \frac{1}{p^{\mathrm{Re}(s)}}}.$$

Therefore

$$\prod_{v\notin S}\left|\frac{1}{1-\frac{\chi_v(\pi_v)}{\mathrm{N}(\mathfrak{p})^s}}\right| \leq \prod_{p\text{ prime}}\left(\frac{1}{1-\frac{1}{p^{\mathrm{Re}(s)}}}\right)^{[K:\mathbb{Q}]} = \zeta(\mathrm{Re}(s))^{[K:\mathbb{Q}]}$$

converges as $\mathrm{Re}(s)>1$. Here

$$S=\{v\mid v\mid\infty\}\cup\{v\nmid\infty\mid \phi_v\neq \mathbf{1}_{\mathcal{O}_v}\}\cup\{v\nmid\infty\mid \chi_v \text{ is ramified}\}.$$

is a finite set. On the other hand Proposition 17.1 implies that $Z_v(\phi_v,\chi_v,s)$ is absolutely converges for $\mathrm{Re}(s)>0$. We conclude that $Z(\phi,\chi,s)$ absolutely converges for $\mathrm{Re}(s)>1$.

Proposition 17.1. For $v\in|K|_f$,

1) $Z_v(\phi_v,\chi_v,s)$ is absolutely converges for $\mathrm{Re}(s)>0$, and it extends to a rational function in q_v^{-s}.

2) There exists $L_v(\chi_v,s)\in\mathbb{C}[[q_v^{-s}]]$, such that $Z_v(\phi_v,\chi_v,s)\in L_v(\chi_v,s)\mathbb{C}[q^{\pm s}]$.

3) If χ_v is unramified (i.e., $\chi_v(\mathcal{O}_v^\times)=1$), then

$$L_v(\chi_v,s)=\frac{1}{1-\frac{\chi_v(\pi_v)}{\mathrm{N}(\mathfrak{p})^s}}$$

and $Z_v(\mathbf{1}_{\mathcal{O}_v},\chi_v,s)=L_v(\chi_v,s)$.

4) If χ_v is ramified with conductor $\mathfrak{p}^{f_v}$, $f_v\geq 1$, then $L_v(\chi_v,s)=1$ and

$$Z_v(\mathbf{1}_{1+\mathfrak{p}^{f_v}},\chi_v,s)=q_v^{1-f_v}(q_v-1)^{-1}.$$

Proof. Since ϕ_v is locally constant and of compact support, it is enough to take $\phi_v=\mathbf{1}_{a+\mathfrak{p}^N}$ (see the proof of Proposition 17.3).

$$Z_v(\mathbf{1}_{a+\mathfrak{p}^N},\chi_v,s)=\int_{K_v^\times}\mathbf{1}_{a+\mathfrak{p}^N}(x)\chi_v(x)|x|_v^s\mathrm{d}^\times x_v.$$

1) If $\mathrm{val}(a)<N$, then $|x|_v^s=|a|_v^s$, the integral is equal to

$$\mathbb{C}[q_v^{\pm s}]\ni\int_{a+\mathfrak{p}^n}\chi_v(x)|a|_v^s\mathrm{d}^\times x_v=|a|_v^s\int_{a+\mathfrak{p}^n}\chi_v(x)\mathrm{d}^\times x_v.$$

2) If $\mathrm{val}(a)\geq N$, then $a+\mathfrak{p}^N=\mathfrak{p}^N$, the integral equals

$$\begin{aligned}\int_{\mathfrak{p}^N\backslash\{0\}}\chi_v(x)|x|_v^s\mathrm{d}^\times x_v&=\sum_{m=N}^{+\infty}\int_{\pi^m\mathcal{O}_v^\times}\chi_v(x)q_v^{-ms}\mathrm{d}^\times x_v\\&=\left(\sum_{m=N}^{+\infty}\chi_v(\pi)^m q_v^{-ms}\right)\int_{\mathcal{O}_v^\times}\chi_v(x)\mathrm{d}^\times x_v\\&=\frac{\chi_v(\pi)^N q_v^{-Ns}}{1-\frac{\chi_v(\pi)}{q_v^s}}\int_{\mathcal{O}_v^\times}\chi_v(x)\mathrm{d}^\times x_v.\end{aligned}$$

