Algebraic Number Theory

Contents

1 Local Fields **5**

1.1 Fractional Ideals . . . 5

1.2 Discrete Valuation Rings . . . 7

1.3 Hensel's lemma . . . 12

1.4 Localization . . . 14

1.4.1 Ideals in the localization . . . 15

1.4.2 Integral dependence . . . 16

1.5 Dedekind Domains . . . 17

1.5.1 Modules and Bilinear Forms . . . 20

1.6 Extensions . . . 23

1.6.1 Krull-Akizuki . . . 23

1.6.2 Trace form . . . 25

1.7 Ramification . . . 26

2 Global Fields **28**

2.1 Valuations . . . 28

2.2 Types of Valuation . . . 28

2.3 Examples of Valuations . . . 28

2.4 Topology . . . 28

2.5 Completeness . . . 28

2.6 Independence . . . 28

2.7 Finite Residue Field Case . . . 29

2.8 Normed Spaces . . . 31

2.9 Tensor Product . . . 31

2.10 Extension of Valuations . . . 34

2.11 Extension of Normalized Valuations . . . 35

2.12 Global Fields . . . 35

2.13 Restricted Topological Product . . . 37

2.14 Adele Ring . . . 37

2.15 Strong Approximation Theorem . . . 42
2.16 Idele Group . . . 42
2.17 Ideal and Divisors . . . 44
2.18 Units . . . 45
2.19 Inclusion and Norm Maps for Adeles, Ideles and Ideals . . . 46

3 Cyclotomic Fields and Kummer Extensions 47
3.1 Cyclotomic Fields . . . 47
3.2 Kummer Extensions . . . 47

4 Cohomology of Groups 48
4.1 Definition of Cohomology . . . 48
4.2 The Standard Complex . . . 48
4.3 Homology . . . 48
4.4 Change of Groups . . . 48
4.5 The Restriction-Inflation Sequence . . . 50
4.6 The Tate Groups . . . 50
4.7 Cup-products . . . 50
4.8 Computations of Cup Products in Low Dimensions . . . 54
4.9 Cyclic Groups: Herbrand Quotient . . . 57
4.10 Coholomogical Triviality . . . 57
4.11 Tate's Theorem . . . 60

5 Local Class Field Theory 63
5.1 The Brauer Group of a Local Field . . . 63
5.1.1 Statements of Theorems . . . 63
5.1.2 Computation of $H^2(K_{nr}/K)$ . . . 63
5.1.3 Some Diagrams . . . 64
5.1.4 Construction of a Subgroup with Trivial Cohomology . . . 64
5.1.5 An Ugly Lemma . . . 64
5.1.6 End of Proofs . . . 64
5.1.7 An Auxiliary Results . . . 64
5.2 Abelian Extension of Local Fields . . . 65
5.2.1 Cohomological Properties . . . 65
5.2.2 The Reciprocity Map . . . 65
5.2.3 Characterization of $(\alpha, L/K)$ by Characters . . . 65
5.2.4 Variations with the Field Involved . . . 66
5.2.5 Unramified Extensions . . . 66
5.2.6 Norm Subgroups . . . 67

5.2.7 Statements of the Existence Theorem 67

5.2.8 Some Characterization of $(\alpha, L/K)$ 67

5.2.9 The Archimedean Case 67

5.3 Formal Multiplication in Local Fields 68

5.3.1 The Case $K = \mathbb{Q}_p$ 68

5.3.2 Formal Groups 69

5.3.3 Lubin-Tate Formal Group Laws 70

5.3.4 Statements 71

5.3.5 Construction of F_f, $[a]_f$ 72

5.3.6 First Properties of the Extension K_π of K 74

5.3.7 The Reciprocity Map 75

5.3.8 The Existence Theorem 79

5.4 Ramification Subgroups of Conductors 79

6 Global Class Field Theory **80**

6.1 Action of the Galois Group on Primes and Completions 80

6.2 Frobenius Automorphisms 80

6.3 Artin's Reciprocity Law 80

6.4 Chevalley's Interpretation by Ideles 80

6.5 Statement of the Main Theorem on Abelian Extensions 82

6.6 Relation between Global and Local Artin Maps 85

6.7 Cohomology of Ideles 86

6.8 Cohomology of Idele Class (I), The First Inequality 88

6.9 Cohomology of Idele Class (II), The Second Inequality 91

6.10 Proof of the Reciprocity Law 98

6.11 Cohomology of Idele Class (III), The Fundamental Class 103

6.12 Proof of the Existence Theorem 109

7 Fourier Analysis in Number Fields and Hecke's Zeta Functions **112**

7.1 The Local Theory 112

7.1.1 Additive Characters and Measure 112

7.1.2 Multiplicative Characters and Measure 116

7.1.3 The Local ζ-function; Functional Equation 118

7.1.4 Computation of $\rho(c)$ by Special ζ-functions 121

7.2 Abstract Restricted Direct Product 125

7.3 The Theory in the Large 129

7.3.1 Additive Theory 129

7.3.2 Riemann-Roch Theorem 132

7.3.3 Multiplicative Theory 135

7.3.4 The ζ-function; Functional Equation 138
7.3.5 Comparison with the Classical Theory 141

8 Exercise 144

8.1 The Power Residue Symbol 144
8.2 The Norm Residue Symbol 147
8.3 The Hilbert Class Field 147
8.3.1 Hilbert class fields of imaginary quadratic fields 149
8.3.2 Big Hilbert class fields 149

Chapter 1

Local Fields

1.1 Fractional Ideals

Let R be an integral domain and K its field of fractions. For R-submodules I, J of K, we can define

$$I + J,\ I \cap J,\ IJ$$

as usual, and all of the operations above are commutative and associative. Moreover, for R-submodules I, I_1, I_2 of K,

$$I(I_1 + I_2) = II_1 + II_2$$

For an R-submodule I of K, define

$$I^{-1} = \{x \in K \mid xI \subseteq R\} = (R : I)$$

$$R(I) = \{x \in K \mid xI \subseteq I\} = (I : I)$$

It is easy to see that

1. $R(I) \supseteq R \supseteq II^{-1}$;
2. if $I \subseteq R$, then $I^{-1} \supseteq R$.

Definition. An R-submodules I of K is a **fractional ideal** of R if

- $I \neq 0$;
- there exists $a \in K^\times$ such that $aI \subseteq R$.

Note that a can always be chosen to lie in R; in particular, $I \cap R \neq \varnothing$. If $R = II^{-1}$, we say I is **invertible**.

Lemma 1.1. If I, I_1, I_2 are fractional ideals, then so are $I_1 + I_2$, $I_1 \cap I_2$, $I_1 I_2$, I^{-1}, $R(I)$.

Proof. It's clear for the first three. For the last two, we prove a more general statement. If I_1, I_2 are fractional, so is

$$J = \{x \in K \mid xI_2 \subseteq I_1\} = (I_1 : I_2)$$

- J is nonzero: Let $a, b \in R \backslash \{0\}$ be such that $aI_2 \subseteq R$, $b \in I_1 \cap R$. Then $baI_2 \subseteq bR \subseteq I_1$ so that $ab \in J \backslash \{0\}$ and J is nonzero.

- J is fractional: Let $c, d \in K^\times$ such that $cI_1 \subseteq R$, $d \in I_2$. Then for $x \in J$, $cdx \in cxI_2 \subseteq cI_1 \subseteq R$, so $cdJ \subseteq R$.

□

Lemma 1.2. Suppose R is Noetherian. A nonzero R-submodule I of K is fractional iff I is finitely generated.

Proof. Suppose I is fractional. Then $I \cong aI \subseteq R\,(a \in R)$ is finitely generated. Conversely, if I is finitely generated, pick $a \in R$ to be the product of the denominators of a finite generating set of I; then $aI \subseteq R$. □

Lemma 1.3. Let I be fractional.

1. If I is invertible, then I is finitely generated.

2. I is invertible if and only if I is a projective R-module

Proof. Assume $II^{-1} = R$. Then $1 = \sum_{i=1}^n a_i b_i$ for some $a_i \in I$, $b_i \in I^{-1}$, and for each $a \in I$,

$$a = a1 = \sum_{i=1}^n a_i(ab_i)$$

Since $b_i \in I^{-1}$, $ab_i \in R$. Hence $I = (a_1, \ldots, a_n)_R$. Let $\bigoplus_{i=1}^n Rx_i \xrightarrow{\pi} I$ defined by $\pi(x_i) = a_i$. Define

$$f : I \longrightarrow \bigoplus_{i=1}^n Rx_i$$

$$a \longmapsto \sum_{i=1}^n (ab_i)x_i$$

Then

$$(\pi \circ f)(a_j) = \pi\left(\sum_{i=1}^n a_j b_i x_i\right) = \sum_{i=1}^n a_j b_i a_i = a_j$$

so that the exact sequence $0 \to \ker \pi \to R^n \xrightarrow{\pi} I \to 0$ splits.

Conversely, suppose I is projective. Let $\{a_s\}_{s\in S}$ be a generating set, and define $\bigoplus_{s\in S} Rx_s \xrightarrow{\pi} I$ defined by $\pi(x_s) = a_s$. Then we can lift id_I to a map $f : I \to R^{\oplus S}$. Write $f = (f_s)_{s\in S}$. Then the f_s satisfy the property: for all $x \in I$, $f_s(x) = 0$ for all but finitely many $s \in S$, and for any $a \in I$,

$$a = \sum_{s\in S} f_s(a)a_s$$

Now let $b \in I\backslash\{0\}$ and let $f_{s_1}, \ldots, f_{s_n}$, $s_i \in S$ be all the maps that $f_s(b) \neq 0$. Let $r \in I^{-1} \cap R\backslash\{0\}$. Then for each $a \in I$, $s \in S$,

$$brf_s(a) = f_s(bra) = f_s(b)ra$$

so that $f_s(a) = b^{-1}f_s(b)a$. This show $f_{s_1}, \ldots, f_{s_i}$ are the only nontrivial maps in $\{f_s\}_{s\in S}$, and $b^{-1}f_s(b) \in I^{-1}$ for each $s \in S$.

Now, for $a \in I\backslash\{0\}$, we have

$$a = \sum_{i=1}^{n} f_{s_i}(a)a_{s_i} = \sum_{i=1}^{n} b^{-1}f_{s_i}(b)aa_{s_i} = a \cdot \sum_{i=1}^{n} b^{-1}f_{s_i}(b)a_{s_i}$$

so that $1 = \sum_{i=1}^{n} b^{-1}f_{s_i}(b)a_{s_i} \in I^{-1}I$. Hence $I^{-1}I = R$. □

1.2 Discrete Valuation Rings

Let K be a field.

Definition. A map $\nu : K \to \mathbb{Z} \cup \{\infty\}$ is a **discrete valuation** of K if

1. $\nu : K^\times \to \mathbb{Z}$ is a surjective homomorphism;
2. $\nu(0) = \infty$;
3. $\nu(x + y) \geqslant \min\{\nu(x), \nu(y)\}$

- $\nu(-1) + \nu(-1) = \nu(1) = 0$, so $\nu(-1) = 0$. Thus $\nu(-y) = \nu(-1) + \nu(y) = \nu(y)$.
- $R_\nu^\times = \{x \in K \mid \nu(x) = 0\}$.
- If $\nu(x) \neq \nu(y)$, then $\nu(x + y) = \min\{\nu(x), \nu(y)\}$.

Proof. Suppose $\nu(x) < \nu(y)$. Then

$$\nu(x + y) \geqslant \nu(x) = \nu(x + y - y) \geqslant \min\{\nu(x + y), \nu(y)\} = \nu(x + y)$$

□

- The set $R_\nu = \{x \in K \mid \nu(x) \geqslant 0\}$ is an integral domain with quotient field K. This is called the **valuation ring** of v.

Theorem 1.4. A discrete valuation ν of a field K can uniquely be extended to a discrete valuation on the completion $\overline{K}$ of K with respect to the valuation topology. Additionally, $\nu(\overline{K}) = \nu(K)$.

Proof. Fix $0 < \rho < 1$ and define $|x|_\nu = \rho^{\nu(x)}$ for each $x \in K$. Then $|\cdot|_\nu$ is a metric on K. Let $\overline{K}$ be the completion of K with respect to $|\cdot|_\nu$; the addition, multiplication and inverse are continuous on K so they're well-defined on $\overline{K}$, making $\overline{K}$ a complete field. The uniqueness is clear for K is dense in $\overline{K}$.

- $|\cdot|_\nu$ is non-Archimedean. Let $x, y \in \overline{K}$ and let $x_n \to x$, $y_m \to y$ in K. Then $|x_n + y_m|_\nu \leqslant \max\{|x_n|_\nu, |y_m|_\nu\}$. Taking limit, we see $|x+y|_\nu \leqslant \max\{|x|_\nu, |y|_\nu\}$.

- The image group is the same. Let $x \in \overline{K}$ and let $a \in K$ be such that $|x-a|_\nu < |x|_\nu$. Then $|a|_\nu = \max\{|a-x|_\nu, |x|_\nu\} = |x|_\nu$.

Define $\overline{\nu} : \overline{K} \to \mathbb{Z} \cup \{\infty\}$ by $\overline{\nu}(x) = \log_\rho |x|_\nu$. Then $\overline{\nu}$ is a discrete valuation on $\overline{K}$ extending ν. □

Choose an element $\pi \in K$ with $\nu(\pi) = 1$; such an element is called a **uniformizer**. Then every $a \in K^\times$ has a unique representation

$$a = \pi^{\nu(a)} u,\ u \in R_\nu^\times$$

This gives a (non-canonical) isomorphism $K^\times \cong \mathbb{Z} \times R_\nu^\times$. We turn to the fractional ideals of R_ν.

Proposition 1.5. R_ν is a local PID with maximal ideal $\mathfrak{p}_\nu = \{x \in K \mid \nu(x) > 0\}$.

Proof. Let I be a nonzero ideal of R_ν. Let $x \in I\backslash\{0\}$ be such that $\nu(x) = \min\{\nu(y) \mid y \in I\backslash\{0\}\}$.

Claim. I is generated by x, and $I = \{y \in I \mid \nu(y) \geqslant \nu(x)\}$.

Indeed, for $y \in I\backslash\{0\}$, we have $\nu(yx^{-1}) = \nu(y) - \nu(x) \geqslant 0$, so $yx^{-1} \in R_\nu$. This shows $I \subseteq xR_\nu \subseteq I$, and hence $I = xR_\nu$.

For each $n \in \mathbb{N} \cup \{0\}$, define $I_n := \{x \in R_\nu \mid \nu(x) \geqslant n\}$. Then we have a descending chain of ideals

$$R_\nu = I_0 \supsetneq I_1 \supsetneq I_2 \supsetneq \cdots$$

consisting of all nonzero ideals of R_ν. Together with the above results, R_ν is PID with the unique maximal ideals $I_1 = \mathfrak{p}_\nu$. □

Corollary 1.5.1. Every fractional ideal I of R_ν takes the form $\mathfrak{p}_\nu^{\nu(I)}$, where $\nu(I) = \min\{\nu(x) \mid x \in I\}$.

Definition. A **discrete valuation ring**, or **DVR** for short, R is a local principal ideal domain but not a field.

Proposition 1.6. Let K be a field with discrete valuation ν, and $(R, \mathfrak{p})$ be its valuation ring. Then the valuation ring of the completion $\overline{K}$ of K at ν is $(\overline{R}, \overline{\mathfrak{p}})$, where $\bar{\cdot}$ denotes the closure of $\cdot$ in $\overline{K}$. Moreover, $\overline{\mathfrak{p}} = \mathfrak{p}\overline{R}$.

Proof. Let $x \in \overline{K}$ with $\nu(x) \geqslant 0$. Find $a_1 \in K$ such that $\nu(x - a_1) > \nu(x)$. Then $\nu(a_1) = \min\{\nu(x - a_1), \nu(x)\} = \nu(x)$, so $a_1 \in R$. Inductively we find $a_n \in K$ such that

$$\nu(x - (a_1 + \cdots + a_{n-1} + a_n)) > \nu(x - (a_1 + \cdots + a_{n-1}))$$

with $a_1, \ldots, a_n \in R$. Then $a_1 + \cdots + a_n \to x$ as $n \to \infty$, so that $x \in \overline{R}$. Conversely, if $x \in \overline{R}$, then we can find $a \in R$ such that $\nu(x - a) > \nu(x)$, and hence $0 \leqslant \nu(a) = \nu(x)$. In the same way we can show the maximal ideal of $\overline{R}$ is $\overline{p}$.

Finally, let π be a uniformizer of R. Then π is also a uniformizer of $\overline{R}$, so

$$\mathfrak{p}\overline{R} = \pi\overline{R} = \overline{\mathfrak{p}}$$

□

Characterizations of DVR

Theorem 1.7. Every valuation ring R_ν of a discrete valuation ν on K is a DVR.

Conversely, every DVR R is the valuation ring R_ν for a unique discrete valuation of its field of fractional K.

Proof. It remains to show the converse. Let $\mathfrak{p} = \pi R$ be the unique maximal ideal of R. R is a UFD, so every nonzero element $x \in R$ has a unique representation

$$x = \pi^n u$$

for u a unit and $n \geqslant 0$. For $ab^{-1} \in K$, $a, b \in R\backslash\{0\}$, write $a = \pi^n u$, $b = \pi^m v$. Thus $ab^{-1} = \pi^{n-m}(uv^{-1})$, so allowing $n \in \mathbb{Z}$ we see every $x \in K^\times$ has the form as above. Define $\nu : K \to \mathbb{Z} \cup \{\infty\}$ by setting $\nu(x) = n$, $\nu(0) = \infty$. Then ν is a discrete valuation on K, and $R = R_\nu$ by definition.

If μ is another discrete valuation on K such that $R_\mu = R$, then $\mathfrak{p}_\mu$ is the unique maximal ideal of $R_\mu = R$, forcing that $\mathfrak{p}_\mu = \mathfrak{p}_\nu$; in particular, $\mu(\pi) = 1$. Hence $\mu = \nu$. □

Theorem 1.8. An integral domain R is a DVR iff it's Noetherian, integrally closed and local, but not a field.

Proof. A PID is necessarily Noetherian, and a UFD is integrally closed. This shows the necessity.

For sufficiency, let I be a fractional ideal. Then $R(I) = (I : I) \subseteq K$ in a ring, and hence for all $x \in R(I) \subseteq K$, $R[x]$ is an R-submodule of $R(I)$. By lemmas in 1.1, $R(I)$ is finitely generated, hence so is $R[x]$. This proves x is integral over R, i.e., $x \in R$, and thus $R(I) = R$.

Let $\mathfrak{p}$ be the maximal ideal of R. We claim that $\mathfrak{p}^{-1} \neq R$. Consider the collection

$$\mathcal{S} := \{0 \neq I \trianglelefteq R \mid I^{-1} \neq R\}$$

this is nonempty, for $aR \in \mathcal{S}$ for $a \neq 0 \in \mathfrak{p}$. Since R is Noetherian, let $J \in \mathcal{S}$ be a maximal element. We show J is a prime, and hence $J = \mathfrak{p}$.

Let $x, y \in R$ be such that $xy \in J$, $x \notin J$. For $z \in J^{-1} \backslash R$, we have $zy(xR + J) \subseteq R$, and hence $zy \in (xR + J)^{-1} = R$ by maximality of J. Then $z(yR + J) \subseteq R$, so $z \in (yR + J)^{-1}$, showing that $(yR + J)^{-1} \neq R$. By maximality, $yR + J = J$; in particular, $y \in J$. This proves $J = \mathfrak{p}$.

By lemmas in 1.1,

$$R \supseteq \mathfrak{p}\mathfrak{p}^{-1} \supseteq \mathfrak{p}R = \mathfrak{p}$$

But $\mathfrak{p}\mathfrak{p}^{-1} = |$ would imply $\mathfrak{p}^{-1} \subseteq R(\mathfrak{p}) = R$ (in the second paragraph), a contradiction. Hence $R = \mathfrak{p}\mathfrak{p}^{-1}$.

Clearly, $\mathfrak{p}^{-1} \subseteq R\left(\bigcap_{n \geqslant 1} \mathfrak{p}^n\right)$. If $\bigcap_{n \geqslant 1} \mathfrak{p}^n \neq 0$, then $\bigcap_{n \geqslant 1} \mathfrak{p}^n = R$ and $\mathfrak{p}^{-1} \subseteq R \subsetneq \mathfrak{p}^{-1}$, a contradiction. Hence

$$\bigcap_{n \geqslant 1} \mathfrak{p}^n = 0 \tag{1.1}$$

Choose $a \in \mathfrak{p} \backslash \mathfrak{p}^2$. Then $a\mathfrak{p}^{-1} \subseteq R$. Since $R = \mathfrak{p}\mathfrak{p}^{-1}$, $a\mathfrak{p}^{-1} \nsubseteq \mathfrak{p}$. Hence $a\mathfrak{p}^{-1}$ is an ideal of R contained in any maximal ideal, so $a\mathfrak{p}^{-1} = R$, and thus

$$\mathfrak{p} = aR$$

is principal. By (1.1) every nonzero element of R has a unique representation $a^n u$, $n \geqslant 0$, $u \in R^\times$: every $x \in R$ lies in $\mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$ for some unique $n \geqslant 0$. Hence R is a DVR. □

Some associated groups

Let K be a field with a discrete valuation ν. Let $(R, \mathfrak{p})$ be its valuation ring. The quotient $\kappa = R/\mathfrak{p}$ is called the **residue class field**.

The additive group of K is the union of open and closed subgroups $\mathfrak{p}^n$ $(n \in \mathbb{Z})$ whose intersection is zero.

Lemma 1.9. For $n \in \mathbb{Z}$, there is an isomorphism

$$\kappa \cong \mathfrak{p}^n / \mathfrak{p}^{n+1}$$

of κ-modules.

Proof. Write $\mathfrak{p} = \pi R$. Then the isomorphism is induced by multiplication by π^n. Pictorially,

$$\begin{tikzcd}
R \arrow[r, "\pi^n"] \arrow[d] & \mathfrak{p}^n \arrow[r] & \mathfrak{p}^n/\mathfrak{p}^{n+1} \\
\kappa = R/\mathfrak{p}^n \arrow[urr] & &
\end{tikzcd}$$

□

We turn to the multiplicative group $K^\times$ of K. Note that the valuation induces an exact sequence

$$0 \longrightarrow U \longrightarrow K^\times \xrightarrow{\nu} \mathbb{Z} \longrightarrow 0$$

where $U = R^\times$ is the group of units of R. For each $n \geqslant 1$, define

$$U_n = 1 + \mathfrak{p}^n$$

this is an open subgroup of U, with $\bigcap_{n\geqslant 1} U_n = \{1\}$ (for $x \in U_n$, if $y \in \mathfrak{p}^n$, then $x + y \in U_n$). The subgroup topology of U induced by the U_n ($n \geqslant 1$) coincides with the subspace topology of $U \subseteq K$.

Proposition 1.10.

1. The residue class map $R \to \kappa$ gives rise to an isomorphisms

$$U/U_1 \cong \kappa^\times$$

   as groups.

2. For each $n \geqslant 1$, the map $u \mapsto u - 1$ gives rise to an isomorphism

$$U_n/U_{n+1} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}$$

   Thus $U_n/U_{n+1} \cong \kappa$.

Proof.

1. $U = R - \mathfrak{p}$, so the image of U equals $\kappa^\times$. Let $x = 1 + \pi u \in U_1$. Then $x \mod \mathfrak{p} = 1$ in κ, and thus $U_1 = \ker(U \to \kappa^\times)$.

2. For $u, v \in U_n$,

$$(uv - 1) - (u - 1) - (v - 1) = uv - u - v + 1 = (u - 1)(v - 1) \in \mathfrak{p}^{2n}$$

□

Proposition 1.11. Let p be the characteristic of κ.

1. If $p > 0$ is a prime, then for $n \geqslant 1$

$$U_n^p \subseteq U_{n+1}$$

2. If K is complete and if $m \in \mathbb{N}$ not divisible by p, then for each $n \geqslant 1$, the map $u \mapsto u^m$ is an automorphism of U_n.

Proof.

1. From the previous proposition, we have $U_n/U_{n+1} \cong \kappa$ for $n \geqslant 1$, a multiplicative-to-additive homomorphism. Hence $U_n^p \subseteq U_{n+1}$.

2. Again by the mentioned isomorphism, the map $f : u \mapsto u^m$ on U_n induces an isomorphism $f_q : U_q/U_{q+1} \to U_q/U_{q+1}$ for $q \geqslant n$. If $x \in \ker f$, then $x^m \in U_{n+1}$, and hence $x \in U_{n+1}$. Repeatedly, we see $x \in \bigcap\limits_{q \geqslant n} U_{q+1} = \{1\}$, proving that $\ker f = \{1\}$, that is, f is injective.

   Let $u \in U_n$. To show f is surjective, start with $v_0 \in U_n$, $w_1 \in U_{n+1}$ such that $u = v_0^m w_1$; this is possible for f_n is bijective. Inductively, let $v_q \in U_{n+q}$, $w_{q+1} \in U_{n+q+1}$ such that $w_q = v_q^m w_{q+1}$ for each $q \geqslant 0$. This gives

$$u = v_0^m w_1 = v_0^m (v_1^m w_2) = (v_0 v_1)^m w_2 = \cdots = (v_0 v_1 \cdots v_q)^m w_{q+1}$$

   Then the sequence $\{w_q\}_{q \geqslant 0}$ tends to 1, and since K is complete, the product $v_0 v_1 \cdots v_q$ converges to an limit $v \in U_n$. But then $u = v^m \in U_n^m$, so $u = f(v)$.

□

1.3 Hensel's lemma

Theorem 1.12. Let K be a field complete with respect to a non-archimedean absolute value $|\cdot|$, and let $f(x) \in \mathfrak{o}[x]$, where $\mathfrak{o}$ is the ring of integers of $|\cdot|$. If

$$|f(\alpha_0)| < |f'(\alpha_0)|^2$$

for some $\alpha_0 \in \mathfrak{o}$, then there exists a unique $\alpha \in \mathfrak{o}$ such that

$$f(\alpha) = 0, \quad |\alpha - \alpha_0| \leqslant \frac{|f(\alpha)|}{|f'(\alpha)|}$$

Corollary 1.12.1. Let K be a field complete with respect to a non-archimedean absolute value $|\cdot|$, and let $f(x) \in \mathfrak{o}[x]$, where $\mathfrak{o}$ is the ring of integers of $|\cdot|$. If

$$f(\alpha_0) \equiv 0 \pmod{\mathfrak{p}}, \quad f'(\alpha_0) \not\equiv 0 \pmod{\mathfrak{p}}$$

for some $\alpha_0 \in \kappa = \mathfrak{o}/\mathfrak{p}$, then there exists a unique $\alpha \in \mathfrak{o}$ such that

$$f(\alpha) = 0, \quad |\alpha - \alpha_0| < 1$$

Proof. (of Theorem 1.12) Write

$$f(x+t) = f(x) + f'(x)t + g(x,t)t^2 \tag{1.2}$$

$$f'(x+t) = f'(x) + f''(x)t + h(x,t)t^2 \tag{1.3}$$

for some $g, h \in \mathfrak{o}[x,t]$. For $n \geqslant 0$, define α_n, $\beta_n \in \mathfrak{o}$ by the equations

$$f(\alpha_n) + \beta_n f'(\alpha_n) = 0, \quad \alpha_{n+1} = \alpha_n + \beta_n$$

For $n \geqslant 0$, using (1.2) and the construction of the β_n, we have

$$|f(\alpha_{n+1})| = |f(\alpha_n + \beta_n)| = |\beta_n^2 g(\alpha_n, \beta_n)| \leqslant |\beta_n|^2 = \frac{|f(\alpha_n)|^2}{|f'(\alpha_n)|^2} \leqslant \cdots \leqslant \frac{|f(\alpha_0)|^{2^{n+1}}}{|f'(\alpha_n)|^2 \cdots |f'(\alpha_0)|^{2^{n+1}}} \tag{1.4}$$

and using (1.3) gives

$$|f'(\alpha_{n+1}) - f'(\alpha_n)| \leqslant |\beta_n| = \frac{|f(\alpha_n)|}{|f'(\alpha_n)|}$$

We prove it by induction on n that

$$|f'(\alpha_n)| = |f'(\alpha_0)|$$

The statements hold when $n = 0$. In general, (1.4) and the assumption give

$$|f'(\alpha_{n+1}) - f'(\alpha_n)| \leqslant \frac{|f(\alpha_n)|}{|f'(\alpha_n)|} \leqslant \frac{|f(\alpha_0)|^{2^{n+1}}}{|f'(\alpha_0)|^{2^{n+2}-1}} = \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right|^{2^{n+1}} |f'(\alpha_0)| < |f'(\alpha_0)| = |f'(\alpha_n)|$$

so $|f'(\alpha_{n+1})| = |f'(\alpha_n)| = |f'(\alpha_0)|$, and (1.4) again gives

$$|f(\alpha_{n+1})| \leqslant \frac{|f(\alpha_0)|^{2^{n+1}}}{|f'(\alpha_0)|^{2^{n+2}-2}} = \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right|^{2^{n+1}} |f'(\alpha_0)|^2$$

Also,

$$|\beta_n| \leqslant \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right|^{2^{n+1}} |f'(\alpha_0)|$$

Finally, for $n \geqslant 0$,

$$|\alpha_n - \alpha_0| \leqslant \max\{|\beta_{n-1}|, \ldots, |\beta_0|\} \leqslant \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right|^2 |f'(\alpha_0)| < \left|\frac{f(\alpha_0)}{f'(\alpha_0)}\right|$$

Since $\left|\dfrac{f(\alpha_0)}{f'(\alpha_0)}\right| < 1$, both $f(\alpha_n)$, $\beta_n \to 0$ as $n \to \infty$, and put $\alpha = \lim\limits_{n\to\infty} \alpha_n \in K$. Hence

$$f(\alpha) = 0, \quad |\alpha - \alpha_0| \leqslant \left|\frac{f(\alpha_0)}{f'(\alpha_0)}\right|$$

The latter property and the assumption give $\alpha \in \mathfrak{o}$, for

$$|\alpha| \leqslant \max\{|\alpha - \alpha_0|, |\alpha_0|\} \leqslant \max\{|f'(\alpha_0)|, |\alpha_0|\} \leqslant 1$$

The uniqueness follows from (1.2) and $|f'(\alpha)| = |f'(\alpha_0)| \neq 0$; indeed, if $\alpha' \in \mathfrak{o}$ is another solution with the desired conditions, then, put $t = \alpha' - \alpha$,

$$|t| = |\alpha' - \alpha_0 + \alpha_0 - \alpha| \leqslant \left|\frac{f(\alpha_0)}{f'(\alpha_0)}\right|$$

and

$$0 = f(\alpha + t) = f(\alpha) + f'(\alpha)t + g(\alpha, t)t^2 = f'(\alpha)t + g(\alpha, t)t^2$$

If $t \neq 0$, then

$$|f'(\alpha_0)| = |f'(\alpha)| = |g(\alpha, t)t| \leqslant |t| \leqslant \left|\frac{f(\alpha_0)}{f'(\alpha_0)}\right|$$

a contradiction to the assumption. Hence $t = 0$. □

Corollary 1.12.2. Let R be a complete DVR and K its field of fractions. Put $U = R^\times$ to be the group of unit. Then for $n \geqslant 1$ not divisible by the characteristic of κ, the n-power subgroup

$$U^n = \{x^n \mid x \in U\}$$

is open in R.

Proof. Let $x \in U$ and $y \in R$ such that $|x^n - y| < 1$; then $y \in U$. Consider the equation $f(X) := X^n - y = 0$. We have $|f(x)| = |x^n - y| < 1$ and $|f'(x)| = |nx^{n-1}| = 1$, so by Hensel's lemma, there exists $\alpha \in R$ such that $y = \alpha^n$. Since $|y| = 1$, $|\alpha| = 1$ as well, implying $\alpha \in U$. Hence $y \in U^n$. □

1.4 Localization

Let A be a commutative ring with identity, and $S \subseteq A$ a multiplicatively closed subset containing 1; we write S is an m.c.s. for short. Define an equivalence relation $\sim$ on $A \times S$:

$$(a, s) \sim (b, r) \Leftrightarrow s'(ar - bs) = 0 \text{ for some } s' \in S$$

Define a ring $S^{-1}A = {}^{A \times S}/_{\sim}$. Symbolically we write an element of $S^{-1}A$ as $\dfrac{a}{s}$, $a \in A$, $s \in S$. This is called the **localization** of R at S. We have the canonical map $\begin{array}{rcl} \iota : A & \longrightarrow & S^{-1}A \\ a & \longmapsto & \dfrac{a}{1} \end{array}$.

Example. Let $\mathfrak{p} \trianglelefteq A$ be an ideal. Then $\mathfrak{p}$ is a prime if and only if $S := A - \mathfrak{p}$ is multiplicatively closed. In this case, we can form $S^{-1}A$, and it is usually denoted as $A_{\mathfrak{p}}$, and called the **localization** of A at $\mathfrak{p}$.

We give the universal property of the localization $S^{-1}A$. For any commutative ring B with identity, define $F(B) := \{\varphi \in \mathrm{Hom}_{\mathrm{Ring}}(A, B) \mid \varphi(S) \subseteq B^\times\}$; then it is easily seen that F is a functor.

Theorem 1.13. The map

$$\begin{array}{rcl} \mathrm{Hom}_{\mathrm{Ring}}(S^{-1}A, B) & \longrightarrow & F(B) \\ f & \longmapsto & f \circ \iota \end{array}$$

is a functorial bijection in B.

Proof. For $\varphi \in F(B)$, define $f_\varphi : S^{-1}A \to B$ by $f_\varphi(a/s) = \varphi(a)\varphi(s)^{-1}$. □

For an A-module M, we can define its localization at S as well. Define an equivalence relation $\sim$ on $M \times S$:

$$(m, s) \sim (n, r) \Leftrightarrow s'(mr - ns) = 0 \text{ for some } s' \in S$$

Define an abelian group $S^{-1}M = {}^{M \times S}/_{\sim}$. Then it's clear that $S^{-1}M$ is a $S^{-1}A$-module. In fact,

Proposition 1.14. $S^{-1}M \cong M \otimes_A S^{-1}A$ as $S^{-1}A$-modules.

Proof. Define

$$\begin{aligned} \varphi : M \times S^{-1}A &\longrightarrow S^{-1}M & \qquad \psi : S^{-1}M &\longrightarrow M \otimes_A S^{-1}A \\ \left(m, \frac{a}{s}\right) &\longmapsto \frac{ma}{s} & \frac{m}{s} &\longmapsto m \otimes \frac{1}{s} \end{aligned}$$

Then φ induces a $S^{-1}A$-homomorphism $M \otimes_A S^{-1}A \to S^{-1}M$ which we still denote by φ. Then

$$(\psi \circ \varphi)(m \otimes a/s) = \psi(ma/s) = ma \otimes 1/s = m \otimes a/s$$

$$(\varphi \circ \psi)(m/s) = \varphi(m \otimes 1/s) = m/s$$

so that ψ and φ are mutually inverses. □

The proposition in particular shows that $S^{-1} : \mathrm{Mod}_A \to \mathrm{Mod}_{S^{-1}A}$ is a functor. To be precise, for $f : M \to N$, define $S^{-1}f := f \otimes \mathrm{id}_{S^{-1}A} : M \otimes_A S^{-1}A \to N \otimes_A S^{-1}A$.

Proposition 1.15. S^{-1} is an exact functor. In other words, $S^{-1}A$ is a flat A-module.

Proof. Let $M \xrightarrow{f} N \xrightarrow{g} L$ be exact in Mod_A. Then

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

is a complex. Now let $\frac{n}{s} \in S^{-1}N$ such that $\frac{g(n)}{s} = 0$ in $S^{-1}L$. Then $0 = s'g(n) = g(s'n)$ in L for some $s' \in S$, so $s'n = f(m)$ for some $m \in M$. Thus

$$\frac{n}{s} = \frac{s'n}{s's} = \frac{f(m)}{s's}$$

□

1.4.1 Ideals in the localization

Proposition 1.16. Let S be an m.c.s. and $I \trianglelefteq A$ an ideal.

1. $S^{-1}I = S^{-1}A$ if and only if $S \cap I \neq \varnothing$.

2. For $J \trianglelefteq S^{-1}A$, $J = (J \cap A)S^{-1}A$.

3. $\begin{aligned} \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\} &\longrightarrow \mathrm{Spec}(S^{-1}A) \\ \mathfrak{p} &\longmapsto \mathfrak{p}S^{-1}A \end{aligned}$ is a bijection.

Proof.

1. For $s \in S$, if $\frac{1}{s} \in S^{-1}I$, then $s'(r - bs) = 0$ for some $r, s' \in S$, $b \in I$, so that $rs' = bss' \in S \cap I$. Conversely, pick $r \in S \cap I$. Then for any $s \in S$, $\frac{1}{s} = \frac{r}{sr} \in S^{-1}I$.

2. Clearly, $(J \cap A)S^{-1}A \subseteq J$. Conversely, for $\dfrac{x}{s} \in J$, $x = s \cdot \dfrac{x}{s} \in J \cap A$, so that $\dfrac{x}{s} \in (J \cap A)S^{-1}A$.

3. For $\mathfrak{P} \in \operatorname{Spec}(S^{-1}A)$, since $(\mathfrak{P} \cap A)S^{-1}A = \mathfrak{P} \subsetneq S^{-1}A$, $(\mathfrak{P} \cap A) \cap S = \varnothing$. Conversely, let $\mathfrak{p} \in \operatorname{Spec}(A)$ with $\mathfrak{p} \cap S = \varnothing$. Then $\mathfrak{p}S^{-1}A$ is an ideal in $S^{-1}A$.

   Claim.

   (a) $\mathfrak{p}S^{-1}A \in \operatorname{Spec}(S^{-1}A)$.

   (b) $(\mathfrak{p}S^{-1}A) \cap A = \mathfrak{p}$

   Proof.

   (a) Let $\dfrac{x}{s}, \dfrac{y}{r} \in S^{-1}A$ with $\dfrac{xy}{sr} = \dfrac{z}{t} \in \mathfrak{p}S^{-1}A$, $z \in \mathfrak{p}$ but $x, y \notin \mathfrak{p}$. Then $s'xyt = s'srt \in \mathfrak{p} \cap S$ for some $s' \in S$, a contradiction.

   (b) Clearly, $\mathfrak{p} \subseteq (\mathfrak{p}S^{-1}A) \cap A$. Conversely, let $\dfrac{a}{1} = \dfrac{x}{s} \in (\mathfrak{p}S^{-1}A) \cap A$, $x \in \mathfrak{p}$. Then $s(x - ra) = 0$ for some $s \in S$. If $a \in A - \mathfrak{p}$, then $\mathfrak{p} \ni sx = sra \in A - \mathfrak{p}$, a contradiction. (Note that $S \subseteq A - \mathfrak{p}$).

   □

□

Note that $IS^{-1}A \cong I \otimes_A S^{-1}A \cong S^{-1}I$ as $S^{-1}A$-modules.

Corollary 1.16.1. If A is Noetherian, so is $S^{-1}A$.

Proof. By the proposition, every ideal of $S^{-1}A$ is of the form $IS^{-1}A \cong S^{-1}I$ for some $I \trianglelefteq A$. A being Noetherian, there is an exact sequence $A^n \to I \to 0$ for some $n \in \mathbb{N}_0$. Since $S^{-1}A$ is flat over A, $(S^{-1}A)^n \to S^{-1}I \to 0$ is exact. Hence $S^{-1}I$ finitely generated. □

1.4.2 Integral dependence

Proposition 1.17. Let $A \subseteq B$ be rings and C be the integral closure of A in B. Let $S \subseteq A$ be an m.s.c. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Proof. Let $bs^{-1} \in S^{-1}B$ integral over $S^{-1}A$. Then $f(bs^{-1}) = 0$ for some monic $f \in S^{-1}A[x]$. Multiplying a multiple of denominators of coefficients, we obtain

$$a_n b^n + a_{n-1} s b^{n-1} + \cdots + a_1 s^{n-1} b + a_0 s^n = 0$$

for some $a_i \in A$ and $a_n \in S$. Then $a_n b \in B$ is integral over A, implying $a_n b \in C$. Hence $\dfrac{b}{s} = \dfrac{a_n b}{a_n s} \in S^{-1}C$.

Conversely, it is easy to see every element in $S^{-1}C$ is integral over $S^{-1}A$. □

1.5 Dedekind Domains

In this section R always means an integral domain with K its field of fraction. If $\mathfrak{p} \in \operatorname{Spec} R$, define the local ring of fractions at $\mathfrak{p}$ by

$$R_{\mathfrak{p}} = \{xy^{-1} \in K \mid x, y \in R,\ y \notin \mathfrak{p}\}$$

Proposition 1.18.

1. $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.
2. $\mathfrak{p} = \mathfrak{p}R_{\mathfrak{p}} \cap R$.
3. If $J \trianglelefteq R_{\mathfrak{p}}$, then $J = (J \cap R)R_{\mathfrak{p}}$.

Proof. We have already seen $2, 3$ in the section for localization. For 1., it suffices to show $R_{\mathfrak{p}}^{\times} = R_{\mathfrak{p}} - \mathfrak{p}R_{\mathfrak{p}}$.

- If $xy^{-1} \in R_{\mathfrak{p}}^{\times}$, then $x^{-1} \in R_{\mathfrak{p}}$, so that $x \notin \mathfrak{p}$. Hence $xy^{-1} \in R_{\mathfrak{p}} - \mathfrak{p}R_{\mathfrak{p}}$.
- If $xy^{-1} \in R_{\mathfrak{p}} - \mathfrak{p}R_{\mathfrak{p}}$, then $x \notin \mathfrak{p}$ so that $x^{-1}y \in R_{\mathfrak{p}}$.

□

Theorem 1.19. Let R be an integral domain. Then TFAE:

1. R is Noetherian, integrally closed and its nonzero primes are maximal.
2. R is Noetherian, any for any non-zero prime $\mathfrak{p}$, $R_{\mathfrak{p}}$ is a DVR.
3. All fractional ideals are invertible.

Proof. If $R = K$ is a field, then everything holds trivially. In the following we assume R is not a field.

1. ⇒ 2. We invoke Theorem 1.8. To show $R_{\mathfrak{p}}$ is a DVR, it suffices to show it is Noetherian, integrally closed and local but not a field. We will implicitly use the results in the section of localization.

   Since R is Noetherian and integrally closed, so is $R_{\mathfrak{p}}$. Since $\mathfrak{p} \neq 0$, $R_{\mathfrak{p}}$ is local with maximal ideal $\mathfrak{p}R_{\mathfrak{p}} \neq 0$.

2. ⇒ 3. Let I be a fractional ideal. By lemmas in 1.1, I is finitely generated; say $I = (a_1, \ldots, a_n)_R$. Let $x = \sum_{i=1}^{n} r_i a_i \in I$. Denote by $\nu_{\mathfrak{p}}$ the valuation in $R_{\mathfrak{p}}$. Then

   $$\nu_{\mathfrak{p}}(x) \geqslant \inf_{i=1,\ldots,n} \nu_{\mathfrak{p}}(r_i a_i) \geqslant \inf_{i=1,\ldots,n} \nu_{\mathfrak{p}}(a_i)$$

   Now assume that a_1 is such that $\nu_{\mathfrak{p}}(a_1) = \inf_{i=1,\ldots,n} \nu_{\mathfrak{p}}(a_i)$. Then $IR_{\mathfrak{p}} = a_1 R_{\mathfrak{p}}$.

   Now let $a_1^{-1}a_i = x_i y_i^{-1}$ with $x_i, y_i \in R$ and $y_i \notin \mathfrak{p}$. Put $y = y_1 \cdots y_n$. Then $ya_1^{-1}a_i \in R$, so that $ya_1^{-1} \in I^{-1}$, whence $y \in II^{-1}$. However $y \notin \mathfrak{p}$, so $II^{-1} \nsubseteq \mathfrak{p}$. Since this is true for all maximal $\mathfrak{p}$, $II^{-1} = R$.

3. $\Rightarrow$ 1. By lemmas in 1.1, every invertible ideal are finitely generated, so that R is Noetherian.

   Let $x \in K$ be integral over R. Then $S := R[x] \subseteq K$ is finitely generated. By lemmas in 1.1, S is fractional. Since S is a ring, $S^2 = S$. Thus

   $$S = SR = S(SS^{-1}) = S^2S^{-1} = SS^{-1} = R$$

   so $x \in R$. Therefore R is integrally closed.

   Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be nonzero and $\mathfrak{m} \in \operatorname{mSpec}(R)$ containing $\mathfrak{p}$. Then $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$ and $(\mathfrak{p}\mathfrak{m}^{-1})\,\mathfrak{m} = \mathfrak{p}$. Since $\mathfrak{p}$ is a prime, we have either $\mathfrak{m} \subseteq \mathfrak{p}$ or $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{p}$; if the latter were to happen,

   $$\mathfrak{m}^{-1} \subseteq \mathfrak{p}^{-1}\mathfrak{p} = R$$

   so that $\mathfrak{m}^{-1} \subseteq R$, i.e., $\mathfrak{m} = R$, a contradiction. Hence $\mathfrak{m} \subseteq \mathfrak{p}$, and thus $\mathfrak{p}$ is maximal.

□

Definition. If R is an integral domain satisfying any of the statements in Theorem 1.19, we call R a **Dedekind domain**.

- If $\mathfrak{p}$ is a nonzero prime of R, we denote by $\nu_{\mathfrak{p}}$ the valuation on the field of fractions K of R with valuation ring $R_{\mathfrak{p}}$.
- If $|\cdot|$ is a nontrivial absolute value (i.e., $|x| \neq 1$ for some $x \in K$) on K with $|R| \leqslant 1$. Then $|x| = \rho^{\nu_{\mathfrak{p}}(x)}$ for some $0 < \rho < 1$ and some nonzero prime $\mathfrak{p}$ of R.

  Proof. Let $\mathfrak{p} = \{x \in R \mid |x| < 1\}$. Then $\mathfrak{p} \in \operatorname{Spec}(R)$ is nonzero. We show

  $$|x| = |\pi|^{\rho_{\mathfrak{p}}(x)}$$

  where π is the uniformizer of $R_{\mathfrak{p}}$.

  - Write $\pi = ab^{-1}$ with $a, b \in R$, $a \in \mathfrak{p} \not\ni b$. Then $|b| = 1$ and $a = b\pi \in \mathfrak{p}$, so $|\pi| < 1$. Since $\pi \neq 0$, $|\pi| > 0$.
  - For $u \in R_{\mathfrak{p}}^{\times}$, write $u = xy^{-1}$ with $x, y \in R - \mathfrak{p}$. Then $|u| = |xy^{-1}| = 1$. Now for every $x \in K^{\times}$, write $x = \pi^n u$ for some unique $u \in R_{\mathfrak{p}}^{\times}$, $n \in \mathbb{Z}$. Then $|x| = |\pi|^n|u| = |\pi|^n = |\pi|^{\nu_{\mathfrak{p}}(x)}$.

  □

- For $\varnothing \neq I \subseteq K$, define $\nu_{\mathfrak{p}}(I) := \inf\limits_{x \in I} \nu_{\mathfrak{p}}(x) \in \mathbb{Z} \cup \{\pm\infty\}$.

Theorem 1.20. Let R be a Dedekind domain.

1. The fractional ideals of R form an abelian group $\mathfrak{I}(R)$ under multiplication.

2. $\mathfrak{I}(R)$ is free on the nonzero primes of R.

3. For a fractional ideal I,
$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(I)}$$
Also, $IR_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^{\nu_{\mathfrak{p}}(I)}$

Proof. The first follows from Theorem 1.19 and lemmas in 1.1. To show the nonzero primes generate $\mathfrak{I}(R)$, it suffices to show every integral ideal $I \subseteq R$ is a product of primes. If $I \neq R$, then $I \subseteq \mathfrak{p}$ for some $\mathfrak{p}$, and $I \subseteq I\mathfrak{p}^{-1} \subseteq R$. Continuing in this way on $I\mathfrak{p}^{-1}$. the result then follows since R is Noetherian.

For each $\mathfrak{p}$, we have a surjective homomorphism
$$f_{\mathfrak{p}} : \mathfrak{I}(R) \longrightarrow \mathfrak{I}(R_{\mathfrak{p}})$$
$$I \longmapsto IR_{\mathfrak{p}}$$

- If $f_{\mathfrak{p}}(\mathfrak{p}^n) = (\mathfrak{p}R_{\mathfrak{p}})^n = R_{\mathfrak{p}}$, then $n = 0$.

- If $\mathfrak{q} \neq \mathfrak{p}$, then $\mathfrak{q} \cap (R - \mathfrak{p}) \neq \varnothing$ so that $f_{\mathfrak{p}}(\mathfrak{q}) = R_{\mathfrak{p}}$.

Hence $\ker f_{\mathfrak{p}}$ contains all nonzero primes other than $\mathfrak{p}$. This shows $\mathfrak{I}(R)$ is free on the set of nonzero primes. Finally, write
$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$
Then $IR_{\mathfrak{p}} = f_{\mathfrak{p}}(I) = (\mathfrak{p}R_{\mathfrak{p}})^{n_{\mathfrak{p}}}$, so that
$$n_{\mathfrak{p}} = \nu_{\mathfrak{p}}(IR_{\mathfrak{p}}) = \nu_{\mathfrak{p}}(I) + \nu_{\mathfrak{p}}(R_{\mathfrak{p}}) = \nu_{\mathfrak{p}}(I)$$

□

Corollary 1.20.1. If $a \in K^{\times}$, then $\nu_{\mathfrak{p}}(a) = 0$ for almost all $\mathfrak{p}$.

Corollary 1.20.2. Let $I, J \in \mathfrak{I}(R)$.

1. $\nu_{\mathfrak{p}}(IJ) = \nu_{\mathfrak{p}}(I) + \nu_{\mathfrak{p}}(J)$;

2. $\nu_{\mathfrak{p}}(I^{-1}) = -\nu_{\mathfrak{p}}(I)$;

3. $\nu_{\mathfrak{p}}(I + J) = \inf\{\nu_{\mathfrak{p}}(I), \nu_{\mathfrak{p}}(J)\}$;

4. $\nu_{\mathfrak{p}}(I \cap J) = \sup\{\nu_{\mathfrak{p}}(I), \nu_{\mathfrak{p}}(J)\}$.

Corollary 1.20.3. The maps $f_{\mathfrak{p}}$ induces a group isomorphism
$$\mathfrak{I}(R) \cong \bigoplus_{\mathfrak{p}} \mathfrak{I}(R_{\mathfrak{p}})$$

Let $\overline{R_{\mathfrak{p}}}$ be the valuation ring of the completion of K at $\nu_{\mathfrak{p}}$. By Proposition 1.6, $\mathfrak{I}(R_{\mathfrak{p}}) \cong \mathfrak{I}(\overline{R_{\mathfrak{p}}})$. Hence

Corollary 1.20.4.
$$\mathfrak{I}(R) \cong \bigoplus_{\mathfrak{p}} \mathfrak{I}(\overline{R_{\mathfrak{p}}})$$

1.5.1 Modules and Bilinear Forms

Throughout this subsection, let R be a Dedekind domain, K its fraction field, U an $n > 0$ dimensional K-vector space. The symbols L, M, N stand for finite R-submodules of U which span U.

Lemma 1.21. For an R-submodule T of U, we have

$$T = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(R)} T_{\mathfrak{p}} = \bigcap_{\mathfrak{p}\in \mathrm{mSpec}(R)} T_{\mathfrak{p}}$$

Lemma 1.22. Given M, N, there is a nonzero element a of K with $aM \subseteq N$.

Proof. Let $\{u_i\}$ be a basis of U contained in N. For a finite generating $\{w_j\}$ set of M, choose $a \in R$ to eliminate the denominators of coefficients of the w_j with respect to $\{u_i\}$. □

Lemma 1.23. For almost all $\mathfrak{p}$, $M_{\mathfrak{p}} = N_{\mathfrak{p}}$.

