Number theory I

Yiwen Ding

Contents

Chapter 1

Algebraic integers

We introduce the basic theory of algebraic integers.

1.1 Gaussian Integers

We begin with a famous theorem.

Theorem 1.1.1. *Let p be an odd prime number, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ if and only if $p \equiv 1 \pmod 4$.*

The direction "only if" is easy. Note $p = a^2 + b^2$ is equivalent to $p = (a + bi)(a - bi)$. Then it is natural to work with the ring $\mathbb{Z}[i]$.

Definition 1.1.2. *Let R be a commutative ring (with unit). We call R is euclidean if there exists $f : R \to \mathbb{Z}_{\geq 0}$ such that for all $\alpha, \beta \in R$,*

1. *$f(\alpha) = 0 \Leftrightarrow \alpha = 0$,*
2. *$f(\alpha\beta) = f(\alpha)f(\beta)$,*
3. *if $\beta \neq 0$, then there exist $\gamma, \delta \in R$ such that $\alpha = \beta\gamma + \delta$ and $f(\delta) < f(\beta)$.*

Example 1.1.3. *$\mathbb{Z}$ is euclidean with $f := |\cdot|$.*

Proposition 1.1.4. *If R is euclidean, then R is a principal ideal domain.*

Proof. Using the conditions 1&2, one sees R is a domain. Let I be an ideal of R, and let $\beta \in I$ such that $f(\beta) = \min_{0 \neq \alpha \in I} f(x)$. For $\alpha \in I$, there exists δ such that $\alpha = \beta\gamma + \delta$ and $f(\delta) < f(\beta)$. Since $\delta \in I$, we deduce by the choice of β that $\delta = 0$. Hence $I = (\beta)$. □

Proposition 1.1.5. *$\mathbb{Z}[i]$ is euclidean.*

Proof. Put $f : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$, $a + bi \mapsto a^2 + b^2$. We check f satisfies the conditions in the definition. The conditions 1 and 2 are clear. Let $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Consider

$\alpha/\beta = x + yi \in \mathbb{C}$. There exists thus $\gamma = a + bi \in \mathbb{Z}[i]$, such that $|x - a| \leq 1/2$ and $|y - b| \leq 1/2$. We deduce $|\alpha/\beta - \gamma|^2 \leq 1/2$. Putting $\delta := \alpha - \beta\gamma$, we have $|\delta| < |\beta|$. The proposition follows. □

Corollary 1.1.6. *$\mathbb{Z}[i]$ is a PID.*

Proposition 1.1.7. *There exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ if and only if (p) is not a prime ideal in $\mathbb{Z}[i]$. (Recall an ideal I is called a prime ideal if $I \supset I_1 I_2 \Rightarrow I \supset I_1$ or $I \supset I_2$).*

Proof. If $p = a^2 + b^2$, then $p = (a+bi)(a-bi)$. If (p) is a prime ideal then $(p) \supset (a+bi)$ or $(p) \supset (a - bi)$. Replacing b by $-b$ if needed, we assume $(p) \supset (a + bi)$. Then there exists $x \in \mathbb{Z}[i]$ such that $a + bi = px$. This implies $p = px(a - bi)$ and hence $p(1 - x(a - bi)) = 0$. Since $\mathbb{Z}[i]$ is a domain, we deduce $x(a - bi) = 1$. Hence $|x|^2|a^2 + b^2| = 1$ a contradiction (noting $|x|^2 \in \mathbb{Z}_{>0}$).

Now assume p is not a prime ideal. By definition (and the fact that $\mathbb{Z}[i]$ is a PID), there exist α, $\beta \in \mathbb{Z}[i]$ such that $p = \alpha\beta$ and that α, β are not units. This implies $|p|^2 = |\alpha|^2|\beta|^2$. Since α, β are not units, $|\alpha|^2 > 1$ and $|\beta|^2 > 1$ (say, if $|\alpha|^2 = 1$, then $\alpha\bar{\alpha} = 1$ and hence α is a unit). We deduce then $|\alpha|^2 = |\beta|^2 = p$. Writing $\alpha = a + bi$, we see the "if" part follows. □

Proof of Theorem 1.1.1. We only need to prove the "if" part. By the above proposition, it suffices to show if $p = 1+4n$, then p is not prime in $\mathbb{Z}[i]$. Consider the finite field $\mathbb{F}_p$. Recall that the multiplicative group of a finite field is a cyclic group (Exercise). In particular, $\mathbb{F}_p^*$ is a cyclic group of order $p - 1 = 4n$. This implies that there exists $x \in \mathbb{Z}$ such that $x^4 \equiv 1 \pmod{p}$, $x^2 \neq 1 \pmod{p}$. So $x^2 \equiv -1 \pmod{p}$. Hence $p|(x^2 + 1) \Rightarrow p|(x + i)(x - i)$. If p is prime, without loss of generality, we have $p|(x + i)$. So there exists $\alpha = y + zi \in \mathbb{Z}[i]$ such that $x + i = p(y + zi) = py + pzi$, hence $pz = 1$, a contradiction. This concludes the proof. □

Remark 1.1.8. *Some key words in the proof: ideals, units, finite field (residue field).*

Definition 1.1.9. *We call a finite extension of $\mathbb{Q}$ a number field.*

Exercise 1.1.10. *Let K be a number field, show that there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.*

The ring $\mathbb{Z}[i]$ plays a key role in the proof of the theorem. A natural question is that what is the analogue of $\mathbb{Z}[i]$ for an arbitrary number field?

Exercise 1.1.11. *Show that $\mathbb{Z}[2i]$ is not a PID.*

1.2 Integral extensions (commutative algebra)

Definition 1.2.1. *Let $A \hookrightarrow B$ be commutative rings with* 1.

(1) An element $b \in B$ is called integral over A if there exists a monic polynomial $f(x) \in A[x]$ such that $f(b) = 0$.

(2) The ring B is called integral over A if all elements of B are integral over A.

Example 1.2.2. *$\mathbb{Z}[i]$ is integral over $\mathbb{Z}$: For any $\alpha = a+bi \in \mathbb{Z}[i]$, $\alpha^2 - 2a\alpha + (a^2+b^2) = 0$.*

Definition 1.2.3. *Let $K/\mathbb{Q}$ be a number field, $\alpha \in K$ is called an algebraic integer, if α is integral over $\mathbb{Z}$.*

Let $\mathcal{O}_K := \{\text{algebraic integers of } K\}$.

Proposition 1.2.4. *Let $A \subset B$ be commutative rings with 1, let $b \in B$. Then b is integral over A if and only if there exists an A-subalgebra C of B that is finitely generated as A-module such that $A[b] \subseteq C$.*

Proof. "Only if": Suppose b is integral over A. There exists thus $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ such that $f(b) = 0$. Then we see $A[b]$ is generated (as an A-module) by $\{1, \cdots, b^{n-1}$. We can then choose $C := A[b]$.

"If": Since C is a finitely generated A-module, there exist $v_1, \cdots, v_k \in C$ such that $C = Av_1 + \cdots Av_k$. Since $bC \subseteq C$ (using $A[b] \subset C$), there exists $M = (a_{ij}) \in M_{k\times k}(A)$ such that

$$\begin{pmatrix} bv_1 \\ \vdots \\ bv_k \end{pmatrix} = M \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}.$$

This implies

$$N \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} := \begin{pmatrix} b - a_{11} & \cdots & -a_{1k} \\ \vdots & \ddots & \vdots \\ -a_{k1} & \cdots & b - a_{kk} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = 0.$$

Let $N^* \in M_{k\times k}(A[b])$ be the adjoint matrix of N, we have $N^*N \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = 0$, and $N^*N = \operatorname{diag}(f(b), \cdots, f(b))$ where $f(b) = \det(N)$ is of the form $b^k + a_{k-1}b^{k-1} + \cdots + a_0$. Thus $f(b)v_i = 0$ for all v_i, implying $f(b)C = 0 \Rightarrow f(b)1 = 0 \Rightarrow f(b) = 0$. So b is integral over A. □

Corollary 1.2.5. *Let $A \hookrightarrow B$ be commutative rings with 1, let $\alpha, \beta \in B$ be integral over A. Then $\alpha + \beta$, $\alpha\beta$ are also integral over A.*

Proof. Since β is integral over A, β is integral over $A[\alpha]$. By the above proposition (and the proof), $A[\alpha][\beta]$ is a fintiely generated $A[\alpha]$-module. Since α is integral over A, $A[\alpha]$ is a finitely generated A-module. Hence $A[\alpha][\beta]$ is a finitely generated A-module. Thus $\alpha + \beta$, $\alpha\beta$ are integral. □

Corollary 1.2.6. *$\mathcal{O}_K$ is a $\mathbb{Z}$-algebra.*

Corollary 1.2.7. *Let $A \subset B \subset C$ be commutative rings with 1. If C is integral over B, and B is integral over A, then C is integral over A.*

Proof. Let $c \in C$, there exist thus $b_0, \cdots, b_{n-1} \in B$ such that

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0.$$

This implies that $A[b_0, \cdots, b_{n-1}][C]$ is a finitely generated $A[b_0, \cdots, b_{n-1}]$-module. Since B is integral over A, $A[b_0, \cdots, b_{n-1}]$ is a finitely generated A-module. Hence $A[b_0, \cdots, b_{n-1}][c]$ is a finitely generated A-module. So c is integral over A. □

Definition 1.2.8. *(1) Let $A \subset B$ be commutative rings with 1, $\{x \in B \mid x$ integral over $A\}$ is called the integral closure of A in B.*

(2) If A is morover a domain, we call A integrally closed if A is equal to its integral closure in $\mathrm{Frac}(A)$.

Proposition 1.2.9. *Let K be a number field, then $\mathcal{O}_K$ is integrally closed.*

Proof. If $x \in K$ is integral over $\mathcal{O}_K$, by the above corollary, x is integral over $\mathbb{Z}$, and hence $x \in \mathcal{O}_K$. □

Lemma 1.2.10. *A UFD R is integrally closed.*

Proof. Let $K := \mathrm{Frac}(R)$, and let $\alpha = \frac{a}{b} \in K$ with $(a, b) = 1$. Suppose α is integral over R, then there exists $c_0, \cdots, c_{n-1} \in R$ such that

$$(\frac{a}{b})^n + c_{n-1}(\frac{a}{b})^{n-1} + \cdots + c_0 = 0$$

which implies $a^n + c_{n-1}ba^{n-1} + \cdots + a_0b^n = 0$. So $b|a^n$, a contradiction. □

Exercise 1.2.11. *Let R be a commutative ring with 1, I, J be ideals of R. Suppose $I + J = R$, show that $I + J^n = R$ for any $n \in \mathbb{Z}_{\geq 1}$.*

Example 1.2.12. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$.

Exercise 1.2.13. *Let K be a number field, $d := [K : \mathbb{Q}]$ and let $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. Show that there exists $x \in \mathbb{Q}$ such that $\alpha_0 := x\alpha \in \mathcal{O}_K$, and conclude that $\mathcal{O}_K \supset \mathbb{Z} \oplus \mathbb{Z}\alpha_0 \oplus \cdots \oplus \mathbb{Z}\alpha_0^{d-1}$.*

Proposition 1.2.14. *Let A be an integral closed domain, $K := \mathrm{Frac}(A)$. Let L be a finite extension of K, B be the integral closure of A in L. Then $b \in B$ if and only if the monic minimal polynomial of b over K has coefficient in A.*

Proof. The "if" part is trivial. For the "only if"' part, it is easy to see that we can replace L be its normal closure, so that we can assume L is normal over K. Let $p(x)$ be the monic minimal polynomial of b in K, and let $g(x) \in A[x]$ be a monic polynomial such that $g(b) = 0$ (since b is integral over A). This implies $p(x)|g(x)$ (as polynomials over K).

However, any root of $g(x)$ are integral over A, and hence any root of $p(x)$ are integral over A. The coefficients of $p(x) \in K[x]$ are polynomially generated by the roots of $p(x)$, hence are also integral over A. Since A is integrally closed, $p(x) \in A[x]$. This concludes the proof. □

Remark 1.2.15. *By the proposition, for a number field $K/\mathbb{Q}$, to check if an element α lies in $\mathcal{O}_K$, we only need to work out its minimal polynomial over $\mathbb{Q}$.*

Exercise 1.2.16. *Let K be a quadratic extension of $\mathbb{Q}$, describe explicitly the ring $\mathcal{O}_K$.*

1.3 Trace and norm

Let L/K be a fintie extension of fields of degree d. In particular L is a d-dimensional K-vector space. To any $x \in L$, we associate a K-linear map $r_x : L \to L$, $\alpha \mapsto x\alpha$.Let $\mathrm{Tr}_{L/K}(x) \in K$ be the trace of r_x, and $N_{L/K}(x) \in K$ be the determinant of r_x, and $f_x(T) := \det(TI_d - r_x) \in K[T]$ be the characteristic polynomial of r_x.

Proposition 1.3.1. *Let L/K be a separable finite extension, $\Sigma_L := \{\sigma : L \hookrightarrow \overline{K} \mid \sigma|_K = \mathrm{id}\}$. Then we have*

1. $f_x(T) = \prod_{\sigma\in\Sigma_L}(T - \sigma(x))$,
2. $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma\in\Sigma_L}\sigma(x)$,
3. $N_{L/K}(x) = \prod_{\sigma\in\Sigma_L}\sigma(x)$.

Proof. Consider $K \subset K(x) \subset L$. Let $p(t)$ be the minimal polynomial of x over K, $d_1 := \deg(p(t))$. Thus $K(x) = K \oplus Kx \oplus \cdots \oplus Kx^{d_1-1}$. Let $\{e_i\}_{i=1,\cdots,d_2}$ be a basis of L over $K(x)$ (so $d_1d_2 = d = [L : K]$). We see $\{x^je_i\}_{\substack{j=0,\cdots,d_1-1,\\ i=1,\cdots,d_2}}$ is a basis of L over K. Suppose $p(x) = x^{d_1} + c_{d_1-1}x^{d_1-1} + \cdot + c_0$, and let

$$A := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{d_1-1} \end{pmatrix} \in \mathrm{GL}_{d_1}(K).$$

Then $r_x(e_1, \cdots, x^{d_1-1}e_1, e_2, \cdots, e_{d_2}, \cdots, e_{d_2}x^{d_1-1}) = (e_1, \cdots, e_{d_2}x^{d_1-1}) \begin{pmatrix} A & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A \end{pmatrix}$. We have $\det(TI_{d_1} - A) = p(T) = \prod_{\sigma\in\Sigma_{K(x)}}(T - \sigma(x))$. Hence $f_x(T) = \prod_{\sigma\in\Sigma_{K(x)}}(T - \sigma(x))^{d_2} = \prod_{\sigma\in\Sigma_L}(T - \sigma(x))$ (noting for all $\sigma \in \Sigma_x$, $\sharp\{\tau : L \hookrightarrow \overline{K} \mid \tau|_{K(x)} = \sigma\} = d_2$). We then deduce $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma\in\Sigma_L}\sigma(x)$ and $N_{L/K}(x) = \prod_{\sigma\in\Sigma_L}\sigma(x)$. □

Corollary 1.3.2. *Let $K \subset L \subset M$ be finite separable extensions, then $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$, $N_{M/K} = N_{L/K} \circ N_{M/L}$.*

Proof. Exercise. □

Remark 1.3.3. *The statement in the above corollary actually holds without the separable assumption.*

Corollary 1.3.4. *Let $A \subset K$ be integral closed, $B \subset L$ be the integral closure of A in L, then for any $x \in B$, $\mathrm{Tr}_{L/K}(x) \in A$, and $N_{L/K}(x) \in A$.*

Proof. Let $p(T) \in A[T]$ be the minimal polynomial of x over K, $r := \deg p(T) = [K(x) : K]$. Thus $\{1, x, \cdots, x^{r-1}\}$ is a basis of $K(x)$ over K. Writing down the matrix of r_x under this basis, it is easy to see that $\mathrm{Tr}_{K(x)/K}(x) \in A$ and $N_{K(x)/K}(x) \in A$. By the above corollary (and the remark), we have $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{K(x)/K} \circ \mathrm{Tr}_{L/K(x)}(x) = [L : K(x)] \mathrm{Tr}_{K(x)/K}(x) \in A$, and $N_{L/K}(x) = N_{K(x)/K} \circ N_{L/K(x)}(x) = N_{K(x)/K}(x)^{[L:K]}$. □

Let L/K be a finite extension of fields. We have K-bilinear form

$$L \times L \xrightarrow{\langle , \rangle} K, \ (x, y) \mapsto \mathrm{Tr}_{L/K}(xy).$$

Proposition 1.3.5. *Suppose L/K is separable, then the above pairing $\langle , \rangle$ is non-degenerate, i.e. for $x \in L$, if $\mathrm{Tr}_{L/K}(xy) = 0$ for all $y \in L$, then $x = 0$.*

Proof. Fact (linear algebra): $\langle , \rangle$ is non-degenerate if and only for any basis $e_1, \cdots, e_d$ of L over K, the matrix $(\mathrm{Tr}_{L/K}(e_i e_j))_{1 \le i,j \le d} \in M_d(K)$ is invertible.

Let $\alpha \in L$ such that $L = K(\alpha)$, then $\{1, \alpha, \cdots, \alpha^{d-1}\}$ is a basis of L over K. By the previous proposition, $\mathrm{Tr}_{L/K}(\alpha^i \alpha^j) = \sum_{\sigma \in \Sigma_L} \sigma(\alpha^i)\sigma(\alpha^j)$. Writing $\Sigma_L = \{\sigma_0, \cdots, \sigma_{d-1}\}$, we see $(\mathrm{Tr}_{L/K}(\alpha^i \alpha^j)) = AA^T$ for $A = (\sigma_i(\alpha^j))_{0 \le i,j \le d-1}$ (that is a Vandermonde matrice). We have then $\det(A) = \prod_{i \neq j}(\sigma_i(\alpha) - \sigma_j(\alpha)) \neq 0$ (using again L is separable over K). Hence $\det(\mathrm{Tr}_{L/K}(\alpha^i \alpha^j))_{0 \le i,j \le d-1} \neq 0$. The proposition follows. □

Remark 1.3.6. *In particular, when L/K is finite separable, we have a natural isomorphism $L \cong L^\vee$ (as K-vector space).*

Proposition 1.3.7. *Let $K/\mathbb{Q}$ be a number field, $d = [K : \mathbb{Q}]$. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank d.*

Proof. By the exercise, there exist $e_1, \cdots, e_d \in \mathcal{O}_K$ such that $\{e_i\}$ form a basis of K over $\mathbb{Q}$, and that

$$M := \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_d \subseteq \mathcal{O}_K.$$

Let $\tilde{M} := \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z}, \ \forall y \in M\}$. Since $M \subseteq \mathcal{O}_K$, and $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$, we see $\mathcal{O}_K \subseteq \tilde{M}$.

Let $e_i^* \in K$ such that $\mathrm{Tr}_{K/\mathbb{Q}}(e_i^* e_j) = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$ (using the fact $\langle , \rangle$ induces an isomorphism $K \cong K^\vee$). It is easy to see that $\{e_i^*\}$ form a basis of K. We then deduce $\tilde{M} = \mathbb{Z}e_1^* \oplus \cdots \oplus \mathbb{Z}e_d^*$.

In summary, we have

$$M \subseteq \mathcal{O}_K \subseteq \tilde{M},$$

M and $\tilde{M}$ are both free $\mathbb{Z}$-modules of rank d. We deduce then $\mathcal{O}_K$ is also a free $\mathbb{Z}$-module of rank d (e.g. using the structure theorem of abelian groups). □

Let $\alpha_1, \cdots, \alpha_d$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}$, $\{\sigma_1, \cdots, \sigma_d\} = \Sigma_{K/\mathbb{Q}}$. Put

$$\Delta_K := \det((\sigma_i(\alpha_j))_{1 \leq i,j \leq n})^2.$$

We see *a priori* Δ_K lies in the normal closure of K. Since $\sigma_i(\Delta_K) = \Delta_K$ for all σ_i, $\Delta_K \in \mathbb{Q}$. It is also clear that Δ_K is integral over $\mathbb{Z}$, so $\Delta_K \in \mathbb{Z}$. Let $\alpha_1', \cdots, \alpha_d'$ be another basis of $\mathcal{O}_K$ over $\mathbb{Z}$, and $A \in \mathrm{GL}_d(\mathbb{Z})$ such that $(\alpha_1', \cdots, \alpha_d') = (\alpha_1, \cdots, \alpha_d)A$. Then $\det((\sigma_i(\alpha_j'))_{1 \leq i,j \leq n})^2 = \det((\sigma_i(\alpha_j))_{1 \leq i,j \leq n})^2 |\det A|^2 = \Delta_K$. So Δ_K is independent of the choice of the bases of $\mathcal{O}_K$ over $\mathbb{Z}$ (also independent of the order of the elements in $\Sigma_{K/\mathbb{Q}}$, and we call Δ_K the *discriminant* of K.

1.4 Prime decomposition

Some history: consider $z^n = x^n + y^n = \prod_{0 \leq i \leq n-1}(x + \zeta_n^i y)$. Here was a **false** statement: if $\{x + \zeta_n^i y\}$ are coprime with each other, then the above equation implies there exists $z_i \in \mathbb{Z}[\zeta_n]$ such that $(x + \zeta_n^i y) = (z_i)$.

Example 1.4.1. *Consider $K = \mathbb{Q}(\sqrt{-5})$, in this case $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5}$. In $\mathcal{O}_K$, we have*

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

We claim $3, 7, (1 + 2\sqrt{-5}), (1 - 2\sqrt{-5})$ are all prime elements in $\mathcal{O}_K$. We only show that $1 + 2\sqrt{-5}$ is a prime element: if not, write $1 + 2\sqrt{-5} = \alpha\beta$, with α, β non-unit. We have $N_{K/\mathbb{Q}}(1 + 2\sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 21$. If $N_{K/Q}(\alpha) = \alpha\alpha^c = 1$, then α is a unit. Without loss of generality, we assume $N_{K/Q}(\alpha) = 3$. Writing $\alpha = x + y\sqrt{-5}$ (for x, $y \in \mathbb{Z}$), we see $x^2 + 5y^2 = 3$, that is impossible.

We begin with some prelimianries on commutative algebra.

Definition 1.4.2. *Let A be a commutative ring with 1. We call A noetherian if it satisfies the following equivalent conditions:*

1. *Every non-empty set of ideals in A has a maximal element;*
2. *Every asscending chain of ideals is stationary;*
3. *Every ideal of A is finitely generated.*

Proof of equivalence of the conditions. (1) $\Rightarrow$ (2) is trivial.

(2) $\Rightarrow$ (1): if (1) does not hold, one can construct an ascending chain that is not stationary.

(2) $\Rightarrow$ (3): If there exists an ideal I that is not finitely generated. We can then find elements $x_1, \cdots, x_n \cdots$ such that

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \cdots, x_n) \subsetneq \cdots$$

This chain is clearly not stationary.

(3) $\Rightarrow$ (2): Consider an ascending chain of ideals:

$$I_1 \subset I_2 \subset \cdots I_n \subset \cdots$$

Let $I := \sum I_n := \{\sum a_i \mid a_i \in I_i, a_i = 0 \text{ for all but finitely many } i\} = \cup I_n$, that is an ideal of A. By (3), there exsit $\alpha_1, \cdots \alpha_k \in I$ that generate I. For each α_i, there exists n_i such that $\alpha_i \in I_{n_i}$. Hence there exists n such that $\alpha_i \in I_n$ for all i, and hence $I \subseteq I_n$. So the chain is stationary. □

Proposition 1.4.3. *Let A be a noetherian (commutative) ring, M is a finitely generated A-module. Then any submodule of M is finitely generated.*

Proof. We run an induction on the numbers of generators of M.

If M can be generated by one element e. Then we have a surjective map $f : A \twoheadrightarrow M$, $a \mapsto ae$. For any submodule N of M, $f^{-1}(N)$ is an ideal of A, hence is finitely generated. We then easily deduce that N is also finitely generated.

Suppose the statement holds if M can be generated by $(n-1)$-elements. Now suppose M can be generated by n-elements, say, $e_1, \cdots, e_n$. Let M_1 be the submodule of M generated by e_1, and consider

$$M_1 \hookrightarrow M \twoheadrightarrow M/M_1 =: M_2.$$

Let N be a submodule of M. Since M_2 can be generated by the image of $e_2, \cdots, e_n$, by induction hypothesis, the image of N in M_2 is finitely generated. Similarly, $M_1 \cap N$ is also finitely generated. Let $n_1, \cdots, n_{k_1} \in N$ such that their image in M_2 generates the image of N in M_2, and let $n_{k_1+1}, \cdots, n_k \in N$ be a generator of $M_1 \cap N$. We can easily check that N can be generated by $\{n_1, \cdots, n_k\}$. □

Be back to number fields.

Theorem 1.4.4. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain, i.e. integrally closed, noetherian, and any non-zero prime ideal of $\mathcal{O}_K$ is maximal.*

Proof. We have seen that $\mathcal{O}_K$ is integrally closed.

Let I be a non-zero ideal of $\mathcal{O}_K$, then there exists $0 \neq n \in \mathbb{Z}$ such that $n \in I$ (e.g. let $\alpha \in I$, then we can take $n := N_{K/\mathbb{Q}}(\alpha)$). We have then a surjection $\mathcal{O}_K/n \twoheadrightarrow \mathcal{O}_K/I$. Since $\mathcal{O}_K$ is a finite free $\mathbb{Z}$-module, $\mathcal{O}_K/n$ is a finite set hence so is $\mathcal{O}_K/I$.

Now we show $\mathcal{O}_K$ is noetherian. Suppose we have an ascending chain of ideals $\{I_i\}$ (we can assume I_i is non-zero for i sufficiently large, and then assume $I_1 \neq 0$), we obtain then $\mathcal{O}_K/I_1 \twoheadrightarrow \mathcal{O}_K/I_2 \cdots$ Since $|\mathcal{O}_K/I_1|$ is finite, we see $\{\mathcal{O}_K/I_i\}$ is stationary. Hence $\{I_i\}$ is also stationary.

Let $\mathfrak{p} \subset \mathcal{O}_K$ be a non-zero prime ideal, then $\mathcal{O}_K/\mathfrak{p}$ is a domain of finite cardinality. This implies $\mathcal{O}_K/\mathfrak{p}$ is a field, and hence $\mathfrak{p}$ is maximal. □

Remark 1.4.5. *Let I be a non-zero ideal of $\mathcal{O}_K$. Since $\mathcal{O}_K/I$ is fintie, we see I is also a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.*

Theorem 1.4.6 (Unique prime factorization)**.** *Let K be a number field, let $\mathfrak{a}$ be a non-zero proper ideal $\mathfrak{a} \subset \mathcal{O}_K$. Then $\mathfrak{a}$ admits a factorization*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into non-zero prime ideals $\mathfrak{p}_i$ of $\mathcal{O}_K$ which is unique up to the order of the factors.

We begin with several lemmas.

Lemma 1.4.7. *For $0 \neq \mathfrak{a} \subset \mathcal{O}_K$, the following holds:*

$$\exists \mathfrak{p}_1, \cdots, \mathfrak{p}_r \text{ prime ideals of } \mathcal{O}_K \text{ such that } \mathfrak{a} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r. \tag{1.1}$$

Proof. Let S be the set: $\{I$ non-zero proper ideal of $\mathcal{O}_K$, I does not satisfy (1.1)$\}$. Suppose the set is non-empty. Since $\mathcal{O}_K$ is noetherian, there exists a maximal element $\mathfrak{a}$ in the set. It is clear that $\mathfrak{a}$ is not a prime ideal. So there exist a, b such that $ab \in \mathfrak{a}$, $a \notin \mathfrak{a}$, $b \notin \mathfrak{a}$. We deduce $\mathfrak{a} \subsetneq \mathfrak{a} + (a)$, and $\mathfrak{a} \subsetneq \mathfrak{a} + (b)$. Since $\mathfrak{a}$ is maximal in the set S, $\mathfrak{a} + (a)$, $\mathfrak{a} + (b)$ do not belong in S. So there exist prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ (resp. $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$) such that $\mathfrak{a} + (a) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ (resp. $\mathfrak{a} + (b) \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$). Hence

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset (\mathfrak{a} + (a))(\mathfrak{a} + (b)) \subset \mathfrak{a}$$

contradicting $\mathfrak{a} \in S$. □

Let $\mathfrak{p}$ be a prime ideal, we define

$$\mathfrak{p}^{-1} := \{x \in K \mid x\mathfrak{p} \subset \mathcal{O}_K\}.$$

It is clear that $\mathfrak{p}^{-1}$ is an $\mathcal{O}_K$-module, and contains $\mathcal{O}_K$.

Lemma 1.4.8. *Let $\mathfrak{a}$ be a non-zero ideal, then $\mathfrak{a}\mathfrak{p}^{-1} := \{\sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a}$.*

Proof. We first show $\mathfrak{p}^{-1} \neq \mathcal{O}_K$. Let $0 \neq a \in \mathfrak{p}$, by the previous lemma, there exist $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ such that

$$\mathfrak{p} \supset (a) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

We choose r as small as possible. Since $\mathfrak{p}$ is prime, there exists i such taht $\mathfrak{p} \supset \mathfrak{p}_i$ and hence $\mathfrak{p} = \mathfrak{p}_i$ (using non-zero prime ideal is maximal). Without loss of generality, assume $\mathfrak{p} = \mathfrak{p}_1$.

Since r is minimal, $\mathfrak{a} \not\supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r$. Hence there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin (a)$ and hence $a^{-1}b \notin \mathcal{O}_K$. However $b\mathfrak{p} \subseteq (a)$, that implies that $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}_K$ and hence $a^{-1}b \in \mathfrak{p}^{-1}$.

Now for general $\mathfrak{a}$. Assume $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Then for all $x \in \mathfrak{p}^{-1}$, $x\mathfrak{a} \subseteq \mathfrak{a}$. This implies that x is integral over $\mathcal{O}_K$ (Exercise, hint: using similar arguments in the proof of Proposition 1.2.4). Since $\mathcal{O}_K$ is integrally closed, we see $x \in \mathcal{O}_K$ hence $\mathfrak{p}^{-1} \subset \mathcal{O}_K$, a contradiction. □

Exercise 1.4.9. $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Proof of Theorem 1.4.6. We first show the existence of the factorization. Let S be the set: $\{I$ non-zero proper ideal of $\mathcal{O}_K$, I does not admit prime factorization$\}$. Let $\mathfrak{a}$ be a maximal element in S, then $\mathfrak{a}$ is not prime. So there exists $\mathfrak{p} \supsetneq \mathfrak{a}$. So we have $\mathfrak{a} \subsetneq \mathfrak{p}^{-1}\mathfrak{a} \subsetneq \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$. Since $\mathfrak{a}$ is maximal, $\mathfrak{p}^{-1}\mathfrak{a}$ is not in S. So there exists $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ such that $\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. So $\mathfrak{a} = \mathfrak{p}\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r$, a contradiction.

Now we show the uniqueness of the factorisation. Suppose $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Since $\mathfrak{p}_1 \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$, there exists $\mathfrak{q}_i$ such that $\mathfrak{p}_1 \supset \mathfrak{q}_i$ hence $\mathfrak{p}_1 = \mathfrak{q}_i$. Reordering $\mathfrak{q}_k$, we assume $\mathfrak{p}_1 = \mathfrak{q}_1$. Hence

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{p}_1^{-1}(\mathfrak{p}_1 \cdots \mathfrak{p}_r) = \mathfrak{q}_1^{-1}(\mathfrak{q}_1 \cdots \mathfrak{q}_s) = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Continuing with the arguments, we deduce $s = r$ and $\mathfrak{p}_i = \mathfrak{q}_i$ (reordering if needed) for all i. □

Exercise 1.4.10. *Prove that any ideal in a Dedekind domain can be generated by two elements.*

Now we define fractional ideals.

Definition 1.4.11. *We call a finitely generated $\mathcal{O}_K$-submodule of K a fractional ideal.*

Lemma 1.4.12. *Let $\mathfrak{a}$ be a fractional ideal, then there exists $c \in K^\times$, $\mathfrak{a}_0 \subset \mathcal{O}_K$ such that $\mathfrak{a} = c\mathfrak{a}_0$.*

Proof. Suppose $\mathfrak{a}$ is generated by $e_1, \cdots, e_n$. Let $c \in K^\times$ such that $\frac{1}{c}e_i \in \mathcal{O}_K$. Thus $\mathfrak{a}_0 := \frac{1}{c}\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{a} = c(\frac{1}{c}\mathfrak{a})$. □

For fractional ideals $\mathfrak{a}$, $\mathfrak{b}$, we define

$$\mathfrak{a}\mathfrak{b} := \{\sum a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}, \tag{1.2}$$

and we define $\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}_K\}$.

Lemma 1.4.13. *Let $\mathfrak{a}$ be a fractional ideal, then $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.*

Proof. For $c \in K^\times$, it is easy to check $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$. Together with the previous lemma, it suffices to prove the lemma for ideal $\mathfrak{a} \subset \mathcal{O}_K$. Using the unique prime factorization, we write $\mathfrak{a}$ as $\mathfrak{p}_1 \cdots \mathfrak{p}_r$. We claim $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$. It is easy to see the lemma follows from the claim.

We prove the claim. By definition, we have $\mathfrak{p}_1^{-1}\cdots\mathfrak{p}_r^{-1} \subset \mathfrak{a}^{-1}$. On the other hand, since $\mathfrak{a}^{-1}\mathfrak{a} \subset \mathcal{O}_K$, we see $\mathfrak{a}^{-1}\mathfrak{a}(\mathfrak{p}_1^{-1}\cdots\mathfrak{p}_r^{-1}) \subset \mathfrak{p}_1^{-1}\cdots\mathfrak{p}_r^{-1}$. Using $\mathfrak{p}_i^{-1}\mathfrak{p}_i = \mathcal{O}_K$, we deduce $\mathfrak{a}^{-1} \subset \mathfrak{p}_1^{-1}\cdots\mathfrak{p}_r^{-1}$. The claim follows. □

Proposition 1.4.14. *Every fractional ideal $\mathfrak{a}$ admits a unique factorization $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}}$, where $v_\mathfrak{p} \in \mathbb{Z}$, and $v_\mathfrak{p} = 0$ for all but finitely many prime ideals $\mathfrak{p}$.*

Proof. Suppose $\mathfrak{a} = \frac{1}{c}\mathfrak{a}_0$, with $\mathfrak{a}_0 \subseteq \mathcal{O}_K$ and $c \in \mathcal{O}_K$. We have $(c) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(c)}$ and $\mathfrak{a}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}_0)}$. Hence

$$\prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(c)}\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}_0)}.$$

So $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}_0)-v_\mathfrak{p}(c)}$. The uniqueness follows easily from the uniqueness of the prime factorization for integral ideals. □

Let $J_K := \{\mathfrak{a} \mid \mathfrak{a} \text{ fractional ideal in } K\}$. Then (1.2) defines a group structure on J_K. By the above proposition, J_K is a free abelian group on the set of non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. Let $P_K := \{a\mathcal{O}_K \mid a \in K^\times\} \subset J_K$, and put $C_K := J_K/P_K$ called the ideal class group of K. For example, we have $C_\mathbb{Q} = \{1\}$. We have the following natural exact sequences:

$$1 \to \mathcal{O}_K^\times \to K^\times \to P_K \to 1,$$

$$1 \to \mathcal{O}_K^\times \to K^\times \to J_K \to C_K \to 1.$$

1.5 Class number I

We define "absolute" norm of ideals. Let $\mathfrak{a} \subset \mathcal{O}_K$, we put $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$.

Lemma 1.5.1. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$, $e_1, \cdots, e_d$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}$, $f_1, \cdots, f_d$ be a basis of $\mathfrak{a}$ over $\mathbb{Z}$, and let $A \in M_n(\mathbb{Z})$ such that $(f_1, \cdots, f_d) = (e_1, \cdots, e_d)A$. Then $N(\mathfrak{a}) = |\det(A)|$. In particular, if $\mathfrak{a} = (\alpha)$, then $N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(\alpha)|$.*

Proof. By the structure theorem of abelian groups, there exist a basis $e_1', \cdots, e_d'$ of $\mathcal{O}_K$ over $\mathbb{Z}$ and $a_1, \cdots, a_d \in \mathbb{Z}_{\geq 1}$ such that $\{a_i e_i\}$ is a basis of $\mathfrak{a}$ over $\mathbb{Z}$. We have $N(\mathfrak{a}) = a_1 \cdots a_d$ by definition. Since both $\{f_i\}$ and $\{a_i e_i\}$ (resp. $\{e_i\}$ and $\{e_i'\}$) are bases of $\mathfrak{a}$ (resp. $\mathcal{O}_K$) over $\mathbb{Z}$, there exists $B \in \mathrm{GL}_d(\mathbb{Z})$ (resp. $C \in \mathrm{GL}_d(\mathbb{Z})$) such that

$$(f_1, \cdots, f_d) = (a_1 e_1', \cdots, a_d e_d')B \ \big(\text{resp. } (e_1, \cdots, e_d) = (e_1', \cdots, e_d')C\big).$$

We deduce hence $|\det(A)| = a_1 \cdots a_d$. The lemma follows. □

Lemma 1.5.2. *Suppose $\mathfrak{a} = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$, then $N(\mathfrak{a}) = \prod_{i=1}^r N(\mathfrak{p}_i)^{e_i}$.*

Proof. By Chinese reminder theorem, we have $\mathcal{O}_K/\mathfrak{a} \cong \prod_{i=1}^r \mathcal{O}_K/\mathfrak{p}_i^{e_i}$. We reduce to show that for a prime ideal $\mathfrak{p}$, $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$. Consider the exact sequence (of $\mathcal{O}_K$-modules)

$$0 \to \mathfrak{p}^{e-1}/\mathfrak{p}^e \to \mathcal{O}_K/\mathfrak{p}^e \to \mathcal{O}_K/\mathfrak{p}^{e-1} \to 0.$$

By an easy induction argument, we reduce to show $|\mathfrak{p}^{e-1}/\mathfrak{p}^e| = |\mathcal{O}_K/\mathfrak{p}|$. Let $x \in \mathfrak{p}^{e-1} \setminus \mathfrak{p}^e$, and consider the morphism

$$\mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^{e-1}/\mathfrak{p}^e, \ a \mapsto ax. \tag{1.3}$$

The morphism is non-zero hence injective. On the other hand, since we have $p^e \subsetneq p^e + (x) \subseteq p^{e-1}$. By prime factorization, we see $p^e + (x) = p^{e-1}$, and so (1.3) is surjective. This concludes the proof. □

Corollary 1.5.3. *Let $\mathfrak{a}$, $\mathfrak{b} \subset \mathcal{O}_K$, then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

Let $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal, then $\mathfrak{p} \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$ (recall any non-zero ideal of $\mathcal{O}_K$ contains certain non-zero integers), say $\mathfrak{p} \cap \mathbb{Z} = (p)$. We have then an injection $\mathbb{Z}/p \hookrightarrow \mathcal{O}_K/\mathfrak{p}$. Thus $\mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic p. So there exsits $f \geq 1$ such that $N(\mathfrak{p}) = p^f$.

Lemma 1.5.4. *For a prime number p, there are finitely many prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ such that $p \in \mathfrak{p}$.*

Proof. Applying prime factorization to the ideal $p\mathcal{O}_K$: $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Then $p \in \mathfrak{p} \Leftrightarrow \mathfrak{p} = \mathfrak{p}_i$ for some i (Or use the fact that $\mathcal{O}_K/p$ has finite cardinality hence has finitely many prime ideals). □

Corollary 1.5.5. *Let $M \in \mathbb{Z}_{\geq 1}$, there exist only finitely many ideals $\mathfrak{a}$ such that $N(\mathfrak{a}) \leq M$.*

Proof. By Lemma 1.5.2, Lemma 1.5.4 and the discussion above it, the corollary follows from the fact that the set $\{p_1^{n_1} \cdots p_r^{n_r} \mid p_i \text{ are prime numbers and } n_i > 0\}$ is finite. □

Theorem 1.5.6. *The class group C_K is finite.*

To prove the theorem, we will show the following statement:

- there exists $M > 0$ such that for any ideal $\mathfrak{a} \subset \mathcal{O}_K$, there exists $\alpha \in \mathfrak{a}$ with $N(\alpha) \leq MN(\mathfrak{a})$.

Actually, if this holds, then we have $N(\mathfrak{a}^{-1}\alpha\mathcal{O}_K) \leq M$ (noting $\mathfrak{a}^{-1}\alpha\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$). However, by the previous lemma, we let $\mathfrak{a}_1, \cdots, \mathfrak{a}_k$ be *all* the ideals of $\mathcal{O}_K$ such that $N(\mathfrak{a}_i) \leq M$. Hence $\mathfrak{a}^{-1}\alpha\mathcal{O}_K = \mathfrak{a}_i$ for some i, and so $\mathfrak{a} \sim \mathfrak{a}_i^{-1} \in C_K$. This implies C_K is finite.