3) If χ is unramified,

$$\int_{\mathcal{O}_v^\times} \chi_v(x)\mathrm{d}^\times x_v = \int_{\mathcal{O}_v^\times} \mathrm{d}^\times x_v = 1.$$

4) If χ is ramified, $\chi_v|_{\mathcal{O}_v^\times}$ is non-trivial,

$$\int_{\mathcal{O}_v^\times} \chi_v(x)\mathrm{d}^\times x_v = 0.$$

We have

$$Z_v(\mathbf{1}_{1+\mathfrak{p}^{f_v}}, \chi_v, s) = \int_{1+\mathfrak{p}^{f_v}} \mathrm{d}^\times x_v = q_v^{1-f_v}(q_v-1)^{-1}.$$

□

Now we consider the Fourier transform on $(\mathbb{A}_K, +)$.

Example 17.2. We define the nontrivial additive character on the local field.

1) If $K_v = \mathbb{R}$, choose $\psi_v(x) = \mathrm{e}^{-2\pi\mathrm{i}x}$; if $K_v = \mathbb{C}$, choose $\psi_v(z) = \mathrm{e}^{-2\pi\mathrm{i}(z+\overline{z})}$.

2) If $K_v = \mathbb{Q}_p$, choose $\psi_v(x) = \mathrm{e}^{2\pi\mathrm{i}\{x\}}$. Here for $x = a_{-n}p^{-n} + \cdots + a_{-1}p^{-1} + a_0 + \cdots \in \mathbb{Q}_p$, define $\{x\} \coloneqq a_{-n}p^{-n} + \cdots + a_{-1}p^{-1} \in \mathbb{Q}$.

3) If $K_v/\mathbb{Q}_p$ is finite extension, consider

$$\psi_v \colon K_v \xrightarrow{\mathrm{Tr}} \mathbb{Q}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{\mathrm{e}^{2\pi\mathrm{i}x}} \mathrm{U}(1).$$

is a continuous character. That is, $\psi_v(x) = \mathrm{e}^{2\pi\mathrm{i}\left\{\mathrm{Tr}_{F/\mathbb{Q}_p} x\right\}}$.

Proposition 17.2. Consider the bilinear pairing

$$K_v \times K_v \longrightarrow \mathbb{Q}_p \longrightarrow \mathrm{U}(1), \quad (x, y) \longmapsto \psi_v(xy).$$

It is non-degenerated. It induces an isomorphism

$$\widehat{K_v} = \mathrm{Hom}(K_v, \mathrm{U}(1)) \cong K_v.$$

Definition 17.4. Function on K_v is called **Bruhat–Schwartz** if it is locally constant and of compact support. Let $\mathcal{S}(K_v)$ be the space of Bruhat–Schwartz functions.

Proposition 17.3. For $\phi_v \in \mathcal{S}(K_v)$, define its **Fourier transform** as

$$\widehat{\phi_v}(\xi) = \int_{K_v} \phi_v(x)\psi_v(x\xi)\mathrm{d}x,$$

then $\widehat{\phi_v}(\xi) \in \mathcal{S}(K_v)$.

Proof. Let $\phi_v \in \mathcal{S}(K_v)$, let $x \in \operatorname{Supp}(\phi_v)$, there exists open neighborhoood $U_x \ni x$ such that $\phi_v|_{U_x}$ is a constant. One can choose $a_x + \varpi^{n_x}\mathcal{O}_v \subseteq U_x$, where ϖ is the uniformizer of $\mathcal{O}_v$. it follows that $\operatorname{Supp}(\phi_v) \subseteq \bigcup_{x\in\operatorname{Supp}(\phi_v)} a_x + \varpi^{n_x}\mathcal{O}_v$. Since $\operatorname{Supp}(\phi_v)$ is compact, there exists finite subcover $\operatorname{Supp}(\phi_v) \subseteq \bigcup_{i=1}^m a_i + \varpi^{n_i}\mathcal{O}_v$. If $(a+\varpi^n\mathcal{O}_v)\cap(b+\varpi^m\mathcal{O}_v) \neq \emptyset$, choose $x \in (a+\varpi^n\mathcal{O}_v)\cap(b+\varpi^m\mathcal{O}_v)$. We may assume $n \geq m$, then $a-x \in \varpi^n\mathcal{O}_v \subseteq \varpi^m\mathcal{O}_v$, $x-b \in \varpi^m\mathcal{O}_v$, and so $a-b \in \varpi^m\mathcal{O}_v$. Thus $a+\varpi^n\mathcal{O}_v \subseteq a+\varpi^m\mathcal{O}_v = b+\varpi^m\mathcal{O}_v$. Thus we may assume $a_i+\varpi^{n_i}\mathcal{O}_v$ are disjoint, get