Proof. By Lemma, we find $a, b \in K^\times$ with $aM \subseteq N \subseteq bM$. Hence $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ if $\nu_{\mathfrak{p}}(a) = 0 = \nu_{\mathfrak{p}}(b)$, which is the case for almost all $\mathfrak{p}$. □

Suppose for a while that M, N are free over R, hence of rank n. Then there exists $\ell \in \mathrm{GL}(U)$ such that $M\ell = N$. The determinant $\det(\ell)$ is non-zero, and solely depends on M, N up to a unit in R. Hence the fractional ideal

$$[M : N] := R\det(\ell)$$

solely depends on M, N.

Now drop the condition that M, N are free. Nevertheless, for each $\mathfrak{p} \in \mathrm{Spec}(R)$, we see $M_{\mathfrak{p}}, N_{\mathfrak{p}}$ are contained in U, and hence they are torsion-free. This shows $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are free over $R_{\mathfrak{p}}$ of the same rank n, so the fractional ideal $[M_{\mathfrak{p}} : N_{\mathfrak{p}}]$ is well-defined. Moreover, by Lemma above, $[M_{\mathfrak{p}} : N_{\mathfrak{p}}] = R_{\mathfrak{p}}$ for almost all $\mathfrak{p}$.

Definition. The **module index** $[M : N] = [M : N]_R$ is defined to be the unique fractional ideal such that

$$[M : N]R_{\mathfrak{p}} = [M_{\mathfrak{p}} : N_{\mathfrak{p}}]$$

for all $\mathfrak{p} \in \mathrm{Spec}(R)$; both existence and uniqueness follow from Corollary 1.20.3.

- When M, N are free, two definition clearly agree.
- When $R = \mathbb{Z}$ and $N \subseteq M$, $[M : N]$ is just the ordinary group index.

Property 1.24. Let U, M, N, L as above. Then

1. $[M : N][N : L] = [M : L]$ and $[M : M] = R$.
2. If $N \subseteq M$, then $[M : N] \subseteq R$, and $[M : N] = R$ iff $M = N$.

3. If $t \in \mathrm{GL}(U)$, then $[Mt : Nt] = [M, N]$.

Proof. Locally, we can suppose M, N, L are free, and all are clear. Then use Lemma 1.21 to obtain the global result. □

Proposition 1.25. $[M : N]$ is a principal fractional ideal if and only if $M \cong N$.

Definition. Let $B : U \times U \to K$ be a nondegenerate, symmetric K-bilinear form on U.

1. For a K-basis $\{u_i\}$ for U, its **dual basis** $\{v_j\}$ is defined by $B(u_i, v_j) = \delta_{ij}$.
2. The **dual module** of T is defined by

$$D(T) = D_R(T) := \{u \in U \mid B(u, T) \subseteq R\}$$

- If M is the free R-module on $\{u_i\}$, then $D(M)$ is the free R-module on the dual basis $\{v_j\}$, and $D(D(M)) = M$.
- In the following we put $D = D_R$ and $D_{\mathfrak{p}} = D_{R_{\mathfrak{p}}}$.

Property 1.26.

1. $D(M)$ is a finite R-module spanning U.
2. $D(M)_{\mathfrak{p}} = D_{\mathfrak{p}}(M_{\mathfrak{p}})$.
3. $D(M) = \bigcap\limits_{\mathfrak{p} \in \mathrm{Spec}(R)} D_{\mathfrak{p}}(M_{\mathfrak{p}})$.
4. $D(D(M)) = M$.
5. $[D(M) : D(N)] = [N : M]$.

Proof.

1. M contains a free R-module N spanning U, and by previous lemma M is contained in $L = bN$ for some $b \in K^\times$. Hence $N \subseteq M \subseteq L$ implies

$$D(N) \supseteq D(M) \supseteq D(L)$$

We know $D(L)$ generates U and $D(N)$ is finite over R, and hence $D(M)$ has the desired properties.

2. Say $\{w_i\}$ is a finite generating set of M. Suppose $v \in D_{\mathfrak{p}}(M_{\mathfrak{p}})$. Then for all i, $B(v, w_i) = b^{-1} a_i$ with $a_i, b \in R$ and $b \notin \mathfrak{p}$. Hence $v \in D(M)b^{-1} \subseteq D(M)_{\mathfrak{p}}$. Conversely, we have

$$B(D(M)_{\mathfrak{p}}, M_{\mathfrak{p}}) \subseteq B(D(M), M)R_{\mathfrak{p}} \subseteq R_{\mathfrak{p}}$$

3. Use 2. and Lemma 1.21.

4. $D(D(M))_{\mathfrak{p}} = D_{\mathfrak{p}}(D_{\mathfrak{p}}(M_{\mathfrak{p}})) = M_{\mathfrak{p}}$. Use Lemma 1.21.

5. Locally we can assume M, N are free. Suppose $\{u_i\}$ and $\{v_j\}$ are dual bases and $\{u_i\ell\}$ and $\{v_j\ell^*\}$ are dual basis, then we must have $\det(\ell)\det(\ell^*) = 1$. Say u_i is a basis for N and $u_i\ell$ is a basis for M, Then
$$[N : M] = \det(\ell)R = \det({\ell^*}^{-1})R = [D(M) : D(N)]$$

□

Definition. For a finite R-submodule M of U which spans U, define the **discriminant** of M to be
$$\mathfrak{d}(M) = \mathfrak{d}(M/R) := [D_R(M) : M]_R$$

Property 1.27. Let M, N as above.

1. $\mathfrak{d}(N) = \mathfrak{d}(M)[M : N]^2$.

2. $\mathfrak{d}(M_{\mathfrak{p}}/R_{\mathfrak{p}}) = \mathfrak{d}(M/R)R_{\mathfrak{p}}$.

3. If M is the free R-module on $\{u_i\}$, then $\mathfrak{d}(M)$ is the fractional ideal generated by $\det B(u_i, u_j)$.

4. If $N \subseteq M$, then $\mathfrak{d}(M) \mid \mathfrak{d}(N)$, and $\mathfrak{d}(M) = \mathfrak{d}(N)$ iff $M = N$.

Proof.

1. $[D(N) : N] = [D(N) : D(M)][D(M) : M][M : N] = [D(M) : M][M : N]^2$.

2. $[D_{\mathfrak{p}}(M_{\mathfrak{p}}) : M_{\mathfrak{p}}] = [D(M)_{\mathfrak{p}} : M_{\mathfrak{p}}] = [D(M) : M]R_{\mathfrak{p}}$.

3. Let $\{v_j\}$ be the dual basis of $\{u_i\}$ and write $u_i = v_i\ell$. Then $[D(M) : M] = \det(\ell)R$. On the other hand,
$$\det B(u_i, u_j) = \det B(u_i, v_j\ell) = \det(\ell)\det B(u_i, v_j) = \det(\ell)$$

4. Since $N \subseteq M$, $[M : N]$ is integral, and equals R iff $N = M$. Then it follows from 1.

□

Proposition 1.28. Let U_i be a finite dimensional K-vector space and M_i, N_i are R-submodules of U_i that span U_i. Set $U = U_1 \oplus U_2$, and similar for M, N.

1. $[M : N] = [M_1 : N_1][M_2 : N_2]$.

Suppose moreover that $B(U_1, U_2) = 0$. Then

2. $D(M) = D(M_1) \oplus D(M_2)$.

3. $\mathfrak{d}(M) = \mathfrak{d}(M_1)\mathfrak{d}(M_2)$

Let $\overline{R}$ be a Dedekind domain containing R with quotient field $\overline{K}$. Embed U into the vector space $\overline{U} := U \otimes_K \overline{K}$. B can be extended uniquely to a non-degenerate symmetric $\overline{K}$-bilinear form $\overline{B}$ on $\overline{U}$.

Proposition 1.29.

1. $[M\overline{R} : N\overline{R}]_{\overline{R}} = [M : N]_R\overline{R}$.

2. $D_{\overline{R}}(M\overline{R}) = D_R(M)\overline{R}$.

3. $\mathfrak{d}(M\overline{R}/\overline{R}) = \mathfrak{d}(M/R)\overline{R}$.

1.6 Extensions

Let R be a Dedekind domain with fraction field K. Let L be a finite extension of K, and let S be the integral closure of R in L. We know that $S \otimes_R R_{\mathfrak{p}}$ is the integral closure of $R_{\mathfrak{p}}$ in L for each $\mathfrak{p} \in \mathrm{Spec}(R)$.

Definition. A prime $\mathfrak{P} \in \mathrm{Spec}(S)$ is said to **lie over** the prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ if $\mathfrak{P} \cap R = \mathfrak{p}$. If it is the case, we write $\mathfrak{P} \mid \mathfrak{p}$.

1.6.1 Krull-Akizuki

We temporarily drop the notation set above. Suppose now A is a Noetherian domain of dimension 1 and K its fraction field. Let M be a torsion-free A-module. Set $\operatorname{rank} M = \dim_K K \otimes_A M$.

Lemma 1.30. For $x \in A$, we have

$$\operatorname{length}_A(M/xM) \leqslant \operatorname{rank}(M) \operatorname{length}_A(A/xA)$$

with equality if M is finite over A.

Proof. Set $r = \operatorname{rank}(M)$; if M is finite over A, then $r < \infty$. If $r = \infty$, there is nothing to prove, so we may assume $r < \infty$.

Assume M is finite over A, and pick $m_1, \ldots, m_r \in M$ such that they form a K-basis for $K \otimes_A M$. Let $\alpha : A^r \to M$ be a homomorphism sending a basis of A^r to the m_i; by construction α is injective, so we may assume A^r as a submodule of M. Put $N = M/A^r$; we have $K \otimes_A N = 0$. Consider the exact sequence

$$0 \longrightarrow A^r \longrightarrow M \longrightarrow N \longrightarrow 0$$

Tensoring with A/xA, we have an exact sequence

$$\mathrm{Tor}_1^A(M, A/xA) \longrightarrow \mathrm{Tor}_1^A(N, A/xA) \longrightarrow A^r/xA^r \longrightarrow M/xM \longrightarrow N/xN \longrightarrow 0$$

Using the free resolution $0 \to A \xrightarrow{x} A \to A/xA \to 0$ of A/xA, we see $\mathrm{Tor}_1^A(M, A/xA) = \{m \in M \mid xm = 0\}$ and similar for $\mathrm{Tor}_1^A(N, A/xA)$. Since M is torsion-free, $\mathrm{Tor}_1^A(M, A/xA) = 0$. Also, consider the exact sequence

$$0 \longrightarrow \mathrm{Tor}_1^A(N, A/xA) \longrightarrow N \xrightarrow{x} N \longrightarrow N/xN \longrightarrow 0$$

Since $K \otimes_A N = 0$ and N is finite over A, there exists $f \in A - \{0\}$ with $fN = 0$, making the modules appearing in the above complex A/fA-module. Since $\dim A = 1$, $\dim A/fA = 0$, implying the modules above are of finite length. Hence

$$\mathrm{length}\, \mathrm{Tor}_1^A(N, A/xA) = \mathrm{length}(N) - \mathrm{length}(N) + \mathrm{length}(N/xN) = \mathrm{length}(N/xN)$$

Using the complex involving M/xM above, and noting that they are all A/xA-module, we have

$$\begin{aligned}\mathrm{length}(M/xM) &= \mathrm{length}(A^r/xA^r) + \mathrm{length}(N/xN) - \mathrm{length}\, \mathrm{Tor}_1^A(N, A/xA) \\ &= \mathrm{length}(A^r/xA^r) \\ &= r\, \mathrm{length}(A/xA)\end{aligned}$$

proving the equality when M is finite over A.

Now drop the condition that M is finite over A. Suppose the inequality in Lemma does not hold, i.e. $\mathrm{length}(M/xM) > r\, \mathrm{length}(A/xA)$. Choose a finite submodule M' of M whose image N' in M/xM has length $> r\, \mathrm{length}(A/xA)$, which is possible. Indeed, we can find a filtration

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell \subseteq M/xM$$

with $\ell > r\, \mathrm{length}(A/xA)$. Pick $m_i \in M$ such that $(m_i \bmod xM) \in M_i \backslash M_{i-1}$, and define $M' = \sum_{i=1}^{\ell} m_i A$. Put $M_i' = ((M_i + xM) \cap M')/xM' \subseteq M'/xM'$. Then M'/xM admits a filtration

$$0 \subsetneq M_1' \subsetneq \cdots \subsetneq M_\ell' \subseteq M'/xM'$$

by our construction. Hence $\mathrm{length}(M'/xM') \geqslant \ell$ as we wish. But then

$$\mathrm{length}(M'/xM') \geqslant \mathrm{length}\, N' > r\, \mathrm{length}(R/xR) \geqslant \mathrm{rank}(M')\, \mathrm{length}(R/xR)$$

contradicting to the equality proved in the finite case. □

Theorem 1.31 (Krull-Akizuki)**.** Let R be a Noetherian domain of dimension 1 with fraction field K and L/K a finite field extension. Let S be any subring of L containing R. Then

1. S is Noetherian and of dimension $\leqslant 1$.

2. For any nonzero ideal J of S, $\mathrm{length}_R\, S/JS < \infty$.

3. $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ has finite fibres.

Proof. Let $0 \neq J \trianglelefteq S$ be an ideal. We first show $J \cap R \neq 0$. Pick $x \in J$. Then x satisfies a polynomial over K; eliminating the denominators, we may assume the polynomial has coefficients in R. Then the constant term lies in $J \cap R$. We contend J/aS is a module of finite length. Since $J/aS \subseteq S/aS$ and S is torsion-free R-module of finite rank, Lemma applies, showing that S/aS has finite length, thus so does J/aS. This implies J is a finite S-module, and hence S is Noetherian.

If J is a nonzero prime, so is $J \cap R$; since $\dim R = 1$, $J \cap R =: \mathfrak{m}$ is a maximal ideal of R. What we proved above show $S/\mathfrak{m}S$ has finite length, and thus $S/\mathfrak{m}S$ is Artinian. Hence every nonzero prime of S containing $\mathfrak{m}S$ is maximal and there are in finite number. This shows J is maximal, proving $\dim S \leqslant 1$.

□

Corollary 1.31.1. Let R be a Dedekind domain with fraction field K and L/K a finite extension. Then the integral closure of R in L is a Dedekind domain.

1.6.2 Trace form

Definition. For a finite field extension L/K, the **trace** $\mathrm{Tr}_{L/K}(x)$ of $x \in L$ is defined to be the trace of the K-linear map $T_x : L \to L$ defined by multiplication by x on L.

- $\mathrm{Tr}_{L/K} : L \to K$ is a K-linear map.

- Let U be a finite dimensional L-vector space and $\varphi \in \mathrm{End}_L(U)$. Then $\mathrm{trace}_K(\varphi) = \mathrm{Tr}_{L/K}(\mathrm{trace}_L(\varphi))$.

  Proof. Say $\{e_i\}$ is an L-basis for U. The identity is L-linear on both side, so we may assume $\varphi(e_i) = ae_j$ ($a \in L^\times$) and zero on other basis elements. Let $\{\alpha_j\}$ be a K-basis for L. Then $\varphi(\alpha_s e_k) = \delta_{ki} T_a(\alpha_s) e_j$. If $i \neq j$, then $\mathrm{trace}_K(\varphi) = 0 = \mathrm{Tr}_{L/K}(\mathrm{trace}_L(\varphi))$. If $i = j$, then

  $$\mathrm{trace}_K(\varphi) = \mathrm{trace}_K(T_a) = \mathrm{Tr}_{L/K}(a) = \mathrm{Tr}_{L/K}\,\mathrm{trace}_L(\varphi)$$

  □

- For a tower of finite extensions $K \subseteq L \subseteq M$, $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$.

- The characteristic polynomial of $T_\alpha \in \mathrm{End}_K(L)$ equals $m_{\alpha,K}^e$ with $e \deg(m_{\alpha,K}) = [L : K]$.

  Proof. Say $\{\beta_i\}_{i=1}^e$ is a basis for $L/K(\alpha)$; then $e \deg(m_{x,K}) = [L : K]$ and $L = \bigoplus_{i=1}^{e} K(\alpha)\beta_i$ is a decomposition of L into α-invariant subspace. Hence the characteristic polynomial of $T_\alpha \in \mathrm{End}_K(L)$ equals that of $T_\alpha \in \mathrm{End}_K(K(\alpha))$ to the power of e.

  Now we can assume $L = K(\alpha)$. By Cayley-Hamilton we have $m_{\alpha,K} \mid \mathrm{Char}_{T_\alpha}$. Since they are both monic of degree $[K(\alpha) : K]$, they are the same. □

Proposition 1.32. Let L/K be a finite field extension. Put $\mathrm{Tr} = \mathrm{Tr}_{L/K}$. TFAE:

1. L/K is separable.

2. Tr is not identically zero, or equivalently, surjective.

3. The pairing $Q : L \times L \to K$ defined by $Q(x, y) = \mathrm{Tr}(xy)$ is non-degenerate.

Proof. $3 \Rightarrow 2$ is clear. Conversely, say $\mathrm{Tr}(x) \neq 0$. Then for each $y \in L^\times$, $Q(y, x/y) = \mathrm{Tr}(x) \neq 0$.

Now suppose L/K is separable. By transitivity of trace together with the induction, we can assume L is a simple extension of K. Let $\alpha_1, \ldots, \alpha_n$ be all conjugates of α over K; they are distinct by separability, and they are the eigenvalues of the map $T_\alpha : x \mapsto \alpha x$. Put $\chi_i : \mathbb{Z} \to L$ to be $\chi_i(r) = \alpha_i^r$. By independence of characters, there exists $e \in \mathbb{Z}$ such that $\chi_1(e) + \cdots + \chi_n(e) \neq 0$, so that $\mathrm{Tr}(\alpha^e) \neq 0$.

Now suppose L/K is not separable. Then by transitivity we have $\mathrm{Tr}_{L/K} = \mathrm{Tr}_{L^{\mathrm{sep}}/L} \mathrm{Tr}_{L/L^{\mathrm{sep}}}$, so it suffices to show $\mathrm{Tr}_{L/L^{\mathrm{sep}}}$ is identically zero. Hence we can assume L/K is purely inseparable, and let $p = \mathrm{Char}(K) > 0$. As above we can assume $L = K(\alpha)$ for some $\alpha \in L^\times$. We have $m_{\alpha,K}(x) = f(x^{p^k})$ for some irreducible separable $f \in K[x]$ and some $k \in \mathbb{Z} - \{0\}$, so $\alpha^{p^k} \in K$. Replace α by $\alpha^{p^{k-1}}$, we assume $\alpha^p \in K$. Now we can obtain $\mathrm{Tr}_{L/K}(\alpha^i) = 0$ for each $i \in \mathbb{Z}$, showing that $\mathrm{Tr}_{L/K} \equiv 0$. □

Proposition 1.33. Let R be a Noetherian integrally closed domain with fraction field K and L/K a finite separable extension. Then the integral closure S of R in L is finite over R.

Proof. Pick a basis $\{u_i\}$ for L/K such that $u_i \in S$. Since L/K is separable, $\mathrm{Tr}_{L/K}$ is non-degenerate; let $\{v_j\}$ be the dual basis of $\{u_i\}$. Now for each $x \in S$, write $x = \sum a_i u_i$. Since $xv_j \in S$, we have $\mathrm{Tr}_{L/K}(xv_j) = a_j \in R$, showing $S \subseteq \sum Ru_i$. □

1.7 Ramification

Lemma 1.34. Let R be a ring and M an R-module of finite length. Let $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ be a composition series of M. Then

1. $M_i/M_{i-1} \cong A/\mathfrak{m}_i$ for some maximal ideal $\mathfrak{m}_i$.

2. For each $\mathfrak{m} \in \mathrm{mSpec}(A)$, we have $\#\{i \mid \mathfrak{m}_i = \mathfrak{m}\} = \mathrm{length}_{A_\mathfrak{m}} M_\mathfrak{m}$.

Proof. Since the M_i is a composition series, each successive quotient is simple, so 1. follows. Now since the localization functor is exact, we then obtain a filtration of $M_\mathfrak{m}$:

$$0 = (M_0)_\mathfrak{m} \subsetneq (M_1)_\mathfrak{m} \subsetneq \cdots \subsetneq (M_n)_\mathfrak{m} = M_\mathfrak{m}$$

Last, we have

$$(R/\mathfrak{m}')_\mathfrak{m} = \begin{cases} 0 & , \mathfrak{m} \neq \mathfrak{m}' \\ R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m} & , \mathfrak{m} = \mathfrak{m}' \end{cases}$$

From these the second statement follows at once. □

Proposition 1.35. Let $(A, \mathfrak{m})$ be a local ring, B an A-algebra and M a B-module of finite length. Suppose B is semilocal with maximal ideal $\mathfrak{n}_1, \ldots, \mathfrak{n}_q$, each of which lying over $\mathfrak{m}$. Then

$$\operatorname{length}_A M = \sum_{i=1}^{q} [\kappa(\mathfrak{n}_i) : \kappa(\mathfrak{m})] \operatorname{length}_{B_{\mathfrak{n}_i}} M_{\mathfrak{n}_i}$$

Proof. Let $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ be a composition series of M. Then by Lemma,

$$\operatorname{length}_A M = \sum_{i=1}^{n} \operatorname{length}_A M_i/M_{i-1} = \sum_{i=1}^{q} \operatorname{length}_A B/\mathfrak{n}_i \cdot \operatorname{length}_{B_{\mathfrak{n}_i}} M_{\mathfrak{n}_i} = \sum_{i=1}^{q} [\kappa(\mathfrak{n}_i) : \kappa(\mathfrak{m})] \operatorname{length}_{B_{\mathfrak{n}_i}} M_{\mathfrak{n}_i}$$

□

Corollary 1.35.1. Let $(A, \mathfrak{m})$ be a Noetherian local ring of dimension 1 and B a finite A-algebra. Suppose B is semilocal with maximal ideal $\mathfrak{n}_1, \ldots, \mathfrak{n}_q$, each of which lying over $\mathfrak{m}$. Then

(a) For $b \in B$ regular, we have

$$\operatorname{length}_A (B/bB) = \sum_{i=1}^{q} [\kappa(\mathfrak{n}_i) : \kappa(\mathfrak{m})] \operatorname{length}_{B_{\mathfrak{n}_i}} (B_{\mathfrak{n}_i}/bB_{\mathfrak{n}_i})$$

(b) If B is free of finite rank n over A, then

$$n = \sum_{i=1}^{q} [\kappa(\mathfrak{n}_i) : \kappa(\mathfrak{m})] \operatorname{length}_{B_{\mathfrak{n}_i}} (B_{\mathfrak{n}_i}/\mathfrak{m}B_{\mathfrak{n}_i})$$

Proof. Since B is finite over A, $\dim B \leqslant \dim A = 1$.

1. Since b is regular, $\dim B/bB = 0$, implying that $\operatorname{length}_B B/bB < \infty$. Apply Proposition with $M = B/bB$.

2. We have $B/\mathfrak{m}B = (A/\mathfrak{m})^n$, a product of field, and thus $B/\mathfrak{m}B$ has finite length over A, and a fortiori over B.

□

Chapter 2

Global Fields

2.1 Valuations

2.2 Types of Valuation

2.3 Examples of Valuations

2.4 Topology

2.5 Completeness

2.6 Independence

Lemma 2.1 (Weak approximation theorem)**.** Let $|\cdot|_n\,(1 \leqslant n \leqslant N)$ be inequivalent non-trivial valuations of a field k. For each n let k_n be the topological space k with topology induced by $|\cdot|_n$. Then the diagonal embedding $k \to \prod_{n=1}^{N} k_n$ has dense image.

Proof. Note that it suffices to find $\theta_n \in k$ such that $|\theta_n|_n > 1$ and $|\theta_m|_m < 1$ for $n \neq m$ for all $1 \leqslant n, m \leqslant N$. For then

$$\lim_{r\to\infty} \frac{\theta_n^r}{1+\theta_n^r} = \lim_{r\to\infty} \frac{1}{1+\theta_n^{-r}} = \begin{cases} 1 & \text{with respect to } |\cdot|_n \\ 0 & \text{with respect to } |\cdot|_m \text{ for } m \neq n \end{cases}$$

To approximate $(\alpha_1, \ldots, \alpha_N)$, it is then enough to take $\xi = \sum_{n=1}^{N} \frac{\theta_n^r}{1+\theta_n^r}\alpha_n$ with sufficiently large r.

It is enough to consider the case when $n = 1$. We do this by induction on N. When $N = 2$, since $|\cdot|_1$ and $|\cdot|_2$ are inequivalent, we can find $\alpha \in k$ such that $|\alpha|_1 < 1$ but $|\alpha|_2 \geqslant 1$, and similarly $\beta \in k$ such that $|\beta|_1 \geqslant 1$ but $|\beta|_2 < 1$. Then $\theta_1 = \beta\alpha^{-1}$ does the job.

For $N \geqslant 3$, by induction hypothesis we can find $\phi \in k$ such that $|\phi|_1 > 1$ but $|\phi|_n < 1$ for $2 \leqslant n \leqslant N-1$, and by the case $N = 2$ we can find $\psi \in k$ with $|\psi_1| > 1$ and $|\psi_N| < 1$. Now put

$$\theta = \begin{cases} \phi & \text{if } |\phi|_N < 1 \\ \phi^r \psi & \text{if } |\phi|_N = 1 \\ \dfrac{\phi^r}{1+\phi^r}\psi & \text{if } |\phi|_N > 1 \end{cases}$$

with $r \in \mathbb{Z}$ sufficiently large. □

Note that when $k = \mathbb{Q}$ and the $|\cdot|_n$ are non-archimedean, this lemma follows from Chinese Remainder theorem.

2.7 Finite Residue Field Case

Let k be a field with non-archimedean valuation $|\cdot|$. We set the following notation.

- $\mathfrak{o} := \{\alpha \in k \mid |\alpha| \leqslant 1\}$ is called the ring of integers for $|\cdot|$.
- $\mathfrak{o}^\times = \{\alpha \in k \mid |\alpha| = 1\}$ is called the group of units.
- $\mathfrak{p} := \{\alpha \in k \mid |\alpha| < 1\}$ is a maximal ideal of $\mathfrak{o}$.

We consider the case $\#\mathfrak{o}/\mathfrak{p} =: P < \infty$ is finite. Suppose further that $|\cdot|$ is discrete, i.e., $\mathfrak{p} = (\pi)$ is principal. Let $\overline{\mathfrak{o}}$, $\overline{\mathfrak{p}}$ be defined with respect to the completion $\overline{k}$ of k; then $\overline{\mathfrak{o}}/\overline{\mathfrak{p}} = \mathfrak{o}/\mathfrak{p}$ and $\overline{\mathfrak{p}} = \pi\overline{\mathfrak{o}}$.

Lemma 2.2. Suppose k is complete with respect to $|\cdot|$. Then $\mathfrak{o}$ is precisely the set of

$$\alpha = \sum_{j=0}^{\infty} a_j \pi^j \tag{♠}$$

where the a_j run independently through some set A of representatives in $\mathfrak{o}$ of $\mathfrak{o}/\mathfrak{p}$.

Proof. Series of the form (♠) clearly converge in $\mathfrak{o}$. Conversely, for $\alpha \in \mathfrak{o}$ let $a_0 \in A$ be the unique element such that $|\alpha - a_0| < 1$; then $\alpha_1 := \pi^{-1}(\alpha - a_0) \in \mathfrak{o}$. Take inductively that $a_n \in A$ such that $|\alpha_n - a_n| < 1$ and put $\alpha_{n+1} = \pi^{-1}(\alpha_n - a_n)$. Then $\alpha = \sum_{j=0}^{\infty} a_j \pi^j$. □

Theorem 2.3. Suppose k is complete with respect to $|\cdot|$. Then $\mathfrak{o}$ is complete. In particular, k is locally compact.

Proof. Let $\{U_i\}$ be an open cover of $\mathfrak{o}$. We must show that the U_i admits a finite subcover of $\mathfrak{o}$. Suppose otherwise.

Let A be a set of representative of $\mathfrak{o}/\mathfrak{p}$. Then

$$\mathfrak{o} = \bigsqcup_{a \in A} a + \pi\mathfrak{o}$$

Then there exists $a_0 \in A$ such that $a_0 + \pi\mathfrak{o}$ cannot be covered by finitely many of the U_i. Inductively find $a_n \in A$ such that $a_0 + a_1\pi + \cdots + a_n\pi^n + \pi^{n+1}\mathfrak{o}$ is not finitely covered by the U_i. Let $\alpha = \sum_{j=0}^{\infty} a_j\pi^j$; then $\alpha \in U_{i_0}$ for some i_0. Since U_{i_0} is open, $\alpha + \pi^m\mathfrak{o}$ for some $m \in \mathbb{N}$, a contradiction. □

Theorem 2.4. Let k be a locally compact field with a non-archimedean valuation $|\cdot|$. Then

(1) k is complete.

(2) The residue field is finite.

(3) The valuation is discrete.

Proof. Since k is locally compact, there exists a compact neighborhood K of 0; then $\pi^\nu\mathfrak{o} \subseteq K$ for $\nu \gg 0$. Hence $\mathfrak{o}$ is compact (for $\pi^\nu\mathfrak{o}$ is closed), and thus (1) holds. Let $(a_\alpha)_\alpha$ be a set of representative in $\mathfrak{o}$ of $\mathfrak{o}/\mathfrak{p}$. Then the open sets $\{x \in \mathfrak{o} \mid |x - a_\alpha| < 1\}$ cover $\mathfrak{o}$, so it admits a finite subcover and hence (2) holds. Finally, since $\mathfrak{p} = \pi\mathfrak{o}$ is compact, the cover $S_n = \{\alpha \in k \mid |\alpha| < 1 - \frac{1}{n}\}$ of $\mathfrak{p}$ has a finite subcover, and thus $\mathfrak{p} = S_N$ for some N, i.e. (3) holds. □

Since k is locally compact Hausdorff, there exists a Haar measure μ on k, invariant under translation, and it is unique up to a positive scalar. Let us normalize μ in the way that $\mu(\mathfrak{o}) = 1$. That μ is invariant together with the disjoint union decomposition

$$\mathfrak{o} = \bigsqcup a + \pi\mathfrak{o}$$

gives $1 = P\mu(\pi\mathfrak{o})$. Inductively we have $\mu(\pi^\nu\mathfrak{o}) = P^{-\nu}$ for $\nu \in \mathbb{Z}$.

Definition. Let k be a field with discrete valuation $|\cdot|$ and residue class field with $P < \infty$ elements. We say that $|\cdot|$ is **normalized** if $|\pi| = P^{-1}$, where $\mathfrak{p} = \pi\mathfrak{o}$.

Theorem 2.5. Let k be as in Theorem 2.3 and suppose $|\cdot|$ is normalized. Then $\mu(\alpha + \beta\mathfrak{o}) = |\beta|$, where μ is the normalized Haar measure on k such that $\mu(\mathfrak{o}) = 1$.

Proof. Write $\beta = \pi^\nu u$ with $\nu \in \mathbb{Z}$ and $u \in \mathfrak{o}^\times$. Then $|\beta| = P^{-\nu}$ and $\mu(\alpha + \beta\mathfrak{o}) = \mu(\pi^\nu\mathfrak{o}) = P^{-\nu}$, as shown above. □

Consider the multiplicative group $k^\times$ which is open in k. The group of unit $\mathfrak{o}^\times$ is compact, by virtue of the isomorphism $\mathfrak{o}^\times/(1+\mathfrak{p}) \cong (\mathfrak{o}/\mathfrak{p})^\times$, and thus $k^\times$ is locally compact.

Let k and μ be as above. The additive measure μ on $1 + \mathfrak{p}$ is also invariant under multiplication in $\mathfrak{o}^\times$; indeed, for $u \in \mathfrak{o}$,

$$\mu(u(\alpha + \mathfrak{p}^n)) = \mu(u\alpha + \mathfrak{p}^n) = \mu(\mathfrak{p}^n)$$

This defines a Haar measure ν on $k^\times$, namely, $\mu(x) := \dfrac{d\mu(x)}{|x|}$. From the isomorphism $\mathfrak{o}^\times/(1+\mathfrak{p}) \cong (\mathfrak{o}/\mathfrak{p})^\times$, we have

$$\mathfrak{o}^\times = \bigsqcup_{\alpha \in (\mathfrak{o}/\mathfrak{p})^\times} f(\alpha) + \mathfrak{p}$$

where $f : (\mathfrak{o}/\mathfrak{p})^\times \to \mathfrak{o}^\times$ is a section of $\mathfrak{o}^\times \to (\mathfrak{o}/\mathfrak{p})^\times$. Then

$$\nu(\mathfrak{o}^\times) = \int_{\mathfrak{o}^\times} d\nu(x) = \mu(\mathfrak{o}^\times) = \sum_{\alpha \in (\mathfrak{o}/\mathfrak{p})^\times} \mu(f(\alpha) + \mathfrak{p}) = (P-1)P^{-1} = 1 - P^{-1}$$

Lemma 2.6. k and $k^\times$ are totally disconnected.

Proof. They admit a base consisting of compact open sets. □

If $\operatorname{Char} k = 0$, then k and $k^\times$ are locally isomorphic, for we have the exponential map

$$\alpha \mapsto \exp \alpha = \sum_{n=0}^{\infty} \frac{\alpha^n}{n!}$$

valid for all sufficiently small α with its inverse

$$\log \alpha = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(\alpha - 1)^n}{n}$$

valid for all α sufficiently near to 1.

2.8 Normed Spaces

2.9 Tensor Product

Let A, B be commutative rings containing a field k and suppose $N := \dim_k B < \infty$, say with the basis $\omega = 1, \omega_2, \ldots, \omega_N$. Then B is determined up to isomorphism by the multiplication table

$$\omega_\ell \omega_m = \sum_{n=1}^{N} c_{\ell m n} \omega_n \qquad c_{\ell m n} \in k$$

We can define a new ring C containing k whose elements are expressions of the type

$$\sum_{m=1}^{N} a_m \overline{\omega}_m \qquad a_m \in A$$

where the $\overline{\omega}_m$ have the same multiplication rule

$$\overline{\omega}_\ell \overline{\omega}_m = \sum_{n=1}^{N} c_{\ell m n} \overline{\omega}_n$$

as the ω_m. There are injective ring homomorphisms

$$\begin{array}{rcl} i : A & \longrightarrow & C \\ a & \longmapsto & a\overline{\omega}_1 \end{array} \quad \text{and} \quad \begin{array}{rcl} j : B & \longrightarrow & C \\ \sum \lambda_m \omega_m & \longmapsto & \sum \lambda_m \overline{\omega}_m \end{array}$$

of A and B into C.

Lemma 2.7.

1. C is independent of the choice of the basis ω_m of B.

2. (C, i, j) is a tensor product of the rings A and B over k.

We will write $C = A \otimes_k B$.

Proof. Let D be a commutative ring containing a field k and $f : A \to N$, $g : B \to N$ such that the diagram

$$\begin{tikzcd}
A \arrow[r, "f"] & N \\
k \arrow[u] \arrow[r] & B \arrow[u, "g"']
\end{tikzcd}$$

commutes. Define $\varphi : C \to N$ by $\varphi(a) = f(a)$ and $\varphi(\overline{\omega}) = g(\omega_i)$. It is clearly well-defined, and it is the unique map making the diagram

$$\begin{tikzcd}
 & & N \\
A \arrow[r, "i"] \arrow[urr, bend left, "f"] & C \arrow[ur, "\varphi"] & \\
k \arrow[u] \arrow[r] & B \arrow[u, "j"'] \arrow[uur, bend right, "g"'] &
\end{tikzcd}$$

commutes. □

Suppose further that A is a topological ring. There is an abelian group isomorphism

$$\begin{tikzcd}
C \arrow[r] & A^N \\
\sum a_m \overline{\omega}_m \arrow[r, mapsto] & (a_1, \dots, a_N)
\end{tikzcd}$$

We use this map to give C the product topology. In fact, this topology is the same as the initial topology induced by the maps $\mathrm{id}_A \otimes f : C \to A$, where $f \in \mathrm{Hom}_k(B, k)$. To see this, note that $\mathrm{Hom}_k(B, k)$ has a basis f_i, $1 \leqslant i \leqslant N$, where $f_i : B \to k$ is given by $f_i(\omega_j) = \delta_{ij}$, so by linearity the initial topology described above the same as that induced by the f_i. From the above isomorphism each f_i corresponds to the i-th projection of A^N to A, whence the the initial topology is the same as the product topology on A^N.

Lemma 2.8.

1. The topology on C is independent of the choice of the basis ω_i.

2. C is a topological ring.

We speak of this topology on C the **tensor product topology**.

Proof.

1. This is clear from the discussion right above.

2. The addition is clearly continuous. The multiplication is given by the map

$$\begin{tikzcd} A^N \times A^N \arrow[r] & A^N \\ (a_1,\dots,a_N,b_1,\dots,b_N) \arrow[r, mapsto] & \left(\sum\limits_{i,j=1}^{N} a_ib_jc_{ij1},\dots,\sum\limits_{i,j=1}^{N} a_ib_jc_{ijN}\right) \end{tikzcd}$$

The map continuous if and only if each component $\sum\limits_{i,j=1}^{N} a_ib_jc_{ijk}$ $(k=1,\dots,N)$ is continuous; but it is the composition of the continuous maps

$$\begin{tikzcd} A^N \times A^N \arrow[r] & A^{2N} \arrow[r] & A \\ (a_1,\dots,a_N,b_1,\dots,b_N) \arrow[r, mapsto] & (a_ib_jc_{ijk})_{1\leqslant i,j\leqslant N} & \\ & (x_{ij})_{1\leqslant i,j\leqslant N} \arrow[r, mapsto] & \sum\limits_{i,j=1}^{N} x_{ij} \end{tikzcd}$$

hence the multiplication is continuous.

□

Let us drop our condition that A has a topology, but suppose that A, B are not merely rings but fields.

Lemma 2.9. Let A, B be field extensions of k, and suppose B/k is finite separable of degree N. Then $C = A \otimes_k B$ is the direct sum of a finite number of fields K_j, each containing an isomorphic image of A and an isomorphic image of B.

Proof. Say $B = k(\beta)$, where the minimal polynomial f over k of β is separable of degree N. Then $1, \beta, \dots, \beta^{N-1}$ is a basis for B/k, so $A \otimes_k B = A[\overline{\beta}]$, where $1, \overline{\beta}, \dots, \overline{\beta}^{N-1}$ are A-linear independent and $f(\overline{\beta}) = 0$.

Write $f(X) = \prod\limits_{j=1}^{J} g_j(X)$, where $g_j(X) \in A[X]$ is irreducible. The g_j are distinct, for f is separable. By Chinese Remainder Theorem

$$(p_1,\dots,p_J) : A \otimes_k B \xrightarrow{\sim} \bigoplus_{i=1}^{J} A[X]/(g_j(X))$$

Each $K_j := A[X]/(g_j(X))$ is a field. It remains to show

$$\lambda_j : B \longrightarrow A \otimes_k B \xrightarrow{p_j} K_j$$

is injective, and it only needs to show λ_j is nontrivial, which is clear. □

Corollary 2.9.1. Let $\alpha \in B$ and let $F(X) \in k[X]$, $G_j(X) \in A[X]\,(1 \leqslant j \leqslant J)$ be the characteristic polynomial of α over k and of the image of α under

$$B \longrightarrow A \otimes_k B \xrightarrow{p_j} K_j$$

over A respectively. Then

$$F(X) = \prod_{1 \leqslant j \leqslant J} G_j(X) \tag{♠}$$

Proof. Let T be the characteristic polynomial of the image of α in $A \otimes_k B$ over A. We claim both sides of (♠) equal T.

- Computing in terms of the basis $\overline{\omega_1}, \dots, \overline{\omega_N}$, where $\omega_1, \dots, \omega_N$ is a basis for B/k, we obtain $T(X) = F(X)$.
- Using a basis of $A \otimes_k B = \bigoplus_{1 \leqslant j \leqslant J} K_j$ composed of bases of the individual K_j/A, we obtain $T(X) = \prod_{1 \leqslant j \leqslant J} G_j(X)$.

□

Corollary 2.9.2. For $\alpha \in B$, we have

$$\mathrm{Norm}_{B/k}\alpha = \prod_{1 \leqslant j \leqslant J} \mathrm{Norm}_{K_j/A}\alpha$$

$$\mathrm{Trace}_{B/k}\alpha = \sum_{1 \leqslant j \leqslant J} \mathrm{Trace}_{K_j/A}\alpha$$

2.10 Extension of Valuations

Let $k \subseteq K$ be fields and $|\cdot|$, $\|\cdot\|$ be valuations on k and K respectively. We say $\|\cdot\|$ **extends** $|\cdot|$ if $\|\cdot\|\,|_k = |\cdot|$.

Theorem 2.10. Let k be complete with respect to the valuation k and let K be an extension of k with $[K : k] = N < \infty$. Then there is precisely one extension of $|\cdot|$ to K namely

$$\|\alpha\| = |\mathrm{Norm}_{K/k}\alpha|^{\frac{1}{N}}$$

Theorem 2.11. Let K/k be a separable extension of degree $N < \infty$. Then there are at most N extensions of a valuation $|\cdot|$ of k to K, say $\|\cdot\|_j$ $(1 \leqslant j \leqslant J)$. Let $\overline{k}$, K_j are the completions of k and K with respect to $|\cdot|$ and $\|\cdot\|_j$, respectively. Then

$$\overline{k} \otimes_k K = \bigoplus_{1 \leqslant j \leqslant J} K_j \tag{♡}$$

algebraically and topologically, where the RHS is given the product topology.

Proof. We already know that $\overline{k}\otimes_k K$ is of the shape (♡), where the K_j/k are finite extensions of $\overline{k}$ (Lemma 2.9). Hence there is a unique extension $|\cdot|_j^*$ of $|\cdot|$ to the K_j, and each K_j is complete with respect to the extended valuation. In the proof of Lemma 2.9, we have the injective homomorphisms λ_j, so we get the extensions $\|\cdot\|_j$ of $|\cdot|$ to K by putting

$$\|\beta\|_j = |\lambda_j(\beta)|_j^*$$

Further, $K \cong \lambda_j(K)$ is dense in K_j with respect to $\|\cdot\|_j$ for $K = k \otimes_k K$ is dense in $\overline{k} \otimes_k K$. Hence K_j is exactly the completion of K.

We show that $\|\cdot\|_j$ are distinct and that they are the only extensions of $|\cdot|$ to K. Let $\|\cdot\|$ be any extension to K of $|\cdot|$. Then it extends by continuity to a real-valued function on $\overline{k}\otimes_k K$, still denoted by $\|\cdot\|$. By continuity we have

$$\begin{aligned} \|\alpha+\beta\| &\leqslant \max\{\|a\|, \|b\|\} \\ \|\alpha\beta\| &= \|a\|\,\|\beta\| \end{aligned}$$

for all $\alpha, \beta \in \overline{k}\otimes_k K$. We consider its restriction to the K_j; they are either identically 0 on K_j or valuations on K_j. Further, $\|\cdot\|$ cannot restrict to two nonzero valuations on the K_j, for the sake of $\|\alpha\beta\| = \|a\|\,\|\beta\|$. Hence $\|\cdot\|$ induces a valuation in precisely one of the K_j, and it clearly extends the given valuation $|\cdot|$ of $\overline{k}$. Hence $\|\cdot\| = \|\cdot\|_j$ for precisely one j by Theorem 2.10.

It remains to show that (♡) is a homeomorphism. For $(\beta_1, \ldots, \beta_J) \in K_1 \oplus \cdots \oplus K_J$, put

$$\|(\beta_1, \ldots, \beta_J)\|_0 := \max_{1\leqslant j\leqslant J} \|\beta_j\|_j$$

Clearly, $\|\cdot\|_0$ is a norm on RHS of (♡), considered as a $\overline{k}$-vector space, and it induces the product topology. On the other hand, any two norms are equivalent by virtue of the completeness of $\overline{k}$, and so $\|\cdot\|_0$ induces the tensor product topology on the LHS of (♡). □

Corollary 2.11.1. Let $K = k(\beta)$ and let $f \in K[X]$ be the irreducible polynomial of β over k. Suppose that

$$f(X) = \prod_{1\leqslant j\leqslant J} g_j(X)$$

in $\overline{k}[X]$, where the g_j are irreducible. Then $K_j = \overline{k}(\beta_j)$ where $g_j(\beta_j) = 0$.

2.11 Extension of Normalized Valuations

2.12 Global Fields

Definition. A **global field** k is either a finite extension of $\mathbb{Q}$ or a finite separable extension of $\mathbb{F}_q(t)$, where q is a rational prime power and t is transcendental over $\mathbb{F}_q$.

Lemma 2.12. Let $\alpha \neq 0$ be in the global field k. Then there are only finitely many unequivalent valuations $|\cdot|$ of k for which $|\alpha| > 1$.

Proof. It is clear for $\mathbb{Q}$ and $\mathbb{F}_q(t)$. Since there are only finitely many archimedean valuations on k, it suffices to consider the non-archimedean ones. Write

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

for some n and $a_1, \ldots, a_n$ in either $\mathbb{Q}$ or $\mathbb{F}_q(t)$. Then

$$|\alpha|^n = |-a_1\alpha^{n-1} - \cdots - a_n| \leqslant \max\{1, |\alpha|^{n-1}\} \max_{1 \leqslant i \leqslant n} |a_i|$$

and so

$$|\alpha| \leqslant \max\{1, |a_1|, \ldots, |a_n|\}$$

The result then follows from the case for $\mathbb{Q}$ and $\mathbb{F}_q(t)$. □

Let K be a finite separable extension of the global field k. Then for every valuation ν of k we have an isomorphism (Theorem 2.11)

$$k_\nu \otimes_k K = K_1 \oplus \cdots \oplus K_J$$

where k_ν is the completion of k with respect to ν and $K_1, \ldots, K_J$ are the completions of K with respect to the extensions $w_1, \ldots, w_J$ of ν to K; the number $J := J(\nu)$ depends on ν.

Lemma 2.13. Let $\omega_1, \ldots, \omega_N$ be a basis for K/k. Then for almost all normalized ν we have

$$\omega_1\mathfrak{o} \oplus \cdots \oplus \omega_N\mathfrak{o} = \mathfrak{O}_1 \oplus \cdots \oplus \mathfrak{O}_J \tag{$\clubsuit$}$$

where $N = [K : k]$, $\mathfrak{o} = \mathfrak{o}_\nu$ is the ring of integers of k for $|\cdot|_\nu$ and $\mathfrak{O}_j \subseteq K_j$ is the ring of integers for $|\cdot|_{w_j}$ $(1 \leqslant j \leqslant J)$. Here we have identified $\alpha \in K$ with its canonical image in $k_\nu \otimes K$.

Proof. The LHS of ($\clubsuit$) is contained in the RHS provided that $|\omega_n|_{w_j} \leqslant 1$ for $1 \leqslant n \leqslant N$ and $1 \leqslant j \leqslant J$. Since $|\alpha|_w \leqslant 1$ for almost all w, it follows that LHS $\subseteq$ RHS for almost all ν.

To get an inclusion the other way we use the discriminant

$$D(\gamma_1, \ldots, \gamma_N) := \det(\mathrm{Tr}_{K/k}(\gamma_m\gamma_n))_{m,n}$$

where $\gamma_1, \ldots, \gamma_N \in k_\nu \otimes_k K$. If $\gamma_n \in$ RHS $(1 \leqslant n \leqslant N)$, we have (Lemma 2.9.2)

$$\mathrm{Tr}_{K/k}(\gamma_m\gamma_n) = \sum_{1 \leqslant j \leqslant J} \mathrm{Tr}_{K_j/k_\nu}(\gamma_m\gamma_n) \in \mathfrak{o}$$

and so $D(\gamma_1, \ldots, \gamma_N) \in \mathfrak{o}$.

Now suppose that

$$\beta = \sum_{n=1}^{N} b_n\omega_n \in \text{RHS} \qquad (b_n \in k_\nu)$$

Then for any $1 \leqslant m \leqslant N$ we have

$$D(\omega_1, \ldots, \omega_{m-1}, \beta, \omega_{m+1}, \ldots, \omega_N) = b_m^2 D(\omega_1, \ldots, \omega_N)$$

and so $b_m^2 D(\omega_1, \ldots, \omega_N) \in \mathfrak{o}$ by the discussion in the second paragraph. But since K/k is separable, $D(\omega_1, \ldots, \omega_N) \neq 0$, and so $|D(\omega_1, \ldots, \omega_N)|_\nu = 1$ for almost all ν. Thus for almost all ν we have $b_m \in \mathfrak{o}_\nu$, and hence RHS $\subseteq$ LHS. □

2.13 Restricted Topological Product

Definition. Let $\Omega_\lambda\,(\lambda \in \Lambda)$ be a family of topological spaces together with $\Theta_\lambda \underset{\text{open}}{\subseteq} \Omega_\lambda$ for all but finitely many $\lambda \in \Lambda$. The **restricted product of the Ω_λ with respect to the Θ_λ** is the set

$$\prod_{\lambda\in\Lambda}{}' \Omega_\lambda := \left\{ (x_\lambda) \in \prod_{\lambda\in\Lambda} \Omega_\lambda \mid x_\lambda \in \Theta_\lambda \text{ for all finitely many } \lambda \in \Lambda \right\}$$

with topology whose basis consists of sets of the form $\prod\limits_{\lambda\in\Lambda} \Gamma_\lambda$, where $\Gamma_\lambda \underset{\text{open}}{\subseteq} \Omega_\lambda$ for all λ and $\Gamma_\lambda = \Theta_\lambda$ for all but finitely many $\lambda \in \Lambda$.

- Let $S \subseteq \Lambda$ be a finite subset and put

  $$\Omega_S := \prod_{\lambda\in S} \Omega_\lambda \times \prod_{\lambda\notin S} \Theta_\lambda$$

  Then Ω_S is open in $\prod'_{\lambda\in\Lambda} \Omega_\lambda$, and the open cover Ω_S induces the same topology on $\prod'_{\lambda\in\Lambda} \Omega_\lambda$ as defined above.

- If $\Theta'_\lambda \underset{\text{open}}{\subseteq} \Omega_\lambda$ is defined for all but finitely many λ, and $\Theta_\lambda = \Theta'_\lambda$ for all but finitely many λ. Then they define the same (canonically isomorphic) restricted product.

Lemma 2.14. Let the notation be as above. Suppose the Ω_λ are locally compact and the Θ_λ are compact. Then the restricted product is locally compact.