1.6 Lattices

Definition 1.6.1. *Let V be an n-dimensional $\mathbb{R}$-vector space.*

(1) A lattice Λ in V is a subgroup of the form $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ where $v_1, \cdots, v_m$ are linearly independent in V. We call $\Phi := \{\sum_{i=1}^m x_i v_i \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$ the fundamental mesh of Λ.

(2) A lattice Λ is called complete if $m = n$, i.e. $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong V$.

Proposition 1.6.2. *A subgroup Λ of V (equipped with the standard topology of $\mathbb{R}^n$) is a lattice if and only if Λ is discrete, i.e. for all $\gamma \in \Lambda$, there exists an open neighborhood U of γ such that $U \cap \Lambda = \{\gamma\}$.*

Proof. "Only if": Suppose $\Lambda = \mathbb{Z}v_1 + \cdots \mathbb{Z}v_m$ and $v_1, \cdots, v_m$ can extend to a basis $v_1, \cdots, v_n$ of V. For $\gamma = \sum_{i=1}^m a_i v_i$. Let $U := \{x = \sum_{i=1}^n x_i v_i \mid |a_i - x_i| < 1 \text{ for all } i = 1, \cdots, m; |a_i| < 1 \text{ for } i = m+1, \cdots, n\}$. It is clear that $U \cap \Lambda = \{\gamma\}$.

"If": Suppose Λ is discrete, we first show that Λ is closed in V. For any open neighborhood U of 0 in V, there exists an open neighborhood $U' \subset U$ of 0 such that for all $x, y \in U'$, we have $x - y \in U$ (using the fact that $V \times V \to V$, $(a, b) \mapsto a - b$ is continuous). If Λ is not closed, there exists $x \notin \Lambda$ such that for all open neighborhood U of 0, $(x + U') \cap \Lambda$ has infinitely many elements (where U' is associated to U as above). Let $\gamma_1 \neq \gamma_2 \in (x + U') \cap \Lambda$ that are of the form $\gamma_i = x + u_i$ for $u_i \in U'$. We see $\gamma_1 - \gamma_2 = u_1 - u_2 \in U$. In summary, for any open neighborhood U of 0, there exists $0 \neq \gamma \in U \cap \Gamma$, contradicting the fact Λ is discrete.

Let V_0 be the subspace of V spanned by Λ, and let $m := \dim_{\mathbb{R}} V_0$. Thus there exist $u_1, \cdots, u_m \in \Lambda$ such that $\{u_i\}$ is a basis of V_0. We have thus $\Lambda_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subset \Lambda$.

Claim: $|\Lambda/\Lambda_0| < \infty$

We prove the claim: Let Φ_0 be the fundamental mesh of Λ_0, we have thus $V_0 = \sqcup_{\beta \in \Lambda_0}(\beta + \Phi_0)$. In particular, any element $\gamma \in \Lambda$ has the form $\gamma = \alpha + \beta$ where $\beta \in \Lambda_0$ and $\alpha \in \Phi_0$ (hence $\alpha \in \Phi_0 \cap \Lambda$). It suffices to show that $\Phi_0 \cap \Lambda$ is finite. However, we know $\Lambda \cap \overline{\Phi_0}$ is closed, bounded (hence compact) and discrete (where $\overline{\Phi}_0$ denotes the closure of Φ_0), hence is a finite set. The claim follows.

By the structure theorem of abelian groups, there exists $v_1, \cdots, v_m$ such that $\Lambda = \mathbb{Z}v_1 + \cdots \mathbb{Z}v_m$. Since $\{u_i\}$ are linearly independent in V_0, we easily see $\{v_i\}$ are linearly independent in V_0 (hence in V). So Λ is a lattice. □

Lemma 1.6.3. *A lattice $\Lambda \subset V$ is complete if and only if there exists a bounded subset $M \subset V$ such that $V = \cup_{\gamma \in \Gamma}(\gamma + M)$.*

Proof. "Only if": One can take M to be the fundamental mesh of Λ.

"If" Let $V_0 \subset V$ be the subspace spanned by Λ. Since $V = \cup_{\gamma \in \Gamma}(\gamma + M)$, we have $V = \cup_{w \in V_0}(w + M)$. For all $v \in V$, and $n \in \mathbb{Z}_{\geq 1}$, we havethus $nv = w_n + \alpha_n$ for some $w_n \in V_0$ and $\alpha_n \in M$. Hence (noting V_0 is closed in V)

$$v = \lim_{n \to \infty} \frac{1}{n} nv = \lim_{n \to \infty} (\frac{v_n}{n} + \frac{\alpha_n}{n}) = \lim_{n \to \infty} \frac{v_n}{n} \in V_0.$$

The lemma follows. □

We fix a basis $e_1, \cdots, e_n$ of V over $\mathbb{R}$, hence an isomoprhism $V \xrightarrow{\sim} \mathbb{R}^n$. We equip $\mathbb{R}^n$ (hence V via the isomorphism) with the standard measure: $\mathrm{Vol}(\{(x_i) \mid 0 \leq x_i \leq 1\}) = 1$.

Lemma 1.6.4. *Let $v_1, \cdots, v_n$ be another basis of V, and let $A \in \mathrm{GL}_n(\mathbb{R})$ such that*

$$(v_1, \cdots, v_n) = (e_1, \cdots, e_n)A.$$

Let Φ be the fundamental mesh of $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$, then $\mathrm{Vol}(\Phi) = |\det(A)|$.

Proof. Writting A as a product of elementary matrices, we reduce to prove the lemma in the case where A is an elementary matrice. However, this case is clear. □

We define $\mathrm{Vol}(\Lambda) := \mathrm{Vol}(\Phi)$ (that is independent of the choice of Φ).

Theorem 1.6.5 (Minkowski's lattice point theorem)**.** *Let Λ be a complete lattice in V, X is a centrally symmetric (i.e. $x \in X \Leftrightarrow -x \in X$), convex subset of V (i.e. if $x, y \in X$, then $tx + (1-t)y \in X$ for all $0 \leq t \leq 1$). If $\mathrm{Vol}(X) > 2^n \mathrm{Vol}(\Lambda)$, then $X \cap \Lambda$ contains a non-zero element.*

Proof. It suffices to show there exist $\gamma_1 \neq \gamma_2 \in \Gamma$ such that $(\gamma_1 + \frac{1}{2}X) \cap (\gamma_2 + \frac{1}{2}X) \neq \emptyset$. Indeed, if so, there exist $x_1, x_2 \in X$ such that $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$ hence $0 \neq \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1 \in X \cap \Gamma$.

Suppose $\{\frac{1}{2}X + \gamma\}_{\gamma \in \Lambda}$ are pairwisely disjoint. Thus $\mathrm{Vol}(\Phi) \geq \sum_{\gamma \in \Lambda} \mathrm{Vol}(\Phi \cap (\gamma + \frac{1}{2}X)) = \sum_{\gamma \in \Lambda} \mathrm{Vol}((\gamma + \Phi) \cap \frac{1}{2}X)$ (noting $\mathrm{Vol}(\Phi \cap (\gamma + \frac{1}{2}X)) = \mathrm{Vol}((-\gamma + \Phi) \cap \frac{1}{2}X)$. Since $\{\gamma + \Phi\}_{\gamma \in \Lambda}$ is a covering of V, we have $\frac{1}{2^n}\mathrm{Vol}(X) = \mathrm{Vol}(\frac{1}{2}X) = \sum_{\gamma \in \Lambda} \mathrm{Vol}((\gamma + \Phi) \cap \frac{1}{2}X) \leq \mathrm{Vol}(\Lambda)$, a contradiction. □

1.7 Geometry of numbers and class number II

Let $K/\mathbb{Q}$ be a number field, $d := [K : \mathbb{Q}]$. Let $K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}^d$, $\Sigma_\infty := \{\tau : K \hookrightarrow \mathbb{C}\}$. There exist $\sigma_1, \cdots, \sigma_r : K \hookrightarrow \mathbb{R}$, and $\tau_1, \cdots, \tau_s : K \hookrightarrow \mathbb{C}$ (that do not factor through $\mathbb{R}$) such that

$$\Sigma_\infty = \{\sigma_1, \cdots, \sigma_r, \tau_1, \cdots, \tau_s, \overline{\tau}_1, \cdots, \overline{\tau}_s\}.$$

In particular, we have $d = r + 2s$. Let $\iota : K \hookrightarrow K_{\mathbb{C}}$, $x \mapsto (\sigma_1(x), \cdots, \sigma_r(x), \tau_1(x), \cdots, \overline{\tau}_s(x))$. Let

$$K_{\mathbb{R}} := \{(x_1, \cdots, x_r, y_1, \cdots, y_s, z_1, \cdots, z_s) \in K_{\mathbb{C}} \mid x_i \in \mathbb{R}, y_i = \overline{z_i}\}.$$

It is clear that the morphism ι factors through $\iota : K \hookrightarrow K_{\mathbb{R}}$ and $\dim_{\mathbb{R}} K_{\mathbb{R}} = r + 2s$.

The $\mathbb{C}$-vector space $K_{\mathbb{C}} \cong \mathbb{C}^d$ is an Hermitian inner product space with the standard Hermitian inner product: $\langle (x_i), (y_i) \rangle = \sum x_i \overline{y_i}$. This induces an inner product $\langle , \rangle_{K_{\mathbb{C}}}$ on $K_{\mathbb{R}}$, which further induces a Haar measure, that we denote by Vol_1, on $K_{\mathbb{R}}$ satisfying that if $e_1, \cdots, e_d$ is an orthogonal normal basis of $K_{\mathbb{R}}$ under $\langle , \rangle_{K_{\mathbb{C}}}$, then

$$\mathrm{Vol}_1(\{\sum a_i e_i \mid 0 \leq a_i \leq 1\}) = 1.$$

Exercise 1.7.1. *We have* $\mathrm{Vol}_1(\{(x_1, \cdots, x_{r+2s}) \in K_{\mathbb{R}} \mid 0 \leq \mathrm{Re}\, x_i \leq 1, 0 \leq \mathrm{Im}\, x_i \leq 1\}) = 2^s$.

Consider the following bijection

$$\begin{aligned} j : \mathbb{R}^{r+2s} &\xrightarrow{\sim} K_{\mathbb{R}}, \\ (x_1, \cdots, x_{r+2s}) &\mapsto (x_1, \cdots, x_r, x_{r+1} + x_{r+s+1}i, \cdots, x_{r+s} + x_{r+2s}i, \\ &\quad x_{r+1} - x_{r+s+1}i, \cdots, x_{r+s} - x_{r+2s}i). \end{aligned}$$

We define an inner product $\langle x, y\rangle_1 := \langle j(x), j(y)\rangle_{K_{\mathbb{C}}} = \sum_{i=1}^{r} x_i y_i + \sum_{i=r+1}^{r+2s} 2x_i y_i$. Denote by Vol_0 the standard Haar measure on $\mathbb{R}$ associated to the standard inner product $\langle x, y\rangle_0 = \sum x_i y_i$. For any Measurable set $X \subseteq \mathbb{R}^{r+2s}$, we have then $\mathrm{Vol}_1(j(X)) = 2^s \mathrm{Vol}_0(X)$.

Proposition 1.7.2. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal, then $\mathfrak{a}$ is a complete lattice in $K_{\mathbb{R}}$ and $\mathrm{Vol}_1(\mathfrak{a}) = \sqrt{|\Delta_K|}N(\mathfrak{a})$.*

Proof. We show $\mathfrak{a}$ is a complete lattice. Let $v_1, \cdots, v_{r+2s}$ be a basis of $\mathfrak{a}$ over $\mathbb{Z}$ (recall $\mathfrak{a}$ is free of rank $r + 2s$ over $\mathbb{Z}$). It suffices to show that $\{\iota(v_i)\}$ are linearly independent over $\mathbb{R}$. Let $A_{\mathfrak{a}} := (\sigma_i(v_j))_{1\leq i,j\leq r+2s}$. It suffices to show $\det A_{\mathfrak{a}} \neq 0$. Let $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. There exists then $M \in \mathrm{GL}_{r+2s}(\mathbb{Q})$ such that

$$(v_1, \cdots, v_{r+2s})^T = M(1, \alpha, \cdots, a^{r+2s-1})^T.$$

This implies that

$$A_{\mathfrak{a}} = M(\sigma_i(\alpha^j))_{\substack{1\leq i\leq r+2s \\ 0\leq j\leq r+2s-1}}.$$

Since $\det((\sigma_i(\alpha^j))_{\substack{1\leq i\leq r+2s \\ 0\leq j\leq r+2s-1}}) \neq 0$, we see $\det A_{\mathfrak{a}} \neq 0$.

We calculate $\mathrm{Vol}_1(\mathfrak{a})$. Let

$$B := \left(j^{-1}(\sigma_1(v_i), \cdots, \sigma_{r+2s}(v_i))^T\right)_{1\leq i\leq r+2s} = \begin{pmatrix} \sigma_1(v_1) & \cdots & \sigma_1(v_{r+2s}) \\ \vdots & \ddots & \vdots \\ \mathrm{Im}(\sigma_{r+2s}(v_1)) & \cdots & \mathrm{Im}(\sigma_{r+2s}(v_{r+2s})) \end{pmatrix}.$$

It is easy to see

$$A_{\mathfrak{a}} = \begin{pmatrix} I_r & 0 & 0 \\ 0 & I_s & iI_s \\ 0 & I_s & -iI_s \end{pmatrix} B,$$

hence $|\det A_{\mathfrak{a}}| = 2^s |\det B|$. We see $\mathrm{Vol}_0(j^{-1}(\mathfrak{a})) = |\det B|$, that implies $\mathrm{Vol}_1(\mathfrak{a}) = 2^s |\det B| = |\det A_{\mathfrak{a}}|$. In particular, $\mathrm{Vol}_1(\mathcal{O}_K) = \sqrt{|\Delta_K|}$.

Let $\beta_1, \cdots, \beta_d$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}$, there exists $M \in M_d(\mathbb{Z})$ such that $(\alpha_1, \cdots, \alpha_d) = (\beta_1, \cdots, \beta_d)M$. Thus by Lemma 1.5.1 and Lemma 1.6.4, $\mathrm{Vol}_1(\mathfrak{a}) = |\det M| \mathrm{Vol}_1(\mathcal{O}_K) = N(\mathfrak{a}) \mathrm{Vol}_1(\mathcal{O}_K)$. □

Theorem 1.7.3. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$, let $c_\sigma > 0$ for all $\sigma \in \Sigma_\infty$ such that $c_{\bar{\sigma}} = c_\sigma$ and*

$$\prod_{\sigma} c_\sigma > (\frac{2}{\pi})^s \sqrt{|\Delta_K|}N(\mathfrak{a}). \tag{1.4}$$

Then there exists $0 \neq \alpha \in \mathfrak{a}$ such that $|\sigma(\alpha)| < c_\sigma$ for all σ. In particular, $N(\alpha) < \prod_\sigma c_\sigma$.

Proof. Let $X := \{(z_\sigma) \in K_{\mathbb{R}} \mid |z_\sigma| < c_\sigma\}$. It is clear that X is centrally symmetric, and convex in $K_{\mathbb{R}}$. By calculation, we have $\mathrm{Vol}_1(X) = 2^{r+s}\pi^s \prod_\sigma c_\sigma$ (Exercise, e.g. by calculating $\mathrm{Vol}_0(j^{-1}(X))$. By (1.4), we have $\mathrm{Vol}_1(X) > 2^{r+2s}\,\mathrm{Vol}_1(\mathfrak{a})$. By Minkowski's lattice point theorem, there exists $0 \neq \alpha \in \mathfrak{a} \cap X$. This concludes the proof. □

Corollary 1.7.4. *For a non-zero ideal $\mathfrak{a}$, there exists $\alpha \in \mathfrak{a}$, $N(\alpha\mathcal{O}_K) \leq (\frac{2}{\pi})^s \sqrt{|\Delta_K|} N(\mathfrak{a})$.*

Proof. For any $\epsilon > 0$, the above theorem implies that there exists $0 \neq \alpha \in \mathfrak{a}$ such that $N(\alpha) < (\frac{2}{\pi})^s \sqrt{|\Delta_K|} N(\mathfrak{a}) + \epsilon$. Together with the fact that $N(\alpha)$ is an integer for $\alpha \in \mathfrak{a}$, the corollary follows. □

This corollary finishes the proof of Theorem 1.5.6.

Remark 1.7.5. *There are two key ingredients in the proof of Theorem 1.5.6:*

Non-archimedean *For $M > 0$, there are finitely many $\mathfrak{a}$ such that $N(\mathfrak{a}) \leq M$.*

Archimedean *There exists $M > 0$ such that for all $0 \neq \mathfrak{a}$, there exists $\alpha \in \mathfrak{a}$ such that $N(\alpha) \leq MN(\mathfrak{a})$.*

Exercise 1.7.6 (I.5.2, I.5.3, I.6.3, I.6.4, I.6.5 of "Algebraic number theory" of Neukirch)**.**
(1) Let $X := \{(z_\sigma) \in K_{\mathbb{R}} \mid \sum_\sigma |z_\sigma| < t\}$, show that $\mathrm{Vol}_1(X) = 2^r \pi^s \frac{t^d}{d!}$.

(2) Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$, show that there exists $0 \neq \alpha \in \mathfrak{a}$ such that $|N_{K/\mathbb{Q}}(\alpha)| \leq MN(\mathfrak{a})$ where $M := \frac{d!}{d^d}(\frac{4}{\pi})^s \sqrt{|\Delta_K|}$.

(3) Show that in every ideal class of K, there exists an integral ideal $\mathfrak{a}$ such that $N(\mathfrak{a}) \leq M$.

(4) Show that $|\Delta_K| > 1$ if $K \neq \mathbb{Q}$.

(5) Show that Δ_K tends to ∞ with the degree $[K : \mathbb{Q}]$.

1.8 Geometry of numbers and group of units

Recall we have an exact sequence

$$1 \to \mathcal{O}_K^\times \to K^\times \to J_K \to C_K \to 1.$$

In this section, we study the structure of $\mathcal{O}_K^\times$. We first give a multiplicative version of Minkowski's theory that we used to prove the finiteness of class numbers. Keep the notation as in § 1.7, and consider the following commutative diagram

$$\begin{array}{ccccccc} K^\times & \longrightarrow & K_{\mathbb{R}}^\times & \longrightarrow & K_{\mathbb{C}}^\times \cong (\mathbb{C}^\times)^d & \xrightarrow{N} & \mathbb{C}^\times \\ & & \ell \downarrow & & \ell \downarrow & & \log|\cdot| \downarrow \\ & & \mathbb{R}^{r+s} & \xrightarrow{i} & \mathbb{R}^d & \xrightarrow{\Sigma} & \mathbb{R} \end{array} \tag{1.5}$$

where ℓ denotes the map $K_{\mathbb{C}}^{\times} \cong (\mathbb{C}^{\times})^d \to (\mathbb{R})^d$, $(x_i) \mapsto (\log|x_i|)$, $N : (\mathbb{C}^{\times})^d \to \mathbb{C}^{\times}$, $(x_i) \mapsto \prod x_i$, $\sum : \mathbb{R}^d \to \mathbb{R}$, $(x_i) \mapsto \sum x_i$, and i denotes the map

$$(x_1, \cdots, x_{r+s}) \mapsto (x_1, \cdots, x_r, x_{r+1}/2, \cdots, x_{r+s}/2, x_{r+1}/2, \cdots, x_{r+s}/2).$$

Indeed, it is easy to see $\ell(K_{\mathbb{R}}^{\times}) \subset \mathrm{Im}(i)$, then we obtain the map $\ell : K_{\mathbb{R}}^{\times} \to \mathbb{R}^{r+s}$ in (1.5) $(x_1, \cdots, x_r, y_1, \cdots, y_s, z_1, \cdots, z_s) \mapsto (\log|x_1|, \cdots, \log|x_r|, \log|y_1| + \log|z_1|, \cdots, \log|y_s| + \log|z_s|)$. Note also that the composition of upper maps in (1.5) is equal to $N_{K/\mathbb{Q}}$. Denote by $S := \{x \in K_{\mathbb{R}}^{\times} \mid N(x) = \pm 1\}$, and $V := \{x \in \mathbb{R}^{r+s} \mid \sum \circ i(x) = 0\}$. It is clear that $\dim_{\mathbb{R}} V = r + s - 1$, and ℓ restricts to a map $S \to V$. For $x \in \mathcal{O}_K^{\times}$, we have $N_{K/\mathbb{Q}}(\mathcal{O}_K^{\times}) \subset \mathcal{O}_{\mathbb{Z}}^{\times} = \{\pm 1\}$. So we have the following composition (induced by (1.5)),

$$\lambda : \mathcal{O}_K^{\times} \to S \xrightarrow{\ell} V. \tag{1.6}$$

Lemma 1.8.1. *We have* $\mathrm{Ker}(\lambda) = \mu(\mathcal{O}_K) = \{$*roots of unity in* $\mathcal{O}_K\}$*, that is a finite group.*

Proof. By definition, $x \in \mathrm{Ker}(\lambda) \Leftrightarrow |\sigma(x)| = 1$ for all $\sigma \in \Sigma_{\infty}$ It is then clear that any root of unity in $\mathcal{O}_K$ is contained in $\mathrm{Ker}(\lambda)$. Consider the following bounded and closed subset of $K_{\mathbb{R}}$:

$$U = \{(x_1, \cdots, x_d) \in K_{\mathbb{R}} \mid |x_i| = 1\}.$$

We see $U \cap j(\mathcal{O}_K)$ is compact and discrete, hence is finite. This implies $\mathrm{Ker}(\lambda)$ is a finite group. Thus any element in $\mathrm{Ker}(\lambda)$ has finite order, and is a root of unity. □

We want to show that $\Lambda := \mathrm{Im}(\lambda)$ is a complete lattice in $V \cong \mathbb{R}^{r+s-1}$.

Proposition 1.8.2. *Λ is a lattice.*

Proof. It suffices to show Λ is discrete. Take $U := \{(x_1, \cdots, x_{r+s}) \in \mathbb{R}^{r+s} \mid |x_i| \le t\}$, then $\ell^{-1}(U) = \{(x_1, \cdots, x_{r+2s}) \in K_{\mathbb{R}} \mid e^{-t} \le |x_i| \le e^t, \forall i = 1, \cdots, r; e^{-t/2} \le |x_i| \le e^{t/2}, \forall i = r+1, \cdots, r+2s\}$. It is clear that $\ell^{-1}(U)$ is a bounded set in $K_{\mathbb{R}}$. Since $\mathcal{O}_K$ is a lattice in $K_{\mathbb{R}}$, we have $\ell^{-1}(U) \cap \mathcal{O}_K$ is a finite set. Hence $U \cap \Lambda$ is also a finite set. There exists thus an open $U' \subset U$ such taht $U' \cap \Lambda = \{0\}$, and so Λ is discrete. □

Lemma 1.8.3. *For $a \in \mathbb{Z}_{>0}$, there are only finitely many, up to multiplication by elements in $\mathcal{O}_K^{\times}$, $\alpha \in \mathcal{O}_K$, such that $N(\alpha) := |N_{K/\mathbb{Q}}(\alpha)| = a$.*

Proof. Recall $|N_{K/\mathbb{Q}}(\alpha)| = N(\alpha\mathcal{O}_K)$. Recall there are only finitely many integral ideal $\mathfrak{a}$ such that $N(\mathfrak{a}) = a$. Note also that if $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$, then $\alpha = \beta\epsilon$ for some $\epsilon \in \mathcal{O}_K^{\times}$. The lemma follows. □

Proposition 1.8.4. *Λ is a complete lattice in $V \cong \mathbb{R}^{r+s-1}$.*

Proof. For $\sigma \in \Sigma_{\infty}$, let $c_{\sigma} > 0$ such that $c_{\bar{\sigma}} = c_{\sigma}$ and $C = \prod_{\sigma \in \Sigma_{\infty}} c_{\sigma} > (\frac{2}{\pi})^s \sqrt{|d_K|}$. Let $X := \{(x_{\sigma}) \in K_{\mathbb{C}}^{\times} \mid |x_{\sigma}| \le c_{\sigma}\}$. Recall by Theorem 1.7.3, there exists $0 \neq \alpha \in \iota(\mathcal{O}_K) \cap X$ $(\iota : \mathcal{O}_K \hookrightarrow K_{\mathbb{C}})$, in particular, $N(\alpha) \le C$.

Observation: For any $y \in S$, let $X_y := \{(x_\sigma y_\sigma) \mid (x_\sigma) \in X\} = \{(z_\sigma) \in K_{\mathbb{C}} \mid |z_\sigma| \leq c_\sigma |y_\sigma| =: c'_\sigma\}$. Since $\prod_{\sigma \in \Sigma_\infty} |y_\sigma| = 1$, we have $\prod_\sigma c'_\sigma = \prod_\sigma c_\sigma = C$. We can again apply Theorem 1.7.3 so there exists $0 \neq \beta \in X_y \cap \iota(\mathcal{O}_K)$ (with $N(\beta) \leq C$).

By Lemma 1.8.3, there exist $\alpha_1, \cdots, \alpha_k \in \mathcal{O}_K$ such that

- $0 < N(\alpha_i) \leq C$,
- all $0 \neq \beta \in \mathcal{O}_K$, if $N(\beta) \leq C$, then there exist α_i and $\epsilon_i \in \mathcal{O}_K^\times$ satisfying $\beta = \alpha_i \epsilon_i$.

Let $T := S \cap (\cup(\iota(\alpha_i^{-1})X))$ where $\iota(\alpha_i^{-1})X = \{\iota(\alpha_i^{-1})x \mid x \in X\}$. It is clear that T is a bounded set in S.

Claim: $S = \cup_{\epsilon \in \mathcal{O}_K^\times} (\iota(\epsilon)T)$.

Assume the claim, then $V = \ell S = \cup_{\epsilon \in \mathcal{O}_K^\times} (\ell T + \lambda(\epsilon))$. It is easy to see that $\ell(T)$ is a bounded set in V. This then implies that Λ is a complete lattice in V.

Proof of the claim: For $y \in S$, there exists $0 \neq \beta \in \iota(\mathcal{O}_K) \cap X_{y^{-1}}$ such that $N(\beta) \leq C$. Hence there exist α_i and $\epsilon_i \in \mathcal{O}_K^\times$ such that $\beta = \alpha_i \epsilon_i$. Hence there exists $x \in X$, such that $xy^{-1} = \iota(\alpha_i)\iota(\epsilon_i)$ and hence $y = x\iota(\alpha_i^{-1})\iota(\epsilon_i^{-1}) \in \iota(\epsilon_i^{-1})T$. □

Theorem 1.8.5. *We have $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$. More precisely, let $\epsilon_1, \cdots, \epsilon_{r+s-1} \in \mathcal{O}_K^\times$ such that $\lambda(\epsilon_1), \cdots, \lambda(\epsilon_{r+s-1})$ form a basis of $\lambda(\mathcal{O}_K^\times)$ over $\mathbb{Z}$, then for all $\epsilon \in \mathcal{O}_K^\times$, there exist unique $\mu \in \mu(K)$, $n_i \in \mathbb{Z}$ for $i = 1, \cdots, r+s-1$, such that $\epsilon = \mu \epsilon_1^{n_1} \cdots \epsilon_{r+s-1}^{n_{r+s-1}}$.*

The units $\epsilon_1, \cdots, \epsilon_{r+s-1}$ in the theorem are called *fundamental units* (i.e. the units that form a basis in $\mathcal{O}_K^\times / \mu_K$).

Exercise 1.8.6. *Let $D > 1$ be a squarefree integer and d the discriminant of the quadratic field $K = \mathbb{Q}(\sqrt{D})$. Let x_1, y_1 be the uniquely determined integer solution of the equation $x^2 - dy^2 = -4$ or in case the equation has no integer solutions, $x^2 - dy^2 = 4$ such that $x_1, y_1 > 0$ are as small as possible. Show that $\frac{x_1 + y_1\sqrt{d}}{2}$ is a fundamental unit of K.*

1.9 Ramification theory

Let L/K be a finite extension of number fields with $\mathcal{O}_K \subset \mathcal{O}_L$ the rings of integers. Note that since both $\mathcal{O}_L$ and $\mathcal{O}_K$ are finitely generated $\mathbb{Z}$-modules, we see $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-modules. However, in general, $\mathcal{O}_L$ is not free over $\mathcal{O}_K$.

Let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$, and consider $\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$.

Exercise 1.9.1. *Prove $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$ (hint: use an argument analoguous to Proposition 1.9.2).*

There exist prime ideals $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ of $\mathcal{O}_L$, $e_1, \cdots, e_g \in \mathbb{Z}_{\geq 1}$ such that $\mathfrak{p}\mathcal{O}_L = \prod_i \mathfrak{P}_i^{e_i}$. For each $\mathfrak{P}_i$, $\mathfrak{P}_i \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ containing $\mathfrak{p}$. Hence $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$. We obtain thus an injection

$$\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}_i.$$

Both $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}_i$ are finite fields, and we put $f_i := [\mathcal{O}_L/fP_i : \mathcal{O}_K/fp]$.

Proposition 1.9.2. *We have* $\sum_{i=1}^{g} e_i f_i = d = [L : K]$.

Proof. We have $|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = \prod_{i=1}^{g} |\mathcal{O}_L/\mathfrak{P}_i|^{e_i}$, and $|\mathcal{O}_L/\mathfrak{P}_i| = |\mathcal{O}_K/fp|^{f_i}$. It suffices to show that $|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K|^d$. Since $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is natural $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$-vector space. We need to show $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = d$.

Let $e_1, \cdots, e_m$ be a basis of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ over $\mathcal{O}_K/\mathfrak{p}$, and let $\alpha_i \in \mathcal{O}_L$ such that $\alpha_i \equiv e_i \pmod{\mathfrak{p}}$. The proposition will follow from:

Claim: $\alpha_1, \cdots, \alpha_m$ is a basis of L over K (so $m = d$).

Proof of the claim: 1. We show $\alpha_1, \cdots, \alpha_m$ are linearly independent: If not, there exists $x_1, \cdots, x_m \in \mathcal{O}_K$ such that $\sum_{i=1}^{m} x_i\alpha_i = 0$. By modulo $\mathfrak{p}$, we see $\sum_{i=1}^{m} \bar{x}_i e_i = 0$ in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Since $\{e_i\}$ is a basis, we see $\bar{x}_i = 0$. So $x_i \in \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{p}\mathcal{O}_K$. We want to "divide x_i by $\mathfrak{p}$", i.e. we want to find $y \in K^\times$ such that

(1) $yx_i \in \mathcal{O}_K$ for all i,

(2) there exists i such that $yx_i \notin \mathfrak{p}$.

Let $\mathfrak{a}$ be the ideal of $\mathcal{O}_K$ generated by $x_1, \cdots, x_m$. Then (1) is equivalent to $\beta \in \mathfrak{a}^{-1}$ and (2) is equivalent to $\beta \notin \mathfrak{p}\mathfrak{a}^{-1}$. The existence of such β is thus clear. Then we have $\sum_{i=1}^{m}(yx_i)\alpha_i = 0$ hence $\sum_{i=1}^{m} \overline{yx_i} e_i = 0$ in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ with $\overline{yx_i}$ not all zero. This contradicts the fact $\{e_i\}$ are linearly independent.

2. We show L can be generated by $\alpha_1, \cdots, \alpha_m$ over K. Let $M := \mathcal{O}_K\alpha_1 + \cdots + \mathcal{O}_K\alpha_m$. Since $\{e_i\}$ is a basis of $\mathcal{O}_L/\mathfrak{p}$, we see $M/(\mathfrak{p}\mathcal{O}_L \cap M) \cong \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, or equivalently, $M + \mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$ (as $\mathcal{O}_K$-module). Consider $\mathcal{O}_L/M$, that is a finitely generated $\mathcal{O}_K$module, and we have $\mathfrak{p}(\mathcal{O}_L/M) = \mathcal{O}_L/M$. Let $\gamma_1, \cdots, \gamma_k$ be a set of generators of $\mathcal{O}_L/M$ over $\mathcal{O}_K$. There exists thus $A = (a_{i,j}) \in M_k(\mathfrak{p}\mathcal{O}_K)$ such that $(\gamma_1, \cdots, \gamma_k) = (\gamma_1, \cdots, \gamma_k)A$. Let $B := I_k - A$, and we see $(\gamma_1, \cdots, \gamma_k)B = 0$. Let $\beta := \det(B) \in 1 + \mathfrak{p}\mathcal{O}_K$, in particular, $\beta \neq 0$. We see $\beta\gamma_i = 0$ for all $\gamma_i \in \mathcal{O}_L/M$. So $\beta\mathcal{O}_L \subset M$, and hence $L = KM$. □

Suppose $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ with $e_i \in \mathbb{Z}_{\geq 1}$. The number $e(\mathfrak{P}_i/\mathfrak{p}) := e_i$ is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$. If $e(\mathfrak{P}_i/\mathfrak{p}) = 1$, $\mathfrak{P}_i$ is called *unramified* over $\mathfrak{p}$; if $\mathfrak{P}_i$ is *unramified* over $\mathfrak{p}$ for all i, then $\mathfrak{p}$ is called unramified in L. If $e(\mathfrak{P}_i/\mathfrak{p}) = 1$, and $f(\mathfrak{P}_i/\mathfrak{p}) := f_i = 1$ for all i, $\mathfrak{p}$ is called *split* in L. If $\mathfrak{p}\mathcal{O}_L$ is prime in $\mathcal{O}_L$, $\mathfrak{p}$ is called *inert* in L. The following lemma is straightforward.

Lemma 1.9.3. *Let* $M \supset L \supset K$, $\wp$ *be a prime ideal of* $\mathcal{O}_M$, $\mathfrak{P} := \wp \cap \mathcal{O}_L$, $\mathfrak{p} := \wp \cap \mathcal{O}_K = \mathfrak{P} \cap \mathcal{O}_K$. *Then* $e(\wp/\mathfrak{p}) = e(\wp/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$, $f(\wp/\mathfrak{p}) = f(\wp/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$.

Let $\theta \in \mathcal{O}_L$ such that $L = K(\theta)$. Let $p(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of θ over K (so $\deg p(x) = d = [L : K]$). Consider the $\mathcal{O}_K$-algebra $\mathcal{O}_K[\theta] = \mathcal{O}_K + \mathcal{O}_K\theta + \cdots + \mathcal{O}_K\theta^{d-1} \subset \mathcal{O}_L$.

Lemma 1.9.4. $|\mathcal{O}_L/\mathcal{O}_K[\theta]|$ *is finite.*

Proof. Let $\alpha_1, \cdots, \alpha_m$ be a set of generators of $\mathcal{O}_L$ over $\mathcal{O}_K$. Since $\alpha_i \in L = K(\theta)$, there exists $a_i \in \mathcal{O}_K \setminus \{0\}$ such that $a_i\alpha_i \in \mathcal{O}_K[\theta]$. Hence there exists $a \in \mathcal{O}_K \setminus \{0\}$ such that $a\mathcal{O}_L \subset \mathcal{O}_K[\theta]$. The lemma follows easily from the fact $\mathcal{O}_L/a\mathcal{O}_L$ is a finite set. □

By the lemma and the proof, we see the set $\{\mathfrak{a} \text{ integral ideals} \mid \mathfrak{a} \subset \mathcal{O}_K[\theta]\}$ is non-empty. Note that if $\mathfrak{a}, \mathfrak{a}' \subset \mathcal{O}_K[\theta]$, then $\mathfrak{a} + \mathfrak{a}' \subset \mathcal{O}_K[\theta]$. Hence there exists a unique maximal element $\mathscr{F}_\theta$ in the set, that we call the *conductor* of $\mathcal{O}_K[\theta]$.

Proposition 1.9.5. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and suppose $\mathfrak{p}$ is relatively prime to $\mathscr{F}_\theta$. Let $\overline{p}(x) := \overline{p}_1(x)^{e_1} \cdots \overline{p}_g(x)^{e_r}$ be the factorization of $\overline{p}(x) \in \mathcal{O}_K/\mathfrak{p}[x]$ into irreducible polynomials in $\mathcal{O}_K/fp[x]$. Let $p_i(x) \in \mathcal{O}_K[x]$ satisfy*

$$\begin{cases} p_i(x) \text{ is monic,} \\ \det p_i(x) = \deg \overline{p}_i(x), \\ p_i(x) \equiv \overline{p}_i(x) \pmod{\mathfrak{p}}. \end{cases}$$

Then $\{\mathfrak{P}_i := \mathfrak{p}\mathcal{O}_L + p_i(\theta)\mathcal{O}_L\}$ are exactly all the different primes of $\mathcal{O}_L$ above $\mathfrak{p}$ with $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$ and $f(\mathfrak{P}_i/\mathfrak{p}) = \det p_i(x)$.

Proof. Consider the natural morphism of $\mathcal{O}_K$-algebras $f : \mathcal{O}_K[\theta]/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{p}$. We show f is an isomorphism. Since $\mathfrak{p}$ is relatively prime to $\mathscr{F}_\theta$, we have

$$\mathcal{O}_K[\theta] + \mathfrak{p}\mathcal{O}_L \supset \mathscr{F}_\theta + \mathfrak{p}\mathcal{O}_L = \mathcal{O}_L \tag{1.7}$$

and so f is surjective. The injectivity of f is equivalent to $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\theta] = \mathfrak{p}\mathcal{O}_K[\theta]$. The direction "$\supset$" is clear. Let $x \in \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\theta]$. By (1.7), we see $\mathscr{F}_\theta \cap \mathcal{O}_K + \mathfrak{p} = \mathcal{O}_K$ (Exercise). There exist $a \in \mathscr{F}_\theta \cap \mathcal{O}_K$ and $b \in \mathfrak{p}$ such that $a + b = 1$. We see $x = x(a+b) = xa + xb$. We have $xa \in \mathfrak{p}\mathscr{F}_\theta \subset \mathfrak{p}\mathcal{O}_K[\theta]$, and $xb \subset \mathfrak{p}\mathcal{O}_K[\theta]$. Hence $x \in \mathfrak{p}\mathcal{O}_K[\theta]$, the direction "$\subset$" follows.

We have $\mathcal{O}_K[x]/p(x) \xrightarrow{\sim} \mathcal{O}_K[\theta]$, $x \mapsto \theta$. Let $k := \mathcal{O}_K/\mathfrak{p}$, and we deduce

$$\mathcal{O}_K[\theta]/\mathfrak{p} \cong \mathcal{O}_K[x]/(\mathfrak{p}, p(x)) \cong k[x]/\overline{p}(x) \cong \prod_{i=1}^{g} k[x]/\overline{p}_i(x)^{e_i}.$$

We see

$$\{\text{prime ideals of } \mathcal{O}_L/\mathfrak{p} \cong \mathcal{O}_K[\theta]/\mathfrak{p}\} \longleftrightarrow \{\overline{p}_i(x)\}.$$

Note also that the kernel of $\mathcal{O}_L \twoheadrightarrow \mathcal{O}_L/\mathfrak{p} \cong \mathcal{O}_K[\theta]/\mathfrak{p} \twoheadrightarrow k[x]/\overline{p}_i(x)$ is $\mathfrak{P}_i := p_i(\theta)\mathcal{O}_K[\theta] + \mathfrak{p}\mathcal{O}_L = p_i(\theta)\mathcal{O}_L + \mathfrak{p}\mathcal{O}_L$ (using $\mathcal{O}_K[\theta] + \mathfrak{p} = \mathcal{O}_L$). Since $\mathcal{O}_L/\mathfrak{P}_i \cong k[x]/\overline{p}_i(x)$, $f(\mathfrak{P}_i/\mathfrak{p}) = \deg p_i(x)$. Since $\prod_{i=1}^g \overline{p}_i(x)^{e_i} = 0 \in \mathcal{O}_K[x]/(\mathfrak{p}, p(x)) \cong \mathcal{O}_K[\theta]/\mathfrak{p} \cong \mathcal{O}_L/\mathfrak{p}$, we see $\prod_{i=1}^g \mathfrak{P}_i^{e_i} \in \mathfrak{p}$ (so $e(\mathfrak{P}_i/\mathfrak{p}) \geq e_i$). However, we have $\sum_{i=1}^g e_i f_i = d$, we conclude by Proposition 1.9.2 that $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$ for all i. This finishes the proof. □

We can define the discriminant of (the $\mathcal{O}_K$-module) $\mathcal{O}_K[\theta]$ over $\mathcal{O}_K$:

$$d(\mathcal{O}_K[\theta]) := \det((\sigma_i(\theta^j))_{0 \leq i,j \leq d})^2,$$

where $\Sigma_{L/K} = \{\sigma_0, \cdots, \sigma_{d-1}\}$. We have

$$d(\mathcal{O}_K[\theta]) = \prod_{i<j} (\sigma_i(\theta) - \sigma_j(\theta))^2 \in \mathcal{O}_K \setminus \{0\}.$$

Lemma 1.9.6. *Keep the above notation, let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}|d(\mathcal{O}_K[\theta])$ if and only if the mod $\mathfrak{p}$ reduction $\overline{p}(x) \in k[x]$ of $p(x)$ is not separable.*

Proof. Let M be the Galois closure of L over K. In $\mathcal{O}_M[x]$, we have thus $p(x) = \prod_{i=0}^{d-1}(x - \sigma_i(\theta))$. For a prime ideal $\mathfrak{P}|\mathfrak{p}$ of $\mathcal{O}_M$, we have $\overline{p}(x) = \prod_{i=0}^{d-1}(x - \overline{\sigma_i(\theta)}) \in \mathcal{O}_M/\mathfrak{P}[x]$. Soe $\overline{\mathfrak{p}}(x)$ is separable if and only if $\overline{\sigma_i(\theta)} \neq \overline{\sigma_j(\theta)}$ or equivalently $\sigma_i(\theta) - \sigma_j(\theta) \notin \mathfrak{P}$ for $i \neq j$. This is further equivalent to $\mathfrak{P} \nmid d(\mathcal{O}_K[\theta]) \Leftrightarrow \mathfrak{p} \nmid d(\mathcal{O}_K[\theta])$. □

Corollary 1.9.7. *For L/K, there are only finitely many $\mathfrak{p} \subset \mathcal{O}_K$ that are ramified in $\mathcal{O}_L$.*

Proof. Let $\theta \in \mathcal{O}_L$ be as above (with $p(x)$ the minimal polynomial of θ over K, and $\mathscr{F}_\theta$ the conduction of $\mathcal{O}_K[\theta]$). We only need to there are only finitely many $\mathfrak{p} \subset \mathcal{O}_K$ that are ramified in $\mathcal{O}_L$ and that are coprime to $\mathscr{F}$. But by Lemma 1.9.6 and Proposition 1.9.5, such $\mathfrak{p}$ has to divide $d(\mathcal{O}_K[\theta])$. The corollary follows. □

1.10 Ramification and Galois theory

Suppose L/K is a Galois extension of number fields. Let $\mathfrak{a} \subset \mathcal{O}_L$ be an ideal, and $\sigma \in \mathrm{Gal}(L/K)$. We denote by $\sigma(\mathfrak{a}) := \{\sigma(x) \mid x \in \mathfrak{a}\} \subset \sigma(\mathcal{O}_L) = \mathcal{O}_L$. One easily sees that $\sigma(\mathfrak{a})$ is also an ideal of $\mathcal{O}_L$.