$$\phi_v = \sum_{i=1}^m c_i \mathbf{1}_{a_i+\varpi^{n_i}\mathcal{O}_v}.$$

So it only suffices to prove the Proposition for

$$\mathbf{1}_{a+\varpi^n\mathcal{O}_v}.$$

We have

$$\widehat{\mathbf{1}_{a+\varpi^n\mathcal{O}_v}}(\xi) = \int_{a+\varpi^n\mathcal{O}_v} \psi_v(x\xi)\mathrm{d}x = \psi_v(a\xi)\int_{\varpi^n\mathcal{O}_v}\psi_v(x\xi)\mathrm{d}x$$

by replacing $x \mapsto a+x$. Since $\mathrm{d}(\varpi^n x) = |\varpi|^n\mathrm{d}x$, by replacing $x \mapsto \varpi^n x$ we obtain

$$\widehat{\mathbf{1}_{a+\varpi^n\mathcal{O}_v}}(\xi) = |\varpi|^n\psi_v(a\xi)\int_{\mathcal{O}_v}\psi_v(x\varpi^n\xi)\,\mathrm{d}x$$

Fix ξ, $x \mapsto \psi_v(x\varpi^n\xi)$ is an additive character. The character is trivial on $\mathcal{O}_v$ iff $\operatorname{Tr}_{K_v/\mathbb{Q}_p}(x\varpi^n\xi) \in \mathbb{Z}_p$ for all $x \in \mathcal{O}_v$ iff $\varpi^n\xi \in \delta^{-1}_{K_v/\mathbb{Q}_p} = \left\{y \in K_v \mid \operatorname{Tr}_{K_v/\mathbb{Q}_p}(xy) \in \mathbb{Z}_p \text{ for all } x \in \mathcal{O}_v\right\}$. If $\varpi^n\xi \in \delta^{-1}_{K_v/\mathbb{Q}_p}$, then

$$\int_{\mathcal{O}_v}\psi_v(x\varpi^n\xi)\,\mathrm{d}x = \int_{\mathcal{O}_v}\mathrm{d}x = \left|\Delta_{K_v/\mathbb{Q}_p}\right|^{-\frac{1}{2}}.$$

If $\varpi^n\xi \notin \delta^{-1}_{K_v/\mathbb{Q}_p}$, there exists x_0 such that $\psi_v(x_0\varpi^n\xi) \neq 1$, so

$$\int_{\mathcal{O}_v}\psi_v(x\varpi^n\xi)\,\mathrm{d}x = \int_{\mathcal{O}_v}\psi_v((x+x_0)\varpi^n\xi)\,\mathrm{d}x = \psi_v(x_0\varpi^n\xi)\int_{\mathcal{O}_v}\psi_v(x\varpi^n\xi)\,\mathrm{d}x,$$

which forces

$$\int_{\mathcal{O}_v}\psi_v(x\varpi^n\xi)\,\mathrm{d}x = 0$$

We conclude

$$\widehat{\mathbf{1}_{a+\varpi^n\mathcal{O}_v}}(\xi) = |\varpi|^n\psi_v(a\xi)\left|\Delta_{K_v/\mathbb{Q}_p}\right|^{-\frac{1}{2}}\mathbf{1}_{\varpi^{-n}\delta^{-1}_{K_v/\mathbb{Q}_p}}(\xi).$$

Since $\xi \mapsto \psi_v(a\xi)$ is locally constant and $\varpi^{-n}\delta^{-1}_{K_v/\mathbb{Q}_p}$ is compact open, we get the conclusion. $\square$