Proof. Let $S \subseteq \Lambda$ be finite. Then Ω_S is locally compact because a finite product of locally compact spaces is locally compact. Since the Ω_S form the basis for the restricted product, the local compactness follows. □

Definition. Let the notation be as above. Suppose that measures μ_λ are defined on the Ω_λ with $\mu_\lambda(\Theta_\lambda) = 1$ when Θ_λ is defined. Define the **product measure** μ on $\prod\limits_{\lambda\in\Lambda}{}' \Omega_\lambda$ to be that for which a basis of measurable sets in the

$$\prod_\lambda M_\lambda$$

where $M_\lambda \subseteq \Omega_\lambda$ has finite μ_λ-measure and $M_\lambda = \Theta_\lambda$ for almost all λ, and where

$$\mu\left(\prod_\lambda M_\mu\right) = \prod_\lambda \mu_\lambda(M_\lambda)$$

2.14 Adele Ring

Lemma 2.15. Let K/k be a finite separable extension of the global field k. Then

$$\mathbb{A}_k \otimes_k K = \mathbb{A}_K \tag{♠}$$

algebraically and topologically. In this correspondence $k \otimes_k K = K \subseteq \mathbb{A}_k \otimes_k K$, where $k \subseteq \mathbb{A}_k$, is mapped identically onto $K \subseteq \mathbb{A}_K$

Proof. Let $\omega_1, \dots, \omega_N$ be a basis for K/k and let ν run through the normalized valuations of k. Then $\mathbb{A}_k \otimes_k K$, with the tensor product topology, is just the restricted product of the

$$k_\nu \otimes_k K = k_\nu \omega_1 \oplus \cdots \oplus k_\nu \omega_N$$

with respect to the $\mathfrak{o}_\nu \omega_1 \oplus \cdots \oplus \mathfrak{o}_\nu \omega_N$. Indeed, the topology on $\mathbb{A}_k \otimes_k K$ is the initial topology with respect to the map

$$\begin{aligned} \mathbb{A}_k \otimes_k K &\longrightarrow \mathbb{A}_k^N \\ \sum_{i=1}^{N} a_i \omega_i &\longmapsto (a_1, \dots, a_N) \end{aligned}$$

It is easy to see $\mathbb{A}_k^N$ is isomorphic to the mentioned restricted product as topological rings (the multiplication on $\mathbb{A}_k^N$ is given by that on $\mathbb{A}_k \otimes_k K$). By Theorem 2.11,

$$k_\nu \otimes_k K = k_\nu \omega_1 \oplus \cdots \oplus k_\nu \omega_N = \bigoplus_{1 \leqslant j \leqslant J} K_{w_j}$$

where $w_1, \dots, w_J \mid \nu$ are normalized extensions of ν to K. Further, this identification also identifies (Lemma 2.13)

$$\mathfrak{o}_\nu \omega_1 \oplus \cdots \oplus \mathfrak{o}_\nu \omega_N = \mathfrak{O}_{w_1} \oplus \cdots \oplus \mathfrak{O}_{w_J}$$

for almost all ν. Hence the LHS of (♠) is the restricted product of the K_w with respect to the $\mathfrak{O}_w$, where w runs over all the normalized valuations of K, and this is just the RHS of (♠). □

Corollary 2.15.1. $\mathbb{A}_K = \underbrace{\mathbb{A}_k \oplus \cdots \oplus \mathbb{A}_k}_{N\text{-copies}}$ as additive topological groups, where $N = [K : k]$. In this isomorphism, the principal adele $K \subseteq \mathbb{A}_K$ is mapped into $k \oplus \cdots \oplus k$.

Proof.

$$\mathbb{A}_K = \mathbb{A}_k \otimes_k K = \mathbb{A}_k \omega_1 \oplus \cdots \oplus \mathbb{A}_k \omega_N = \mathbb{A}_k \oplus \cdots \oplus \mathbb{A}_k$$

□

Theorem 2.16. k is discrete in $\mathbb{A}_k$, and $\mathbb{A}_k/k$ is compact in the quotient topology.

Proof. The previous topology shows that it suffices to consider the case for $\mathbb{Q}$ and $\mathbb{F}_q(t)$. For the first assertion, since $\mathbb{A}_k$ is a topological group, it suffices to show $0 \in k$ is isolated, and we shall do this by constructing a neighborhood U of 0 that contains no other elements of k.

- $k = \mathbb{Q}$. Take

  $$U = \{(\alpha_\nu)_\nu \in \mathbb{A}_\mathbb{Q} \mid |\alpha_\infty|_\infty < 1, \ |\alpha_p|_p \leqslant 1 \text{ for all } p < \infty\}$$

  where $|\cdot|_\infty$ and $|\cdot|_p$ are respectively the usual and p-adic absolute values on $\mathbb{Q}$. If $b \in \mathbb{Q} \cap U$, then $b \in \mathbb{Z}$ for $|b|_p \leqslant 1$ for all p. Since $|b|_\infty < 1$, $b = 0$.

- $k = \mathbb{F}_q(t)$. Take
$$U = \{(\alpha_\nu)_\nu \in \mathbb{A}_k \mid |\alpha_\infty|_\infty > 1,\ |\alpha_p|_p \leqslant 1 \text{ for all } p\}$$
where p runs over all irreducible polynomials in $\mathbb{F}_q(t)$, $|\cdot|_p$ and $|\cdot|_\infty$ are the normalized absolute values corresponding to $p(t)$ and t^{-1}. If $f \in \mathbb{F}_q(t) \cap U$, then $f \in \mathbb{F}_q[t]$ for $|f|_p \leqslant 1$ for all p, and this also implies $|f|_\infty = c^{-\deg f}$ for some chosen $0 < c < 1$; $c^{-\deg f} > 1$ implies $\deg f < 0$, i.e. $f = 0$.

We proceed to prove the second assertion separately.

- $k = \mathbb{Q}$. Let $\beta = (\beta_\nu)_\nu \in \mathbb{A}_\mathbb{Q}$. For each finite p, choose $r_p = z_p p^{-x_p}$ with $z_p \in \mathbb{Z}$ and $x_p \geqslant 0$ such that $|\beta_p - r_p|_p \leqslant 1$; since x is an adele, we can take $r_p = 0$ for almost all p, and thus $r := \sum\limits_{p<\infty} r_p \in \mathbb{Q}$ is well-defined. Thus $|\beta_p - r| \leqslant 1$ for all $p < \infty$. Now choose $s \in \mathbb{Z}$ such that $|\beta_\infty - r - s| \leqslant \dfrac{1}{2}$, and put $b = r + s$. Then $\beta - b \in W$, where
$$W := \left\{(\alpha_\nu)_\nu \in \mathbb{A}_\mathbb{Q} \mid |\alpha_\infty|_\infty \leqslant \frac{1}{2},\ |\alpha_p|_p \leqslant 1 \text{ for all } p < \infty\right\}$$
In sum, we have proved $\mathbb{A}_\mathbb{Q} = \mathbb{Q} + W$.

- $k = \mathbb{F}_q(t)$. Let $\beta = (\beta_\nu)_\nu \in \mathbb{A}_k$. Similar to the case $\mathbb{Q}$, we can find $r \in \mathbb{F}_q(t)$ such that $|\beta_p - r|_p \leqslant 1$ for all irreducible $p(t)$. Note that $(\mathbb{F}_q(t))_\infty = \mathbb{F}_q(\!(1/t)\!)$. Write $\beta_\infty - r = \sum\limits_{n \gg -\infty} c_n t^{-n} = \sum\limits_{n \ll \infty} c_{-n} t^n$, and let $s(t) = \sum\limits_{n \geqslant 0} c_{-n} t^n$. Then
$$|\beta_\infty - r - s|_\infty = \left|\sum_{n>0} c_n t^{-n}\right| = c^{\min_{c_n \neq 0,\, n \geqslant 1} n} \leqslant c < 1$$
where $0 < c < 1$ is a chosen constant. Since $s \in \mathbb{F}_q[t]$, $|s|_p \leqslant 1$ for all p. Hence $\beta - r - s \in W$, where
$$W := \{(\alpha_\nu)_\nu \in \mathbb{A}_k \mid |\alpha_\infty|_\infty \leqslant c,\ |\alpha_p|_p \leqslant 1 \text{ for all } p\}$$
In sum, we obtain a similar result $\mathbb{A}_{\mathbb{F}_q(t)} = \mathbb{F}_q(t) + W$.

In either case, we have $\mathbb{A}_k = k + W$, and hence a surjective continuous map $W \to \mathbb{A}_k/k$ induced by the quotient map $\mathbb{A}_k \to \mathbb{A}_k/k$. By Tychonov's theorem, W is compact, and being a continuous image of W, $\mathbb{A}_k/k$ is also compact. □

Corollary 2.16.1. There is a subset U of $\mathbb{A}_k$ defined by the inequalities of the type $|\xi_\nu|_\nu \leqslant \delta_\nu$ where $\delta_\nu = 1$ for almost all ν, such that
$$\mathbb{A}_k = k + U$$

Proof. Let $\omega_1, \ldots, \omega_N$ be a basis for k/k'. Then
$$\mathbb{A}_k = \mathbb{A}_{k'} \otimes_{k'} k = \mathbb{A}_{k'}\omega_1 \oplus \cdots \oplus \mathbb{A}_{k'}\omega_N$$
where $k' = \mathbb{Q}$ or $\mathbb{F}_q(t)$, and k is mapped into $k'\omega_1 \oplus \cdots \oplus k'\omega_N$. Take $U' = W\omega_1 \oplus \cdots \oplus W\omega_N$, where W is the subset constructed in the proof of the Theorem. Note that for almost all ν on k, $|\omega_i|_\nu \leqslant 1$. Then it is clear from the definition of W that U' is contained in some U of the type described above. □

We give $\mathbb{A}_k$ a measure by the way described in the previous section; it is a Haar measure on $\mathbb{A}_k$ (invariant under translation). Since k is discrete, the Haar measure on k can be chosen to be the counting measure, and we always make this choice.

Corollary 2.16.2. $\mathbb{A}_k/k$ has finite measure in the quotient measure induced by the Haar measure on $\mathbb{A}_k$ and the counting measure on k.

Proof. For $\mathbb{A}_k/k$ is compact. □

Corollary 2.16.3 (Product Formula)**.** $\prod\limits_{\nu} |\xi|_\nu = 1$ for all $\xi \in k^\times$.

Proof. We use the surjectivity of the map

$$\begin{tikzcd}
C_c(G) \arrow[r] & C_c(G/H) \\
f \arrow[r, mapsto] & \left[f^H : xH \mapsto \displaystyle\int_H f(xh)dh\right]
\end{tikzcd}$$

where G is an LCH group and $H \leqslant G$ is a closed subgroup, and the quotient integral formula

$$\int_G f(x)dx = \int_{G/H}\int_H f(xh)dhdx$$

Put $K = \mathbb{A}_k/k$. Since $\xi k \subseteq k$, we have $\xi K = K$. Let $f \in C_c(\mathbb{A}_k)$ such that $f^k = \mathbf{1}_K$, the characteristic function of K. Then

$$\int_K \mathbf{1}_{\xi K}(\beta)d\beta = \int_K \mathbf{1}_K(\xi^{-1}\beta)d\beta = \int_K\int_k f(\xi^{-1}(\beta + r))drd\beta = \int_{\mathbb{A}_k} f(\xi^{-1}x)dx$$

By Theorem 2.5, for a measurable set M in $\mathbb{A}_k$ and $\beta \in \mathbb{A}_k$, we have $\mathrm{vol}(\beta M) = \mathrm{vol}(M)\prod\limits_{\nu}|\beta_\nu|$. Hence

$$\int_K \mathbf{1}_{\xi K}(\beta)d\beta = \int_{\mathbb{A}_k} f(\xi^{-1}x)dx = \prod_{\nu}|\xi|_\nu \int_{\mathbb{A}_k} f(x)dx = \prod_{\nu}|\xi|_\nu \int_K \mathbf{1}_K(\beta)d\beta$$

Since $\xi K = K$ and K is compact (so the integral is finite), it follows that $\prod\limits_{\nu}|\xi|_\nu = 1$. □

Lemma 2.17. There is a constant $C > 0$ depending only on the global field k with the following property: let $\alpha \in \mathbb{A}_k$ be such that $\prod\limits_{\nu}|\alpha_\nu|_\nu > C$. Then there exists a principal adele $\beta \in k \subseteq \mathbb{A}_k$, $\beta \neq 0$ such that $|\beta|_\nu \leqslant |\alpha_\nu|_\nu$ for all ν.

Proof. Let c_0 be the total volume of $\mathbb{A}_k/k$, and let c_1 be that of the set

$$\left\{\gamma \in \mathbb{A}_k \mid |\gamma_\nu|_\nu \leqslant \frac{1}{10} \text{ for archimedean } \nu,\ |\gamma_\nu|_\nu \leqslant 1 \text{ for non-archimedean } \nu\right\}$$

Then $0 < c_0 < \infty$ and $0 < c_1 < \infty$ for the number of archimedean places is finite. We show that $C = \dfrac{c_0}{c_1}$ will do.

The set

$$T = \left\{ \tau \in \mathbb{A}_k \mid |\tau_\nu|_\nu \leqslant \frac{1}{10} |\gamma_\nu|_\nu \text{ for archimedean } \nu,\ |\tau_\nu|_\nu \leqslant |\gamma_\nu|_\nu \text{ for non-archimedean } \nu \right\}$$

has measure $c_1 \prod_\nu |\alpha_\nu|_\nu > c_1 C = c_0$ by Theorem 2.5. Hence in the quotient $\mathbb{A}_k/k$, there must be a pair of distinct points of T which have the same image in $\mathbb{A}_k/k$, say $\tau', \tau'' \in T$ and $\tau' - \tau'' =: \beta \in k$. Then

$$|\beta|_\nu = |\tau'_\nu - \tau''_n u| \leqslant |\alpha_\nu|_\nu$$

for all ν, as required. □

Remark 2.18. Let $M \subseteq \mathbb{A}_k$ be measurable such that the restriction to M of the quotient map $\pi : \mathbb{A}_k \to \mathbb{A}_k/k$ is injective. We claim

$$\int_{\mathbb{A}_k} \mathbf{1}_M(x) dx = \int_{\mathbb{A}_k/k} \mathbf{1}_{\pi(K)}(x) dx$$

By the quotient integral formula, one has

$$\int_{\mathbb{A}_k} \mathbf{1}_M(x) dx = \int_{\mathbb{A}_k/k} \int_k \mathbf{1}_M(x+h) dh dx$$

We have a bijection

$$\{h \in k \mid x + h \in M\} \longleftrightarrow \{\alpha \in M \mid \alpha - x \in k\}$$

Since the measure on k is the counting measure, we have

$$\int_k \mathbf{1}_M(x+h) dh = \#\{h \in k \mid x + h \in M\} = \#\{\alpha \in M \mid \alpha - x \in k\}$$

Now consider $\pi(M)$. We have $x + k \in \pi(M) \Leftrightarrow \#\{g \in M \mid g - x \in k\} \geqslant 1$, which implies the inequality

$$\int_{\mathbb{A}_k/k} \mathbf{1}_{\pi(M)}(x) dx \leqslant \int_{\mathbb{A}_k/k} \#\{g \in M \mid g - x \in H\} dx$$

with inequality $\#\{g \in M \mid g - x \in k\} = 1$ for almost every x such that $x + k \in \pi(M)$. In particular, since $\pi|_M$ is injective, $\#\{g \in M \mid g - x \in k\} = 1$ for every x (if $g_1, g_2 \in k$ lie in that set, then $g_1 + k = x + k = g_2 + k$, so $g_1 = g_2$ by injectivity). Hence in our case, we have

$$\int_{\mathbb{A}_k} \mathbf{1}_M(x) dx = \int_{\mathbb{A}_k/k} \#\{g \in M \mid g - x \in H\} dx = \int_{\mathbb{A}_k/k} \mathbf{1}_{\pi(M)}(x) dx$$

From the above discussion we also see that in general there is an inequality

$$\int_{\mathbb{A}_k} \mathbf{1}_M(x) dx \geqslant \int_{\mathbb{A}_k/k} \mathbf{1}_{\pi(M)}(x) dx$$

That is, π is measure-decreasing.

Corollary 2.17.1. Let ν_0 be a normalized valuation and let $\delta_\nu > 0$ be given for all $\nu \neq \nu_0$ with $\delta_\nu = 1$ for almost all ν. Then there exists a $\beta \neq 0 \in k$ with $|\beta|_\nu \leqslant \delta_\nu$ for all $\nu \neq \nu_0$

Proof. Choose $\alpha_\nu \in k_\nu$ with $0 < |\alpha_\nu|_\nu \leqslant \delta_\nu$ and $|\alpha_\nu|_\nu = 1$ if $\delta_\nu = 1$. We then can choose $\alpha_{\nu_0} \in k_{\nu_0}$ so that $\prod_\nu |\alpha_\nu|_\nu > C$, where C is as in Lemma 2.17. The resulting $\beta \in k$ given by the same lemma does the job. □

2.15 Strong Approximation Theorem

Theorem 2.18. Let ν_0 be any valuation of the global field k. Let V to be the restricted product of the k_ν with respect to the $\mathfrak{o}_\nu$, where ν runs through all normalized $\nu \neq \nu_0$. Then k is dense in V.

Proof. It is equivalent to proving the following statements: given $\varepsilon > 0$ and a finite set S of valuations $\nu \neq \nu_0$, together with elements $\alpha_\nu \in k_\nu$ for $\nu \in S$, there exists $\beta \in k$ such that $|\beta - \alpha_\nu|_\nu < \varepsilon$ for all $v \in S$ and $|\beta|_\nu \leqslant 1$ for all $\nu \notin S$, $\nu \neq \nu_0$.

Let δ_ν and $U \subseteq \mathbb{A}_k$ be as in Corollary 2.16.1. By Corollary 2.17 there is a $\lambda \neq 0 \in k$ such that

$$\begin{aligned} |\lambda|_\nu &\leqslant \delta_\nu^{-1}\varepsilon \qquad (\nu \in S) \\ |\lambda|_\nu &\leqslant \delta_\nu^{-1} \qquad (\nu \notin S,\, \nu \neq \nu_0) \end{aligned}$$

Then we have $\mathbb{A}_k = \lambda U + k$. Let $\alpha \in \mathbb{A}_k$ have component α_ν at $\nu \in S$ and 0 elsewhere, and write $\alpha = x + \beta$ for $x \in \lambda U$ and $\beta \in k$. Then

- for $\nu \in S$, $|\alpha_\nu - \beta|_\nu = |\alpha - \beta|_\nu = |x|_\nu \leqslant \varepsilon$, and
- for $\nu \notin S$, $\nu \neq \nu_0$, $|\beta|_\nu = |-x|_\nu \leqslant 1$.

□

2.16 Idele Group

Let R be a commutative topological ring. The group of units $R^\times$ need not be a topological group if it is equipped with the subspace topology because the inversion need not be continuous. To make it a topological group, we equip $R^\times$ with the topology generated by the subspace topology from R and the final topology of the inversion $x \mapsto x^{-1}$. It is convenient to state this as follows. There is an injection

$$\begin{aligned} R^\times &\longrightarrow R \times R \\ x &\longmapsto (x, x^{-1}) \end{aligned}$$

of $R^\times$ into the topological product $R \times R$. Topologize $R^\times$ with the subspace topology inherited from $R \times R$. Then clearly $R^\times$ becomes a topological group, and the inclusion $R^\times \to R$ is continuous.

Definition. The **idele group** I_k is the group of units $\mathbb{A}_k^\times$ in $\mathbb{A}_k$ with the topology defined above.

- For each rational prime p, let $\alpha^p \in I_{\mathbb{Q}}$ be such that $\alpha_p^p = p$ and $\alpha_q^p = 1$ for $q \neq p$. Then $a^p \to 1$ as $p \to \infty$ in $\mathbb{A}_k$, but not in the topology of $I_{\mathbb{Q}}$.
- The multiplicative group $k^\times$ of k is naturally embedded into I_k. Elements of $k^\times$ are called **principal ideles**.

- $k^\times \subseteq I_k$ is a discrete subgroup. For since $k \subseteq \mathbb{A}_k$ is discrete, it follows that $k^\times$ injects into $\mathbb{A}_k \times \mathbb{A}_k$ as a discrete subset.

- I_k is the restricted direct product of the $k_\nu^\times$ with respect to the units $\mathfrak{o}_\nu^\times$.

For $\alpha \in I_k$, we write $|\alpha| := \prod_\nu |\alpha|_\nu$, where ν runs over all normalized valuations of k. Then

$$\begin{aligned} I_k &\longrightarrow \mathbb{R}_{>0} \\ \alpha &\longrightarrow |\alpha| \end{aligned}$$

is a continuous homomorphism. Let I_k^1 be the kernel of this homomorphism.

- By the product formula 2.16.3, we have $k^\times \subseteq I_k^1$.

Lemma 2.19. I_k^1 is a closed subset of $\mathbb{A}_k$, and the induced topology from $\mathbb{A}_k$ on I_k^1 coincides with that of from I_k.

Proof. Let $\alpha \in \mathbb{A}_k \backslash I_k^1$. We must find an open neighborhood W of α in $\mathbb{A}_k$ that is disjoint from I_k^1.

- $|\alpha| < 1$. Then there is a finite set S of places such that

  - S contains all the places ν with $|\alpha_\nu|_\nu > 1$ and
  - $\prod_{\nu \in S} |\alpha_\nu|_\nu < 1$.

  Now take $0 < \varepsilon < \min_{\nu \in S} |\alpha|_\nu$ and define

  $$W := \{x = (x_\nu) \in \mathbb{A}_k \mid |x_\nu - \alpha_\nu|_\nu < \varepsilon \text{ for } \nu \in S,\ |x_\nu|_\nu \leqslant 1 \text{ for } \nu \notin S\}$$

  Clearly, every element x in W has $|x| < 1$.

- $|\alpha| > 1$. Put $C = \prod_{\nu : |\alpha_\nu|_\nu > 1} |\alpha_\nu|_\nu > 1$. Then there is a finite set S of places such that S contains

  - all the places ν with $|\alpha_\nu|_\nu > 1$,
  - all archimedean places, and
  - all non-archimedean places ν with $N\mathfrak{p} \leqslant 2C$.

  For $\varepsilon > 0$ define

  $$W := \{x = (x_\nu) \in \mathbb{A}_k \mid |x_\nu - \alpha_\nu|_\nu < \varepsilon \text{ for } \nu \in S,\ |x_\nu|_\nu \leqslant 1 \text{ for } \nu \notin S\}$$

  Take $\varepsilon > 0$ small enough so that $x \in W$ implies $1 < \prod_{\nu \in S} |x_\nu| < 2C$. Then for $x \in W$, if $|x_\nu|_\nu = 1$ for all $\nu \notin S$, then

  $$|x| = \prod_{\nu \in S} |x_\nu|_\nu > 1$$

Otherwise, if $|x_\nu|_\nu < 1$ for some $\nu \notin S$, then $|x_\nu|_\nu \leqslant (N\mathfrak{p})^{-1} < C^{-1}$ so that

$$|x| < \left(\prod_{\nu \in S} |x_\nu|_\nu\right) (2C)^{-1} < 1$$

It remains to show the second statement. Let $\alpha \in I_k^1$. A neighborhood basis of α in $\mathbb{A}_k$ consists of sets of the form

$$W = W_{\varepsilon,S} := \{x \in \mathbb{A}_k \mid |x_\nu - \alpha_\nu|_\nu < \varepsilon \text{ for } \nu \in S,\ |x_\nu|_\nu \leqslant 1 \text{ for } \nu \notin S\}$$

where $\varepsilon > 0$ and S is a finite set of primes. By replacing $\leqslant$ with $=$, we see every such a set contains a neighborhood of α in I_k. Conversely, a neighborhood basis of α in I_k consists of sets of the form

$$H = H_{\varepsilon,S} := \{x \in I_k \mid |x_\nu - \alpha_\nu|_\nu < \varepsilon \text{ for } \nu \in S,\ |x_\nu|_\nu = 1 \text{ for } \nu \notin S\}$$

where $\varepsilon > 0$ and S is a finite set of places containing all archimedean places and all ν with $|\alpha_\nu|_\nu \neq 1$. We claim for ε small enough

$$H_{\varepsilon,S} \cap I_k^1 = W_{\varepsilon,S} \cap I_k^1$$

$\subseteq$ is clear. Let $x \in W_{\varepsilon,S} \cap I_k^1$. Let ε small enough so that $|x_\nu|_\nu = |\alpha_\nu|_\nu$ for all non-archimedean places ν in S. Since x is an idele, we then have $|x_\nu|_\nu = 1$ for almost all $\nu \notin S$. Now it follows from the discreteness of $\nu \notin S$ that it we take ε far smaller, then we must have $|x_\nu|_\nu = 1$ for all $\nu \notin S$. (The argument is similar to that of $|\alpha| > 1$ case in the proof of the first statement.) □

Theorem 2.20. The quotient $I_k^1/k^\times$ is compact.

Proof. By the previous lemma it suffices to find a compact subset W of $\mathbb{A}_k$ such that the projection $W \cap I_k^1 \to I_k^1/k^\times$ is surjective.

Let C be as in Lemma 2.17, and take $\alpha \in I_k$ such that $|\alpha| > C$. Take

$$W = \{x \in \mathbb{A}_k \mid |x_\nu|_\nu \leqslant |\alpha_\nu|_\nu \text{ for all } \nu\}$$

Let $y \in I_k^1$. By the same lemma there exists $r \in k^\times$ such that $|r|_\nu \leqslant |y_\nu^{-1}\alpha_\nu|$ for all ν. Then $ry \in W$, as required. □

2.17 Ideal and Divisors

First let k be a number field. The set of all fractional ideals forms an abelian group $\mathfrak{I}_k$ free on the set of finite primes of the ring of integers $\mathfrak{o}_k$ of k. Denote by P_k the subgroup of all principal fractional ideals in k.

Definition. The **ideal class group** of k is the quotient $\mathrm{Cl}(k) := \mathfrak{I}_k/P_k$

Equip $\mathfrak{I}_k$ with the discrete topology. Then the natural map

$$\begin{tikzcd}
I_k \arrow[r] & \mathfrak{I}_k \\
\alpha \arrow[r, mapsto] & \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} \alpha}
\end{tikzcd}$$

is continuous, and the image of $k^\times \subseteq I_k$ is exactly the subgroup of principal ideals.

Theorem 2.21. $\# \operatorname{Cl}(k) < \infty$.

Proof. The continuous map $I_k \to \mathfrak{I}_k$ is surjective, and so is the induced map $I_k/k^\times \to \operatorname{Cl}(k)$. Since $I_k/k^\times$ is compact by Theorem 2.20, so is the continuous image $\operatorname{Cl}(k)$. But $\operatorname{Cl}(k)$ is equipped with the discrete topology, this means $\operatorname{Cl}(k)$ is a finite group. □

Now consider a finite separable extension k of $\mathbb{F}_q(t)$, where t is transcendental over the finite field $\mathbb{F}_q$.

2.18 Units

Let S be a finite set of places containing all archimedean places. The intersection $k_S := I_{k,S} \cap k^\times$ is called the **group of S-units**. Explicitly,

$$k_S := \{r \in k^\times \mid |r|_\nu = 1 \text{ for all } \nu \notin S\}$$

When $S = S_\infty$ consists of only archimedean places of k, then k_{S_∞} is the usual group of units $\mathfrak{o}_k^\times$.

Lemma 2.22. Let $0 < c \leqslant C < \infty$. Then the set

$$\{r \in k_S \mid c \leqslant |x|_\nu \leqslant C \text{ for } \nu \in S\}$$

is finite.

Proof. We have

$$\{r \in k_S \mid c \leqslant |x|_\nu \leqslant C \text{ for } \nu \in S\} = k^\times \cap I_{k,S} \cap \{x \in I_k \mid c \leqslant |x|_\nu \leqslant C \text{ for } \nu \in S\}$$

$k^\times$ is discrete and the latter two sets are compact, so the required set is both discrete and compact, whence finite. □

Lemma 2.23. The set

$$\{r \in k \mid |r|_\nu = 1 \text{ for all places } \nu\}$$

is finite, and consists of all roots of unity of k.

Proof. A root of unity $r \in k^\times$ clearly satisfies $|r|_\nu = 1$ for all ν. Conversely, by the previous lemma with $c = C = 1$ and any S we see $\#\{r \in k \mid |r|_\nu = 1 \text{ for all places } \nu\} < \infty$, and since they form a (finite) group, they are all roots of unity. □

Theorem 2.24. k_S is a direct sum of a finite cyclic group and a free abelian group of rank $s - 1$, where $s = \#S$.

Proof. Let I_S consist of ideles α with $|\alpha_\nu|_\nu = 1$ for all $\nu \notin S$. By definition, this is an open subgroup of I_k. If we put

$$I_S^1 := I_S \cap I_k^1$$

then I_S^1 is an open subgroup of I_k^1, and

$$I_S^1/k_S = I_S^1/(I_S^1 \cap k^\times) \subseteq I_S^1/k^\times$$

is also open. Since it is a subgroup, it is also closed, and hence compact by Theorem 2.20.

Consider the map

$$\begin{array}{rcl} \log : I_S & \longrightarrow & \mathbb{R}^S \\ \alpha & \longmapsto & (\log|\alpha_\nu|_\nu)_{\nu\in S} \end{array}$$

where $\nu_1, \dots, \nu_s$ are the places in S. We have the following properties.

(i) $k_S \cap \ker\log$ is a finite group consisting of roots of unity of k. This follows from Lemma 2.23.

(ii) $\log k_S$ is discrete. This is because by Lemma 2.22

$$\{r \in k_S \mid 2^{-1} \leqslant |r|_\nu \leqslant 2 \text{ for all } \nu \in S\}$$

is a finite set.

(iii) $\log I_S = \prod_{\nu\in S,\, \nu\nmid\infty} \mathbb{Z}\log\left(\#\mathfrak{o}_\nu/\mathfrak{p}_\nu\right) \times \prod_{\nu\in S,\, \nu\mid\infty} \mathbb{R}$. This is clear.

(iv) $\log I_S^1 = \left\{(x_\nu)_{\nu\in S} \in \log I_S \mid \sum_{\nu\in S} x_\nu = 0\right\}$. Indeed, $\alpha \in I_S^1$ if and only if $\prod_{\nu\in S}|\alpha_\nu|_\nu = 1$, or $\sum_{\nu\in S}\log|\alpha_\nu|_\nu = 0$.

Since I_S^1/k_S is compact and $\log$ is continuous, it follows that $\log I_S^1/\log k_S$ is compact as well. Hence, $\mathbb{R}\otimes\log k_S$ is the same rank as $\mathbb{R}\otimes\log I_S^1$. But it follows from (iii) and (iv) that $\dim\mathbb{R}\otimes\log I_S^1 = \#S - 1$. This finishes the proof. □

2.19 Inclusion and Norm Maps for Adeles, Ideles and Ideals

Chapter 3

Cyclotomic Fields and Kummer Extensions

3.1 Cyclotomic Fields

3.2 Kummer Extensions

Lemma 3.1. The discriminant of $K(\sqrt[n]{a})$ over K divides $n^n a^{n-1}$; $\mathfrak{p}$ is unramified if $\mathfrak{p} \nmid na$. If a^f is the least power of a such that $x^n - a^f \equiv 0 \pmod{)}p$ is solvable, then f is the residue class degree.

Chapter 4

Cohomology of Groups

4.1 Definition of Cohomology

4.2 The Standard Complex

4.3 Homology

4.4 Change of Groups

Let A be a G-module and A' a G'-module. If $\varphi : G' \to G$ is a group homomorphism and $f : A \to A'$ is a $\mathbb{Z}$-homomorphism with the property that for each $g' \in G'$ and $a \in A$

$$f(\varphi(g')a) = g'f(a)$$

then the pair (φ, f) induces a cochain map on the $\operatorname{Hom}_G(P, A) \to \operatorname{Hom}_{G'}(P', A)$ (with P, P' the standard complex)

$$\operatorname{Hom}_G(P_i, A) \longrightarrow \operatorname{Hom}_{G'}(P_i', A)$$

$$\mathbb{Z}[G^{i+1}] \xrightarrow{\alpha} A \longmapsto \mathbb{Z}[G'^{i+1}] \xrightarrow{f\circ\alpha\circ\varphi} A'$$

hence a homomorphism on cohomology class

$$(\varphi, f)^* : H^q(G, A) \longrightarrow H^q(G', A')$$

for any G-module A, where we regard A as a G'-module via f. On the other hand,

- Take $G' = H \leqslant G$ and $\varphi : H \to G$ to be the embedding. Then the induced map is called the **restriction** homomorphism

$$\text{res} = (\varphi, \text{id})^* : H^q(G, A) \longrightarrow H^q(H, A)$$

- Take $G' = H \trianglelefteq G$ and $\varphi : G \to G/H$ to be the quotient map. For any G-module A we have a G/H-module A^H and the natural inclusion $\iota : A^H \to A$. The map
$$\inf = (\varphi, \iota)^* : H^q(G/H, A^H) \longrightarrow H^q(G, A)$$
is called the **inflation** homomorphism.

- Let $t \in G$. Take $\varphi : s \mapsto tst^{-1}$ and $f : a \mapsto t^{-1}a$. Then we have the map
$$\sigma_t = (\varphi, f)^* : H^q(G, A) \longrightarrow H^q(G, A)$$

Proposition 4.1. σ_t defined right above is the identity map for all $q \geqslant 0$.

Proof. When $q = 0$, we think of σ_t as the composition
$$A^G \xrightarrow{\varphi^*} A^G \xrightarrow{f_*} A^G$$
on which the G-action on the second A is via φ; for clarity we denote it by B. φ^* gives an isomorphism $t.A^G \cong B$, and f_* is just the multiplication by t^{-1}. Hence σ_t is the identity map when $q = 0$. For general case, we conduct dimension shifting. We have a commutative diagram
$$\begin{tikzcd}
H^q(G, J_G \otimes_G A) \arrow[r, "\delta"] \arrow[d, "\sigma_t", "\wr"'] & H^{q+1}(G, A) \arrow[r] \arrow[d, "\sigma_t"] & H^{q+1}(G, \mathbb{Z}[G] \otimes_G A) = 0 \\
H^q(G, J_G \otimes_G A) \arrow[r, "\delta", "\sim"'] & H^{q+1}(G, A) \arrow[r] & H^{q+1}(G, \mathbb{Z}[G] \otimes_G A) = 0
\end{tikzcd}$$
By induction hypothesis the leftmost arrow is identity, and hence so is the middle one. Here J_G is defined by the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z}[G] \to J_G \to 0$. □

Now consider homology. A group homomorphism $\varphi : G' \to G$ induces a chain map $\varphi \otimes \mathrm{id} : P' \otimes_{G'} A \to P \otimes_G A$, and hence a homomorphism of homology class
$$\varphi_* : H_q(G', A) \longrightarrow H_q(G, A)$$

- Take $G' = H \leqslant G$ and $\varphi : H \to G$ to be the embedding. The induced map
$$\mathrm{cores} = \varphi_* : H_q(H, A) \longrightarrow H_q(G, A)$$
is called the **corestriction** map.

Let $H \leqslant G$ and A an H-module. Form a G-module $\mathrm{ind}_H^G A := \mathrm{Hom}_H(\mathbb{Z}[G], A)$ on which G acts by $(\sigma f)(g) := f(g\sigma)$; this makes $\mathrm{ind}_H^G A$ a left G-module. Consider the homomorphism
$$f : \mathrm{ind}_H^G A \longrightarrow A$$
$$\varphi \longmapsto \varphi(1)$$
which is compatible with the inclusion $\iota : H \to G$. Hence the pair (ι, f) induces a map on cohomology class
$$(\iota, f)^* : H^q(G, \mathrm{ind}_H^G A) \longrightarrow H^q(H, A)$$

Proposition 4.2 (Shapiro's lemma)**.** The map $(\iota, f)^*$ is an isomorphism.

Proof. Suppose $q = 0$; the map becomes

$$\begin{aligned}(\operatorname{ind}_H^G A)^G = H^0(G, \operatorname{ind}_H^G(A)) &\longrightarrow H^0(H, A) = A^H \\ \varphi : G \to A &\longmapsto \varphi(1)\end{aligned}$$

Since φ is fixed by G, $\varphi(g) = \sigma\varphi(g) = \varphi(g\sigma)$ for all $\sigma, g \in G$; taking $g = 1$, we obtain $\varphi(1) = \varphi(\sigma)$ for all $\sigma \in G$. Hence it is an isomorphism. The general $q > 0$ case follows from dimension shifting. □

4.5 The Restriction-Inflation Sequence

4.6 The Tate Groups

Proposition 4.3. If $[G : H] = n$, then $\operatorname{cores} \circ \operatorname{res} = n$.

Corollary 4.3.1. If $\#G = n$, then all the groups $\hat{H}^q(G, A)$ are annihilated by n.

Corollary 4.3.2. If A is a finite G-module, then all the groups $\hat{H}^q(G, A)$ are finite.

Corollary 4.3.3. Let S be a Sylow p-subgroup of G. Then

$$\operatorname{res} : \hat{H}^q(G, A) \longrightarrow \hat{H}^q(S, A)$$

is injective on the p-primary component of $\hat{H}^q(G, A)$.

Corollary 4.3.4. If an element $x \in \hat{H}^q(G, A)$ restricts to zero in $\hat{H}^q(S, A)$ for all Sylow subgroups S of G, then $x = 0$.

4.7 Cup-products

Theorem 4.4. Let G be a finite group. Then there exists one and only one family of homomorphisms

$$\begin{aligned}\hat{H}^q(G, A) \otimes \hat{H}^q(G, B) &\longrightarrow \hat{H}^{p+q}(G, A \otimes B) \\ a \otimes b &\longmapsto a.b\end{aligned}$$

(the unadorned tensor product is over $\mathbb{Z}$) defined for all integers p, q and all G-modules A, B such that

(i) These homomorphisms are functorial in A and B;

(ii) For $p = q = 0$ they are induced by the natural product

$$A^G \otimes B^G \longrightarrow (A \otimes B)^G$$

(iii) If $0 \to A \to A' \to A'' \to 0$ is an exact sequence of G-modules, and if $0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$ is exact, then for $a'' \in \hat{H}^q(G, A'')$ and $b \in \hat{H}^q(G, B)$ we have

$$\delta(a'').b = \delta(a''.b) \in \hat{H}^{p+q+1}(G, A \otimes B)$$

(iv) If $0 \to B \to B' \to B'' \to 0$ is an exact sequence of G-modules, and if $0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$ is exact, then for $a \in \hat{H}^p(G, A)$ and $b'' \in \hat{H}^q(G, B'')$ we have

$$a.(\delta b'') = (-1)^p \delta(a.b) \in \hat{H}^{p+q+1}(G, A \otimes B)$$

Proof. Let $(P_n)_{n \in \mathbb{Z}}$ be a complete resolution for G. The proof of existence depends on constructing G-module homomorphisms

$$\varphi_{p,q} : P_{p+q} \longrightarrow P_p \otimes P_q$$

for all pairs of integers p, q satisfying the following two conditions:

(1) $\varphi_{p,q} \circ d = (d \otimes 1) \circ \varphi_{p+1,q} + (-1)^p (1 \otimes d) \circ \varphi_{p,q+1}$

(2) $(\varepsilon \otimes \varepsilon) \circ \varphi_{0,0} = \varepsilon$

where $\varepsilon : P_0 \to \mathbb{Z}$ is defined by $\varepsilon(g) = 1$ for all $g \in G$. Once the $\varphi_{p,q}$ are defined, we proceed as follows. Let $f \in \mathrm{Hom}_G(P_p, A)$, $g \in \mathrm{Hom}_G(P_q, B)$ be cochains, and define the product cochain $f.g \in \mathrm{Hom}_G(P_{p+q}, A \otimes B)$ by

$$f.g = (f \otimes g) \circ \varphi_{p+q}$$

Then it follows from (1) that

$$\begin{aligned} d(f.g) &= (f \otimes g) \circ \varphi_{p+q} \circ d \\ &= (f \otimes g) \circ ((d \otimes 1) \circ \varphi_{p+1,q} + (-1)^p (1 \otimes d) \circ \varphi_{p,q+1}) \\ &= (df \otimes g) \circ \varphi_{p+1,q} + (-1)^p (f \otimes dg) \circ \varphi_{p,q+1} \\ &= df.g + (-1)^p f.dg \end{aligned}$$

Hence if f, g are cocycles, so is $f.g$, and the cohomology class of $f.g$ depends only on the classes of f, g: in other words, we have a homomorphism

$$\hat{H}^q(G, A) \otimes \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, A \otimes B)$$

(i) is clear, and (ii) follows from (2). For (iii), we compute directly. Consider the exact sequence

$$0 \longrightarrow \mathrm{Hom}_G(P_p, A) \longrightarrow \mathrm{Hom}_G(P_p, A') \longrightarrow \mathrm{Hom}_G(P_p, A'') \longrightarrow 0$$

Let $\alpha'' \in \mathrm{Hom}_G(P_p, A'')$ be a representative cocycle of the class a'', and lift α'' back to $\alpha' \in \mathrm{Hom}(P_p, A')$; $d\alpha'$ has zero image in $\mathrm{Hom}_G(P_{p+1}, A'')$ and therefore lies in $\mathrm{Hom}_G(P_{p+1}, A)$. The class of $d\alpha'$ in $\hat{H}^{p+1}(G, A)$ is $\delta(\alpha'')$. Hence if $\beta \in \mathrm{Hom}_G(P_p, B)$ is a cocycle in the class b, then

- $\alpha''.\beta$ represents the class $a''.b$;
- $d(\alpha'.\beta)$ represents $\delta(a''.b)$;
- $d\alpha'.\beta$ represents $\delta a''.b$.

But since $d\beta = 0$, we have $d(\alpha'.\beta) = d\alpha'.\beta$; hence $\delta(a''.b) = \delta a''.b$. The proof of (iv) is similar.

It remains to construct the $\varphi_{p,q}$ which we shall do for the standard complete resolution ($P_q = \mathbb{Z}[G^{q+1}]$ if $q \geqslant 0$; $P_{-q} = P_{q-1}^\vee$ if $q \geqslant 1$). If $q \geqslant 1$, $P_{-q} = P_{q-1}^\vee$ has a $\mathbb{Z}$-basis consisting of all $(g_1^*, \ldots, g_q^*)$ that sends $(g_1, \ldots, g_q)$ to 1 and every other basis element to 0. In terms of this basis of P_{-q}, the coboundary map $d : P_{-q} \to P_{-q-1}$ is given by

$$d(g_1^*, \ldots, g_q^*) = \sum_{s \in G} \sum_{i=0}^{q} (-1)^i (g_1^*, \ldots, g_i^*, s^*, g_{i+1}^*, \ldots, g_q^*)$$

and $d : P_0 \to P_{-1}$ by $d(g_0) = \sum\limits_{s \in G} (s^*)$.

Now define $\varphi_{p,q} : P_{p+q} \to P_p \otimes P_q$ as follows:

(a) if $p \geqslant 0$ and $q \geqslant 0$,

$$\varphi_{p,q}(g_0, \ldots, g_{p+q}) = (g_0, \ldots, g_p) \otimes (g_p, \ldots, g_{p+q})$$

(b) if $p \geqslant 1$ and $q \geqslant 1$,

$$\varphi_{-p,-q}(g_1^*, \ldots, g_{p+q}^*) = (g_0^*, \ldots, g_p^*) \otimes (g_p^*, \ldots, g_{p+q}^*)$$

(c) if $p \geqslant 0$ and $q \geqslant 1$,

$$\begin{aligned}
\varphi_{p,-p-q}(g_1^*, \ldots, g_p^*) &= \sum (g_1, s_1, \ldots, s_p) \otimes (s_p^*, \ldots, s_1^*, g_1^*, \ldots, g_q^*) \\
\varphi_{-p-q,p}(g_1^*, \ldots, g_p^*) &= \sum (g_1^*, \ldots, g_q^*, s_1^*, \ldots, s_p^*) \otimes (s_p, \ldots, s_1, g_q) \\
\varphi_{p+q,-q}(g_0, \ldots, g_p) &= \sum (g_0, \ldots, g_p, s_1, \ldots, s_q) \otimes (s_q^*, \ldots, s_1^*) \\
\varphi_{-q,p+q}(g_0, \ldots, g_p) &= \sum (s_1^*, \ldots, s_q^*) \otimes (s_q, \ldots, s_q, g_0, \ldots, g_p)
\end{aligned}$$

Note that $\varphi_{0,0}(g) = (g) \otimes (g)$, so (2) is verified easily. The verification of (1) is tedious but straightforward. This proves the existence part. The uniqueness follows easily via dimension shifting. □

Proposition 4.5. Let us use the identification $A \otimes B = B \otimes A$ and $(A \otimes B) \otimes C = A \otimes (B \otimes C)$. Then

1. $(a.b).c = a.(b.c)$.
2. $a.b = (-1)^{\dim a . \dim b} b.a$.
3. $\operatorname{res}(a.b) = \operatorname{res}(a). \operatorname{res}(b)$.
4. $\operatorname{cores}(a. \operatorname{res}(b)) = \operatorname{cores}(a).b$.

Proof.

1.

2.

3.

4. Let $H \leqslant G$ be a subgroup, $a \in \hat{H}^p(H,A)$ and $b \in \hat{H}^q(G,B)$. In the case $p = q = 0$, a is represented by $\alpha \in A^H$ so $\operatorname{cores}(a)$ is represented by $N_{G/H}\alpha \in A^G$; b is represented by $\beta \in B^G$ so that $\operatorname{cores}(a).b$ is represented by
$$N_{G/H}\alpha \otimes \beta = \sum s_i\alpha \otimes \beta = \sum s_i(\alpha \otimes \beta) = N_{G/H}(\alpha \otimes \beta)$$
On the other hand, $a.\operatorname{res}(b)$ is represented by $\alpha \otimes \beta \in (A \otimes B)^H$ so that $\operatorname{cores}(a.\operatorname{res}(b))$ is represented by $N_{G/H}(\alpha \otimes \beta)$.

   Now we apply dimension shifting to finish the general case. Let $\delta_* : \hat{H}^0(G,A^*) \xrightarrow{\sim} \hat{H}^*(G,A)$ be the connecting homomorphisms $(* = p,q)$. Then for $a \in \hat{H}^p$ and $b \in\in \hat{H}^q$
$$\begin{aligned}
\operatorname{cores}(a.\operatorname{res}(b)) &= \operatorname{cores}(\delta_p a'.\operatorname{res}(\delta_q b')) \\
&= \operatorname{cores}(\delta_p(a'.\delta_q(\operatorname{res} b'))) \\
&= \delta_p \operatorname{cores}((-1)^p\delta_q(a'.\operatorname{res} b')) \\
&= (-1)^p\delta_p\delta_q \operatorname{cores}(a'.\operatorname{res} b') \\
&= (-1)^p\delta_p\delta_q(\operatorname{cores}(a').b) = \cdots\cdots = \operatorname{cores}(a).b
\end{aligned}$$

   Here we use the fact that res and cores commute with $\delta_\bullet$.

□

Proposition 4.6. Let $H \trianglelefteq G$, $p,q > 0$, $\alpha \in H^p(G/H,A)$ and $\beta \in H^q(G/H,B)$. Then
$$\inf_{G/H}(\alpha) \cup \inf_{G/H}(\beta) = \inf_{G/H}(\alpha \cup \beta) \in H^{p+q}(G, A \otimes B)$$

Proof. This follows at once from the definition of inflation and that of cup product in positive dimension.

□

Let A, B, C be G-modules and $\varphi : A \otimes B \to C$ a G-homomorphism. Then we have a map
$$\begin{tikzcd}
\hat{H}^p(G,A) \otimes \hat{H}^q(G,B) \arrow[r, "\cup"] & \hat{H}^q(G, A \otimes B) \arrow[r, "\varphi^*"] & \hat{H}^q(G,C) \\
a \otimes b \arrow[rr, mapsto] & & \varphi^*(a \cup b)
\end{tikzcd}$$
called the **cup-product relative to** φ.

4.8 Computations of Cup Products in Low Dimensions

In the following G denotes a finite group, and $A, B, \dots$ are G-modules. If $a \in A^G$, we denote by $\overline{a}^0$ its image in $\hat{H}^0(G, A)$. If $a \in A$ with $Na = 0$, denote by $\overline{a}_0$ its image in $\hat{H}^{-1}(G, A)$.

Lemma 4.7. Let $a \in A^G$, $f_a \in \operatorname{Hom}_G(\mathbb{Z}, A)$ such that $f_a(1) = a$ and $x \in \hat{H}^n(G, B)$. Then the cup product

$$\overline{a}^0 \cup x \in \hat{H}^n(G, A \otimes B)$$

equals the image of x under the homomorphism induced by $f_a \otimes 1 : B = \mathbb{Z} \otimes B \to A \otimes B$.

Proof. Consider first the case $n \geqslant 0$, and we deal with it by induction. Say x is represented by the cycle ξ. When $n = 0$, $\overline{a}^0 \cup x$ is represented by $a \otimes \xi$, and $(f_a \otimes 1)(\xi) = f_a(1) \otimes \xi = a \otimes \xi$. For $n > 0$, consider the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G] \longrightarrow J_G \longrightarrow 0$$

Since it splits, it remains exact after tensoring with B, and since $\mathbb{Z}[G] \otimes B$ is free over G, the connecting homomorphism

$$\delta : \hat{H}^{n-1}(G, J_G \otimes B) \longrightarrow \hat{H}^n(G, B)$$

is an isomorphism; say $x = \delta y$, $y \in \hat{H}^{n-1}$. Then

$$\overline{a}^0 \cup x = \overline{a}^0 \cup \delta y = \delta(\overline{a}^0 \cup y) = \delta((f_a \otimes 1)^*(y)) = (f_a \otimes 1)^*(\delta y) = (f_a \otimes 1)^*(x)$$

For the case $n \geqslant 0$, use another exact sequence, namely

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

to do dimension shifting. □

Lemma 4.8. Given $a \in A$ with $Na = 0$, and let $f : G \to B$ be a 1-cocycle, $\overline{f} \in \hat{H}^1(G, B)$ its cohomology class. Then

$$\overline{a}_0 \cup \overline{f} = \overline{c}^0 \in \hat{H}^0(G, A \otimes B)$$

with

$$c = -\sum_{t \in G} ta \otimes f(t)$$

Proof. Use the exact sequence as above.

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G] \longrightarrow J_G \longrightarrow 0$$

Since $\hat{H}^1(G, \mathbb{Z}[G] \otimes B) = 0$, there exists $b' \in \mathbb{Z}[G] \otimes B$ such that $f(t) = db'(t) = tb' - b'$ for all $t \in G$. Let $b'' \in B'' := J_G \otimes B$ be the image of b'; then $\overline{f} = \delta(\overline{b''}) \in \hat{H}^1(G, B)$. By the preceding lemma

$$\overline{a_0} \cup \overline{f} = -\delta(\overline{a_0} \cup b'') = -\delta(\overline{a \otimes b''})$$

Recall that $\delta : \hat{H}^{-1}(G, A \otimes B'') \to \hat{H}^0(G, A \otimes B)$ is defined by norm. Thus

$$-\delta(\overline{a \otimes b''}) = -\overline{N_G(a \otimes b')} = -\overline{\sum_{t \in G} ta \otimes tb'}$$

But

$$-\overline{\sum_{t \in G} ta \otimes tb'} = -\overline{\sum_{t \in G} ta \otimes f(t) + \sum_{t \in G} ta \otimes b'} = -\overline{\sum_{t \in G} ta \otimes f(t)}$$

for $Na = 0$. □

Recall the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I_G \arrow[r] & \mathbb{Z}[G] \arrow[r] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

Also, for $s \in G$ denote by i_s the element $s - 1 \in I_G$. Then $(\overline{i_s})_0 \in \hat{H}^{-1}(G, I_G)$. Let $\overline{s} \in \hat{H}^{-2}(G, \mathbb{Z})$ be such that $d\overline{s} = (\overline{i_s})_0$; this defines by passing to the quotient the canonical isomorphism

$$\begin{tikzcd} G/G' \arrow[r] & \hat{H}^{-2}(G, \mathbb{Z}) \\ s \arrow[r, mapsto] & \overline{s} \end{tikzcd}$$

Lemma 4.9. Let $f : G \to B$ be a 1-cocycle and $\overline{f} \in H^1(G, B)$ its cohomological class. Then for every $s \in G$,

$$\overline{s} \cup \overline{f} = \overline{f(s)}_0 \in \hat{H}^{-1}(G, B)$$

where we identity $\mathbb{Z} \otimes B$ with B.