Lemma 1.10.1. *Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$, then $\sigma(\mathfrak{P})$ is also a prime ideal of $\mathcal{O}_L$.*

Proof. Suppose $\mathfrak{ab} \subset \sigma(fP)$. Then $\sigma^{-1}(\mathfrak{a})\sigma^{-1}(\mathfrak{b}) \subset \mathfrak{P}$. Since $\mathfrak{P}$ is prime, we have $\sigma^{-1}(\mathfrak{a}) \subset \mathfrak{P}$ or $\sigma^{-1}(\mathfrak{b}) \subset \mathfrak{P}$. Hence $\mathfrak{a} \subset \sigma(\mathfrak{P})$ or $\mathfrak{b} \subset \sigma(\mathfrak{P})$. □

Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$, and $\mathfrak{P}|\mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$. Since $\mathfrak{P} \cap \mathcal{O}_K = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma(\mathfrak{P}) \cap \mathcal{O}_K$, we see $\sigma(\mathfrak{P})|\mathfrak{p}$.

Proposition 1.10.2. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$, then $\mathrm{Gal}(L/K)$ acts transitively on $\{\mathfrak{P}_i \subset \mathcal{O}_L \mid \mathfrak{P}_i|\mathfrak{p}\}$. Moreover, $e(\mathfrak{P}_i/\mathfrak{p}) = e(\mathfrak{P}_j/\mathfrak{p}) =: e$ and $f(\mathfrak{P}_i/\mathfrak{p}) = f(\mathfrak{P}_j/\mathfrak{p}) =: f$ for all $\mathfrak{P}_i, \mathfrak{P}_j|\mathfrak{p}$.*

Proof. Let $\mathfrak{P}|\mathfrak{p}$, and suppose there exists $\mathfrak{P}_i|\mathfrak{p}$ such that for all $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathfrak{P}) \neq \mathfrak{P}_i$. So $\mathfrak{P}_i$ and $\{\sigma(\mathfrak{P})\}$ are coprime, and there exsits hence $x \in \mathfrak{P}_i$ and $x \notin \sigma(\mathfrak{P})$ for all σ. The latter means $\sigma(x) \notin \mathfrak{P}$ for all σ. However $\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p} \subset \mathfrak{P}$, contradicting $\mathfrak{P}$ is prime. The first part of the proposition follows.

Let $\mathfrak{P}_i = \sigma(\mathfrak{P})$. We write $\mathfrak{p} = \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}\mathfrak{a}$ where $\mathfrak{a}$ is coprime to $\mathfrak{P}$. Then $\sigma(\mathfrak{p}) = \mathfrak{P}_i^{e(\mathfrak{P}/\mathfrak{p})}\sigma(\mathfrak{a})$ (with $\sigma(\mathfrak{a})$ coprime to $\mathfrak{P}_i$). Since $\mathfrak{p} = \sigma(\mathfrak{p})$, we deduce $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}_i/\mathfrak{p})$. Finally, σ induces a bijection $\mathcal{O}_L/\mathfrak{P} \xrightarrow{\sigma} \mathcal{O}_L/\mathfrak{P}_i$, and hence $f(\mathfrak{P}_i/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$. □

Put $g := |\{\mathfrak{P} \subset \mathcal{O}_L \mid \mathfrak{P}|\mathfrak{p}\}|$, we have hence $n = efg$.

For a non-zero prime ideal $\mathfrak{P} \subset \mathcal{O}_L$, put $D_\mathfrak{P} := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$. For $\sigma \in \mathrm{Gal}(L/K)$, it is easy to check $D_{\sigma(\mathfrak{P})} = \sigma D_\mathfrak{P} \sigma^{-1}$. Let $H_\mathfrak{P} := L^{D_\mathfrak{P}}$ hence $D_\mathfrak{P} =$

$\mathrm{Gal}(L/H_{\mathfrak{P}})$. Denote by $\mathfrak{P}_D := \mathfrak{P} \cap \mathcal{O}_{H_{\mathfrak{P}}}$, that is a prime ideal of $\mathcal{O}_{H_{\mathfrak{p}}}$. By Proposition 1.10.2, we easily deduce

Lemma 1.10.3. *We have* $D_{\mathfrak{P}} = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$.

Proposition 1.10.4. *(1) The ideal* $\mathfrak{P}$ *is the unique prime ideal of* $\mathcal{O}_L$ *such that* $\mathfrak{P}|\mathfrak{P}_D$. *(2) We have* $e(\mathfrak{P}/\mathfrak{P}_D) = e(\mathfrak{P}/\mathfrak{p})$ *(*$\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$*),* $f(\mathfrak{P}/\mathfrak{p}_D) = f(\mathfrak{P}/\mathfrak{p})$, $e(\mathfrak{P}_D/\mathfrak{p}) = 1$ *and* $f(\mathfrak{P}_D/\mathfrak{p}) = 1$.

Proof. (1) We know $D_{\mathfrak{P}} = \mathrm{Gal}(L/H_{\mathfrak{P}})$ acts transitively on the prime ideals of $\mathcal{O}_L$ above $\mathfrak{P}_D$. However, $\sigma(\mathfrak{P}) = \mathfrak{P}$ for all $\sigma \in \mathrm{Gal}(L/H_{\mathfrak{p}})$. (1) follows.

(2) We have by (1) $e(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}/\mathfrak{P}_D) = D_{\mathfrak{P}} = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$. Together with Lemma 1.9.3, (2) follows. □

For $\sigma \in D_{\mathfrak{P}}$, σ induces $\overline{\sigma} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}$. We put $k_{\mathfrak{P}} := \mathcal{O}_L/\mathfrak{P}$, and $\mathcal{O}_K/\mathfrak{p}$. We have hence a morphism

$$D_{\mathfrak{P}} \to \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}),\ \sigma \mapsto \overline{\sigma}. \tag{1.8}$$

Denote by $I_{\mathfrak{P}}$ the kernel of the above map, i.e.

$$I_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \equiv x \mod \mathfrak{P},\ \forall x \in \mathcal{O}_L\}.$$

Proposition 1.10.5. *The morphism* $D_{\mathfrak{P}}/I_{\mathfrak{P}} \to \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ *is an isomorphism.*

Proof. First by replacing K by $H_{\mathfrak{P}}$, we can reduce to the case where $D_{\mathfrak{P}} = \mathrm{Gal}(L/K)$.

The injectivity is by definition. Let $\alpha \in \mathcal{O}_L$ such that the reduction $\overline{\alpha} \in k_{\mathfrak{P}}$ satisfies $k_{\mathfrak{P}} = k_{\mathfrak{p}}(\overline{\alpha})$. Let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α over K, and $\overline{p}(x)$ be the minimal polynomial of $\overline{\alpha}$ over $k_{\mathfrak{p}}$. Since L is Galois over K, we have $f(x) = \prod_{\sigma \in \Sigma(K(\alpha)/K)}(x - \sigma(\alpha))$. By modulo $\mathfrak{P}$, we get $\overline{f}(x) = \prod_{\sigma \in \Sigma(K(\alpha)/K)}(x - \overline{\sigma(\alpha)}) \in k_{\mathfrak{p}}[x]$. Since $\overline{f}(\overline{\alpha}) = 0$, we see $\overline{p}(x)|\overline{f}(x)$. Thus for all $\tau \in \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ (that is determined by $\tau(\overline{\alpha})$), there exists $\sigma \in \Sigma(K(\alpha)/K)$ such that $\overline{\sigma(\alpha)} = \tau(\overline{\alpha})$. Recall $\mathrm{Gal}(L/K) \twoheadrightarrow \Sigma(K(\alpha)/K)$. Let $\tilde{\sigma} \in \mathrm{Gal}(L/K)$ such that $\tilde{\sigma}(\alpha) = \sigma(\alpha)$. Then (1.8) sends $\tilde{\sigma}$ to $\overline{\sigma}$. This concludes the proof. □

Let $U_{\mathfrak{P}} := L^{I_{\mathfrak{P}}}$, $\mathfrak{P}_I := \mathfrak{P} \cap \mathcal{O}_{U_{\mathfrak{P}}}$.

Proposition 1.10.6. *We have* $e(\mathfrak{P}/\mathfrak{P}_I) = e(\mathfrak{P}/\mathfrak{P}_D) = e(\mathfrak{P}/\mathfrak{p})$, $e(\mathfrak{P}_I/\mathfrak{P}_D) = 1$, $f(\mathfrak{P}/fp_I) = 1$ *and* $f(\mathfrak{P}_I/\mathfrak{P}_D) = f(\mathfrak{P}/\mathfrak{P}_D) = f(\mathfrak{P}/\mathfrak{p})$.

Proof. Since $\{\sigma \in \mathrm{Gal}(L/U_{\mathfrak{P}}) \mid \sigma(x) \equiv x \pmod{\mathfrak{P}}\} = \mathrm{Gal}(L/U_{\mathfrak{P}})$, applying Proposition 1.10.5 to the case $K = U_{\mathfrak{P}}$, we see $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{P}_I}) = 1$. Hence $f(\mathfrak{P}/\mathfrak{P}_I) = 1$. The others then follows from Lemma 1.9.3. □

In summary, for a finite Galois extension L/K, and $\mathfrak{P}|\mathfrak{p}$. We obtain $K \subset H_{\mathfrak{P}} \subset U_{\mathfrak{P}} \subset L$ such that $\mathrm{Gal}(L/U_{\mathfrak{P}}) \cong I_{\mathfrak{P}}$, $\mathrm{Gal}(L/H_{\mathfrak{P}}) \cong D_{\mathfrak{P}}$, $[L : U_{\mathfrak{P}}] = e(\mathfrak{P}/\mathfrak{p})$, $[U_{\mathfrak{P}} : H_{\mathfrak{P}}] = f(\mathfrak{P}/\mathfrak{p})$, $[H_{\mathfrak{P}} : K] = g$.

Chebotarev's density theorem (statement)

Let L/K be a finite Galois extension. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$, $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$, $\mathfrak{P}|\mathfrak{p}$. We have then $D_{\mathfrak{P}} \cong \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$. Let $q := |k_{\mathfrak{p}}|$. Then $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is generated by $\mathrm{Frob}_q : x \mapsto x^q$. We have thus

Lemma 1.10.7. *Keep the notation.*

(1) There exists a unique element $\left(\frac{L/K}{\mathfrak{P}}\right) \in \mathrm{Gal}(L/K)$ *such that* $\left(\frac{L/K}{\mathfrak{P}}\right)(x) \equiv x^q \pmod{\mathfrak{P}}$.

(2) Let $\sigma \in \mathrm{Gal}(L/K)$*, then*

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}.$$

Proof. Exercise. □

We use $\left(\frac{L/K}{\mathfrak{p}}\right)$ denote the conjugacy class of $\left(\frac{L/K}{\mathfrak{P}}\right)$ for $\mathfrak{P}|\mathfrak{p}$.

Let $\mathcal{P}_K$ be the set of prime ideals of $\mathcal{O}_K$, and let $\mathcal{S} \subset \mathcal{P}_K$. The Dirichlet density of $\mathcal{S}$ is defined to be

$$\delta(\mathcal{S}) = \varinjlim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}} N(\mathfrak{p})^{-s}}.$$

One can also define the so-called natural density

$$\delta_0(\mathcal{S}) = \varinjlim_{m \to +\infty} \frac{|\{\mathfrak{p} \in S \mid N(\mathfrak{P}) \leq m\}|}{|\{\mathfrak{p} \mid N(\mathfrak{p}) \leq m\}|}.$$

One can show that if $\delta_0(\mathcal{S})$ exists then $\delta_0(\mathcal{S}) = \delta(\mathcal{S})$.

We can now state the Chebotarev density theorem:

Theorem 1.10.8. *Let L be a Galois extension of K. For $\sigma \in \mathrm{Gal}(L/K)$, let $\langle\sigma\rangle$ be the conjugacy class of σ. Then the set*

$$\mathcal{S} = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ is unramified in } L \text{ and } \left(\frac{L/K}{\mathfrak{p}}\right) = \langle\sigma\rangle\}$$

has Dirichlet density $\delta(\mathcal{S}) = \frac{|\langle\sigma\rangle|}{|\mathrm{Gal}(L/K)|}$.

Remark 1.10.9. *In particular, for any $\sigma \in \mathrm{Gal}(L/K)$, there exists infinitely many prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ such that* $\left(\frac{L/K}{\mathfrak{P}}\right) = \sigma$.

Hilbert class field (statement)

Suppose L/K is a finite abelian extension, i.e. L/K is Galois and $\mathrm{Gal}(L/K)$ is abelian. In this case, we have $\left(\frac{L/K}{\mathfrak{p}}\right)$ has a unique element, still denoted by $\left(\frac{L/K}{\mathfrak{p}}\right)$. Suppose moreover

L/K is unramified for all prime ideals in $\mathcal{O}_K$, thus $\left(\frac{L/K}{\mathfrak{p}}\right)$ is well-defined for all $\mathfrak{p}$. For a fractional ideal $\mathfrak{a} = \prod \mathfrak{p}_i^{e_i}$, we put

$$\left(\frac{L/K}{\mathfrak{a}}\right) := \prod \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i} \in \mathrm{Gal}(L/K).$$

In this way, we get a well defined map $J_K \to \mathrm{Gal}(L/K)$.

Lemma 1.10.10. *Let L_1, L_2 be finite Galois extensions of K.*

(1) Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, suppose $\mathfrak{p}$ is unramified in L_1 and L_2, show $\mathfrak{p}$ is unramified in L_1L_2.

(2) Suppose L_1/K, L_2/K are abelian, show that L_1L_2/K is abelian.

Proof. Exercise. □

We call L/K is *unramified* if L/K is unramified for all prime ideals on $\mathcal{O}_K$, and for any $\sigma : K \hookrightarrow \mathbb{C}$, and $\sigma_L : L \hookrightarrow \mathbb{C}$ with $\sigma_L|_K = \sigma$, we have $\mathrm{Im}(\sigma) \subset \mathbb{R} \Leftrightarrow \mathrm{Im}(\sigma_L) \subset \mathbb{R}$.

Definition 1.10.11. *We call the maximal abelian unramified extension H of K the Hilbert class field of K.*

Theorem 1.10.12. *Let H be the Hilbert class field of K, then the morphism $J_K \to \mathrm{Gal}(L/K)$ factors through an isomorphism*

$$C_K \cong J_K/P_K \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Chapter 2

Local fields

2.1 p-adic numbers

We have maps $\cdots \mathbb{Z}/p^{n+1}\ ra\mathbb{Z}/p^n \to \cdots \to \mathbb{Z}/p$ (that form a projective system), and we put

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \{(x_n) \in \prod_n \mathbb{Z}/p^n\mathbb{Z} \mid \overline{x_{n+1}} = x_n \in \mathbb{Z}/p^n\mathbb{Z}\}.$$

We define the addition and multiplication on $\mathbb{Z}_p$:

$$\begin{cases} (x_n) + (y_n) := (x_n + y_n) \\ (x_n)(y_n) := (x_n y_n). \end{cases}$$

Note we have an injective ring homomorphism $\mathbb{Z} \to \mathbb{Z}_p$, $x \mapsto (\overline{x} \pmod{p^n})$.

Exercise 2.1.1. *Show that* $p^m\mathbb{Z}_p = \{(x_n) \in \mathbb{Z}_p \mid x_n \equiv 0 \pmod{p^m},\ \forall n \geq m\}$.

Proposition 2.1.2. *$\mathbb{Z}_p$ is a domain, and the unique maximal ideal of $\mathbb{Z}_p$ is $p\mathbb{Z}_p$.*

Proof. Suppose $(x_n)(y_n) = 0$, and $(x_n) \neq 0$, $(y_n) \neq 0$. There exists k such that $x_k \neq 0$, $y_k \neq 0$. So there exist $i, j < k$ such that $x_k \in p^i\mathbb{Z}/p^k \backslash p^{i+1}\mathbb{Z}_p/p^k$ and $y_k \in p^j\mathbb{Z}/p^k \backslash p^{j+1}\mathbb{Z}_p/p^k$. For any $N \geq k$, we have $x_N \notin p^{i+1}\mathbb{Z}/p^N$, $y_N \notin p^{j+1}\mathbb{Z}/p^N$. If $N \geq \max\{k, i+j+2\}$, we see $x_N y_N \neq 0$ in $\mathbb{Z}/p^N$, a contradiction.

We have $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p$, $(x_n) \mapsto x_1$. Hence $p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$. For any $x = (x_n) \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$, and for all $n \in \mathbb{Z}_{\geq 1}$, there exists a unique $y_n \in \mathbb{Z}/p^n$ such that $x_n y_n = 1$. Since $\overline{x_{n+1}} = x_n$, we deduce by the uniqueness that $\overline{y_{n+1}} = y_n$. Thus $y = (y_n) \in \mathbb{Z}_p$ and $xy = 1$. This implies that $p\mathbb{Z}_p$ is the unique maximal ideal. □

Exercise 2.1.3. *Any non-zero ideal of $\mathbb{Z}_p$ is of the form $p^m\mathbb{Z}_p$.*

The ring $\mathbb{Z}_p$ is equipped with a natural topology with an open basis given by $\{x + p^n\mathbb{Z}_p\}_{x \in \mathbb{Z}_p, n \in \mathbb{Z}_{\geq 1}}$. This topology can be defined in the following more conceptual way: consider $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n \hookrightarrow \prod_n \mathbb{Z}/p^n$. We equip each $\mathbb{Z}/p^n$ with the discrete topology, and $\prod_n \mathbb{Z}/p^n$ with the product topology, and $\mathbb{Z}_p$ with the induced topology.

Exercise 2.1.4. *Check that the above two topologies on $\mathbb{Z}_p$ coincide.*

Lemma 2.1.5. *$\mathbb{Z}_p$ is a topological ring, i.e. the operations*

$$\begin{cases} \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p, \ (x,y) \mapsto x+y, \\ \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p, \ (x,y) \mapsto xy, \\ \mathbb{Z}_p \to \mathbb{Z}_p, \ x \mapsto -x. \end{cases}$$

are continuous.

Proof. Exercises. □

Proposition 2.1.6. *$\mathbb{Z}_p$ is complete, i.e. any Cauchy sequence has a limit in $\mathbb{Z}_p$. And $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

Proof. Let $\{a_n\}$ be a Cauchy sequence in $\mathbb{Z}_p$. Thus for any $m \in \mathbb{Z}_{\geq 1}$, there exists N such that for any $n_1, n_2 > N(m)$, $a_{n_1} - a_{n_2} \in p^m\mathbb{Z}_p$. This implies that for any $n > N(m)$, the image of a_n in $\mathbb{Z}/p^m$ is independent of n, that we denote by b_m. Let $b := (b_m)$. It is easy to see $b \in \mathbb{Z}_p$ and for all $n > N(m)$, $a_n - b \in p^m\mathbb{Z}_p$. Thus b is a limit of $\{a_n\}$. One can check that b is the unique limit of $\{a_n\}$ (exercise).

For any $x = (x_n) \in \mathbb{Z}_p$, let $\tilde{x}_n$ be a lifting of x_n in $\mathbb{Z}$. Then $x - \tilde{x}_n \in p^n\mathbb{Z}_p$. Hence $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. □

We define $\mathbb{Q}_p$ to be the fractional field of $\mathbb{Z}_p$. Since $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p$, we see for any element $x \in \mathbb{Q}_p$, there exists $n \in \mathbb{Z}_{\geq 0}$ such that $p^n x \in \mathbb{Z}_p$. We equip $\mathbb{Q}_p$ with the topology such that an open basis is given by $\{x + p^n\mathbb{Z}_p\}_{x \in \mathbb{Q}_p, n \in \mathbb{Z}_{\geq 1}}$.

Next we give an "alternative" construction of $\mathbb{Q}_p$ using p-adic norm on $\mathbb{Q}$: Put $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ such that $|p^r\frac{a}{b}|_p := p^{-r}$ where $a, b \in \mathbb{Z} \neq \{0\}$, and a, b are prime to p, and that $|0|_p = 0$.

Proposition 2.1.7. *We have:*

(1) $|x|_p = 0$ if and only $x = 0$.

(2) $|xy|_p = |x|_p|y|_p$.

(3) (Non-archimedean) $|x+y|_p \leq \max\{|x|_p, |y|_p\}$.

Thus $|\cdot|_p$ is a metric.

Proof. (1) and (2) are clear. For (3), we have (suppose $r \leq s$)

$$p^r\frac{a}{b} + p^s\frac{c}{d} = p^r(\frac{a}{b} + p^{s-r}\frac{c}{d}) = p^r\big(\frac{ad + p^{s-r}bc}{bd}\big),$$

hence (the equality follows from (2) and the inequality follows from $(p, bd) = 1$)

$$\big|p^r\frac{a}{b} + p^s\frac{c}{d}\big|_p = p^{-r}\big|\big(\frac{ad + p^{s-r}bc}{bd}\big)\big|_p \leq p^{-r}.$$

(3) follows. □

Remark 2.1.8. *By the proof, we see if* $|x|_p \neq |y|_p$, *then* $|x+y|_p = \max\{|x|_p, |y|_p\}$.

We can define an additive p-adic valuation (that determines $|\cdot|_p$ and vice versa): $\mathrm{val}_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$, $\mathrm{val}_p(0) := +\infty$, and $\mathrm{val}_p(p^r \frac{a}{b}) = r$ (for $a, b \in \mathbb{Z} \setminus \{0\}$, $(ab, p) = 1$). We have then

(1) $\mathrm{val}_p(x) = +\infty$ if and only $x = 0$,

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

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

Proposition 2.1.9. $\mathbb{Q}_p$ *is the completion of* $\mathbb{Q}$ *with respect to* $|\cdot|_p$

Proof. Let $\{a_n\}$ be a Cauchy sequence in $\mathbb{Q}$. Then the set $\{a_n\}$ is bounded. There exists thus $M \in \mathbb{Z}_{\geq 0}$ such that $|p^M a_n|_p \leq 1$ for all n.

Claim: If $a \in \mathbb{Q}$, $|a|_p \leq 1$, then for any $\epsilon > 0$, there exists $b \in \mathbb{Z}$ such that $|a - b|_p < \epsilon$.

We prove the claim. Since $|a|_p \leq 1$, $a = \frac{r}{s}$ with $(s, p) = 1$. So for an integer b, we have $a - b = \frac{r - bs}{s}$. Let $N \in \mathbb{Z}_{\geq 1}$ such that $p^{-N} < \epsilon$. Since $(s, p) = 1$, s is invertible in $\mathbb{Z}/p^N$. We let $b \in \mathbb{Z}$ be a lifting of $s^{-1}r$ in $\mathbb{Z}/p^N$. We have $|a - b|_p \leq p^{-N} < \epsilon$.

By the claim, we see the Cauchy sequence $\{p^M a_n\}$ is equivalent to a Cauchy sequence $\{b_n\}$ with $b_n \in \mathbb{Z}$. However, $\{b_n\}$ is a Cauchy sequence for $|\cdot|_p$ is equivalent to $\{b_n\}$ form a Cauchy sequence in $\mathbb{Z}_p$. We let $b := \lim_n b_n \in \mathbb{Z}_p$. In this way, we get a map from the completion of $\mathbb{Q}$ (with respect to $|\cdot|_p$) to $\mathbb{Q}_p$, $\{a_n\} \mapsto p^{-M} b$. It is straightforward to check this map is a homemorphism. □

We can now define $|x|_p$ for $x \in \mathbb{Q}_p$: let $\{x_n\}$ be a Cauchy sequence with $x_n \in \mathbb{Q}$ that converges to x, then $|x|_p := \lim_n |x_n|_p = |x_N|_p$ for N sufficiently large. One easily check the statements in Proposition 2.1.7 hold for $|\cdot|_p$ on $\mathbb{Q}_p$.

Lemma 2.1.10. $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$.

Proof. Let $x \in \mathbb{Q}_p$ such that $|x|_p \leq 1$. By the claim in the proof of Proposition 2.1.9, we can find a Cauchy sequence in $\mathbb{Z}$ that converges to x, hence $x \in \mathbb{Z}_p$. □

Exercise 2.1.11. *Let* $a_n \in \mathbb{Q}_p$ *for* $n \in \mathbb{Z}_{\geq 0}$, *then* $\sum_{n=0}^{\infty} a_n$ *converges in* $\mathbb{Q}_p$ *if and only if* $\lim_{n \to \infty} |a_n|_p = 0$.

Lemma 2.1.12. *Every element* x *in* $\mathbb{Q}_p$ *can be written uniquely of the form* $x = \sum_{n \gg -\infty} a_n p^n$, *with* $a_n \in \{0, \cdots, p-1\}$.

Proof. For the uniqueness, if $\sum_{n \gg -\infty} a_n p^n = \sum_{n \gg -\infty} b_n p^n$, letting m be the minimal integer such that $b_m \neq a_m$, we see $0 = \sum_{i=m}^{+\infty} (b_i - a_i) p^i$. However, $|\sum_{i=m}^{+\infty} (b_i - a_i) p^i|_p = p^{-m}$, a contradiction.

For the existence of the form, by multiplying x by p^M for M sufficiently large, we can and do assume $x \in \mathbb{Z}_p$. Now we choose $a_n \in \{0, \cdots, p-1\}$ for n such that $\sum_{n=0}^{k} a_n p^n \equiv x \pmod{p^k}$ for all k. One easily checks $x = \sum_{n=0}^{+\infty} a_n p^n$. □

Exercise 2.1.13. *In $\mathbb{Q}_3$, expand $-\frac{1}{2}$ in the form of the lemma.*

2.2 Absolute value

Definition 2.2.1. *A valuation field (or a normed field) $(K, |\cdot|)$ is a field k together with an absolute value: $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that*

(1) $|x| = 0$ if and only if $x = 0$,

(2) $|xy| = |x||y|$,

(3) $|x + y| \leq |x| + |y|$.

The norm $|\cdot|$ is called non-archimedean if $|x + y| \leq \max\{|x|, |y|\}$. Two norms $|\cdot|_1$, $|\cdot|_2$ on K are called equivalent if there exists $r > 0$ such that $|\cdot|_2^r = |\cdot|_1$.

Let $(K, |\cdot|)$ be a valuation field, $|\cdot|$ defines then a topology on K such that $U(a, \epsilon) := \{x \in K \mid |x - a| < \epsilon\}$ form an open basis.

Example 2.2.2. *The followings are valuation fields: $(\mathbb{Q}, |\cdot|)$, $(\mathbb{Q}, |\cdot|_p)$, $(\mathbb{R}, |\cdot|)$, $(\mathbb{Q}_p, |\cdot|_p)$.*

Proposition 2.2.3. *Let $(K, |\cdot|)$ be a valuation field. Then there exists a unique valuation field $(\widehat{K}, |\cdot|_{\widehat{K}})$ such that*

1. *K is a subfield of $\widehat{K}$, and the restriction of $|\cdot|_{\widehat{K}}$ on K is equal to $|\cdot|$.*
2. *K is dense in $\widehat{K}$,*
3. *$\widehat{K}$ is complete for $|\cdot|_{\widehat{K}}$,*
4. *if $f : (K, |\cdot|) \hookrightarrow (L, |\cdot|_L)$ is an embedding of valuation fields (i.e. $|\cdot|_L \sim |\cdot|$ when restricted to K) with L complete, then f extends uniquely to an embedding $\widehat{f} : (\widehat{K}, |\cdot|_{\widehat{K}}) \hookrightarrow (L, |\cdot|_L)$ of valuation fields.*

Proof. Define $\widehat{K}$ to be the completion of k via $|\cdot|$. Let (a_n), (b_n) be two Cauchy sequences in K, one can check

- $(a_n b_n)$, $(a_n + b_n)$ are Cauchy sequences in K,
- if $(a'_n) \sim (a_n)$, $(b'_n) \sim (b_n)$, then $(a_n b_n) \sim (a'_n b'_n)$, $(a_n + b_n) \sim (a'_n + b'_n)$.

Then $\widehat{K}$ has a natural algebraic structure: for equivalent classes (a_n), (b_n) of Cauchy sequences in K, define $(a_n)(b_n) := (a_n b_n)$ and $(a_n) + (b_n) := (a_n + b_n)$. For a Cauchy sequence $(a_n) \nsim (0)$ (noting this implies there exist r_1, $r_2 > 0$ and $N \in \mathbb{Z}_{\geq 1}$ such that $r_1 \leq |a_n| \leq r_2$ for $n \geq N$), (a_n^{-1}) (removing the terms $a_m = 0$) is a Cauchy sequcence in K and $(a_n^{-1})(a_n) = (1)$. Thus we see $\widehat{K}$ is a field. For $x \in \widehat{K}$, represented by (a_n), we put $|x|_{\widehat{K}} := \lim_{n\to\infty} |a_n|$. By definition, the properties 1, 2, 3 hold for $\widehat{K}$. For 4, we define $\widehat{f} : \widehat{K} \to L$, $(a_n) \mapsto \lim_{n\to\infty} f(a_n)$. Actually, it is straightforward to check if (a_n) is a Cauchy sequence in K, then $(f(a_n))$ is a Cauchy sequence in L, and that if $(a_n) \sim (a'_n)$, then $(f(a_n)) \sim (f(a'_n))$. The existence of $(\widehat{K}, |\cdot|_{\widehat{K}})$ follows. The uniqueness follows from the properties 4 and 1. □

Definition 2.2.4. *An additive valuation υ on K is a map $\upsilon : K \to \mathbb{R} \cup \{+\infty\}$ such that*

1. *$\upsilon(x) = +\infty$ if and only if $x = 0$,*
2. *$\upsilon(xy) = \upsilon(x) + \upsilon(y)$,*
3. *$\upsilon(x + y) \geq \min\{\upsilon(x), \upsilon(y)\}$.*

Two additive valuations υ_1, υ_2 are called equivalent if there exists $r > 0$ such that $\upsilon_2 = r\upsilon_1$.

The following lemma is clear.

Lemma 2.2.5. *Let $q > 1$, the map $\upsilon \mapsto [x \mapsto q^{-\upsilon(x)}]$ gives a bijection between the set of additive valuations on K and the set of non-archimedean norms on K, where the inverse is given by $|\cdot| \mapsto [x \mapsto -\log_q(|x|)$.*

Theorem 2.2.6 (Ostrouski)**.** *Let $|\cdot|$ be a non-trivial norm on $\mathbb{Q}$.*

(a) If $|\cdot|$ is archimedean, then $|\cdot|$ is equivalent to the standard absolute value $|\cdot|_\infty$.

(b) If $|\cdot|$ is non-archimedean, then it is equivalent to $|\cdot|_p$ for prime number p.

2.3 Non-archimedean valuation field

Let $(K, |\cdot|)$ be a non-archimedean valuation field, let υ be an associated additive valuation.

Lemma 2.3.1. $|x + y| = \max\{|x|, |y|\}$ *if* $|x| \neq |y|$.

Proof. Suppose $|x| > |y|$, then $|x| \leq \max\{|x + y|, |-y|\}$. Note $|-y| = |-1||y| = |y|$ ($|1 \cdot x| = |x| = |1||x| \Rightarrow |1| = 1$ and $|(-1)(-1)| = |1| \Rightarrow |-1| = 1$). The lemma follows. □

Lemma 2.3.2. *Let $r > 0$, then $\{x \in K \mid |x| \leq r\}$ is an open subset of K.*

Proof. For any $a \in \{x \in K \mid |x| \leq r\}$, $0 < s < r$, we have $\{x \in K \mid |x - a| < s\} \subset \{x \in K \mid |x| \leq r\}$. □

Put $\mathcal{O}_K := \{x \in K \mid |x| \leq 1\} = \{x \in K \mid \upsilon(x) \geq 0\}$.

Lemma 2.3.3. *$\mathcal{O}_K$ is a subring of K.*

Proof. Let x, $y \in \mathcal{O}_K$, then $|xy| \leq 1$, and $|x \pm y| \leq 1$. □

We call $\mathcal{O}_K$ the valuation ring of $(K, |\cdot|)$.

Proposition 2.3.4. *Two non-trivial non-archimedean norms $|\cdot|_1$ and $|\cdot|_2$ on a field K are equivalent if and only if their valuation rings are the same.*

Proof. "Only if" is clear. Suppose for any $x \in K$, $|x|_1 \leq 1$ if and only if $|x|_2 \leq 1$. Let $b \in K$ such that $|b|_1 > 1$, there exists $r > 0$ such that $|b|_2 = |b|_1^r$. For any $x \in K \setminus \{0\}$, there exists ρ such that $|x|_1 = |b|_1^\rho$. For any $u, v, u', v' \in \mathbb{Z}$ such that $v, v' \neq 0$ and $\frac{u}{v} \leq \rho \leq \frac{u'}{v'}$, we have $|b|_1^{\frac{u}{v}} \leq |x|_1 \leq |b|_1^{\frac{u'}{v'}}$, that is equivalent to $|b^u/x^v|_1 \leq 1$ and $|x^{v'}/b^{u'}|_1 \leq 1$. Hence $|b^u/x^v|_2 \leq 1$ and $|x^{v'}/b^{u'}|_2 \leq 1$, and thus $|b|_2^{\frac{u}{v}} \leq |x|_2 \leq |b|_2^{\frac{u'}{v'}}$. Let $\frac{u}{v}$ and $\frac{u'}{v'}$ converge to ρ, we see $|x|_2 = |b|_2^\rho = |x|_1^r$ and hence $|\cdot|_1 \sim |\cdot|_2$. □

Definition 2.3.5. *If $v|_{\mathcal{O}_K \setminus \{0\}}$ has discrete image, then we call $\mathcal{O}_K$ a discrete valuation ring.*

Remark 2.3.6. *Let $\mathcal{O}_K$ be a discrete valuation ring, then $v(K \setminus \{0\})$ is a lattice in $\mathbb{R}$. We call the valuation v normalized if $v(K \setminus \{0\}) = \mathbb{Z}$.*

Example 2.3.7. *$\mathbb{Z}_p$ is a discrete valuation ring.*

Proposition 2.3.8. *Let $(K, |\cdot|)$ be a non-archimedean valuation field.*

(1) $\mathcal{O}_K$ is integrally closed and is a local ring with maximal ideal $\mathfrak{m}_K := \{x \in K \mid |x| < 1\}$ (a ring is called local if it has a unique maximal ideal).

(2) Let $\widehat{K}$ be the completion of K, then $\mathcal{O}_{\widehat{K}}$ is the completion of $\mathcal{O}_K$ under $|\cdot|$. If $\pi \in \mathfrak{m}_K$ is a non-zero element, then one has a canonical isomorphism (where $\mathcal{O}_K/\pi^n$ is equipped with the discrete topology)

$$\mathcal{O}_{\widehat{K}} \cong \varprojlim_n \mathcal{O}_K/\pi^n = \{(x_n) \in \prod_{n \geq 1} \mathcal{O}_K/\pi^n \mid x_{n+1} \equiv x_n \pmod{\pi^n}\}.$$

(3) If $|\cdot|$ is a discrete valuation, then $\mathfrak{m}_K$ is principal and all the non-zero ideals of $\mathcal{O}_K$ are of the form $\mathfrak{m}_K^n$ with $n \in \mathbb{Z}_{\geq 0}$.

Proof. (1) Let $x \in K$ and suppose $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, $a_i \in \mathcal{O}_K$. If $|x| > 1$, then $|x^n| > |a_i x^i|$ for all $i = 0, \cdots, n-1$. So $0 = |x^n + \cdots + a_0| = |x^n| > 1$, a contradiction.

(2) Let $x \in \mathcal{O}_{\widehat{K}} \subset \widehat{K}$, thus $x = \lim_{n\to\infty} a_n$ with $a_n \in K$. Since $|x| \leq 1$, we have $|a_n| \leq 1$ for n sufficiently large. This implies $x \in \widehat{\mathcal{O}_K}$ (i.e. the completion of $\mathcal{O}_K$ under $|\cdot|$). Conversely if $x \in \widehat{\mathcal{O}_K}$, then it is clear that $|x|_{\widehat{K}} \leq 1$.

For any $x \in \mathcal{O}_{\widehat{K}} \cong \widehat{\mathcal{O}_K}$, let (a_n) be a Cauchy sequence in $\mathcal{O}_K$ that converges to x. By removing certain terms, we can and do assume $|x - a_n| \leq |\pi|^n$ that implies $|a_m - a_n| \leq |\pi|^n$

for $m \geq n$. Thus $|\pi^{-n}(a_m - a_n)| \leq 1 \Leftrightarrow \pi^{-n}(a_m - a_n) \in \mathcal{O}_K \Leftrightarrow a_m - a_n \in \pi^n \mathcal{O}_K$. If (a'_n) is another Cauchy sequence that converges to x satisfying the same condition, we see $|a'_n - a_n| \leq |\pi|^n$ and hence $a'_n - a_n \in \pi^n \mathcal{O}_K$ by the same argument as above. In particular, we obtain a well-defined map

$$\mathcal{O}_{\widehat{K}} \to \varprojlim_n \mathcal{O}_K/\varpi^n, \ x \mapsto (a_n).$$

It is straightforward to check this map is a bijective ring homomorphism and is a homemorphism (Exercise).

(3) Suppose $|\cdot|$ is discrete, and let υ be the corresponding normalized additive valuation. Let $\alpha \in \mathcal{O}_K$ such that $\upsilon(\alpha) = 1$. For $\beta \in \mathfrak{m}_K$, $\upsilon(\beta) \in \mathbb{Z}_{>0}$ and hence $\upsilon(\beta/\alpha) \geq 0 \Rightarrow \beta \in \alpha\mathcal{O}_K$. Thus $\mathfrak{m}_K = \alpha\mathcal{O}_K$. Let I be a non-zero ideal, and let $m := \inf\{\upsilon(x) \mid x \in I\}$. Thus For $x \in I$, $\upsilon(x/\alpha^m) \geq 0$ hence $x \in \alpha^m\mathcal{O}_K = \mathfrak{m}_K^m$. If $x \in I$ satisfies $\upsilon(x) = m$, then $\alpha^m \in x\mathcal{O}_K \subset I$. Thus $I = \mathfrak{m}_K^m$. □

Definition 2.3.9. *Let $(K, |\cdot|)$ be a non-archimedean valuation field. We call $\mathcal{O}_K/\mathfrak{m}_K$ the residue field of $\mathcal{O}_K$. If $\mathcal{O}_K$ is a discrete valuation ring, we call a generator π of $\mathfrak{m}_K$ a uniformizer of K (or of $\mathcal{O}_K$).*

Proposition 2.3.10. *For a domain R, R is a discrete valuation ring if and only if R is a local Dedekind domain.*

Proof. The "only if" part follows from the above proposition. Suppose R is a local Dedekind domain, and let $\mathfrak{m}$ be the unique maximal ideal (that is also the unique non-zero prime ideal). Let $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, using prime factorization (since R is Dedekind), we have $\mathfrak{m} = (x)$. For $0 \neq y \in R$, there exists a unique $\upsilon(y) \in \mathbb{Z}_{\geq 0}$ such that $y \in \mathfrak{m}^{\upsilon(y)} \setminus \mathfrak{m}^{\upsilon(y)+1}$. So $\upsilon(y)$ is the integer such that $y \in x^{\upsilon(y)}R^\times$. One can check the map $\upsilon : R \to \mathbb{Z}_{\geq 0}$, $y \mapsto \upsilon(y)$ defines a discrete valuation on R. □

Let K be a complete discrete valuation field. Let $S \subset \mathcal{O}_K$ be a set of representatives of $\mathcal{O}_K/\mathfrak{m}_K = k$, and let π be a uniformizer of K

Lemma 2.3.11. *For all $x \in K$, x can be uniquely written as $x = \sum_{n \gg -\infty} a_n\pi^n$, $a_n \in S$.*

Proof. It suffices to show for $x \in \mathcal{O}_K$, x can be uniquely written as $\sum_{n=0}^{+\infty} a_n\pi^n$. Let $a_0 \in S$ be the unique element such that $x - a_0 \in \pi\mathcal{O}_K$. We use induction to construct $\{a_i\}$: suppose there exists $a_0, \cdots, a_i \in S$ such that $x - \sum_{j=0}^{i} a_j\pi^j = pi^{j+1}x_{j+1} \in \pi^{j+1}\mathcal{O}_K$, then let $a_{j+1} \in S$ be the unique element such that $a_{j+1} - x_{j+1} \in \pi\mathcal{O}_K$. It is easy to see $x = \sum_{n=0}^{+\infty} a_n\pi^n$. If $\sum_{n=0}^{+\infty} a_n\pi^n = \sum_{n=0}^{+\infty} b_n\pi^n$, and suppose m is the minimal element such that $a_m \neq b_m$. Then $a_m\pi^m - b_m\pi^m \in \pi^{m+1}$ and thus $a_m \equiv b_m \pmod{\pi}$ a contradiction. The uniqueness follows. □

If the residue field k is finite, we have a natural choice of the representative set S. We begin with a lemma.