Proposition 17.4. Consider the bilinear form

$$\mathbb{A}_K \times \mathbb{A}_K \longrightarrow \mathrm{U}(1), \quad (x,y) \longmapsto \prod_{v\in|K|}\psi_v(x,y),$$

it is non-degenerated, hence

$$\widehat{\mathbb{A}_K} = \mathrm{Hom}(\mathbb{A}_K, \mathrm{U}(1)) \cong \mathbb{A}_K.$$

Proposition 17.5. For $\phi \in \mathcal{S}(\mathbb{A}_K) = \prod' \mathcal{S}(K_v)$, define its Fourier transform as

$$\widehat{\phi}(\xi) = \int_{\mathbb{A}_K} \phi(x)\psi(x\xi)\mathrm{d}x,$$

then $\widehat{\phi}(\xi) \in \mathcal{S}$.

Theorem 17.1 (Poisson summation formula)**.** For arbitrary $\phi \in \mathcal{S}(\mathbb{A}_K)$, then

$$\sum_{x\in K} \phi(x) = \sum_{\xi \in K} \widehat{\phi}(\xi).$$

Proof. Consider

$$\varphi(y) = \sum_{x\in K} \phi(y+x), \quad y \in \mathbb{A}_K.$$

The sum is convergent since ϕ is Bruhat–Schwartz. Then we have

$$\varphi(x) = \sum_{\xi\in K} C(\xi)\psi(-\xi x),$$

where

$$C(\xi) = \int_{K\backslash \mathbb{A}_K} \varphi(x)\psi(\xi x)\mathrm{d}x.$$

One compute

$$\begin{aligned} C(\xi) &= \int_{K\backslash \mathbb{A}_K} \sum_{y\in K} \phi(x+y)\psi(\xi x)\mathrm{d}x \\ &= \int_{K\backslash \mathbb{A}_K} \sum_{y\in K} \phi(x+y)\psi(\xi(x+y))\mathrm{d}x \\ &= \int_{\mathbb{A}_K} \phi(x)\psi(\xi x)\mathrm{d}x \\ &= \widehat{\phi}(\xi). \end{aligned}$$

Here $\xi y \in K$ implies that $\psi(\xi y) = 1$. Hence

$$\sum_{x\in K} \phi(x+y) = \sum_{\xi\in K} \widehat{\phi}(\xi)\psi(\xi y).$$

Setting $y = 0$ we finish the proof. ∎

Theorem 17.2.

$$Z(\phi, \chi, s) = Z\left(\widehat{\phi}, \chi^{-1}, 1-s\right).$$

Proof. By definition

$$Z(\phi,\chi,s)=\int_{\mathbb{A}_K^\times}\phi(x)\chi(x)\|x\|_K^s\mathrm{d}^\times x=\left(\int_{\mathbb{A}_K^{>1}}+\int_{\mathbb{A}_K^{<1}}\right)\phi(x)\chi(x)\|x\|_K^s\mathrm{d}^\times x,$$

where $\mathbb{A}_K^{<1}=\left\{x\in\mathbb{A}_K^\times \mid \|x\|_K<1\right\}$. Indeed, the measure of $\mathbb{A}_K^{\times,1}$ is zero. For arbitrary $s\in\mathbb{C}$, there exists $\sigma_0>\max\{1,\mathrm{Re}(s)\}$, so $\|x\|_K^{\mathrm{Re}(s)}\le\|x\|_K^{\sigma_0}$ on $\mathbb{A}_K^{>1}$. Hence

$$Z^{>1}=\int_{\mathbb{A}_K^{>1}}\phi(x)\chi(x)\|x\|_K^s\mathrm{d}^\times x$$

converges for all s and

$$Z^{<1}=\int_{\mathbb{A}_K^{<1}}\phi(x)\chi(x)\|x\|_K^s\mathrm{d}^\times x$$

converges for $\mathrm{Re}(s)>1$.