Proof. The connecting homomorphism $\delta : \hat{H}^{-1}(G, B) \to \hat{H}^0(G, I_G \otimes B)$ is an isomorphism, so it suffices to show $\delta(\overline{s} \cup \overline{f}) = \delta(\overline{f(s)}_0) \in \hat{H}^0(G, B \otimes I_G)$. By definition,

$$\delta(\overline{f(s)}_0) = \overline{\sum_{t \in G} t \otimes tf(s)}$$

On the other hand, by the preceding lemma

$$\delta(\overline{s} \cup \overline{f}) = \delta(\overline{s}) \cup \overline{f} = (\overline{i_s})_0 \cup \overline{f} = \overline{-\sum_{t \in G} ti_s \otimes f(t)} = \overline{\sum_{t \in G} (t - ts) \otimes f(t)}$$

But $f(t) = f(ts) - tf(s)$, we then have

$$\begin{aligned} \sum_{t \in G} (t - ts) \otimes f(t) &= \sum_{t \in G} t \otimes f(t) - \sum_{t \in G} ts \otimes (f(ts) - tf(s)) \\ &= \sum_{t \in G} t \otimes f(t) - \sum_{t \in G} ts \otimes f(ts) + \sum_{t \in G} ts \otimes tf(s) \\ &= \sum_{t \in G} ts \otimes tf(s) \end{aligned}$$

Finally,

$$\sum_{t \in G} ts \otimes tf(s) - \sum_{t \in G} t \otimes tf(s) = N((s-1) \otimes f(s))$$

□

Lemma 4.10. Let $u : G \times G \to B$ be a 2-cocycle, $\overline{u} \in H^2(G, B)$ its cohomological class. Then for all $s \in G$,

$$\overline{s} \cup \overline{u} = \overline{a}^0 \in \hat{H}^0(G, B)$$

where $a = \sum\limits_{t \in G} u(t, s)$.

Proof. Use the exact sequence

$$0 \longrightarrow B \longrightarrow B' \longrightarrow B'' \longrightarrow 0$$

Since $H^2(G, B') = 0$, $u = du'$ for some 1-cocycle $u' : G \to B'$. Let $u'' : G \to B''$ be the image of u'; then $\delta(\overline{u''}) = \overline{u}$. Then by the preceding lemma

$$\overline{s} \cup \delta\overline{u''} = \delta(\overline{u''(s)_0}) = \overline{\sum_{t \in G} tu'(s)}$$

But $u(t, s) = du'(t, s) = tu'(s) - u'(ts) + u'(t)$, hence

$$\sum_{t \in G} tu'(s) = \sum_{t \in G} u(t, s) + u'(ts) - u'(t) = \sum_{t \in G} u(t, s)$$

□

Corollary 4.10.1. Let G be a finite group of order n. Then the cupping

$$\hat{H}^{-2}(G, \mathbb{Z}) \times H^2(G, \mathbb{Z}) \longrightarrow \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$$

is given by $\overline{s} \cup \delta_\chi = n\overline{\chi}(s) \bmod n$, where $\overline{\chi}(s) \in \mathbb{Q}$ is such that $\chi(s) \equiv \overline{\chi}(s) \pmod 1$.

Proof. Define $\delta_{\overline{\chi}} : G \times G \to \mathbb{Z}$ by

$$\delta_{\overline{\chi}}(\tau, \sigma) := \overline{\chi}(\tau) + \overline{\chi}(\sigma) - \overline{\chi}(\tau\sigma)$$

Then $\delta_{\overline{\chi}}$ represents $\delta_\chi \in H^2(G, \mathbb{Z})$. Summing over $\tau \in G$, we obtain

$$\sum_{\tau \in G} \delta_{\overline{\chi}}(\tau, \sigma) = n\overline{\chi}(\sigma)$$

The result follows from Lemma above. □

Corollary 4.10.2. Let G be a finite cyclic group of order n, A a G-module and φ a generator of G. Let χ be a generator of $\mathrm{Hom}_\mathbb{Z}(G, \mathbb{Q}/\mathbb{Z})$. Then cupping with δ_χ and with $\overline{\varphi}$ give mutually inverse isomorphism

$$\begin{tikzcd} \hat{H}^p(G, A) \arrow[r, shift left, "\cup\delta_\chi"] & H^{p+2}(G, A) \arrow[l, shift left, "\cup\overline{\varphi}"] \end{tikzcd}$$

Proof. Indeed, we have $\overline{s} \cup \delta_\chi = \delta_\chi \cup \overline{s} = n\overline{\chi}(\varphi) \equiv 1 \pmod n$. □

4.9 Cyclic Groups: Herbrand Quotient

Lemma 4.11. Let G be a finite group and let M M' be two finite-dimensional $\mathbb{Q}[G]$-modules such that $M_{\mathbb{R}} = M \otimes_{\mathbb{Q}} \mathbb{R}$ and $M'_{\mathbb{R}} = M' \otimes_{\mathbb{Q}} \mathbb{R}$ are isomorphic as $\mathbb{R}[G]$-modules. Then M, M' are isomorphic as $\mathbb{Q}[G]$-modules.

Proof. Let K be any field, L/K be a field extension and A a K-algebra. If V is any K-vector space denote by V_L the L-vector space $V \otimes_K L$. Let M, M' be A-modules which are finite dimensional as K-vector space. An A-homomorphism $\varphi : M \to M'$ induces an A_L-homomorphism $\varphi \otimes 1 : M_L \to M'_L$, and $\varphi \mapsto \varphi \otimes 1$ gives rise to an L-isomorphism

$$\mathrm{Hom}_A(M.M')_L \cong \mathrm{Hom}_{A_L}(M_L, M'_L)$$

Now take $K = \mathbb{Q}$, $L = \mathbb{R}$, $A = \mathbb{Q}[G]$, so that $A_L = \mathbb{R}[G]$. The hypotheses imply M, M' have the same dimension over $\mathbb{Q}$, so by choosing bases of M, M' we can speak of the determinant of an element of $\mathrm{Hom}_{\mathbb{Q}[G]}(M, M')$, or of $\mathrm{Hom}_{\mathbb{R}[G]}(M_{\mathbb{R}}, M'_{\mathbb{R}})$. (It will of course depends on the bases chosen.)

From the isomorphism above it follows that if ξ_i are a $\mathbb{Q}$-basis of $\mathrm{Hom}_{\mathbb{Q}[G]}(M, M')$, they are also an $\mathbb{R}$-basis of $\mathrm{Hom}_{\mathbb{R}[G]}(M_{\mathbb{R}}, M'_{\mathbb{R}})$. Since $M_{\mathbb{R}}$, $M_{\mathbb{R}'}$ are $\mathbb{R}[G]$-isomorphic, there exist $a_i \in \mathbb{R}$ such that $\det(\sum a_i \xi_i) \neq 0$. Hence the polynomial

$$F(t) := \det(\sum t_i \xi_i) \in \mathbb{Q}[t_1, \dots, t_m]$$

where t_i are independent indeterminants over $\mathbb{Q}$, are not identically zero, since $F(a) \neq 0$. Since $\mathbb{Q}$ is infinite, there exist $b_i \in \mathbb{Q}$ such that $F(b) \neq 0$, and then $\sum b_i \xi_i$ is a $\mathbb{Q}[G]$-isomorphism of M onto M'. □

Proposition 4.12. Let E be a finite-dimensional real representation space of G, and let L, L' be two lattices of E which span E and are invariant under G. Then if either of $h(L)$, $h(L')$ is defined, so is the other, and they are equal.

Proof. Apply Lemma with $M = L \otimes \mathbb{Q}$, $M' = L' \otimes \mathbb{Q}$; $M_{\mathbb{R}}$ and $M'_{\mathbb{R}}$ are $\mathbb{R}[G]$-isomorphic to E. Hence there exists a $\mathbb{Q}[G]$-isomorphism $\varepsilon : L \otimes \mathbb{Q} \to L' \otimes \mathbb{Q}$. Say $\varphi(L) \subseteq \dfrac{1}{N} L'$ for some $N \in \mathbb{N}$. Hence $f = N\varphi$ maps L injectively into L'. Consider the exact sequence

$$0 \longrightarrow L \xrightarrow{f} L' \longrightarrow \mathrm{coker}(f) \longrightarrow 0$$

Since L, L' have the same rank as abelian groups, $\mathrm{coker}(f)$ is finite, and hence $h(L) = h(L')$ if either one is defined. □

4.10 Coholomogical Triviality

A G-module A is **cohomologically trivial** if for every subgroup $H \leqslant G$, $\hat{H}^q(H, A) = 0$ for all $q \in \mathbb{Z}$.

Lemma 4.13. Let p be a prime number, G a p-group and A a G-module such that $pA = 0$. TFAE

(i) $A = 0$.

(ii) $H^0(G, A) = 0$.

(iii) $H_0(G, A) = 0$.

Proof. Clearly (i) implies (ii) and (iii).

Assume (ii). Suppose $A \neq 0$ and pick a nonzero element $x \in A$. The submodule $B = x\mathbb{Z}[G]$ is finite of order a power of p. Consider the G-orbit of the elements of B; the orbit-stabilizer formula tells us that every orbit is of p-power order. There is at least one fixed point, namely 0, so there are at least p fixed point; hence $H^0(G, A) = A^G \neq 0$.

Assume (iii). Consider $H^0(G, \mathrm{Hom}_{\mathbb{F}_p}(A, \mathbb{F}_p)) = (\mathrm{Hom}_{\mathbb{F}_p}(A, \mathbb{F}_p))^G = \mathrm{Hom}_G(A, \mathbb{F}_p) = \mathrm{Hom}_{\mathbb{F}_p}(A_G, \mathbb{F}_p)$. Since $A_G = H_0(G, A) = 0$, it follows $H^0(G, \mathrm{Hom}_{\mathbb{F}_p}(A, \mathbb{F}_p)) = 0$, and thus $\mathrm{Hom}_{\mathbb{F}_p}(A, \mathbb{F}_p) = 0$. Hence $A = 0$. □

Lemma 4.14. With the same hypothesis as above, suppose $H_1(G, A) = 0$. Then A is a free module over $\mathbb{F}_p[G]$.

Proof. Since $pA = 0$, $pH_0(G, A) = 0$, and therefore $H_0(G, A)$ is a $\mathbb{F}_p$-vector space. Take a basis e_λ of this space and lift each e_λ to $a_\lambda \in A$. Let A' be the submodule of A generated by the a_λ, and let $A'' = A/A'$. We then have an exact sequence

$$\begin{tikzcd} H_0(G, A') \arrow[r, "\alpha"] & H_0(G, A) \arrow[r] & H_0(G, A'') \arrow[r] & 0 \end{tikzcd}$$

where by our construction α is an isomorphism. Hence $H_0(G, A'') = 0$, and by Lemma 4.13 $A'' = 0$. Thus the a_λ generate A as a G-module, and hence define a surjective $\mathbb{F}_p[G]$-homomorphism $\varphi : L \to A$ where L is a free $\mathbb{F}_p[G]$-module. Since $H_1(G, A) = 0$, there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & H_0(G, \ker\varphi) \arrow[r] & H_0(G, L) \arrow[r, "\beta"] & H_0(G, A) \arrow[r] & 0 \end{tikzcd}$$

By construction β is an isomorphism, so $H_0(G, \ker\varphi) = 0$ and hence $\ker\varphi = 0$ by Lemma 4.13. Thus $\varphi : L \to A$ is an isomorphism. □

Theorem 4.15. Let G be a p-group and A a G-module such that $pA = 0$. TFAE

(i) A is a free $\mathbb{F}_p[G]$ module.

(ii) A is an induced module.

(iii) A is cohomologically trivial.

(iv) $\hat{H}^q(G, A) = 0$ for some $q \in \mathbb{Z}$.

Proof. Clearly (i) ⇒ (ii) ⇒ (iii) ⇒ (iv). Now suppose (iv). By dimension shifting we construct a module B such that $pB = 0$ and $\hat{H}^n(G, A) = \hat{H}^{n-q-2}(G, B)$ for all n.

- $n = q$: Then $0 = \hat{H}^q(G, A) = \hat{H}^{-2}(G, B) = H_1(G, B)$. Thus B is free over $\mathbb{F}_p[G]$ by Lemma 4.14.

- $n = -2$: $H_1(G, A) = \hat{H}^{-2}(G, A) = \hat{H}^{-q-4}(G, B) = 0$, for B is free. Hence A is free over $\mathbb{F}_p[G]$ by Lemma 4.14.

□

Theorem 4.16. Let G be a p-group and A a G-module without p-torsion. TFAE:

(i) A is cohomologically trivial.

(ii) $\hat{H}^q(G, A) = \hat{H}^{q+1}(G, A) = 0$ for some $q \in \mathbb{Z}$.

(iii) A/pA is free over $\mathbb{F}_p[G]$.

Proof. (i) ⇒ (ii) is clear. Assume (ii). Consider the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "p"] & A \arrow[r] & A/pA \arrow[r] & 0 \end{tikzcd}$$

Passing to the cohomology gives the exact sequence

$$\begin{tikzcd} \hat{H}^q(G, A) \arrow[r] & \hat{H}^q(G, A) \arrow[r] & \hat{H}^q(G, A/pA) \arrow[r] & \hat{H}^{q+1}(G, A) \arrow[r] & \hat{H}^{q+1}(G, A) \end{tikzcd}$$

Then $\hat{H}^q(G, A/pA) = 0$, and thus A/pA is free over $\mathbb{F}_p[G]$ by Theorem 4.15 above. Finally, assume (iii). From the same exact sequence we see $\hat{H}^q(H, A) = 0$ for all q and all subgroups $H \leqslant G$ (note that A/pA is also $\mathbb{F}_p[H]$-free). □

Corollary 4.16.1. Let A be a G-module free over $\mathbb{Z}$ satisfying the equivalent conditions of Theorem 4.16. Then for any torsion-free G-module B, the G-module $N = \mathrm{Hom}_{\mathbb{Z}}(A, B)$ is cohomologically trivial.

Proof. Since A is free over $\mathbb{Z}$, the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r, "p"] & B \arrow[r] & B/pB \arrow[r] & 0 \end{tikzcd}$$

gives an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "p"] & N \arrow[r] & \mathrm{Hom}_{\mathbb{Z}}(A, B/pB) \arrow[r] & 0 \end{tikzcd}$$

so that N has no p-torsion point and $N/pN \cong \mathrm{Hom}_{\mathbb{Z}}(A, B/pB) = \mathrm{Hom}_{\mathbb{Z}}(A/pA, B/pB)$. Since A/pA is $\mathbb{F}_p[G]$-free, it is a direct sum of the $s.A'$, where $A' \leqslant A/pA$ is some subgroup. Hence N/pN is a direct sum of the $s.\mathrm{Hom}_{\mathbb{Z}}(A', B/pB)$, and hence N/pN is induced. That N is cohomologically trivial now follows from Theorem 4.15 and Theorem 4.16. □

Theorem 4.17. Let G be a finite group, A a G-module which is $\mathbb{Z}$-free, and G_p a Sylow p-subgroup of G. TFAE

(i) For each prime p, the G_p-module A satisfies the equivalent conditions of Theorem 4.16.

(ii) A is a projective G-module.

Proof. That (ii) $\Rightarrow$(i) is clear. Assume (i). Choose an exact sequence

$$0 \longrightarrow Q \longrightarrow G \longrightarrow A \longrightarrow 0$$

where F is a free G-module. Since A is $\mathbb{Z}$-free, this gives an exact sequence

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(A,Q) \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(A,F) \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(A,A) \longrightarrow 0$$

By Corollary 4.16.1 $\operatorname{Hom}_{\mathbb{Z}}(A,Q)$ is cohomologically trivial as a G_p-module for all p, and hence the group $H^1(G,\operatorname{Hom}_{\mathbb{Z}}(A,Q))$ is trivial by Corollary 4.3.4; it follows that $\operatorname{Hom}_G(A,F) \to \operatorname{Hom}_G(A,A)$ is surjective, and hence the identity map id_A extends to a G-homomorphism $A \to F$, i.e. A is G-projective. □

Theorem 4.18. Let A be any G-module. TFAE

(i) For each prime p, $\hat{H}^q(G_p,A) = 0$ for two consecutive values of q (which may depend on p).

(ii) A is cohomologically trivial.

(iii) There is an exact sequence $0 \to B_1 \to B_0 \to A \to 0$ in which B_0 and B_1 are G-projective.

Proof. That (iii) $\Rightarrow$(ii) $\Rightarrow$(i) is clear. Assume (i) and choose an exact sequence

$$0 \longrightarrow B_1 \longrightarrow B_0 \longrightarrow A \longrightarrow 0$$

with B_0 free over $\mathbb{Z}[G]$. Then $\hat{H}^q(G_p,B_1) \cong \hat{H}^{q-1}(G_p,A)$ for all q and all p, and hence the condition (i) holds for B_1. Since B_1 is a subgroup of B_0, B_1 is $\mathbb{Z}$-free. Therefore B_1 is G-projective by Theorem 4.17 □

4.11 Tate's Theorem

Theorem 4.19. Let G be a finite group, B and C two $G - modules$ and $f : B \to C$ a G-homomorphism. For each prime p, let G_p be a Sylow p-subgroup of G, and suppose that there exists an integer n_p such that

$$f_q^* : \hat{H}^q(G_p,B) \longrightarrow \hat{H}^q(G_p,C)$$

is surjective for $q = n_p$, bijective for $q = n_p + 1$ and injective for $q = n_p + 2$. Then for any subgroup $H \leqslant G$ and any integer q,

$$f_q^* : \hat{H}^q(G_p,B) \longrightarrow \hat{H}^q(G_p,C)$$

is an isomorphism.

Proof. Let $B^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], B)$ and let $i : B \to B^*$ be the injection defined by $i(b)(g) = gb$. Then $(f, i) : B \to C \oplus B^*$ is injective, so that we have an exact sequence

$$0 \longrightarrow B \longrightarrow C \oplus B^* \longrightarrow D \longrightarrow 0$$

Since B^* is cohomologically trivial, the cohomology of $C \oplus B^*$ is the same as that of C. Hence the cohomology sequence and the assumption imply $\hat{H}^q(G_p, D) = 0$ for $q = n_p$ and $q = n_p + 1$. It follows from Theorem 4.18 that D is cohomologically trivial, whence the result. □

Theorem 4.20. Let A, B, C be three G-modules and $\varphi : A \otimes B \to C$ a G-homomorphism. Let q be a fixed integer and a a given element of $\hat{H}^q(G, A)$. Assume that for each prime p there exists an integer n_p such that the map

$$\begin{aligned} \hat{H}^q(G_p, B) &\longrightarrow \hat{H}^q(G_p, C) \\ b &\longmapsto \varphi_q^*(\mathrm{res}_{G/G_p}(a) \cup b) \end{aligned}$$

is surjective for $q = n_p$, bijective for $q = n_p + 1$ and injective for $q = n_p + 2$. Then for all subgroups $H \leqslant G$ and all integers, the cup-product with $\mathrm{res}_{G/H}(a)$ induces an isomorphism

$$\begin{aligned} \hat{H}^n(H, B) &\longrightarrow \hat{H}^{n+q}(H, C) \\ b &\longmapsto \varphi_{n+q}^*(\mathrm{res}_{G/H}(a) \cup b) \end{aligned}$$

Proof. The case $q = 0$ is essentially Theorem 4.19. We have $a \in \hat{H}^0(G, A)$; choose $\alpha \in A^G$ representing a. Then α also represented $\mathrm{res}_{G/H}(a)$ for all $H \leqslant G$. Define

$$\begin{aligned} f : B &\longrightarrow C \\ \beta &\longmapsto \varphi(\alpha \otimes \beta) \end{aligned}$$

Since $\alpha \in A^G$, f is a G-homomorphism. We claim that for every $b \in \hat{H}^n(H, B)$

$$\varphi^*(\mathrm{res}_{G/H}(a) \cup b) = f^*(b) \in \hat{H}^n(H, C) \qquad (\spadesuit)$$

The $n = 0$ is just definition, and the general case follows from dimension shifting: for example, consider the commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & B' \arrow[r] \arrow[d, "f'"] & B_* \arrow[r] \arrow[d, "1\otimes f"] & B \arrow[r] \arrow[d, "f"] & 0 \\ 0 \arrow[r] & C' \arrow[r] & C_* \arrow[r] & C \arrow[r] & 0 \end{tikzcd} \qquad (\diamond)$$

where $B_* = \mathbb{Z}[G] \otimes B$ and $C_* = \mathbb{Z}[G] \otimes C$. Then we have the commutative diagram with horizontal arrows being isomorphisms

$$\begin{tikzcd} \hat{H}^n(H, B) \arrow[r, "\delta"] \arrow[d, "f^*"] & \hat{H}^{n+1}(H, B') \arrow[d, "f'^*"] \\ \hat{H}^n(H, C) \arrow[r, "\delta"] & \hat{H}^{n+1}(H, C') \end{tikzcd}$$

The diagram ($\diamond$) remains exact after tensoring with A over $\mathbb{Z}$; let $\varphi'' : A \otimes B' \to C'$ be the homomorphism induced by $\varphi : A \otimes B \to C$. Then by induction hypothesis

$$\begin{aligned} \delta(f^*(b)) &= f'^*\delta(b) = \varphi''^*(\mathrm{res}_{G/H}(a) \cup \delta(b)) \\ &= \varphi''^*\delta(\mathrm{res}_{G/H}(a) \cup b) \\ &= \delta\varphi^*(\mathrm{res}_{G/H}(a) \cup b) \end{aligned}$$

Since δ is an isomorphism, the result follows.

The general case $q \in \mathbb{Z}$ now follows by another piece of dimension shifting. For example, consider the exact sequence

$$0 \longrightarrow A' \longrightarrow A_* \longrightarrow A \longrightarrow 0$$

where $A_* = \mathbb{Z}[G] \otimes A$; this gives rise to isomorphisms $\delta : \hat{H}^q(H, A) \to \hat{H}q + 1(H, A')$. Let $u = \mathrm{res}_{G/H}(a) \in \hat{H}^q(H, A)$; then $u' = \delta u = \mathrm{res}_{G/H}(\delta a)$. Also $\varphi : A \otimes B \to C$ induces $\varphi' : A' \otimes B \to C'$. Consider the diagram

$$\begin{tikzcd} \hat{H}^n(H,B) \arrow[r, "u\cup"] \arrow[d, equal] & \hat{H}^{n+q}(H, A \otimes B) \arrow[r, "\varphi^*"] & \hat{H}^{n+q}(H, C) \arrow[d, "\delta"] \\ \hat{H}^n(H,B) \arrow[r, "u'\cup"] & \hat{H}^{n+q+1}(H, A' \otimes B) \arrow[r, "\varphi'^*"] & \hat{H}^{n+q+1}(H, C') \end{tikzcd}$$

which is commutative, for

$$\delta\varphi^*(u \cup b) = \varphi'^*\delta(u \cup b) = \varphi'^*(\delta(u) \cup b) = \varphi'^*(u' \cup b)$$

By induction hypothesis, the bottom line is an isomorphism, and since δ is an isomorphism, so is the top line. □

Theorem 4.21. Let A be a G-module and $a \in H^2(G, A)$. For each prime p, let G_p be a Sylow p-subgroup of G, and assume that

(i) $H^1(G_p, A) = 0$.

(ii) $H^2(G_p, A)$ is generated by $\mathrm{res}_{G/G_p}(a)$ and has order equal to that of G_p.

Then for all $H \leqslant G$ and all integers n, cupping with $\mathrm{res}_{G/H}(a)$ induces an isomorphism

$$\hat{H}^n(H, \mathbb{Z}) \longrightarrow \hat{H}^{n+2}(H, A)$$

Proof. Take $B = \mathbb{Z}$, $C = A$, $q = 2$, $n_p = -1$ in Theorem 4.20.

- $n = -1$. The surjectivity follows from (i).
- $n = 0$. $\hat{H}^0(G_p, \mathbb{Z})$ is cyclic of order $\#G_p$, so the bijectivity follows from (ii).
- $n = 1$. The injectivity follows from the fact that $\hat{H}^1(G_p, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G_p, \mathbb{Z}) = 0$.

Hence all the hypotheses of Theorem 4.20 are satisfied. □

Chapter 5

Local Class Field Theory

5.1 The Brauer Group of a Local Field

Let K be a local field and L a finite Galois extension of K. We write $H^2(L/K)$ instead of $H^2(\mathrm{Gal}(L/K), L^\times)$. By definition, the Brauer group $\mathrm{Br}(K)$ is the direct limit

$$\mathrm{Br}(K) := \varinjlim_{L/K:\text{ finite Galois}} H^2(L/K) = H^2(K^{\mathrm{sep}}/K).$$

In order to compute $\mathrm{Br}(K)$ we look first at the intermediate field K^{ur}, the maximal unramified extension of K. If k denotes the residue field of K, then the algebraic closure $\overline{k}$ of k is the residue field of K, and the reduction $\mathrm{Gal}(K^{\mathrm{ur}}/K) \to \mathrm{Gal}(\overline{k}/k)$ is an isomorphism. We denote by Frob_K the Frobenius element in $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ pulling back from the one on k. Then the map

$$\begin{tikzcd}
\widehat{\mathbb{Z}} \arrow[r] & \mathrm{Gal}(K^{\mathrm{ur}}/K) \\
\nu \arrow[r] & \mathrm{Frob}_k^\nu
\end{tikzcd}$$

is an isomorphism of topological groups.

Since K^{ur} is a subfield of K^{sep}, $H^2(K^{\mathrm{ur}}/K)$ is a subgroup of $\mathrm{Br}(K)$. In fact

Theorem 5.1. $\mathrm{Br}(K) = H^2(K^{\mathrm{ur}}/K) \cong H^2(\widehat{\mathbb{Z}}, (K^{\mathrm{ur}})^\times)$.

Theorem 5.2. The evaluation $\nu : (K^{\mathrm{ur}})^\times \to \mathbb{Z}$ defines an isomorphism

$$H^2(K^{\mathrm{ur}}/K) \to H^2(\widehat{\mathbb{Z}}, \mathbb{Z}).$$

5.1.1 Statements of Theorems

5.1.2 Computation of $H^2(K_{nr}/K)$

Proposition 5.3. Let K_n be an unramified extension of K of degree n and let $G = \mathrm{Gal}(K_n/K)$. Then for all $q \in \mathbb{Z}$ we have

(1) $H^q(G, U_n) = 0$, where $U_n = U_{K_n}$.

(2) the map $v : H^q(G, K_n^\times) \to H^q(G, \mathbb{Z})$ is an isomorphism.

5.1.3 Some Diagrams

5.1.4 Construction of a Subgroup with Trivial Cohomology

Let L/K be a finite Galois extension with Galois group G, where L and K are local fields. We already know that U_L has trivial cohomology when L/K is unramified.

Proposition 5.4. There exists an open subgroup V of U_L with trivial cohomology, that is, $H^q(G, V) = 0$ for all q.

Corollary 5.4.1. Let L/K be a cyclic extension of degree n. Then we have $h(U_L) = 1$ and $h(L^\times) = n$.

Corollary 5.4.2. Let L/K be a cyclic extension of degree n. Then $H^2(L/K)$ is of order $n = [L : K]$.

5.1.5 An Ugly Lemma

Lemma 5.5. Let G be a finite group and let M be a G-module and suppose that ρ, q are non-negative integers. Assume that

(a) $H^i(H, M) = 0$ for all $0 < i < q$ and all subgroups H of G;

(b) if $H \trianglelefteq K \leqslant G$ with K/H cyclic of prime order, then the order of $H^q(H, M)$ (resp. $\hat{H}^0(H, M)$ if $q = 0$) divides $[K : H]^\rho$.

Then the same is true of G. That is, $H^q(G, M)$ (resp. $\hat{H}^0(G, M)$) is of order dividing $[G : 1]^\rho$.

5.1.6 End of Proofs

5.1.7 An Auxiliary Results

Let A be an abelian group and let n be an integer $\geqslant 1$. Consider the cyclic group $\mathbb{Z}/n\mathbb{Z}$ with trivial action on A. We shall denote the corresponding Herbrand quotient by $h_n(A)$, whenever it is defined. We have

$$h_n(A) = \frac{\#(A/nA)}{\#\,{}_nA}$$

where ${}_nA$ is the set of $\alpha \in A$ such that $n\alpha = 0$. Alternatively, we could begin with the map $A \xrightarrow{n} A$ and take $h_n(A)$ to be

$$\frac{\#\operatorname{coker}(n)}{\#\ker(n)}$$

Now let K be a local field. Then for $\alpha \in K$ there is a normalized absolute value, denoted by $|\alpha|_K$. If $\alpha \in O_K$, then $|\alpha|_K = \dfrac{1}{\#(O_K/\alpha O_K)}$.

Proposition 5.6. Let K be a local field and let $n \geqslant 1$ be an integer prime to the characteristic of K. Then $h_n(K^\times) = \dfrac{n}{|n|_K}$.

5.2 Abelian Extension of Local Fields

5.2.1 Cohomological Properties

5.2.2 The Reciprocity Map

5.2.3 Characterization of $(\alpha, L/K)$ by Characters

Let L/K be a Galois extension with Galois group G. We start from an $\alpha \in K^\times$ and we seek a characterization of $(\alpha, L/K) \in G^{\mathrm{ab}}$. Let us set some notations.

- $s_\alpha := (\alpha, L/K)$.
- For $\chi \in \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$, let $\delta_\chi \in H^2(G, \mathbb{Z})$ be its image under the connecting homomorphism $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$.
- Let $\overline{\alpha} \in \hat{H}^0(G, L^\times) = K^\times / N_{L/K} L^\times$ be the image of α.

Proposition 5.7. $\chi(s_\alpha) = \mathrm{inv}_K(\overline{\alpha} \cup \delta_\chi)$.

Proof. Identifying s_α with an element of $\hat{H}^{-2}(G, \mathbb{Z})$, one has $s_\alpha \cup u_{L/K} = \overline{\alpha}$ by definition. Then

$$\overline{\alpha} \cup \delta_\chi = u_{L/K} \cup (s_\alpha \cup \delta_\chi) = u_{L/K} \cup \delta(s_\alpha \cup \chi) \overset{4.9}{=} u_{L/K} \cup \delta(\overline{\chi(s_\alpha)_0})$$

If $\chi(s_\alpha) = \dfrac{r}{n}$ for some $r \in \mathbb{Z}$, then $\delta(\overline{\chi(s_\alpha)_0}) = r$. Hence

$$u_{L/K} \cup \delta(\overline{\chi(s_\alpha)_0}) = u_{L/K} \cup r$$

and thus $\mathrm{inv}_K(\overline{\alpha} \cup \delta_\chi) = \mathrm{inv}_K(u_{L/K} \cup r) = \dfrac{r}{n} = \chi(s_\alpha)$ □

As an application we consider the following situation. Consider a tower of Galois extension $K \subseteq L' \subseteq L$ with $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/L')$.

Corollary 5.7.1. For $\alpha \in K^\times$, we have $(\alpha, L/K)|_{L'} = (\alpha, L'/K) \in (G/H)^{\mathrm{ab}}$.

Proof. Let $\psi \in \mathrm{Hom}((G/H)^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z})$ and put $\chi = \inf_{G/H} \psi$. Then

$$\begin{aligned}
\psi((\alpha, L/K)|_{L'}) &= \chi((\alpha, L/K)) \\
&= \mathrm{inv}_K(\overline{\alpha} \cup \delta_\chi) \\
&= \mathrm{inv}_K(\overline{\alpha} \cup \inf_{G/H} \delta_\psi) \\
&= \mathrm{inv}_K(\inf_{G/H}(\overline{\alpha} \cup \delta_\psi)) \\
&= \mathrm{inv}_K(\overline{\alpha} \cup \delta_\psi) = \psi((\alpha, L'/K))
\end{aligned}$$

The second last equality results from the very definition of Brauer group (inf is the inclusion map).

□

This compatibility allows us to define $(\alpha, L/K)$ for any abelian extension; in particular, taking $L = K^{\mathrm{ab}}$, the maximal abelian extension of K, we get a homomorphism

$$\begin{aligned} \theta_K : K^\times &\longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \alpha &\longmapsto (\alpha, K^{\mathrm{ab}}/K) \end{aligned}$$

The effect of $(\alpha, K^{\mathrm{ab}}/K)$ on $K \subseteq L \subseteq K^{\mathrm{ab}}$ is then that of $(\alpha, K^{\mathrm{ab}}/K)|_L := (\alpha, L/K)$.

5.2.4 Variations with the Field Involved

5.2.5 Unramified Extensions

In this case it is possible to compute the norm residue symbol explicitly in terms of the Frobenius elements:

Proposition 5.8. Let L/K be an unramified extension of degree n and let normalized valuation. Let $\alpha \in K^\times$ and let $\nu(a) \in \mathbb{Z}$ be its normalized valuation. Then $(\alpha, L/K) = F^{\nu(\alpha)}$.

Proof. Let $\chi \in \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$. Then

$$\chi((\alpha, L/K)) = \mathrm{inv}_K(\overline{\alpha} \cup \delta_\chi).$$

The map $\mathrm{inv}_K : H^2(\mathrm{Gal}(L/K), L^\times) \to \mathbb{Q}/\mathbb{Z}$ has been defined as a composition

$$H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\nu} H^2(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z}.$$

Hence

$$\mathrm{inv}_K(\overline{\alpha} \cup \delta_\chi) = \gamma \circ \delta^{-1} \circ \nu(\overline{\alpha} \cup \delta_\chi)$$

□

Corollary 5.8.1. Let E/K be a finite abelian extension. The norm residue symbol $K^\times \to \mathrm{Gal}(E/K)$ maps U_K onto the inertia subgroup $I := I_{E/K}$ of $G_{E/K}$.

Proof. Put $E_0 = E^I$; then E_0/K unramified. By Proposition 5.8, U_K has trivial image in $\mathrm{Gal}(E_0/K)$ so that it is mapped into $\mathrm{Gal}(E/L) = I \subseteq \mathrm{Gal}(E/K)$. Conversely, let $t \in I$ and let $f = [E_0 : K]$. There exists $a \in K^\times$ such that $t = (a, E/K)$. Since $t \in I$, Proposition 5.8 shows $1 = (a, E/K)|_{E_0} = \mathrm{Frob}_{E_0/K}^{\nu_K(a)}$, so that $f \mid \nu_K(a)$. Considering the ramification, one see there exists $b \in E^\times$ such that $\nu_K(a) = \nu_K(Nb)$. If we put $u = a(Nb)^{-1}$, we have $u \in U_K$ and $(u, E/K) = (a, E/K) = t$. □

5.2.6 Norm Subgroups

5.2.7 Statements of the Existence Theorem

Theorem 5.9. A subgroup M of $K^\times$ is a norm subgroup if and only if it satisfies the following two conditions

(1) The index $[K^\times : M]$ is finite.

(2) M is open in $K^\times$.

We give now some equivalent formulations.

Consider the reciprocity map $\theta_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. By Proposition 5.8, the composition

$$K^\times \xrightarrow{\theta_K} \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow \mathrm{Gal}(K_{\mathrm{nr}}/K) = \widehat{\mathbb{Z}}$$

is just the valuation map $\nu : K^\times \to \mathbb{Z}$. Hence we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & U_K \arrow[r] \arrow[d, "\theta"] & K^\times \arrow[r] \arrow[d, "\theta"] & \mathbb{Z} \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & I_K \arrow[r] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[r] & \widehat{\mathbb{Z}} \arrow[r] & 0
\end{tikzcd}$$

where $I_K = \mathrm{Gal}(K^{\mathrm{ab}}/K_{\mathrm{nr}})$ is the **inertia group** of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

The map $\theta : U_K \to I_K$ is continuous, and its image is dense by Corollary 5.8.1; since U_K is compact, it follows that θ is surjective.

We can now state two equivalent formulations of the existence theorem.

Theorem A The map $\theta : U_K \to I_K$ is an isomorphism.

Theorem B The topology induced on U_K by the norm subgroups is the natural topology on U_K.

The group I_K is just $\varprojlim U_K/(M \cap U_K)$, where M runs over all norm subgroups of $K^\times$ (if $M = NL^\times$, then $U_K/(M \cap U_K) = I_{L/K}$ is the inertia group of L/K, by Corollary 5.8.1). The equivalence of Theorem A and Theorem B follows from this and a compacity argument. That Theorem 5.9 implies Theorem B is clear. The converse follows from Proposition 5.8.

Corollary 5.9.1. The exact sequence $0 \to U_K \to K^\times \to \mathbb{Z}$ gives by completion the exact sequence $0 \to U_K \to \tilde{K} \to \widehat{\mathbb{Z}} \to 0$.

5.2.8 Some Characterization of $(\alpha, L/K)$

5.2.9 The Archimedean Case

For the global class field theory, it is necessary to extend these results to the (trivial) cases in which K is either $\mathbb{R}$ or $\mathbb{C}$. Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. We have $\mathrm{Br}(\mathbb{C}) = 0$ and $\mathrm{Br}(\mathbb{R}) = H^2(G, \mathbb{C}^\times) = \mathbb{R}^\times/\mathbb{R}^\times_+$.

The invariant $\text{inv}_{\mathbb{R}} : \text{Br}(\mathbb{R}) \to \mathbb{Q}/\mathbb{Z}$ has image $\{0, 1/2\} \subseteq \mathbb{Q}/\mathbb{Z}$, and $\text{inv}_{\mathbb{C}} : \text{Br}(\mathbb{C}) \to \mathbb{Q}/\mathbb{Z}$ has image $\{0\}$. The group $H^2(G, \mathbb{C}^\times) = H^2(\mathbb{C}/\mathbb{R})$ is cyclic of order 2 and is generated by $u \in \text{Br}(\mathbb{R})$ such that $\text{inv}_{\mathbb{R}}(u) = 1/2$.

Under the reciprocity law map (or rather its inverse) we have an isomorphism

$$G = H^{-2}(G, \mathbb{Z}) \longrightarrow H^0(G, \mathbb{C}^\times) = \mathbb{R}^\times/\mathbb{R}_+^\times$$

5.3 Formal Multiplication in Local Fields

For our purposes, the main consequence will be

1. the construction of a cofinal system of abelian extension of a given local field K;

2. a formula giving $(\alpha, L/K)$ explicitly in such extensions;

3. the Existence Theorem.

5.3.1 The Case $K = \mathbb{Q}_p$

Theorem 5.10. Let $\mathbb{Q}_p^{\text{cycl}}$ be the field generated over $\mathbb{Q}_p$ by all roots of unity. Then $\mathbb{Q}_p^{\text{cycl}}$ is the maximal abelian extension of $\mathbb{Q}_p$.

In order to determine $(\alpha, L/K)$ it is convenient to split $\mathbb{Q}_p^{\text{cycl}}$ into parts. Define $\mathbb{Q}_{\text{nr}}$ to be the field generated over $\mathbb{Q}_p$ by roots of unity of order prime to p (so $\mathbb{Q}_{\text{nr}}$ is the maximal unramified extension of $\mathbb{Q}_p$) and define $\mathbb{Q}_{p^\infty}$ to be the field generated over $\mathbb{Q}_p$ by p^v-th roots of unity, $v = 1, 2, \ldots,$ (so $\mathbb{Q}_{p^\infty}$ is totally ramified). Then $\mathbb{Q}_{\text{nr}}$ and $\mathbb{Q}_{p^\infty}$ are linearly disjoint we have a diagram

$$\begin{tikzcd}
& Q_p^{\text{cycl}} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}_{\text{nr}} \arrow[dr, dash] & & \mathbb{Q}_{p^\infty} \arrow[dl, dash] \\
& \mathbb{Q}_p &
\end{tikzcd}$$

Now $\text{Gal}(\mathbb{Q}_{\text{nr}}) = \widehat{\mathbb{Z}}$ and if $\sigma \in \text{Gal}(\mathbb{Q}_{p^\infty}/\mathbb{Q}_p)$, then σ is known by its action on the roots of unity. Let E be the group of p^v-th roots of unity, $v = 1, 2, \ldots, $. As an abelian group, E is isomorphic to $\varinjlim_v \mathbb{Z}/p^v\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p$. We shall view E as a $\mathbb{Z}_p$-module. There is a canonical map $\mathbb{Z}_p \to \text{End}(E)$, defined in an obviously way and this map is an isomorphism. The action of the Galois group on E defines a homomorphism

$$\text{Gal}(\mathbb{Q}_{p^\infty}/\mathbb{Q}_p) \longrightarrow \text{Aut}(E) = U_p$$

and it is known that this is an isomorphism. If $u \in U_p$, we shall denote by $[u]$ the corresponding automorphism of $\mathbb{Q}_{p^\infty}/\mathbb{Q}_p$.

Theorem 5.11. If $\alpha = p^n u$ where $u \in U_p$, then $(\alpha, \mathbb{Q}_p^{\text{cycl}}/\mathbb{Q}_p) = \sigma_\alpha$ is described by

1. on $\mathbb{Q}_{\text{nr}}$, σ_α induces the n-th power of the Frobenius automorphisms;
2. on $\mathbb{Q}_{p^\infty}$, σ_α induces the automorphism $[u^{-1}]$.

5.3.2 Formal Groups

Definition. Let A be a commutative ring with 1 and let $F \in A[\![X, Y]\!]$. We say F is a **commutative formal group law** if

(a) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;

(b) $F(0, Y) = Y$ and $F(X, 0) = X$;

(c) there is a unique $G(X)$ such that $F(X, G(X)) = 0$;

(d) $F(X, Y) = F(Y, X)$;

(e) $F(X, Y) \equiv X + Y \pmod{\deg 2}$

- One can show that (c) and (b) are consequences of (a) and (e).

  Proof. Write $F(X, Y) = X + Y + \sum_{i,j \geqslant 1} a_{ij} X^i Y^j$. We prove by induction that $a_{0j} = 0 = a_{j0}$ for $j \geqslant 2$. Write $F(0, Y) \equiv Y + a_{0m} Y^m \pmod{\deg m+1}$ and $F(X, 0) \equiv X + a_{m0} X^m \pmod{\deg m+1}$ By (a) one has

  $$F(F(X, 0), Y) = F(X, F(0, Y))$$

  so that

  $$F(X, 0) + Y + \sum_{i,j \geqslant 1} a_{ij} F(X, 0)^i Y^j = X + F(0, Y) + \sum_{i,j \geqslant 1} a_{ij} X^i F(0, Y)^j$$

  Then

  $$X + a_{m0} X^m + Y + \sum_{i,j \geqslant 1} a_{ij} X^j Y^j \equiv X + Y + a_{0m} Y^m + \sum_{i,j \geqslant 1} X^i Y^j \pmod{\deg m+1}$$

  from which we see $a_{m0} = a_{0m}$. This shows (b). Suppose $G(X) = \sum_{k=0}^{\infty} b_k X^k$ verifies $F(X, G(X)) = 0$. A computation gives

  $$0 = F(X, G(X)) = \sum_{m=0}^{\infty} \left(\sum_{\ell=0}^{m} \sum_{\substack{j \geqslant 0 \\ k_1 + \cdots + k_j = m - \ell \\ 0 \leqslant k_1, \ldots, k_j}} a_{\ell j} b_{k_1} \cdots b_{k_j} \binom{m - \ell}{k_1 \cdots k_j} \right) X^m$$

  Each coefficient has the form $b_m + c_m$ by (b), where c_m involves no b_m. Thus we can solve the b_m inductively. □

Definition. Let F, G be two formal group law over a commutative ring A with 1. A **homomorphism** $f : F \to G$ between two formal groups is a formal power series $f \in A[\![X]\!]$ such that $f(F(X, Y)) = G(f(X), f(Y))$.

Take $A = O_K$, and let $F(X, Y)$ be a commutative formal group law defined over O_K. If $\mathfrak{m}_K$ is the maximal ideal of O_K and $x, y \in \mathfrak{m}_K$, then $F(x, y)$ converges and it sum belongs to O_K; then $\mathfrak{m}_K$ is made into a group via F which we denote by $F(\mathfrak{m}_K)$.

The same argument applies to an extension L/K and the maximal ideal $\mathfrak{m}_L$ of O_L. We then obtain a group $F(\mathfrak{m}_L)$ defined for any algebraic extension of K by passage to inductive limit from the finite case.

If $F(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1$, then we recover the multiplicative group law of $1 + \mathfrak{m}_K$.

The elements of finite order of $F(\mathfrak{m}_{K_s})$ form a torsion group and $\mathrm{Gal}(K_s/K)$ operates on this group. The structure of this Galois module presents an interesting problem which up to now has been solved only in special case.

5.3.3 Lubin-Tate Formal Group Laws

Let K be a local field, $q = \mathrm{Char}(k)$ and choose a uniformizer $\pi \in O_K$. Let $\mathfrak{F}_\pi$ be the set of formal power series f with:

(1) $f(X) \equiv \pi X \pmod{\deg 2}$;

(2) $f(X) \equiv X^q \pmod{\pi}$

The second condition means that if we go to the residue field k and denote by $\overline{f}(X)$ the corresponding element of $k[\![X]\!]$, then $\overline{f}(X) = X^q$.

Example.

(a) $f(X) = \pi X + X^q$.

(b) $K = \mathbb{Q}_p$, $\pi = p$, $f(X) = \sum_{i=1}^{p} \binom{p}{i} X^i = (1 + X)^p - 1$.

Proposition 5.12. Let $f \in \mathfrak{F}_\pi$. Then there exists a unique formal group law F_f with coefficients in A for which f is an endomorphism on F_f.

Proposition 5.13. Let $f \in \mathfrak{F}_\pi$ and let F_f be the corresponding group law in the above proposition. Then for any $a \in A = O_K$, there exists a unique $[a]_f \in A[\![A]\!]$ such that

(1) $[a]_f$ commutes with f;

(2) $[a]_f \equiv aX \pmod{\deg 2}$

Moreover, $[a]_f$ is then an endomorphism of the group law F_f.

From the above proposition we obtain a mapping

$$\begin{aligned} A &\longrightarrow \mathrm{End}(F_f) \\ a &\longmapsto [a]_f \end{aligned}$$

For example, consider the case $K = \mathbb{Q}_p$ and $f(X) = (1 + X)^p - 1$; then F_f is the multiplicative law $X + Y + XY$, and

$$[a]_f = (1 + X)^a - 1 := \sum_{i=1}^{\infty} \binom{a}{i} X^i$$

Proposition 5.14. The map $a \mapsto [a]_f$ is an injective ring homomorphism from A to $\mathrm{End}(F_f)$.

Proposition 5.15. Let $f, g \in \mathfrak{F}_\pi$. Then the corresponding group laws are isomorphic.

5.3.4 Statements

Let K be a local field and let π be a uniformizer. Let $f \in \mathfrak{F}_\pi$ and let F_f be the corresponding group law (of Proposition 5.12). We denote by $M_f = F_f(\mathfrak{m}_{K_s})$ the group of points is the separable closure equipped with the group law deduced from F. Let $a \in A$, $x \in M_f$ and put $ax := [a]_f x$. By Proposition 5.14, this defines a structure of an A-module on M_f. Let E_f be the torsion submodule of M_f; that is the set of elements of M_f killed by a power of π.

Theorem 5.16. The following statements hold.

1. The torsion submodule E_f is A-isomorphic to K/A.
2. Let $K_\pi = K(E_f)$ be the field generated by E_f over K. Then K_π is an abelian extension of K.
3. Let u be a unit in $K^\times$. Then the element $\sigma_u = (u, K_\pi/K)$ of $\mathrm{Gal}(K_\pi/K)$ acts on E_f via $[u^{-1}]_f$.
4. The operation described in (c) defined an isomorphism $U_K \to \mathrm{Gal}(K_\pi/K)$.
5. The norm residue symbol $(\pi, K_\pi/K)$ is 1.
6. The field K_{nr} and K_π are linearly disjoint and $K^{\mathrm{ab}} = K_{\mathrm{nr}} K_\pi$.

We may express the results of Theorem 5.16 as follows. We have diagram

$$\begin{tikzcd} & K^{\mathrm{ab}} \arrow[dl, dash] \arrow[dr, dash] & \\ K_{\mathrm{nr}} \arrow[dr, dash] & & K_\pi \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Here $\mathrm{Gal}(K_{\mathrm{nr}}/K) = \widehat{\mathbb{Z}}$ and $\mathrm{Gal}(K_\pi/K) = U_K$. Moreover every $\alpha \in K^\times$ can be written in the form $\alpha = u\pi^n$, and σ_π gives $\sigma = \mathrm{Frob}_K$ on K_{nr}/K whilst σ_u gives $[u^{-1}]$ on K_π/K.

Example. Take $K = \mathbb{Q}_p$, $\pi = p$ and $f(X) = (1+X)^p - 1$. The formal group law is the multiplicative group law; E_f is the set of p^ν-th roots of unity; K_π is the field denoted by $\mathbb{Q}_{p^\infty}$ in subsection 1, and we recover Theorem 5.10.

5.3.5 Construction of F_f, $[a]_f$

Proposition 5.17. Let $f, g \in \mathfrak{F}_\pi$, $n \in \mathbb{N}$ and let $\phi_1(X_1, \ldots, X_n)$ be a linear form in $X_1, \ldots, X_n$ with coefficients in A. Then there exists a unique $\phi \in A[\![X_1, \ldots, X_n]\!]$ such that

(i) $\phi \equiv \phi_1 \pmod{\deg 2}$;

(ii) $f \circ \phi = \phi \circ (g \times \cdots \times g)$.

Moreover, ϕ is the only power series with coefficients in an extension of A, which is torsion free as an A-module, satisfying (a) and (b).

Proof. We shall construct ϕ be successive approximation. More precisely, we construct a sequence $(\phi^{(p)})$ such that $\phi^{(p)} \in A[\![X_1, \ldots, X_n]\!]$ satisfies (a) and (b) $\pmod{\deg p+1}$, and $\phi^{(p)}$ is unique $\pmod{\deg p+1}$. We shall then define $\phi := \lim_p \phi^{(p)}$, and this will be the ϕ whose existence is asserted.

Take $\phi^{(1)} = \phi_1$. Suppose that the approximation $\phi_1 + \cdots + \phi_p = \phi^{(p)}$ has been constructed, that is, $f \circ \phi^{(p)} \equiv \phi^{(p)} \circ (g \times \cdots \times g) \pmod{\deg p+1}$. For convenience, we shall replace $g \times \cdots \times g$ by the single variable g. Now write $\phi^{(p+1)} = \phi^{(p)} + \phi_{p+1}$, where ϕ_{p+1} is to be determined with $\phi_{p+1} \equiv 0 \pmod{\deg p+1}$. Write

$$f \circ \phi^{(p)} \equiv \phi^{(p)} \circ g + E_{p+1} \pmod{\deg p+2}$$

where E_{p+1} ("the error") satisfies $E_{p+1} \equiv 0 \pmod{\deg p+1}$. Consider $\phi^{(p+1)}$; by Taylor's expansion we have

$$f \circ \phi^{(p+1)} = f \circ (\phi^{(p)} + \phi_{p+1}) \equiv f \circ \phi^{(p)} + \pi\phi_{p+1} \pmod{\deg p+2}$$

(recall $f(X) \equiv \pi X \pmod{\deg 2}$) and

$$\phi^{(p)} \circ g + \phi_{p+1} \circ g \equiv \phi^{(p)} \circ g + \pi^{p+1}\phi_{p+1} \pmod{\deg p+2}$$

Thus

$$f \circ \phi^{(p+1)} - \phi^{(p+1)} \circ g \equiv E_{p+1} + (\pi - \pi^{p+1})\phi_{p+1} \pmod{\deg p+2}$$

These equations show that we must take

$$\phi_{p+1} = \frac{-E_{p+1}}{\pi(1-\pi^p)}$$

The unicity is now clear and it remains to show that ϕ_{p+1} has coefficients in A, that is, $E_{p+1} \equiv 0 \pmod{\pi}$. Now for $\phi \in \mathbb{F}_q[\![X]\!]$, we have $\phi(X^q) = \phi(X)^q$ and together with $f(X) \equiv X^q \pmod{\pi}$ this gives

$$f \circ \phi^{(p)} - \phi^{(p)} \circ g \equiv (\phi^{(p)}(X))^q - \phi^{(p)}(X^q) \equiv 0 \pmod{\pi}$$

as wanted. So, given $\phi^{(p)}$ we can construct a unique $\phi^{(p+1)}$ and the proof is completed by induction and passage to the limit. □

Proof. (of Proposition 5.12) For each $f \in \mathfrak{F}_\pi$, let $F_f(X,Y)$ be the unique solution of $F_f(X,Y) \equiv X+Y \pmod{\deg 2}$ and $f \circ F_f = F_f \circ (f \times f)$ whose existence and uniqueness is assured by Proposition 5.17. It remains to show that F_f is a formal group law.