Lemma 2.3.12. *For any $x \in \mathcal{O}_K$, $(1 + \pi x)^{p^n} \in 1 + \pi^{n+1}\mathcal{O}_K$.*

Proof. We have $(1+\pi^n x)^p = \sum_{i=0}^{p} \binom{p}{i} (pi^n x)^i$. Since $p \in \pi\mathcal{O}_K$, we see $(1+\pi^n x)^p \in 1+\pi^{n+1}\mathcal{O}_K$. The lemma then follows by induction. □

Now let $a \in k$, and let $\tilde{a} \in \mathcal{O}_K$ be an arbitrary lifting of a. Let $q := |k|$.

Proposition 2.3.13. *The sequence $\tilde{a}^{q^n}$ converges. Let $[a] := \lim_n \tilde{a}^{q^n}$, then $[a] \equiv a \pmod{\mathfrak{m}_K}$. The map $k \to \mathcal{O}_K$, $a \mapsto [a]$ is multiplicative.*

Proof. We have $\tilde{a}^{q^m} - \tilde{a}^{q^n} = \tilde{a}^{q^n}(\tilde{a}^{q^m-q^n}-1) = \tilde{a}^{q^n}((\tilde{a}^{q^{m-n}-1})^{q^m}-1)$. We have $\tilde{a}^{q^{m-n}-1} \equiv 1 \pmod{\mathfrak{m}_K}$. The first part follows from the above lemma. We have $\tilde{a}^{q^n} \equiv a \pmod{\mathfrak{m}_K}$ and hence $[a] \equiv a \pmod{\mathfrak{m}_K}$. Finally, we have $[ab] = \lim_n (\tilde{a}\tilde{b})^{q^n} = (\lim_n \tilde{a}^{q^n})(\lim_n \tilde{b}^{q^n}) = [a][b]$. □

Remark 2.3.14. *The element $[a]$ is called the Teichmüler lifting of a.*

The additive structure of $\mathcal{O}_K$ is rather clear:

$$0 \subsetneq \cdots \subseteq \mathfrak{m}_K^n \subsetneq \cdots \subsetneq \mathfrak{m}_K \subsetneq \mathcal{O}_K.$$

Consider $U_K := \mathcal{O}_K^\times = \mathcal{O}_K \setminus \mathfrak{m}_K = \{x \in K^\times \mid \upsilon(x) = 0\}$. Put $U_K^n := \{x \in U_K \mid x \equiv 1 \pmod{\mathfrak{m}_K^n}\}$. We have

Proposition 2.3.15. *(1) $\cap_n U_K^n = 1$.*

(2) $U_K \cong \varprojlim_n U_K/U_K^n$.

(3) We have isomorphisms of groups $U_K/U_K^1 \cong k^\times$ and $U_K^n/U_K^{n+1} \cong k$ for $n \geq 1$.

Proof. (1) (2) are clear. The first isomorphism is given by $x \mapsto \bar{x} \in k^\times$. Let $n \geq 1$, and consider the bijective map

$$U_K^n/U_K^{n+1} \to k, 1+\pi^n x \mapsto \bar{x}.$$

We have $(1+\pi^n x)(1+\pi^n y) \mapsto \overline{x+y}$. The second isomorphism follows. □

Exercise 2.3.16. *Suppose $p \geq 3$, show that*

$$1 + p\mathbb{Z}_p \to p\mathbb{Z}_p,\ x \mapsto \log x = \sum_{n=1}^{\infty} \frac{(-1)^n}{n}(x-1)^n$$

is an isomorphism of topological groups.

2.4 Extensions of valuations

Theorem 2.4.1 (Hensel's Lemma)**.** *Let $(K, |\cdot|)$ be a complete non-archimedean field, $f(x) \in \mathcal{O}_K[x]$ such that $0 \neq \overline{f(x)} \in k[x]$ (such polynomial $f(x)$ is called primitive). Suppose we have $\overline{f(x)} = \overline{u}(x)\overline{v}(x)$ such that $(\overline{u}(x), \overline{v}(x)) = 1$. Then $f(x)$ admits a factorization $f(x) = u(x)v(x)$ where $u(x), v(x) \in \mathcal{O}_K[x]$, such that $\deg u(x) = \deg \overline{u}(x)$, $u(x) \equiv \overline{u}(x) \pmod{\mathfrak{m}_K}$, $v(x) \equiv \overline{v}(x) \pmod{\mathfrak{m}_K}$.*

Proof. Let $r := \deg \overline{u}(x)$, $s := \deg f - r$ (thus $s \geq \deg \overline{v}(x)$). Let $u_0(x)$, $v_0(x) \in \mathcal{O}_K[x]$ such that $\overline{u_0(x)} \equiv \overline{u}(x) \pmod{\mathfrak{m}_K}$, $\deg u_0(x) = r$, $\overline{v_0(x)} \equiv \overline{v}(x)$ and $\deg v_0(x) \leq s$. Thus $f \equiv u_0 v_0 \pmod{\mathfrak{m}_K}$. Since $(\overline{u}(x), \overline{v}(x)) = 1$, there exists $a(x)$, $b(x) \in \mathcal{O}_K[x]$ such that $a(x)u_0(x) + b(x)v_0(x) \equiv 1 \pmod{\mathfrak{m}_K}$. We remark that the leading coefficient of $u_0(x)$ is a unit. If $f(x) = u_0(x)v_0(x)$, then we are done. If not, by the above discussion, we have $f(x) - u_0(x)v_0(x) \in \mathfrak{m}_K[x]$ and $a(x)u_0(x) + b(x)v_0(x) - 1 \in \mathfrak{m}_K[x]$. Thus there exist $\pi \in \mathfrak{m}_K$ and $f_1(x) \in \mathcal{O}_K[x]$ such that (so $\deg f_1(x) \leq \deg f(x)$)

$$\begin{cases} f(x) - u_0(x)v_0(x) = \pi f_1(x) \\ a(x)u_0(x) + b(x)v_0(x) - 1 \in (\pi\mathcal{O}_K)[x]. \end{cases}$$

We will use an induction argument to construct sequences of polynomials $\{u_n(x)\}$ and $\{v_n(x)\}$ such that they converge the desired $u(x)$ and $v(x)$ respectively. To start, we want $u_1(x)$, $v_1(x)$ to have the form $u_1(x) = u_0(x) + \pi p_1(x)$ and $v_1(x) = v_0(x) + \pi q_1(x)$. Then

$$\begin{aligned} f(x) - u_1(x)v_1(x) &= f(x) - u_0(x)v_0(x) - \pi(u_0(x)q_1(x) + v_0(x)p_1(x)) - \pi^2 p_1(x)q_1(x) \\ &= \pi\big(f_1(x) - u_0(x)q_1(x) - v_0(x)p_1(x)\big) + \pi^2 p_1(x)q_1(x). \end{aligned}$$

Claim: There exist $p_1(x)$, $q_1(x)$ such that $\deg p_1(x) \leq r$, $\deg q_1 \leq s$, and $f_1(x) - u_0(x)q_1(x) - v_0(x)p_1(x) = \pi f_2(x) \in \pi\mathcal{O}_K[x]$.

We prove the claim. Since $a(x)u_0(x) + b(x)v_0(x) \equiv 1 \pmod{\pi}$, we see $a(x)u_0(x)f_1(x) + b(x)v_0(x)f_1(x) \equiv f_1(x) \pmod{\pi}$. We need to control the degrees of the polynomials. Let $q_1'(x) \in \mathcal{O}_K[x]$ and $p_1(x) \in \mathcal{O}_K[x]$ such that $b(x)f_1(x) = q_1'(x)u_0(x) + p_1(x)$ and $\deg p_1(x) \leq \deg u_0(x) = r$. And let $q_1(x)$ be the degree $\leq s$ part of $a(x)f_1(x) + q_1'(x)$. Then we have $(a(x)f_1(x) + q_1'(x))u_0(x) + p_1(x)v_0(x) \equiv f_1(x) \pmod{\pi}$, and hence (by comparing degrees and noting $\deg f_1(x) \leq r + s$) $q_1(x)u_0(x) + p_1(x)v_0(x) \equiv f_1(x)$. The claim follows.

Note we have $\deg f_2(x) \leq \deg f(x)$, so we can continue with the argument. Indeed, suppose we have $\{u_i(x)\}_{i=0,\cdots,n-1}$ and $\{v_i(x)\}_{i=0,\cdots,n-1}$ such that $\deg u_i(x) = r$, $\deg v_i(x) \leq s$, $u_i(x) \equiv u_{i-1}(x) \pmod{\pi^i}$, $v_i(x) \equiv v_{i-1}(x) \pmod{\pi^i}$ and $f(x) - u_i(x)v_(x) \in \pi^i\mathcal{O}_K[x]$. Let $f_{n-1}(x) \in \mathcal{O}_K[x]$ such that $f(x) - u_{n-1}(x)v_{n-1}(x) = \pi^{n-1}f_n(x)$ and $\deg f_{n-1}(x) \leq \deg f(x)$. Applying the claim with (u_0, v_0, f_1) replaced by (u_{n-1}, v_{n-1}, f_n), noting $a(x)u_{n-1}(x) + b(x)v_{n-1}(x) - 1 \in (\pi\mathcal{O}_K)[x])$, we obtain polynomials $p_n(x)$, $q_n(x)$ such that $\deg p_n(x) \leq r$, $\deg q_n(x) \leq s$ and $f_n(x) - u_{n-1}(x)q_n(x) - v_{n-1}(x)p_n(x) \in \pi\mathcal{O}_K[x]$. Hence for $u_n(x) := u_{n-1}(x) + \pi^n p_n(x)$, $v_n(x) := v_{n-1}(x) + \pi^n q_n(x)$, we have $f(x) - u_n(x)v_n(x) = \pi^{n-1}(f_n(x) - u_{n-1}(x)q_n(x) - v_{n-1}(x)p_n(x)) + \pi^{2n}p_n(x)q_n(x) \in \pi^n\mathcal{O}_K[x]$. Let $u(x) := \lim_n u_n(x)$ and $v(x) := \lim_n v_n(x)$. Thus $f(x) = u(x)v(x)$ and the theorem follows. □

Corollary 2.4.2. *Let $f(x) \in \mathcal{O}_K[x]$, $\alpha_0 \in \mathcal{O}_K$ such that $f(\alpha_0) \equiv 0 \pmod{\mathfrak{m}_K}$ and $f'(\alpha_0) \neq 0 \pmod{\mathfrak{m}_K}$. Then there exists a unique $\alpha \in \mathcal{O}_K$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{\mathfrak{m}_K}$.*

Proof. Exercise. □

Corollary 2.4.3. *Let $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$ and suppose $f(x)$ is irreducible. Then $\max\{|a_i|\} = \max\{|a_0|, |a_k|\}$.*

Proof. Exercise. □

Theorem 2.4.4. *Let $(K, |\cdot|)$ be a complete non-archimedean field. Let L/K be a finite extension of degree n. Then there exists a unique extension $|\cdot|_L$ of $|\cdot|$ to a non-archimedean valuation on L. Moreover, for any $x \in L$, $|x|_L = |N_{L/K}(x)|^{\frac{1}{n}}$ and L is complete for $|\cdot|_L$.*

Proof. Put $|x|_L := |N_{L/K}(x)|^{\frac{1}{n}}$. It is easy to see $|x|_L = 0 \Leftrightarrow x = 0$ and $|xy|_L = |x|_L|y|_L$. We show $|x+y|_L \leq \max\{|x|_L, |y|_L\}$. Assume $|x|_L \leq |y|_L$ and $|y|_L \neq 0$, it suffices to show

$$|1 + \frac{x}{y}|_L \leq 1. \tag{2.1}$$

Put $\mathcal{O}_L$ to be the integral closure of $\mathcal{O}_K$ in L.

Claim: $\mathcal{O}_L = \{x \in L \mid |x|_L \leq 1\}$ (in particular, the latter set is a ring, and (2.1) follows).

We prove the claim. For $\alpha \in \mathcal{O}_L$, we have $N_{L/K}(\alpha) \in \mathcal{O}_K$ hence $|\alpha|_L \leq 1$. Suppose $|\alpha|_L \leq 1$, and let $f(x) = x^m + \cdots + a_0 \in K[x]$ be the minimal polynomial of α over K. Since $N_{L/K}(\alpha) \in \mathcal{O}_K$, one deduces $a_0 \in \mathcal{O}_K$. If $f(x) \in \mathcal{O}_K[x]$, then $x \in \mathcal{O}_L$. If not, let $c \in \mathfrak{m}_K$ such that $cf(x) \in \mathcal{O}_K[x]$ is primitive. Using $a_0 \in \mathcal{O}_K$, we see $0 < \deg \overline{cf(x)} < m$. By Hensel's lemma applied to $cf(x)$ and the decomposition $\overline{cf(x)} = \overline{cf(x)} \cdot 1$, there exists $u(x) \in \mathcal{O}_K[x]$, $0 < \deg u(x) < m$ such that $u(x)|f(x)$, a contradiction.

We have shown that $|\cdot|_L$ is a non-archimedean norm that extends $|\cdot|$. We prove $|\cdot|_L$ is unique. Suppose we have another $|\cdot|'_L$ that extends $|\cdot|$. We will show $|\cdot|_L \sim |\cdot|'_L$. Indeed, if so, using the fact the both are the same when restricted to K, we see $|\cdot|_L = |\cdot|'_L$. By Proposition 2.3.4, it suffices to show that for all $\alpha \in L$, $|\alpha|_L \leq 1 \Leftrightarrow |\alpha|'_L \leq 1$. Let $f(x) = x^k + \cdots + a_0$ be the monic minimal polynomial of α over K. If $|\alpha|_L \leq 1$, then $f(x) \in \mathcal{O}_K[x]$, we deduce then $|\alpha|'_L \leq 1$ (otherwise, $|f(\alpha)|'_L = |\alpha^{\deg f(x)}|_{L'} \neq 0$). We prove the other direction. If $|\alpha|_L < 1$, we see the constant term of $f(x)$ lies in $\mathfrak{m}_K$. We claim $a_i \in \mathfrak{m}_K$ for all $i = 1, \cdots, k-1$. In fact, if not, then $\overline{f(x)} = x^r v(x)$ where r is the minimal integer such that $a_r \notin \mathfrak{m}_K$, and $(x^r, v(x)) = 1$. Using Hensel's lemma, we see $f(x)$ is reducible, a contradiction. Since $f(\alpha) = 0$, and $a_i \in \mathfrak{m}_K$, we see $|\alpha|'_L < 1$ (otherwise, $|f(\alpha)|'_L = |\alpha^k|'_L \neq 0$). So $|\alpha|'_L \geq 1 \Rightarrow |\alpha|_L \geq 1$ and hence $|\alpha|'_L \leq 1 \Rightarrow |\alpha|_L \leq 1$. This concludes the uniqueness of $|\cdot|_L$.

The completeness of L will follow from Lemma 2.4.6 on topological vector space. □

Definition 2.4.5. *Let V be a vector space over $(K, |\cdot|)$. Then a (ultra-metric) norm on V is a map $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ such that*

- $\|x\| = 0 \Leftrightarrow x = 0$,
- $\|\lambda x\| = |\lambda|\|x\|$,
- $\|x + y\| \leq \max\{\|x\|, \|y\|\}$.

Tow norms $\|\cdot\|_1$ and $\|\cdot\|_2$ are called equivalent if there exist $c_1, c_2 > 0$ such that $c_1\|x\|_1 \leq \|x\|_2 \leq c_2\|x\|_1$ for all $x \in V$.

Lemma 2.4.6. *Let V be a finite dimensional vector space over $(K, |\cdot|)$. Then any two norms on V are equivalent and V is complete.*

Proof. Let $e_1, \cdots, e_n$ be a basis of V over K. For $x = \sum_{i=1}^n a_i e_i$, put $\|x\| := \max_{1\le i\le n}\{|a_i|\}$. This defines a norm on V, and it is easy to see V si complete for $\|\cdot\|$.

Let $\|\cdot\|'$ be a norm on V, and let $c_2 := \max_{1\le i\le n}\{\|e_i\|'\}$. We have then $\|x\|' \le c_2\|x\|$.

We use an induction argument on the dimension of V. Suppose any norm on a K-vector space of dimension $\le n-1$ is complete (the one dimensional case is clear). Let $V_i := Ke_1 + \cdots + Ke_{i-1} + Ke_{i+1} + \cdots + Ke_n$, that is complete for $\|\cdot\|'$. This implies $e_i + V_i$ is closed in $(V, \|\cdot\|')$. As $0 \notin e_i + V_i$, there exists $\epsilon > 0$ such that $U(0,\epsilon) = \{x \in V \mid \|x\|' < \epsilon\}$ is disjoint from all $e_i + V_i$. Let $x = \sum a_i e_i$ and let r such that $\|x\| = |a_r|$, then

$$\|x\|' = \|\sum a_i e_i\|' = |a_r|\|\sum \frac{a_i}{a_r} v_i\|' \ge |a_r|\epsilon = \|x\|\epsilon.$$

Hence $\|\cdot\| \sim \|\cdot\|'$ and V is also complete for $\|\cdot\|'$. □

Remark 2.4.7. *By induction, the statement in Theorem 2.4.4 also holds for algebraic extensions of K.*

Let $(K, |\cdot|)$ be a complete non-archimedean valuation field. By Theorem 2.4.4, there exists a (unique) norm, still denoted by $|\cdot|$, on $\overline{K}$ that extends $|\cdot|$ on K.

Lemma 2.4.8 (Krasner's lemma)**.** *Let $(K, |\cdot|)$ be a complete non-archimedean valuation field. Let α, $\beta \in \overline{K}$ such that $|\alpha - \beta| < |\alpha - \alpha'|$ for all Galois conjugate α' of α different from α. Then $\alpha \in K(\beta)$.*

Proof. It suffices to show that for any $\sigma : K(\alpha,\beta) \hookrightarrow \overline{K}$, if $\sigma(\beta) = \beta$ then $\sigma(\alpha) = \alpha$. However, we have $|\sigma(\alpha) - \alpha| = |\sigma(\alpha) - \sigma(\beta) + \beta - \alpha| \le |\beta - \alpha|$. By assumption, $\sigma(\alpha) = \alpha$. □

Corollary 2.4.9. *Let $f(x) = x^n + \cdots + a_0 \in \mathcal{O}_K[x]$ be an irreducible monic polynomial of degree n. Put $d_0 := \min_{\alpha\ne\alpha'}\{|\alpha - \alpha'|\}$ where α, α' run through distinct roots of $f(x)$. Let $g(x) := x^n + \cdots + b_0 \in \mathcal{O}_K[x]$. Suppose $|b_i - a_i| < d_0^n$. Let β be a root of $g(x)$, then there exists α such that $f(\alpha) = 0$ and $\alpha \in K(\beta)$ (in particular, $g(x)$ is irreducible).*

Proof. Let β be a root of $g(x)$. Then $|\prod_{\alpha'}(\beta - \alpha')| = |f(\beta)| = |f(\beta) - g(\beta)| \le \max_{0\le i\le n-1}\{|b_i - a_i|\}$. So there exists a root α of $f(x)$ such that $|\beta - \alpha| < d_0$. By Krasner's lemma, $\alpha \in K(\beta)$. □

Corollary 2.4.10. *The algebraic closure $(\overline{\mathbb{Q}_p}, |\cdot|)$ is not complete.*

Proof. Let $\{\alpha_i\}_{i=1}^\infty$ be a set of elements in $\overline{\mathbb{Q}_p}$ that are linearly independent over $\mathbb{Q}_p$. It is easy to inductively find $c_i \in \mathbb{Q}_p^\times$ such that $|c_n\alpha_n| \to 0$ when $n \to +\infty$, and that $|c_{n+1}\alpha_{n+1}| < |\sigma(s_k) - s_k|$ for all $k \le n$, $\sigma(s_k) \ne s_k$, where $s_k := \sum_{i=1}^k c_i\alpha_i$. Let $s := \lim s_n$. If $s \in \overline{\mathbb{Q}_p}$, then $|s - s_n| \le \max_{i\ge n+1}|c_i\alpha_i| \le |\sigma(s_n) - s_n|$ for all $\sigma(s_n) \ne s_n$. Using Krasner's lemma, we see $s_n \in K(s)$ for all n. But $\{s_i\}$ are linearly independent over $\mathbb{Q}_p$, a contradiction. □

Let $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$ be the completion of $\overline{\mathbb{Q}_p}$.

Corollary 2.4.11. *$\mathbb{C}_p$ is algebraic closed.*

Proof. Let $p(x) = x^d + \cdots + a_0 \in \mathbb{C}_p[x]$, $d > 1$. It suffices to show $p(x)$ has a root in $\mathbb{C}_p$. We can and do assume $a_i \in \mathcal{O}_{\mathbb{C}_p}$ (e.g. by replacing x by x/p^k with k sufficiently large). Let C' be the splitting field of $p(x)$, and let $\lambda := \min_{\alpha \neq \alpha'|}\{|\alpha - \alpha'\}$ where α, α' run though distinct roots of $p(x)$. Let $q(x) := x^d + \cdots + b_0 \in \overline{\mathbb{Q}_p}[x]$ such that $|b_i - a_i| < \lambda^d$. By Corollary 2.4.9, there exist a root α of $p(x)$ and a root β of $q(x)$ such that $\alpha \in \mathbb{C}_p(\beta) = \mathbb{C}_p$. The corollary follows. □

Corollary 2.4.12. *Let K be a finite extension of $\mathbb{Q}_p$. Then there exists a (irreducible) polynomial $f(x) \in \mathbb{Q}[x]$ such that $K \cong \mathbb{Q}_p[x]/f(x)$.*

Proof. Exercise. □

2.5 Finite extensions of complete discrete valuation fields

Let K be a complete discrete valuation field, $\upsilon_K : K \to \mathbb{Z} \cup \{+\infty\}$ be the nomalized additive valuation, and we have $(\pi_K) = \mathfrak{m}_K \subset \mathcal{O}_K \subset K$, $k = \mathcal{O}_K/\mathfrak{m}_K$. Let L/K be a finite extension. Then L is also a complete discrete valuation field. Let υ_L be the normalized additive valuation on L, and we have $(\pi_L) = \mathfrak{m}_L \subset \mathcal{O}_L \subset L$.

Lemma 2.5.1. *$\mathcal{O}_L$ is a finite free $\mathcal{O}_K$-module of rank $[L : K]$.*

Proof. Let b_i *in*$\mathcal{O}_L$ such that $\{\overline{b_i}\}$ form a basis of $\mathcal{O}_L/\varpi_K$ over $\mathcal{O}_K/\varpi_K = k$.

We show first $\{b_i\}$ are linearly independent of K. Indeed, if not, suppose $\sum_i x_i b_i = 0$, there exists thus $a \in K$ such that $ax_i \in \mathcal{O}_K$ but not all in $\mathfrak{m}_K$. Hence $\sum_i (ax_i)b_i = 0 \Rightarrow \sum_i \overline{ax_i}\overline{b_i} = 0$ a contradiction.

For all $x \in \mathcal{O}_L$, there exist $x_{i,n} \in \mathcal{O}_K$, $x_i \in \mathcal{O}_L$ such that $x = \sum_i x_{i,0} b_i + \pi_K x_1 = \sum_i x_{i,0} b_i + \sum_i (\pi_K x_{i,1} b_i) + \pi_K^2 x_2 = \cdots$.

Thus there exists $y_n \in \mathcal{O}_K b_1 \oplus \cdots \oplus \mathcal{O}_K b_n =: \mathcal{O}'_L$ such that $x - y_n \in \pi_K^n \mathcal{O}_L$. Since $\mathcal{O}'_L$ is complete, this implies $x \in \mathcal{O}'_L$. The proposition follows. □

Remark 2.5.2. *By the proof, we see $b_1, \cdots, b_n$ form a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$ if and only if $\overline{b_1}, \cdots, \overline{b_n}$ form a basis of $\mathcal{O}_L/\varpi_K$ over k.*

Let $e \in \mathbb{Z}_{\geq 1}$ such that $\pi_K \mathcal{O}_L = \pi_L^e \mathcal{O}_L$, called the ramification index of L over K. Note that $\mathcal{O}_L/\pi_L$ is a finite extension of $\mathcal{O}_K/\pi_K$, and we put $f := [\mathcal{O}_L/\pi_L : \mathcal{O}_K/\pi_K]$. We call L/K totally ramified if $f = 1$, and L/K unramified if $e = 1$.

Proposition 2.5.3. *$fe = [L : K] = [\mathcal{O}_L : \mathcal{O}_K]$.*

Proof. We know $\mathcal{O}_L/\pi_K = \mathcal{O}_L/\pi_L^e$ is a k-vector space of dimension $[\mathcal{O}_L : \mathcal{O}_K]$. And $\mathcal{O}_L/\pi_L^e$ is isomorphic to a successive extension of $\pi_L^i\mathcal{O}_L/\pi_L^{i+1}\mathcal{O}_L \cong k_L$ for $i = 0, \cdots, e-1$. Hence $\dim_k \mathcal{O}_L/\pi_L^e = e \dim_k k_L = ef$. So $[\mathcal{O}_L : \mathcal{O}_K] = ef$. □

Lemma 2.5.4. *Let $\alpha_1, \cdots, \alpha_f \in \mathcal{O}_L$ such that $\overline{\alpha_i} \in k_L$ form a basis of k_L over k. Then $\{\alpha_i\pi_L^j \mid 1 \le i \le f, 0 \le j \le e-1\}$ form a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$.*

Proof. Using dévissage ($0 \to \mathcal{O}_L/\pi_L^{j-1} \xrightarrow{\pi_L} \mathcal{O}_L/\pi_L^j \to k_L \to 0$) and an induction argument, it is easy to see $\{\alpha_i\pi_L^j \mid 1 \le i \le f, 0 \le j \le e-1\}$ form a basis of $\mathcal{O}_L/\pi_L^e$ over k. The proposition then follows from Remark 2.5.2. □

Proposition 2.5.5. *Suppose k_L/k is separable, then there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.*

Proof. Let $\beta \in \mathcal{O}_L$ such that $k_L = k(\overline{\beta})$, then $\mathcal{O}_L$ is generated by $\{\beta^i\pi_L^j\}_{\substack{0\le i\le f-1\\ 0\le j\le e-1}}$.

Claim: There exists $\beta \in \mathcal{O}_L$ such that $k_L = k(\overline{\beta})$ and that there exists a monic polynomial $f(x) \in \mathcal{O}_K[x]$ of degree f satisfying that $f(\beta)$ is a uniformizer of $\mathcal{O}_L$.

Assume the claim, then we see $\mathcal{O}_L$ is generated by $\{\beta^i\}_{0\le i\le n-1}$. We prove the claim. First let $\beta_0 \in \mathcal{O}_L$ such that $k_L = k(\overline{\beta})$, and let $f(x)$ be the monic polynomial lifting the minimal polynomial of $\overline{\beta}$ over k. Then we have $f(\beta_0) \in \mathfrak{m}_L$. If $f(\beta_0) \in \mathfrak{m}_L/\mathfrak{m}_L^2$ then we are done with $\beta = \beta_0$. Suppose $\upsilon_L(f(\beta_0)) \ge 2$, and let π_L be an arbitrary uniniformizer of $\mathcal{O}_L$. Let $\beta_0 + \pi_L$, then using Taylor expansion, we have $f(\beta_0 + \pi_L) = f(\beta_0) + \pi_L f'(\beta_0) + \pi_L^2 b$ for some $b \in \mathcal{O}_L$. Since k_L/k is separable, $\overline{f'(\beta_0)} \ne 0$. We deduce $f(\beta_0 + \pi_L) \in \mathfrak{m}_L \setminus \mathfrak{m}_L^2$. The claim (hence the proposition) follows. □

Exercise 2.5.6. *Suppose L is totally ramified over K. Then $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Let $f(x) = x^n + \cdots + a_0$ be the minimal polynomial of π_L over $\mathcal{O}_K$. Show that $a_i \in \mathfrak{m}_K$ and $a_0 \in \mathfrak{m}_K \setminus \mathfrak{m}_K^2$ (i.e. $f(x)$ is Esenstein).*

Theorem 2.5.7. *Let k'/k be a finite separable extension.*

(1) There exists an unramified exetnsion K'/K with residue field k'. This extension is unique up to isomorphism and K'/K is Galois if and only if k'/k is Galois.

(2) For any finite extension L/K with residue field k_L. There is a natural bijection between the set of K-embeddings of K' in L and the set of k-embeddings of k' in k_L. In particular, if k'/k is Galois, then $\mathrm{Gal}(K'/K) \cong \mathrm{Gal}(k'/k)$.

Proof. (a) Let $\beta \in k'$ such that $k(\beta) = k'$, and let $f(x) \in \mathcal{O}_K[x]$ be a monic polynomial such that $\overline{f(x)} \in k[x]$ is the minimal polynomial of $\overline{\alpha}$ over k. It is clear that $f(x)$ is irreducible. Put $K' := K[x]/f(x)$. Let $\alpha \in \mathcal{O}_{K'}$ be a root of $f(x)$. Thus $\overline{f}(\overline{\alpha}) = 0$, and hence $f(K'/K) \ge \deg \overline{f(x)} = \deg f(x)$. So K'/K is unramified, and $\mathcal{O}_{K'} = \mathcal{O}_K[\alpha]$.

(b) Let L be a finite extension of K with the residue field k_L a finite extension of k'. Let $\iota : k' \hookrightarrow k_L$, and consider $f(x) \in \mathcal{O}_K[x] \hookrightarrow \mathcal{O}_L[x]$. By Hensel's lemma, there exists a unique $\gamma \in \mathcal{O}_L$ such that $f(\gamma) = 0$ and $\overline{\gamma} = \iota(\overline{\alpha})$ (where α is as in (1)). We obtain then

an embedding $\tilde{\iota} : K' \hookrightarrow L$, $\alpha \mapsto \gamma$. Conversely, an embedding $K' \hookrightarrow L$ induces $\mathcal{O}_{K'} \hookrightarrow \mathcal{O}_L$ and hence $k' \hookrightarrow k_L$. It is clear this gives an inverse of the map $\iota \mapsto \tilde{\iota}$.

The existence in (1) then follows from (a), and the uniqueness from (b). (2) also follows from (b). □

Exercise 2.5.8. *Suppose L_1, L_2 are finite unramified extensions over K (with separable extensions on residue fields), show that L_1L_2 is unramified over K.*

Let L/K be a finite extension (with k_L/k separable). By the theorem, there exists a unique subextension L_0 over K such that L_0 is unramified over K and has residue field k_L. We call L_0 the *maximal unramified extension* in L.

Exercise 2.5.9. *Let $L_1 := \mathbb{Q}_3(\sqrt{3})$, and $L_2 = \mathbb{Q}_3(\sqrt{-3})$, show that L_1L_2 is not totally ramified over $\mathbb{Q}_3$.*

2.6 Different and discriminant

Let L/K be a finite extension of complete discrete valuation fields, we keep using the notation: $(\pi_L) = \mathfrak{m}_L \subset \mathcal{O}_L \subset L$, $(\pi_K) = \mathfrak{m}_K \subset \mathcal{O}_K \subset K$, $\mathcal{O}_K/\pi_K = k$, $\mathcal{O}_L/\pi_L = k_L$, $\pi_K\mathcal{O}_L = \pi_L^e\mathcal{O}_L$, $f = [k_L : k]$. For a fractional ideal $\mathfrak{a}$ of L (i.e. a finitely generated $\mathcal{O}_L$-module of L), there exists $k \in \mathbb{Z}$ such that $\mathfrak{a} = \pi_L^k$. We define $N_{L/K}(\mathfrak{a}) := N_{L/K}(\pi_L)^k\mathcal{O}_K$. It is easy to see this definition does not depend on the choice of generators of $\mathfrak{a}$.

Lemma 2.6.1. *We have $N_{L/K}(\mathfrak{m}_L) = \pi_K^f\mathcal{O}_K$.*

Proof. Let L_0 be the maximal unramified subextension of L over K. Then $N_{L/K}(\pi_L) = N_{L_0/K} \circ N_{L/L_0}(\pi_L)$. Since L is totally ramified over L_0, we deduce by Exercise 2.5.6 that $N_{L/L_0}(\pi_L)$ is a uniformizer of L_0, denoted by π_{L_0}. Since L_0 is unramified over K, pi_K is also a uniformizer of L_0. So there exists $\alpha \in \mathcal{O}_{L_0}^\times$ such that $\pi_{L_0} = \pi_K\alpha$. Hence $N_{L/K}(\pi_L) = N_{L_0/K}(\pi_K\alpha) = \pi_K^f N_{L_0/K}(\alpha)$. Since $\alpha \in \mathcal{O}_{L_0}^\times$, $N_{L_0/K}(\alpha) \in \mathcal{O}_K^\times$ and the lemma follows. □

Lemma 2.6.2. *Let $e_1, \cdots, e_d$ be a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$, $\mathfrak{a} \subset \mathcal{O}_L$, $\alpha_1, \cdots, \alpha_d$ be a basis of $\mathfrak{a}$ over $\mathcal{O}_K$. Let $A \in M_d(K)$ such that $(\alpha_1, \cdots, \alpha_d) = (e_1, \cdots, e_d)A$, then $N_{L/K}(\mathfrak{a}) = (\det(A))$.*

Proof. The both sides of the equation is multiplicative, hence we reduce to the case where $\mathfrak{a} = \pi_L\mathcal{O}_L$. However, if $\pi_L(e_1, \cdots, e_d) = (e_1, \cdots, e_d)A$, then by definition $N_{L/K}(\pi_L) = \det(A)$. □

Now assume L/K is finite and separable. Recall the (K-bilinear) map $\langle , \rangle : L \times L \to K$, $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is non-degenerate. We define

$$\mathcal{D}_{L/K}^{-1} := \{x \in L \mid \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K, \ \forall y \in \mathcal{O}_L\}.$$

It is easy to see $\mathcal{D}_{L/K}^{-1}$ is a fractional ideal of L and contains $\mathcal{O}_L$. We call $\mathcal{D}_{L/K} := (\mathcal{D}_{L/K}^{-1})^{-1}$ the different of L over K, and $\delta_{L/K} := N_{L/K}(\mathcal{D}_{L/K})$ the discriminant of L/K. Note $\mathcal{D}_{L/K}$

is an ideal of $\mathcal{O}_L$. If $e_1, \cdots, e_n$ for a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$, and let $\{e_i^*\}$ be the dual basis with respect to $\langle , \rangle$, i.e. $\mathrm{Tr}_{L/K}(e_i^* e_j) = \delta_{ij}$. Let $A \in \mathrm{GL}_n(K)$ such that $(e_1, \cdots, e_n) = (e_1^*, \cdots, e_n^*)A$, then we have $\delta_{L/K} = (\det A)$.

Proposition 2.6.3. *Let $\mathfrak{a}$ (resp. $\mathfrak{b}$) be a fractional ideal of K (resp. L), then $\mathrm{Tr}_{L/K}(\mathfrak{b}) \subset \mathfrak{a}$ if and only if $\mathfrak{b} \subset \mathfrak{a}\mathcal{D}_{L/K}^{-1}$.*

Proof. We have

$$\mathrm{Tr}_{L/K}(\mathfrak{b}) \subset \mathfrak{a} \Leftrightarrow \mathrm{Tr}_{L/K}(\mathfrak{a}^{-1}\mathfrak{b}) \subset \mathcal{O}_K \Leftrightarrow \mathfrak{a}^{-1}\mathfrak{b} \subset \mathcal{D}_{L/K}^{-1} \Leftrightarrow \mathfrak{b} \subset \mathfrak{a}\mathcal{D}_{L/K}^{-1}.$$

□

Corollary 2.6.4. *Let $M/L/K$ be separable extensions of finite degrees. Then $\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$.*

Proof. We have

$$\mathfrak{a} \subset \mathcal{D}_{M/K}^{-1} \Leftrightarrow \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}(\mathfrak{a}) = \mathrm{Tr}_{M/K}(\mathfrak{a}) \subset \mathcal{O}_K \Leftrightarrow \mathrm{Tr}_{M/L}(\mathfrak{a}) \subset \mathcal{D}_{L/K}^{-1} \Leftrightarrow \mathfrak{a} \subset \mathcal{D}_{L/K}^{-1}\mathcal{D}_{M/L}^{-1}.$$

□

Proposition 2.6.5. *Suppose there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α over K, then $\mathcal{D}_{L/K} = (f'(\alpha))$.*

Proof. Let $\{e_i\}$ be the dual basis of $\{1, \cdots, \alpha^{n-1}\}$ with respect to $\langle , \rangle$, then we have

$$(1, \cdots, \alpha^{n-1}) = (e_1, \cdots, e_{n-1})(\mathrm{Tr}_{L/K}(\alpha^i \alpha^j))_{\substack{0 \le i \le n-1 \\ 0 \le j \le n-1}}.$$

We deduce hence $\delta_{L/K} = \det((\mathrm{Tr}_{L/K}(\alpha^i\alpha^j))) = \prod_{i \neq j}(\alpha_i - \alpha_j)$ where $\{\alpha_i\}$ are the roots of $f(x)$ (in the Galois closure of L). Since $N_{L/K}((f'(\alpha))) = (\prod_{i \neq j}(\alpha_i - \alpha_j)) = \delta_{L/K} = N_{L/K}(\mathcal{D}_{L/K})$, we see $\mathcal{D}_{L/K} = (f'(\alpha))$. □

Corollary 2.6.6. *(1) Assume L/K is totally ramified of degree e, then $\mathcal{D}_{L/K} \subset \mathfrak{m}_L^{e-1}$. Moreover the equality holds if and only if e is prime to $\mathrm{char}\, k$.*

(2) Assume k_L/k is separable. The extension L/K is unramified if and only if $\mathcal{D}_{L/K} = \mathcal{O}_L$.

Proof. (1) Since L/K is totally ramified, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Recall the minimal polynomial $f(x) = x^e + \cdots + a_0$ of π_L over K is Eisenstein. We have $f'(\pi_L) = e\pi_L^{e-1} + \cdots + a_1$ (with $a_i \in \pi_K \mathcal{O}_K$). We have $v_L(ia_i\pi_L^{i-1}) \ge e+i-1$ for $1 \le i \le e-1$ and $v_L(e\pi_L^{e-1}) = v_L(e)+e-1$. Thus $v_L(f'(\pi_L)) \ge e-1$. Moreover, we see the equality holds if and only if $v_L(e) = 0$ if and only if e is prime to $\mathrm{char}\, k$.

(2) Suppose L/K is unramified, let $\alpha \in \mathcal{O}_L$ such that $k_L = k[\overline{\alpha}]$ and let $f(x)$ be the minimal polynomial of α over $\mathcal{O}_K$. Since k_L is separable over k, $\overline{f'(\alpha)} \neq 0$. Hence $f'(\alpha) \in \mathcal{O}_L^\times$. Conversely, let L_0 be the maximal unramified subextension of L over K, then we have $\mathcal{D}_{L/K} = \mathcal{D}_{L/L_0}\mathcal{D}_{L_0/K}$. Since $\mathcal{D}_{L/L_0}$ is totally ramified and $\mathcal{D}_{L/K} = \mathcal{O}_L$, we deduce by (1) $[L : L_0] = 1$. □

Suppose $\operatorname{char} k = p$, a totally ramified extension L/K is called *tamely ramified* if $p \nmid [L : K]$ (so $G_1 = \{1\}$ and $\mathrm{Gal}(L/K)$ is cyclic) and is called *wildly ramified* if $[L : K] = p^r$ for some $r \in \mathbb{Z}_{\geq 1}$.