Now compute

$$\begin{aligned}Z^{<1}&=\int_{K^\times\backslash\mathbb{A}_K^{<1}}\sum_{\alpha\in K^\times}\phi(\alpha x)\chi(\alpha x)\|\alpha x\|_K^s\mathrm{d}^\times x\\&=\int_{K^\times\backslash\mathbb{A}_K^{<1}}\sum_{\alpha\in K^\times}\phi(\alpha x)\chi(x)\|x\|_K^s\mathrm{d}^\times x\\&=\int_{K^\times\backslash\mathbb{A}_K^{<1}}\sum_{\alpha\in K}\phi(\alpha x)\chi(x)\|x\|_K^s\mathrm{d}^\times x-\phi(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}}\chi(x)\|x\|_K^s\mathrm{d}^\times x.\end{aligned}$$

Apply Theorem 17.1 to $x\mapsto\phi(\alpha x)$, note that

$$\begin{aligned}\int_{K_v}\phi_v(\alpha_vx_v)\psi_v(x_vy_v)\mathrm{d}x_v&=\frac{1}{|\alpha_v|_v}\int_{K_v}\phi_v(x_v)\psi\left(\alpha_v^{-1}x_vy_v\right)\mathrm{d}x_v\\&=\frac{1}{|\alpha_v|_v}\widehat{\phi_v}\left(\alpha_v^{-1}y_v\right),\end{aligned}$$

we obtain

$$\|\alpha\|_K\sum_{x\in K}\phi(\alpha x)=\sum_{x\in K}\widehat{\phi}\left(\alpha^{-1}x\right).$$

That is,

$$\sum_{\alpha\in K}\phi(\alpha x)=\|x\|_K^{-1}\sum_{\alpha\in K}\widehat{\phi}\left(\alpha x^{-1}\right).$$

It follows that

$$\begin{aligned}Z^{<1}&=\int_{K^\times\backslash\mathbb{A}_K^{<1}}\sum_{\alpha\in K}\widehat{\phi}\left(\alpha x^{-1}\right)\chi(x)\|x\|_K^{s-1}\mathrm{d}^\times x-\phi(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}}\chi(x)\|x\|_K^s\mathrm{d}^\times x\\&=\int_{K^\times\backslash\mathbb{A}_K^{<1}}\sum_{\alpha\in K^\times}\widehat{\phi}\left(\alpha x^{-1}\right)\chi(x)\|x\|_K^{s-1}\mathrm{d}^\times x+\widehat{\phi}(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}}\chi(x)\|x\|_K^{s-1}\mathrm{d}^\times x-\phi(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}}\chi(x)\|x\|_K^s\mathrm{d}^\times x\\&=\int_{\left(K^\times\backslash\mathbb{A}_K^{<1}\right)^{-1}}\sum_{\alpha\in K^\times}\widehat{\phi}\left(\alpha x\right)\chi(x)^{-1}\|x\|_K^{1-s}\mathrm{d}^\times x+\widehat{\phi}(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}}\chi(x)\|x\|_K^{s-1}\mathrm{d}^\times x-\phi(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}}\chi(x)\|x\|_K^s\mathrm{d}^\times x\\&=\int_{\mathbb{A}_K^{>1}}\widehat{\phi}\left(x\right)\chi(x)^{-1}\|x\|_K^{1-s}\mathrm{d}^\times x+\widehat{\phi}(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}}\chi(x)\|x\|_K^{s-1}\mathrm{d}^\times x-\phi(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}}\chi(x)\|x\|_K^s\mathrm{d}^\times x.\end{aligned}$$

Similarly

$$\int_{\mathbb{A}_K^{\geq 1}} \widehat{\phi}(x)\,\chi(x)^{-1}\|x\|_K^{1-s}\mathrm{d}^\times x$$

converges for all s.

We have split exact sequence

$$0 \longrightarrow \mathbb{A}_K^{\times,1} \longrightarrow \mathbb{A}_K^\times \xrightarrow{\|\cdot\|_K} \mathbb{R}_+^\times \longrightarrow 0\ ,$$