- Associativity. Note that both

  $$F_f(F_f(X,Y),Z) \text{ and } F_f(X,F_f(Y,Z))$$

  are solutions to $H(X,Y,Z) \equiv X+Y+Z \pmod{\deg 2}$ and $H(f(X),f(Y),f(Z)) = f(H(X,Y,Z))$, so by unicity part in Proposition 5.17, both expressions are identical.

- Commutativity. $F(X,Y)$ and $F(Y,X)$ are solutions to $H \circ (f \times f) = f \circ H$ and $H(X,Y) \equiv X+Y \pmod{\deg 2}$.

□

Proof. (of Proposition 5.13) For each $a \in A$ and $f,g \in \mathfrak{F}_\pi$, let $[a]_{f,g}(T)$ be the unique solution to $[a]_{f,g}(T) \equiv aT \pmod{\deg 2}$ and $f \circ [a]_{f,g} = [a]_{f,g} \circ g$. Now we have

$$F_f \circ ([a]_{f,g} \times [a]_{f,g}) = [a]_{f,g} \circ F_g$$

for each side is congruent to $aX + aY \pmod{\deg 2}$ and

$$F_f([a]_{f,g}g(X),[a]_{f,g}g(Y)) = F_f(f([a]_{f,g}(X)),f([a]_{f,g}(Y))) = f(F_f([a]_{f,g}(X),[a]_{f,g}(Y)))$$

and

$$[a]_{f,g}F_g(g(X),g(Y)) = [a]_{f,g}(g(F_g(X,Y))) = f([a]_{f,g}F_g(X,Y))$$

so that by Proposition 5.17 the both sides coincide. Thus $[a]_{f,g} : F_g \to F_f$ is a formal homomorphism, and if we put $[a]_f = [a]_{f,g}$, this shows that $[a]_f \in \mathrm{End}(F_f)$. □

Proof. (of Proposition 5.14) In the same way as outlined above, one proves that

$$[a+b]_{f,g} = F_f \circ ([a]_{f,g} \circ [a]_{f,g})$$

and

$$[ab]_{f,h} = [a]_{f,g} \circ [b]_{g,h}$$

This shows $a \mapsto [a]_f$ is a ring homomorphism from A into $\mathrm{End}(F_f)$. It is injective since the term of degree 1 of $[a]_f$ is aX. □

Proof. (of Proposition 5.15) If $a \in A^\times$, then $[a]_{f,g}$ is invertible, so $F_g \cong F_f$ by means of the isomorphism $[a]_{f,g}$. Note that $[\pi]_f = f$ and $[1]_f$ is the identity. □

5.3.6 First Properties of the Extension K_π of K

From now on, we confine our attention to subfields of a fixed separable closure K_s of K. Given $f \in \mathfrak{F}_\pi$, let

- F_f: the corresponding formal group law;
- E_f: the torsion submodule of the A-module $F_f(\mathfrak{m}_K)$;
- $E_f^n := \ker[\pi^n]_f$, $K_\pi^n := K(E_f^n)$ and $K_\pi = \bigcup_{n \geqslant 1} K_\pi^n$.
- $G_{\pi,n} := \mathrm{Gal}(K(E_f^n)/K)$, so that $\mathrm{Gal}(K_\pi/K) = \varprojlim_n G_{\pi,n}$

Proposition 5.18. The natural homomorphism $\mathrm{Gal}(K_\pi/K) \to U_K$ is an isomorphism.

Proof. We are free to choose f as we please by Proposition 5.15; take $f = \pi X + X^q$. Then

$$f^{(n)} := \underbrace{f \circ \cdots \circ f}_{n\text{-times}} = [\pi^n]_f$$

Since $f^{(n)}$ is separable, $\# E_f^n = \# \ker[\pi^n]_f = q^n$. Pick $\lambda \in E_f^n \backslash E_f^{n-1}$ and consider the map

$$\begin{aligned} A &\longrightarrow E_f^n \\ a &\longmapsto a\lambda \end{aligned}$$

it has kernel $A/\pi^n A$, and thus induces an injection $A/\pi^n A \to E_f^n$. Since both sides have order q^n, it follows that $A/\pi^n \cong E_f^n$. Then

$$\mathrm{End}(E_f^n) \cong \mathrm{End}(A/\pi^n A) = A/\pi^n A$$

and so

$$\mathrm{Aut}(E_f^n) \cong (A/\pi^n A)^\times = U_K/U_K^n$$

where $U_K^n = 1 + \pi^n A$. This gives an injection $\mathrm{Gal}(K_\pi^n/K) \to \mathrm{Aut}(E_f^n) = U_K/U_K^n$. Define

$$\phi = \frac{f^{(n)}}{f^{(n-1)}} = \frac{f(f^{(n-1)})}{f^{(n-1)}}$$

Since $f(X) = X^q + \pi X$, $\dfrac{f(X)}{X} = X^{q-1} + \pi$ and hence

$$\frac{f(f^{(n-1)})}{f^{(n-1)}} = (f^{(n-1)}(X))^{q-1} + \pi$$

which is of degree $q^n - q^{n-1}$ and which is irreducible for it is Eisenstein. All elements of $E_f^n \backslash E_f^{n-1}$ are roots of ϕ, so the order $\# \mathrm{Gal}(K_\pi^n/K) \geqslant (q-1)q^{n-1}$. On the order hand, this is actually the order of U_K/U_K^n, hence $\mathrm{Gal}(K_\pi^n/K) = U_K/U_K^n$. It follows that

$$\mathrm{Gal}(K_\pi/K) = \varprojlim_n \mathrm{Gal}(K_\pi^n/K) = \varprojlim_n U_K/U_K^n = U_K$$

□

Corollary 5.18.1. $K(E_f^n)/K$ is totally ramified.

Proof. We have seen, in the proof above, that ϕ is Eisenstein, so that $K(E_f^n)/K$ is totally ramified. □

Corollary 5.18.2. The element π is a norm from $K(\lambda) = K_\pi^n$, where $\lambda \in E_f^n \backslash E_f^{n-1}$ is a primitive element.

Proof. The polynomial ϕ constructed above is monic with constant term π; hence $N_{K_\pi^n/K}(-\lambda) = \pi$. □

5.3.7 The Reciprocity Map

We shall study the compositum $L = K_{\text{nr}}K_\pi$ and the symbol $(\alpha, L/K)$, $\alpha \in K^\times$. We need to compare two uniformizers π and $\varpi = \pi u$, $u \in U_K$.

Let $\widehat{K}_{\text{nr}}$ be the completion of K_{nr} (remember that K_{nr} is an increasing union of complete fields but is not itself complete) and denote by $\widehat{A}_{\text{nr}}$ and $\widehat{\mathfrak{m}}_{\text{nr}}$ the ring of integers of $\widehat{K}_{\text{nr}}$ and the valuation ideal. By definition $\widehat{K}_{\text{nr}}$ is complete; π is a uniformizer of $\widehat{K}_{\text{nr}}$. Let $\sigma = \text{Frob}_K \in \text{Gal}(K_{\text{nr}}/K)$ and extend it to $\widehat{K}_{\text{nr}}$ by continuity.

Lemma 5.19.

(i) $\sigma - 1 : \widehat{A}_{\text{nr}} \to \widehat{A}_{\text{nr}}$ is surjective with kernel A.

(ii) $\sigma - 1 : \widehat{U}_{\text{nr}} \to \widehat{U}_{\text{nr}}$ is surjective with kernel $A^\times$.

Proof. Let A_{nr} be the ring of integers of K_{nr} and $\mathfrak{m}_{\text{nr}}$ the maximal ideal; then $\widehat{A}_{\text{nr}} = \varprojlim_n A_{\text{nr}}/\mathfrak{m}_{\text{nr}}^n$ and $\widehat{A}_{\text{nr}}/\widehat{\mathfrak{m}}_{\text{nr}} = A_{\text{nr}}/\mathfrak{m}_{\text{nr}} = \overline{k}$, where k is the residue field $A/\mathfrak{m}_K$ and $\overline{k}$ is its separable closure. We prove by induction that for each $n \geqslant 1$ there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & A/\mathfrak{m}_K^n \arrow[r] & A_{\text{nr}}/\mathfrak{m}_{\text{nr}}^n \arrow[r, "\sigma-1"] & A_{\text{nr}}/\mathfrak{m}_{\text{nr}}^n \arrow[r] & 0 \end{tikzcd}$$

For $n = 1$, it is simply the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & k \arrow[r] & \overline{k} \arrow[r, "\sigma-1"] & \overline{k} \arrow[r] & 0 \end{tikzcd}$$

(recall that $\text{Gal}(K_{\text{nr}}/K)$ is generated by $\sigma = \text{Frob}_K$.) For $n \geqslant 2$ consider the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & A_{\text{nr}}/\mathfrak{m}_{\text{nr}} \arrow[r] \arrow[d, "\sigma-1"] & A_{\text{nr}}/\mathfrak{m}_{\text{nr}}^n \arrow[r] \arrow[d, "\sigma-1"] & A_{\text{nr}}/\mathfrak{m}_{\text{nr}}^{n-1} \arrow[r] \arrow[d, "\sigma-1"] & 0 \\ 0 \arrow[r] & A_{\text{nr}}/\mathfrak{m}_{\text{nr}} \arrow[r] & A_{\text{nr}}/\mathfrak{m}_{\text{nr}}^n \arrow[r] & A_{\text{nr}}/\mathfrak{m}_{\text{nr}}^{n-1} \arrow[r] & 0 \end{tikzcd}$$

By induction hypothesis and snake's lemma we see the middle arrow is surjective and its kernel has order q^n. Since $A/\mathfrak{m}_K^n$ is contained in the kernel and it has order q^n as well, it is the whole kernel. This finishes the induction and passing to the inverse limit, we obtain (i).

For (ii), note that $\widehat{U}_{\mathrm{nr}} = \varprojlim_n U_{\mathrm{nr}}/U_{\mathrm{nr}}^n$, where $U_{\mathrm{nr}}^n = 1 + \mathfrak{m}_{\mathrm{nr}}^n$. Similar to the argument above, we show there is an exact sequence

$$0 \longrightarrow U_K/U_K^n \longrightarrow U_{\mathrm{nr}}/U_{\mathrm{nr}}^n \xrightarrow{\sigma-1} U_{\mathrm{nr}}/U_{\mathrm{nr}}^n \longrightarrow 0$$

When $n = 1$, since $U_K/U_K^1 \cong k^\times$ under the quotient map $A \to A/\mathfrak{m}_K = k$ (and the same for U_{nr}), the complex becomes

$$0 \longrightarrow k^\times \longrightarrow \overline{k}^\times \xrightarrow{\sigma-1} \overline{k}^\times \longrightarrow 0$$

which is clearly exact. The case for $n \geqslant 2$, consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & U_{\mathrm{nr}}^{n-1}/U_{\mathrm{nr}}^n \arrow[r] \arrow[d, "\sigma-1"] & U_{\mathrm{nr}}/U_{\mathrm{nr}}^n \arrow[r] \arrow[d, "\sigma-1"] & U_{\mathrm{nr}}/U_{\mathrm{nr}}^{n-1} \arrow[r] \arrow[d, "\sigma-1"] & 0 \\
0 \arrow[r] & U_{\mathrm{nr}}^{n-1}/U_{\mathrm{nr}}^n \arrow[r] & U_{\mathrm{nr}}/U_{\mathrm{nr}}^n \arrow[r] & U_{\mathrm{nr}}/U_{\mathrm{nr}}^{n-1} \arrow[r] & 0
\end{tikzcd}$$

The isomorphism $U_{\mathrm{nr}}^{n-1}/U_{\mathrm{nr}}^n \cong \overline{k}$ is σ-invariant (note that $\pi \in K$), so the leftmost vertical arrow, under the mentioned isomorphism, becomes $\overline{k} \overset{\sigma-1}{\to} \overline{k}$, which is surjective and its kernel has order q. Now by snake's lemma the middle arrow is surjective whose kernel has order $q^{n-1}(q-1)$. Since U_K/U_K^n lies in the kernel and it has order exactly $q^{n-1}(q-1)$, it follows it is the whole kernel. The proof is finished by passing to the limit. □

Take $f \in \mathfrak{F}_\pi$ and $g \in \mathfrak{F}_\varpi$.

Lemma 5.20. There exists a power series $\phi \in \widehat{A}_{\mathrm{nr}}[\![X]\!]$ with $\phi(X) \equiv \varepsilon X \pmod{\deg 2}$ and ε a unit, such that

(a) ${}^\sigma\phi = \phi \circ [u]_f$;

(b) $\phi \circ F_f = F_g \circ (\phi \times \phi)$;

(c) $\phi \circ [a]_f = [a]_f \circ \phi$ for all $a \in A$.

Proof. For $\psi \in \widehat{A}_{\mathrm{nr}}[\![X]\!]$, denote by $\psi^{-1} \in \widehat{A}_{\mathrm{nr}}[\![X]\!]$ such that $\psi \circ \psi^{-1} = \mathrm{id} = \psi^{-1} \circ \psi$.

1° Since $\sigma - 1$ is surjective on $\widehat{U}_{\mathrm{nr}}$, we can find $\varepsilon \in \widehat{U}_{\mathrm{nr}}$ such that $\sigma\varepsilon = \varepsilon u$. Now define $\phi_1(X) = \varepsilon X$. For $n \geqslant 1$, define $\phi_{n+1}(X) = \phi_n(X) + bX^{n+1}$. Suppose we have found ϕ_n such that ${}^\sigma\phi_n = \phi_n \circ [u]_f + E_n$ with $E_n = aX^{n+1} + \cdots \equiv 0 \pmod{\deg n+1}$. We have

$${}^\sigma\phi_{n+1}(X) - \phi_{n+1}([u]_f(X)) = E_n + \sigma(b)X^{n+1} - b([u]_fX)^{n+1} \equiv (a + \sigma(b) - bu^{n+1})X^{n+1} \pmod{\deg n+2}$$

Write $b = \varepsilon^{n+1}b'$; then

$$\sigma(b) - bu = \sigma(\varepsilon^{n+1}b') - b'\varepsilon^{n+1}u = \varepsilon^{n+1}u(\sigma(b') - b')$$

Since $\sigma - 1$ is surjective on $\widehat{A}_{\mathrm{nr}}$, we can find $b' \in \widehat{A}_{\mathrm{nr}}$ such that $\sigma(b') - b' = \dfrac{-a}{\varepsilon^{n+1}u}$, so we finish our construction of ϕ_{n+1} with ${}^\sigma\phi_{n+1} \equiv \phi_{n+1} \circ [u]_f \pmod{\deg n+2}$. Now taking limit we obtain $\phi \in \widehat{A}_{\mathrm{nr}}[\![X]\!]$ satisfying $\phi(X) \equiv \varepsilon X \pmod{\deg 2}$ and (a).

2° We adjust ϕ so that $g = {}^\sigma\phi \circ f \circ \phi^{-1}$. Put $h = {}^\sigma\phi \circ f \circ \phi^{-1}$. Then

$$h = {}^\sigma\phi \circ f \circ \phi^{-1} = \phi \circ [u]_f \circ f \circ \phi^{-1} = \phi \circ f \circ [u]_f \circ \phi^{-1}$$

Since $f, [u]_f$ have coefficients in A, we have

$${}^\sigma h = {}^\sigma\phi \circ f \circ [u]_f \circ {}^\sigma(\phi^{-1}) = {}^\sigma\phi \circ f \circ \phi^{-1} = h$$

for $\mathrm{id} = {}^\sigma\phi \circ {}^\sigma(\phi^{-1}) = \phi \circ [u]_f \circ {}^\sigma(\phi^{-1})$, so that h has coefficients in $\widehat{A}_{\mathrm{nr}}$. Also,

$$h(X) \equiv \sigma(\varepsilon)\pi\varepsilon^{-1}X \equiv u\pi X \pmod{\deg 2}$$

and

$$h(X) \equiv \phi^q \circ \phi^{-1}(X) \equiv \phi \circ \phi^{-1}(X^q) \equiv X^q \pmod{\mathfrak{m}_K}$$

so that $h \in \mathfrak{F}_\varpi$ $(\varpi = \pi u)$. Now let $\varphi = [1]_{g,h} \circ \phi$; then φ still satisfies (a) and $\varphi(X) \equiv \varepsilon X \pmod{\deg 2}$, and, moreover,

$${}^\sigma\varphi \circ f \circ \varphi^{-1} = [1]_{g,h} \circ \left({}^\sigma\phi \circ f \circ \phi^{-1}\right) \circ [1]_{g,h}^{-1} = [1]_{g,h} \circ h \circ [1]_{g,h}^{-1} = g$$

From now on we replace ϕ by φ.

3° We prove $F_g = \phi \circ F_f \circ (\phi \times \phi)^{-1}$. One has

$$\phi \circ F_f \circ (\phi \times \phi)^{-1}(X, Y) \equiv \varepsilon(\varepsilon^{-1}X + \varepsilon^{-1}Y) \equiv X + Y \pmod{\deg 2}$$

and

$$\begin{aligned} g \circ \phi \circ F_f \circ (\phi \times \phi)^{-1} &= {}^\sigma\phi \circ f \circ F_f \circ (\phi^{-1} \circ \phi^{-1}) \\ &= {}^\sigma\phi \circ F_f \circ ((f \circ \phi^{-1}) \times (f \circ \phi^{-1})) \\ &= {}^\sigma\phi \circ F_f \circ ((({}^\sigma\phi)^{-1} \circ g) \times (({}^\sigma\phi)^{-1} \circ g)) \\ &= {}^\sigma\phi \circ F_f(({}^\sigma\phi)^{-1} \times ({}^\sigma\phi)^{-1}) \circ (g \times g) \\ &= \phi \circ [u]_f \circ F_f([u]_f^{-1} \times [u]_f^{-1}) \circ (\phi^{-1} \times \phi^{-1}) \circ (g \times g) \\ &= \phi \circ F_f \circ (\phi \times \phi)^{-1} \circ (g \times g) \end{aligned}$$

so by Proposition 5.17, $F_g = \phi \circ F_f \circ (\phi \times \phi)^{-1}$ so that (b) holds. The proof for (c) is similar to that of (b).

□

Computation of the norm reciprocity map in L/K

Let $L_\pi = K_{\mathrm{nr}}K_\pi$. Since K_{nr} and K_π are linearly disjoint (one unramified and one totally ramified), we have

$$\mathrm{Gal}(L_\pi/K) = \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K_{\mathrm{nr}}/K)$$

For each uniformizer $\pi \in A$ of A, define $r_\pi : K^\times \to \mathrm{Gal}(L_\pi/K)$ such that

- $r_\pi(\pi) = 1$ on K_π, and is Frob_K on K_{nr};
- for $u \in U_K$, $r_\pi(u) = [u^{-1}]_f$ on K_π and is 1 on K_{nr}.

We want to prove that the field L_π and the homomorphism r_π are independent of π. Let $\varpi = \pi u$ be the second uniformizer.

First, $L_\pi = L_\varpi$. For by Lemma 5.20, F_f and F_g are isomorphic over $\widehat{K}_{\mathrm{nr}}$. Hence the field generated by their division points are the same; so $\widehat{K}_{\mathrm{nr}}K_\pi = \widehat{K}_{\mathrm{nr}}K_\varpi$. On taking completions we find

$$\widehat{K_{\mathrm{nr}}K_\pi} = \widehat{K_{\mathrm{nr}}K_\varpi}$$

Lemma 5.21. *Let E be any algebraic extension of a local field and let $\alpha \in \widehat{E}$. If α is separable over E, then $\alpha \in E$.*

Proof. Let E_s be the separable closure of E. It suffices to show $\widehat{E} \cap E_s = E$. Let $s \in \mathrm{Gal}(E_s/E)$. Since s is continuous and is the identity on E, it extends to the identity on $\widehat{E}$. Hence $\mathrm{Gal}(E_s/E) = \mathrm{Gal}(E_s/\widehat{E} \cap E_s)$, and by Galois theory, $\widehat{E} \cap E_s = E$. □

Hence, intersecting with the separable closure K_s of K, we obtain $K_{\mathrm{nr}}K_\pi = K_{\mathrm{nr}}K_\varpi$, so that $L_\pi =: L$ is independent of π.

We turn now to the homomorphism $r_\pi : K^\times \to \mathrm{Gal}(L/K)$. We shall show that $r_\pi(\varpi) = r_\varpi(\varpi)$; this will imply that $r_\pi(\varpi)$ is independent of π, and so the r_π's coincide on the local uniformizer. Since these generate $K^\times$, the result will follow.

We look first at $r_\varpi(\varpi)$. On K_{nr}, $r_\varpi(\varpi) = \mathrm{Frob}_K$, and on K_ϖ it is 1. On the other hand, $r_\pi(\varpi)$ is $\sigma = \mathrm{Frob}_K$ on K_{nr}; so we must look at $r_\pi(\varpi)$ on K_ϖ.

Now $K_\varpi = K(E_g)$, where $g \in \mathfrak{F}_\varpi$. Let $\phi \in \widehat{A}[\![X]\!]$ be as in Lemma **??**; ϕ determines an isomorphism of E_f onto E_g. So if $\lambda \in E_g$, then we can write $\lambda = \phi(\mu)$ with $\mu \in E_f$. We look at $r_\pi(\varpi)\lambda$, and we want to show that this is λ. Write $s = r_\pi(\varpi)$. We want to show ${}^s\lambda = \lambda$, or ${}^s\phi(\mu) = \phi(\mu)$. Now $r_\pi(\varpi) = r_\pi(\pi)r_\pi(u)$. Since ϕ has coefficients in $\widehat{K}_{\mathrm{nr}}$, ${}^s\phi = {}^\sigma\phi = \phi \circ [u]_f$ by Lemma **??**. But

$${}^s(\phi(\mu)) = {}^s\phi({}^s\mu) = {}^s\phi([u^{-1}]_f(\mu))$$

Hence

$${}^s\phi(\mu) = \phi \circ [u]_f \circ [u^{-1}]_f(\mu) = \phi(\mu)$$

so r_π is the identity on K_ϖ. We conclude that r_π is independent of π.

5.3.8 The Existence Theorem

Let K^{ab} be the maximal abelian extension of K; it contains K_{nr}. We prove Theorem A: if $I_K = \text{Gal}(K^{\text{ab}}/K_{\text{nr}})$ is the inertia subgroup of $\text{Gal}(K^{\text{ab}}/K)$, then the reciprocity map $\theta : U_K \to I_K$ is an isomorphism.

Let $L = K_\pi K_{\text{nr}}$ and let $I'_K = \text{Gal}(L/K_{\text{nr}})$ be the inertial subgroup of $\text{Gal}(L/K)$. Consider the map

$$U_K \xrightarrow{\theta} I_K \xrightarrow{e} I'_K$$

where θ is the reciprocity map and $e : I_K \to I'_K$ is the canonical map; both of them are surjective.

On the other hand, the composition $e \circ \theta : U_K \to I'_K$ has just been computed. If we identify I'_K with U_K, it is $u \mapsto u^{-1}$. Hence the composed map $e \circ \theta$ is an isomorphism, and it follows that both of them are isomorphisms.

- θ is an isomorphism. This gives Theorem A.

- e is an isomorphism. This implies $L = K^{\text{ab}}$, since both L and K^{ab} contain K_{nr}.

Alternatively, let us prove that every open subgroup M of $K^\times$ of finite index is a norm subgroup corresponding to a finite subextension of L. This will prove both the existecne theorem and that $L = K^{\text{ab}}$.

Since M is open, $U_K^n \subseteq M$ for some $n \geqslant 1$; since M is of finite index, $\pi^m \in M$ for some $m \geqslant 1$. Hence M contains the subgroup $V_{n,m}$ generated by U_K^n and π^m. Now let K_m be the unramified extension of K of degree m, and consider the subfield $L_{n,m} = K_\pi^n K_m$ of L. If $u \in U_K$ and $a \in \mathbb{Z}$, we know that $(u\pi^a, L_{n,m}/K)$ is equal to $[u^{-1}]$ on K_π^n, and to Frob_K^a on K_m; hence

$$(u\pi^a, L_{n,m}/K) = 1 \Leftrightarrow u \in U_K^n \text{ and } a \equiv 0 \pmod{m} \Leftrightarrow u\pi^a \in V_{n,m}$$

This shows that $V_{n,m} = NL_{n,m}$, and since M contains $V_{n,m}$, M is the norm group of a subextension of $L_{n,m}$.

5.4 Ramification Subgroups of Conductors

Chapter 6

Global Class Field Theory

6.1 Action of the Galois Group on Primes and Completions

6.2 Frobenius Automorphisms

6.3 Artin's Reciprocity Law

Proposition 6.1. The diagram

$$\begin{tikzcd}
I^{S'} \arrow[r, "\mathrm{Frob}_{L'/K'}"] \arrow[d, "N_{K'/K}"'] & \mathrm{Gal}(L'/K') \arrow[d, "\theta"] \\
I^{S} \arrow[r, "\mathrm{Frob}_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

are commutative, where N denotes "norm".

Theorem 6.2. If L/K is a finite abelian extension, and S is the set of primes of K consisting of the archimedean ones and those ramified in L, then there exists $\varepsilon > 0$ such that if $a \in K^\times$ and $|a-1|_\nu < \varepsilon$ for all $\nu \in S$, then $\mathrm{Frob}_{L/K}((a)^S) = 1$.

Corollary 6.2.1. Let L, K, S be as in the theorem. If L/K are number fields, then the condition $|a-1|_\nu < \varepsilon$ can be replaced by $a \in (K_\nu^\times)^n$ with $n = [L : K]$.

6.4 Chevalley's Interpretation by Ideles

Proposition 6.3. Let K and S be as before, G be a complete abelian topological group and ϕ an admissible homomorphism of I^S into G. Then there exists a unique homomorphism $\phi : J_K \to G$ such that

(i) ψ is continuous;

(ii) $\psi(K^\times) = 1$;

(iii) $\psi(x) = \phi((x)^S)$ for all $x \in J_K^S$.

Conversely, if $\psi : J_K \to G$ is a continuous homomorphism such that $\psi(K^\times) = 1$, then ψ comes from some admissible pair (S, ϕ) as defined above, provided that there exists a neighborhood of 1 in G such that $\{1\}$ is the only subgroup.

Corollary 6.3.1. The reciprocity law holds for a finite extension L/K if and only if there exists a continuous homomorphism $\psi : J_K \to \mathrm{Gal}(L/K)$ such that

(i) ψ is continuous;

(ii) $\psi(K^\times) = 1$;

(iii) $\psi(x) = \mathrm{Frob}_{L/K}((x)^S)$ for all $x \in J_K^S$, where S consists of all archimedean primes of K and those ramified in L.

Proposition 6.4. If the reciprocity law holds for L/K and L'/K', then

$$\begin{tikzcd}
J_{K'} \arrow[r, "\psi_{L'/K'}"] \arrow[d, "N_{K'/K}"'] & \mathrm{Gal}(L'/K') \arrow[d, "\theta"] \\
J_K \arrow[r, "\psi_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

is a commutative diagram.

Proof. Let S be a large finite set of primes of K, and S' be the set of primes of K' above S. We have then a diagram

$$\begin{tikzcd}
& I_{K'}^{S'} \arrow[dr, "\mathrm{Frob}_{L'/K'}"] \arrow[dd] & \\
J_{K'}^{S'} \arrow[ur] \arrow[rr, "\psi_{L'/K'}"'] \arrow[dd, "N_{K'/K}"'] & & \mathrm{Gal}(L'/K') \arrow[dd, "\theta"] \\
& I_K^S \arrow[dr, "\mathrm{Frob}_{L/K}"] & \\
J_K^S \arrow[ur] \arrow[rr, "\psi_{L/K}"] & & \mathrm{Gal}(L/K)
\end{tikzcd}$$

The non-rectangular parallelograms are commutative by compatibility of ideal and idele norms, and by Proposition 6.1. The triangles are commutative by Corollary 6.3.1.(iii). Thus the front rectangle is commutative. But $\psi_{L/K} \circ N_{K'/K}$ and $\theta \circ \psi_{L'/K'}$ take value 1 on principal ideles by Corollary 6.3.1.(ii), so they coincide on $(K')J_{K'}^{S'}$, which is a dense subset of $J_{K'}$ by weak approximation. Since the two maps are continuous, they coincide on the whole $J_{K'}$ which is what we wished to prove. □

Variant. Suppose L/K satisfies the reciprocity law, and $K \subseteq M \subseteq L$. Then $\psi_{L/K}(N_{M/K}J_M) \subseteq \mathrm{Gal}(L/M)$.

6.5 Statement of the Main Theorem on Abelian Extensions

Theorem 6.5.

(A) Every abelian extension L/K satisfies the reciprocity law, i.e., there is an Artin map $\psi_{L/K} : J_K \to \mathrm{Gal}(L/K)$.

(B) The Artin map $\psi_{L/K}$ is surjective with kernel $K^\times N_{L/K} J_L$ and hence induces an isomorphism of $C_K/N_{L/K}C_L$ onto $\mathrm{Gal}(L/K)$.

(C) If $M \supseteq L \supseteq K$ are abelian extensions, then the diagram

$$\begin{tikzcd}
C_K/N_{M/K}C_M \arrow[r, "\psi_{M/K}"] \arrow[d] & \mathrm{Gal}(M/K) \arrow[d] \\
C_K/N_{L/K}C_L \arrow[r, "\psi_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

where the horizontal arrows are natural maps (note that $N_{M/K}C_M \subseteq N_{L/K}C_L$).

(D) (Existence theorem) For every open subgroup N of finite index in C_K there exists a unique abelian extension L/K (in a fixed separable closure of K) such that $N_{L/K}C_L = N$.

The subgroup N of (D) are called **norm groups**, and the abelian extension L such that $N_{L/K}C_L = N$ is called the **class field** belonging to N.

1. Given (A) and (B), then (C) is a special case of Proposition 6.4 (put $K' = K$ and $L' = M$)

2. The uniqueness part of (D) follows from the rest. Given the existence, let L and L' be two finite abelian extensions of K in a fixed separable closure of K and let M be the compositum of L and L' (which is again a finite abelian extension of K). Now consider the diagram in (C). Since the horizontal arrows are isomorphisms by (B) we see that $\ker\theta = \mathrm{Gal}(M/K)$ is the isomorphic images under $\psi_{M/K}$ of the group $N_{L/K}C_L/N_{M/K}C_M$. Thus L, as the fixed field of the group $\ker\theta$, is uniquely determined, as a subfield of M, by $N_{L/K}C_L$. Applying the same reasoning with L replaced by L', we see that if $N_{L'/K'}C_{L'} = N_{L/K}C_L$, then $L = L'$.

The commutative diagram of (C) allows us to pass to the inverse limit, as L runs over all finite abelian extensions of K. We obtain a homomorphism

$$\psi_K : C_K \longrightarrow \varprojlim_L \mathrm{Gal}(L/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

where K^{ab} is the maximal abelian extension of K; and then, by (D),

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \varprojlim_N C_K/N$$

where the limit is taken over all open subgroups N of finite index in C_K. Thus we know the Galois groups of all abelian extensions of K from a knowledge of the idele class group of K. The nature of the homomorphism $\psi_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is somewhat different in the function field and number field cases. The facts, which are not hard to derive from the main theorem, but whose proofs we omit, are as follows:

Function Field Case. Here the map ψ_K is injective and its image is the dense subgroup of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ consisting of those automorphisms whose restriction to the algebraic closure $\overline{K}$ of the field of constants k is simply an integer power of the Frobenius automorphism F_k.

Number Field Case. Here ψ_K is surjective and its kernel is the connected component D_K of C_K. So we have obtained a canonical isomorphism $C_K/D_K \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Example. Cyclotomic Fields.

Consider $\mathbb{Q}^{\mathrm{mc}}/\mathbb{Q}$, the maximal cyclotomic extension of $\mathbb{Q}$. Let $\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$; by Chinese Remainder theorem we have $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers.

(i) $\widehat{\mathbb{Z}}$ acts on any abelian torsion group, for $\mathbb{Z}/n\mathbb{Z}$ acts on any abelian group whose exponent divides n.

(ii) The invertible elements of $\widehat{\mathbb{Z}}$ are those in $\prod_p U_p$, where $U_p = \mathbb{Z}_p^\times$.

Now consider the torsion group μ consisting of all roots of unity. If $\zeta \in \mu$, we can define ζ^u for all $u \in \prod_p U_p$; explicitly, if ζ is a primitive m-th root of unity, write m_p the "p-primary part" of m and u_p the p-component of u. Take an $n \in \mathbb{Z}$ that solves the simultaneous congruence $n \equiv u_p \pmod{m_p}$ for all p; then $(n, m) = 1$ and $n \mod m$ is uniquely determined. Then $\zeta^u = \zeta^n$.

u induces an automorphism on μ. On the other hand,

$$J_{\mathbb{Q}} \cong \mathbb{Q}^\times \times \mathbb{R}_+ \times \prod_p U_p$$

Indeed, if $x = (x_\infty, x_2, x_3, \ldots) \in J_{\mathbb{Q}}$, we have $x = a \cdot (t, u_2, u_3, \ldots)$, where

$$a = \operatorname{sign} x_\infty \cdot \prod_p p^{\nu_p(x_p)} \in \mathbb{Q}^\times$$

and where $t > 0$ and $u_p \in U_p$ for $p = 2, 3, \ldots$. Moreover, this decomposition is unique because 1 is the only positive rational number which is a p-adic unit for all primes p. Hence we have a canonical isomorphism

$$C_{\mathbb{Q}} \cong \mathbb{R}_+ \times \prod_p U_p$$

so there is a map of $C_{\mathbb{Q}}$ onto $\prod_p U_p$, which is the Galois group of the maximal cyclotomic extension.

What in fact happens is the following.

Lemma 6.6. If $x \in C_{\mathbb{Q}}$ and $x \mapsto u \in \prod_p U_p$, then $\zeta^{\psi(x)} = \zeta^{u^{-1}}$.

Proof. Suppose ζ is a primitive m-th root of unity and let $S \subseteq M_K$ consist of ∞ and all prime factors of m. We have three cases.

- $x \in \mathbb{R}_+$. Let $a_n \in \mathbb{Q}$ be such that $a_n \to x$ at all places in S; particularly $a_n \in J^S_{\mathbb{Q}}$. Then

  $$\psi(x) = \psi(a_n x) = \lim_{n\to\infty} \psi((a_n x)^S) \cdot \lim_{n\to\infty} \prod_{q \in S} \psi((a_n x)_q) = \lim_{n\to\infty} \mathrm{Frob}_{\mathbb{Q}(\zeta)/\mathbb{Q}}((a_n)^S)$$

  Write $a_n = b_n/c_n$ with $b_n, c_n \in \mathbb{Z}$ coprime to m and $b_n \equiv c_n \pmod m$ (the latter condition can be satisfied by, for example, Fermat little theorem). Then

  $$\mathrm{Frob}_{\mathbb{Q}(\zeta)/\mathbb{Q}}((b_n)^S).\zeta = \zeta^{b_n} = \zeta^{c_n} = \mathrm{Frob}_{\mathbb{Q}(\zeta)/\mathbb{Q}}((c_n)^S).\zeta$$

  so that $\mathrm{Frob}_{\mathbb{Q}(\zeta)/\mathbb{Q}}((a_n)^S) = 1$.

- $x \in U_p$ with $p \mid m$. Take $a_n \in \mathbb{Z}_{>0}$ such that $a_n \to x^{-1}$ at all finite places in S.

  $$\psi(x) = \psi(a_n x) = \lim_{n\to\infty} \psi((a_n x)_\infty) \cdot \lim_{n\to\infty} \psi((a_n x)^S) \cdot \lim_{n\to\infty} \prod_{q \in S_{\mathrm{fin}}} \psi((a_n x)_q) = \lim_{n\to\infty} \mathrm{Frob}_{\mathbb{Q}(\zeta)/\mathbb{Q}}((a_n)^S)$$

  Let us assume $a_n \equiv (x^{-1})_q \pmod{m_q}$ for all $n \geqslant 1$. Then $\zeta^{u^{-1}} = \zeta^{a_n}$. Since the a_n are coprime to m,

  $$\mathrm{Frob}_{\mathbb{Q}(\zeta)/\mathbb{Q}}((a_n)^S).\zeta = \zeta^{a_n}$$

  for each n.

- $x \in U_p$ with $p \nmid m$. In this case, $\psi(x) = \mathrm{Frob}_{\mathbb{Q}(\zeta)/\mathbb{Q}}((x)^S) = 1$.

□

Proposition 6.7 (Kronecker-Weber)**.** $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{mc}}$.

Proof. From the lemma above we see $\ker\psi = \mathbb{R}_+$, which is the connected component $D_{\mathbb{Q}}$ of $C_{\mathbb{Q}}$. The discussion above gives an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & D_{\mathbb{Q}} = \mathbb{R}_+ \arrow[r] & C_{\mathbb{Q}} \arrow[r] & \prod_p U_p = \mathrm{Gal}(\mathbb{Q}^{\mathrm{mc}}/\mathbb{Q}) \arrow[r] & 0 \end{tikzcd}$$

Assuming (B) of the main theorem, we have

$$\begin{tikzcd} 0 \arrow[r] & D_{\mathbb{Q}} \arrow[r] & C_{\mathbb{Q}} \arrow[r, "\psi"] & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \arrow[r] & 0 \end{tikzcd}$$

Adjusting in accordance with the above lemma, we see the natural map $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{mc}}/\mathbb{Q})$ is an isomorphism, hence $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{mc}}$. □

6.6 Relation between Global and Local Artin Maps

We continue to deduce results on the assumption that the reciprocity law (but not necessarily the whole main theorem) is true for an abelian extension L/K.

For each prime v of K, we let K_v denote the completion of K at v. If L/K is a finite Galois extension, then the various completions of L_w with w over v are isomorphic. It is convenient to write L^v for "any one of the completions L_w for $w \mid v$", and we write $G^v = \mathrm{Gal}(L^v/K_v)$ for the local Galois group, which we can identity with a decomposition subgroup of G. In the abelian case this subgroup is unique, i.e. independent of the choice of w.

Assume that L/K is abelian and that there exists an Artin map

$$\psi_{L/K} : J_K \to \mathrm{Gal}(L/K) =: G$$

For each prime v of K we have

$$\begin{tikzcd} K_v^\times \arrow[r, shift left, "i_v"] & J_K \arrow[l, shift left, "j_v"] \arrow[r, "\psi_{L/K}"] & G \end{tikzcd}$$

where

- $i_v : K_v^\times \hookrightarrow J_K$ maps $x \in K_v^\times$ to the element of J_K whose v-th component is x, and the others are 1;
- $j_v : J_K \to K_v^\times$ is the projection to v-th component.

Call $\psi_v = \psi_{L/K} \circ i_v$; so $\psi_v : K_v^\times \to G$. In fact

Proposition 6.8. If $K_v \subseteq \mathcal{M} \subseteq L^v$, then $\psi_v(N_{\mathcal{M}/K_v}\mathcal{M}^\times) \subseteq \mathrm{Gal}(L^v/\mathcal{M})$. In particular, $\psi_v(K_v^\times) \subseteq G^v$, and $\psi_v(N_{L^v/K_v}(L^v)^\times) = 1$.

Proof. Let $M = L \cap \mathcal{M}$ be the fixed field of $\mathrm{Gal}(L^v/\mathcal{M})$ in L, so that $\mathrm{Gal}(L/M)$ is identified with $\mathrm{Gal}(L^v/\mathcal{M})$ under our identification of the decomposition group with the local Galois group. Then $\mathcal{M} = M_v$, where w is a prime above v, and the diagram

$$\begin{tikzcd} \mathcal{M} = M_v \arrow[r, "i_w"] \arrow[d, "N_{\mathcal{M}/K_v}"'] & J_M \arrow[d, "N_{M/K}"] \\ K_v \arrow[r, "i_v"] & J_K \end{tikzcd}$$

is commutative. By Variant of Proposition 6.4 we conclude that

$$\psi_v(N_{\mathcal{M}/K_v}\mathcal{M}^\times) \subseteq \psi_{L/K}(N_{M/K}J_M) \subseteq \mathrm{Gal}(L/M) \cong \mathrm{Gal}(L^v/\mathcal{M})$$

□

We shall call $\psi_v : K_v^\times \to G^v$ the **local Artin homomorphism**, or by its classical name: **norm residue homomorphism**. If $x = (x_v) \in J_K$, then we have

$$x = \lim_S \left(\prod_{v \in S} i_v(x_v) \right)$$

and consequently, by continuity, we have

$$\psi_{L/K}(x) = \prod_v \psi_v(x_v)$$

this product is actually finite since if x_v is a v-unit and v is not ramified, then it is a norm of L^v/K_v. Thus knowledge of all the local Artin maps ψ_v is equivalent to knowledge of the global Artin map $\psi_{L/K}$.

6.7 Cohomology of Ideles

Let L/K be a finite Galois extension (not necessarily abelian) with Galois group G. Write $\mathbb{A}_L$ for the adele ring of L and J_L for the idele group, the invertible elements in $\mathbb{A}_L = L \otimes_K \mathbb{A}_K$, and G acts on $L \otimes_K \mathbb{A}_K$ by $\sigma \mapsto \sigma \otimes 1$; so G acts on J_L.

However, we want to look at the action of G on the cartesian product structure of J_L. Suppose $x \in J_L$, then $x = (x_w)_{w \in M_L}$; $\sigma \in G$ induces $\sigma_w : L_w \to L_{\sigma w}$. Then $(\sigma x)_{\sigma w} = \sigma_w x_w$. Indeed, the identification $\mathbb{A}_L = L \otimes_K \mathbb{A}_K$ is given by

$$L \otimes_K K_v \longrightarrow \prod_{w|v} L_w$$

$$a \otimes x \longmapsto (i_w(a)x)_w$$

We transfer the G-module structure to RHS by this identification; using $\sigma \circ i_w = i_{\sigma w} \circ \sigma$, we see $(\sigma x)_{\sigma w} = \sigma_w x_w$. Hence we have two commutative diagrams

$$\begin{tikzcd} L_w^\times \arrow[r, "\sigma_w"] \arrow[d, "i_w"'] & L_{\sigma w}^\times \arrow[d, "i_{\sigma w}"] \\ J_L \arrow[r, "\sigma"] & J_L \end{tikzcd} \qquad \begin{tikzcd} L_w^\times \arrow[r, "\sigma_w"] & L_{\sigma w}^\times \\ J_L \arrow[r, "\sigma"] \arrow[u, "j_w"] & J_L \arrow[u, "j_{\sigma w}"'] \end{tikzcd}$$

Proposition 6.9. Let $v \in M_K$ and $w_0 \in M_L$ with $w_0 \mid v$. Then there are mutually inverse isomorphisms

$$H^r\left(G, \prod_{w|v} L_w^\times\right) \underset{j_{w_0}\cdot \operatorname{res}}{\overset{\operatorname{cores}. i_{w_0}}{\rightleftarrows}} H^r(G_{w_0}, L_{w_0}^\times)$$

and

$$H^r\left(G, \prod_{w|v} U_w\right) \underset{j_{w_0}\cdot \operatorname{res}}{\overset{\operatorname{cores}. i_{w_0}}{\rightleftarrows}} H^r(G_{w_0}, U_{w_0})$$

where U_w denotes the group of units in L_w. The assertion remains valid when H^r is replaced by $\hat{H}^r$.

Proof. This follows from Shapiro's lemma once

$$\begin{tikzcd} \operatorname{ind}^G_{G_{w_0}} L^\times_{w_0} \arrow[r] & \prod_{w|v} L^\times_w \\ f : G \to L^\times_{w_0} \arrow[r, mapsto] & (\sigma f \sigma^{-1})_{\sigma w_0} \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} \prod_{w|v} L^\times_w \arrow[r] & \operatorname{ind}^G_{G_{w_0}} L^\times_{w_0} \\ \alpha \arrow[r, mapsto] & f_\alpha : \sigma \mapsto \sigma \alpha_{\sigma^{-1} w_0} \end{tikzcd}$$

are shown to be mutually inverse. □

Thus the cohomology groups $H^r(G_w, L_w^\times)$ are canonically isomorphic for all w over v, so it is permissible to use the notation $H^r(G^v, (L^v)^\times)$ for any one of these.

Proposition 6.10.

(a) Under the inclusion $J_K \subseteq J_L$, one has $J_L^G = J_K$.

(b) $\hat{H}^r(G, J_L) \cong \bigoplus_{v \in M_K} \hat{H}^r(G^v, (L^v)^\times)$.

Proof.

1. It is clear $J_K \subseteq J_L^G$. Let $x = (x_w)_w \in \prod_{w|v} L_w^\times$. Suppose x is fixed by G; in particular, for each $w \mid v$, x_w is fixed by $\operatorname{Gal}(L_w/K_v)$, so that $x_w \in K_v^\times$. But if $\sigma w = w'$, then $x_{w'} = x_{\sigma w} = (\sigma x)_{\sigma w} = \sigma_w x_w$. Hence all $x_w \in K_v^\times$ are the same, and thus $x \in K_v^\times$.

2. Recall that
$$J_L = \varinjlim_S J_{L,S} \text{ where } J_{L,S} := \prod_{v \in S} \prod_{w|v} L_w^\times \times \prod_{v \notin S} \prod_{w|v} U_w$$
and S is a finite set of primes of K containing all the ramified primes in L/K and the archimedean primes. The limit is taken over an increasing sequence of S with $S \to M_K$. Note that

   - the cohomology of finite groups commutes with direct limits, and
   - any cohomology theory commutes with products

   so it is enough to look at the cohomology of the various parts. By the above Proposition and Proposition 5.3, $\prod_{v \notin S} \prod_{w|v} U_w$ has trivial cohomology for S contains all ramified primes. Hence
$$\hat{H}^r(G, J_{L,S}) \cong \prod_{v \in S} \hat{H}^r(G^v, (L^v)^\times) \cong \bigoplus_{v \in S} \hat{H}^r(G^v, (L^v)^\times)$$
by above Proposition, and
$$\hat{H}^r(G, J_L) \cong \varinjlim_S \bigoplus_{v \in S} \hat{H}^r(G^v, (L^v)^\times) = \bigoplus_{v \in M_K} \hat{H}^r(G^v, (L^v)^\times)$$

□

Corollary 6.10.1.

(a) $H^1(G, J_L) = 0$.

(b) $H^2(G, J_L) \cong \bigoplus_{v \in M_K} \left(\frac{1}{n_v}\mathbb{Z}/\mathbb{Z}\right)$, where $n_v = [L^v : K_v]$.

Proof. These follow from local class field theory. □

6.8 Cohomology of Idele Class (I), The First Inequality

We recollect the exact sequence $0 \to L^\times \to J_L \to C_L \to 0$. The action of G on C_L is that induced by its action on J_L.

Proposition 6.11. $C_K \cong C_L^G$.

Proof. The above exact sequence gives rise to the cohomology sequence

$$0 \to H^0(G, L^\times) \to H^0(G, J_L) \to H^0(G, C_L) \to H^1(G, L^\times)$$

that is

$$0 \to K^\times \to J_L^G = J_K \to C_L^G \to 0$$

□

Remark 6.12. Our object in the abelian case is to define

$$\psi_{L/K} : C_K/N_{L/K}C_L \to \mathrm{Gal}(L/K) = G$$

By the above Proposition $C_K/N_{L/K}C_L = \hat{H}^0(G, C_L)$, and on the other hand $G = \hat{H}^{-2}(G, \mathbb{Z})$. Comparison with local class field theory suggests that the global theorem we want to prove about the cohomology of C_L is essentially the same as the local theorem about the cohomology of $L^\times$. This is in fact the case. Abstracting the common features, one get the general notion of “class formation”.

We recollect that if G is cyclic and A a G-module, the Herbrand quotient is defined by

$$h(G, A) = \frac{\# H^2(G, A)}{\# H^1(G, A)}$$

if both these cardinalities are finite.

Theorem 6.13. Let L/K be a cyclic extension of degree n. Then $h(G, C_L) = n$.

Proof. Take $S \in M_K$ to be a finite containing all ramified primes of K in L, all archimedean primes of K and all primes of K which lie below some primes that generates the ideal class group of L. Then $J_L = L^\times J_{L,S}$, where

$$J_{L,S} := \prod_{v \in S} \prod_{w|v} L_w^\times \times \prod_{v \notin S} \prod_{w|v} U_w$$

Let $T \subseteq M_L$ collect those primes that lies above S. Then

$$C_L \cong J_L/L^\times \cong J_{L,S}/(L^\times \cap J_{L,S}) = J_{L,S}/L_T$$

where $L_T = L^\times \cap J_{L,S}$ is the set of T-units of L. It follows that

$$h(C_L) = \frac{h(J_{L,S})}{h(L_T)}$$

if the right hand side is defined.

First we determine $h(J_{L,S})$. Since S contains all ramified primes, $\prod_{v \notin S} \prod_{w|v} U_w$ has trivial cohomology, so that

$$h(J_{L,S}) = h\left(\prod_{v \in S} \prod_{w|v} L_w^\times\right) = \prod_{v \in S} h\left(\prod_{w|v} L_w^\times\right)$$

Now by Proposition 6.9 and Corollary 5.4.1

$$h(J_{L,S}) = \prod_{v \in S} n_v$$

where $n_v = [L^v : K_v]$ is the local degree. This is the "local part" of the proof.

The "global part" consists in determining $h(L_T)$; in order the prove that $h(C_L) = n$, we have the show that $nh(L_T) = \prod_{v \in S} n_v$. We do this by constructing a real vector space, on which G acts, with two lattices such that one has Herbrand quotient $nh(L_T)$ and the other has quotient $\prod_{v \in S} n_v$.

Let $V = \mathrm{Hom}_{\mathbb{R}}(T, \mathbb{R}) \cong \mathbb{R}^t$, where $t = \#T$. Make G act on V by defining

$$(\sigma f)(w) = f(\sigma^{-1} w)$$

for all $f \in V$, $\sigma \in G$, $w \in T$ (so that $(\sigma f)(\sigma w) = f(w)$). Put

$$N = \{f \in V \mid f(T) \subseteq \mathbb{Z}\}$$

Clearly, N spans V and is G-invariant. We have $N \cong \prod_{v \in S} \prod_{w|v} \mathbb{Z}_w$, where $\mathbb{Z}_w \cong \mathbb{Z}$ for all w, and the action of G on N is to permute the $\mathbb{Z}_w$ over a given $v \in S$. Then by Shapiro's lemma

$$\hat{H}^r(G, N) \cong \prod_{v \in S} \hat{H}^r\left(G, \prod_{w|v} \mathbb{Z}_w\right) \cong \prod_{v \in S} \hat{H}^r(G^v, \mathbb{Z})$$

so that

$$h(N) = \prod_{v \in S} \frac{\#\hat{H}^0(G^v, \mathbb{Z})}{\#\hat{H}^1(G^v, \mathbb{Z})} = \prod_{v \in S} n_v$$

Now we define another lattice. Let $\lambda : L_T \to V$ given by $\lambda(a) = f_a$, where $f_a(w) = \log |a|_w$ for all $w \in T$. The unit theorem tells us that $\ker \lambda$ is finite and $\lambda(L_T)$ is a lattice M^0 of V spanning the subspace $V^0 = \{f \in V \mid \sum f(w) = 0\}$. Since $\ker \lambda$ is finite, $h(L_T) = h(M^0)$. Now let $V = V^0 + \mathbb{R}g$, where $g : T \to V$ is defined by $g(w) = 1$ for all $w \in S$. Our second lattice is $M = M^0 + \mathbb{Z}g$. Then M spans V and both M^0, $\mathbb{Z}g$ are invariant under G. Hence $h(M) = h(M^0)h(\mathbb{Z}) = nh(M^0) = nh(L_T)$.