2.7 Ramification groups and Galois theory

Let L/K be a finite Galois extension of complete discrete valuation fields. Let $I := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) \equiv x \pmod{\mathfrak{m}_L}\}$. By restriction, we have a natural surjection: $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(L_0/K) \cong \mathrm{Gal}(k_L/k)$. It is easy to see this map coincides with the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ (induced by modulo $\mathfrak{m}_L$). The kernel of the latter map is I, hence we have $L^I = L_0$.

We assume henceforth L/K totally ramified. For $n \geq 0$, we put

$$G_n := \{\sigma \in \mathrm{Gal}(L/K) \mid \upsilon_L(\sigma(x) - x) \geq n + 1,\ \forall x \in \mathcal{O}_L\}.$$

For $\tau \in \mathrm{Gal}(L/K)$, we have

$$\upsilon_L(\tau\sigma\tau^{-1}(x) - x) = \upsilon_L(\sigma\tau^{-1}(x) - \tau^{-1}(x)).$$

Hence G_n is a normal subgroup of $\mathrm{Gal}(L/K)$. We call $\{G_n\}$ *higher ramification subgroups* of $\mathrm{Gal}(L/K)$.

Lemma 2.7.1. *Let π_L be a uniformizer of $\mathcal{O}_L$, and $\sigma \in \mathrm{Gal}(L/K)$. Then the followings are equivalent:*

(1) $\upsilon_L(\sigma(x) - x) \geq n + 1$, $\forall x \in \mathcal{O}_L$,

(2) $\upsilon_L(\sigma(\pi_L) - \pi_L) \geq n + 1$.

Proof. (1) $\Rightarrow$ (2) is clear. (2) $\Rightarrow$ (1) follows from the fact $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. □

Corollary 2.7.2. *We have*

$$G_n = \{g \in \mathrm{Gal}(L/K) \mid \frac{g(\pi_L)}{\pi_L} \in U_L^n\}.$$

We define a map

$$G_n \to U_L^n/U_L^{n+1}, g \mapsto \frac{g(\pi_L)}{\pi_L}. \tag{2.2}$$

Lemma 2.7.3. *The map (2.2) is a group homomorphism and factors through an injection $G_n/G_{n+1} \hookrightarrow U_L^n/U_L^{n+1}$. Moreover, the map is independent of the choice of π_L.*

Proof. Let $g, h \in G_n$, we have

$$\frac{gh(\pi_L)}{\pi_L} = \frac{g(h(\pi_L))}{h(\pi_L)}\frac{h(\pi_L)}{\pi_L}. \tag{2.3}$$

For another uniformizer π'_L of L, let $s \in \mathcal{O}_L^\times$ such that $h(\pi_L) = \pi_L s$. Then we have

$$\frac{g(\pi'_L)}{\pi'_L} = \frac{g(\pi_L)}{\pi_L}\frac{g(s)}{s} \in \frac{g(\pi_L)}{\pi_L} U_L^{n+1}.$$

Since $v_L(g(s)-s) \geq n+1$, we see $\frac{g(s)}{s}$, thus $\frac{g(\pi'_L)}{\pi'_L} \in \frac{g(\pi_L)}{\pi_L} U_L^{n+1}$. Applying this to $\pi'_L = h(\pi_L)$ (in (2.3)), we see $\frac{gh(\pi_L)}{\pi_L} \equiv \frac{g(\pi_L)}{\pi_L}\frac{h(\pi_L)}{\pi_L} \pmod{U_L^{n+1}}$. The lemma follows. □

By the lemma and Proposition 2.3.15 (3), we have:

Proposition 2.7.4. *(1) If* $\operatorname{char} k = 0$*, then* $G_1 = \{1\}$*, and* G_0 *is a finite abelian group.*

(2) If $\operatorname{char} k = p$*, then* G_1 *is a finite group of* p*-power order, and* G_0/G_1 *is a cyclic group of order prime to* p*.*

Exercise 2.7.5. *Let* $n \geq 1$*, calculate the higher ramification groups of* $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$ *(where* ζ_{p^n} *is a primitive* p^n*-th root of unity).*

Infinite Galois theory

Definition 2.7.6. *A profinite group* G *is a topological group that is an inverse limit of finite groups, each equipped with the discrete topology:* $G \cong \varprojlim_{i\in I} G_i$ *(for an inverse system of finite groups* $(\{G_i\}_{i\in I}, \{f_{ij}\}_{i\geq j})$*:* I *is a directed set,* $f_{ij} : G_i \to G_j$ *for* $i \geq j$ *satisfies* $f_{ii} = \mathrm{id}$*, and* $f_{ik} = f_{jk} \circ f_{ij}$ *if* $i \geq j \geq k$*).*

Example 2.7.7. *A discrete valuation ring with finite residue field is a profinite group.*

Proposition 2.7.8. *A profinite group is totally disconnected, compact and Hausdorff.*

Proof. Let $G \cong \varprojlim_{i\in I} G_i$. Since G_i is compact, so is $\prod_i G_i$. We show G is closed in $\prod_i G_i$. Let $x = (x_i) \in \prod_i G_i \setminus \varprojlim_n G_i$. By definition, there exist $j > k$ such that $f_{jk}(x_j) \neq x_k$. Consider the open subset $U = \{x_j\} \times \{x_k\} \times \prod_{i\neq j,k} G_i \subset \prod_i G_i$. It is clear that $U \cap G = \emptyset$, so G is closed in $\prod_i G_i$ and hence also compact. Suppose $V \subset G$ is a connected component, and $(x_i) \neq (y_i) \in G$. Then there exists j such that $x_j \neq y_j$. Then we see $V = (V \cap ((G_j \setminus \{y_j\}) \times \prod_{i\neq j} G_i)) \cup (V \cap (\{y_j\} \times \prod_{i\neq j} G_i))$, a contradiction. From the proof, we also see G is Hausdorff. □

Remark 2.7.9. *The converse of the proposition is also true, see for example*

Corollary 2.7.10. *For a subgroup* H *of a profinite group* G*,* H *is open if and only if* H *is closed of finite index.*

We briefly discuss infinite Galois theory.

Lemma 2.7.11. *Let* L/K *be a Galois extension (not necessarily finite),* $G := \mathrm{Gal}(L/K)$*. If* F/K *is a normal subextension of* L/K*, then* $H = \mathrm{Gal}(L/F)$ *is a nomral subgroup of* G *and* $F = L^H$*. And we have an exact sequence* $1 \to \mathrm{Gal}(L/F) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K) \to 1$*.*

Proof. Since F/K is normal, we have a natural morphism

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K) \tag{2.4}$$

and let H be its kernel.

Claim: The map (2.4) is surjective.

Let F' be a normal extension over K such that $F \subset F' \subset L$ and F' is a finite extension of F. We show first $\mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K)$ is surjective. Suppose $F' = F(\alpha)$, and let F'_0 be the splitting filed of $K(\alpha)$, $F_0 := F'_0 \cap F$ (the both being finite Galois extensions over K). For $\sigma \in \mathrm{Gal}(F/K)$, by Galois theory for finte extensions, there exists $\tau \in \mathrm{Gal}(F'_0/K)$ such that $\tau|_{F_0} = \sigma|_{F_0}$. Then $\tilde{\sigma} : F(\alpha) \to F(\alpha), x\alpha^i \mapsto \sigma(x)\tau(\alpha)$ defines a lifting of σ in $\mathrm{Gal}(F'/F)$. Indeed, to see $\tilde{\sigma}$ is a well-defined map (namely if $\sum x_i\alpha^i = \sum y_i\alpha^i$, then $\sum \sigma(x_i)\tau(\alpha)^i = \sum \sigma(y_i)\tau(\alpha)^i$) and gives an isomorphism, one can reduce to show these hold with F replaced by any sufficiently large finite Galois subextensions $F_i \supset F_0$ of F over K. But for finte extensions, these follow from the standard Galois theory. Now let J be the set consisting of normal subextensions F' of L over K and $\sigma' \in \mathrm{Gal}(F'/K)$ such that $F' \supset F$ and $\sigma'|_F = \sigma$. Then J is equipped with a natural partial order: $(F', \sigma') \leq (F'', \sigma'')$ if $F' \subset F''$ and $\sigma''_{F'} = \sigma'$. Then it is clear that any non-empty chain in J has an upper bound (given by taking union). By Zorn's lemma, J has a maximal element L'. However, since $\mathrm{Gal}(L''/K) \to \mathrm{Gal}(L'/K)$ is surjective (as shown above) for any finite normal extension L'' of L, we see L' has to be L.

Finally we show $L^{\mathrm{Gal}(L/F)} = F$. Suppose there exists $\alpha \in L^{\mathrm{Gal}(L/F)}$ such that $\alpha \notin F$. Let $E \subset L$ be the splitting field of α over F, and let α' be a conjugate of α in E. There exists $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(\alpha) = \alpha'$. By the above claim, σ can lift to an element in $\mathrm{Gal}(L/F) = H$. However, α is fixed by $\mathrm{Gal}(L/F)$ a contradiction. So we have $L^{\mathrm{Gal}(L/F)} = F$. □

We equip $\mathrm{Gal}(L/K)$ with the topology such that all cosets of $\mathrm{Gal}(L/F)$ with F finite normal over K form a topological basis. This is referred to as the Krull topology on $\mathrm{Gal}(L/K)$.

Theorem 2.7.12. *(1) We have* $\mathrm{Gal}(L/K) \cong \varprojlim_F \mathrm{Gal}(F/K)$ *where* F *runs though finite normal extensions of* K *in* L.

(2) The maps $F \mapsto \mathrm{Gal}(L/F)$ *and* $H \mapsto L^H$ *define a bijection between subextensions* F/K *of* L/K *and closed subgroups* H *of* $\mathrm{Gal}(L/K)$.

Proof. By the above lemma, we have a natural map $\mathrm{Gal}(L/K) \to \varprojlim_F \mathrm{Gal}(F/K)$ such that for each F, the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ is surjective. We deduce hence the map itself is surjective. We also see the kernel is $\cap_F \mathrm{Gal}(L/F) = \mathrm{Gal}(L/\cup_F F) = 1$ since $\cup F = L$. Finally, it is easy to verify the Krull topology on $\mathrm{Gal}(L/K)$ coincides with the inverse limit topology on $\varprojlim_F \mathrm{Gal}(F/K)$.

Let F/K be a subextension of L/K, and write $F = \cup F_i$ with F_i finite over F. It is easy to see $\mathrm{Gal}(L/F) = \cap_i \mathrm{Gal}(L/F_i)$. Let E_i be the Galois closure of F_i over K. Then $\mathrm{Gal}(L/E_i)$ is a closed (and open) subgroup of $\mathrm{Gal}(L/K)$. Since $\mathrm{Gal}(L/E_i)$ has finite

index in $\mathrm{Gal}(L/F_i)$, we see $\mathrm{Gal}(L/F_i)$ is a finite union of $g\,\mathrm{Gal}(L/E_i)$ for finitely many g, and hence is also a closed subgroup of $\mathrm{Gal}(L/K)$. Thus $\mathrm{Gal}(L/F) = \cap_i \mathrm{Gal}(L/F_i)$ is a closed subgroup of $\mathrm{Gal}(L/K)$. The same argument as in the proof of Lemma 2.7.11 shows $L^{\mathrm{Gal}(L/F)} = F$.

Now let H be a closed subgroup of $\mathrm{Gal}(L/K)$. For a finite Galois extension F over K in L, let H_F be the image of H in $\mathrm{Gal}(F/K)$ via $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(F/K)$. Let $\tilde{H}_F \supset H$ be the preimage of H_F in $\mathrm{Gal}(L/K)$. We claim $\cap \tilde{H}_F = H$. Indeed, otherwise, there exists $\sigma = (\sigma_F) \in \cap \tilde{H}_F \backslash H$ and an open subgroup U such that $\sigma U \cap H =$. Shrinking U, we can and so assume $U \cong \mathrm{Gal}(L/F')$ for some finite Galois extension F' over K. Since $\sigma U \cap H = \emptyset$, we see $\sigma|_{\mathrm{Gal}(F'/K)} \notin H_{F'}$, however $\sigma \in \tilde{H}_{F'}$, a contradiction. Now let $F_H := F^{H_F}$, and L_H be the subextension generated by $\{F_H\}_F$. We have $H_F \cong \mathrm{Gal}(F/F_H)$ and $\tilde{H}_F \cong \mathrm{Gal}(F/F_H)$. So $\mathrm{Gal}(L/L_H) \cong \cap \tilde{H}_F \cong H$.

□

Local class field theory (rough statement)

Put $\mathrm{Gal}(L/K)^{\mathrm{ab}}$ to be the maximal abelian quotient of $\mathrm{Gal}(L/K)$, and $L^{\mathrm{ab}} = L^{\mathrm{Gal}(L/K)^{\mathrm{ab}}}$, that is the maximal abelian subextension of K in L (noting the composition of abelian extensions are abelian). We have $\mathrm{Gal}(L^{\mathrm{ab}}/K) \cong \mathrm{Gal}(L/K)^{\mathrm{ab}}$. We can now state (a not-so-precise version of) the local class field theory for finite extensions of $\mathbb{Q}_p$:

Theorem 2.7.13. *Let K be a finite extension of $\mathbb{Q}_p$, then there exists a canonical continuous injection $K^\times \hookrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$, and the image is dense.*

The map is called local reciprocity map. There are many features that characterize the local reciprocity map in a unqiue way. However, we won't discuss these in the note. Recall we have a canonical exact sequence $1 \to \mathcal{O}_K^\times \to K^\times \to \mathbb{Z} \to 0$, and the quotient $\mathbb{Z}$ corresponds, via the local reciprocity map, to unramified extensions of K in the following way

$$\begin{array}{ccc} K^\times & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathrm{Gal}(K^{\mathrm{unr}}/K) \end{array}$$

where K^{unr}/K denotes the maximal unramified extension over K, and the bottom map sends 1 to a Frobenius element (that is a topological generator) in $\mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \mathrm{Gal}(\overline{k}/k) \cong \widehat{\mathbb{Z}}$. By a chocie of uniformizer π_K, we have an exact sequence $0 \to \mathbb{Z} \xrightarrow{1 \mapsto \pi_K} K^\times \to \mathcal{O}_K^\times \to 1$. By the local reciprocity map, then there should exist an abelian extension K_{π_K} of K such that K_{π_K} is disjoint from K^{unr} (so K_{π_K} is totally ramified), and that $\mathrm{Gal}(K_{\pi_K}/K) \cong \mathcal{O}_K^\times$. The extension K_{π_K} can be explicitly constructed by the theory of Lubin-Tate formal groups. We end the discussion by the following exercise (as a special case of K_{π_K}).

Exercise 2.7.14. *Let $\mathbb{Q}_p(\zeta_{p^\infty}) := \cup_n \mathbb{Q}_p(\zeta_{p^n})$ where ζ_{p^n} is a primitive p^n-th root of unity. Prove the following map is an isomorphism*

$$\mathbb{Z}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p), a \mapsto [\zeta_{p^n} \mapsto \zeta_{p^n}^{\overline{a}_n}],$$

where $\overline{a}_n \in (\mathbb{Z}_p/p^n)^\times$ denotes the reduction of a.

The Fontaine ring R (a glance)

Let $R := \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbb{C}_p}$.

Lemma 2.7.15. *The map $R \to \varprojlim_{x\mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/p$, $(x^{(n)}) \mapsto \left(\overline{x^{(n)}}\right)$ is bijective.*

Proof. We construct an inverse of the map. Let $(x_n) \in \varprojlim_{x\mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/p$, and for each n, let $\widetilde{x}_n$ be a lifting of x_n in $\mathcal{O}_{\mathbb{C}_p}$. Put $x^{(n)} := \lim_{m\to+\infty} \widetilde{x}_{n+m}^{p^m}$ (Exercise: show that $\{\widetilde{x}_{n+m}^{p^m}\}$ converges). Then one can check $(x^{(n)}) \in R$, and is sent to (x_n). □

The ring structure on $\mathcal{O}_{\mathbb{C}_p}$ induces a ring structure on $\varprojlim_{x\mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/p \cong R$.

Exercise 2.7.16. *(1) Show that the map $\upsilon_R : R \to \mathcal{O}_{\mathbb{C}_p} \xrightarrow{\mathrm{val}_p} \mathbb{Q} \cup \{+\infty\}$, $(x^{(n)}) \mapsto x^{(0)} \mapsto \mathrm{val}_p(x^{(0)})$ defines an additive valuation on R.*

(2) Show that R is a domain.

One can show that R is complete for the valuation υ_R. Consider the fractional field $\mathrm{Fr}\, R$ of R. One can show that $\mathrm{Fr}\, R$ is algebraically closed, complete for υ_R, and is of characteristic p. It is clear that $\epsilon := (\zeta_{p^n}) \in R$, and put $\pi = \epsilon - 1$. A direct calculation shows $\upsilon_R(\pi) = \frac{1}{(p-1)}$. We have thus $\mathbb{F}_p[[\pi]] \hookrightarrow R$, and hence $\mathbb{F}_p((\pi)) \hookrightarrow \mathrm{Fr}\, R$. The $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-action on $\mathcal{O}_{\mathbb{C}_p}$ induces a $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-action on R (and hence on $\mathrm{Fr}\, R$). Let $\mathbb{Q}_{p,\infty} := \cup \mathbb{Q}_p(\zeta_{p^n})$, then we see π is fixed by $H_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_{p,\infty})$.

Theorem 2.7.17 ((Fontaine-Wintenberger))**.** *One has $\widehat{\overline{\mathbb{F}_p((\pi))}} \xrightarrow{\sim} \mathrm{Fr}\, R$. The $H_{\mathbb{Q}_p}$-action on $\mathrm{Fr}\, R$ induces an isomorphism*

$$H_{\mathbb{Q}_p} \cong \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_{p,\infty}) \xrightarrow{\sim} \mathrm{Gal}\left(\mathbb{F}_p((\pi))^s/\mathbb{F}_p((\pi))\right)$$

where $\mathbb{F}_p((\pi))^s$ denotes the separable closure of $\mathbb{F}_p((\pi))$ (in $\mathrm{Fr}\, R$).

2.8 Places of number fields

Let K be a number field.

Archimedean places: We let $S_\infty := \Sigma_\infty/\sim$, where $\sigma \sim \sigma'$ if $\sigma' = \overline{\sigma} : K \hookrightarrow \mathbb{C}$. For each embedding $\sigma : K \hookrightarrow \mathbb{C}$, we get a (archimedean) norm $|\cdot|_\sigma : K \to \mathbb{R}_{\geq 0}$, $x \mapsto |\sigma(x)|$ which only depends on the conjugate class of σ.

Non-archimedean places: Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. For $x \in K$, we define $\upsilon_\mathfrak{p} : K \to \mathbb{Z} \cup \{+\infty\}$ such that $(x) = \mathfrak{p}^{\upsilon_\mathfrak{p}}\mathfrak{a}$ with $\mathfrak{a}$ a fractional ideal that does not have $\mathfrak{p}$-factor and $\upsilon_\mathfrak{p}(0) = +\infty$. One can show this is an additive valuation (exercise). Put $|\cdot|_\mathfrak{p} : K \to \mathbb{R}_{\geq 0}$, $x \mapsto N(\mathfrak{p})^{-\upsilon_\mathfrak{p}(x)}$ (recall $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$), that is thus a non-archimedean norm on K. By definition, the valuation ring of $|\cdot|_\mathfrak{p}$ (in K) is the localization $\mathcal{O}_{K,\mathfrak{p}}$ of $\mathcal{O}_K$

at $\mathfrak{p}$. Let $K_\mathfrak{p}$ be the completion of K with respect to $|\cdot|_\mathfrak{p}$, $\mathcal{O}_{K_\mathfrak{p}}$ the valuation ring of $K_\mathfrak{p}$. Let $\pi_\mathfrak{p} \in \mathfrak{p} \setminus \mathfrak{p}^2$. Thus $\mathcal{O}_{K_\mathfrak{p}} \cong \varprojlim_n \mathcal{O}_{K,\mathfrak{p}}/\pi_\mathfrak{p}^n \cong \varprojlim_n \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}^n \cong \varprojlim_n \mathcal{O}_K/\mathfrak{p}^n$. Indeed, the second isomorphism follows from the fact $\mathcal{O}_{K,\mathfrak{p}}$ is a discrete valuation ring hence a PID. For the third isomorphism, consider the natural morphism $\mathcal{O}_K/\mathfrak{p}^n \to \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}^n$. We prove this map is bijective. To see it is injective, let $x \in \mathcal{O}_K \cap (\mathfrak{p}^n\mathcal{O}_{K,\mathfrak{p}})$, by definition there exists $y \in \mathcal{O}_K \setminus \mathfrak{p}$ such that $xy \in \mathfrak{p}^n\mathcal{O}_K$. Using prime decomposition, we see $x \in \mathfrak{p}^n\mathcal{O}_K$. To see it is surjective, let $x \in \mathcal{O}_{K,\mathfrak{p}}$, there exists $y\mathcal{O}_K \setminus \mathfrak{p}$ such that $xy \in \mathcal{O}_K$. Let $z \in \mathcal{O}_K$ such that $zy \equiv 1 \pmod{\mathfrak{p}^n}$. Then $xyz \equiv x \pmod{\mathfrak{p}^n}$. Thus the residue field of $\mathcal{O}_{K_\mathfrak{p}}$ is just the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$.

An element in the set $S_\infty \cup \{\text{prime ideals of } \mathcal{O}_K\}$ is called a place of K.

Theorem 2.8.1. *(1) Any two of the absolute valuations $|\cdot|_v$ for places v of K are not equivalent to each other.*

(2) Any absolute value of K is equivalent to $|\cdot|_v$ for some place v of K.

Proof. (1) If v_1 is an archimedean norm, and v_2 is a non-archimedean norm. Then there exist non-zero $x, y \in K$ such that $|x+y|_{v_1} > \max\{|x|_{v_1}, |y|_{v_1}\}$, hence $|(x+y)/x|_{v_1} > 1$ and $|(x+y)/y|_{v_1} > 1$. However, since v_2 is non-archimedean, $|(x+y)/x|_{v_2} \leq 1$ or $|(x+y)/y|_{v_2} \leq 1$. So they are not equivalent.

Let $\mathfrak{p}_1 \neq \mathfrak{p}_2$ be two prime ideals of $\mathcal{O}_K$, then by Chinese reminder theorem, there exists $x \in \mathfrak{p}_1$ and $x \notin \mathfrak{p}_2$. We see $|x|_{\mathfrak{p}_1} < 1$ and $|x|_{\mathfrak{p}_2} = 1$, so $|\cdot|_{\mathfrak{p}_1} \nsim |\cdot|_{\mathfrak{p}_2}$.

Let $\{\sigma_1, \cdots, \sigma_r\}$ be the set of real emeddings of K, $\{\sigma_{r+1}, \cdots \sigma_{r+s}, \overline{\sigma}_{r+1}, \cdots, \overline{\sigma}_{r+s}\}$ be the set of non-real embeddings of K. We identify S_∞ with the set $\{\sigma_1, \cdots, \sigma_{r+s}\}$. Consider the embedding $K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s (\cong K_\mathbb{R})$, $x \mapsto (\sigma_1(x), \cdots, \sigma_{r+s}(x))$. Recall $\mathcal{O}_K$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$ via the embedding. Hence K is dense in $\mathbb{R}^r \times \mathbb{C}^s$. For any σ_i, there exists thus $x \in K$ such that $|x|_{\sigma_i} > 1$ and $|x|_{\sigma_j} < 1$ for $j \neq i$. This implies that $|\cdot|_{\sigma_i} \nsim |\cdot|_{\sigma_j}$ for $i \neq j$.

(2) If $|\cdot|$ is non-archimedean, $|\cdot|\big|_\mathbb{Q}$ is non-archimedean. Thus $|x| \leq 1$ for all $x \in \mathbb{Z}$. For any $y \in \mathcal{O}_K$, y is integral over $\mathbb{Z}$. Hence $|y| \leq 1$. Consdier $\{y \in \mathcal{O}_K \mid |y| < 1\}$. One check by definition this is a prime ideal, denoted by $\mathfrak{p}$, of $\mathcal{O}_K$. One sees the localization $\mathcal{O}_{K,\mathfrak{p}} \subset \{x \in K \mid |x| \leq 1\}$. Conversely, for any $0 \neq x \in K$, $|x| \leq 1$, consider the prime factorization $(x) = \mathfrak{p}^{e_\mathfrak{p}} \prod_{\mathfrak{p}' \neq \mathfrak{p}} (\mathfrak{p}')^{e_{\mathfrak{p}'}}$. We claim $e_\mathfrak{p} \geq 0$. Indeed, suppose $e_\mathfrak{p} < 0$, there exists $0 \neq y \in \mathfrak{p}^{-e_\mathfrak{p}}$ such that $(xy) = \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{m_\mathfrak{q}}$. There exists $z \in \mathcal{O}_K \setminus \mathfrak{p}$ such that $xyz \in \mathcal{O}_K \setminus \mathfrak{p}$. We see $|xyz| = 1$, $|yz| < 1$ and hence $|x| > 1$, a contradiction. Since $|\cdot|_\mathfrak{p}$ and $|\cdot|$ have the same valuation ring $\mathcal{O}_{K,\mathfrak{p}}$, they are equivalent.

Suppose now $|\cdot|$ is archimedean, and let $\widehat{K}$ be the completion of K via $|\cdot|$. Consider the closure $\widehat{\mathbb{Q}}$ of $\mathbb{Q}$ in $\widehat{K}$, that is the same as the completion of $\mathbb{Q}$ via $|\cdot|_\mathbb{Q}$. Since $|\cdot|_\mathbb{Q}$ is a archimedean hence is equivalent to the standard absolute value by Ostrouski's theorem, $\widehat{\mathbb{Q}} \cong \mathbb{R}$. Let $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.Consider $\widehat{\mathbb{Q}}(\alpha)$ that is a finite extension of $\widehat{\mathbb{Q}}$. We see by Lemma 2.4.6 that $\widehat{\mathbb{Q}}(\alpha)$ is also complete for $|\cdot|$. Hence $\widehat{\mathbb{Q}}(\alpha)$ is closed in $\widehat{K}$ and contains K. Since K is dense in $\widehat{K}$, $\widehat{K} = \widehat{\mathbb{Q}}(\alpha) = \mathbb{R}$ or $\mathbb{C}$. Let σ denote the tautological embedding $\sigma : K \hookrightarrow \widehat{K} \to \mathbb{C}$. It suffices to show $|\cdot|_{\widehat{K}}$ is equivalent to the standard absolute value. If $K = \mathbb{R} = \widehat{\mathbb{Q}}$, it follows from Ostrouski's theorem. Assume $K = \mathbb{C}$, modifying $|\cdot|$,

we can and do assume $|\cdot|\big|_{\mathbb{R}}$ is equal to the standard absolute value $\|\cdot\|$. We show $|\cdot| = \|\cdot\|$ on $\mathbb{C}$. Let $z = ru = re^{i\theta}$, we only need to show $|u| = 1$. Let $u_n = x_n + y_n i$ be a sequence of roots of unity for $\|\cdot\|$ such that $u_n \to u$ and such that x_n, y_n are Cauchy sequences for $\|\cdot\|$ hence also for $|\cdot|$. We deduce u_n is also a Cauchy sequence for $|\cdot|$. Since $u_n^N = 1$, we have $|u_n| = 1$ and hence $|u| = 1$. This concludes the proof. □

Proposition 2.8.2. *Let $S = \{v_1, \cdots, v_r\}$ be a finite set of places of K. Then the image of the diagonal map $K \hookrightarrow \prod_{v_i \in S} K_{v_i}$ is dense.*

Proof. We need to show for any $(z_i) \in \prod K_{v_i}$, and any $\epsilon > 0$, there exists $z \in K$ such that $|z - z_i|_{v_i} \leq \epsilon$. Since K is dense in K_{v_i} for all v_i, we can and do assume $z_i \in K$ for all i. Let $z := \sum_{i=1}^r x_i z_i \in K$, so $z - z_i = (1 - x_i)z_i + \sum_{j \neq i} x_j z_j$. We reduce to show that for i, and for any $\epsilon > 0$, there exist$x_i \in K$ such that

$$|x_i - 1|_{v_i} < \epsilon \text{ and } |x_i|_{v_j} < \epsilon \text{ for } j \neq i. \tag{2.5}$$

Claim: There exists $y_i \in K$ such that $|y_i|_{v_i} \geq 1$ and $|y_i|_j < 1$.

Assume the claim, then $\left|\frac{y_i^n}{1+y_i^n}\right|_{v_i} \to 1$ (for odd n, and replacing y_i by $-y_i$ if necessary) and $\left|\frac{y_i^n}{1+y_i^n}\right|_{v_j} \to 0$. Let $x_i := \frac{y_i^N}{1+y_i^N}$ for $N \gg 0$, then (2.5) holds.

Now we prove the claim. We use induction on $|S|$. If $|S| = 2$, the claim follows easily from the fact $|\cdot|_{v_1} \nsim |\cdot|_{v_2}$. Suppose the claim holds for $|S| < d$. Now suppose $|S| = d$, without lost of generality, let $i = 1$. By the induction hypothesis, there exists $y \in K$ such that $|y|_{v_1} \geq 1$ and $|y|_{v_i} < 1$ for $2 \leq i \leq d-1$. If $|y|_{v_d} < 1$, then we are done. Suppose $|y|_{v_d} \geq 1$. Let $\alpha \in K$ such that $|\alpha|_{v_1} \geq 1$ and $|\alpha|_{v_d} < 1$. If $|y|_{v_d} = 1$, then put $y_1 := \alpha y^N$ with N sufficiently large; if $|y|_{v_d} > 1$, then put $y_1 := \frac{\alpha y^N}{1+y^N}$ with N odd sufficiently large (replacing y by $-y$ if necessary). The claim follows. □

Exercise 2.8.3. *Let $S = \{v_1, \cdots, v_r\}$ be a finite set of finite places of K, prove that the image of the diagonal map $\mathcal{O}_K \hookrightarrow \prod_{v_i \in S} \mathcal{O}_{K_{v_i}}$ is dense.*

Now let L/K be a finite extension, and w be a place of L. The restriction $|\cdot|_w$ on K then corresponds to a place v of K. We write $w|v$ for this relation. Let K_v be the closure of K in L_w, that is also isomoprhic to the completion of K at v. We have that L_w is a finite extension of K_v. Indeed, let $\alpha \in L \hookrightarrow L_w$ such that $L = K(\alpha)$, and consider the subextension $K_v(\alpha) \subset L_w$. Since α is algebraic over K hence over K_v, $K_v(\alpha)$ is a finite extension of K_v and thus is complete and closed in L_w. Also the embedding $L \hookrightarrow L_w$ factors through $K_v(\alpha)$. Since L is dense in L_w, we see $K_v(\alpha) = L_w$.

If w is archimedean, then either $L_w = K_v$ or $L_w = \mathbb{C}$ and $K_v = \mathbb{R}$. Suppose w is non-archimedean, let $\mathfrak{P}_w \subset \mathcal{O}_L$ be the prime ideal corresponding to w. Then the place v of K is also non-archimedean, and we let $\mathfrak{p}_v$ denote the corresponding prime ideal. We have thus

$$\mathfrak{p}_v = \{x \in \mathcal{O}_K \mid |x|_v < 1\} = \{x \in \mathcal{O}_K \mid |x|_w < 1\} = \mathfrak{P}_w \cap \mathcal{O}_K.$$

Lemma 2.8.4. *We have $e(\mathfrak{P}_w/\mathfrak{p}_v) = e(L_w/K_v) =: e(w/v)$ and $f(\mathfrak{P}_w/\mathfrak{p}_v) = f(L_w/K_v) =: f(w/v)$.*

Proof. Let $\pi_v \in \mathfrak{p}_v \setminus \mathfrak{p}_v^2$, $\pi_w \in \mathfrak{P}_w \setminus \mathfrak{P}_w^2$. Then π_v (resp. π_w) is a uniformizer of $\mathcal{O}_{K_v}$ (resp. $\mathcal{O}_{L_w}$). By prime factorization, we deduce $\pi_v/\pi_w^{e(\mathfrak{P}_w/\mathfrak{p}_v)} \in \mathcal{O}_{L,\mathfrak{P}}^\times$. Hence $e(L_w/K_v) = \upsilon_w(\pi_v) = e(\mathfrak{P}_w/\mathfrak{p}_v)$. We also have $\mathcal{O}_K/\pi_v \cong \mathcal{O}_{K_v}/\pi_v$ and $\mathcal{O}_L/\pi_w \cong \mathcal{O}_{L_w}/\pi_w$. The second equality follows. □

Proposition 2.8.5. *The morphism $\iota : K_v \otimes_K L \to \prod_{w|v} L_w$, $x \otimes y \mapsto (xy)_w$ is an isomorphism of K_v-algebras.*

Proof. It is clear $\operatorname{Im}\iota$ is a finite dimensional K_v-vector subspace, hence is complete and closed in $\prod_{w|v} L_w$. Consider the map $L \to \prod_{w|v} L_w$, we know this map has dense image. Hence $\operatorname{Im}\iota = \prod_{w|v} L_w$. Since

$$\dim_{K_v} \prod_{w|v} L_w = \sum_{w|v} e(w|v)f(w/v) = \sum_{w|v} e(\mathfrak{P}_w/\mathfrak{p}_v)f(\mathfrak{P}_w/\mathfrak{p}_v) = [L:K],$$

we see f is bijective. □

Remark 2.8.6. *(1) Note that the map ι is a homemorphism if we equip $K_v \otimes_K L$ with a norm (compatible with $|\cdot|_v$ on K_v).*

(2) Let $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x)$ be the minimal polynomial of α over K. Then we have $K_v \otimes_K L \cong K_v \otimes_K K[x]/f(x) \cong K_v[x]/f(x)$. Suppose $f(x) = \prod_{i=1}^r f_i(x) \in K_v[x]$. We have thus $K_v \otimes_K L \cong \prod_{i=1}^r K_v[x]/f_i(x)$. In particular, we see there is a bijection $\{w|v\} \leftrightarrow \{f_i(x)\}$.

(3) The statement in the proposition also holds when v is an archimedean place of K. Actually, by the same argument in the proof, we see ι is injective. It suffices to show $\dim_{K_v} \prod_{w|v} L_w = [L:K]$. However, let $\sigma_K : K \to \mathbb{C}$ be an embedding corresponding to v, then one can check that $\dim_{K_v} \prod_{w|v} L_w = |\{\sigma : L \hookrightarrow \mathbb{C} \mid \sigma|_K = \sigma_K\}$ and hence is equal to $[L:K]$.

Corollary 2.8.7. *Let $x \in K_v \otimes_K L$, and $(x_w)_{w|v} = \iota(x)$. Then*

$$\operatorname{Tr}_{K_v \otimes_K L/K_v}(x) = \sum_{w|v} \operatorname{Tr}_{L_w/K_v}(x_w) \tag{2.6}$$

$$N_{K_v \otimes_K L/K_v}(x) = \prod_{w|v} N_{L_w/K_v}(x_w). \tag{2.7}$$

Proposition 2.8.8. *Let $e_1, \cdots, e_d$ be a basis of L/K. For a non-archimedean place v of K, let M_v be the free $\mathcal{O}_{K_v}$-submodule of $K_v \otimes_K L$ generated by $e_1, \cdots, e_d$. Then for all but finitely many places v, the isomorphism ι induces an isomorphism $M_v \xrightarrow{\sim} \prod_{w|v} \mathcal{O}_{L_w}$.*

Proof. Let $\alpha \in K^\times$ such that $\alpha e_1, \cdots, \alpha e_d \in \mathcal{O}_L$. If $|\alpha|_v = 1$ (note this hods for all but finitely many v), then $M_v \cong \mathcal{O}_{K_v}(\alpha e_1) \oplus \cdots \oplus \mathcal{O}_{K_v}(\alpha e_d)$. We reduce then to the case

$e_1, \cdots, e_d \in \mathcal{O}_L$, then ι induces an injection $M_v \hookrightarrow \prod_{w|v} \mathcal{O}_{L_w}$. Let $e_1^*, \cdots, e_d^* \in L$ be the dual basis of $e_1, \cdots, e_d$ with respect to the perfect pairing $L \times L \to K$. By tensoring with K_v, this perfect pairing induces a perfect pairing of K_v-vector spaces:

$$K_v \otimes_K L \times K_v \otimes_K L \longrightarrow K_v, \ (x, y) \mapsto \mathrm{Tr}_{K_v \otimes_K L / K_v}(xy).$$

Let M_v^* be the $\mathcal{O}_{K_v}$-submodule of $K_v \otimes_K L$ generated by $e_1^*, \cdots, e_d^*$. By the above corollary, this pairing is compatible with:

$$\prod_{w|v} L_w \times \prod_{w|v} L_w \to K_v, ((x_w), (y_w)) \mapsto \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(x_w y_w), \tag{2.8}$$

so in particular, $e_1^*, \cdots, e_d^*$ are dual basis of $e_1, \cdots, e_d$ with respect to (2.8). Since $M_v \subset \prod_{w|v} \mathcal{O}_{L_w}$, $\prod_{w|v} \mathcal{O}_{L_w} \subset M_v^*$. In summary, we have $M_v \subset \prod_{w|v} \mathcal{O}_{L_w} \subset M_v^*$. Consider

$$M := \mathcal{O}_K e_1 \oplus \cdots \oplus \mathcal{O}_K e_d \subset \mathcal{O}_L \subset \mathcal{O}_K e_1^* \oplus \cdots \oplus \mathcal{O}_K e_d^*.$$

There exists $\alpha \in K^\times$ such that $\alpha M^* \subset M$. For a finite place v, if $|\alpha|_v = 1$, then $\alpha \in \mathcal{O}_{K_v}$ and hence $M_v = M_v^*$ and $\iota : M_v \xrightarrow{\sim} \prod_{w|v} \mathcal{O}_{L_w}$. □

Let

$$\mathcal{D}_{L/K}^{-1} = \{x \in L \mid \ \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K, \ \forall y \in \mathcal{O}_L\}.$$

Then $\mathcal{D}_{L/K}^{-1}$ is a fractional ideal in L. Indeed, it is clear that $\mathcal{D}_{L/K}^{-1} \supset \mathcal{O}_L$ is an $\mathcal{O}_L$-module; let $e_1, \cdots, e_d \in \mathcal{O}_L$ be a basis of L over K, and e_i^* be the dual basis with respect to the perfect pairing $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$, then $\mathcal{D}_{L/K}^{-1} \subset \mathcal{O}_K e_1^* \oplus \cdots \mathcal{O}_K e_d^*$ and hence is a finitely generated $\mathcal{O}_L$-module. Put $\mathcal{D}_{L/K} := (\mathcal{D}_{L/K}^{-1})^{-1}$, called the different of L/K.

Proposition 2.8.9. *We have* $\mathcal{D}_{L/K} = \prod_w (\mathcal{D}_{L_w/K_v} \cap \mathcal{O}_L)$.

Proof. For a finite place w of L, and a fractional ideal I in L , denote by $\upsilon_w(I) \in \mathbb{Z}$ the exponent of $\mathfrak{P}_w$ in the prime factorization of I. For a fractional ideal $I_w \subset L_w$, denote by $\upsilon_w(I_w) \in \mathbb{Z}$ such that $I_w = (\pi_w)^{\upsilon_w(I_w)}$. The statement in proposition is equivalent to $\upsilon_w(\mathcal{D}_{L/K}) = \upsilon_w(\mathcal{D}_{L_w/K_v})$, that is then equivalent to $\upsilon_w(\mathcal{D}_{L/K}^{-1}) = \upsilon_w(\mathcal{D}_{L_w/K_v}^{-1})$ for all finite places w.

Let $x \in \mathcal{D}_{L/K}^{-1}$, and v be a finite place of K. By definition and (2.6), $\sum_{w|v} \mathrm{Tr}_{L_w/K_v}(xy) = \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K$ for all $y \in \mathcal{O}_L$. Since $\mathcal{O}_L$ is dense in $\prod_{w|v} \mathcal{O}_{L_w}$, for any $(y_w) \in \prod_{w|v} \mathcal{O}_{L_w}$, we can find $y \in \mathcal{O}_L$ such that $y - y_w \in \pi_w^N$ with $N \gg 0$. Then we have $\sum_{w|v} \mathrm{Tr}_{L_w/K_v}(xy_w) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(xy) + \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(x(y - y_w)) \in \mathcal{O}_{K_v}$. In particular, $\mathrm{Tr}_{L_w/K_v}(xy_w) \in \mathcal{O}_{K_v}$ for all $y_w \in \mathcal{O}_{L_w}$, so $x \in \mathcal{D}_{L_w/K_v}^{-1}$. This implies $\upsilon_w(\mathcal{D}_{L/K}^{-1}) \geq \upsilon_w(\mathcal{D}_{L_w/K_v}^{-1})$.