It follows that $\mathbb{A}_K^\times = \mathbb{A}_K^{\times,1} \times \mathbb{R}_+^\times$, so $\mathbb{A}_K^{<1} = \mathbb{A}_K^{\times,1} \times (0,1)$, and so $K^\times\backslash\mathbb{A}_K^{<1} = \left(K^\times\backslash\mathbb{A}_K^{\times,1}\right) \times (0,1)$. Thus

$$\begin{aligned}&\widehat{\phi}(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}} \chi(x)\|x\|_K^{s-1}\mathrm{d}^\times x - \phi(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}} \chi(x)\|x\|_K^{s}\mathrm{d}^\times x\\ =&\ \widehat{\phi}(0)\int_{K^\times\backslash\mathbb{A}_K^{\times,1}} \chi(x)\mathrm{d}^\times x\int_0^1 t^{s-1}\frac{\mathrm{d}t}{t} - \phi(0)\int_{K^\times\backslash\mathbb{A}_K^{\times,1}} \chi(x)\mathrm{d}^\times x\int_0^1 t^{s}\frac{\mathrm{d}t}{t}.\end{aligned}$$

If $\chi|_{\mathbb{A}_K^{\times,1}}$ is nontrivial, then the above equation equals to zero. If not, χ depends only on $\|x\|$ for $x \in \mathbb{A}_K^\times$, and there character $\mathbb{R}_+^\times \to \mathbb{C}^\times$ must be $(\cdot)^\lambda$ where $\lambda = \mathrm{i}\mathbb{R}$. Hence χ is trivial on $\mathbb{A}_K^{\times,1}$ iff there exists $\lambda = \mathrm{i}\mathbb{R}$ such that $\chi(x) = \|x\|^\lambda$. It follows that

$$\begin{aligned}&\widehat{\phi}(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}} \chi(x)\|x\|_K^{s-1}\mathrm{d}^\times x - \phi(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}} \chi(x)\|x\|_K^{s}\mathrm{d}^\times x\\ =&\ \widehat{\phi}(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}} \|x\|_K^{s-1+\lambda}\mathrm{d}^\times x - \phi(0)\int_{K^\times\backslash\mathbb{A}_K^{<1}} \|x\|_K^{s+\lambda}\mathrm{d}^\times x\\ =&\ \widehat{\phi}(0)\int_{K^\times\backslash\mathbb{A}_K^{\times,1}}\int_0^1 t^{s-1+\lambda}\frac{\mathrm{d}t}{t} - \phi(0)\int_{K^\times\backslash\mathbb{A}_K^{\times,1}}\int_0^1 t^{s+\lambda}\frac{\mathrm{d}t}{t},\end{aligned}$$

which is absolutely converges for $\mathrm{Re}(s)$ sufficiently large, and equals to

$$\frac{\widehat{\phi}(0)\,\mathrm{vol}\left(K^\times\backslash\mathbb{A}_K^{\times,1}\right)}{s-1+\lambda} - \frac{\phi(0)\,\mathrm{vol}\left(K^\times\backslash\mathbb{A}_K^{\times,1}\right)}{s+\lambda}.$$

Consequently, if $\chi|_{\mathbb{A}_K^{\times,1}}$ is nontrivial,

$$Z(\phi,\chi,s) = \int_{\mathbb{A}_K^{\geq 1}} \phi(x)\chi(x)\|x\|_K^s\mathrm{d}^\times x + \int_{\mathbb{A}_K^{\geq 1}} \widehat{\phi}(x)\,\chi(x)^{-1}\|x\|_K^{1-s}\mathrm{d}^\times x;$$

if $\chi(x) = \|x\|^\lambda$, $\lambda \in \mathrm{i}\mathbb{R}$, then

$$Z(\phi,\chi,s) = \int_{\mathbb{A}_K^{\geq 1}} \phi(x)\chi(x)\|x\|_K^s\mathrm{d}^\times x + \int_{\mathbb{A}_K^{\geq 1}} \widehat{\phi}(x)\,\chi(x)^{-1}\|x\|_K^{1-s}\mathrm{d}^\times x + \frac{\widehat{\phi}(0)\,\mathrm{vol}\left(K^\times\backslash\mathbb{A}_K^{\times,1}\right)}{s-1+\lambda} - \frac{\phi(0)\,\mathrm{vol}\left(K^\times\backslash\mathbb{A}_K^{\times,1}\right)}{s+\lambda}.$$

We conclude that $Z(\phi,\chi,s)$ admits meromorphic continuation, and satisfies the following functional equation:

$$Z(\phi,\chi,s) = Z\left(\widehat{\phi},\chi^{-1},1-s\right).$$

$\square$