Now M, N are lattices spanning the same vector space, so $h(N) = h(M)$ by Proposition 4.12. This finishes the proof. □

Corollary 6.13.1 (First inequality)**.** If L/K is cyclic of degree n, then

$$\#\left(\frac{J_K}{K^\times N_{L/K} J_L}\right) \geqslant n$$

Proof. From the Theorem and Proposition 6.11, we have

$$n = h(G, C_L) \leqslant \#\hat{H}^0(G, C_L) = \#\left(\frac{J_K}{K^\times N_{L/K} J_L}\right)$$

□

Corollary 6.13.2. If L/K is a finite abelian extension and $D \leqslant J_K$ is a subgroup such that

(a) $D \subseteq N_{L/K} J_L$,

(b) $K^\times D$ is dense in J_K,

then $L = K$.

Proof. If $L \supseteq L' \supseteq K$, then $D \subseteq N_{L/K} J_L \subseteq N_{L'/K} J_{L'}$. Thus we may assume L/K is cyclic. From local class field theory we know that the local norms $N_{L_w/K_v} L_w^\times$ are open in $K_v^\times$ which contains U_v for almost all v; so $N_{L/K} J_L$ and $K^\times N_{L/K} J_L$ are open, and hence closed in J_K. By assumption $K^\times N_{L/K} J_L$ is dense in J_K, so $J_K = K^\times N_{L/K} J_L$. By first inequality we obtain $n = 1$. □

Recall that in the Galois case an element $x = (x_v) \in J_K$ is in $N_{L/K} J_L$ if and only if it is a local norm everywhere, i.e. $x_v \in N_{L^v/K_v}(L^v)^\times$ for all $v \in M_K$.

Corollary 6.13.3. If $S \subseteq M_K$ is a finite set and L/K is a finite abelian extension, then $\mathrm{Gal}(L/K)$ is generated by the elements $\mathrm{Frob}_{L/K}(v)$ for $v \notin S$, i.e. the map $\mathrm{Frob}_{L/K} : I^S \to \mathrm{Gal}(L/K)$ is surjective.

Proof. Replacing S by $G.S$, we may assume S is G-invariant. Then the subgroup $G' \leqslant \mathrm{Gal}(L/K)$ generated by the $\mathrm{Frob}_{L/K}(v)$, $v \notin S$ is normal. Let M be the fixed field of G'. For $v \notin S$, the $\mathrm{Frob}_{L/K}(v)$ viewed in

$\mathrm{Gal}(M/K) \cong G/G'$ are all trivial, so for all $v \notin S$, $M_w = k_v$ if $w \in M_M$ is over v. Trivially every element of $K_v^\times$ is a norm of this extension.

Take $D = J_K^S$, the subgroup of ideles with $x_v = 1$ for $v \notin S$. Then $D \subseteq N_{M/K} J_M$, as stated right before the corollary. Now $K^\times J_K^S$ is dense in J_K; indeed, for $x = (x_v) \in J_K$, by weak approximation we can find $b \in K^\times$ such that b is closed to x_v for $v \in S$. Pick $y \in J_K^S$ with $by_v = x_v$ for $v \notin S$. Then by is closed to x in J_K. By Corollary 6.13.2 we have $M = K$ and thus $G' = G$. □

Corollary 6.13.4. If L is a nontrivial abelian extension of K, there are infinitely many primes v of K that do not split completely, i.e. $\mathrm{Frob}_{L/K}(v) \neq 1$.

Proof. Suppose there are only finitely such primes and let $S \subseteq M_K$ be a finite set containing those primes. Then $\mathrm{Gal}(L/K)$ is generated by $\mathrm{Frob}_{L/K}(v)$, $v \notin S$. But $\mathrm{Frob}_{L/K}(v) = 1$ for all $v \notin S$, so $\mathrm{Gal}(L/K)$ is trivial, i.e. $L = K$. □

6.9 Cohomology of Idele Class (II), The Second Inequality

Theorem 6.14. Let L/K be a Galois extension of degree n, with Galois group G. Then

(1) $\#\hat{H}^0(G, C_L)$ and $\#\hat{H}^2(G, C_L)$ divide n.

(2) $\#\hat{H}^1(G, C_L) = 0$.

Proof. The proof will be in several steps.

1° Suppose that the theorem has been proved when G is cyclic and n is prime. By Ugly Lemma, with $(\rho, q) = (1,0)$, $(0,1)$ it follows that $\#\hat{H}^0(G, C_L)$ divides n and $\hat{H}^1(G, C_L) = 0$. Using the triviality of $\hat{H}^1$, it follows again from Ugly Lemma, with $(\rho, q) = (1,2)$, that $\#\hat{H}^2(G, C_L) \mid n$.

To see how the condition (b) of Ugly Lemma is satisfied, if $H \trianglelefteq K \leqslant G$ with K/H cyclic of prime order, then L^H/L^K is cyclic with Galois group K/H. By hypothesis $\hat{H}^1(H, M) = 1$ and $\hat{H}^0(H, M) \mid [K : H]$, i.e. $\hat{H}^q(H, M) \mid [K : H]^\rho$ for $(\rho, q) = (1,0)$, $(0,1)$.

2° Now assume that G is cyclic of prime order; in this case we know that $\hat{H}^0 \cong \hat{H}^2$ and by the first inequality that $\#\hat{H}^0 = n\#\hat{H}^1$. So it suffices to show that $\#\hat{H}^0(G, C_L) = [C_K : N_{L/K} C_L]$ divides n.

(♠) We will make one assumption that in the function field case n is not equal to the characteristic of K (so that the Kummer theory is valid).

3° We now show that we may further assume that K contains the n-th roots of unity.

In fact, if we adjoin a primitive n-th root of unity ζ to K, we get an extension $K' = K(\zeta)$ whose degree m divides $(n-1)$, and so is prime to n. So

$$\begin{tikzcd}
L' = LK \arrow[r, dash, "n"] \arrow[d, dash, "m"'] & K' = K(\zeta) \arrow[d, dash, "m"] \\
L \arrow[r, dash, "n"'] & K
\end{tikzcd}$$

The degree of LK' over K' is n, and L and K' are linearly disjoint over K. So there is a commutative diagram with exact rows

$$\begin{tikzcd}
C_L \arrow[r] \arrow[d, "\mathrm{Con}"'] & C_K \arrow[r] \arrow[d, "\mathrm{Con}"'] & C_K/NC_L \arrow[r] \arrow[d, "\mathrm{Con}"'] & 0 \\
C_{L'} \arrow[r] \arrow[d, "N"'] & C_{K'} \arrow[r] \arrow[d, "N"'] & C_{K'}/NC_{L'} \arrow[r] \arrow[d, "N"'] & 0 \\
C_L \arrow[r] & C_K \arrow[r] & C_K/NC_L \arrow[r] & 0
\end{tikzcd}$$

Here Con is the conorm map and $N \circ \mathrm{Con}$ is simply raising to the m-th power. The group C_K/NC_L is torsion in which each element has order n, for if $a \in C_K$, then $a^n = N_{L/K}(a) \in NC_L$. Thus

$$N_{K'/K}\mathrm{Con}_{K'/K} : C_K/NC_L \to C_K/NC_L$$

is surjective since $\gcd(n, m) = 1$. Hence $N_{K'/K} : C_{K'}/NC_{L'} \to C_K/NC_L$ is surjective; so if the index $[C_{K'} : NC_{L'}]$ divides n, so does $[C_K : NC_L]$.

4° We are thus reduced to the case where n is a prime and K contains the n-th roots of unity. In fact we call prove directly in this case the more general result.

Lemma Let K contain the n-th roots of unity and L/K be an abelian extension of prime exponent n, with say $\mathrm{Gal}(L/K) =: G \cong (\mathbb{Z}/n\mathbb{Z})^r$. Then $[C_K : N_{L/K}C_L]$ divides $[L : K] = n^r$.

Although, as we have just seen, the case of arbitrary r does follow from the case $r = 1$, yet the method to be used does no simplify at all if one puts $r = 1$, and some of the construction in the proof are useful for large r.

By Kummer theory, we know that $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$ for some $a_1, \ldots, a_r \in K$. Take S to be a finite set of (bad) primes, such that

(i) S contains all archimedean primes,

(ii) S contains all divisors of n,

(iii) $J_K = K^\times J_{K,S}$,

(iv) S contains all factors for the numerators and denominators of any a_i.

Condition (iv) just means that all the a_i are S-units, that is, they belong to $K_S := K \cap J_{K,S}$: they are units for all $v \notin S$.

Write $M := K(\sqrt[n]{K_S})$ for the field obtained from K by adjoining n-th roots of all S-units. By the unit theorem the group K_S has a finite basis, so this extension M/K is finite, and M is unramified outside S by Kummer theory and condition (ii), (iv) (we know divisors of the discriminant of M/K). Now $M \supseteq L \supseteq K$ and

$$K_S = (M^\times)^n \cap K_S \supseteq (L^\times)^n \cap K_S \supseteq (K^\times)^n \cap K_S = K_S^n$$

By Kummer theory with $[M : K] = n^t$, $[L : K] = n^r$ and $[M : K] = n^s$, we have

$$[K_S : (L^\times)^n \cap K_S] = n^t,\ [(L^\times)^n \cap K_S : K_S^n] = n^r \text{ and } [K_S : K_S^n] = n^s \tag{*}$$

respectively. We claim that $s = \#S$. By unit theorem, there are $\#S - 1$ fundamental units, and the roots of unity include the n-th roots of unity; so $K_S \cong \mathbb{Z}^{\#S-1} \times$(cyclic group of order divisible by n) and

$$[K_S : K_S^n] = n^{\#S} = n^s \text{ where } s = t + r$$

We recall we want to show that $[C_K : N_{L/K}C_L]$ divides n^r, i.e. divides $[(L^\times)^n \cap K_S : K_S^n]$. So we need to show that $N_{L/K}C_L$ is fairly large — we have to provide a lot of norms.

If w is a prime of L above a $v \notin S$, then $\operatorname{Frob}_{M/L}(w)$ is well-defined for M/K is unramified outside S. By Corollary 6.13.3, the $\operatorname{Frob}_{M/L}(w)$ generates $\operatorname{Gal}(M/L)$. Choose $w_1, \ldots, w_t$ so that $\operatorname{Frob}_{M/L}(w_i)$ $(i = 1, \ldots, t)$ are a basis for $\operatorname{Gal}(M/L)$, and let $v_1, \ldots, v_t$ be primes of K below them. We assert that $\operatorname{Frob}_{M/L}(w_i) = \operatorname{Frob}_{M/K}(v_i)$ (the latter is well-defined for M/K is unramified at each of them). The M/K decomposition group $\operatorname{Gal}(M^v/K_v)$ is a cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^s$, so is either of prime order n or trivial. The w's were chosen so that the $\operatorname{Frob}_{M/L}(w)$ were nontrivial, so that $\operatorname{Gal}(M^w/L_w) \neq 0$; so that L/K decomposition group

$$\operatorname{Gal}(L_w/K_v) \cong \operatorname{Gal}(M^v/K_v)/\operatorname{Gal}(M^w/L_w)$$

is trivial, i.e. v splits completely in L. Therefore $\operatorname{Gal}(M^v/K_v) = \operatorname{Gal}(M^w/L_w)$ and it is generated by the $\operatorname{Frob}_{M/L}(v_i) = \operatorname{Frob}_{M/K}(w_i)$. Notice also that we have $L_{w_i} = K_{v_i}$ for all $i = 1, \ldots, t$.

Write $T = \{v_1, \ldots, v_t\} \subseteq M_K$. We claim that

$$(L^\times)^n \cap K_S = \{a \in K_S \mid a \in K_v^n \text{ for all } v \in T\} \tag{$\diamond$}$$

In fact, since $L_w = K_v$ for all $v \in T$ and w above v, it follows trivially that $(L^\times)^n \cap K_S$ is contained in the right-hand side. Conversely, if $a \in K_S$, then $\sqrt[n]{a} \in M$. If further $a \in K_v^n$ for all $n \in T$, then $\sqrt[n]{a} \in K_v$ for all $v \in T$, and so is left fixed by all $\operatorname{Frob}_{M/K}(v) = \operatorname{Frob}_{M/L}(v)$; these generate $\operatorname{Gal}(M/L)$ so $\sqrt[n]{a} \in L$. This proves $(\diamond)$.

Let

$$E = \prod_{v \in S} (K_v^\times)^n \times \prod_{v \in T} K_v^\times \times \prod_{s \notin S \cup T} U_v$$

where U_v is the set of v-unit in K_v; so $E \subseteq J_{K,S\cup T}$. Also $E \subseteq N_{L/K} J_L$ – for every element of $(K_v^\times)^n$ is a norm, since $K_v^\times / N L_w^\times \cong \mathrm{Gal}(L_w/K_v)$, which is killed by n; we have $K_v^\times = L_w^\times$ for all $v \in T$, and so all the elements of these $K_v^\times$ are norms, and the elements of U_v are all norms for v unramified.

Now

$$[C_K : N_{L/K} C_L] = [J_K : K^\times N_{L/K} J_L]$$

divides $[J_K : K^\times E]$ because $E \subseteq N_{L/K} J_L$. The set S was chosen (condition (ii)) so that

$$J_K = K^\times J_{K,S} = K^\times J_{K,S\cup T}$$

therefore $[C_K : N_{L/K} C_L]$ divides $[K^\times J_{K,S\cup T} : K^\times E]$. A general formula for indices of group is

$$[CA : CB][C \cap A : C \cap B] = [A : B]$$

so to prove Lemma it will be enough to show that (with $A = J_{K,S\cup T}$, $E = B$, $C = K^\times$)

$$\frac{[J_{K,S\cup T} : E]}{[K_{S\cup T} : K \cap E]} = n^r \tag{$\clubsuit$}$$

where $K_{S\cup T} = K^\times \cap J_{K,S\cup T}$.

First we calculate $[J_{K,S\cup T} : E]$.

$$J_{K,S\cup T} = \prod_{v \in S} K_v^\times \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} U_v$$

so $[J_{K,S\cup T} : E] = \prod_{v \in S} [K_v^\times : (K_v^\times)^n]$ From Proposition 5.6 we see that the "trivial action" Herbrand quotient $h(K_v^\times) = \dfrac{n}{|n|_v}$, where $|\cdot|_v$ denotes the normed absolute value. But also $h(K_v^\times) = \dfrac{[K_v^\times : (K_v^\times)^n]}{n}$ because the n-th roots of unity are in $K_v^\times$. This means that $[K_v^\times : (K_v^\times)^n] = \dfrac{n^2}{|n_v|}$, and

$$[J_{K,S\cup T} : E] = n^{2s} \prod_{v \in S} |n|_v^{-1} = n^{2s} \tag{$\heartsuit$}$$

by product formula and that $|n|_v = 1$ if $v \notin S$.

We will also need in a moment the formula

$$[U_v : U_v^n] = \frac{n}{|n|_v}$$

which follows from the fact that $h(U_v) = \dfrac{1}{|n|_v}$ (for $K^\times \cong U \times \mathbb{Z}$).

By ($\heartsuit$) we see to prove ($\clubsuit$), it will be enough to show that

$$[K_{S\cup T} : K^\times \cap E] = n^{2s-r} = n^{s+t}$$

As in ($*$), replacing S by $S\cup T$, we have $[K_{S\cup T} : K^n_{S\cup T}] = n^{s+t}$. Also $K^\times \cap E \supseteq K^n_{S\cup T}$, so it will be enough to show that $K^\times \cap E = K^n_{S\cup T}$.

It remains to prove

$$K^\times \cap E \subseteq K^n_{S\cup T}$$

and this will result from the following lemma.

Lemma 6.15. Let K contain the n-th roots of unity. Let S be a subset of M_K satisfying the conditions (i)$\sim$(iv), and let T be a set of primes disjoint from S, and independent for K_S in the sense that the map $K_S \to \prod_{v\in T} U_v/U_v^n$ is surjective.

Suppose that $b \in K^\times$ is an n-th power in S, arbitrary in T, and a unit outside $S\cup T$. Then $b \in (K^\times)^n$.

Proof. Consider the extension $K' = K(\sqrt[n]{b})$; it will be enough to deduce that $K' = K$. Put

$$D = \prod_{v\in S} K_v^\times \times \prod_{v\in T} U_v^n \times \prod_{v\notin S\cup T} U_v$$

By argument similar to the ones used before (next to the proof of ($\diamond$)), $D \subseteq N_{K'/K} J_{K'}$. By Corollary 6.13.2 it is sufficient to show $K^\times D = J_K$. But by hypothesis, the map $K_S \to \prod_{v\in T}(U_v/U_v^n) \cong J_{K,S}/D$ is surjective. Hence $J_{K,S} = K_S D$ and $J_K = K^\times J_{K,S} = K^\times D$ as required. □

To deduce $K^\times \cap E \subseteq K^n_{S\cup T}$ from Lemma, we have to check that T is independent for S in the sense of Lemma. Let H denote the kernel of the map $K_S \to \prod_{v\in T} U_v/U_v^n$. To prove that he map is surjective it suffices tot show that $[K_S : H] = \prod_{v\in T}[U_v : U_v^n]$. The latter product is just n^t (right below ($\heartsuit$)), because $|n|_v = 1$ for $v \in T$. On the other hand, by ($\diamond$) we have $H = K_S \cap (L^\times)^n$, and consequently $[K_S : H] = n^t$ by ($*$).

The proof of the theorem is now complete.

□

Remark 6.16. Even the case of the Lemma 6.15 with $T = \varnothing$ is interesting: if S satisfies conditions (i), (ii) and (iii), then an S-unit which is a local n-th power at all primes in S is an n-th power.

Corollary 6.16.1. If L/K is abelian with Galois group G, and there is an Artin map $\psi : \hat{H}^0(G, C_L) = C_K/NC_L \to G$, then ψ must be an isomorphism.

Proof. From Corollary 6.13.3 we know ψ is surjective. Now $\#\hat{H}^0(G, C_L) \leqslant \#G$ so ψ must be an isomorphism. □

Corollary 6.16.2. Let n be a prime and let K be a field, not of characteristic n, containing the n-th roots of unity. Let S be a finite set of primes of K satisfying the conditions (i), (i), (iii), and let $M = K(\sqrt[n]{K_S})$. Then if the reciprocity law holds for M/K, we have

$$K^\times N_{M/K} J_M = K^\times E, \text{ where } E = \prod_{v \notin S} (K_v^\times)^n \times \prod_{s \notin S} U_v$$

Proof. Consider the case $L = M$ of the proof of Theorem 6.14 (so that $T = \varnothing$, $t = 0$ and $s = r$). Then the E of that proof is as given above, and $E \subseteq N_{M/K} J_M$. By (♣) with $L = M$, we have $[J_K : K^\times E] = n^s = [M : K]$. On the other hand, if the reciprocity law holds, we know that

$$[C_K : N_{M/K} C_M] = [J_K : K^\times N_{M/K} J_M] = n^s$$

This shows the result. □

Corollary 6.16.3 (Albert-Brauer-Hasse-Noether)**.** Let L/K be a finite (not necessarily abelian) Galois extension. Then we have an injection

$$0 \to H^2(G, L^\times) \to \bigoplus_{v \in M_K} H^2(G^v, (L^v)^\times)$$

In other words, a central simple algebra over K splits over K if and only if it splits locally everywhere.

Proof. Since $H^1(G, C_L) = 0$, the exact sequence $0 \to L^\times \to J_L \to C_L \to 0$ gives rise to a very short exact sequence $0 \to H^2(G, L^\times) \to H^2(G, J_L)$. Now $H^2(G, J_L) = \bigoplus_{v \in M_K} H^2(G^v, (L^v)^\times)$ by Proposition 6.10, so

$$0 \to H^2(G, L^\times) \to \bigoplus_{v \in M_K} H^2(G^v, (L^v)^\times)$$

□

Corollary 6.16.4 (Hasse norm theorem)**.** If $a \in K^\times$ and L/K is cyclic, then $a \in N_{L/K} L^\times$ if and only if $a \in N_{L^v/K_v}(L^v)^\times$ for all $v \in M_K$.

Proof. Since $\mathrm{Gal}(L/K)$ is cyclic, $\hat{H}^0 \cong \hat{H}^2$, so the result follows from Corollary above. □

Specializing further, take G of order 2, so $L = K(\sqrt{b})$.

$$N_{L/K}(x + y\sqrt{b}) = x^2 - by^2$$

so (if the characteristic if not 2) we deduce that a has the form $x^2 - b^2$ if and only if it has this form locally everywhere. It follows that a quadratic form $Q(x, y, z)$ in three variables over K has a non-trivial zero in K if and only if it has a non-trivial zero in every completion of K. Extending to n-variables, we may obtain the Hasse-Minkowski theorem.

One may consider the general problem, "if $a \in K^\times$ and $a \in NL^{v\times}$ for all v, is $a \in NL^\times$?" Unfortunately, the answer is not always yes!

We return to the sequence

$$0 \to H^2(G, L^\times) \to \bigoplus_{v \in M_K} H^2(G^v, (L^v)^\times)$$

We write $H^2(L/K)$ for $H^2(G, L^\times)$ and $H^2(L^v/K_v)$ for $H^2(G^v/L^{v\times})$. Thus it becomes

$$0 \to H^2(L/K) \to \bigoplus_{v \in M_K} H^2(G^v/L^{v\times})$$

From local class field theory, $H^2(G^v/L^{v\times})$ is cyclic of order $n_v = [L^v : K_v]$, with a canonical generator. Thus

$$H^2(G, J_L) = \bigoplus_{v \in M_K} H^2(G^v/L^{v\times}) \cong \bigoplus_{v \in M_K} \left(\frac{1}{n_v} \mathbb{Z}/\mathbb{Z} \right)$$

and

$$0 \to H^2(L/K) \to \bigoplus_{v \in M_K} \left(\frac{1}{n_v} \mathbb{Z}/\mathbb{Z} \right) \tag{$\diamond$}$$

If $\alpha \in \bigoplus_{v \in M_K} \left(\frac{1}{n_v} \mathbb{Z}/\mathbb{Z} \right)$, or $\alpha \in H^2(L/K)$, we can find its local invariant $\operatorname{inv}_v(\alpha)$ (more precisely $\operatorname{inv}_v(j_v(\alpha))$, where j_v is the projection on the v-component of α), which will determine it precisely.

We are interested in the functorial properties of the map inv_v. Let $L \supseteq K \supseteq K$ be finite Galois extensions withe groups

$$G' = \operatorname{Gal}(L'/K)$$

and

$$G = \operatorname{Gal}(L/K) \cong G'/H$$

where $H = \operatorname{Gal}(L'/L)$. If $\alpha \in H^2(G, J_L)$, then $\inf \alpha \in H^2(G', J_{L'})$, and

$$\operatorname{inv}_v(\inf \alpha) = \operatorname{inv}_v \alpha$$

Indeed, choosing a prime w' of L' above a prime w of L above v, one reduces this to the corresponding local statement for the tower $L'_{w'} \supseteq L_w \supseteq K_v$.

Thus nothing changes under inflation so we can pass in an invariant manner to the Brauer group of K, and get the **local invariants** for $\alpha \in \operatorname{Br}(K) = H^2(\overline{K}, K)$, where $\overline{K}$ is the algebraic closure of K, and more generally for

$$\alpha \in H^2(\operatorname{Gal}(\overline{K}/K), J_{\overline{K}}) = \varinjlim_L H^2(\operatorname{Gal}(L/K), J_L)$$

where $J_{\overline{K}} := \varinjlim_L J_L$, by definition, the limits being taken over all finite Galois extensions L of K.

If now $\alpha \in H^2(G', J_{L'})$, then $\operatorname{res}^{G'}_H \alpha \in H^2(H, J_{L'})$ and

$$\operatorname{inv}_w(\operatorname{res}^{G'}_H \alpha) = n_{w/v} \operatorname{inv}_v \alpha \tag{$\spadesuit$}$$

where $w \in M_L$ lies above $v \in M_K$ and $n_{w/v} = [L_w : K_v]$. This again immediately reduces to the local case. Moreover, L/K need not be Galois here.

Finally we mention the result for corestriction. Again L/K need not be Galois. If $\alpha' \in H^2(H, J_{L'})$, then $\operatorname{cores}_H^{G'} \alpha' \in H^2(G', J_{L'})$ and

$$\operatorname{inv}_v(\operatorname{cores}_H^{G'} \alpha') = \sum_{w|v} \operatorname{inv}_w \alpha'$$

where the sum is over all primes $w \in M_L$ over $v \in M_K$.

Corollary 6.16.5. Let $\alpha \in \operatorname{Br}(K)$ or $H^2(\operatorname{Gal}(\overline{K}/K), J_K)$, where $\overline{K}$ is the separable algebraic closure of K. Let L be finite Galois over K in $\overline{K}$. Then $\operatorname{res}_L^K(\alpha) = 0$ if and only if $[L_w : K_v] \operatorname{inv}_v \alpha = 0$ for every w over v (this is only a finite condition, since almost all the $\operatorname{inv}_v \alpha$ are zero).

Proof. There is an exact sequence

$$0 \longrightarrow H^2(L/K) \xrightarrow{\text{inf}} \operatorname{Br}(K) \xrightarrow{\text{res}} \operatorname{Br}(L) \tag{$\clubsuit$}$$

Hence TFAE:

- $\operatorname{res}_L^K(\alpha) = 0$.

- $\alpha \in H^2(L/K)$ by ($\clubsuit$).

- $\operatorname{inv}_w(\operatorname{res}_L^K \alpha) = 0$ for all $w \mid v$, by ($\diamond$).

- $[L_w : K_v] \operatorname{inv}_v \alpha = 0$ for all $w \mid v$, by ($\spadesuit$).

□

6.10 Proof of the Reciprocity Law

Let L/K be a finite abelian extension with Galois group G. Let the local Artin maps be denoted by $\theta_v : K_v^\times \to G^v$; we define the map

$$\begin{aligned} \theta : J_K &\longrightarrow G = \operatorname{Gal}(L/K) \\ x &\longmapsto \prod_{v \in M_K} \theta_v(x_v) \end{aligned}$$

This is a proper definition, for $\theta_v(x_v) = F_{L^v/K_v}(v)^{v(x_v)}$ ($v(x_v)$ being the normalized valuation of x_v) when v is unramified, and $v(x_v) = 0$ if $x_v \in U_v$ so that $\theta_v(x_v) = 0$ for all but finitely many v. Also θ is continuous.

Take $S_o \subseteq M_K$ as the set of archimedean primes plus the primes ramified in L/K; then $x \in J_K^{S_o}$ implies $\theta = F((x)^{S_o})$. Thus θ satisfies two of the conditions for an Artin map ((i) and (iii) in Corollary 6.3.1). It remains to prove

$$\theta(a) = \prod_{v \in M_K} \theta_v(a) = 1$$

for all $a \in K^\times$. We will simultaneously prove the following two theorems.

Theorem 6.17. Every finite abelian extension L/K satisfies the reciprocity law, and the Artin map $\theta : J_K \to \mathrm{Gal}(L/K)$ is given by $\theta = \prod_v \theta_v$.

Theorem 6.18. If $\alpha \in \mathrm{Br}(K)$, then $\sum_{v \in M_k} \mathrm{inv}_v(\alpha) = 0$. (It is a finite sum, for $\mathrm{inv}_v(\alpha) := \mathrm{inv}_v(j_v\alpha) = 0$ for all but finitely many v.)

Logically, the proof is in four main steps.

1° Prove Theorem 6.17 for an arbitrary finite cyclotomic extension L/K.

2° Deduce Theorem 6.18 for α split by a cyclic cyclotomic extension.

3° Deduce Theorem 6.18 for arbitrary $\alpha \in \mathrm{Br}(K)$.

4° Deduce Theorem 6.17 for all abelian extensions.

We first clarify the relation between 6.17 and 6.18 and deduce 2° that 6.17 implies 6.18 for cyclic extensions and 4° that 6.18 implies 6.17 for arbitrary abelian extensions. Then we will prove 1° directly, and finally push through 3°, by showing that every element of $\mathrm{Br}(K)$ has a cyclotomic splitting field.

6.17 is about $\hat{H}^0$ and 6.18 is about H^2, so we need a lemma connecting them. Let L/K be a finite abelian extension with Galois group G. Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$ be a character, where $\mathbb{Q}/\mathbb{Z}$ is a trivial G-module. If $v \in M_K$, denote by χ_v the restriction to the decomposition group $G^v = \mathrm{Gal}(L^v/K_v)$. Let δ be the connecting homomorphism

$$\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z})$$

If $x = (x_v) \in J_K$, let $\overline{x}$ be its image in $J_K/N_{L/K}J_L \cong \hat{H}^0(G, J_L)$. Then the cup product $\overline{x}.\delta_\chi \in H^2(G, J_L)$.

Lemma 6.19. For each v we have

$$\mathrm{inv}_v(\overline{x} \cup \delta_\chi) = \chi_v(\theta_v(x_v))$$

and so

$$\sum_v \mathrm{inv}_v(\overline{x} \cup \delta_v) = \chi(\theta(x))$$

Proof. The projection $j_v : J_L \to (L^v)^\times$ induces a map

$$j_v \,\mathrm{res}^G_{G_v} : H^2(G, J_L) \longrightarrow H^2(G_v, J_L) \longrightarrow H^2(G_v, (L^v)^\times)$$

and as restriction commutes with the cup product, so

$$\begin{aligned} \mathrm{inv}_v(\overline{x} \cup \delta_\chi) &\overset{6.9,6.10}{:=} \mathrm{inv}_v(j_v \,\mathrm{res}^G_{G_v}(\overline{x} \cup \delta_\chi)) \\ &= \mathrm{inv}_v(\overline{x}_v \cup \delta_{\chi_v}) \\ &= \chi_v(\theta_v(x_v)) \end{aligned}$$

Then

$$\chi(\theta(x)) = \chi\left(\prod_v \theta_v(x_v)\right) = \sum_v \chi_v(\theta_v(x_v)) = \sum_v \mathrm{inv}_v(\overline{x} \cup \delta_\chi)$$

□

To check 4°, apply the lemma with $x = a \in K^\times \subseteq J_K$. Denote by $\tilde{a}$ is image of a in $\hat{H}^0(G, L^\times)$. Then $\tilde{a} \cup \delta_\chi \in \hat{H}^2(G, L^\times) \subseteq \mathrm{Br}(K)$, as we need. The image of $\tilde{a} \cup \delta_\chi$ is $H^2(G, J_L)$ is $\overline{a} \cup \delta_\chi$, where $\overline{a}$ is the image of a in $\hat{H}^0(G, J_L)$, by functoriality of cup product, and by the lemma above, $\sum_v \mathrm{inv}_v(\overline{a} \cup \delta_\chi) = \chi(\theta(a))$; so if 6.18 is true for all $\alpha \in \mathrm{Br}(K)$, it follows that $\chi(\theta(a)) = 0$, and since it is true for all χ, thus $\theta(a) = 0$. This is 6.17.

To check 2°, take L/K cyclic. Choose $\chi : G \to \mathbb{Q}/\mathbb{Z}$ as a generating character, i.e. an injection. Then cupping with δ_χ gives an isomorphism $\hat{H}^0 \xrightarrow{\sim} \hat{H}^2$ (Corollary 4.10.2), so every element of $H^2(\mathrm{Gal}(L/K), L^\times)$ is of the form $\tilde{a} \cup \delta_\chi$. If 6.17 is true, then by the above lemma

$$\sum_v \mathrm{inv}_v(\overline{a} \cup \delta_\chi) = \chi(\theta(a)) = 0$$

for all $a \in K^\times$, which is 6.18.

We start to prove 1° in number field case. Let L/K be a finite cyclotomic extension; then $L \subseteq K(\zeta)$ for some root of unity ζ. We make some reduction.

- It suffices to consider the case $L = K(\zeta)$. Indeed, set $M = K(\zeta)$. Since the diagram

$$\begin{tikzcd}
(K^v)^\times \arrow[r, "\theta_{v,M}"] \arrow[d, equal] & \mathrm{Gal}(M^v/K_v) \arrow[d] \\
(K^v)^\times \arrow[r, "\theta_{v,L}"] & \mathrm{Gal}(L^v/K_v)
\end{tikzcd}$$

  commutes, if $\prod_{v \in M_K} \theta_{v,M}(a) = 1$, then obviously $\prod_{v \in M_K} \theta_{v,L}(a) = 1$.

- It suffices to consider the case $K = \mathbb{Q}$. Put $M = K(\zeta)$ and $L = \mathbb{Q}(\zeta)$; then $M = LK$, and the diagram

$$\begin{tikzcd}
J_K \arrow[r, "\theta"] \arrow[d, "N_{K/\mathbb{Q}}"'] & \mathrm{Gal}(M/K) \arrow[d, "i"] \\
J_\mathbb{Q} \arrow[r, "\theta"] & \mathrm{Gal}(L/\mathbb{Q})
\end{tikzcd}$$

  commutes for $(N_{K/\mathbb{Q}}x)_p = \prod_{v|p} N_{K_v/\mathbb{Q}_p} x_v$, and the diagram

$$\begin{tikzcd}
K_v \arrow[r] \arrow[d, "N_{K_v/\mathbb{Q}_p}"'] & \mathrm{Gal}(M^v/K_v) \arrow[d, "i"] \\
\mathbb{Q}_p \arrow[r] & \mathrm{Gal}(K_v/\mathbb{Q}_p)
\end{tikzcd}$$

commutes whenever $v \mid p$. Thus $i\theta'(x) = \theta N x$ for all $x \in J_K$, and so, in particular, $i\theta' a = \theta N a$ for all $a \in K$. If 6.17 is true for $L/\mathbb{Q}$, then $\theta b = 1$ for all $b \in \mathbb{Q}$, and hence $\theta' a = 1$ for all $a \in K$, for i is injective.

Hence it suffices to deal with the case when $L/\mathbb{Q}$ is cyclotomic. We give two proofs.

First proof

Second proof We proceed entirely locally without using any result of the early section, but using the explicit local computation of the norm residue symbol in cyclotomic extension, due originally to Dwork.

Let ζ be a root of unity. From local class field theory we know

- $\zeta^{\theta_\infty(x)} = \zeta^{\mathrm{sign}(x)}$ for all $x \in \mathbb{R}^\times$.
- $\zeta^{\theta_p(p^v u)} = \begin{cases} \zeta^{p^v} & \text{, if } \zeta \text{ has order prime to } p \\ (\zeta^u)^{-1} & \text{, if } \zeta \text{ has } p\text{-power order} \end{cases}$ if $x = p^v u \in \mathbb{Q}_p^\times$ with $u \in \mathbb{Z}_p^\times$ and $v \in \mathbb{Z}$.

We need to check that $\prod_p \theta_p(a) = 1$ for all $a \in \mathbb{Q}^\times$, and to do this it is sufficient to prove

- $\prod_p \theta_p(q) = 1$ for all primes $q > 0$;
- $\prod_p \theta_p(-1) = 1$.

Furthermore, it is enough to consider the effect on ζ, and ℓ-th power root of unity (ℓ a prime). From above we know

$$\zeta^{\theta_p(-1)} = \begin{cases} \zeta^{-1} & , p = \infty \\ \zeta^{-1} & , p = \ell \\ \zeta & , p \neq \infty, \ell \end{cases} \qquad \zeta^{\theta_p(q)} = \begin{cases} \zeta & , p = q = \ell \\ \zeta^q & , p = q \neq \ell \\ \zeta^{q^{-1}} & , p = \ell \neq q \\ \zeta & , p \neq q,\ p \neq \ell \text{ (including the case } p = \infty) \end{cases}$$

Note that the Galois group is abelian.

Finally, we deal with 3° in number field case. It is enough to show that every element of $\mathrm{Br}(K)$ has a cyclic cyclotomic splitting field; in other words, for every $\alpha \in \mathrm{Br}(K)$ there is a cyclic cyclotomic extension L/K such that for every $v \in M_K$ the local degree $[L^v : K_v]$ is a multiple of the denominator of $\mathrm{inv}_v(\alpha)$ (Corollary 6.16.5). Now $\mathrm{inv}_v(\alpha) = 0$ for all but a finite number of primes and so we need only prove the

Lemma 6.20. Given a number field K, a finite set of primes $S \subseteq M_K$ and a positive integer m, there exists a cyclic, cyclotomic extension L/K whose local degrees are divisible by m at the non-archimedean primes v of S and divisible by 2 at real archimedean primes v of S (in other words, L is complex).

Proof. It suffices to construct L in the case $K = \mathbb{Q}$. Indeed, if we can find $L/\mathbb{Q}$ such that L is complex and $m[K : \mathbb{Q}]$ divides all local degrees at non-archimedean $p \in S'$, where $S' \subseteq M_{\mathbb{Q}}$ consists of primes of $\mathbb{Q}$ lying below those in S, then $m[K : \mathbb{Q}]$ divides $[L^p : Q_p] = [L^v : K_v][K_v : Q_p]$ for some $S \ni v \mid p$; this implies $m \mid [L^v : K_v]$ as wanted.

Now take $r \gg 0$ and q an odd prime. The extension $L(q) = \mathbb{Q}(\sqrt[q^r]{1})$ has a Galois group $\mathrm{Gal}(L(q)/\mathbb{Q}) \cong \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/q^r\mathbb{Z}$, so it has a subextension $L'(q)$ which is a cyclic cyclotomic over $\mathbb{Q}$ of degree q^{r-1}. Now

$$[L(q) : L'(q)] = q - 1$$

and so on localizing at a fixed prime $p \neq \infty$ of $\mathbb{Q}$ we have

$$[L(q)^{(p)} : L'(q)^{(p)}] \leqslant q - 1$$

Note that $\lim\limits_{r\to\infty}[L(q)^{(p)} : \mathbb{Q}_p] = \infty$; this follows for example from the fact that each finite extension of $\mathbb{Q}_p$ contains only a finite number of roots of unity. It follows that $\lim\limits_{r\to\infty}[L'(q)^{(p)} : \mathbb{Q}_p] = \infty$. Therefore, since $[L'(q)^{(p)} : \mathbb{Q}_p]$ is always a power of q, it is divisible by a sufficiently large power of q if we take r large enough.

Now let $q = 2$ and put $L(2) = \mathbb{Q}(\sqrt[2^r]{1})$; $\mathrm{Gal}(L(2)/\mathbb{Q}) \cong \{\pm 1\} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$. Let ζ be a primitive 2^r-th root of unity, set $\xi = \zeta - \zeta^{-1}$ and $L'(2) = \mathbb{Q}(\xi)$. The automorphisms of $\mathbb{Q}(\zeta)/\mathbb{Q}$ are of the form $\sigma_\mu : \zeta \mapsto \zeta^\mu$ for μ odd, and $\sigma_\mu(\xi) = \zeta^\mu - \zeta^{-\mu}$. Since $\zeta^{2^{r-1}} = -1$, one sees that $\sigma_{-\mu+2^{r-1}}(\xi) = \sigma_\mu(\xi)$; since either μ or $-\mu + 2^{r-1}$ is $\equiv 1 \pmod 4$, this implies that the automorphism of $\mathbb{Q}(\xi)/\mathbb{Q}$ are induced by those σ_μ where $\mu \equiv 1 \pmod 4$ and that they form a cyclic group of order 2^{r-2}. Also, since $\sigma_{-1}\xi = -\xi$, $\mathbb{Q}(\xi)$ is not real, and so its local degree at an infinite real prime is 2.

Now $[L(2) : L'(2)] = 2$ and the same argument as above shows that for $p \neq \infty$ we can make $[L'(2)^{(p)} : \mathbb{Q}_p]$ divisible by as large a power of 2 as we like by taking r large enough.

If now the prime factors of m are $q_1, \dots, q_n$ and possibly 2, then for large enough r, the compositum of $L'(q_1), \dots, L'(q_n)$ and possibly $L'(2)$ is a complex cyclic cyclotomic extension of $\mathbb{Q}$ whose local degree over $\mathbb{Q}_p$ is divisible by m for all $p \in S$. □

Turn to the function field cases. The proof is on the same line, but the special role of "cyclic cyclotomic extensions" in the proof is taken over by "constant field extensions".

3° The proof goes through if we replace "cyclic cyclotomic extensions" by "constant field extensions"; we have only to take for the L in the lemma the constant field extension whose degree is m times the least common multiple of the degrees of the primes in S.

1° We check the reciprocity law directly for constant field extensions. Denote by σ the Frobenius automorphism of $\overline{k}/k$, where k is the constant field of K. Then for each prime v of K, the effect of $F(v)$ on $\overline{k}$ is just $\sigma^{\deg v}$, where $\deg v := [k(v) : k]$. Hence the effect on $\overline{k}$ of $\theta(a)$ is

$$\prod_v \sigma^{v(a)\deg v} = \sigma^{\sum_v v(a)\deg v} = 1$$

for all $a \in K^\times$. The last equality results from the fact $\sum_v v(a) \deg v = 0$, which is equivalent to saying that the number of zeros of a rational function equals the number of poles.

Lemma 6.21. Let q be a power of some prime and let $n \in \mathbb{N}$. Then $\mathbb{F}_q[t] \to \mathbb{F}_{q^n}[t]$ is unramified.

Proof. Let $f \in \mathbb{F}_{q^n}[t]$ be irreducible and let $g \in \mathbb{F}_q[t]$ be such that $g\mathbb{F}_q[t] = f\mathbb{F}_{q^n}[t] \cap \mathbb{F}_q[t]$; then g is irreducible. Say $g = fh$ for some $h \in \mathbb{F}_{q^n}[t]$. Since g is irreducible over $\mathbb{F}_q$, g is separable, implying f and h are coprime. This proves $\mathbb{F}_{q^n}[t]/g\mathbb{F}_{q^n}[t] = \mathbb{F}_{q^n}[t]/f\mathbb{F}_{q^n}[t]$. □

Lemma 6.22. Let k be a finite field and $a \in k(t)$. Then $\sum_v v(a) \deg v = 0$.

Proof. Suppose $a = g/h \neq 0$ with $g, h \in k[t]$ coprime and write the irreducible decomposition $a = f_1^{r_1} \cdots f_n^{r_n}$ of a. Each f_i correspond to distinct place v_i, and $\deg v_i = \deg f$. On the other hand, there is a place v_∞ corresponding to t^{-1} with $\deg v = 1$ and $v(a) = \deg h - \deg g$. Hence

$$\sum_v v(a) \deg v = (\deg h - \deg g) + \sum_{i=1}^n r_i \deg f_i$$

Note $\deg g = \sum_{i:r_i>0} r_i \deg f_i$ and $\deg h = \sum_{i:r_i<0} r_i \deg f_i$ so that the above sum $= 0$. □

6.11 Cohomology of Idele Class (III), The Fundamental Class

Let $K \subseteq L \subseteq E$ be finite Galois extensions of K. Then we have a following exact commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & H^2(L/K, L^\times) \arrow[r] \arrow[d, "\mathrm{inf}"] & H^2(L/K, J_L) \arrow[r] \arrow[d, "\mathrm{inf}"] & H^2(L/K, C_L) \arrow[d, "\mathrm{inf}"] \\
0 \arrow[r] & H^2(E/K, E^\times) \arrow[r] \arrow[d, "\mathrm{res}"] & H^2(E/K, J_E) \arrow[r] \arrow[d, "\mathrm{res}"] & H^2(E/K, C_E) \arrow[d, "\mathrm{res}"] \\
0 \arrow[r] & H^2(E/L, E^\times) \arrow[r] & H^2(E/L, J_E) \arrow[r] & H^2(E/L, C_E)
\end{tikzcd}$$

where we have written $H^2(L/K, L^\times)$ for $H^2(\mathrm{Gal}(L/K), L^\times)$, etc. We elaborate on the morphisms involved.

- The vertical lines are inflation-restriction sequences (c.f. Proposition 6.10.(a) and Proposition 6.11) These are exact for Hilbert 90, Corollary 6.10.1.(a) and Theorem 6.14.(2).

- The horizontal lines result from the exact sequences $0 \to L^\times \to J_L \to C_L \to 0$, etc, and are exact by Theorem 6.14.(2).

- The diagram commutes by functoriality.

We pass to limit and let $E \to \overline{K}$, where $\overline{K}$ is the separable algebraic closure of K, to obtain the new commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & H^2(L/K, L^\times) \arrow[r, "\gamma_1"] \arrow[d] & H^2(L/K, J_L) \arrow[r, "\varepsilon_1"] \arrow[d] & H^2(L/K, C_L) \arrow[d] \\
0 \arrow[r] & H^2(K, \overline{K}^\times) \arrow[r, "\gamma_2"] \arrow[d] & H^2(K, J_{\overline{K}}) \arrow[r, "\varepsilon_2"] \arrow[d] & H^2(K, C_{\overline{K}}) \arrow[d] \\
0 \arrow[r] & H^2(L, \overline{K}^\times) \arrow[r, "\gamma_3"] & H^2(L, J_{\overline{K}}) \arrow[r, "\varepsilon_3"] & H^2(L, C_{\overline{K}})
\end{tikzcd}$$

where we have written $H^2(K, \overline{K}^\times)$ for $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$, $H^2(L, \overline{K}^\times)$ for $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$, etc. Next we are going to enlarge the above diagram.

For the Galois extension L/K we have the map

$$\mathrm{inv}_1 = \sum_v \mathrm{inv}_v : H^2(L/K, J_L) \to \mathbb{Q}/\mathbb{Z}$$

Theorem 6.18 tells use that the sequence

$$\begin{tikzcd}
0 \arrow[r] & H^2(L/K, L^\times) \arrow[r, "\gamma_1"] & H^2(L/K, J_L) \arrow[r, "\mathrm{inv}_1"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

is a complex. Since $\mathrm{inv}_v(\inf \alpha) = \mathrm{inv}_v(\alpha)$ for all $\alpha \in H^2(L/K, J_L)$, by the universal property of direct limits, we have a map $\mathrm{inv}_2 : H^2(K, J_{\overline{K}}) \to \mathbb{Q}/\mathbb{Z}$ such that the diagram

$$\begin{tikzcd}
H^2(L/K, J_L) \arrow[r, "\mathrm{inv}_1"] \arrow[d, "\inf"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\mathrm{id}"] \\
H^2(K, J_{\overline{K}}) \arrow[r, "\mathrm{inv}_2"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd} \qquad (*)$$

is commutative. Furthermore, the sequence

$$\begin{tikzcd}
0 \arrow[r] & H^2(K, \overline{K}^\times) \arrow[r, "\gamma_2"] & H^2(K, J_{\overline{K}}) \arrow[r, "\mathrm{inv}_2"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

is a complex. In a similar manner we have a complex

$$\begin{tikzcd}
0 \arrow[r] & H^2(L, \overline{K}^\times) \arrow[r, "\gamma_3"] & H^2(L, J_{\overline{K}}) \arrow[r, "\mathrm{inv}_3"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

But now $\mathrm{inv}_w(\mathrm{res}\, \alpha) = n_{w/v}\, \mathrm{inv}_v(\alpha)$, where $\alpha \in H^2(K, J_{\overline{K}})$, w is a prime of L over v of K and $n_{w/v} = [L_w : K_v]$. Thus we have the commutative diagram

$$\begin{tikzcd}
H^2(K, J_{\overline{K}}) \arrow[r, "\mathrm{inv}_2"] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[d, "n"] \\
H^2(L, J_{\overline{K}}) \arrow[r, "\mathrm{inv}_3"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

as the sum of the local degrees $\sum\limits_{w|v} n_{w/v} = n = [L : K]$.

Now put $H^2(K, C_{\overline{K}})_{\text{reg}} = \operatorname{Im} \varepsilon_2$ and $H^2(L, C_{\overline{K}})_{\text{reg}} = \operatorname{Im} \varepsilon_3$. It follows that we have the induced maps

$$\beta_2 : H^2(K, C_{\overline{K}})_{\text{reg}} \to \mathbb{Q}/\mathbb{Z}$$

$$\beta_3 : H^2(L, C_{\overline{K}})_{\text{reg}} \to \mathbb{Q}/\mathbb{Z}$$

induced by inv_2 and inv_3 respectively. Define

$$H^2(L/K, C_L)_{\text{reg}} := \{a \in H^2(L/K, C_L) \mid \inf a \in H^2(K, C_{\overline{K}})_{\text{reg}}\}$$

Since $n\beta_2 \inf a = 0$, β_2 induces a homomorphism

$$\beta_1 : H^2(L/K, C_L)_{\text{reg}} \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

such that $\beta_1(a) = \beta_2(\inf a)$. We put all information above together to obtain a extended commutative 3-dimensional diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & H^2(L/K, L^\times) \arrow[r, "\gamma_1"] \arrow[dd] & H^2(L/K, J_L) \arrow[r, "\varepsilon_1"] \arrow[dd] \arrow[drrr, "\text{inv}_1"] & H^2(L/K, C_L)_{\text{reg}} \arrow[dd] \arrow[drr, "\beta_1"] & & 0 \arrow[d] \\
 & & & & & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[dd, "i"] \\
0 \arrow[r] & H^2(K, \overline{K}^\times) \arrow[r, "\gamma_2"] \arrow[dd] & H^2(K, J_{\overline{K}}) \arrow[r, "\varepsilon_2"] \arrow[dd] \arrow[drrr, "\text{inv}_2"] & H^2(K, C_{\overline{K}})_{\text{reg}} \arrow[r] \arrow[dd] \arrow[drr, "\beta_2"] & 0 & \\
 & & & & & \mathbb{Q}/\mathbb{Z} \arrow[dd, "n"] \\
0 \arrow[r] & H^2(L, \overline{K}^\times) \arrow[r, "\gamma_3"] & H^2(L, J_{\overline{K}}) \arrow[r, "\varepsilon_3"] \arrow[drrr, "\text{inv}_3"] & H^2(L, C_{\overline{K}})_{\text{reg}} \arrow[r] \arrow[drr, "\beta_3"] & 0 & \\
 & & & & & \mathbb{Q}/\mathbb{Z}
\end{tikzcd} \tag{$\heartsuit$}$$

where i is the inclusion map, n is the multiplication by n, the "bent" sequences are complex and the horizontal and vertical sequences are exact.

We propose to show that

$$H^2(K, C_{\overline{K}})_{\text{reg}} = H^2(K, C_{\overline{K}}) \cong \mathbb{Q}/\mathbb{Z}$$

Now $\operatorname{Im}(\text{inv}_1) \subseteq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is the subgroup $\frac{1}{n_0}\mathbb{Z}/\mathbb{Z}$, where n_0 is the lowest common multiple of all the local degrees of L/K by Corollary 6.10.1.(b), and so since $\operatorname{Im} \beta_1 \supseteq \operatorname{Im} \text{inv}_1$ we have the inequalities

$$n \geqslant \# H^2(L/K, C_L) \geqslant \# H^2(L/K, C_L)_{\text{reg}} \geqslant \# \operatorname{Im} \beta_1 \geqslant \# \operatorname{Im} \text{inv}_1 = n_0$$

by the second inequality. It follows that if $n = n_0$ for this particular finite extension L/K, then we have equality throughout so that β_1 is bijective and the sequence

$$0 \longrightarrow H^2(L/K, L^\times) \xrightarrow{\gamma_1} H^2(L/K, J_L) \xrightarrow{\mathrm{inv}_1} \mathbb{Q}/\mathbb{Z} \qquad (\spadesuit)$$

is exact, for if $0 = \mathrm{inv}_1(b) = \beta_1\varepsilon_1(b)$, then $\varepsilon_1 b = 0$ and $b \in \operatorname{Im}\gamma_1$.