Let v be a finite place of K, and let $x \in L \cap \mathcal{D}_{L_w/K_v}^{-1}$ such that $\upsilon_w(x) = \upsilon_w(\mathcal{D}_{L_w/K_v}^{-1})$ for all $w|v$ (one can show such x exists using Chinese reminder theorem). Then $\mathrm{Tr}_{L/K}(xy) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(xy) \in \mathcal{O}_{K_v} \cap K$ for all $y \in \mathcal{O}_L$. We have $\mathcal{O}_{K_v} \cap K = \mathcal{O}_{K,v}$. Let $y_1, \cdots, y_r$ be a set of generators of $\mathcal{O}_L$ over $\mathcal{O}_K$. Since $\mathrm{Tr}_{L/K}(xy_i) \in \mathcal{O}_{K,v}$, there exists $z \in \mathcal{O}_K \setminus \mathfrak{p}_v$ such that $\mathrm{Tr}_{L/K}(zxy_i) \in \mathcal{O}_K$ for all y_i. Hence $zx \in \mathcal{D}_{L/K}^{-1}$. We see then $\upsilon_w(\mathcal{D}_{L/K}^{-1}) \leq \upsilon_w(x) = \upsilon_w(\mathcal{D}_{L_w/K_v}^{-1})$. The proposition follows. □

For a fractional ideal $I = \prod_w \mathfrak{P}_w^{\upsilon_w(I)}$ in L, denote by $N_{L/K}(I) := \prod_w \mathfrak{p}_v^{\upsilon_w(I)f(w/v)}$ that is a fractional ideal in K. Let $\delta_{L/K} := N_{L/K}(\mathcal{D}_{L/K})$. Then by the above proposition and Lemma 2.6.1, we have $\delta_{L/K} = \prod_w (\delta_{L_w/K_v} \cap \mathcal{O}_K)$.

Corollary 2.8.10. *For a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{p}$ is ramified in $\mathcal{O}_L$ if and only if $\mathfrak{p} | \delta_{L/K}$.*

Proposition 2.8.11. *Suppose L is Galois over K. Let w be a finite place of L and $\mathfrak{P}_w$ be the associated prime ideal of $\mathcal{O}_L$. Then the natural restriction map $j : \mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(L/K)$ factors through an isomorphism $\mathrm{Gal}(L_w/K_v) \xrightarrow{\sim} D_{\mathfrak{P}_w} \subset \mathrm{Gal}(L/K)$, and induces an isomorphism $I(L_w/K_v) \xrightarrow{\sim} I_{\mathfrak{P}_w}$.*

Proof. Since L is dense in L_w, we see j is injective (noting $\sigma \in \mathrm{Gal}(L_w/K_v)$ acts continuously on L_w). Let $\sigma \in \mathrm{Gal}(L_w/K_v)$, then $\sigma(\mathfrak{m}_w) = \mathfrak{m}_w$. We deduce $j(\sigma)(\mathfrak{m}_w \cap \mathcal{O}_L) = \mathfrak{m}_w \cap \mathcal{O}_L$. Together with the fact $\mathfrak{m}_w \cap \mathcal{O}_L = \mathfrak{P}_w$, we see $\mathrm{Im}(j) \subset D_{\mathfrak{P}_w}$. Since $|\mathrm{Gal}(L_w/K_v)| = f(w/v)e(w/v) = |D_{\mathfrak{P}_w}|$, the first part of the proposition follows. The second part follows by similar argument, that we leave as an exercise. □

Chapter 3

Adeles and Ideles

3.1 Adeles

Definition 3.1.1. *A locally compact group is a topological group G such that G is Hausdorff (in group case, this is equivalent to that any point is closed) and any point in G admits a compact neighbourhood (i.e. there exists an open U containing the point such that $\overline{U}$ is compact).*

Example 3.1.2. *The followings are locally compact groups:* $(\mathbb{Q}_p, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}_p, *)$, $(\mathbb{R}, *)$, $(\mathbb{C}^*, *)$.

Let J be a index set, J_∞ be a finite subset of J. Suppose for all $j \in J$, we have a locally compact group G_j. Moreover, suppose for $j \notin J_\infty$, G_j admits a compact open subgroup $H_j \subset G_j$.

Definition 3.1.3. *Put $\prod'_{j\in J} G_j = \{(x_j) \mid x_j \in G_j$ and $x_j \in H_j$ for all but finitely many $j\}$, called the restricted direct product of $\{G_j\}_{j\in J}$ with respect to $\{H_j\}$.*

It is clear that $\prod'_{j\in J} G_j$ has natural group structure. We equip $\prod'_{j\in J} G_j$ with the topology such that an open basis at $1 \in \prod'_{j\in J} G_j$ given by

$$\Pi_{j\in S} U_j \times \Pi_{j\notin S} H_j \subset \Pi'_{j\in J} G_j$$

where S runs though finite subset of J containing J_∞, and U_j runs through open neighbourhoods of 1 in G_j.

Remark 3.1.4. *Let $S \supset J_\infty$ be a finite set of J, we have a natural injection*

$$\Pi_{j\in S} G_j \times \Pi_{j\notin S} H_j \hookrightarrow \Pi'_{j\in J} G_j.$$

One can easily check that the induced topology on $\prod_{j\in S} G_j \times \prod_{j\notin S} H_j$ coincides with the product topology.

Exercise 3.1.5. *Prove that the topology on $\prod'_{j\in J} G_j$ is finer than the topology induced from the product topology on $\prod_{j\in J} G_j$ via the natural injection $\prod'_{j\in J} G_j \hookrightarrow \prod_{j\in J} G_j$.*

Proposition 3.1.6. *$\prod'_{j\in J} G_j$ is a locally compact group.*

Proof. Exercise. □

Now let K be a number field, J be the set of all places of K, J_∞ be the set of archimedean places of K, and $G_v := K_v$ for $v \in J$, and $H_v := \mathcal{O}_{K_v}$ for $v \in J \setminus J_\infty$. Let $\mathbb{A}_K := \prod'_{v\in J} K_v$, called the ring of adeles of K.

Exercise 3.1.7. *Prove that the multiplication map $\mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$ is continuous.*

Lemma 3.1.8. *The diagonal map $K \hookrightarrow \prod_{v\in J} K_v$ factors though an injection $K \hookrightarrow \mathbb{A}_K$.*

Proof. For any $x \in K$, there are only finitely many $v \in J \setminus J_\infty$ such that $x \notin \mathcal{O}_{K_v}$. The lemma follows. □

For a finite set $S \supset J_\infty$, denote by $\mathbb{A}_S := \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_{K_v}$.

Proposition 3.1.9. *We have $K + \mathbb{A}_{J_\infty} = \mathbb{A}_K$.*

Proof. We need to show that for all $(x_v)_{v\in J} \in \mathbb{A}_K$, there exists $x \in K$ such that $(x - x_v) \in \mathbb{A}_{J_\infty}$. Let $m \in \mathcal{O}_K \setminus \{0\}$ such that $mx_v \in \mathcal{O}_{K_v}$ for all v. Let S be the set of finite places v such that $m \in \mathfrak{p}_v$, and for $v \in S$, denote by e_v the maximal integer such that $m \in \mathfrak{p}_v^{e_v}$. Let $x \in \mathcal{O}_K$ such that $x \equiv mx_v \pmod{\mathfrak{p}_v^{e_v}}$ for all $v \in S$ (the existence following from Chinese reminder theorem). Then we have $x - mx_v \in \mathcal{O}_{K_v}$ for all fintie places v and $x - mx_v \in m\mathcal{O}_{K_v}$ for $v \in S$. Hence $\frac{x}{m} - x_v \in \mathcal{O}_{K_v}$ for all finite places v. The proposition follows. □

Let L/K be a finite extension. Denote by ι the injection $\iota : \mathbb{A}_K \hookrightarrow \mathbb{A}_L$, $(a_v) \mapsto (x_w)$, $x_w = a_v$ for $w|v$.

Proposition 3.1.10. *Let $e_1, \cdots, e_d$ be a basis of L over K. The morphism*

$$f : \mathbb{A}_K e_1 \oplus \cdots \oplus \mathbb{A}_k e_d \longrightarrow \mathbb{A}_L, \sum a_i e_i \mapsto \sum \iota(a_i) e_i$$

is well defined and is an isomorphism of topological groups.

Proof. Recall for all places v of K, the morphism $\iota_v : K_v e_1 \oplus \cdots K_v e_d \to \prod_{w|v} L_w$ is an isomorphism. Moreover, for all but finitely many finite places v, ι_v induces an isomorphism $\mathcal{O}_{K_v} e_1 \oplus \cdots \oplus \mathcal{O}_{K_v} e_d \xrightarrow{\sim} \prod_{w|v} \mathcal{O}_{L_w}$. So the map f is well defined. Since ι_v is injective for all v, we deduce f is injective. For any $(x_w)_w = ((x_w)_{w|v})_v \in \mathbb{A}_L$, since ι_v is surjective, there exist $a_{v,i} \in K_v$ such that $\iota_v(\sum a_{v,i} e_i) = (x_w)_{w|v} \in \prod_{w|v} L_w$. Since ι_v induces an isomorphism $\mathcal{O}_{K_v} e_1 \oplus \cdots \oplus \mathcal{O}_{K_v} e_d \xrightarrow{\sim} \prod_{w|v} \mathcal{O}_{L_w}$ for all but finitely many v, we see $a_{v,i} \in \mathcal{O}_{K_v}$ for all i for all but finitely many places v. In particular, the element $(a_{v,i})_v$ lies in $\mathbb{A}_K$ for any i. So f is surjective.

Let S_0 be a finite set of places of K containing all the archimedean places, and let $S_L := \{w|v \mid w \in S\}$. Let S_0 be large enough such that for all $v \notin S$, $L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w$ induces

an isomorphism $\mathcal{O}_{K_v}e_1 \oplus \cdots \oplus \mathcal{O}_{K_v}e_d \xrightarrow{\sim} \prod_{w|v} \mathcal{O}_{L_w}$. We see $\{U = U_S \times \prod_{v \notin S}(\mathcal{O}_{K_v}e_1 \oplus \cdots \oplus \mathcal{O}_{K_v}e_d)\}_{S \supset S_0}$, with U_S running though open neighbourhood of 0 in $\prod_{v\in S}(K_v e_1 \oplus \cdots \oplus K_v e_d)$, form an open basis of $\mathbb{A}_K e_1 \oplus \cdots \oplus \mathbb{A}_K e_d$ of 0. Using $L \otimes_K K_v \cong \prod_{w|v} L_w$, $f(U_S)$ form an open basis of $\prod_{v\in S}\prod_{w|v} L_w$. We see $\{f(U) = f(U_S) \times_{w \notin S_L} \mathcal{O}_{L_w}\}$ form an open basis of 0 in $\mathbb{A}_L$. So f is a homemorphism. □

Theorem 3.1.11. *K is a discrete, cocompact subgroup of $\mathbb{A}_K$ (i.e. $\mathbb{A}_K/K$ is compact).*

Proof. Let $e_1, \cdots, e_d$ be a basis of K over $\mathbb{Q}$. We have by the above proposition

$$\begin{array}{ccc} K & \xrightarrow{\sim} & \mathbb{Q}e_1 \oplus \cdots \oplus \mathbb{Q}e_d \\ \downarrow & & \downarrow \\ \mathbb{A}_K & \xrightarrow{\sim} & \mathbb{A}_{\mathbb{Q}}e_1 \oplus \cdots \oplus \mathbb{A}_{\mathbb{Q}}e_d \end{array}.$$

It thus suffices to show the statement for $K = \mathbb{Q}$.

Let $U := \{(x_v) \in \mathbb{A}_{\mathbb{Q}} \mid |x_\infty|_\infty \leq 1/2, |x_v|_v \leq 1, \text{ for all finite places } v\}$, that is an open neighbourhood of 0 in $\mathbb{A}_{\mathbb{Q}}$. It is clear that $U \cap \mathbb{Q} = \{0\}$. We deduce $\mathbb{Q}$ is discrete in $\mathbb{A}_{\mathbb{Q}}$. By Proposition 3.1.9, for any $x \in \mathbb{A}_{\mathbb{Q}}$, there exists $y \in \mathbb{Q}$ such that $|x - y|_v \leq 1$ for all finite places v of $\mathbb{Q}$. Replacing y by $y - n$ for a certain integer n, we can and do assume $x - y \in U$. Hence $U \xrightarrow{\sim} \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$. Since U is compact, we see $\mathbb{Q}$ is cocompact in $\mathbb{A}_{\mathbb{Q}}$. □

3.2 Ideles

Let $I_K := \prod'_{v\in J} K_v^\times$ where the restricted product is with respect to $\{\mathcal{O}_{K_v}^\times\}_{v \in J \setminus J_\infty}$.

Lemma 3.2.1. *As a set, we have $I_K = \mathbb{A}_K^\times$.*

Proof. For $(x_v) \in I_K \subset \mathbb{A}_K$, we have $x_v^{-1} \in \mathcal{O}_{K_v}$ for all but finitely many places v. Hence $(x_v^{-1}) \in \mathbb{A}_K$, so $I_K \subset \mathbb{A}_K^\times$. Conversely, if $(x_v) \in \mathbb{A}_K$ and $(x_v^{-1}) \in \mathbb{A}_K$, there exists a finite set S of places of K such that for all $v \notin S$, $x_v \in \mathcal{O}_{K_v}$ and $x_v^{-1} \in \mathcal{O}_{K_v}$. Hence $(x_v) \in I_K$. □

It is clear that the injection $I_K \hookrightarrow \mathbb{A}_K$ is continuous. However, the topology on I_K is finer than the topology induced from $\mathbb{A}_K$ via $I_K \hookrightarrow \mathbb{A}_K$.

Lemma 3.2.2. *If we equip $\mathbb{A}_K^\times$ with the topology induced from $\mathbb{A}_K$, then the morphism $\iota : \mathbb{A}_K^\times \to \mathbb{A}_K^\times$, $x \mapsto x^{-1}$ is not continuous.*

Proof. If ι is continuous, then it is a homemorphism. For the induced topology, we see $U := \mathbb{A}_K^\times \cap (U_S \times \prod_{v\notin S}(\mathcal{O}_{K_v} \setminus \{0\}))$, where S runs through finite subset of places of K including all archimedean places of K and U_S runs through open neighbourhoods of 1 in $\prod_{v\in S} K_v^\times$, form an open basis of 1 in $\mathbb{A}_K^\times$. If ι is a homemorphism, then $V := \iota^{-1}(U) = (V_S \times \prod_{v\notin S}(K_v \setminus \mathfrak{m}_{K_v})) \cap \mathbb{A}_K^\times$ (where $V_S = U_S^{-1}$) forms an open basis of 1 in $\mathbb{A}_K^\times$. However, one can check U does not contain any subset of the form $V' = \iota^{-1}(U')$ with $U' = \mathbb{A}_K^\times \cap (U'_{S'} \times \prod_{v\notin S'}(\mathcal{O}_{K_v} \setminus \{0\}))$, a contradiction. □

Exercise 3.2.3. *Prove that $I_K \to \mathbb{A}_K \times \mathbb{A}_K$, $x \mapsto (x, x^{-1})$ induces a homemorphism of I_K onto its image, equipped with the topology induced from $\mathbb{A}_K \times \mathbb{A}_K$.*

By the exercise and Theorem 3.1.11, we easily see:

Corollary 3.2.4. *We have $K^\times$ is a discrete subgroup of I_K.*

For each place v of K, we equip K_v with the normalized norm: if $K_v \cong \mathbb{C}$, then $|x|_v := |x\bar{x}|$, if $K_v \cong \mathbb{R}$, then $|x|_v := |x|$; if v is non-archimedean, then $|x|_v := q_v^{-\upsilon_v(x)}$ where $q_v := |k_v| = |\mathcal{O}_{K_v}/\mathfrak{m}_{K_v}|$ and υ_v is the additive valuation sending uniformizers to 1. Note in all cases, we have $|x|_v = |N_{K_v/\mathbb{Q}_p}(x)|_p$ for $p = \{\text{prime integer}\} \cup \{\infty\}$ ($\mathbb{Q}_\infty = \mathbb{R}$). We define $|\cdot|_K : I_K \to \mathbb{R}_{\geq 0}$, $(a_v) \mapsto \prod_v |a_v|_v$. Since $|a_v|_v = 1$ for all but finitely many v, μ is well-defined. It is also clear that $|\cdot|_K$ is continuous. Denote by $I_K^1 := \{x \in I_K \mid |x|_K = 1\}$.

Theorem 3.2.5 (Product formula)**.** *The natural embedding $K^\times \hookrightarrow I_K$ factors through I_K^1.*

Proof. By the discussion above the theorem, for $(x_v) \in I_K$, $|(x_v)_v|_K = |(\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v))_p|_{\mathbb{Q}}$. Thus for $x \in K$, we have $|x|_K = |N_{K/\mathbb{Q}}(x)|_{\mathbb{Q}}$. It then suffices to prove the theorem in the case $K = \mathbb{Q}$. Since $|\cdot|_{\mathbb{Q}}$ is multiplicative, the theorem then follows from: $|1|_{\mathbb{Q}} = 1$ (clear), $|-1|_{\mathbb{Q}} = 1$ (clear) and $|p|_{\mathbb{Q}}$=1 (using $|p|_\infty = p$, $|p|_p = 1/p$). □

3.3 Idele class group

A digression: Haar measure (a survey)

Let G be a locally compact group. Let $\mathcal{B} := \{\text{Borel subsets of } G\}$ (recall a Borel subset is an element in the smallest σ-algebra generated by open subsets of G. Let μ be a Borel measure on G (i.e. $\forall U \in \mathcal{B}$, U is measurable for μ). The measure μ is called outer regular if $\mu(E) = \inf\{\mu(U) \mid U \supset E,\ U \text{ open}\}$; μ is called inner regular if $\mu(E) = \sup\{\mu(K) \mid K \subset E,\ K \text{ compact}\}$.

A Radon measure on G is a Borel measure that is finite on compact sets, is outer regular on all Borel subsets and is inner regular on all open subsets. Note that a Randon measure s determined by its value on compact subsets.

Let μ is a Borel measure on G, we call μ left invariant (resp. right invariant) if $\mu(gE) = \mu(E)$ (resp. $\mu(Eg) = \mu(E)$) for all Borel subset $E \subset G$ and $g \in G$.

Definition 3.3.1. *Let G be a locally compact topological group. A left (resp. right) Haar measure on G is a nonzero Radon measure that is left (resp. right) invariant.*

Example 3.3.2. *Let $G = (\mathbb{R}^n, +)$. Then the standard Lebesgue measure μ is a left and right Haar measure on G, as it is clear that $\mu(x + U) = \mu(U)$ for any measurable subset.*

Theorem 3.3.3. *Let G be a locally compact group. Then G admits a left (also a right) Haar measure. Moreover, the measure if unique up to scalar multiple.*

Example 3.3.4. *(1) Let K be a number field, v be a finite place of K, and $G = (K_v, +)$. Let μ_v be a Haar measure on K_v (the existence following from the above theorem). We have $\mu_v(\mathcal{O}_{K_v}) \neq 0$, since otherwise $\mu_v = 0$. By multiplying μ by a non-zero scalar, we can assume $\mu_v(\mathcal{O}_{K_v}) = 1$. Then we have $\mu_v(x\mathcal{O}_{K_v}) = |x|_v$. Indeed, let π_v be a uniformizer and suppose $x \in \pi_v^n \mathcal{O}_{K_v}^\times$ and $n \geq 0$ (the case $n < 0$ being similar). Let $\{x_1, \cdots, x_{q_v^n}\}$ be a set of representatives of $\mathcal{O}_{K_v}/\pi_v^n$ in $\mathcal{O}_{K_v}$. Then we have $\mathcal{O}_{K_v}$ is a disjoint union of $x_i + x\mathcal{O}_{K_v}$. Since μ_v is left invariant, we have $\mu(x_i + x\mathcal{O}_{K_v}) = \mu(x\mathcal{O}_{K_v})$. Hence $\mu_v(\mathcal{O}_{K_v}) = q_v^n \mu_v(x\mathcal{O}_{K_v}) \Rightarrow \mu_v(x\mathcal{O}_{K_v}) = q_v^{-n} = |x|_v$.*

(2) If v is an archimedean place of K, we let μ_v denote the standard Lebesgue measure on K_v (that is isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

(3) Let $G = \mathbb{A}_K = \prod'_{v \in J} K_v$. Then there exists a unique Haar measure μ on G such that for any $U = \prod_v U_v \subset G$ with all U_v compact and $U_v \subset \mathcal{O}_{K_v}$ for all but finitely many v, we have

$$\mu(U) = \prod_v \mu_v(U_v). \tag{3.1}$$

Actually, let μ be the Haar measure satisfying $\mu(\prod_{v|\infty} C_v \times \prod_{v \nmid \infty} \mathcal{O}_{K_v}) = 1$ where $C_v = [0,1]$ if $K_v \cong \mathbb{R}$ and $C_v = [0,1] \times [0,1]$ if $K_v \cong \mathbb{C}$, then one can check (3.1) holds.

Lemma 3.3.5. *Let $x = (x_v) \in I_K$, μ be a Haar measure on $\mathbb{A}_K$, and let E be a compact subset in $\mathbb{A}_K$ such that $\mu(E) \neq 0$. Then $\mu(xE) = |x|_K \mu(E)$ (noting by Exercise 3.1.7, xE is a compact subset of $\mathbb{A}_K$).*

Proof. Since μ is a Haar measure, we deduce $U \mapsto \mu(xU)$ is also a Haar measure. Actually, by Exercise 3.1.7, the element x induces a homemorphism $\mathbb{A}_K \to \mathbb{A}_K$, $a \mapsto xa$. By Theorem 3.3.3, it suffices to show the statement for a single compact subset E with $\mu(E) \neq 0$. Multiplying μ by a scalar, we can and do assume μ is the one in Example 3.3.4 (3). Let $E := \prod_v \{|x_v|_v \leq 1\} = \prod_{v|\infty} \{|x_v|_v \leq 1\} \times \prod_{v \nmid \infty} \mathcal{O}_{K_v}$, so $\mu(E) = \pi^s$ (where s denotes the number of complex places of K). One easily checks that $\mu(xE) = \pi^s \prod_v |x_v|_v$. The lemma follows. □

Idele class group

The group $\mathscr{C}_K := I_K/K^\times$ is called the idele class group.

Theorem 3.3.6. *$I_K^1/K^\times$ is compact.*

Proof. Consider the natural map $I_K^1 \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$, $x \mapsto (x, x^{-1})$. Recall there exists a compact subset $\Phi \subset \mathbb{A}_K$ such that $K + \Phi = \mathbb{A}_K$. Indeed if $K = \mathbb{Q}$, we can take Φ to be the set U in the proof of Theorem 3.1.11. In general, letting $e_1, \cdots, e_d$ be a basis of K over $\mathbb{Q}$ and U as above, then the compact set $\Phi = \prod_i U e_i$ satisfies $\Phi + K = \mathbb{A}_K$. Let μ be a Haar measure on $\mathbb{A}_K$. We have $\mu(\Phi) \neq 0$ since otherwise $\mu(\mathbb{A}_K) \leq \sum_{x \in K} \mu(x + \Phi) = 0$. Let Z be a compact subset of $\mathbb{A}_K$ such that $\mu(Z) > \mu(\Phi)$. For $x \in I_K^1$, we have thus $\mu(xZ) = \mu(x^{-1}Z) = \mu(Z) > \mu(\Phi)$.

Claim: Let $U \subset \mathbb{A}_K$ such that $\mu(U) > \mu(\Phi)$. Then there exists $u_1 \neq u_2 \in U$ such that $u_1 - u_2 \in K$.

We prove the claim. If not, we have $(r_1 + U) \cap (r_2 + U) = \emptyset$ for all $r_1 \neq r_2 \in K$. So $\mu(\Phi) \geq \sum_{r \in K} \mu(\Phi \cap \{r + U\}) = \sum_{r \in K} \mu((r + \Phi) \cap U) \geq \mu(U)$, a contradiction.

By the claim, for any $x \in I_K^1$ there exist $u_1, u_2, u_3, u_4 \in Z$ such that $x(u_1 - u_2) \in K^\times$, $x(u_3 - u_4) \in K^\times$. Let Z_1 be the image of $Z \times Z$ via the continuous map $\mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$, $(a, b) \mapsto a - b$. So Z_1 is also compact, and we see $x \in K^\times Z_1$, $x^{-1} in K^\times Z_1$. We write $x = yz_1$, $x^{-1} = y'z_2$ with $y, y' \in K^\times$, $z_i \in Z_1$. So $z_1 z_2 = (yy')^{-1} \in K^\times$. Let Z_2 be the image of $Z_1 \times Z_1$ via the continuous morphism $\mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$, $(a, b) \mapsto ab$, that is a compact subset of $\mathbb{A}_K$. Then we see $(yy')^{-1} \in K^\times \cap Z_2$. However $K^\times \cap Z_2$ is both compact and discrete, hence finite, say, $K^\times \cap Z_2 = \{y_1, \cdots, y_m\}$. Thus there exists y_i such that $y' = y^{-1} y_i^{-1}$. We embed $K^\times$ into $\mathbb{A}_K \times \mathbb{A}_K$ via $a \mapsto (a, a^{-1})$. And consider the set $K^\times(\cup_{i=1}^m (Z_1, y_i^{-1} Z_1)) \subset \mathbb{A}_K \times \mathbb{A}_K$. By the above discussion, we see for any $x \in I_K^1$, there exist $y \in K^\times$, and $i \in \{1, \cdots, m\}$ such that $x \in yZ_1$ and $x^{-1} \in y^{-1} y_i^{-1} Z_1$. Thus the image of $I_K^1 \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$, $a \mapsto (a, a^{-1})$ is contained in $K^\times(\cup_{i=1}^m (Z_1, y_i^{-1} Z_1)) \subset \mathbb{A}_K \times \mathbb{A}_K$. Since $(\cup_{i=1}^m (Z_1, y_i^{-1} Z_1))$ is compact, so is $I_K^1 / K^\times$. □

Recall J_K denotes the group of fractional ideals of K. We have a natural map

$$\jmath : I_K \to J_K, \ (x_v) \mapsto \prod_{v \nmid \infty} \mathfrak{p}_v^{\mathrm{ord}_v(x_v)}.$$

Then we see $\mathrm{Ker}(\jmath) = \Omega(J_\infty) := \prod_{v \in J_\infty} K_v^\times \times \prod_{v \notin J_\infty} \mathcal{O}_{K_v}^\times$. It is also easy to see $\jmath$ sends $K^\times$ onto the subgroup of principal fractional ideals of K. Thus $\jmath$ induces an isomorphism

$$I_K / K^\times \Omega(J_\infty) \xrightarrow{\sim} C_K.$$

We have $I_K^1 \Omega(J_\infty) = I_K$. Indeed, for any $x \in I_K$, let v be an archimedean place of K, and consider the element $y := (y_v, 1, \cdots) \in \Omega(J_\infty)$ with $|y_v|_v = |x|_K$, then $x/y \in I_K^1$. The embedding $I_K^1 \hookrightarrow I_K$ induces thus an isomorphism

$$I_K^1 / K^\times (\Omega(J_\infty) \cap I_K^1) \xrightarrow{\sim} I_K / K^\times \Omega(J_\infty) (\cong C_K).$$

Since $I_K^1 / K^\times$ is compact, and $\Omega(J_\infty) \cap I_K^1$ is open in I_K^1, we deduce:

Corollary 3.3.7. *The group C_K is finite.*

Let $C := \{(x_v) \in I_K \mid |x_v|_v = 1\} = \prod_{v \in J_\infty} \{|x|_v = 1\} \times \prod_{v \notin J_\infty} \mathcal{O}_{K_v}^\times$. We see C is a compact closed subgroup of I_K^1.

Proposition 3.3.8. *We have $C \cap K^\times = \{x \in K^\times \mid x^n = 1 \text{ for some } n\}$.*

Proof. Since $K^\times$ is a discrete subgroup of I_K, we see $C \cap K^\times$ (with the induced topology) is both compact and discrete, and hence is a finite set. So $C \cap K^\times$ is a finite (hence cyclic) subgroup of $K^\times$. Any element in $C \cap K^\times$ is thus a root of unity. Conversely, if $x \in K^\times$ satisfies $x^n = 1$, we see $|x|_v^n = 1$ for all v, and so $x \in K^\times \cap C$. □

Let $S \supset J_\infty$ be a finite set of places in K, and we put

$$\begin{aligned} I_{K,S} &:= \prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_{K_v}^\times, \\ \mathbb{A}_{K,S} &:= \prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_{K_v} \end{aligned}$$

Then $I_{K,S}$ (resp. $\mathbb{A}_{K,S}$) is an open subgroup of I_K (resp. $\mathbb{A}_K$). If $S = J_\infty$, we have $\mathbb{A}_{K,J_\infty} \cap K = \mathcal{O}_K$, and $I_{K,J_\infty} \cap K^\times = \mathcal{O}_K^\times$. We call $\mathcal{O}_{K,S} := \mathbb{A}_{K,S} \cap K$ the ring of S-integers in K, and $\mathcal{O}_{K,S}^\times$ the group of S-units K. The following theorem generalizes Dirichlet's unit theorem.

Theorem 3.3.9. *We have $\mathcal{O}_{K,S}^\times \cong \mu_K \times \mathbb{Z}^{|S|-1}$.*

Proof. The goal is to realize $\mathcal{O}_{K,S}^\times$ as a lattice of certain $\mathbb{R}$-vector space. Let $I_{K,S}^1 := I_K^1 \cap I_{K,S}$, that is an open subgroup of $I_{K,S}$. We have $\mathcal{O}_{K,S}^\times = I_{K,S}^1 \cap K^\times$. We have an exact sequence

$$1 \to I_{K,S}^1/\mathcal{O}_{K,S}^\times \to I_{K,S}/\mathcal{O}_{K,S}^\times \xrightarrow{|\cdot|_K} \mathbb{R}_{>0} \to 1.$$

Since $I_{K,S}^1$ is open in I_K^1 and $I_K^1/K^\times$ is compact, we deduce $I_{K,S}^1/\mathcal{O}_{K,S}^\times$ is compact. Consider the following commutative diagram

$$\begin{array}{ccccccccc} & & \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times \cap C) & \xrightarrow{\mathrm{id}} & \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times \cap C) & & & & \\ & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & I_{K,S}^1/C & \longrightarrow & I_{K,S}/C & \xrightarrow{\log\circ|\cdot|_K} & \mathbb{R} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & I_{K,S}^1/C\mathcal{O}_{K,S}^\times & \longrightarrow & I_{K,S}/C\mathcal{O}_{K,S}^\times & \xrightarrow{\log\circ|\cdot|_K} & \mathbb{R} & \longrightarrow & 0. \end{array}$$

Since $I_{K,S}^1/\mathcal{O}_{K,S}^\times$ is compact, so is $I_{K,S}^1/C\mathcal{O}_{K,S}^\times$. We have $\mathcal{O}_{K,S} \cap C = \mu_K$. It is clear that $I_{K,S}/C \cong \prod_{v|\infty} \mathbb{R}_{>0} \times \prod_{v\in S\setminus J_\infty} \mathbb{Z} \cong \mathbb{R}^{|J_\infty|} \times \mathbb{Z}^{|S\setminus J_\infty|}$. We show $\mathcal{O}_{K,S}^\times/\mu_K$ is discrete in $I_{K,S}/C$ (hence also discrete in $I_{K,S}^1/C$). Let U be an open neighbourhood of 1 in $I_{K,S}$ with $\overline{U}$ compact (recalling $I_{K,S}$ is locally compact). Consider $UC \cap K^\times \subset \overline{U}C \cap K^\times$. Since $\overline{U}C$ is the image of the compact set $\overline{U} \times C$ in I_K via the continuous morphism $I_K \times I_K \to I_K$, $(a, b) \mapsto ab$, $\overline{U}C$ is compact. Recall $K^\times$ is closed and discrete in I_K. So $K^\times \cap \overline{U}C$ is discrete and compact hence finite. The image U in $I_{K,S}/C$ is open in $I_{K,S}/C$ and only has finite intersection with the image of $\mathcal{O}_{K,S}^\times$. Together with te fact $I_{K,S}/C$ is Hausdorff (using C is closed, fact: a topological group is Hausdorff if and only if $\{1\}$ is closed), we deduce $\mathcal{O}_{K,S}^\times/\mu_K$ is discrete in $I_{K,S}/C$.

The embedding $\mathbb{Z} \hookrightarrow \mathbb{R}$ induces an embedding $I_{K,S}/C \cong \mathbb{R}^{|J_\infty|} \times \mathbb{Z}^{|S\setminus J_\infty|} \hookrightarrow \mathbb{R}^{|J_\infty|} \times \mathbb{R}^{|S\setminus J_\infty|} := V$. The map $f : \mathbb{R}^{|J_\infty|} \times \mathbb{Z}^{|S\setminus J_\infty|} \cong I_{K,S}/C \xrightarrow{\log\circ|\cdot|_K} \mathbb{R}$ has the form $(\lambda_1, \cdots, \lambda_{|S|}) \mapsto \sum a_i\lambda_i$ for certain $a_i \in \mathbb{R}$ ($\lambda_1, \cdots, \lambda_{|J_\infty|} \in bR$ and $\lambda_{|J_\infty|+1}, \cdots \lambda_{|S|} \in \mathbb{Z}$). We extend the

map to $\tilde{f} : V \to \mathbb{R}$, $(\lambda_1, \cdots, \lambda_{|S|}) \mapsto \sum a_i\lambda_i$. Let $V_1 := \mathrm{Ker}(\tilde{f})$ that is $\mathbb{R}$-vector space of dimension $|S| - 1$, and we have $I^1_{K,S}/\mathcal{O}^\times_{K,S} = V_1 \cap I_{K,S}/C$.

Since $\mathcal{O}^\times_{K,S}/\mu_K$ is discrete in $I^1_{K,S}/\mathcal{O}^\times_{K,S}$, it is also discrete in V_1. Since $V/(I_{K,S}/C)$ is compact ($\cong (\mathbb{R}/Z)^{|S\setminus J_\infty|}$), $V_1/(I^1_{K,S}/C)$ is also compact. This, together with the fact $(I^1_{K,S}/C)/(\mathcal{O}^\times_{K,S}/\mu_K)$ is compact, imply $V_1/(\mathcal{O}^\times_{K,S}/\mu_K)$ is compact (Exercise). Hence $\mathcal{O}^\times_{K,S}/\mu_K$ is a lattice in V_1. The theorem follows. □

Global class field theory (some statements)

Theorem 3.3.10. *Let K be a number field. There is a canonical morphism (called Artin map) $\mathrm{rec} : \mathscr{C}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ that induces an isomorphism $\widehat{\mathscr{C}_K} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$, where $\widehat{\mathscr{C}_K} := \varprojlim_U \mathscr{C}_K/U$ where U runs though open subgroups of finite index in $\mathscr{C}_K$.*

Exercise 3.3.11. *Let $K_\infty := \prod_{v|\infty} K_v$, and $(K^\times_\infty)^o$ be the connected component of 1 in $K^\times_\infty$. Show that for any open subgroup U of finite index in $\mathscr{C}_K$, U contains $(K^\times_\infty)^o$.*

Consequently, the map $\mathscr{C}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ factors through

$$K^\times\backslash I_K/(K^\times_\infty)^o = \mathbb{G}_m(K)\backslash\mathbb{G}_m(\mathbb{A}_K)/\mathbb{G}_m(K_\infty)^o.$$

We describe in more details of the structure of $\mathscr{C}_K$ (and of $\widehat{\mathscr{C}_K}$).

Lemma 3.3.12. *Let S be a finite set of places of K containing all archimedean places such that $\{\mathfrak{p}_v\}_{v\in S\setminus J_\infty}$ can generate C_K. Then $K^\times I_{K,S} = I_K$.*

Proof. Let $x = (x_v) \in I_K$, and consider the fractional ideal $\mathfrak{a}_x := \prod_{v\nmid\infty} \mathfrak{p}_v^{\mathrm{ord}_v(x_v)}$. By the assumption on S, there exists $\alpha \in K^\times$ such that $\mathfrak{a}_x\alpha^{-1} = \prod_{v\in S\setminus J_\infty} \mathfrak{p}_v^{e_v}$ for certain $e_v \in \mathbb{Z}$. So $x\alpha^{-1} \in I_{K,S}$. The lemma follows. □

Proposition 3.3.13. *We have an isomorphism $\widehat{\mathscr{C}_K} \cong I_K/\overline{K^\times(K^\times_\infty)^o}$ (where $\overline{(\cdot)}$ denotes the closure).*

Proof. It suffices to show $I_K/\overline{K^\times(K^\times_\infty)^o}$ is profinite. Let S be as in the above lemma, we have $I_{K,S}/\overline{\mathcal{O}^\times_{K,S}(K^\times_\infty)^o} \xrightarrow{\sim} I_K/\overline{K^\times(K^\times_\infty)^o}$.

One can prove that the open subgroup $I_{K,J_\infty}\mathcal{O}^\times_{K,S}(K^\times_\infty)^o \subset I_{K,S}$ has finite index (Exercise). So t is also closed, and contains $\overline{\mathcal{O}^\times_{K,S}(K^\times_\infty)^o}$. We also deduce

$$I_{K,J_\infty}\mathcal{O}^\times_{K,S}(K^\times_\infty)^o/\overline{\mathcal{O}^\times_{K,S}(K^\times_\infty)^o} \cong I_{K,J_\infty}/\overline{\mathcal{O}^\times_K(K^\times_\infty)^o}$$

is an open subgroup of finite index in $I_{K,S}/\overline{\mathcal{O}^\times_{K,S}(K^\times_\infty)^o}$. It suffices to show $I_{K,J_\infty}/\overline{\mathcal{O}^\times_K(K^\times_\infty)^o}$ is profinite. One can show the morphism

$$\iota : \{\pm 1\}^r \times \prod_{v\nmid\infty} \mathcal{O}^\times_{K_v} \twoheadrightarrow I_{K,J_\infty}/\overline{\mathcal{O}^\times_K(K^\times_\infty)^o}$$

factors though an isomorphism $\left(\{\pm 1\}^r \times \prod_{v\nmid\infty} \mathcal{O}_{K_v}^\times\right)/\operatorname{Ker}\iota \cong I_{K,J_\infty}/\overline{\mathcal{O}_K^\times(K_\infty^\times)^o}$. The proposition then follows from the fact $\left(\{\pm 1\}^r \times \prod_{v\nmid\infty} \mathcal{O}_{K_v}^\times\right)/\operatorname{Ker}\iota$ is profinite (noting $\operatorname{Ker}\iota$ is closed). □

Exercise 3.3.14. *Prove the map $\mathbb{Q}^\times \times \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^\times \to I_\mathbb{Q}$, $(x, x_\infty, (x_p)) \mapsto (xx_\infty, (xx_p))$ is an isomorphism of topological groups. Deduce $\mathscr{C}_K \cong \widehat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times$.*

Theorem 3.3.15 (Kronecker-Weber)**.** *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

We give a more explicit description of the artin map using the language of modulus. A modulus $\mathfrak{m}$ of K is a formal product $\mathfrak{m}^\infty\mathfrak{m}_\infty$ where $\mathfrak{m}^\infty = \prod_v \mathfrak{p}_v^{e_v}$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a subset of $\{\sigma : K \hookrightarrow \mathbb{R}\}$. For a place v of K, we write $v|\mathfrak{m}$ if $\mathfrak{p}_v|fm^\infty$ when v is non-archimedean, and if $v \in \mathfrak{m}_\infty$ when v is archimedean. For $v|\mathfrak{m}$, define

$$U_v(\mathfrak{m}) := \begin{cases} \mathbb{R}_{>0} & v|\infty \\ 1 + \mathfrak{p}_v^{e_v}\mathcal{O}_{K_v} & v \nmid \infty \end{cases}.$$

Define $J_K(\mathfrak{m}) \subset J_K$ to be the group of fractional ideals that are relatively prime to $\mathfrak{m}^\infty$ (i.e. that do not have $\mathfrak{p}_v$-factor in the prime decomposition for all $\mathfrak{p}_v|\mathfrak{m}^\infty$). Put $P_K(\mathfrak{m}) = \{(\alpha) \mid \alpha \in K^\times, \alpha \in U_v(\mathfrak{m})\ \forall v|\mathfrak{m}\}$. The quotient $J_K(\mathfrak{m})/P_K(\mathfrak{m})$ is called a Ray class group of K.

Put $I_K(\mathfrak{m}) := I_K \cap \prod_{v|\mathfrak{m}} U_v(\mathfrak{m}) \times \prod_{v\nmid\mathfrak{m}} K_v^\times$, $W_K(\mathfrak{m}) := I_K(\mathfrak{m}) \cap I_{K,J_\infty}$ that is a open subgroup of $I_K(\mathfrak{m})$. Consider the natural morphism

$$I_K(\mathfrak{m}) \longrightarrow J_K(\mathfrak{m}),\ (x_v) \mapsto \prod_v \mathfrak{p}_v^{\operatorname{ord}_v(x_v)}.$$

It is clear that this map is surjective, with the kernel equal to $W_K(\mathfrak{m})$. We deduce then an isomorphism

$$I_K(\mathfrak{m})/W_K(\mathfrak{m})(K^\times \cap I_K(\mathfrak{m})) \xrightarrow{\sim} I_K(\mathfrak{m})/P_K(\mathfrak{m}),$$

which gives an adelic description of the ray class group.