Suppose L/K is a finite cyclic extension. Then $n = n_0$ for the Frobenius elements $F_{L/K}(v)$, whose orders are equal to the local degrees n_v, generates the cyclic group $\mathrm{Gal}(L/K)$ by Corollary 6.13.3. So if, in particular, the extension L/K is cyclic cyclotomic, then the sequence ($\spadesuit$) is exact. But by Lemma 6.20 says that the group $H^2(K, \overline{K}^\times)$ and $H^2(K, J_{\overline{K}})$ are the unions (of the isomorphic images under inflation) of the groups $H^2(L/K, L^\times)$ and $H^2(L/K, J_L)$, where L runs over all cyclic cyclotomic extensions of K. Consequently, in ($\heartsuit$)

$$0 \longrightarrow H^2(K, \overline{K}^\times) \xrightarrow{\gamma_2} H^2(K, J_{\overline{K}}) \xrightarrow{\mathrm{inv}_2} \mathbb{Q}/\mathbb{Z}$$

and

$$0 \longrightarrow H^2(L, \overline{K}^\times) \xrightarrow{\gamma_3} H^2(L, J_{\overline{K}}) \xrightarrow{\mathrm{inv}_3} \mathbb{Q}/\mathbb{Z}$$

are exact (direct limits are exact functors). Therefore $\ker(\mathrm{inv}_2) = \ker\varepsilon_3$, so β_2 (and similarly β_3) must be injective maps into $\mathbb{Q}/\mathbb{Z}$. They are surjective, since there exist finite extensions with arbitrary high local degrees (Lemma 6.20) and consequently even inv_2 and inv_3 are surjective.

Now letting L be an arbitrary finite Galois extension, by an easy diagram chasing we conclude that β_1 is a bijection:

$$H^2(L/K, C_L)_{\mathrm{reg}} \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

But $H^2(L/K, C_L)_{\mathrm{reg}}$ is a subgroup of $H^2(L/K, C_L)$ which has order dividing n, it is the whole of $H^2(L/K, C_L)$. Letting $L \to \overline{K}$ we see that

$$H^2(K, C_{\overline{K}})_{\mathrm{reg}} = H^2(K, C_{\overline{K}})$$

Thus we can remove the subscript "reg" from our diagram ($\heartsuit$). Also we have proved the following

Proposition 6.23. $H^2(L/K, C_L)$ is cyclic of order n, and it has a canonical generator $u_{L/K}$, called the **fundamental class** of L/K, with invariant $\frac{1}{n}$, i.e., $\mathrm{inv}_1(u_{L/K}) = \frac{1}{n}$.

The two lower layers of diagram ($\heartsuit$) and the vertical arrow between them make sense for an arbitrary finite separable extension L/K of finite degree n, and in this more general case, that much of the diagram is still commutative, because the argument showing the commutativity of ($*$) did not require L/K to be Galois. Using this, and replacing L by K', we see that if $L \supseteq K' \supseteq K$ with L/K Galois, then restricting $u_{L/K}$ from L/K to L/K' gives the fundamental class $u_{L/K'}$. It follows from Tate's theorem the cup product with the fundamental class $u_{L/K}$ gives isomorphisms

$$\hat{H}^r(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} \hat{H}^{r+2}(\mathrm{Gal}(L/K), C_L)$$

for $-\infty < r < \infty$, such that for $L \supseteq K' \supseteq K$ with L/K Galois the diagrams

$$\begin{tikzcd} \hat{H}^r(\mathrm{Gal}(L/K),\mathbb{Z}) \arrow[r, "\sim"] \arrow[d, "\mathrm{res}"] & \hat{H}^{r+2}(\mathrm{Gal}(L/K),C_L) \arrow[d, "\mathrm{res}"] \\ \hat{H}^r(\mathrm{Gal}(L/K'),\mathbb{Z}) \arrow[r, "\sim"] & \hat{H}^{r+2}(\mathrm{Gal}(L/K'),C_L) \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} \hat{H}^r(\mathrm{Gal}(L/K),\mathbb{Z}) \arrow[r, "\sim"] & \hat{H}^{r+2}(\mathrm{Gal}(L/K),C_L) \\ \hat{H}^r(\mathrm{Gal}(L/K'),\mathbb{Z}) \arrow[r, "\sim"] \arrow[u, "\mathrm{cores}"] & \hat{H}^{r+2}(\mathrm{Gal}(L/K'),C_L) \arrow[u, "\mathrm{cores}"] \end{tikzcd}$$

are commutative.

Applications

Case $r = -2$. There is a canonical isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \longrightarrow C_K/N_{L/K}C_L = J_K/K^\times N_{L/K}J_L$$

which is inverse to the Artin map. Using this as a definition in the local case, Serre deduced the formula $\mathrm{inv}(\overline{a}.\Delta_\chi) = \chi(\theta(a))$; we have proved the formula in the global case, so one can reverse the argument. (The isomorphism $G^{\mathrm{ab}} \cong H^{-2}(G,\mathbb{Z})$ is chosen in such a manner that for $\chi \in \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \cong H^1(G,\mathbb{Q}/\mathbb{Z})$ and $\sigma \in G$, we have $\chi.\sigma = \chi(\sigma)$ upon identifying $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ with $H^{-1}(G,\mathbb{Q}/\mathbb{Z})$ via the connecting homomorphism.)

Reversing the horizontal arrows in the diagrams above, with $r = -2$, and letting $L \to \overline{K}$, we obtain the commutative diagrams

$$\begin{tikzcd} C_K \arrow[r, "\psi"] \arrow[d, "\mathrm{con}"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[d, "V"] \\ C_{K'} \arrow[r, "\psi'"] & \mathrm{Gal}((K')^{\mathrm{ab}}/K') \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} C_K \arrow[r, "\psi"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ C_{K'} \arrow[r, "\psi'"] \arrow[u, "N"] & \mathrm{Gal}((K')^{\mathrm{ab}}/K') \arrow[u] \end{tikzcd}$$

where the ψ's are the Artin map and V is the transfer map. The right diagram expresses the so-called *translation theorem.*

Application to the Cohomology of $L^\times$

The general idea is to determine the cohomology of $L^\times$ from a knowledge of the cohomology of the ideles and the idele classes.

Let L/K be a finite extension, with Galois group G. Then the exact sequence $0 \to L^\times \to J_L \to C_L \to 0$ gives an exact sequence

$$\cdots \longrightarrow \hat{H}^{r-1}(G,J_L) \xrightarrow{g} \hat{H}^{r-1}(G,C_L) \longrightarrow \hat{H}^r(G,L^\times) \xrightarrow{f} \hat{H}^r(G,J_L) \longrightarrow \cdots$$

in which $\ker f \cong \operatorname{coker} g$. We know

$$\hat{H}^{r-1}(G,J_L) = \bigoplus_{v \in M_K} \hat{H}^{r-1}(G^v, L^{v\times}) = \bigoplus_{v \in M_K} \hat{H}^{r-3}(G^v,\mathbb{Z})$$

and

$$\hat{H}^{r-1}(G, C_L) = \hat{H}^{r-3}(G, \mathbb{Z})$$

so the kernel of

$$f : \hat{H}^r(G, L^\times) \longrightarrow \bigoplus_{v \in M_K} \hat{H}^r(G^v, L^{v\times})$$

is isomorphic ot the cokernel of

$$g_1 : \bigoplus_{v \in M_K} \hat{H}^{r-3}(G^v, \mathbb{Z}) \longrightarrow \hat{H}^{r-3}(G, \mathbb{Z})$$

where g_1 is given by $g_1 \left(\sum_v z_v \right) = \sum_v \mathrm{cores}_G^{G_v} z_v$. Using the fundamental duality theorem in the cohomology of finite groups, which states that the cup product pairing

$$\hat{H}^r(G, \mathbb{Z}) \times \hat{H}^r(G, \mathbb{Z}) \longrightarrow \hat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$$

is a perfect duality of finite groups, one sees that the cokernel of g_1 is the dual of the kernel of the map

$$h : \hat{H}^{3-r}(G\mathbb{Z}) \longrightarrow \prod_{v \in M_K} \hat{H}^{3-r}(G^v, \mathbb{Z})$$

which is defined by $(h(z))_v = \mathrm{res}_{G_v}^G(z)$ for all $v \in M_K$.
Case $r = 0$.
Case $r = 3$. $H^3(G, L^\times)$ is cyclic of order n/n_0, the global degree divided by the lower common multiple of the local degrees, generated by the **Teichmüller 3-class** $\delta u_{L/K}$, where $\delta : H^2(G, C_L) \to H^3(G, L^\times)$. This can be killed by inflation (replace L by a bigger L' so that the n_0 for L' is divisible by n); so $H^3(\overline{K}/K, \overline{K}^\times) = 0$.
Group Extensions. Consider extensions $K \subseteq L \subseteq M$, where L/K is Galois with group G, and M/K is Galois with group E and M is a class field over L with abelian Galois group A. So $1 \to A \to E \to G$ is exact. By the Artin isomorphism $A \cong C_L/N_{M/L}C_M$. We want to know about E.

Theorem 6.24.

(i) Let $\sigma \in E$ have image $\overline{\sigma} \in G$. Let $x \in C_L$. Then $\psi(\overline{\sigma}x) = \sigma\psi(x)\sigma^{-1}$, where $\psi : C_L \to A$ is the Artin map.

(ii) Let $v \in H^2(G, A)$ be the class of the group extension E. Then $v = \psi_*(u_{L/K})$, where $\psi_* : H^2(G, C_L) \to H^2(G, A)$ is the map induced by $\psi : C_L \to A$ and where $u_{L/K}$ is the fundamental class for L/K.

Proof. We only prove (i). Let S be a finite set of primes consisting of the archimedean primes of L and those ramified in M. For $x = (x_v)_v \in J_L$ by weak approximation we can find $a_n \in L^\times$ such that $a_n \to x_v^{-1}$ as $n \to \infty$ at all $v \in S$. Then (with an obvious notation)

$$\psi(x) = \lim_{n\to\infty} \psi(a_n x) = \lim_{n\to\infty} \psi((a_n x)_1 \cdot \lim_{n\to\infty} \psi((a_n x)_2) = \lim_{n\to\infty} \psi((a_n x)_1)$$

for $\psi(K^\times) = 1$. Hence it suffices to consider the case $x \in J_L^S$; in this case we have $\psi(x) = \mathrm{Frob}_{M/L}((x)^S)$, where $\mathrm{Frob}_{M/L}$ is the Frobenius substitution and $(x)^S = \sum_v (\mathrm{ord}_v\, x)v$. By linearity one reduces to show the identity $\mathrm{Frob}_{M/L}(\sigma v) = \sigma F_{M/L}(v)\sigma^{-1}$. For $x \in L^v$, by definition $\mathrm{Frob}_{M/L}(v)(x) \equiv x^{Nv} \pmod{\mathfrak{P}}$ for some $\mathfrak{P} \mid v$ so that

$$\mathrm{Frob}_{M/L}(\sigma v)(\sigma x) \equiv (\sigma x)^{N\sigma(v)} = (\sigma x)^{Nv} = \sigma(x^{Nv}) \equiv \sigma\,\mathrm{Frob}_{M/L}(v)(x) \pmod{\sigma\mathfrak{P}}$$

Hence $\mathrm{Frob}_{M/L}(\sigma v) = \sigma\,\mathrm{Frob}_{M/L}(v)\sigma^{-1}$. □

6.12 Proof of the Existence Theorem

If H is an open subgroup of C_K of finite index, we say temporarily that H is **normic** if and only if there is an abelian extension L/K such that $H = N_{L/K}C_L$. The existence theorem asserts that every open subgroup H of finite index in C_K is normic. (We have already shown that if L/K is abelian, then $N_{L/K}C_L$ is an open subgroup of C_K of finite index.)

First, two obvious remarks:

- If $H_1 \supseteq H$ and H is normic, then H_1 is normic. Say $H = N_{L/K}C_L$ for some abelian L/K and consider the composition

$$C_K \xrightarrow{\psi} \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(L^{\psi(H_1)}/K) = \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/L^{\psi(H_1)})} = \frac{\mathrm{Gal}(L/K)}{\psi(H_1)}$$

  where ψ is the Artin map. The kernel of the whole map is $\psi^{-1}(\psi(H_1)) = H_1 + H = H_1$. Hence we have a diagram with all vertical maps being invertible (with $M = L^{\psi(H_1)}$)

$$\begin{tikzcd} C_K/H \arrow[r, "\psi", "\sim"'] \arrow[d] & \mathrm{Gal}(L/K) \arrow[d] \\ C_K/H_1 \arrow[r, "\psi'", "\sim"'] & \mathrm{Gal}(M/K) \end{tikzcd}$$

  But by functoriality we know $\ker\psi' = N_{M/K}C_M$, so that H_1 is normic.

- If H_1 and H_2 are normic, so is $H_1 \cap H_2$. Say $H_1 = N_{L/K}C_L$ and $H_2 = N_{M/K}C_M$. Consider the Artin map $\psi : C_K \to \mathrm{Gal}(LM/K) \subseteq \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$; the kernel of ψ is $H_1 \cap H_2$, so that $H_1 \cap H_2 = N_{LM/K}C_{LM}$ is normic.

Key Lemma Let n be a prime and K a field not of characteristic n containing the n-th roots of unity. Then every open subgroup H of index n in C_K is normic.

Proof. Suppose $H \leqslant C_K$ is open of index n. Let H' be the inverse image of H in J_K; then $H' \leqslant J_K$ is open, so there is a finite set $S \subseteq M_K$ such that

$$H' \supseteq \prod_{v \in S} (1) \times \prod_{v \notin S} U_v =: U^S$$

Furthermore, $n = [C_K : H]$ so that $H' \supseteq J_K^n$. Therefore

$$H' \supseteq \prod_{v \in S} (K^\times)^n \times \prod_{v \notin S} U_V \overset{\text{say}}{=} E$$

and from Corollary 6.16.2 (extend S large enough to match the condition) we obtain $K^\times N_{M/K} J_M = K^\times E$ for some abelian M/K. Hence $EK^\times / K^\times$ is a normic subgroup contained in $H = H'/K^\times$, and from above we know H is normic as well. □

Lemma 6.25. If L/K is cyclic and $H \leqslant C_K$, and if $N_{L/K}^{-1}(H) \leqslant C_L$ is normic for L, then H is normic for K.

Proof. Put $H' = N_{L/K}^{-1}(H)$ and let M/L be the class field of H'. We claim M/K is abelian, and $N_{M/K} C_M \subseteq H$, so H is normic. For the latter, we have

$$N_{M/K} C_M = N_{L/K} N_{M/L} C_M = N_{L/K} H' \subseteq H$$

by transitivity of norm. It remains to show the first, which is the main difficulty.

M/K is Galois for H' is invariant under $\mathrm{Gal}(L/K)$. The Galois group $E = \mathrm{Gal}(M/K)$ is a group extension

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

Since $E/A \cong G = \mathrm{Gal}(L/K)$ is *cyclic*, it is enough to show that $A = \mathrm{Gal}(M/L)$ lies in the center of E. We use Theorem 6.24.(i). Let $\psi : C_L \to A$ be the Artin map. To show A lies in the center, it is enough to check that

$$\psi(x) = \sigma \psi(x) \sigma^{-1} \overset{\text{(i)}}{=} \psi(\sigma x)$$

for all $x \in C_L$ and $\sigma \in E$. Now $\psi : C_L \to A$ has kernel H', so we want to check that $\sigma x / x \in H'$, which is clear since $N_{L/K}(\sigma x / x) = 1 \in H$. □

Proceed to prove the Existence theorem. Use induction on the index of H in C_K. If $[C_K : H] = 1$, everything is clear. Now let n be a prime dividing the index. Adjoin the n-th roots of unity to K to get K', and replace H by $H' = N_{K'/K}^{-1}(H)$. By the last lemma it suffices to consider H'. We have $[C_{K'} : H'] \mid [C_K : H]$, and by induction we may assume $[C_{K'} : H'] = [C_K : H]$.

So $n \mid [C_{K'} : H']$. Take H_1' so that $H_1' \geqslant H$ and $[C_{K'} : H'] = n$. By Key Lemma H_1' is normic; let L be its class field and put $H'' = N_{L/K'}^{-1}(H')$. Then

$$[C_L : H''] < [C_{K'} : H'] = [C_K : H]$$

for $C_L/H'' \overset{N_{L/K'}}{\longrightarrow} C_{K'}/H'$ is injective with image H'_1/H' properly contained in $C_{K'}/H'$. Hence H'' is normic by induction hypothesis; L/K' is cyclic ($\mathrm{Gal}(L/K') \cong C_{K'}/H'_1$ has prime order), so we can apply the last lemma again; so H' is normic.

$$\begin{tikzcd}
L \arrow[d, dash, "\text{cyclic}"', "H'_1"] \\
K' \arrow[ddd, equal] \\
{} \\
{} \\
K' = K(\sqrt[n]{1}) \arrow[d, dash, "\text{cyclic}"'] \\
K
\end{tikzcd}
\qquad
\begin{tikzcd}
H'' \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & C_L \arrow[r] \arrow[d] & C_L/H'' \arrow[dd, two heads] & & \\
H'_1 \arrow[r, dash, "n"] \arrow[dd, dash] & C_{K'} \arrow[rr] \arrow[dd, equal] & & C'_K/H'_1 \arrow[r, "\sim", "\text{Key Lemma}"'] & \mathrm{Gal}(L/K') \\
 & & H'_1/H' \arrow[d, hook] & & \\
H' \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & C_{K'} \arrow[r] \arrow[d] & C_{K'}/H' \arrow[d] & & \\
H \arrow[r] & C_K \arrow[r] & C_K/H & &
\end{tikzcd}$$

Chapter 7

Fourier Analysis in Number Fields and Hecke's Zeta Functions

7.1 The Local Theory

In this section, let k denote the completion of an algebraic number field at a place $\mathfrak{p}$. Accordingly,

- if $\mathfrak{p}$ is archimedean, then k is either real or complex;
- if $\mathfrak{p}$ is non-archimedean, k is an finite extension of $\mathbb{Q}_p$, where p is the rational prime lying below $\mathfrak{p}$.

In the latter case, we denote by $\mathfrak{o}$ the ring of integer in k, and $N\mathfrak{p} = \#\mathfrak{o}/\mathfrak{p}$. We select the following norm:

- k real. Choose $|\cdot|$ to be the ordinary absolute value on $\mathbb{R}$;
- k complex. Then $|z| = z\overline{z}$ for all $z \in \mathbb{C} = k$;
- k $\mathfrak{p}$-adic. Then $|\alpha| = (N\mathfrak{p})^{-\nu_{\mathfrak{p}}(a)}$.

Lemma 7.1. k is locally compact. More precisely, a subset $A \subseteq k$ is relatively compact if and only if A is bounded in absolute value.

Proof. It is clear when k is real or complex. When k is $\mathfrak{p}$-adic, it is Theorem 2.3. □

7.1.1 Additive Characters and Measure

Denote by k^+ the additive group of k, as a locally compact abelian group, and denote by $\widehat{k^+}$ the group of characters, i.e., continuous homomorphisms $\chi : k^+ \to S^1$. It can be shown that $\widehat{k^+}$ is, equipped with the compact open topology, also a locally compact abelian group.

Lemma 7.2. A continuous homomorphism $f : k^+ \to \mathbb{C}^\times$ has image in S^1.

Proof. Every $\mathfrak{p}^n$ $(n \in \mathbb{Z})$ is a compact subgroup of k^+, so $f(\mathfrak{p}^n) \subseteq S^1$. Since $k^+ = \bigcup_{n=1}^{\infty} \mathfrak{p}^{-n}$, it follows $f(k^+) \subseteq S^1$.

□

Lemma 7.3. Suppose $\chi \in \widehat{k^+}$ is a nontrivial character. Then the map

$$\begin{tikzcd}
k^+ \arrow[r] & \widehat{k^+} \\
x \arrow[r, mapsto] & {[\chi_x : y \mapsto \chi(xy)]}
\end{tikzcd}$$

is an isomorphism of topological groups.

Proof.

1) We first show that if $y \in k$ is such that $\chi(xy) = 1$ for all $x \in k$, then $y = 0$. Since χ is nontrivial, we can find $z \in k$ such that $\chi(z) \neq 1$. If $y \neq 0$, then $1 = \chi((zy^{-1})y) = \chi(z) \neq 1$, a contradiction; thus $y = 0$. This shows $x \mapsto \chi_x$ is injective.

2) We claim the set $H := \{\chi_x \mid x \in k\}$ is dense in $\widehat{k^+}$, or equivalently, $\widehat{k^+}/\overline{H} = 0$. By Pontryagin duality, it is equivalent to saying
$$0 = \left(\widehat{k^+}/\overline{H}\right)^{\wedge} \cong \overline{H}^{\perp} = H^{\perp}$$
where $H^{\perp} := \{y \in k \mid \chi_x(y) = 0 \text{ for all } x \in k\}$. But as said in the first paragraph, $H^{\perp} = 0$, so $\overline{H} = \widehat{k^+}$ as desired.

3) We show the map is a topological embedding.

   - Continuity. Let $N \in \mathbb{Z}$ and $\varphi > 0$. We must show the set
   $$A = A_{N,\varepsilon} := \{x \in k \mid |\chi_x(\mathfrak{p}^N) - 1| < \varepsilon\}$$
   is a neighborhood of 0 in k^+. Since χ is a continuous group homomorphism, we can find $M \gg 0$ such that $\chi(\mathfrak{p}^M) = 1$. Then it is clear that $\mathfrak{p}^M \subseteq A$; this shows the continuity.
   - Continuous inverse.

     $\mathfrak{p}$ discrete. Let $n \in \mathbb{Z}$. We must show $B = B_n := \{\chi_x \mid x \in \mathfrak{p}^n\}$ is a neighborhood of the trivial character 1. Let $\xi \in \mathfrak{p}^M \backslash \mathfrak{p}^{M+1}$ such that $\chi(\xi) \neq 1$. Then we claim $\{\chi_x \mid |\chi_x(\mathfrak{p}^{M+1-n}) - 1| < |\chi(\xi) - 1|\} \subseteq B$. Indeed, if $0 \neq x \in k$ is such that $|\chi_x(\mathfrak{p}^{M+1-n}) - 1| < |\chi(\xi) - 1|$, then in particular, $\xi \notin x\mathfrak{p}^{M+1-n}$. Say $x \in \mathfrak{p}^m \backslash \mathfrak{p}^{m+1}$; then $\xi \notin \mathfrak{p}^{M+1-n+m}$, i.e., $n + 1 < m$. Hence $x \in \mathfrak{p}^m \subseteq \mathfrak{p}^n$, or $x \in B$.

     $\mathfrak{p}$ archimedean. For each $r > 0$, we show that $B = B_r := \{\chi_x \mid x \in B_r(0)\}$ is a neighborhood of the trivial character 1. Let $\xi \neq 0$ such that $\chi(\xi) \neq 1$. Then we claim $\{\chi_x \mid |\chi_x(B_{|\xi|/r}(0)) - 1| < |\chi(\xi) - 1|\} \subseteq B$. For if $0 \neq x \in k$ is such that $|\chi_x(B_{|\xi|/r}(0)) - 1| < |\chi(\xi) - 1|$, then in particular, $\xi \notin xB_{|\xi|/r}(0) = B_{|x||\xi|/r}$, i.e. $\dfrac{|x||\xi|}{r} < |\xi|$, or $|x| < r$. (Here $|\cdot|$ denote the usual euclidean distance.)

4) Thus, we see $\{\chi_x \mid x \in k^+\}$ is a locally compact subgroup of $\widehat{k^+}$. To complete the proof we need to show it is surjective. For this, we apply the following interesting lemma.

   Lemma 7.4. Let G be a Hausdorff topological group and $H \leqslant G$ be a locally compact subgroup. Then H is closed in G.

   Proof. Replacing G with the closure of H in G, we may assume H is dense in G. Let $x \in H$ and choose a neighborhood U of x in H with compact closure C. Write $U = V \cap H$ for some open $V \subseteq G$. Since C is compact and G is Hausdorff, C is closed in G, and thus $V \backslash C$ is open in G. But for $V \cap H = U \subseteq C$, it forces $(V \backslash C) \cap H = \varnothing$, and since H is dense in G, it must be the case $V \subseteq C$; in particular, $V \subseteq H$. This shows H is open in G, and since they are topological groups, H is closed in G. □

   This means $\{\chi_x \mid x \in k^+\}$ is closed in $\widehat{k^+}$, and since we already saw the former set is dense in the latter in the second paragraph, it turns out that $\{\chi_x \mid x \in k^+\} = \widehat{k^+}$.

□

To fix the identification of k^+ with its character group promised by the proceeding lemma, we must construct a special non-trivial character. Let p be the rational place lying below $\mathfrak{p}$, and $\mathbb{Q}_p$ the completion of the rational field at p. Define a map

$$\lambda : \mathbb{Q}_p \longrightarrow \mathbb{R}/\mathbb{Z}$$

as follows:

- $p = \infty$, so $\mathbb{Q}_\infty = \mathbb{R}$. Let $\lambda(x) \equiv -x \pmod 1$.
- $p < \infty$. Write $x = \sum_{n \geqslant N} a_i p^n$ and put $\lambda(x) \equiv \sum_{0 > n \geqslant N} a_i p^n \pmod 1$.

Lemma 7.5. $\lambda : \mathbb{Q}_p \to \mathbb{R}/\mathbb{Z}$ is a nontrivial character.

Proof. The case $p = \infty$ is clear. Suppose $p < \infty$. Then λ is clearly a continuous additive group homomorphism, and it is nontrivial for $\lambda(x) = 0$ if and only if $x \in \mathbb{Z}_p$.

□

Return to the local field k^+. Define

$$\begin{tikzcd} \Lambda : k^+ \arrow[r] & R \arrow[r] & \mathbb{R}/\mathbb{Z} \\ x \arrow[r, mapsto] & \mathrm{Tr}_{k/R}(x) \arrow[r, mapsto] & \lambda(\mathrm{Tr}_{k/R}(x)) \end{tikzcd}$$

Then we have an isomorphism

$$\begin{tikzcd} k^+ \arrow[r] & \widehat{k^+} \\ x \arrow[r, mapsto] & {[y \mapsto e^{2\pi i \Lambda(xy)}]} \end{tikzcd}$$

Denote by $\mathfrak{d}$ the (absolute) different of k, i.e., the inverse of the fractional ideal $\{x \in k \mid \mathrm{Tr}_{k/R}(x\mathfrak{o}) \subseteq \mathfrak{o}_R\}$.

Lemma 7.6. Suppose $\mathfrak{p}$ is non-archimedean. Then $[y \mapsto e^{2\pi i \Lambda(xy)}]$ is trivial if and only if $x \in \mathfrak{d}^{-1}$.

Proof. For $x \in k$, we have $\Lambda(x\mathfrak{o}) = 0 \Leftrightarrow \lambda(\mathrm{Tr}_{k/\mathbb{Q}_p}(x\mathfrak{o})) = 0 \Leftrightarrow \mathrm{Tr}_{k/\mathbb{Q}_p}(x\mathfrak{o}) \subseteq \mathbb{Z}_p \Leftrightarrow x \in \mathfrak{d}^{-1}$. □

Lemma 7.7. Let μ be a Haar measure on k^+. Then for each $\alpha \in k^\times$ and measurable M, one has $\mu(\alpha M) = |\alpha|\mu(M)$.

Proof. The case k being archimedean is clear by our choice of $|\cdot|$. The case k being $\mathfrak{p}$-adic is Theorem 2.5. □

Let us now select a fixed Haar measure for our additive group k^+, and write dx instead of $d\mu(x)$ for this measure.

- dx is the usual Lebesgue measure on $\mathbb{R}$ if k is real.
- dx is twice the usual Lebesgue measure on $\mathbb{C}$ if k is complex.
- dx is the Haar measure for which $\mathfrak{o}$ has measure $(N\mathfrak{d})^{-\frac{1}{2}}$ if k is $\mathfrak{p}$-adic. (For an integral ideal $\mathfrak{a} \subseteq \mathfrak{o}$, $N\mathfrak{a} := \#(\mathfrak{o}/\mathfrak{a})$.)

Define the Fourier transform $\hat{f}$ of a function $f \in L^1(k^+)$ by

$$\hat{f}(x) := \int_k f(y) e^{-2\pi i \Lambda(xy)} dy$$

Theorem 7.8. With our choice of measure, the inversion formula

$$f(x) = \int_k \hat{f}(y) e^{2\pi i \Lambda(xy)} dy = \hat{\hat{f}}(-x)$$

holds for $f \in \mathrm{inv}(k^+)$. Here for a LCA group G

$$\mathrm{inv}(G) := \{f \in L^1(G) \cap C(G) \mid \hat{f} \in L^1(\hat{G})\}$$

Proof. It suffices to show the inversion formula holds for one non-trivial function, since from abstract Fourier analysis we know it is true.

- k real. Take $f(x) = e^{-\pi x^2}$. Using Cauchy integral formula, we compute

$$\begin{aligned}
\hat{f}(x) &= \int_{\mathbb{R}} e^{-\pi y^2} e^{2\pi i x y} dy = \int_{\mathbb{R}} e^{-\pi (y - ix)^2 - \pi x^2} dy \\
&= e^{-\pi x^2} \left(\lim_{M \to \infty} \int_0^x e^{-\pi(-M - it)^2} dt + \lim_{\substack{N \to \infty \\ M \to \infty}} \int_{-M}^{N} e^{-\pi y^2} dy + \lim_{N \to \infty} \int_0^x e^{-\pi(N - it)^2} dt \right) \\
&= e^{-\pi x^2} \int_{\mathbb{R}} e^{-\pi y^2} dy = e^{-\pi x^2} = f(x)
\end{aligned}$$

- k complex. Take $f(z) = e^{-2\pi|z|}$ (recall $|z| = z\overline{z}$ here). Writing $z = \sigma + i\tau$, we have
$$\hat{f}(z) = 2\int_{\mathbb{R}}\int_{\mathbb{R}} e^{-2\pi(x^2+y^2)} e^{4\pi i(\sigma x - \tau y)} dxdy = e^{-\pi(\sqrt{2}\sigma)^2} e^{-\pi(\sqrt{2}\tau)^2} = e^{-2\pi|z|} = f(z)$$
- k $\mathfrak{p}$-adic. Take $f(x) = \mathbf{1}_{\mathfrak{o}}(x)$, the characteristic function of $\mathfrak{o}$. By Lemma 7.6, we have
$$\hat{f}(x) = \int_k \mathbf{1}_{\mathfrak{o}}(y) e^{-2\pi i\Lambda(xy)} dy = \int_{\mathfrak{o}} e^{-2\pi i\Lambda(xy)} dy = \mu(\mathfrak{o})\mathbf{1}_{\mathfrak{d}^{-1}}(x)$$
and
$$\widehat{\mathbf{1}_{\mathfrak{d}^{-1}}}(x) = \int_k \mathbf{1}_{\mathfrak{d}^{-1}}(y) e^{-2\pi i\Lambda(xy)} dy = \int_{\mathfrak{d}^{-1}} e^{-2\pi i\Lambda(xy)} dy = \mu(\mathfrak{d}^{-1})\mathbf{1}_{\mathfrak{o}}(x)$$
Write $\mathfrak{d}^{-1} = \mathfrak{p}^n$; then $N\mathfrak{d} = (N\mathfrak{p})^n$ and $\mu(\mathfrak{p}^n) = \mu(\mathfrak{o})(N\mathfrak{p})^{-n}$, so
$$\mu(\mathfrak{o})\mu(\mathfrak{d}^{-1}) = \mu(\mathfrak{o})\mu(\mathfrak{p}^{-n}) = \mu(\mathfrak{o})^2(N\mathfrak{p})^n = (N\mathfrak{d})^{-1}N\mathfrak{d} = 1$$

□

7.1.2 Multiplicative Characters and Measure

Let $U = U_k := \{x \in k \mid |x| = 1\} \subseteq k^\times$; then we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & U \arrow[r] & k^\times \arrow[r, "|\cdot|"] & \mathbb{R}_{>0} \arrow[r] & 0 \end{tikzcd}$$

In all cases, U is compact, and in case k is $\mathfrak{p}$-adic, U is also open.

Definition.

1. A **quasi-character** is a continuous group homomorphism $c : k^\times \to \mathbb{C}^\times$.
2. A quasi-character c is **unramified** if $\chi(U) = \{1\}$.

Lemma 7.9. The unramified quasi-characters are precisely the maps of the form

$$c(x) = |x|^s := e^{s\log|x|}\,(x \in k^\times)$$

where s is a complex number. When $\mathfrak{p}$ is archimedean, s is uniquely determined by c, while in case $\mathfrak{p}$ is non-archimedean, s is determined mod $\dfrac{2\pi i}{\log N\mathfrak{p}}$.

Proof. For any s, $x \mapsto |x|^s$ is obviously an unramified quasi-character. Conversely, suppose $c : k^\times \to \mathbb{C}^\times$ is an unramified quasi-character. In all cases, the value of $c(x)$ depends only on $|x|$.

- k real. Consider $f := c|_{\mathbb{R}_{>0}} : \mathbb{R}_{>0} \to \mathbb{C}^\times$. Then $g := f \circ \exp : \mathbb{R} \to \mathbb{C}^\times$ is a continuous function such that $g(x+y) = g(x)g(y)$ and $g(0) = 1$. Taking $\gamma \in \mathbb{R}$ such that $A := \displaystyle\int_0^\gamma g(t)dt \neq 0$. Then

  $$Ag(x) = \int_0^\gamma g(t+x)dt = \int_x^{x+\gamma} g(t)dt$$

  is differentiable. Applying $\left.\dfrac{\partial}{\partial y}\right|_{y=0}$ to the equation $g(x+y) = g(x)g(y)$, we see $g'(x) = g'(0)g(x)$ so that $g(x) = e^{sx}$ with uniquely determined constant $s = g'(0)$. Thus $f(x) = x^s$, and hence $c(x) = |x|^s$.

- k complex. Similarly, consider $f := c|_{\mathbb{R}_{>0}} : \mathbb{R}_{>0} \to \mathbb{C}^\times$. As in the case k real, we see $f(x) = x^s$ for some unique $s \in \mathbb{C}$. Thus $c(z) = f(|z|^{1/2}) = |z|^{s/2} = z^{s/2}\overline{z}^{s/2}$.

- k $\mathfrak{p}$-adic. Fix a uniformizer ϖ of k. Then

  $$c(x) = c(x\varpi^{-\operatorname{ord}_\mathfrak{p}(x)}\varpi^{\operatorname{ord}_\mathfrak{p}(x)}) = c(\varpi^{\operatorname{ord}_\mathfrak{p}(x)}) = c(\varpi)^{\operatorname{ord}_\mathfrak{p} x} = c(\varpi)^{-\log_{N\mathfrak{p}}|x|}$$

  Write $c(\varpi) = Re^{2\pi i\theta}$; then

  $$c(\varpi)^{-\log_{N\mathfrak{p}}|x|} = R^{-\log_{N\mathfrak{p}}|x|}e^{-2\pi i\theta\log_{N\mathfrak{p}}|x|} = |x|^{-\log_{N\mathfrak{p}}R}|x|^{\frac{-2\pi i\theta}{\log N\mathfrak{p}}}$$

  Since θ is determined mod 1, $s := -\log_{N\mathfrak{p}} R + \dfrac{2\pi i\theta}{\log N\mathfrak{p}}$ is determined mod $\dfrac{2\pi i}{\log N\mathfrak{p}}$.

□

When $\mathfrak{p}$ is archimedean, there is an canonical decomposition $k^\times \cong U \times \mathbb{R}_{>0}$, while $\mathfrak{p}$ is discrete, by choosing a uniformizer ϖ, we still have a non-canonical decomposition $k^\times \cong U \times \mathbb{Z}$. Thus for an element $x \in k^\times$, we can write $x = \tilde{x}\rho$ with $\tilde{x} \in U$ according to the aforementioned decomposition.

Theorem 7.10. The quasi-characters of $k^\times$ are precisely the maps of the form

$$c(x) = \tilde{c}(\tilde{x})|x|^s$$

where $\tilde{c}$ is any character of U. $\tilde{c}$ is uniquely determined by c, and s is determined as in the preceding lemma.

Proof. A map of the described form is obviously a quasi-character. Conversely, suppose $c : k^\times \to \mathbb{C}^\times$ is a quasi-character. Define $\tilde{c} := c|_U$; since U is compact, $\tilde{c}$ has image contained in S^1, and hence it is a character on U. The map $x \mapsto c(x)/\tilde{c}(\tilde{x})$ is then an unramified quasi-character, and therefore is of the form $|x|^s$ according to the preceding lemma. □

The problem of quasi-characters of $k^\times$ therefore boils down to that of the characters $\tilde{c}$ to U.

- k real. Then $U = \{\pm 1\}$, and the characters are $\tilde{c}(\tilde{x}) = \tilde{x}^n$, $n = 0, 1$.

- k complex. Then $U = S^1$. Since the continuous endomorphisms on $\mathbb{R}$ have the form $x \mapsto ax$ with $a \in \mathbb{R}$, we see that the characters on S^1 are $\tilde{c}(\tilde{x}) = \tilde{x}^n$, $n \in \mathbb{Z}$ (by viewing S^1 as $\mathbb{R}/\mathbb{Z}$).

- k $\mathfrak{p}$-adic. The subgroup $1 + \mathfrak{p}^\nu$, $\nu > 0$ of U form a fundamental system of neighborhoods of 1 in U; we must have then that $\tilde{c}(1 + \mathfrak{p}^\nu) = 1$ for $\nu \gg 0$. Selecting ν minimal ($\nu = 0$ if $\tilde{c} \equiv 1$), we call the ideal $\mathfrak{f} := \mathfrak{p}^\nu$ the **conductor** of $\tilde{c}$. Then $\tilde{c}$ is a character of the finite group $U/1 + \mathfrak{f}$.

From the expression $c(x) = \tilde{c}(\tilde{x})|x|^s$ in the Theorem, we see $|c(x)| = |x|^\sigma$, where $\sigma := \mathrm{Re}(s)$ is uniquely determined by $c(x)$, called the **exponent** of c. We shall denote it by $\mathrm{Re}(c)$. A quasi-character is a character if and only if its exponent is 0.

We now choose a Haar measure $d^\times x$ on $k^\times$.

- $\mathfrak{p}$ archimedean. Choose $d^\times x := \dfrac{dx}{|x|}$.

- $\mathfrak{p}$ discrete. Choose $d^\times x := \dfrac{N\mathfrak{p}}{N\mathfrak{p} - 1} \dfrac{dx}{|x|}$

Lemma 7.11. In case $\mathfrak{p}$ is discrete, $\mathrm{vol}(U, d^\times x) = (N\mathfrak{d})^{-\frac{1}{2}}$.

Proof. By definition,

$$\int_U d^\times x = \frac{N\mathfrak{p}}{N\mathfrak{p} - 1} \int_U \frac{dx}{|x|} = \frac{N\mathfrak{p}}{N\mathfrak{p} - 1} \int_U dx$$

Since $U = \bigsqcup_{a \in (\mathfrak{o}/\mathfrak{p})^\times} a(1 + \mathfrak{p})$, it follows

$$\int_U dx = (N\mathfrak{p} - 1) \int_{1+\mathfrak{p}} dx = \frac{N\mathfrak{p} - 1}{N\mathfrak{p}} \int_{\mathfrak{o}} dx = \frac{N\mathfrak{p} - 1}{N\mathfrak{p}} (N\mathfrak{d})^{-\frac{1}{2}}$$

so that $\mathrm{vol}(U, d^\times x) = (N\mathfrak{d})^{-\frac{1}{2}}$. □

7.1.3 The Local ζ-function; Functional Equation

Denote by $\mathfrak{z}$ the class of all functions satisfying the following two conditions:

$\mathfrak{z}_1$) $f \in \mathrm{inv}(k^+)$ (as in Theorem 7.8);

$\mathfrak{z}_2$) $f(x)|x|^\sigma$ and $\hat{f}(x)|x|^\sigma$ are in $L^1(k^\times)$ for $\sigma > 0$.

Definition. For $f \in \mathfrak{z}$ and a quasi-character c of exponent > 0, define a **ζ-function**

$$\zeta(f, c) := \int_{k^\times} f(x) c(x) d^\times x$$

Two quasi-characters on $k^\times$ are called **equivalent** if their quotient is an unramified quasi-character. By Lemma 7.9, an equivalence class consists of all quasi-characters of the form $c(x) = c_0(x)|x|^s$, where $c_0(x)$ is a fixed representative of the class and $s \in \mathbb{C}$. By introducing this complex parameter s, we may view each class as a Riemann surface.

- $\mathfrak{p}$ archimedean. Since s is uniquely determined by c, the Riemann surface is isomorphic to the complex plane $\mathbb{C}$.
- $\mathfrak{p}$ discrete. Since s is determined mod $\dfrac{2\pi i}{\log N\mathfrak{p}}$, the Riemann surface is isomorphic to $\mathbb{C}$ quotient by $\mathbb{Z}\dfrac{2\pi i}{\log N\mathfrak{p}}$.

Thus it is clear that what we mean when we talk of the holomorphicity of a function of quasi-characters at a point or in a region, or of singularity. We may also consider the question of analytic continuation of such a function, though this must of course be carried out on each surface (class) separately.

Lemma 7.12. For $f \in \mathfrak{z}$ and a quasi-character c of exponent > 0, the integral

$$\int_{k^\times} f(x)c(x)|x|^s d^\times x$$

defines a holomorphic function of s near $s = 0$. In other words, a ζ-function is holomorphic in the domain of all quasi-characters of exponent greater than 0.

Proof. Write $c(x) = \tilde{c}(\tilde{x})|x|^t$; by assumption $\mathrm{Re}(t) > 0$. By $\mathfrak{z}_2$), we see the integral is absolutely convergent for all s near 0 (precisely, those s such that $\mathrm{Re}(s + t) > 0$). The same holds for the integral

$$\int_{k^\times} f(x)c(x)|x|^s \log|x| d^\times x$$

for $\lim\limits_{x\to 0} x^\epsilon \log x = 0$ whenever $\epsilon > 0$. Thus we can differentiate under the integral sign (by DCT), proving our assertion. □

It is our aim to show that the ζ-functions have a meromorphic continuation to the domain of all quasi-characters by means of a simple functional equation.

Lemma 7.13. For the quasi-character c with $0 < \mathrm{Re}(c) < 1$, we have

$$\zeta(f, c)\zeta(\hat{g}, \hat{c}) = \zeta(\hat{f}, \hat{c})\zeta(g, c)$$

for any $f, g \in \mathfrak{z}$, where $\hat{c}(x) := |x|c^{-1}(x)$.

Proof. Note that $\hat{c}(x) = |x|c^{-1}(x)$ has exponent > 0 under our condition. Write $\zeta(f, c)\zeta(\hat{g}, \hat{c})$ as a double integral

$$\zeta(f, c)\zeta(\hat{g}, \hat{c}) = \iint_{k^\times \times k^\times} f(x)\hat{g}(y)c(xy^{-1})|y| d^\times x d^\times y$$

which is absolutely convergent. Under the translation $(x, y) \mapsto (x, xy)$, it becomes

$$\iint_{k^\times \times k^\times} f(x)\hat{g}(xy)c(y^{-1})|xy| d^\times x d^\times y \overset{\text{Fubini's}}{=} \int_{k^\times} \left(\int_{k^\times} f(x)\hat{g}(xy)|x| d^\times x \right) c(y^{-1})|y| d^\times y$$

By writing down the definition, the parenthetical term is

$$\int_{k^\times} f(x)\hat{g}(xy)|x|d^\times x = \int_{k^\times}\left(\left(\int_k g(z)e^{-2\pi i\Lambda(xyz)}dz\right) f(x)|x|d^\times x\right.$$

Using Fubini's again, we obtain

$$\zeta(f,c)\zeta(\hat{g},\hat{c}) = \iiint_{k\times k\times k} f(x)g(z)c(y^{-1})e^{-2\pi i\Lambda(xyz)}dxdydz$$

The RHS is symmetric in f, g, and this proves the lemma. □

Theorem 7.14. A ζ-function has an analytic continuation to the domain of all quasi-characters given by a functional equation of the type

$$\zeta(f,c) = \rho(c)\zeta(\hat{f},\hat{c})$$

The factor $\rho(c)$, which is independent of the function f, is a meromorphic function of quasi-characters defined in the domain $0 < \mathrm{Re}(c) < 1$ by the functional equation, and for all quasi-characters by analytic continuation. The function ρ satisfies the following properties:

1. $\rho(c)\rho(\hat{c}) = c(-1)$.

2. $\rho(\overline{c}) = c(-1)\overline{\rho(c)}$.

3. $|\rho(c)| = 1$ if $\mathrm{Re}(c) = \dfrac{1}{2}$.

Proof. In the next subsection we will find for each equivalence class C of quasi-character a function $f_C \in \mathfrak{z}$ such that $\zeta(\hat{f_C},\hat{c})$ is not identically zero for $0 < \mathrm{Re}(c) < 1$ on C, and thus the function

$$\rho(c) := \frac{\zeta(f_C, c)}{\zeta(\hat{f_C},\hat{c})}$$

is defined on the same domain. Moreover, our explicit formula for ρ will show ρ has a analytic continuation.

We now prove the described properties for ρ by the functional equation.

1. We have $\zeta(f,c) = \rho(c)\zeta(\hat{f},\hat{c}) = \rho(c)\rho(\hat{c})\zeta(\hat{\hat{f}},\hat{\hat{c}})$. Now

$$\zeta(\hat{\hat{f}},\hat{\hat{c}}) = \int_{k^\times}\hat{\hat{f}}(x)\hat{\hat{c}}(x)d^\times x = \int_{k^\times} f(-x)c(x)d^\times x = c(-1)\zeta(f,c)$$

so that $\zeta(f,c) = \rho(c)\rho(\hat{c})c(-1)\zeta(f,c)$.

2. $\overline{\zeta(f,c)} = \zeta(\overline{f},\overline{c}) = \rho(\overline{c})\zeta(\hat{\overline{f}},\hat{\overline{c}})$. But

$$\hat{\overline{f}}(x) = \int_k \overline{f}(y)e^{-2\pi i\Lambda(xy)}dy = \overline{\int_k f(y)e^{-2\pi i\Lambda(-xy)}dy} = \overline{\hat{f}}(-x)$$

and by writing $c(x) = \chi(x)|x|^s$ with $\chi(x) := \tilde{c}(\tilde{x})$,

$$\hat{\overline{c}}(x) = |x|\overline{c}^{-1}(x) = |x|\chi(x)\overline{|x|^s}^{-1} = |x|\chi(x)\overline{|x|^{-s}} = |x|\overline{c^{-1}(x)} = \overline{|x|c^{-1}(x)} = \overline{\hat{c}}(x)$$

we then have

$$\overline{\zeta(f,c)} = \rho(\bar{c})c(-1)\zeta(\bar{\hat{f}}, \bar{\hat{c}}) = \rho(\bar{c})c(-1)\overline{\zeta(\hat{f}, \hat{c})}$$

On the other hand, $\overline{\zeta(f,c)} = \overline{\rho(c)}\,\overline{\zeta(\hat{f}, \hat{c})}$, and therefore $\rho(\bar{c})c(-1) = \overline{\rho(c)}$.

3. Since $\mathrm{Re}(s) = \dfrac{1}{2}$, it follows $c(x)\bar{c}(x) = |c(x)|^2 = |x| = c(x)\hat{c}(x)$, and thus $\bar{c}(x) = \hat{c}(x)$. By 1. and 2., $|\rho(c)|^2 = \rho(c)\overline{\rho(c)} = 1$.