Lemma 3.3.16. *The natural map $I_K(\mathfrak{m}) \to I_K$ induces an isomorphism*

$$I_K(\mathfrak{m})/(I_K(\mathfrak{m}) \cap K^\times) \xrightarrow{\sim} I_K/K^\times.$$

Proof. The injectivity is trivial. For $(x_v) \in I_K$, since K is dense in $\prod_{v|\mathfrak{m}} K_v$, there exists $\alpha \in K^\times$ such that α is arbitrarily close to x_v for all $v|\mathfrak{m}$. In particular, if v is non-archimedean, α can be chosen to have the same norm as x_v, and $\frac{x_v}{\alpha} \in U_v(\mathfrak{m})$; if v is archimedean, then α has the same sign as x_v (so $\frac{x_v}{\alpha} \in U_v(\mathfrak{m})$). The lemma follows. □

Using similar argument as for Corollary 3.3.7, one can prove

Proposition 3.3.17. *The ray class group $J_K(\mathfrak{m})/P_K(\mathfrak{m})$ is finite.*

Proof. Exercise. □

Let L/K be a finite abelian extension. Let $\mathfrak{m}$ be a modulus divisible by all ramified primes (including infinite primes) of K in the extension L/K. For $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{p} \nmid \mathfrak{m}$, recall we have the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$: $\left(\frac{L/K}{\mathfrak{p}}\right)(x) \equiv x^{N(\mathfrak{p})} \equiv \mathfrak{P}$ for all $x \in \mathcal{O}_L$, and for $\mathfrak{P}$ a (or any) prime ideal of $\mathcal{O}_L$ dividing $\mathfrak{p}$. We have then a morphism

$$J_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K),\ \prod \mathfrak{p}^{e_\mathfrak{p}} \mapsto \prod \left(\frac{L/K}{\mathfrak{p}}\right)^{e_\mathfrak{p}}.$$

Theorem 3.3.18. *The above morphism is surjective, and factors through $J_K(\mathfrak{m})/P_K(\mathfrak{m})$ when the exponents of the finite primes in $\mathfrak{m}$ are sufficiently large. Moreover, the induced map $\mathscr{C}_K \twoheadrightarrow J_K(\mathfrak{m})/P_K(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(L/K)$ is equal to $\mathscr{C}_K \xrightarrow{\mathrm{rec}} \mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(L/K)$.*

Chapter 4

Zeta functions

4.1 Riemann-Zeta function

Let $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, called the Riemann-Zeta function. Recall the power series $\sum_{n=1}^{\infty} \frac{1}{n}$ is not convergent: $\sum_{n=2^k+1}^{2^{k+1}} \frac{1}{n} > \frac{1}{2}$.

Proposition 4.1.1. *There are infinitely many primes.*

Proof. Suppose there are only finitely many prime numbers $p_1, \cdots, p_r$. Then we have

$$\sum_{n=1}^{p_1^N \cdots p_r^N} \frac{1}{n} = \prod_{i=1}^{r} (1 + \frac{1}{p_i} + \cdots + \frac{1}{p_i^N}).$$

We then deduce $\sum_{n=1}^{p_1^N \cdots p_r^N} \frac{1}{n}$ converges as $N \to \infty$, a contradiction. □

Proposition 4.1.2. $\sum_{n=1}^{\infty} \frac{1}{n^s}$ *is absolutely convergent if* $\operatorname{Re} s > 1$ *and* $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ *is holomorphic for* $\operatorname{Re} s > 1$.

Proof. We have $|\frac{1}{n^s}| = |\frac{1}{n^{\operatorname{Re} s}}|$ and $\sum_{n=1}^{\infty} \frac{1}{n^a}$ is absolutely convergent for $a \in \mathbb{R}_{>1}$: $\sum_{n=1}^{\infty} \frac{1}{n^a} \sim \int_1^{\infty} x^{-a} dx = \frac{1}{1-a}$. Recall the following fact in complex analysis:

- Let $\Omega \subset \mathbb{C}$ be an open subset, f_n be a sequence of holomorphic functions on Ω such that $\{f_n\}$ uniformly converge to f on each compact subset $K \subset \Omega$, then f is holomophic on Ω.

We then deduce $\zeta(s)$ is holomorphic on $\operatorname{Re} s > 1$. □

Remark 4.1.3. *In fact, we have* $\sum_{n=1}^{\infty} \frac{1}{n^s} - \frac{1}{s-1} = \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - x^{-s}) dx$. *Since* $|n^{-s} - x^{-s}| = |s \int_n^x y^{-1-s} dy| \leq |s| n^{-1-\operatorname{Re} s}|$, *we see* $\sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - x^{-s}) dx$ *is absolutely convergent and is holomorphic for* $\operatorname{Re} s > 0$. *In this way, we get an analytic continuation of* $\zeta(s)$ *on* $\operatorname{Re} s > 0$ *given by*

$$\frac{1}{s-1} + \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - x^{-s}) dx. \tag{4.1}$$

Recall $\prod_{n=1}^{\infty} a_n$ (with $a_n \neq 0$ for all n) is called convergent if $\prod_{n=1}^{N} a_n$ converges to a *non-zero* element in $\mathbb{C}$. In particular, if $\prod_{n=1}^{\infty} a_n$ converges then $a_n \to 1$. We recall the following basis facts:

- The followings are equivalent:
  - $\prod_{n=1}^{\infty}(1+a_n)$ is convergent,
  - $\sum_{n=1}^{\infty}\log(1+a_n)$ is convergent (where log denotes the principal branch of the logarithm, i.e. $\mathrm{Im}(\log(z)) \in (-\pi, \pi]$),
  - $\sum_{n=1}^{\infty} a_n$ is convergent.
- We call $\prod_{n=1}^{\infty}(1+a_n)$ absolutely convergent if $\sum_{n=1}^{\infty}\log(1+a_n)$ is absolutely convergent. Then $\prod_{n=1}^{\infty}(1+a_n)$ is absolutely convergent if and only if $\sum_{n=1}^{\infty}|a_n|$ is convergent.
- Let $\Omega \subset \mathbb{C}$ be an open subset, and assume $a_n(z)$ is holomorphic on Ω. Let K be a compact subset of Ω. Then $\prod_{n=1}^{\infty}(1+a_n(z))$ is absolutely and uniformly convergent on K if and only if $\sum_{n=1}^{\infty}|a_n(z)|$ is uniformly convergent on K. And if this holds for any compact $K \subset \Omega$, then $\prod_{n=1}^{\infty}(1+a_n(z))$ is holomorphic on Ω.

Proposition 4.1.4. *The product* $\prod_p(1-\frac{1}{p^s})^{-1}$ *is absolutely convergent for* $\mathrm{Re}\, s > 1$ *and* $\prod_p(1-\frac{1}{p^s})^{-1} = \zeta(s)$.

Proof. We have $|\zeta(s) - \prod_{\mathfrak{p}\leq\mathfrak{p}_N}\frac{1}{(1-\frac{1}{p^s})}| \leq \sum_{n>\mathfrak{p}_N}|\frac{1}{n^s}| \to 0$ as $\mathfrak{p}_N \to \infty$. The proposition follows. □

Exercise 4.1.5. *Show that* $\zeta(s) \neq 0$ *for* $\mathrm{Re}\, s > 1$.

Theorem 4.1.6. *The Riemann zeta function* $\zeta(s)$ *extends (uniquely) to a meromorphic function on* $\mathbb{C}$*, holomorphic everywhere except for a simple pole at* $s = 1$*. We have the so-called functional equation:*

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s).$$

Recall $\Gamma(s) = \int_0^{\infty} e^{-t}t^s\frac{dt}{t}$ (that can be viewed as the ∞-Euler factor). Recall the following fact:

- Let D be a measurable subset of $\mathbb{R}$, $U \subset \mathbb{C}$ open. Suppose
  1. f is measurable on $D \times U$,
  2. $f(x,z)$ is analytic on U for any $x \in D$,
  3. there exists a measurable function $M : D \to \mathbb{R}$ such that $|f(x,z)| \leq M(x)$ for $x \in D$, $z \in U$ and $\int_D M(x)dx < \infty$.

  Then $F(z) = \int_D f(x,z)dx$ is analytic on U.

We write $\Gamma(s) = \int_0^1 e^{-t}t^s\frac{dt}{t} + \int_1^\infty e^{-t}t^s\frac{dt}{t}$. Since $|e^{-t}t^{s-1}| < e^{-t/2}$ when t is sufficiently large, we see the second term is always analytic (for $s \in \mathbb{C}$). We have $|e^{-t}t^{s-1}| \leq |t^{\operatorname{Re} s-1}|$ for $t \in (0,1]$. So for $\operatorname{Re} s > 0$, we have $|\int_0^1 e^{-t}t^s\frac{dt}{t}| \leq \int_0^1 t^{\operatorname{Re} s-1}\frac{dt}{t} = \frac{1}{\operatorname{Re} s}$. Using the above fact, we deduce $\Gamma(s)$ is holomorphic on $\operatorname{Re} s > 0$.

Using $\Gamma(s+1) = s\Gamma(s)$ (exercise), $\Gamma(s)$ extends to a meromorphic function with poles at non-positive integers. Note we have $\Gamma(1) = \int_0^\infty e^{-t}dt = 1$, so $\Gamma(n) = n!$.

Proof of Theorem 4.1.6. We have $\pi^{\frac{s}{2}}\Gamma(\frac{s}{2})\frac{1}{n^s} = \int_0^\infty t^{\frac{s}{2}-1}e^{-n^2\pi t}dt$ (for $\operatorname{Re} s > 0$). Thus

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \int_0^\infty t^{\frac{s}{2}-1}(\sum_{n=1}^\infty e^{-n^2\pi t})dt = \int_0^1 t^{\frac{s}{2}-1}w(t)dt + \int_1^\infty t^{\frac{s}{2}-1}w(t)dt,$$

where $w(t) = \sum_{n=1}^\infty e^{-n^2\pi t}$. For $t \geq 1$, we have $w(t) = O(e^{-\pi t})$ (for $t \to \infty$): $w(t) \leq (\sum_{i=0}^\infty e^{-n\pi t})e^{-\pi t}$. Hence the term $\int_1^\infty t^{\frac{s}{2}-1}w(t)dt$ is holomorphic for on $\mathbb{C}$. We have $\int_1^\infty t^{\frac{s}{2}-1}w(t)dt = \int_1^\infty w(1/t)t^{-\frac{s}{2}-1}dt$. Using Lemma 4.1.7, we see

$$\begin{aligned}\int_1^\infty w(1/t)t^{-\frac{s}{2}-1}dt &= \int_1^\infty t^{-\frac{s}{2}-\frac{1}{2}}w(t)dt - \frac{1}{2}\int_1^\infty t^{-\frac{s}{2}-1}dt + \frac{1}{2}\int_1^\infty t^{-\frac{s}{2}-\frac{1}{2}}dt \\ &= \int_1^\infty t^{-\frac{s}{2}-\frac{1}{2}}w(t)dt - \frac{1}{s} + \frac{1}{s-1}.\end{aligned}$$

In summary, we have

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = -\frac{1}{s(1-s)} + \int_1^\infty (t^{\frac{s}{2}-1} + t^{\frac{1-s}{2}-1})w(t)dt. \tag{4.2}$$

We see thus $\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$ has a meromorphic continuation that has simple poles at 0, 1. The functional equation also follows.

We know $\Gamma(s)$ only has simple poles at non-positive integers, and $\Gamma(s)$ has no zeros (using the fact $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$). We deduce hence $\zeta(s)$ has only one pole at $s = 1$. □

Lemma 4.1.7. *We have* $w(1/t) = -\frac{1}{2} + \frac{1}{2}t^{\frac{1}{2}} + t^{\frac{1}{2}}w(t)$.

Let $\theta(x) := \sum_{n=-\infty}^\infty e^{-n^2\pi x}$, then $2w(x) = \theta(x) - 1$. It suffices to show $\theta(1/x) = x^{\frac{1}{2}}\theta(x)$.

We first recall some facts on Fourier transform. A function $f : \mathbb{R} \to \mathbb{C}$ is called a Schwartz function, if $f \in \mathcal{C}^\infty$ and f is or rapid decay, i.e. $|f^{(n)}(t)| = o(|t|^c)$ $(t \to \pm\infty)$ for all $n \in Z_{\geq 0}$ and $c \in \mathbb{R}$. Denote by $S(\mathbb{R})$ the space of Schwartz functions.

Example 4.1.8. *The function* $f(x) = e^{-\pi x^2}$ *is a Schwartz function.*

Let $f : \mathbb{R} \to \mathbb{C}$ be an absolutely integrable function (for the Lebesgue measure). The Fourier transform $\widehat{f} : \mathbb{R} \to \mathbb{C}$ is defined by:

$$\widehat{f}(s) := \int_{-\infty}^{+\infty} e^{-2\pi isx}f(x)dx$$

that is a uniformly continuous function. We have the following facts:

- If $f \in S(\mathbb{R})$, then $\widehat{f} \in S(\mathbb{R})$ and $\widehat{f^{(n)}} = (ix)^n \widehat{f}$, $\widehat{x^n f} = i^n \widehat{f}^{(n)}$.
- $\widehat{\widehat{f}}(x) = f(-x)$.
- $\widehat{f * g}(s) = \widehat{f}(s)\widehat{g}(s)$ where $f * g(y) = \int_{-\infty}^{+\infty} f(y-x)g(x)dx$.

Theorem 4.1.9 (Poisson formula)**.** *Let $f : \mathbb{R} \to \mathbb{C}$ be a Schwartz function, then*

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

Proof. Let $F(x) := \sum_{n\in\mathbb{Z}} f(n+x)$. Note since f is Schwartz, the series is absolutely convergent and uniformly continuous for compact sets in $\mathbb{R}$. Hence $F(x)$ is continuous, and $F(x+1) = F(x)$. We have $F(x) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi inx}$ where

$$a_n = \int_0^1 F(x)e^{-2\pi inx}dx = \int_0^1 (\sum_{n\in\mathbb{Z}} f(n+x))e^{-2\pi inx}dx = \int_{-\infty}^{+\infty} f(x)e^{-2\pi inx}dx = \widehat{f}(n).$$

Hence $F(0) = \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)$. □

Let $g(x) = e^{-\pi x^2} \in S(\mathbb{R})$. Then

$$\begin{aligned}\widehat{g}(x) &= \int_{\mathbb{R}} e^{-2\pi ixy}e^{-\pi y^2}dy = \int_{\mathbb{R}} e^{-\pi(y^2+2ixy)}dy \\ &= \int_{\mathbb{R}} e^{-\pi((y+ix)^2+x^2)}dy = e^{-\pi x^2}\int_{\mathbb{R}} e^{-\pi(y+ix)^2}dy = e^{-\pi x^2}\int_{z=ix+\mathbb{R}} e^{-\pi z^2}dz.\end{aligned}$$

We have $|\int_{ix-N}^{ix+N} e^{-\pi z^2}dz - \int_{-N}^{N} e^{-\pi z^2}dz| \le 2|x|e^{-\pi N^2} \to 0$ as $N \to +\infty$. We deduce $\int_{ix+\mathbb{R}} e^{-\pi z^2}dz = \int_{\mathbb{R}} e^{\pi z^2}dz = 1$:

$$\begin{aligned}\int_{\mathbb{R}} e^{\pi z^2}dz = 2\int_0^{+\infty} e^{-\pi z^2}dz &= 2\sqrt{\int_0^{+\infty} e^{-\pi z^2}dz \int_0^{+\infty} e^{-\pi x^2}dx} \\ &= 2\sqrt{\int_0^{+\infty}\int_0^{\frac{\pi}{2}} e^{-\pi r^2}rdrd\theta} = 2\sqrt{\frac{\pi}{2}(-\frac{1}{2\pi}e^{-\pi r^2})|_0^{+\infty}} = 1.\end{aligned}$$

Let $f_t(x) = e^{-\pi x^2 t}$, then $\theta(t) = \sum_{n\in\mathbb{Z}} f_t(n) = \sum_{n\in\mathbb{Z}} \widehat{f}_t(n)$. We have

$$\widehat{f}_t(y) = \int_{\mathbb{R}} e^{-\pi x^2 t}e^{2\pi ixy}dx = \frac{1}{\sqrt{t}}\int_{bR} e^{-\pi x^2}e^{2\pi i\frac{x}{\sqrt{t}}y}dx = \frac{1}{\sqrt{t}}\widehat{g}(y/\sqrt{t}) = \frac{1}{\sqrt{t}}e^{-\pi\frac{y^2}{t}}.$$

Thus $\sum_{n\in\mathbb{Z}} \widehat{f}_t(n) = \frac{1}{\sqrt{t}}\theta(\frac{1}{t})$. Lemma 4.1.7 follows.

Exercise 4.1.10. *Let $\mu(n)$ be the Möbius function:*

$$\mu(n) = \begin{cases}(-1)^{e_n} & n \text{ is square free and } e_n \text{ is the number of prime factors of } n \\ 0 & n \text{ has a squared prime factor}\end{cases}.$$

Prove $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$.

4.2 Prime number theorem

For $x \in \mathbb{R}_{\geq 0}$, denote by $\pi(x) := \#\{p \leq x\}$. In this section, we prove the following famous theorem.

Theorem 4.2.1. *We have* $\pi(x) \sim \frac{x}{\log x}$.

Let $\vartheta(x) := \sum_{p \leq x} \log p$.

Lemma 4.2.2. *If* $\vartheta(x) \sim x$, *then* $\pi(x) \sim \frac{x}{\log(x)}$.

Proof. It is clear that $\vartheta(x) \leq \pi(x)\log(x)$. On the other hand, for any $\epsilon > 0$, $\vartheta(x) \geq \sum_{x^{1-\varepsilon} < p \leq x} \log p \geq (1-\epsilon)\sum_{x^{1-\varepsilon} < p \leq x} \log x = (1-\epsilon)(\log x)(\pi(x) - \pi(x^{1-\epsilon}))$. If $\vartheta(x) \sim x$, then $(\log x)x^{1-\epsilon} = o(\vartheta(x))$. Hence $\vartheta(x) \sim \pi(x)\log x$ and $x \sim \pi(x)\log(x)$. The lemma follows. □

Lemma 4.2.3. *We have* $\vartheta(x) = O(x)$.

Proof. We have

$$2^{2n} \geq \binom{2n}{n} \geq \prod_{n < p \leq 2n} p = e^{\vartheta(2n) - \vartheta(n)}.$$

Hence $\vartheta(2n) - \vartheta(n) \leq 2n \log 2$, thus $\vartheta(2x) - \vartheta(x) = O(2x)$. From which, one easily deduces the lemma. □

Lemma 4.2.4. *If* $\int_1^\infty \frac{\vartheta(x)-x}{x^2} dx$ *exists, then* $\vartheta(x) \sim x$.

Proof. Let $\lambda > 1$, and $x > 0$ such that $\vartheta(x) \geq \lambda x$ then

$$\sum_x^{\lambda x} \frac{\vartheta(t) - t}{t^2} dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2} dt = \int_1^\lambda \frac{\lambda - t}{t^2} dt > 0.$$

Thus if $\int_1^\infty \frac{\vartheta(x)-x}{x^2} dx$ exists, then $\limsup_{x\to\infty} \vartheta(x)/x \leq 1$. Similarly, let $\lambda < 1$, and $x > 0$ such that $\vartheta(x) \leq \lambda x$, then

$$\int_{\lambda x}^x \frac{\vartheta(t) - t}{t^2} \leq \int_{\lambda x}^x \frac{\lambda x - t}{t^2} dt = \int_\lambda^1 \frac{\lambda - t}{t^2} dt < 0.$$

We deduce $\liminf_{x\to\infty} \vartheta(x)/x \geq 1$. The lemma follows. □

Theorem 4.2.5. *Let* $f(t)$ *be a bounded, locally integrable function. Suppose* $g(z) = \int_0^\infty f(t)e^{-zt}dt$ *(that is absolutely convergent and holomorphic for* $\operatorname{Re} z > 0$*) extends holomorphically to* $\operatorname{Re} z \geq 0$. *Then* $\int_0^\infty f(t)dt$ *exists and is equal to* $g(0)$.

We first assume the theorem. To prove $\int_1^\infty \frac{\vartheta(x)-x}{x^2}dx = \int_0^\infty (\frac{\vartheta(e^t)}{e^t}-1)dt$ exists, we are led to study the function

$$\int_0^\infty (\frac{\vartheta(e^t)}{e^t}-1)e^{-st}dt = \int_0^\infty (e^{-(s+1)t}\vartheta(e^t)-e^{-st})dt = \int_0^\infty e^{-(s+1)t}\vartheta(e^t)dt - \frac{1}{s}.$$

We put $\Phi(s) := \sum_p \frac{\log p}{p^s}$ (that is absolutely convergent and holomorphic for $\operatorname{Re} s > 1$).

Lemma 4.2.6. *We have* $\int_0^\infty e^{-(s+1)t}\vartheta(e^t)dt = \frac{\Phi(s+1)}{s+1}$ *(for* $\operatorname{Re} s > 0$*).*

Proof. We have (for $\operatorname{Re} s \gg 0$)

$$\Phi(s) = \sum_{i=1}^\infty \big((\sum_{j\le i}\log p_j)(\frac{1}{p_i^s}-\frac{1}{p_{i+1}^s})\big) = -\sum_{i=1}^\infty \int_{p_i}^{p_{i+1}} \vartheta(x)dx^{-s}$$
$$= s\int_1^\infty \vartheta(x)x^{-s-1}dx = s\int_0^\infty \vartheta(e^t)e^{-st}dt.$$

The lemma follows. □

Lemma 4.2.7. *We have (for* $\operatorname{Re} s > 1$*)*

$$-\frac{\zeta'(s)}{\zeta(s)} = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s-1)}. \tag{4.3}$$

In particular, $\Phi(s)$ *can extend to a meromorphic functor on* $\operatorname{Re} z > \frac{1}{2}$*, that has a simple at* $s=1$ *with residue* 1*.*

Proof. We have

$$\big(\prod_{p\le p_N}(1-p^{-s})^{-1}\big)' = \sum_{p\le p_N}\big(-\prod_{\substack{p'\le p_N\\ p'\ne p}}(1-(p')^{-s})^{-1}(1-p^{-s})^{-2}p^{-s}\log p\big)$$
$$= -\sum_{p\le p_N}(1-p^{-s})^{-1}\sum_{p\le p_N}\frac{\log p}{p^s-1}.$$

Thus for $\operatorname{Re} s > 1$:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p}{p^s-1} = \Phi(s) + \sum_p \big(\frac{\log p}{p^s-1} - \frac{\log p}{p^s}\big) = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s-1)}.$$

The function $\sum_p \frac{\log p}{p^s(p^s-1)}$ is holomorphic on $\operatorname{Re} s > \frac{1}{2}$. Recall also $\zeta(s)$ is also meromorphic on $\operatorname{Re} s > \frac{1}{2}$ and has a simple pole at $s=1$ with residue 1. The lemma follows. □

Now we want to show $\frac{\Phi(s+1)}{s+1} - \frac{1}{s}$ can extend holomorphically on $\operatorname{Re} s \ge 0$. By the above lemma, it is sufficient to show $\Phi(s)$ has no other poles on $\operatorname{Re} s = 1$ (except for $s=1$). Again by (4.3), this is equivalent to the statement in the following proposition.

Proposition 4.2.8. *We have $\zeta(s) \neq 0$ for any $\operatorname{Re} s = 1$ and $s \neq 1$.*

Proof. First by (4.2) (or (4.1)), if $\zeta(s) = 0$, then $\zeta(\bar{s}) = 0$ for $\operatorname{Re} s > 0$. Suppose $1 + \alpha i$ is a zero of $\zeta(s)$ of order λ, and $1 + 2\alpha i$ is a zero of $\zeta(s)$ of order μ (with μ, $\nu \in \mathbb{Z}_{\geq 0}$, $\alpha \in \mathbb{R}^*$). Then $\lim_{\epsilon \to 0} \epsilon \Phi(1 \pm \alpha i + \epsilon) = -\lambda$, and $\lim_{\epsilon \to 0} \epsilon \Phi(1 \pm 2\alpha i + \epsilon) = -\mu$. Let $\epsilon > 0$, consider

$$\sum_{j=-2}^{2} \binom{4}{2+j} \Phi(1 \pm j\alpha i + \epsilon) = \sum_{j=-2}^{2} \binom{4}{2+j} (\sum_{p} \frac{\log p}{p^{1 \pm j\alpha i + \epsilon}} = \sum_{p} \frac{\log p}{p^{1+\epsilon}} (p^{\frac{\alpha}{2} i} + p^{-\frac{\alpha}{2} i})^4 > 0.$$

We deduce $\lim_{\epsilon \to 0} \epsilon (\sum_{j=-2}^{2} \binom{4}{2+j} \Phi(1 \pm j\alpha i + \epsilon)) \geq 0$. However, we have (recall $\lim_{\epsilon} \epsilon \Phi(1 + \epsilon) = 1$)

$$\lim_{\epsilon \to 0} \epsilon (\sum_{j=-2}^{2} \binom{4}{2+j} \Phi(1 \pm j\alpha i + \epsilon)) = -8\lambda - 2\mu + 6,$$

and hence $\lambda = 0$. The proposition follows. □

As discussed above, Theorem 4.2.1 follows from the proposition. We finally prove the analytic theorem:

Proof of Theorem 4.2.5. For $T > 0$, let $g_T(z) := \int_0^T f(t) e^{-zt} dt$, that is holomolorphic on $\mathbb{C}$. We need to show $\lim_{T \to \infty} (g_T(0) - g(0)) = 0$. Let $R > 0$, and let $\delta > 0$ such that $g(z)$ is holomorphic on the region $\Omega := \{\operatorname{Re} z > \delta\} \cap \{|z| < R\}$ (so δ depends on R). Let- C be the boundary of Ω. We have thus

$$g_T(0) - g(0) = \frac{1}{2\pi i} \int_C (g_T(z) - g(z)) e^{zT} (1 + \frac{z^2}{R^2}) \frac{dz}{z}.$$

Let $C^+ := C \cap \{\operatorname{Re} z > 0\}$, and $B := \sup |f(t)|$. Then for $z \in C^+$, we have

$$|g_T(z) - g(z)| = |\int_T^{\infty} f(t) e^{-zt} dt| \leq B \frac{e^{-\operatorname{Re} zT}}{\operatorname{Re} z};$$

and (noting $R^2 = z\bar{z}$)

$$|e^{zT} (1 + \frac{z^2}{R^2}) \frac{1}{z}| = e^{\operatorname{Re} zT} \frac{1}{R^2} |z + \bar{z}| = 2 e^{\operatorname{Re} zT} \frac{1}{R^2} \operatorname{Re} z. \tag{4.4}$$

So $|\int_{C^+} (g_T(z) - g(z)) e^{zT} (1 + \frac{z^2}{R^2}) \frac{dz}{z}| \leq 2\pi \frac{B}{R}$. Let $C^- := C \cap \{\operatorname{Re} z < 0\}$, and $C_1^- := \{|z| = R, \operatorname{Re} z < 0\}$. Since $g_T(z) e^{zT} (1 + \frac{z^2}{R^2}) \frac{1}{z}$ is holomorphic,

$$\int_{C^-} g_T(z) e^{zT} (1 + \frac{z^2}{R^2}) \frac{dz}{z} = \int_{C_1^-} g_T(z) e^{zT} (1 + \frac{z^2}{R^2}) \frac{dz}{z}.$$

For $z \in C_1^-$, we have

$$|g_T(z)| \leq B \int_{-\infty}^{T} |e^{-zt}| dt = B \frac{e^{-\operatorname{Re} zT}}{|\operatorname{Re} z|},$$

and (4.4) holds. Hence $|\int_{C^-} g_T(z) e^{zT} (1 + \frac{z^2}{R^2}) \frac{dz}{z}| \leq 2\pi \frac{B}{R}$. The only left term is $\int_{C^-} g(z) e^{zT} (1 + \frac{z^2}{R^2}) \frac{1}{z} dz$, that goes to zero when $T \to \infty$ (since $\operatorname{Re} z < 0$, e.g. using $g(z)(1 + \frac{z^2}{R^2})/z$ is bounded on C^-). We deduce then $\limsup_{T \to \infty} |g_T(0) - g(0)| \leq 2B/R$. As R is arbitrary, the theorem follows. □

4.3 Dedekind Zeta functions

Let K be a number field. Put $\zeta_K(s) := \sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}$.

Lemma 4.3.1. *The series $\sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}$ is absolutely and uniformly convergent on any compact subset of $\operatorname{Re} s > 1$, and we have*

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}.$$

Proof. We first show $\prod_{\mathfrak{p}}(1 - N(\mathfrak{p})^{-s})^{-1}$ is absolutely and uniformly convergent on any compact subset of $\operatorname{Re} s > 1$. It is sufficient show the same convergence for $\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}$. For any prime number p, there are at most $[K : \mathbb{Q}_p]$-prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) = p$. We deduce that for $\operatorname{Re} s > 1$ (noting $|p^{-ms}| \leq |p^{-s}|$ for $m \in \mathbb{Z}_{\geq 1}$):

$$|\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}| \leq \sum_{\mathfrak{p}} |\frac{1}{N(\mathfrak{p})^s}| \leq \sum_{p} |\frac{[K:\mathbb{Q}]}{p^s}| = \sum_{p} \frac{[K:\mathbb{Q}]}{p^{\operatorname{Re} s}}.$$

The convergence then follows from the same result for $\zeta(s)$. The power series $\sum_{m=0}^{\infty} N(\mathfrak{p})^{-ms}$ is also absolutely and uniformly convergent on any compact subset of $\operatorname{Re} s > 1$. We have then

$$g_n(s) := \prod_{\mathfrak{p}, N(\mathfrak{p})\leq n} (1 - N(\mathfrak{p})^{-s})^{-1} = \prod_{\mathfrak{p}, N(\mathfrak{p})\leq n} (\sum_{m=0}^{\infty} N(\mathfrak{p})^{-ms}) = \sum_{\mathfrak{a}\in I_n} \frac{1}{N(\mathfrak{a})^s}$$

where I_n denotes the set of ideals $\mathfrak{a}$ satisfying all the prime factors of $\mathfrak{a}$ has norm at most n. And $\{g_n(s)\}$ is absolutely and uniformly convergent on any compact subset of $\operatorname{Re} s > 1$. We then deduce the same holds for $\zeta_K(s)$. □

Proposition 4.3.2. *Let $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ that absolutely converges for $\operatorname{Re} s$ sufficiently large. Let $S_t = \sum_{n\leq t} a_n$ for $t > 0$. Suppose there exists $\kappa \in \mathbb{C}$ and $0 < \delta \leq 1$ such that $S_t = \kappa t + O(t^{1-\delta})$ as $t \to +\infty$. Then $f(s)$ can extend to a meromorphic function on $\operatorname{Re} s > 1 - \delta$ with only one simple pole at $s = 1$ with residue κ.*

Proof. Consider $f(s) - \kappa\zeta(s) =: \sum_n \frac{b_n}{n^s}$, and put $S'_t := \sum_{n\leq t} b_n$. So $S'_t = O(t^{1-\delta})$. It is sufficient to show $\sum_n \frac{b_n}{n^s}$ can extend to a holomorphic function on $\operatorname{Re} s > 1 - \delta$. First, $\sum_n \frac{b_n}{n^s}$ is absolutely convergent for $\operatorname{Re} s$ sufficiently large. We have thus for $\operatorname{Re} s \gg 0$:

$$\begin{aligned}\sum_n \frac{b_n}{n^s} = \sum_n \frac{S'_n - S'_{n-1}}{n^s} &= \sum_n \frac{S'_n}{n^s} - \sum_n \frac{S'_n}{(n+1)^s} \\ &= \sum_n (S'_n \int_n^{n+1} \frac{s}{x^{s+1}} dx) = s \sum_n (S'_n \int_n^{n+1} x^{-s-1} dx).\end{aligned}$$

Let $C > 0$ such that $S_t \leq Ct^{1-\delta}$, we have

$$\sum_n |S'_n \int_n^{n+1} x^{-s-1} dx| \leq C|s| \sum_n \int_n^{n+1} x^{-s-\delta} dx = C|s| \int_1^{\infty} x^{-s-\delta} dx$$

that is absolutely convergent for $\operatorname{Re} s > 1 - \delta$. The proposition follows. □

We want to apply the proposition to Dedekind zeta functions. We can write $\zeta_K(s) = \sum_n \frac{a_n}{n^s}$, where $a_n = \#\{\mathfrak{a} \subset \mathcal{O}_K \mid N(\mathfrak{a}) = n\}$. We see $S(t) = \sum_{n \le t} a_n = \#\{\mathfrak{a} \subset \mathcal{O}_K \mid N(\mathfrak{a}) \le n\}$. In the rest of the section, we will prove

Theorem 4.3.3. *Keep the above notation, then*

$$S(t) = \frac{2^r(2\pi)^s R_K h_K}{w\sqrt{|\Delta_K|}} t + O(t^{1-\frac{1}{n}}),$$

where R_K is the regulator of K (that will be defined later), h_K is the class number of K, $w = |\mu_K|$, Δ_K is the discriminant of K.

Corollary 4.3.4. *The function $\zeta_K(s)$ can extend to a meromorphic function on $\operatorname{Re} s > 1 - \frac{1}{n}$, that only has a simple pole at $s = 1$ of residue $\frac{2^r(2\pi)^s R_K h_K}{w\sqrt{|\Delta_K|}}$.*

Let $\mathscr{C}$ be an ideal class in C_K. We will estimate $\#\{\mathfrak{a} \subset \mathcal{O}_K \mid [\mathfrak{a}] = \mathscr{C},\ N(\mathfrak{a}) \le t\} = N_{\mathscr{C}}(t)$.

Lemma 4.3.5. *Let J be a fractional ideal such that $[J^{-1}] = \mathscr{C}$. Then the following map is a bijection*

$$\{\alpha \in J \mid N(\alpha) \le tN(J)\}/\mathcal{O}_K^\times \to \{\mathfrak{a} \subset \mathcal{O}_K \mid [\mathfrak{a}] = \mathscr{C},\ N(\mathfrak{a}) \le t\}, \alpha \mapsto \alpha J^{-1}.$$

Proof. The map is clearly well-defined and injective. For $\mathfrak{a} \subset \mathcal{O}_K$ such that $[\mathfrak{a}] = \mathscr{C}$ and $N(\mathfrak{a}) \le t$, there exists $\alpha \in K^\times$ such that $\mathfrak{a} = \alpha J^{-1}$. Since $\mathfrak{a} \subset \mathcal{O}_K$, $\alpha \in J$. Using $N(\mathfrak{a}) = N(\alpha)N(J)^{-1}$, $N(\alpha) \le tN(J)$. The surjectivity follows. □

We discuss some examples on the calculation of $N_{\mathscr{C}}(t)$.

Example 4.3.6. *(1) Suppose $K/\mathbb{Q}$ is an imaginary quadratic field. Let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding. Recall $\sigma(J)$ is a lattice in $\mathbb{C} \cong \mathbb{R}^2$, and we have $\operatorname{Vol}(\mathbb{R}^2/\sigma(J)) = \frac{1}{2}N(J)\sqrt{|\Delta_K|}$ (where $\operatorname{Vol}(.)$ is with respect to the standard Lebesgue measure on $\mathbb{C}$, and hence is equal to $\operatorname{Vol}_0(.)$ in §1.7). We need to estimate $m_{N(J)t} := \#(\sigma(J) \cap \{x \mid |x|^2 \le N(J)t\})$. Let e_1, e_2 be a basis of $\lambda(J)$, and $\Omega = \{x_1e_1 + x_2e_2 \mid x_i \in (-1/2, 1/2]\}$. For $s > 0$, denote by m_s^+ (resp. m_s^-) be the cardinality of the set consisting of $\alpha \in J$ such that $(\alpha + \Omega) \cap \{x \mid |x|^2 \le s\} \ne \emptyset$ (resp. such that $(\alpha + \Omega) \subset \{x \mid |x|^2 \le s\}$). We have $m_s^- \le \pi s^2 / \operatorname{Vol}(\mathbb{R}^2/\sigma(J)) = \frac{2\pi s^2}{N(J)\sqrt{|\Delta_K|}}$ and $m_s^+ \ge \frac{2\pi s^2}{N(J)\sqrt{|\Delta_K|}}$. Let $\delta := \sup_{x,y\in\Omega} |x - y|$, then*

$$m^+_{((N(J)t)^{1/2}-\delta)^2} \le m^-_{N(J)t} \le m_{N(J)t} \le m^+_{N(J)t} \le m^-_{((N(J)t)^{1/2}+\delta)^2}.$$

We deduce thus $m_{N(J)t} = \frac{2\pi}{\sqrt{|\Delta_K|}} + O(t^{1/2})$ and hence $N_{\mathscr{C}}(t) = \frac{2\pi}{w\sqrt{|\Delta_K|}} t + O(t^{1/2})$.

(2) Suppose $K/\mathbb{Q}$ is a real quadratic field. Let $\lambda : K \hookrightarrow \mathbb{R}^2$, $\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha))$. Let $\varepsilon \in \mathcal{O}_K^\times$ be a fundamental unit, and we assume $\sigma_1(\varepsilon) > 1$ (hence $|\sigma_2(\varepsilon)| < 1$). For

any $x=(x_1,x_2)\in\mathbb{R}$ *with* $x_1x_2\neq 0$, *there exists thus a unique* $y=(y_1,y_2)$ *such that* $1<\frac{|y_1|}{|y_2|}\leq\frac{\sigma_1(\varepsilon)}{|\sigma_2(\varepsilon)|}=\sigma_1(\varepsilon)^2$ *and* $xy^{-1}\in\varepsilon^{\mathbb{Z}}$. *We deduce hence a bijection*

$$\begin{aligned}&\big(\lambda(J)\cap\{(x_1,x_2)\mid |x_1x_2|\leq N(J)t\}\big)/\mathcal{O}_K^\times\\ \longleftrightarrow\quad &\big(\lambda(J)\cap\{(x_1,x_2)\mid |x_1x_2|\leq N(J)t, 1<|\frac{x_1}{x_2}|<\sigma_1(\varepsilon)^2\}\big)/\mu_K.\end{aligned}$$

Let $D_t:=\{(x_1,x_2)\mid |x_1x_2|\leq N(J)t, 1<|\frac{x_1}{x_2}|<\sigma_1(\varepsilon)^2\}$. *We see the length* $|\partial D_t|=O(t^{\frac{1}{2}})$. *We can find* $[|\partial D_t|]$*-points* $\{x_i\}$ *on* ∂D_t, *such that for any* $x\in\partial D_t$, $|x-x_i|\leq 1$ *for some* x_i. *As in (1), let* α_1, α_2 *be a basis of* $\lambda(J)$, *and* $\Omega:=\{x_1\alpha_1+x_2\alpha_2\mid |x_i|\leq 1/2\}$. *We see if* r *is sufficiently large (depending on* Ω*), then* $\lambda(J)\cap D_t$ *is bigger than the number* M_1 *of elements* α *in* J *such that* $\alpha+\Omega\cap D_t\setminus(\cup_i B(x_i,r))\neq\emptyset$, *and is smaller than the number* M_2 *of elements* α *in* J *such that* $\alpha+\Omega\subset D_t\cup(\cup_i B(x_i,r))$. *We have* $M_1\geq(\mu(D_t)-\sum_i\pi r^2)/\operatorname{Vol}(\mathbb{R}^2/\lambda(J))$, *and* $M_2\leq(\mu(D_t)+\sum_i\pi r^2)/\operatorname{Vol}(\mathbb{R}^2/\lambda(J))$. *Note that the term* $\sum_i\pi r^2/\operatorname{Vol}(\mathbb{R}^2/\lambda(J))=O(t^{\frac{1}{2}})$. *For* D_t, *we have*

$$\begin{aligned}\mu(D_t)=4\int_{\substack{0<x_1x_2\leq N(J)t,x_i>0\\ 1<\frac{x_1}{x_2}\leq\sigma_1(\varepsilon)^2}}dx_1dx_2&=4\int_{\substack{y_1+y_2\leq\log(N(J)t)\\ 0<y_1-y_2\leq 2\log(\sigma_1(\varepsilon))}}e^{y_1+y_2}dy_1dy_2\\ &=2\int_{\substack{z_1\leq\log(N(J)t)\\ 0<z_2\leq 2\log(\sigma_1(\varepsilon))}}e^{z_1}dz_1dz_2=4N(J)\log(\sigma_1(\varepsilon))t.\end{aligned}$$

Together with $\operatorname{Vol}(\mathbb{R}^2/\lambda(J))=N(J)\sqrt{|\Delta_K|}$, *we deduce* $N_{\mathscr{C}}(t)=\frac{2\pi}{\sqrt{|\Delta_K|}}t+O(t^{\frac{1}{2}})$.

To prove the theorem for general K, we start with some preliminaries.

Definition 4.3.7. *(1) A function* $f:[0,1]^{n-1}\to\mathbb{R}^n$ *is called Lipschitz, if the ratio* $\frac{|f(x)-f(y)|}{|x-y|}$ *is uniformly bounded for* $x\neq y\in[0,1]^{n-1}$.

(2) Let B *be a bounded region in* $\mathbb{R}^n$. *We call* $\partial B=\overline{B}\setminus B^o$ *is* $(n-1)$*-Lipschitz parametrizable, if it is covered by the images of finitely many Lipschitz functions:* $f:[0,1]^{n-1}\to\mathbb{R}^n$.

Lemma 4.3.8. *Let* B *be a bounded region in* $\mathbb{R}^n$ *such that* ∂B *is* $(n-1)$*-Lipschitz parametrizable, and* $\Lambda\subset\mathbb{R}^n$ *be a complete lattice. Then for* $a>1$, *we have*

$$\#(\Lambda\cap aB)=\frac{\mu(B)}{\operatorname{Vol}(\mathbb{R}^n/\Lambda)}a^n+O(a^{n-1}).$$

Proof. We give a sketch of the proof. First the map $x\mapsto ax$ induces a bijection between $(\frac{1}{a}\Lambda)\cap B\to\Lambda\cap aB$. Let $e_1,\cdots,e_n$ be a basis of Λ, and $\Omega:=\{\sum_i x_ie_i\mid -\frac{1}{2a}<x_i\leq\frac{1}{2a}\}$. Since ∂B is $(n-1)$-Lipschitz parametrizable, for any $r>0$, there exists M_r-points $\{x_i\}$ such that $M_r=O(a^{n-1})$ and for any $x\in\partial B$, there exists x_i such that $|x-x_i|<\frac{r}{a}$. We can then choose r (independent of a) and $M=O(a^{n-1})$-points $\{x_i\}$, such that if $(\alpha+\Omega)\cap\partial B\neq\emptyset$, then $(\alpha+\Omega)\subset B(x_i,r/a)$ for some x_i. Similarly as in Example 4.3.6, we have

$$\frac{\mu(B\setminus\cup_iB(x_i,r/a))}{\mu(\Omega)}\leq\#(\frac{1}{a}\Lambda)\cap B\leq\frac{\mu(B\cup(\cup_iB(x_i,r/a))}{\mu(\Omega)}.$$

Using $\frac{\mu(B)}{\mu(\Omega)} = \frac{\mu(B)}{\mathrm{Vol}(\mathbb{R}^n/\Lambda)}a^n$, and $\frac{\mu(\cup_i B(x_i, r/a))}{\mu(\Omega)} = O(a^{n-1})$, the lemma follows. □

We now calculate $\#\big(J \cap \{\alpha \in K \mid N(\alpha) \leq tN(J)\}\big)/\mathcal{O}_K^\times$. Let $\lambda : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$, $x \mapsto (\sigma_1(x), \cdots, \sigma_r(x), \sigma_{r+1}(x), \cdots, \sigma_{r+s}(x))$. Let $\varepsilon_1, \cdots, \varepsilon_{r+s-1}$ be a set of fundamental units (that are a basis of $\mathcal{O}_K^\times/\mu_K$). Consider

$$\begin{array}{ccc} \mathcal{O}_K^\times & \xrightarrow{\lambda} & \mathbb{R}^r \times \mathbb{C}^s \\ {\scriptstyle \ell}\downarrow & & \downarrow{\scriptstyle \mathrm{Log}} \\ H & \longrightarrow & \mathbb{R}^{r+s} \end{array}$$

where $\mathrm{Log}(x_1, \cdots, x_s) := (\log|x_1|, \cdots, \log|x_r|, 2\log|x_{r+1}|, \cdots, 2\log|x_{r+s}|)$, and where H is the hyperplane of $\mathbb{R}^{r+s}$ defined by $\sum_{i=1}^{r+s} x_i = 0$. Recall $\ell(\mathcal{O}_K^\times)$ is a complete lattice in H. Let $X_t := \big(J \cap \{\alpha \in K \mid N(\alpha) \leq tN(J)\}\big)$, and $X_t^* := X_t \setminus \{0\}$. The image of the region X_t^* under the morphism Log is the region $X_t^{\mathrm{Log}} := \{(x_i) \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r+s} x_i \leq \log(tN(J))\}$. The natural $\mathcal{O}_K^\times$-action on X_t^* transfers to an $\ell(\mathcal{O}_K^\times)$-action on X_t^{Log} by addition. Put $v := \frac{1}{r+s}(1, \cdots, 1) \in bR^{r+s}$, then $(v, \ell(\varepsilon_1), \cdots, \ell(\varepsilon_{r+s-1}))$ form a basis of $\mathbb{R}^{r+s}$. Let $D_t^{\mathrm{Log}} := \{t_0 v + \sum_{i=1}^{r+s-1} t_i \ell(\varepsilon_i) \mid t_0 \in (-\infty, \log(tN(J))), t_i \in [0,1)\}$.

Lemma 4.3.9. *For any $x \in X_t^{\mathrm{Log}}$, there exists a unique $y \in D_t^{\mathrm{Log}}$ such that $x - y \in \ell(\mathcal{O}_K^\times)$.*

Proof. The lemma follows easily from the fact $\{\sum_{i=1}^{r+s-1} t_i \ell(\varepsilon_i) \mid t_i \in [0,1)\}$ is a fundamental mesh of the lattice $\oplus\mathbb{Z}\ell(\varepsilon_i)$ in H. □

Let $D_t \subset X_t^*$ be the inverse image of D_t^{Log} under the morphism Log. By Lemma 4.3.9, we have

Lemma 4.3.10. *For any $x \in X_t^*$, there exists a unique $y \in D_t$ such that $xy^{-1} \in \prod_{i=1}^{r+s-1} \varepsilon_i^{\mathbb{Z}} \hookrightarrow \mathcal{O}_K^\times$.*

Consequently, we have a bijection

$$\big(J \cap \{\alpha \in K \mid N(\alpha) \leq tN(J)\}\big)/\mathcal{O}_K^\times \longleftrightarrow (\lambda(J) \cap D_t)/\mu_K.$$

We have $D_t = t^{\frac{1}{n}} D_1$ and ∂D is $(n-1)$-Lipschitz. By Lemma 4.3.8, we have

$$N_C(t) = \frac{\mu(D_1)}{|\mu_K| \,\mathrm{Vol}(\mathbb{R}^n/\lambda(J))} + O(t^{1-\frac{1}{n}}).$$

We have $\mathrm{Vol}(\mathbb{R}^n/\lambda(J)) = 2^{-s}\sqrt{|\Delta_K|}N(J)$. Now we calculate $\mu(D_1)$:

$$\mu(D_1) = \int_{D_1} dy_1 \cdots dy_r dz_1, \cdots dz_s.$$

Writing $z_j = \rho_j e^{i\theta_j}$ then $x_i = \log|y_i|$ for $1 \leq i \leq r$, and $x_i = 2\log\rho_i$ for $r+1 \leq i \leq r+s$, we have

$$\mu(D_1) = \int_{D_1} dy_1 \cdots dy_r \rho_1 \cdots \rho_s d\rho_1 \cdots d\rho_s d\theta_1 \cdots d\theta_s = 2^r \pi^s \int_{D_1^{\mathrm{Log}}} e^{\sum_{i=1}^{r+s} x_i} dx_1 \cdots dx_{r+s}.$$

Let $t_0, \cdots, t_{r+s-1}$ be the new variables such that

$$(x_1, \cdots, x_{r+s})^T = (v, \ell(\varepsilon_1), \cdots, \ell(\varepsilon_{r+s-1}))(t_0, \cdots, t_{r+s-1})$$

then we have

$$\mu(D_1) = |\det(v, \ell(\varepsilon_1), \cdots, \ell(\varepsilon_{r+s-1}))| \int_{-\infty}^{\log(tN(J))} e^{t_0} \prod_{i=1}^{r+s-1} \int_0^1 dt_i.$$

We define $R_K := |\det(v, \ell(\varepsilon_1), \cdots, \ell(\varepsilon_{r+s-1}))|$, called the regulator of K. We see that R_K is independent of the choice of the fundamental units, and is unchanged if v is replaced by any vector $(x_1, \cdots, x_{r+s}) \in \mathbb{R}^{r+s}$ such that $\sum_{i=1}^{r+s} x_i = 1$. Thus $\mu(D_1) = 2^r \pi^s R_K N(J)$ and the theorem follows.

4.4 Dirichlet L-functions

We first discuss characters of finite groups. Let G be a finite abelian group, we let $\widehat{G} := \{\chi : G \to \mathbb{C}^\times\}$ be the set of characters of G. Then $\widehat{G}$ has a natural (abelian) group structure: $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$.

Lemma 4.4.1. *(1) We have a (non-canonical) isomoprhism $\widehat{G} \cong G$.*

(2) Given an exact sequence $1 \to H \to G \to G/H \to 1$, the induced sequence $1 \to \widehat{G/H} \to \widehat{G} \to \widehat{H} \to 1$ is exact.

(3) The morphism $G \to \widehat{\widehat{G}}$, $g \mapsto (\chi \mapsto \chi(g))$ is an isomorphism.

Proof. (1) By the structure theorem of finite abelian groups, it suffices to show $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$. However, it is clear that $\chi \in \widehat{\mathbb{Z}/n\mathbb{Z}}$ is determined by $\chi(1) \in \mu_n(\mathbb{C}) = \{\zeta \in \mathbb{C}^\times \mid \zeta^n = 1\}$.

(2) One directly checks that the sequence $1 \to \widehat{G/H} \to \widehat{G} \to \widehat{H}$ is exact. By comparing the orders and using (1), we deduce $\widehat{G} \to \widehat{H}$ is surjective.

(3) Both of the groups having the same order, it suffices to show the morphism is injective. Let $H := \cap_{\chi \in \widehat{G}} \mathrm{Ker}(\chi)$. Since $\widehat{G} \to \widehat{H}$ is surjective by (2), we see $H = 1$ and the injectivity follows. □

Proposition 4.4.2. *Let $\chi \in \widehat{G}$, $\chi \neq 1$, then $\sum_{g \in G} \chi(g) = 0$*

Proof. Let $h \in G$ such that $\chi(h) \neq 1$, then $\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g)$. The proposition follows. □

Remark 4.4.3. *Using the canonical isomorphism $G \cong \widehat{\widehat{G}}$, we see for $g \neq 1$, $\sum_{\chi \in \widehat{G}} \chi(g) = 0$.*

Let $N \in \mathbb{Z}_{>1}$, and we call a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a Dirichlet character. If $m|N$, we have a natural (surjective) morphism $(\mathbb{Z}/N\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$. A Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is called primitive if χ is not induced from a character $(\mathbb{Z}/m\mathbb{Z})^\times$ for $m|N$, $m \neq N$ (i.e. $\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$ does not lie in the image of $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times} \hookrightarrow \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$ for $m|N$, $m \neq N$). In this case, we call N the conductor of χ, denoted by f_χ. We call χ even if $\chi(-1) = 1$ and odd if $\chi(-1) = -1$.

Let χ be a Dirichlet character of conductor f_χ, we extend χ to a morphism $\chi : \mathbb{Z} \to \mathbb{C}$ such that

$$\chi(a) = \begin{cases} \chi(\overline{a}) & (a, f_\chi) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We put $L(\chi, s) := \sum_{n=1}^\infty \frac{\chi(n)}{n^s}$, called Dirichlet L-function. It is easy to see $\sum_{n=1}^\infty \frac{\chi(n)}{n^s}$ is absolutely convergent on $\operatorname{Re} s > 1$, and hence $L(\chi, s)$ is holomorphic on $\operatorname{Re} s > 1$. By similar arguments as in Proposition 4.1.4, we also have for $\operatorname{Re} s > 1$,

$$L(\chi, s) = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

Proposition 4.4.4. *If $\chi \neq 1$, then $L(\chi, s)$ can extend to a holomorphic function on $\operatorname{Re} s > 0$.*

Proof. By Proposition 4.4.2, the absolute value of $S_t := \sum_{n \leq t} \chi(n)$ is bounded by f_χ. The proposition then follows from Proposition 4.3.2 (with $\kappa = 0$, $\delta = 1$). □

We study the relation between Dirichlet L-functions and Dedekind zeta functions. Let K be a finite extension of $\mathbb{Q}$, and suppose there exists N such that $K \subset \mathbb{Q}(\zeta_N)$ (ζ_N being a primitive N-th root of unity). Note by the theorem of Kronecker-Weber, this is equivalent to that K is a finite abelian extension of $\mathbb{Q}$. Recall we have $\iota_N : \operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$ such that $g(\zeta_N) = \zeta_N^{\iota(g)}$. Let $H := \operatorname{Gal}(K/\mathbb{Q})$, then we have a natural morphism $(\mathbb{Z}/N\mathbb{Z})^\times \cong \operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \twoheadrightarrow H$, that induces $\jmath : \widehat{H} \hookrightarrow \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$ (we omit $\jmath$ if there is no ambiguity). In particular, any character of H is a Dirichlet character (of conductor dividing N).

Theorem 4.4.5. *We have*

$$\prod_{\chi \in \widehat{H}} L(\chi, s) = \zeta_K(s). \tag{4.5}$$

Proof. It suffices to prove the equality for $\operatorname{Re} s \gg 0$. Using the formulas of Euler product for both $L(\chi, s)$ and $\zeta_K(s)$, we reduce to show

$$\prod_{\chi \in \widehat{H}} (1 - \chi(p)p^{-s}) = \prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s}) \tag{4.6}$$

for all prime number p.

We first show some facts on cyclotomic field. For a prime number p, we have

- if $p \nmid N$, then p is unramified in $\mathbb{Q}(\zeta_N)$,
- if $N = p^r$, then p is totally ramified in $\mathbb{Q}(\zeta_N)$.

Indeed, to see these, we consider the extension $\mathbb{Q}_p(\zeta_N)$ over $\mathbb{Q}_p$. If $p \nmid N$, using Hensel's lemma it is easy to see $\mathbb{Q}_p(\zeta_N)$ is unramified over $\mathbb{Q}_p$. If $N = p^r$, by Exercise 2.7.5, $\mathbb{Q}_p(\zeta_{p^r})$ is totally ramified over $\mathbb{Q}_p$. Suppose $p \nmid N$, then the decomposition group $D_p \subset \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is generated by the absolute Frobenius Frob_p, i.e. the element satisfying $\mathrm{Frob}_p(x) \equiv x^p \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_{\mathbb{Q}(\zeta_N)}$ and $\mathfrak{p} \subset \mathcal{O}_{\mathbb{Q}(\zeta_N)}$ dividing p (actually, one can show that $\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_N]$, but we don't need this fact). We claim Frob_p is the element sending ζ_N to ζ_N^p. Suppose $\mathrm{Frob}_p(\zeta_N) = \zeta_N^r$ for $r \in (\mathbb{Z}/NZ)^\times$, and suppose $r \neq p \pmod{N}$. By assumption, $\zeta_N^r - \zeta_N^p \in \mathfrak{p}$ for $\mathfrak{p}|p$. However, in $\mathbb{Q}_p(\zeta_N)$, we see easily that $\zeta_N^r - \zeta_N^p$ is a unit, a contradiction. We conclude that the map $\iota_N : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/Q) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$ sends Frob_p to p.

Back to the proof of (4.6). First consider the case $p \nmid N$. For (any) $\mathfrak{p}|p$, denote by $f := [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$, and hence $N(\mathfrak{p}) = p^f$. Let $g := d/f$ ($d = [K : \mathbb{Q}]$). Then $\prod_{\mathfrak{p}|p}(1 - N(\mathfrak{p})^{-s}) = (1 - p^{-fs})^g$. We calculate now $\prod_{\chi \in \widehat{H}}(1 - \chi(p)p^{-s})$. We have

$$\widehat{D_p} \twoheadleftarrow \widehat{H} \hookrightarrow \mathrm{Gal}(\widehat{\mathbb{Q}(\zeta_N)}/\mathbb{Q}) \underset{\sim}{\overset{\iota_N}{\leftarrow}} (\widehat{\mathbb{Z}/N\mathbb{Z}})^\times.$$

We have $\chi(p) = \chi(\mathrm{Frob}_p)$ for $\chi \in \widehat{H}$, in particular, $\chi(p) = \chi|_{D_p}(\mathrm{Frob}_p)$. Thus $\prod_{\chi \in \widehat{H}}(1 - \chi(p)p^{-s}) = \prod_{\chi_0 \in \widehat{D_p}}(1 - \chi_0(\mathrm{Frob}_p)p^{-s})^g$. Since D_p is a cyclic group of order f generated by Frob_p, we have $\{\chi_0(\mathrm{Frob}_p) \mid \chi_0 \in \widehat{D_p}\} = \{\zeta_f^i \mid i = 0, \cdots, f-1\}$. We have

$$\prod_{\chi_0 \in \widehat{D_p}} (1 - \chi_0(\mathrm{Frob}_p)p^{-s})^g = \prod_{i=0}^{f-1}(1 - \zeta_f^i p^{-s})^g = (1 - p^{-fs})^g,$$

where the last equation follows from $(1 - X^f) = \prod_{i=0}^{f-1}(1 - \zeta_f^i X)$. The equation in (4.6) follows in this case.

Consider the case $p|N$. We write $N = p^r M$ with $(p, M) = 1$. Let $K_M := K \cap \mathbb{Q}(\zeta_M)$. For any prime ideal $\mathfrak{p}_M$ of $\mathcal{O}_{K_M}$ dividing p, $\mathfrak{p}_M$ is totally ramified in K (for example by looking at the corresponding extensions with $\mathbb{Q}$ replaced by $\mathbb{Q}_p$). In fact $\mathrm{Gal}(K/K_M) \subset H$ is exactly the inertial group I_p at p. For the prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, $\mathfrak{P}|\mathfrak{p}_M$, we have $N(\mathfrak{P}) = \#\mathcal{O}_K/\mathfrak{P} = \#\mathcal{O}_{K_M}/\mathfrak{p}_M = N(\mathfrak{p}_M)$. Hence $\prod_{\mathfrak{p}|p}(1-N(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p}_M|p}(1-N(\mathfrak{p}_M)^{-s})$. We have $(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p^r\mathbb{Z})^\times \times (\mathbb{Z}/M\mathbb{Z})^\times$, and by definition $\chi(p) \neq 0$ if and only if $\chi|_{(\mathbb{Z}/p^r\mathbb{Z})^\times} = 1$. We have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_{p^r})) & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K/K_M) & \longrightarrow & \mathrm{Gal}(K/\mathbb{Q}) \end{array}$$

Hence for $\chi \in \widehat{H}$, $\chi(p) \neq 0$ if and only if χ is trivial on $I_p \cong \mathrm{Gal}(K/K_M)$. Then by Lemma 4.4.1 (2), this is equivalent to $\chi \in \widehat{\mathrm{Gal}(K_M/\mathbb{Q})}$. So we have

$$\prod_{\chi \in \widehat{H}} (1 - \chi(p)p^{-s})^{-1} = \prod_{\chi \in \widehat{\mathrm{Gal}(K_M/\mathbb{Q})}} (1 - \chi(p)p^{-s}) = \prod_{\mathfrak{p}_M | p} (1 - N(\mathfrak{p}_M)^{-s}) \tag{4.7}$$

where the last equality follows from our previous results in the case $p \nmid N$. This concludes the proof. □

Note $L(1, s) = \zeta(s)$ has a simple pole at $s = 1$ of residue 1. We deduce from Theorem 4.4.5 and Corollary 4.3.4:

Corollary 4.4.6. *We have*

$$\prod_{\substack{\chi \in \widehat{H} \\ \chi \neq 1}} L(\chi, 1) = \frac{2^{r+s}\pi^s R_K h_K}{w_K \sqrt{|\Delta_K|}}.$$

In particular, $L(\chi, s) \neq 0$ if $1 \neq \chi \in \widehat{H}$. As an application, we prove Dirichlet's theorem on arithmetic progressions. Let $N > 2$, and $a \in \mathbb{Z}$. Consider $\sum_{p \equiv a \pmod N} \frac{1}{p^s}$ (that is absolutely convergent on $\mathrm{Re}\, s > 1$).

Theorem 4.4.7. *We have* $\sum_{p \equiv a \pmod N} \frac{1}{p^s} \sim \frac{1}{\varphi(N)} \log(s-1)$ *as* $s \to 1^+$. *In particular, there are infinitely many prime numbers* p *such that* $p \equiv a \pmod N$.

Proof. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. We have (for $\mathrm{Re}\, s > 1$

$$\log L(\chi, s) = -\sum_p \log(1 - \frac{\chi(p)}{p^s}) = \sum_p \sum_{n=1}^{\infty} \frac{\chi(p^n)}{np^{ns}}.$$

Consider

$$\sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \chi(a)^{-1} \log L(\chi, s) = \sum_p \sum_{n=1}^{\infty} \Big(\big(\sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \chi(a^{-1}p^n) \big) \frac{1}{np^{ns}} \Big).$$

Using Proposition 4.4.3, we see

$$\sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \chi(a)^{-1} \log L(\chi, s) = \varphi(N) \sum_{p \equiv a \pmod N} \frac{1}{p^s} + \varphi(N) \sum_{n=2}^{\infty} \sum_{p^n \equiv a \pmod N} \frac{1}{np^{ns}}. \tag{4.8}$$

We have

$$\Big| \sum_{n=2}^{\infty} \sum_{p^n \equiv a \pmod N} \frac{1}{np^{ns}} \Big| \leq \sum_{n=2}^{\infty} \sum_{p^n \equiv a \pmod N} \Big| \frac{1}{p^{ns}} \Big| \leq \sum_{n=2}^{\infty} \sum_p \Big| \frac{1}{p^{ns}} \Big| = \sum_p \frac{1}{|p^s|(1 - |p^s|)}$$

and hence the second term of the right hand side of (4.8) is holomorphic on $\mathrm{Re}\, s > 1/2$. By Corollary 4.4.6, we see $\sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \chi(a)^{-1} \log L(\chi, s) \sim \log \zeta(s) \sim \log \frac{1}{s-1}$ and we deduce hence $\varphi(N) \sum_{p \equiv a \pmod N} \frac{1}{p^s} \sim \log \frac{1}{s-1}$. □

Exercise 4.4.8. *Prove (without using the theorem)* $\sum_p \frac{1}{p^s} \sim \log \frac{1}{s-1}$.

Exercise 4.4.9. *Deduce from Theorem 4.4.7 Chebotarev's density Theorem 1.10.8 in the case* $L = \mathbb{Q}(\zeta_N)$ *and* $K = \mathbb{Q}$

Let χ be a Dirichlet character of conductor f, and ζ_f be a primitive f-th root of unity. For $a \in \mathbb{Z}/f\mathbb{Z}$, consider the so-called Gauss sum (that can be viewed as the Fourier transform of the function χ on $\mathbb{Z}/f/Z$)

$$\tau_a(\chi) := \sum_{z \in \mathbb{Z}/f/Z} \chi(z)\zeta_f^{az}.$$

We put $\tau(\chi) := \tau_1(\chi)$. Note we have $\bar{\chi} = \chi^{-1}$.

Lemma 4.4.10. *(1)* $\tau_a(\chi) = \bar{\chi}(a)\tau(\chi)$.

(2) $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)f$.

(3) $|\tau(\chi)| = \sqrt{f}$.

Proof. (1) Assume first $(a, f) = 1$. Then we have

$$\tau_a(\chi) = \sum_{z \in \mathbb{Z}/f\mathbb{Z}} \chi(z)\zeta_f^{az} = \bar{\chi}(a) \sum_{z \in \mathbb{Z}/f\mathbb{Z}} \chi(az)\zeta_f^{az} = \bar{\chi}(a)\tau(z).$$

Assume now $(a, f) = m > 1$, and put $f_0 := f/m$, $a_0 = a/m$. We have

$$\tau_a(\chi) = \sum_{z \in \mathbb{Z}/f\mathbb{Z}} \chi(z)\zeta_{f_0}^{a_0 z} = \sum_{i=0}^{f_0-1} \zeta_{f_0}^{a_0 i} \Big(\sum_{\substack{z=0,\cdots f-1 \\ z \equiv i \pmod{f_0}}} \chi(z) \Big)$$

For $i = 0, \cdots, f_0 - 1$, if $(i, f_0) > 1$, and $z \equiv i \pmod{f_0}$, then $\chi(z) = 0$. If $(i, f_0) = 1$, letting H be the kernel of $(\mathbb{Z}/f\mathbb{Z})^\times \to (\mathbb{Z}/f_0\mathbb{Z})^\times$, then

$$\sum_{\substack{z=0,\cdots f-1 \\ z \equiv i \pmod{f_0}}} \chi(z) = \chi(i) \sum_{z \in H} \chi(z).$$

Since χ is of conductor f, $\chi|_H$ is not trivial and hence $\sum_{z \in H} \chi(z) = 0$. We see $\tau_a(\chi) = 0$. This conlcudes the proof of (1).

(2) We have

$$\tau(\chi)\tau(\bar{\chi}) = \sum_{a \in \mathbb{Z}/f\mathbb{Z}} \tau(\chi)\bar{\chi}(a)\zeta_f^a = \sum_{a \in \mathbb{Z}/f/Z} \tau_a(\chi)\zeta_f^a = \sum_{a \in \mathbb{Z}/f\mathbb{Z}} \Big(\sum_{z \in \mathbb{Z}/f\mathbb{Z}} \chi(z)\zeta_f^{az} \Big)\zeta_f^a$$
$$= \sum_{z \in \mathbb{Z}/fZ} \chi(z) \Big(\sum_{a \in \mathbb{Z}/f\mathbb{Z}} \zeta_f^{az+a} \Big).$$

If $z \neq -1$, one easily calculates $\sum_{a \in \mathbb{Z}/f\mathbb{Z}} \zeta_f^{az+a} = 0$. Hence $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)f$.

(3) It suffices to show $|\tau(\bar{\chi})| = |\tau(\chi)|$. We have $\tau(\bar{\chi}) = \sum_{z \in \mathbb{Z}/f\mathbb{Z}} \bar{\chi}(z)\zeta_f^z$ and hence $\overline{\tau(\bar{\chi})} = \sum_{z \in \mathbb{Z}/f\mathbb{Z}} \chi(z)\zeta_f^{-z} = \chi(-1)\tau(\chi)$. □

Theorem 4.4.11. *Let χ be a Dirichlet character of conductor $f \geq 3$. Then $L(\chi,1) = -\tau(\bar{\chi})^{-1}\sum_{a=1}^{f-1}\left(\bar{\chi}(a)\log(1-\zeta_f^a)\right)$ (recalling* log *denotes the principal branch of the logarithm).*

Proof. Let $a \in \{1,\cdots,f-1\}$, and consider $u_a(s) = \sum_{n=1}^{\infty}\frac{\zeta_f^{an}}{n^s}$. Then $u(s)$ is absolutely convergent for $\operatorname{Re} s > 1$. By Proposition 4.3.2, $u_a(s)$ extends to a holomophic function on $\operatorname{Re} s > 0$ (using $\sum_{n\leq t}\zeta_f^{an} = O(1)$ as $t \to +\infty$).

Claim: $u_a(1) = \sum_{n=1}^{\infty}\frac{\zeta_f^{an}}{n} = -\log(1-\zeta_f^a)$.

We prove the claim. By the proof of Proposition 4.3.2, $u_a(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}\left(\frac{\zeta_f^a(1-\zeta_f^{an})}{1-\zeta_f^a} - \frac{\zeta_f^a(1-\zeta_f^{a(n-1)})}{1-\zeta_f^a}\right) = \sum_{n=1}^{\infty}\frac{\zeta_f^a(1-\zeta_f^{an})}{1-\zeta_f^a}\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)$ with the right hand side absolutely convergent on $\operatorname{Re} s > 0$. Hence $u_a(1) = \sum_{n=1}^{\infty}\frac{\zeta_f^a(1-\zeta_f^{an})}{1-\zeta_f^a}\frac{1}{n(n+1)}$. One can directly check

$$\sum_{n=1}^{\infty}\frac{\zeta_f^a(1-\zeta_f^{an})}{1-\zeta_f^a}\frac{1}{n(n+1)} = \sum_{n=1}^{\infty}\frac{\zeta_f^{an}}{n}.$$

Moreover, we have

$$\lim_{\substack{z\to\zeta_f^a\\|z|<1}}\sum_{n=1}^{\infty}\frac{z(1-z^n)}{1-z}\frac{1}{n(n+1)} = \sum_{n=1}^{\infty}\frac{\zeta_f^a(1-\zeta_f^{an})}{1-\zeta_f^a}\frac{1}{n(n+1)},$$

and for $|z|<1$, we have

$$-\log(1-z) = \sum_{n=1}^{\infty}\frac{z^n}{n} = \sum_{n=1}^{\infty}\frac{z(1-z^n)}{1-z}\frac{1}{n(n+1)}.$$

Putting these together, we see $u_a(1) = \lim_{\substack{z\to\zeta_f^a\\|z|<1}} -\log(1-z) = -\log(1-\zeta_f^a)$.

For $\operatorname{Re} s \gg 0$, we have

$$\sum_{a=1}^{f-1}(\bar{\chi}(a)u_a(s)) = \sum_{n=1}^{\infty}\frac{\sum_{a\in\mathbb{Z}/f\mathbb{Z}}\bar{\chi}(a)\zeta_f^{an}}{n^s} = \sum_{n=1}^{\infty}\frac{\tau_n(\bar{\chi})}{n^s} = \tau(\bar{\chi})\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} = \tau(\bar{\chi})L(\chi,s).$$

The both being holomorphic on $\operatorname{Re} s > 0$, we deduce hence $L(\chi,1) = -\frac{1}{\tau(\bar{\chi})}\sum_{a=1}^{f-1}\left(\bar{\chi}(a)\log(1-\zeta_f^a)\right)$. □

Remark 4.4.12. *By a bit more work, one can obtain more user-friendly version of formulas on $L(\chi,1)$, and hence, combing with Corollary 4.4.6, more user-friendly version of formulas on class numbers. For example, let K be a quadratic extension of $\mathbb{Q}$ with $\Delta_K \in \mathbb{Z}$ the discriminant of $K/\mathbb{Q}$. Let $\chi_K : \operatorname{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$ be the unique non-trivial character. One can prove that χ_K is a Dirichlet character of conductor $|\Delta_K|$. In this case, the term on the*

left hand side of Corollary 4.4.6 is just $L(\chi_K, 1)$. With a bit more work (say, on $\tau(\chi_K)$), one can prove the so-called Dirichlet's class number formula:

$$h_K = \begin{cases} -\frac{1}{|\Delta_K|}\sum_{a=1}^{|\Delta_K|-1}\chi_K(a)a & \Delta_K < -4 \\ = -\frac{1}{\log(\varepsilon)}\sum_{a=1}^{[\frac{\Delta_K}{2}]}\chi_K(a)\log(\sin\frac{\pi a}{\Delta_K}) & \Delta_K > 0, \end{cases}$$

where ε is a fundamental unit of K.

4.5 Adelic point of view (à la Tate)

Let k be $\mathbb{R}$, $\mathbb{C}$ or a finite extension of $\mathbb{Q}_p$. Let $\psi : k \to \mathbb{C}^\times$ be the following (unitary) continuous character ("unitary" means that $\mathrm{Im}(\psi) \subseteq S^1 := \{x \in \mathbb{C}^\times \mid |x| = 1\}$):

$$\psi(x) = \begin{cases} e^{-2\pi i x} & k = \mathbb{R} \\ e^{-2\pi i x}(x + \bar{x}) & k = \mathbb{C} \\ e^{2\pi i \lambda_p(\mathrm{Tr}_{k/\mathbb{Q}_p}(x))} & [k : \mathbb{Q}_p] < +\infty, \end{cases} \tag{4.9}$$

where for $x \in \mathbb{Q}_p$, $\lambda_p(x)$ is an element in $\sum_n \frac{1}{p^n}\mathbb{Z}$ such that $\lambda_p(x) - x \in \mathbb{Z}_p$ (it is clear that such element exists and that $e^{2\pi i r_p(x)}$ does not depend on the choice of $\lambda_p(x)$).

Remark 4.5.1. *For an abelian locally compact group G, one can consider the group $G^\vee$ of continuous (unitary) characters on G. The group $G^\vee$ can be equipped with the so-called compact open topology: the sets $\{W(Z,U)\}$ with $W(Z,U) = \{\chi \in G^\vee \mid \chi(Z) \subset U\}$, Z (resp. U) running through compact (resp. open) subsets of G (resp. S^1) form a topology basis. Then a fact is that $G^\vee$ is also a locally compact group. Moreover, for k, ψ as above, one obtains a morphism $k \to k^\vee$, $x \mapsto [y \mapsto \psi(xy)]$. A factis that the morphism is actually a topological isomorphism (and this is referred to as the self-duality of k).*

We define the space $S(k, \mathbb{C})$ of Schwartz functions on k. If $k = \mathbb{R}$ or $\mathbb{C}$, then the definition is standard: $S(k, \mathbb{C})$ consists of smooth functions of rapid decay (see the discussion above Example 4.1.8). If k is a finite extension of $\mathbb{Q}_p$, then $S(k, \mathbb{C})$ consists of locally constant functions with compact support.

We fix a Haar measure on k such that: if $k = \mathbb{R}$, then dx denotes the standard Lebesgue measure; if $k = \mathbb{C}$, then dx denotes the twice of the standard Lebesgue measure on $\mathbb{C}$; if k is a finite extension of $\mathbb{Q}_p$, then dx is chosen such that $\int_{\mathcal{O}_k} dx = N(\mathcal{D}_{k/\mathbb{Q}_p})^{-\frac{1}{2}}$ (for a fractional ideal $\mathfrak{a}$ of k, $N\mathfrak{a} = p^r$ such that $N_{k/\mathbb{Q}_p}\mathfrak{a} = (N(\mathfrak{a}))$).

For $f \in S(k, \mathbb{C})$, Fourier transform $f^\vee$ of f is defined to be $\hat{f}(x) = \int_k f(y)\psi(xy)dy$. Note since $f \in S(k, \mathbb{C})$, f is absolutely integrable, so $\hat{f}$ is well-defined. Moreover, one can show that $\hat{f} \in S(k, \mathbb{C})$ and $\hat{\hat{f}}(x) = f(-x)$ (actually, we normalize the Haar measure as above to make this equality hold).

Let $|\cdot| : k \to \mathbb{R}_{\geq 0}$ be normalized such that

$$|x| = \begin{cases} |x|_{\mathbb{R}} & k = \mathbb{R} \\ |x|_{\mathbb{C}}^2 & k = \mathbb{C} \\ N(\mathfrak{p})^{-\operatorname{val}_k(x)} & [k : \mathbb{Q}_p] < +\infty \end{cases}$$

where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_k$, and $\operatorname{val}_k(k^\times) = \mathbb{Z}$. We denote by

$$d^\times x := \delta(k)\frac{dx}{|x|} \tag{4.10}$$

the Haar measure on $k^\times$, i.e. $\int_U d^\times x = \delta(k)\int_U \frac{dx}{|x|}$ (using $\int_{aU} f(x)dx = \int_U f(au)|a|dx$, it is not difficult to check $d^\times x$ is invariant under the $k^\times$-action) where $\delta(k) = 1$ if $k = \mathbb{R}$ or $\mathbb{C}$, and $\delta(k) = \frac{N(\mathfrak{p})}{N(\mathfrak{p})-1}$ if $[k : \mathbb{Q}_p] < \infty$.

A continuous morphism $\chi : k^\times \to \mathbb{C}^\times$ is called a quasi-character of $k^\times$, and χ is called unitary if $\operatorname{Im}(\chi) \subseteq S^1$.

Fact: For any χ, there exist a unitary character χ_0 and $s \in \mathbb{C}$ such that $\chi = \chi_0|\cdot|^s$.

We can now define the local zeta function: for $f \in S(k, \mathbb{C})$, $\chi = \chi_0|\cdot|^s$ a quasi-character of $k^\times$,

$$\zeta(f, \chi) := \int_{k^\times} f(x)\chi(x)d^\times x.$$

It is not difficult to see that $\zeta(f, \chi_0|\cdot|^s)$ is absolutely convergent on $\operatorname{Re} s > 0$.

Example 4.5.2. *(1) Suppose $k = \mathbb{R}$, $f = e^{-\pi x^2}$ and $\chi = |\cdot|^s$. Then*

$$\zeta(f, \chi) = \int_{\mathbb{R}^\times} e^{-\pi x^2}|x|^{s-1}dx = 2\int_0^{+\infty} e^{-\pi x^2}x^{s-1}dx = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2}).$$

(2) Suppose $k = \mathbb{C}$, $f = e^{-\pi z\bar{z}}$ and $\chi = |\cdot|^s$. Similarly, one can calculate $\zeta(f, \chi) = 2\pi^{1-s}\Gamma(s)$.

(3) Suppose k is a finite extension of $\mathbb{Q}_p$, $f = 1_{\mathcal{O}_k}$, and $\chi = |\cdot|^s$. Then

$$\begin{aligned}\zeta(f, \chi) &= \delta(k)\int_{k^\times} 1_{\mathcal{O}_k}|\cdot|^{s-1}dx = \delta_k \sum_{n\geq 0}\int_{\varpi^n\mathcal{O}_K^\times} |\cdot|^{s-1}dx \\ &= \delta(k)\sum_{n\geq 0} N(\mathfrak{p})^{(1-s)n}\int_{\varpi^n\mathcal{O}_k^\times} dx = \delta(k)N(\mathcal{D}_{k/\mathbb{Q}_p})^{-\frac{1}{2}}\sum_n N(\mathfrak{p})^{(1-s)n}(1-\frac{1}{N(\mathfrak{p})})\frac{1}{N(\mathfrak{p})^n} \\ &= N(\mathcal{D}_{k/\mathbb{Q}_p})^{-\frac{1}{2}}\frac{1}{1-N(\mathfrak{p})^{-s}}.\end{aligned}$$

Theorem 4.5.3. *The function $\zeta(f, \chi_0|\cdot|^s)$ can extend to a meromorphic function on $\mathbb{C}$.*

Now let K be a number field. The local Haar measure defined as above gives a Haar measure $dx = \prod_v dx_v$ on $\mathbb{A}_K$. We use dx to denote the quotinet Haar measure on $\mathbb{A}_K/K$.

Then one can show that $\int_{\mathbb{A}_K/K} dx = 1$. For each place v of K, let $\psi_v : K_v \to S^1$ be the character defined as in (4.9). And put $\psi := \prod_v \psi_v : \mathbb{A}_K \to S^1$. One can check ψ is trivial on K. Let $S(\mathbb{A}_K, \mathbb{C})$ be the space of Schwartz functions on $\mathbb{A}_K$, i.e. the space of linear combinations of funtions on $\mathbb{A}_K$ of the form $f = \prod_v f_v$ where $f_v \in S(K_v, \mathbb{C})$ and $f_v = 1_{\mathcal{O}_{K_v}}$ for all but finitely many v. Then one can define the Fourier transform of $f \in S(\mathbb{A}_K, \mathbb{C})$:

$$\hat{f}(y) = \int_{\mathbb{A}_K} f(x)\psi(xy)dx.$$

A fact is that $\hat{f} \in S(\mathbb{A}_K, \mathbb{C})$.

We have a Haar measure $d^\times x = \prod_v d^\times x_v$ with $d^\times x_v$ defined as in (4.10). A Hecke character of K is defined to be a continuous morphism $\chi : I_K/K^\times \to \mathbb{C}^\times$. Similarly as in the local setting, there exists a unitary character $\chi_0 : I_K/K^\times \to S^1$ and $s \in \mathbb{C}$ such that $\chi = \chi_0|\cdot|_K^s$ (recall $|\cdot|_K$ is trivial on $K^\times$). Let $f \in S(\mathbb{A}_K, \mathbb{C})$, χ be a Hecke character, we define the zeta function of f at χ to be

$$\zeta(f, \chi) = \int_{I_K} f(x)\chi(x)d^\times x.$$

When $\operatorname{Re} s > 1$, $f = \otimes f_v$, one can decompose $\zeta(f, \chi_0|\cdot|^s)$ into a product $\prod_v \zeta(f_v, \chi_v)$ where $\chi_v = \chi|_{k_v^\times}$. Then it is not difficulet to show that $\zeta(f, \chi_0|\cdot|^s)$ is absolutely convergent on $\operatorname{Re} s > 1$.

Theorem 4.5.4 (Tate)**.** *The zeta function $\zeta(f, \chi_0|\cdot|^s)$ extends to a meromorphic function on $\mathbb{C}$ satisfying the functional equation $\zeta(f, \chi) = \zeta(\hat{f}, \chi_0^{-1}|\cdot|^{1-s})$. Moreover, $\zeta(f, \chi_0|\cdot|^s)$ is holomorphic everywhere except that when $\chi_0 = 1$ there are two simple poles at $s = 0$ with residue $-f(0)\frac{2^{r+s}\pi^s h_K R_K}{w_K\sqrt{|\Delta_K|}}$ and at $s = 1$ with residue $\hat{f}(0)\frac{2^{r+s}\pi^s h_K R_K}{w_K\sqrt{|\Delta_K|}}$.*

Remark 4.5.5. *Applying the theorem to the case $\chi_0 = 1$, $f = \otimes_v f_v$ where*

$$f_v = \begin{cases} e^{-\pi x_v^2} & K_v = \mathbb{R} \\ e^{-\pi x_v \bar{x}_v} & K_v = \mathbb{C} \\ 1_{\mathcal{O}_{K_v}} & K_v \text{ non-archimedean} \end{cases}$$

one obtains the analytic continuation of $\zeta_K(s)$ to the whole complex plane.