□

7.1.4 Computation of $\rho(c)$ by Special ζ-functions

Real

There are two equivalence classes of quasi-characters: one of the form $x \mapsto |x|^s\,(s \in \mathbb{C})$, and the other of the form $x \mapsto \mathrm{sign}(x)|x|^s\,(s \in \mathbb{C})$. We consider $f(x) = e^{-\pi x^2}$ and $g(x) = xe^{-\pi x^2}$. We already saw in Theorem 7.8 that $\hat{f} = f$; explicitly,

$$e^{-\pi x^2} = \int_{\mathbb{R}} e^{-\pi y^2 + 2\pi i x y}dy$$

By applying $\dfrac{d}{dx}$ to both sides, we obtain

$$-2\pi x e^{\pi x^2} = \int_{\mathbb{R}} 2\pi i x e^{-\pi y^2 + 2\pi i x y}dy$$

or $ig = \hat{g}$. This shows $f, g \in \mathfrak{z}$. Now we compute the ζ-functions.

$$\zeta(f, |\cdot|^s) = \int_{\mathbb{R}^\times} e^{-\pi x^2}|x|^s\frac{dx}{|x|} = 2\int_0^\infty e^{-\pi x^2}x^s\frac{dx}{x} = 2\pi^{-\frac{s}{2}}\int_0^\infty e^{-x^2}x^s\frac{dx}{x} = \pi^{-\frac{s}{2}}\int_0^\infty e^{-x}x^{\frac{s}{2}}\frac{dx}{x} = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)$$

$$\zeta(g, \mathrm{sign}|\cdot|^s) = \int_{\mathbb{R}^\times} xe^{-\pi x^2}\mathrm{sign}(x)|x|^s\frac{dx}{|x|} = 2\int_0^\infty xe^{-\pi x^2}x^s\frac{dx}{x} = \pi^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right)$$

$$\zeta(\hat{f}, \widehat{|\cdot|^s}) = \zeta(f, |\cdot|^{1-s}) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)$$

$$\zeta(\hat{g}, \widehat{\mathrm{sign}|\cdot|^s}) = i\zeta(g, \mathrm{sign}|\cdot|^{1-s}) = i\pi^{-\frac{(1-s)+1}{2}}\Gamma\left(\frac{(1-s)+1}{2}\right)$$

From these we can derive explicit expression for ρ :

$$\rho(|\cdot|^s) = \frac{\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)}{\pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)} = 2^{1-s}\pi^{-s}\cos\frac{\pi s}{2}\Gamma(s)$$

$$\rho(\mathrm{sign}|\cdot|^s) = \frac{\pi^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right)}{i\pi^{-\frac{(1-s)+1}{2}}\Gamma\left(\frac{(1-s)+1}{2}\right)} = -i2^{1-s}\pi^{-s}\sin\frac{\pi s}{2}\Gamma(s)$$

where the second equality follows from the Legendre's duplication formula:

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

and the Euler's reflection formula

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$$

Complex

The characters $c_n(re^{i\theta}) = e^{in\theta}$, $n \in \mathbb{Z}$ represent the different equivalence classes, and the n-th class consists of the quasi-characters $c_n(z)|z|^s$ ($s \in \mathbb{C}$). Consider the functions

$$f_n(z) := \begin{cases} \overline{z}^{|n|} e^{-2\pi z\overline{z}} & \text{, if } n \geqslant 0 \\ z^{|n|} e^{-2\pi z\overline{z}} & \text{, if } n \leqslant 0 \end{cases}$$

We contend that (which also shows $f_n \in \mathfrak{z}$)

$$\hat{f}_n(z) = i^{|n|} f_{-n}(z) \text{ for all } n \in \mathbb{Z}$$

Induction on $n \geqslant 0$, $n = 0$ being shown in Theorem 7.8. Suppose we have proved the contention for some $n \geqslant 0$, i.e., we have established the formula

$$\int_{\mathbb{C}} \overline{s}^n e^{-2\pi s\overline{s}} e^{-2\pi i\Lambda(sz)} ds = i^n z^n e^{-2\pi z\overline{z}}$$

Applying the operator $\dfrac{\partial}{\partial \overline{z}}$ to both sides, we obtain

$$\int_{\mathbb{C}} \overline{s}^n e^{-2\pi s\overline{s}} e^{-2\pi i\Lambda(sz)} \left(-2\pi i(-\overline{s})\right) ds = i^n z^n (-2\pi z) e^{-2\pi z\overline{z}}$$

or

$$\int_{\mathbb{C}} \overline{s}^{n+1} e^{-2\pi s\overline{s}} e^{-2\pi i\Lambda(sz)} = i^{n+1} z^{n+1} e^{-2\pi z\overline{z}}$$

which is the contention for $n+1$. The induction step is carried out. For the case $n < 0$, put a roof on the formula $\hat{f_{-n}}(z) = i^{|n|} f_n(z)$, which we have already proved, and remember that

$$\hat{\hat{f_{-n}}}(z) = f_{-n}(-z) = (-1)^{|n|} f_{-n}(z)$$

Now we compute the ζ-function. Write $z = re^{i\theta}$; then

$$f_n(z) = r^{|n|} e^{-in\theta} e^{-2\pi r^2}$$

$|z|^s = r^{2s}$ and that $d^\times z = \dfrac{2rdr\theta}{r^2}$. Thus

$$\zeta(f_n, c_n|\cdot|^s) = \int_0^\infty \int_0^{2\pi} r^{|n|} e^{-in\theta} e^{-2\pi r^2} e^{in\theta} r^{2s} \frac{2rdrd\theta}{r^2} = 2\pi \int_0^\infty (r^2)^{s-1+\frac{|n|}{2}} e^{-2\pi r^2} d(r^2) = (2\pi)^{1-s+\frac{|n|}{2}} \Gamma\left(s + \frac{|n|}{2}\right)$$

$$\zeta(\hat{f}_n, \widehat{c_n|\cdot|^s}) = \zeta(i^{|n|} f_{-n}, c_{-n}|\cdot|^{1-s}) = i^{|n|}(2\pi)^{s+\frac{|n|}{2}} \Gamma\left(1 - s + \frac{|n|}{2}\right)$$

Thus

$$\rho(c_n|\cdot|^s) = (-i)^{|n|} \frac{(2\pi)^{1-s}\Gamma\left(s + \frac{|n|}{2}\right)}{(2\pi)^s\Gamma\left(1 - s + \frac{|n|}{2}\right)}$$

$\mathfrak{p}$-adic

Let $c_n(x)\,(n \geqslant 0)$ be any character of $k^\times$ with conductor exactly $\mathfrak{p}^n$ such that $c_n(\pi) = 1$. (c.f. discussion below Theorem 7.10). These characters represent the different equivalence classes of quasi-characters. Consider the functions

$$f_n(x) = e^{2\pi i\Lambda(x)} \mathbf{1}_{\mathfrak{d}^{-1}\mathfrak{p}^{-n}}(x)$$

Then

$$\hat{f}_n(x) = (N\mathfrak{b})^{\frac{1}{2}} (N\mathfrak{p})^n \mathbf{1}_{1+\mathfrak{p}^n}(x)$$

Indeed,

$$\hat{f}_n(x) = \int_k f_n(y) e^{-2\pi i\Lambda(xy)} dy = \int_{\mathfrak{d}^{-1}\mathfrak{p}^{-n}} e^{-2\pi i\Lambda((x-1)y)} dy$$

If $x - 1 \in \mathfrak{p}^n$, then $\Lambda((x-1)y) = 0$ for $y \in \mathfrak{d}^{-1}\mathfrak{p}^{-n}$, and thus the integrand is a trivial character. Otherwise, the character is not trivial, and since $\mathfrak{d}^{-1}\mathfrak{p}^{-n}$ is a compact subgroup, the integral vanishes. Thus

$$\hat{f}_n(x) = \text{vol}(\mathfrak{d}^{-1}\mathfrak{p}^{-n}, dy) \mathbf{1}_{1+\mathfrak{p}^n}(x) = (N\mathfrak{b})^{\frac{1}{2}} (N\mathfrak{p})^n \mathbf{1}_{1+\mathfrak{p}^n}(x)$$

Now we compute the ζ-function. We first treat the unramified case: $n = 0$. The only character of type c_0 is the identity character, and f_0 is the characteristic function of $\mathfrak{d}^{-1}$. Let $\mathfrak{d} = \mathfrak{p}^d$. Then

$$\begin{aligned}
\zeta(f_0, |\cdot|^s) &= \int_{\mathfrak{p}^{-d}} |x|^s d^\times x = \sum_{m=-d}^{\infty} \int_{\mathfrak{p}^m \setminus \mathfrak{p}^{m+1}} |x|^s d^\times x \\
&= \sum_{m=-d}^{\infty} (N\mathfrak{p})^{-ms} \int_{\mathfrak{o}^\times} d^\times x = \frac{(N\mathfrak{p})^{ds}}{1 - (N\mathfrak{p})^{-s}} (N\mathfrak{d})^{-\frac{1}{2}} = \frac{(N\mathfrak{d})^{s-\frac{1}{2}}}{1 - (N\mathfrak{p})^{-s}} \\
\zeta(\hat{f}_0, \widehat{|\cdot|^s}) &= \zeta((N\mathfrak{d})^{\frac{1}{2}} \mathbf{1}_{\mathfrak{o}}, |\cdot|^{1-s}) = (N\mathfrak{b})^{\frac{1}{2}} \int_{\mathfrak{o}} |x|^{1-s} d^\times x \\
&= (N\mathfrak{d})^{\frac{1}{2}} \sum_{m=0}^{\infty} (N\mathfrak{p})^{-m(1-s)} \int_{\mathfrak{o}^\times} d^\times x = \frac{1}{1 - (N\mathfrak{p})^{s-1}}
\end{aligned}$$

For the ramified case, $n > 0$.

$$\zeta(f_n, c_n|\cdot|^s) = \int_{\mathfrak{d}^{-1}\mathfrak{p}^{-n}} e^{2\pi i\Lambda(x)} c_n(x)|x|^s d^\times x = \sum_{m=-d-n}^{\infty} (N\mathfrak{p})^{-ms} \int_{\mathfrak{p}^m \backslash \mathfrak{p}^{m+1}} e^{2\pi i\Lambda(x)} c_n(x) d^\times x$$

We contend that

$$\int_{\mathfrak{p}^m \backslash \mathfrak{p}^{m+1}} e^{2\pi i\Lambda(x)} c_n(x) d^\times x = 0 \qquad \text{for } m > -d-n$$

- $m \geqslant -d$. Then $\mathfrak{p}^m \backslash \mathfrak{p}^{m+1} \subseteq \mathfrak{d}^{-1}$, so $e^{2\pi i\Lambda(x)} = 1$ on $\mathfrak{p}^m \backslash \mathfrak{p}^{m+1}$, and thus the integral is

$$\int_{\mathfrak{p}^m \backslash \mathfrak{p}^{m+1}} c_n(x) d^\times x = \int_{\mathfrak{o}^\times} c_n(x\varphi^m) d^\times x = \int_{\mathfrak{o}^\times} c_n(x) d^\times x = 0$$

- $-d > m > -d-n$. Break $\mathfrak{p}^m \backslash \mathfrak{p}^{m+1}$ into a disjoint union of the sets of the form $a + \mathfrak{d}^{-1} = a(1+\mathfrak{p}^{-d-m})$, on which Λ is a constant $\Lambda(a)$, and thus

$$\int_{a+\mathfrak{d}^{-1}} e^{2\pi i\Lambda(x)} c_n(x) d^\times x = e^{2\pi i\Lambda(a)} c_n(a) \int_{1+\mathfrak{p}^{-d-m}} c_n(x) d^\times x$$

The character c_n is not trivial on the subgroup $1 + \mathfrak{p}^{-d-m}$, for

$$1 + \mathfrak{p}^n \subsetneq 1 + \mathfrak{p}^{-d-m} \Leftrightarrow \mathfrak{p}^n \subsetneq \mathfrak{p}^{-d-m} \Leftrightarrow n > -d-m \Leftrightarrow m > -d-n$$

Hence the last integral vanishes, and the contention is proved.

We have now shown

$$\zeta(f_n, c_n|\cdot|^s) = (N\mathfrak{p})^{(d+n)s} \int_{\mathfrak{p}^{-d-n} \backslash \mathfrak{p}^{-d-n+1}} e^{2\pi i\Lambda(x)} c_n(x) d^\times x$$

To write this in a better form, let $\{\varepsilon\}$ be a set of representatives of $\mathfrak{o}^\times/(1+\mathfrak{p}^n)$ in $\mathfrak{o}^\times$, so that $\mathfrak{o}^\times = \bigsqcup_\varepsilon \varepsilon(1+\mathfrak{p}^n)$. Then

$$\int_{\mathfrak{p}^{-d-n} \backslash \mathfrak{p}^{-d-n+1}} e^{2\pi i\Lambda(x)} c_n(x) d^\times x = \sum_\varepsilon \int_{1+\mathfrak{p}^n} e^{2\pi i\Lambda(\varepsilon x\varpi^{-d-n})} c_n(\varepsilon x\varpi^{-d-n}) d^\times x = \sum_\varepsilon e^{2\pi i\Lambda(\varepsilon\varpi^{-d-n})} c_n(\varepsilon) \int_{1+\mathfrak{p}^n} d^\times x$$

The pay-off comes in computing

$$\zeta(\hat{f}_n, \widehat{c_n|\cdot|^s}) = (N\mathfrak{b})^{\frac{1}{2}} (N\mathfrak{p})^n \zeta(\mathbf{1}_{1+\mathfrak{p}^n}, c_n^{-1}|\cdot|^{1-s}) = (N\mathfrak{b})^{\frac{1}{2}} (N\mathfrak{p})^n \zeta(\mathbf{1}_{1+\mathfrak{p}^n}, 1) = (N\mathfrak{b})^{\frac{1}{2}} (N\mathfrak{p})^n \int_{1+\mathfrak{p}^n} d^\times x$$

for on the set $1+\mathfrak{p}^n$, $c_n^{-1}|\cdot|^{1-s}$ is trivial. Finally,

$$\rho(|\cdot|^s) = (N\mathfrak{d})^{s-\frac{1}{2}} \frac{1-(N\mathfrak{p})^{s-1}}{1-(N\mathfrak{p})^{-s}}$$
$$\rho(c|\cdot|^s) = (N\mathfrak{d}\mathfrak{f})^{s-\frac{1}{2}} \rho_0(c)$$

where c is a ramified character with conductor $\mathfrak{f}$ such that $c(\pi) = 1$, where

$$\rho_0(c) = (N\mathfrak{f})^{-\frac{1}{2}} \sum_{\varepsilon} c(\varepsilon) e^{2\pi i \Lambda(\varepsilon \varpi^{-\operatorname{ord} \mathfrak{d}\mathfrak{f}})}$$

is a so-called **root number** and has absolute value 1, and where $\{\varepsilon\}$ is a set of representatives of $\mathfrak{o}^\times/(1+\mathfrak{f})$ in $\mathfrak{o}^\times$. The fact that $|\rho_0(c)| = 1$ results from Theorem 7.14.(3); namely,

$$1 = |\rho(c|\cdot|^{\frac{1}{2}})| = |\rho_0(c)|$$

for c is a character, $c|\cdot|^{\frac{1}{2}}$ has exponent $\dfrac{1}{2}$.

7.2 Abstract Restricted Direct Product

We consider the restricted product defined in 2.13. Let $\{\mathfrak{p}\}$ be an index set. For each $\mathfrak{p}$ let $G_\mathfrak{p}$ be an LCA group and for all but finitely many $\mathfrak{p}$ let $H_\mathfrak{p} \leqslant G_\mathfrak{p}$ be a compact open subgroup. We can form the restricted product $G := \prod_{\mathfrak{p}}' G_\mathfrak{p}$ of the $G_\mathfrak{p}$ with respect to $H_\mathfrak{p}$.

- G is naturally a group whose multiplication is defined componentwise and is a topological group.
- For a finite subset $S \subseteq \{\mathfrak{p}\}$ (when saying this, S is always required to contain those $\mathfrak{p}$ such that $H_\mathfrak{p}$ is not defined) we put

  $$G_S := \prod_{\mathfrak{p}\in S} G_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} H_\mathfrak{p}$$

  Then the G_S induce a neighborhood system of identity in G. The G_S and G are LCA groups.
- We naturally identify $G_\mathfrak{p}$ with the subgroup of G. For a finite set $S \subseteq \{\mathfrak{p}\}$, define

  $$G^S := \prod_{\mathfrak{p}\in S} \{1\} \times \prod_{\mathfrak{p}\notin S} H_\mathfrak{p}$$

  Then G^S is naturally isomorphic to the compact group $\prod_{\mathfrak{p}\notin S} H_\mathfrak{p}$, and we have the identification

  $$G_S = \prod_{\mathfrak{p}\in S} G_\mathfrak{p} \times G^S$$

Lemma 7.15. A subset $C \subseteq G$ is relatively compact if and only if it is contained in $\prod_{\mathfrak{p}} B_\mathfrak{p}$, where $B_\mathfrak{p} \subseteq G_\mathfrak{p}$ is compact for all $\mathfrak{p}$, and $B_\mathfrak{p} = H_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$.

Proof. Every compact subset of G is contained in some G_S, for the G_S cover G and a finite union of the G_S is again of type G_S. Any compact subset of a G_S is contained in a set described in the statement, for it is contained in the cartesian product of its projection onto the component $G_\mathfrak{p}$.

□

Let $c : G \to \mathbb{C}^\times$ be a quasi-character, i.e., a continuous group homomorphism into $\mathbb{C}^\times$. Denote by $c_\mathfrak{p}$ the restriction of c to $G_\mathfrak{p}$; then $c_\mathfrak{p}$ is a quasi-character of $G_\mathfrak{p}$.

Lemma 7.16. $c_\mathfrak{p}$ is trivial on $H_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$, and we have for $\mathfrak{a} = (\mathfrak{a}_\mathfrak{p}) \in G$

$$c(\mathfrak{a}) = \prod_{\mathfrak{p}} c_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})$$

Proof. For $\mathbb{C}^\times$ has no small subgroup. □

Lemma 7.17. For each $\mathfrak{p}$ let $c_\mathfrak{p}$ be a given quasi-character of $G_\mathfrak{p}$ and $c_\mathfrak{p}$ is trivial on $H_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$. Then $c : G \to \mathbb{C}^\times$ defined by

$$c(\mathfrak{a}) = \prod_{\mathfrak{p}} c_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})$$

is a quasi-character.

Proof. c is clearly multiplicative. To see continuity let $S \subseteq \{\mathfrak{p}\}$ be a finite subset consisting of all $\mathfrak{p}$ with $c_\mathfrak{p}(H_\mathfrak{p}) \neq 1$ and let $s = \#S$. Given a neighborhood U of 1 in $\mathbb{C}^\times$ choose a neighborhood V of 1 such that $V^s \subseteq U$. Let $N_\mathfrak{p}$ be a neighborhood of 1 in $G_\mathfrak{p}$ such that $c_\mathfrak{p}(N_\mathfrak{p}) \subseteq V$ for all $\mathfrak{p} \in S$, and let $N_\mathfrak{p} = H_\mathfrak{p}$ for $\mathfrak{p} \notin S$. Then

$$c\left(\prod_{\mathfrak{p}} N_\mathfrak{p}\right) \subseteq V^s \subseteq U$$

□

Now consider the (unitary) characters. Note that $c(\mathfrak{a}) = \prod\limits_{\mathfrak{p}} c_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})$ defines a character if and only if all $c_\mathfrak{p}$ are characters.

- For each $\mathfrak{p}$ let $\widehat{G_\mathfrak{p}}$ denote the character group of $G_\mathfrak{p}$.
- For those $\mathfrak{p}$ where $H_\mathfrak{p}$ is defined, let $H_\mathfrak{p}^\perp \leqslant \widehat{G_\mathfrak{p}}$ be the subgroup of all $c_\mathfrak{p} \in \widehat{G_\mathfrak{p}}$ which are trivial on $H_\mathfrak{p}$.

That $H_\mathfrak{p}$ is compact implies $\widehat{H_\mathfrak{p}} \cong \widehat{G}_\mathfrak{p}/H_\mathfrak{p}^\perp$ is discrete, and thus $H_\mathfrak{p}^\perp$ is open. Also, since $H_\mathfrak{p}$ is open, $G_\mathfrak{p}/H_\mathfrak{p}$ is discrete, and thus $H_\mathfrak{p}^\perp \cong \widehat{G_\mathfrak{p}/H_\mathfrak{p}}$ is compact.

Theorem 7.18. The restricted product of the groups $\widehat{G_\mathfrak{p}}$ with respect to the subgroups $H_\mathfrak{p}^\perp$ is naturally isomorphic to the character group $\widehat{G}$ of G as topological groups.

Proof. The isomorphism is given by

$$\begin{tikzcd}
\prod_{\mathfrak{p}}' \widehat{G_\mathfrak{p}} \arrow[r] & \widehat{G} \\
(c_\mathfrak{p}) \arrow[r, mapsto] & c := \prod_{\mathfrak{p}} c_\mathfrak{p}
\end{tikzcd}$$

The preceding lemmas show that this is an abstract group isomorphism. It remains to show it is a homeomorphism. Let K be a compact set in G and $\varepsilon > 0$. We may assume $K = \prod_{\mathfrak{p}} B_{\mathfrak{p}}$ as described in Lemma 7.15. Let S consist of all $\mathfrak{p}$ with $B_{\mathfrak{p}} \neq H_{\mathfrak{p}}$ and $n = \#S$. Then

$$c \in \{\chi \in \widehat{G} \mid |\chi(K) - 1| < \varepsilon\} \Leftrightarrow \left|\prod_{\mathfrak{p}} c_{\mathfrak{p}}(B_{\mathfrak{p}}) - 1\right| < \varepsilon$$

For $\mathfrak{p} \in S$ let $V_{\mathfrak{p}} := \{\chi \in \widehat{G_{\mathfrak{p}}} \mid |\chi(B_{\mathfrak{p}}) - 1| < \rho := (\varepsilon + 1)^{\frac{1}{n}} - 1\}$, and for $\mathfrak{p} \notin S$ let $V_{\mathfrak{p}} = H_{\mathfrak{p}}^{\perp}$. Now for $(c_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} V_{\mathfrak{p}}$, we have

$$\left|\prod_{\mathfrak{p}} c_{\mathfrak{p}}(B_{\mathfrak{p}}) - 1\right| < (1 + \rho)^n - 1 = \varepsilon$$

so that $(c_{\mathfrak{p}}) \mapsto c$ is continuous. Conversely, let $S \subseteq \{\mathfrak{p}\}$ be a finite set with $\#S = n$ and $1 > \varepsilon > 0$. For $\mathfrak{p} \in S$ let $K_{\mathfrak{p}}$ be a compact set in $G_{\mathfrak{p}}$ and put $V_{\mathfrak{p}} = \{\chi \in \widehat{G_{\mathfrak{p}}} \mid |\chi(K_{\mathfrak{p}}) - 1| < \varepsilon\}$, and for $\mathfrak{p} \notin S$ put $V_{\mathfrak{p}} = H_{\mathfrak{p}}^{\perp}$. Put $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and let $K = \left(\{1\} \times \cdots \times \{1\} \cup \bigcup_{i=1}^{n} \left(K_{\mathfrak{p}_i} \times \prod_{j \neq i} \{1\}\right)\right) \times \prod_{\mathfrak{p} \notin S} H_{\mathfrak{p}}$ which is a compact set in G. Then for $c \in \widehat{G}$ with $|c(K) - 1| < \varepsilon$, we have the following:

- $|c_{\mathfrak{p}}(H_{\mathfrak{p}}) - 1| < \varepsilon$ for $\mathfrak{p} \notin S$. This implies $c_{\mathfrak{p}}(H_{\mathfrak{p}}) = 1$ because $c_{\mathfrak{p}}(H_{\mathfrak{p}})$ is a subgroup of S^1.
- $|c_{\mathfrak{p}_i}(K_{\mathfrak{p}_i}) - 1| < \varepsilon$ for $1 \leqslant i \leqslant n$.

Hence $(c_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} V_{\mathfrak{p}}$, showing $c \mapsto (c_{\mathfrak{p}})$ is continuous. □

Finally we consider the measure on the restricted product G. For each $\mathfrak{p}$ let $dx_{\mathfrak{p}}$ be a Haar measure on $G_{\mathfrak{p}}$ such that $\mathrm{vol}(H_{\mathfrak{p}}, dx_{\mathfrak{p}}) = 1$ for all but finitely many $\mathfrak{p}$. Define a measure $dx = \bigotimes_{\mathfrak{p}} dx_{\mathfrak{p}}$ on G as in 2.13. Then for $S \subseteq \{\mathfrak{p}\}$ finite, the restriction of dx to G^S is $dx_S := \bigotimes_{\mathfrak{p} \in S} dx_{\mathfrak{p}} \otimes dx^S$, where dx^S is the measure on the compact group G^S such that $\mathrm{vol}(G^S, dx^S) = \prod_{\mathfrak{p} \notin S} \mathrm{vol}(H_{\mathfrak{p}}, dx_{\mathfrak{p}}) = 1$.

Lemma 7.19. Let $f : G \to \mathbb{C}$ be a function. Then

$$\int_G f(x)dx = \lim_{S \subseteq \{\mathfrak{p}\},\, \#S < \infty} \int_{G_S} f(x)dx$$

if either

(i) f is measurable and $f \geqslant 0$, in which case $+\infty$ is allowed as value of the integral; or

(ii) $f \in L^1(G)$.

Proof. In either case,

$$\int_G f(x)dx = \lim_{K \underset{\text{cpt}}{\subseteq} G, K \nearrow G} \int_K f(x)dx$$

and the result follows from Lemma 7.15. □

Lemma 7.20. For each $\mathfrak{p}$ let $f_\mathfrak{p} \in L^1(G_\mathfrak{p})$ be continuous and $f_\mathfrak{p}(H_\mathfrak{p}) = 1$ for all but finitely many $\mathfrak{p}$. Define $f : G \to \mathbb{C}$ by

$$f(x) = \prod_\mathfrak{p} f_\mathfrak{p}(x_\mathfrak{p})$$

Then f is continuous on G, and for any set S containing at least those $\mathfrak{p}$ for which either $f_\mathfrak{p}(H_\mathfrak{p}) \neq 1$ or $\mathrm{vol}(H_\mathfrak{p}, dx_\mathfrak{p}) \neq 1$, we have

$$\int_{G_S} f(x)dx = \prod_{\mathfrak{p}\in S} \int_{G_\mathfrak{p}} f_\mathfrak{p}(x_\mathfrak{p})dx_\mathfrak{p}$$

Proof. f is clearly continuous on each G_S, whence continuous on the entire G. For the second, note that if $x \in G_S$, then $f(x) = \prod_{\mathfrak{p}\in S} f_\mathfrak{p}(x_\mathfrak{p})$. Hence

$$\begin{aligned}\int_{G_S} f(x)dx = \int_{G_S} f(x)dx_S &= \int_{G_S} \prod_{\mathfrak{p}\in S} f_\mathfrak{p}(x_\mathfrak{p}) \left(\bigotimes_{\mathfrak{p}\in S} dx_\mathfrak{p} \otimes dx^S\right) \\ &= \prod_{\mathfrak{p}\in S} \int_{G_\mathfrak{p}} f_\mathfrak{p}(x_\mathfrak{p})dx_\mathfrak{p} \cdot \int_{G^S} dx^S \\ &= \prod_{\mathfrak{p}\in S} \int_{G_\mathfrak{p}} f_\mathfrak{p}(x_\mathfrak{p})dx_\mathfrak{p}\end{aligned}$$

□

Theorem 7.21. Let $f_\mathfrak{p}$ and f be defined as above, and if furthermore

$$\prod_\mathfrak{p} \int_{G_\mathfrak{p}} |f_\mathfrak{p}(x_\mathfrak{p})|dx_\mathfrak{p} = \lim_{S\subseteq\{\mathfrak{p}\}, \#S<\infty} \prod_{\mathfrak{p}\in S} \int_{G_\mathfrak{p}} |f_\mathfrak{p}(x_\mathfrak{p})|dx_\mathfrak{p} < \infty$$

then $f \in L^1(G)$, and

$$\int_G f(x)dx = \prod_\mathfrak{p} \int_{G_\mathfrak{p}} f_\mathfrak{p}(x_\mathfrak{p})dx_\mathfrak{p}$$

Let $dc_\mathfrak{p}$ be the measure on $\widehat{G_\mathfrak{p}}$ dual to the measure $dx_\mathfrak{p}$ on $G_\mathfrak{p}$. Note that if $f_\mathfrak{p} = \mathbf{1}_{H_\mathfrak{p}}$, then the Fourier transform

$$\widehat{f}_\mathfrak{p}(c_\mathfrak{p}) = \int_{G_\mathfrak{p}} f_\mathfrak{p}(x_\mathfrak{p})\overline{c_\mathfrak{p}(x_\mathfrak{p})}dx_\mathfrak{p}$$

is $\operatorname{vol}(H_{\mathfrak{p}}, dx_{\mathfrak{p}})\mathbf{1}_{H_{\mathfrak{p}}^{\perp}}$. A consequence of this fact and the inversion formula is that

$$\operatorname{vol}(H_{\mathfrak{p}}, dx_{\mathfrak{p}})\operatorname{vol}(H_{\mathfrak{p}}^{\perp}, dc_{\mathfrak{p}}) = 1$$

Therefore $\operatorname{vol}(H_{\mathfrak{p}}, dc_{\mathfrak{p}}) = 1$ for all but finitely many $\mathfrak{p}$, and we may put $dc = \bigotimes_{\mathfrak{p}} dc_{\mathfrak{p}}$.

Lemma 7.22. If $f_{\mathfrak{p}} \in \operatorname{inv}(G_{\mathfrak{p}})$ for all $\mathfrak{p}$ and $f_{\mathfrak{p}} = \mathbf{1}_{H_{\mathfrak{p}}}$ for all but finitely many $\mathfrak{p}$, then the function $f(x) := \prod_{\mathfrak{p}} f_{\mathfrak{p}}(x_{\mathfrak{p}})$ has the Fourier transform

$$\widehat{f}(c) = \prod_{\mathfrak{p}} \widehat{f}_{\mathfrak{p}}(c_{\mathfrak{p}})$$

and $f \in \operatorname{inv}(G)$.

Proof. Apply the previous theorem to the function $f(x)\overline{c(x)}$ to see the first statement. Since $f_{\mathfrak{p}} \in \operatorname{inv}(G_{\mathfrak{p}})$, $\widehat{f}_{\mathfrak{p}} \in L^1(\widehat{G_{\mathfrak{p}}})$ (by definition) for all $\mathfrak{p}$. For all but finitely many $\mathfrak{p}$ we have $\widehat{f}_{\mathfrak{p}} = \mathbf{1}_{H_{\mathfrak{p}}^{\perp}}$ as said above, so $\widehat{f} \in L^1(\widehat{G})$, whence $f \in \operatorname{inv}(G)$. □

Corollary 7.22.1. The measure $dc = \bigotimes_{\mathfrak{p}} dc_{\mathfrak{p}}$ is dual to $dx = \bigotimes_{\mathfrak{p}} dx_{\mathfrak{p}}$.

Proof. Apply the preceding lemma to the group $\widehat{G}$ with the measure dc and the "product" functions. To be precise, we have

$$\widehat{\widehat{f}}(x) = \prod_{\mathfrak{p}} \widehat{\widehat{f}}_{\mathfrak{p}}(x_{\mathfrak{p}}) = \prod_{\mathfrak{p}} f_{\mathfrak{p}}(-x_{\mathfrak{p}}) = f(-x)$$

□

7.3 The Theory in the Large

7.3.1 Additive Theory

Let k denote an algebraic number field and $\mathfrak{p}$ the generic prime divisor of k. The completion of k at $\mathfrak{p}$ is denoted by $k_{\mathfrak{p}}$, and all the symbol $\mathfrak{o}$, Λ, $\mathfrak{d}$, $|\cdot|$, c, etc. defined before for this local field $k_{\mathfrak{p}}$ will also receive the subscript $\mathfrak{p}$, namely $\mathfrak{o}_{\mathfrak{p}}$, $\Lambda_{\mathfrak{p}}$, $\mathfrak{d}_{\mathfrak{p}}$, $|\cdot|_{\mathfrak{p}}$, $c_{\mathfrak{p}}$, etc.

Definition. The **ring of adele** $\mathbb{A}_k$ of k is the restricted product of the additive groups $k_{\mathfrak{p}}$ (over all prime divisors $\mathfrak{p}$) with respect to the subgroups $\mathfrak{o}_{\mathfrak{p}}$.

- The multiplication on $\mathbb{A}_k$ is defined componentwise.

- From Theorem 7.18, Lemma 7.3 and Lemma 7.6, we see the continuous dual $\widehat{\mathbb{A}_k}$ of $\mathbb{A}_k$ is naturally isomorphic to the restrict product of the $k_\mathfrak{p}$ with respect to the $\mathfrak{d}_\mathfrak{p}^{-1}$. Since $\mathfrak{d}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$ ($\mathfrak{d}_\mathfrak{p}$ is the closure of $\mathfrak{d} \subseteq \mathfrak{o}_k$ in $k_\mathfrak{p}$), so $\widehat{\mathbb{A}_k} \cong \mathbb{A}_k$, namely, $\mathbb{A}_k$ is self-dual.

  Explicitly, there is an isomorphism

  $$\begin{tikzcd}
\mathbb{A}_k \arrow[r] & \widehat{\mathbb{A}_k} \\
\eta = (\eta_\mathfrak{p}) \arrow[r, mapsto] & {[x = (x_\mathfrak{p}) \mapsto \prod_\mathfrak{p} \exp(2\pi i \Lambda_\mathfrak{p}(\eta_\mathfrak{p} x_\mathfrak{p}))]}
\end{tikzcd}$$

  Let us define the additive function $\Lambda(x) := \sum_\mathfrak{p} \Lambda_\mathfrak{p}(x_\mathfrak{p})$ on $\mathbb{A}_k$. Then

  $$\prod_\mathfrak{p} \exp(2\pi i \Lambda_\mathfrak{p}(\eta_\mathfrak{p} x_\mathfrak{p})) = \exp\left(2\pi i \sum_\mathfrak{p} \Lambda_\mathfrak{p}(\eta_\mathfrak{p} x_\mathfrak{p})\right) = e^{2\pi i \Lambda(\eta x)}$$

- On $\mathbb{A}_k$ we have the measure $dx = \bigotimes_\mathfrak{p} dx_\mathfrak{p}$ described in the previous section, where $dx_\mathfrak{p}$ is the local measure chosen to be self-dual (see the discussion before Theorem 7.8). Then by Corollary 7.22.1, the measure dx is also self-dual.

Theorem 7.23. For $f \in L^1(\mathbb{A}_k)$ define the Fourier transform

$$\hat{f}(\eta) = \int_{\mathbb{A}_k} f(x) e^{-2\pi i \Lambda(\eta x)} dx$$

Then for $f \in \operatorname{inv}(\mathbb{A}_k)$ the inversion formula

$$f(x) = \int_{\mathbb{A}_k} \hat{f}(\eta) e^{2\pi i \Lambda(\eta x)} d\eta$$

holds.

Lemma 7.24. For $a \in \mathbb{A}^\times$, $d(ax) = |a| dx$, where $|a| := \prod_\mathfrak{p} |a_\mathfrak{p}|_\mathfrak{p}$.

Proof. Let $N = \prod_\mathfrak{p} N_\mathfrak{p}$ be a compact neighborhood of 0 in V. Then

$$\operatorname{vol}(aN, dx) = \prod_\mathfrak{p} \operatorname{vol}(a_\mathfrak{p} N_\mathfrak{p}, dx_\mathfrak{p}) = |a| \prod_\mathfrak{p} \operatorname{vol}(N_\mathfrak{p}, dx_\mathfrak{p}) = |a| \operatorname{vol}(N, dx)$$

□

Lemma 7.25. Let S_∞ denote the set of all infinite places of k.

1. $k \cap \mathbb{A}_{k,S_\infty} = \mathfrak{o}$.

2. $k + \mathbb{A}_{k,S_\infty} = \mathbb{A}_k$.

Proof. 1. is simply the statement that an element in k is an algebraic integer if and only if it is an integer at all finite primes. 2. is the Chinese Remainder theorem. □

In the following we write $\mathbb{A} = \mathbb{A}_k$ and denote by $\mathbb{A}_\infty$ the infinite part of $\mathbb{A}$, i.e., the cartesian product of the archimedean completions of k. Suppose k has r_1 real places and r_2 pairs of conjugate non-real places; then $\mathbb{A}_\infty \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is naturally a real vector space of dimension $n = r_1 + 2r_2 = [k : \mathbb{Q}]$. For $x \in \mathbb{A}$ let x_∞ denote its projection onto $\mathbb{A}_\infty$.

Lemma 7.26. If $\{\omega_1, \dots, \omega_n\}$ is an integral basis for $\mathfrak{o}$, then $\{\omega_{1,\infty}, \dots, \omega_{n,\infty}\}$ is an $\mathbb{R}$-basis for $\mathbb{A}_\infty$. The parallelotope

$$D_\infty = \left\{ \sum_{\nu=1}^{n} x_\nu \omega_{\nu,\infty} \mid 0 \leqslant x_\nu < 1 \text{ for } 1 \leqslant \nu \leqslant x \right\} \subseteq \mathbb{A}_\infty$$

has volume $\sqrt{|\operatorname{disc} k|}$, where $\operatorname{disc} k$ is the absolute discriminant of k and we use the measure $dx_\infty := \bigotimes_{\mathfrak{p} \in S_\infty} dx_{\mathfrak{p}}$.

Proof. This is the classical Minkowski theory. Note that for complex $\mathfrak{p}$ the measure we choose is twice the ordinary measure on the complex plane. □

Definition. The set $D := \prod_{\mathfrak{p} \nmid \infty} \mathfrak{o}_{\mathfrak{p}} \times D_\infty$ is called the **additive fundamental domain**.

Theorem 7.27.

1. D deserves its name, i.e., every element $x \in \mathbb{A}$ is congruent mod k to one and only one element in D.

2. $\operatorname{vol}(D, dx) = 1$.

Proof.

1. Let $x \in \mathbb{A}$. Use Chinese Remainder theorem to find a unique element modulo $\mathfrak{o}$ that brings x into $\mathbb{A}_{S_\infty}$, and find a unique element in $\mathfrak{o}$ which takes x into D_∞.

2.
$$\operatorname{vol}(D, dx) = \operatorname{vol}(D, dx_{S_\infty}) = \operatorname{vol}(D_\infty, dx_\infty) \operatorname{vol}(\mathbb{A}^{S_\infty}, dx^{S_\infty}) = \sqrt{|\operatorname{disc} k|} \prod_{\mathfrak{p} \notin S_\infty} (N_{\mathfrak{p}} \mathfrak{d}_{\mathfrak{p}})^{-\frac{1}{2}}$$

   As ideals, $\operatorname{disc} k$ is the norm of the absolute different $\mathfrak{d}$ of k, and $\mathfrak{d}$ is the product of the local differents $\mathfrak{d}_{\mathfrak{p}}$, we have

$$|\operatorname{disc} k| = \prod_{\mathfrak{p} \nmid \infty} N_{\mathfrak{p}} \mathfrak{d}_p$$

   and thus $\operatorname{vol}(D, dx) = 1$.

□

Corollary 7.27.1. $k \subseteq \mathbb{A}$ is discrete and $\mathbb{A}/k$ is compact.

Proof. k is discrete since D has an interior, and $\mathbb{A}/k$ is compact since D is relatively compact. □

Lemma 7.28. $\Lambda(\xi) = 0$ for all $\xi \in k$.

Proof.

$$\Lambda(\xi) = \sum_{\mathfrak{p}} \Lambda_{\mathfrak{p}}(\xi) = \sum_{\mathfrak{p}} \lambda_p(\mathrm{Tr}_{k_{\mathfrak{p}}/\mathbb{Q}_p}(\xi)) = \sum_{p} \lambda_p \left(\sum_{\mathfrak{p}|p} \mathrm{Tr}_{k_{\mathfrak{p}}/\mathbb{Q}_p}(\xi) \right) = \sum_{p} \lambda_p(\mathrm{Tr}_{k/\mathbb{Q}}(\xi))$$

since the trace is the sum of the local traces. Since $\mathrm{Tr}_{k/\mathbb{Q}}(\xi) \in \mathbb{Q}$, it suffices to show $\sum_p \lambda_p(x) \equiv 0 \pmod 1$ for $x \in \mathbb{Q}$. For any finite prime q

$$\sum_p \lambda_p(x) = \sum_{p \neq q, \infty} \lambda_p(x) + \lambda_q(x) + \lambda_\infty(x) = \sum_{p \neq q, \infty} \lambda_p(x) + (\lambda_q(x) - x)$$

is a q-adic integer. This shows $\sum_p \lambda_p(x) \equiv 0 \pmod 1$. □

Theorem 7.29. We have $k^\perp = k$, i.e., $\Lambda(x\xi) = 0$ for all $\xi \in k$ if and only if $x \in k$.

Proof. Since $k^\perp = \widehat{\mathbb{A}/k}$ and $\mathbb{A}/k$ is compact, $k^\perp$ is discrete. By Lemma 7.28, $k^\perp$ contains k. We consider the quotient $k^\perp/k$. As a discrete subgroup of the compact group $\mathbb{A}/k$, $\#k^\perp/k < \infty$ (a discrete subgroup is locally compact, so it is closed by Lemma 7.4). Since $k^\perp$ is also a vector space over k and k is not a finite field, $\#k^\perp/k$ cannot be finite unless $\#k^\perp/k = 1$, i.e., $k^\perp = k$. □

7.3.2 Riemann-Roch Theorem

We use the notations in the previous subsection.

Definition. A function $\varphi : \mathbb{A}_k \to \mathbb{C}$ is called **periodic** if $\varphi(x + r) = \varphi(x)$ for all $x \in \mathbb{A}_k$ and $r \in k$.

Lemma 7.30. If $\varphi : \mathbb{A}_k \to \mathbb{C}$ is continuous and periodic, then

$$\int_D \varphi(x)dx = \int_{\mathbb{A}_k/k} \varphi(\overline{x})d\overline{x}$$

where $\varphi(\overline{x}) : \mathbb{A}_k/k \to \mathbb{C}$ is the map induced by φ, and $d\overline{x}$ is the Haar measure on $\mathbb{A}_k/k$ such that $\mathrm{vol}(\mathbb{A}_k/k, d\overline{x}) = 1$.

Proof. The map $\varphi \mapsto \int_D \varphi(x)dx$ defines a Haar integral on $\mathbb{A}_k/k$, and it has norm 1 since $\mathrm{vol}(D, dx) = 1$ (c.f. Theorem 7.27.2). □

By Theorem 7.29, $\widehat{\mathbb{A}_k/k} \cong k^{\perp} = k$. The Fourier transform of a continuous function on $\mathbb{A}_k/k$ induced by $\varphi : \mathbb{A}_k \to \mathbb{C}$ is then represented by

$$\widehat{\varphi}(r) = \int_D \varphi(x) e^{-2\pi i \Lambda(xr)} dx$$

where $r \in k$.

Lemma 7.31. If $\varphi : \mathbb{A}_k \to \mathbb{C}$ is continuous and periodic and $\sum\limits_{r \in k} |\widehat{\varphi}(r)| < \infty$, then

$$\varphi(x) = \sum_{r \in k} \widehat{\varphi}(r) e^{2\pi i \Lambda(xr)}$$

Proof. The hypothesis $\sum\limits_{r \in k} |\widehat{\varphi}(r)| < \infty$ means $\widehat{\varphi} \in L^1(k) = L^1(\widehat{\mathbb{A}_k/k})$, so the inversion formula holds, whence the asserted identity in L^1 sense. Since the series on RHS defines a continuous function, the identity in fact holds for every $x \in \mathbb{A}_k$. □

Lemma 7.32. Let $f : \mathbb{A}_k \to \mathbb{C}$ be continuous and integrable. Suppose $\sum\limits_{r \in k} |f(x+k)|$ is uniformly convergent for $x \in D$. Then for the resulting continuous periodic function $\varphi(x) := \sum\limits_{r \in k} f(x+r)$, we have $\widehat{\varphi}(y) = \widehat{f}(y)$.

Proof.

$$\begin{aligned}
\widehat{\varphi}(y) &= \int_D \varphi(x) e^{-2\pi i \Lambda(xy)} dx \\
&= \int_D \left(\sum_{r \in k} f(x+r) e^{-2\pi i \Lambda(xy)} \right) dx \\
&= \sum_{r \in k} \int_D f(x+r) e^{-2\pi i \Lambda(xy)} dx \\
&= \sum_{r \in k} \int_{r+D} f(x) e^{-2\pi i \Lambda((x-r)y)} dx \\
&= \sum_{r \in k} \int_{r+D} f(x) e^{-2\pi i \Lambda(xy)} dx \\
&= \int_{\mathbb{A}_k} f(x) e^{-2\pi i \Lambda(xy)} dx \\
&= \widehat{f}(y)
\end{aligned}$$

We explain some equalities. The third equality is due to the uniform convergence and that $\mathrm{vol}(D, dx) < \infty$. Precisely, for each $\varepsilon > 0$ we can find a finite $S \subseteq k$ such that $|\sum_{r \in k} f(x+r) - \sum_{r \in S} f(x+r)| < \varepsilon$ for all $x \in D$. Hence

$$\begin{aligned}
&\left| \int_D \left(\sum_{r \in k} f(x+r) e^{-2\pi i \Lambda(xy)} \right) dx - \sum_{r \in S} \int_D f(x+r) e^{-2\pi i \Lambda(xy)} dx \right| \\
&\leqslant \int_D \left| \sum_{r \in k} f(x+r) - \sum_{r \in S} f(x+r) \right| dx < \mathrm{vol}(D, dx)\varepsilon
\end{aligned}$$

The fifth equality follows from Lemma 7.28, and the sixth results from the fact $\mathbb{A}_k = \bigsqcup_{r\in k} r + D$. □

Lemma 7.33 (Poisson summation formula)**.** Let $f : \mathbb{A}_k \to \mathbb{C}$ be a continuous and integrable map. If

- $\sum_{r\in k} |f(x+r)|$ converges uniformly for $x \in D$ and
- $\sum_{r\in k} |\widehat{f}(r)|$ converges,

then we have

$$\sum_{r\in k} \widehat{f}(r) = \sum_{r\in k} f(r)$$

.

Proof. Consider the series $\varphi(x) := \sum_{r\in k} f(x+r)$. By Lemma 7.32 we see $\widehat{\varphi}(x) = \widehat{f}(x)$, and by Lemma 7.31

$$\sum_{r\in k} f(x+r) = \varphi(x) = \sum_{r\in k} \widehat{\varphi}(r) e^{2\pi i \Lambda(xr)} = \sum_{r\in k} \widehat{f}(r) e^{2\pi i \Lambda(xr)}$$

Now the result following once we taking $x = 0$ in the above identity. □

Theorem 7.34 (Riemann-Roch)**.** Let $f : \mathbb{A}_k \to \mathbb{C}$ be a continuous and integrable map. If

- $\sum_{r\in k} |f(a(x+r))|$ converges for all $a \in \mathbb{A}_k^\times$ and $x \in \mathbb{A}_k$ and converges uniformly for $x \in D$, and
- $\sum_{r\in k} |\widehat{f}(ar)|$ converges for all ideles $a \in \mathbb{A}_k^\times$,

then for all $a \in \mathbb{A}_k^\times$ we have

$$\frac{1}{|a|} \sum_{r\in k} \widehat{f}\left(\frac{r}{a}\right) = \sum_{r\in k} f(ar)$$

Proof. Let $a \in \mathbb{A}_k^\times$. Define $g : \mathbb{A}_k \to \mathbb{C}$ by $g(x) := f(ax)$. We have

$$\widehat{g}(x) = \int_{\mathbb{A}_k} f(ay) e^{-2\pi i \Lambda(xy)} dy = \frac{1}{|a|} \int_{\mathbb{A}_k} f(y) e^{-2\pi i \Lambda(xy/a)} dy = \frac{1}{|a|} \widehat{f}\left(\frac{x}{a}\right)$$

and from this equality we can easily see that g satisfies all assumptions in Poisson summation formula. Therefore we obtain

$$\frac{1}{|a|} \sum_{r\in k} \widehat{f}\left(\frac{r}{a}\right) = \sum_{r\in k} \widehat{g}(r) = \sum_{r\in k} g(r) = \sum_{r\in k} f(ar)$$

□

Remark 7.35. Suppose we do not know $\mathrm{vol}(D, dx)$. Then the Poisson summation formula would read

$$\frac{1}{\mathrm{vol}(D, dx)} \sum_{r\in k} \widehat{f}(r) = \sum_{r\in k} f(r)$$

Iteration of this yields $\mathrm{vol}(D, dx)^2 = 1$, whence $\mathrm{vol}(D, dx) = 1$.

Remark 7.36. For the relation between Theorem 7.34 and the classical Riemann-Roch, see GTM186.

7.3.3 Multiplicative Theory

Definition. The **idele group** $\mathbb{A}_k^\times$ is topologized as the restricted product of the group $k_\mathfrak{p}^\times$ with respect to the unit groups $\mathfrak{o}_\nu^\times$.

- For each $\mathfrak{p}$ we choose a local measure $d^\times x_\mathfrak{p}$ as in the discussion preceding Lemma 7.11, and patch them together to obtain a Haar measure $d^\times x$ on $\mathbb{A}_k^\times$ by the method of 2.13.
- The natural map

$$\begin{aligned} \varphi : \mathbb{A}_k^\times &\longrightarrow \{\text{all fractional ideals of } k\} \\ x &\longmapsto \prod_{\mathfrak{p}\notin S_\infty} \mathfrak{p}^{\operatorname{ord}_\mathfrak{p} x_\mathfrak{p}} \end{aligned}$$

  is a continuous homomorphism from $\mathbb{A}_k^\times$ onto the discrete group of fractional ideals with kernel $\mathbb{A}_{k,S_\infty}^\times$.
- We embed $k^\times$ into $\mathbb{A}_k^\times$ diagonally.

Theorem 7.37 (Product formula)**.** For all $r \in k^\times$, $|r| := \prod_{\mathfrak{p}} |r|_\mathfrak{p} = 1$.

Proof. This is Corollary 2.16.3. Alternatively, we can argue as follows. Consider an additive fundamental domain D. Since $rk = k$, rD is also an additive fundamental domain. Since $\operatorname{vol}(rD, dx) = |r| \operatorname{vol}(D, dx)$ by Lemma 7.24, it suffices to show $\operatorname{vol}(rD, dx) = \operatorname{vol}(D, dx)$. We have

$$D = D \cap \mathbb{A}_k = D \cap \bigsqcup_{\alpha\in k} (\alpha + rD) = \bigsqcup_{\alpha\in k} D \cap (\alpha + rD)$$

and

$$rD = rD \cap \mathbb{A}_k = rD \cap \bigsqcup_{\alpha\in k} (-\alpha + D) = \bigsqcup_{\alpha\in k} rD \cap (-\alpha + D)$$

Since dx is a Haar measure, $\operatorname{vol}(D \cap (\alpha + rD), dx) = \operatorname{vol}((-\alpha + D) \cap rD, dx)$, and thus

$$\operatorname{vol}(D, dx) = \sum_{\alpha\in k} \operatorname{vol}(D \cap (\alpha + rD), dx) = \sum_{\alpha\in k} \operatorname{vol}((-\alpha + D) \cap rD, dx) = \operatorname{vol}(rD, dx)$$

□

Definition. The kernel of the surjective continuous homomorphism

$$\begin{aligned} \mathbb{A}_k^\times &\longrightarrow \mathbb{R}_{>0} \\ x &\longmapsto |x| = \prod_{\mathfrak{p}} |x_\mathfrak{p}|_\mathfrak{p} \end{aligned}$$

is denoted by $(\mathbb{A}_k^\times)^1$, and it consists of ideles of norm 1.

- By the product formula, we have $k^\times \subseteq (\mathbb{A}_k^\times)^1$.

Let $\mathfrak{p}_0$ be an arbitrary archimedean prime of k, and let

$$T := \left\{(a_\mathfrak{p}) \in \mathbb{A}_k^\times \mid a_{\mathfrak{p}_0} > 0 \text{ and } a_\mathfrak{p} = 1 \text{ if } \mathfrak{p} \neq \mathfrak{p}_0\right\}$$

An idele in T is uniquely determined by its norm, so it will cause no confusion if we denote an idele in T simply by the real number which is its norm. Thus a positive real number t also stands either for the idele $(t, 1, 1, \ldots)$ or for the idele $(\sqrt{t}, 1, 1, \ldots)$ depending on whether $\mathfrak{p}_0$ is real or complex. For each idele $x \in \mathbb{A}_k^\times$, we can write it uniquely as $x = |x|x'$ with $|x| \in T$ and $x' = x|x|^{-1} \in (\mathbb{A}_k^\times)^1$, so $\mathbb{A}_k^\times \cong T \times (\mathbb{A}_k^\times)^1$. On T we choose the Haar measure $d^\times t = t^{-1}dt$; then there exists a unique Haar measure d^1x on $(\mathbb{A}_k^\times)^1$ such that the integration formula

$$\int_{\mathbb{A}_k^\times} f(x)d^\times x = \int_0^\infty \left(\int_{(\mathbb{A}_k^\times)^1} f(tx)d^1x\right)\frac{dt}{t} = \int_{(\mathbb{A}_k^\times)^1}\left(\int_0^\infty f(tx)\frac{dt}{t}\right)d^1x$$

is valid for all $f \in L^1(\mathbb{A}_k^\times)$.

We wish to describe a fundamental domain for $(\mathbb{A}_k^\times)^1$ mod $k^\times$. Let S'_∞ be the set of all archimedean primes except $\mathfrak{p}_0$. Consider the log map

$$\begin{aligned} \ell : (\mathbb{A}_k^\times)^1_{S_\infty} := (\mathbb{A}_k^\times)^1 \cap \left(\mathbb{A}_k^\times\right)_{S_\infty} &\longrightarrow \mathbb{R}^{r_1+r_2-1} \\ x &\longmapsto (\log|x|_\mathfrak{p})_{\mathfrak{p}\in S'_\infty} \end{aligned}$$

where r_1 is the number of real primes and r_2 the number of complex primes. This is a surjective continuous homomorphism. The surjectivity is because we can adjust the $\mathfrak{p}_0$-component.

The subgroup $k^\times \cap (\mathbb{A}_k^\times)^1_{S_\infty}$ is simply the unit group $\mathfrak{o}^\times$ of the ring $\mathfrak{o}$. The units $\zeta \in \mathfrak{o}^\times$ for which $\ell(\zeta) = 0$ are the roots of unity in k and form a finite cyclic group. By Dirichlet unit theorem, $\mathfrak{o}^\times$ modulo the group of roots of unity in k is a free abelian group of rank $r := r_1 + r_2 - 1$; say $\{\varepsilon_i\}_{1\leqslant i\leqslant r}$ is a basis. Then $\{\ell(\varepsilon_i)\}_{1\leqslant i\leqslant r}$ forms a basis for $\mathbb{R}^r$, and we may write for any $x \in (\mathbb{A}_k^\times)^1_{S_\infty}$

$$\ell(x) = \sum_{i=1}^r x_i\ell(\varepsilon_i)$$

with unique real numbers x_i. Let P be the fundamental parallelotope in $\mathbb{R}^r$ spanned by the $\ell(\varepsilon_i)$, $1 \leqslant i \leqslant r$, that is

$$P := \left\{\sum_{i=1}^r x_i\ell(\varepsilon_i) \in \mathbb{R}^r \mid 0 \leqslant x_i < 1,\ 1 \leqslant i \leqslant r\right\}$$

and let Q denote the unit cube in $\mathbb{R}^r$, i.e., $Q := \left\{(x_\mathfrak{p})_{\mathfrak{p}\in S'_\infty} \in \mathbb{R}^r \mid 0 \leqslant x_\mathfrak{p} < 1 \text{ for all } \mathfrak{p} \in S'_\infty\right\}$.

Lemma 7.38. We have

$$\operatorname{vol}(\ell^{-1}(P), d^1x) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\operatorname{disc} k|}}R$$

where

$$R = \pm \det(\log |\varepsilon_i|_{\mathfrak{p}})_{1 \leqslant i \leqslant r,\, \mathfrak{p} \in S'_\infty} > 0$$

is the regulator of k.

Proof. Since ℓ is a continuous surjective homomorphism (with compact kernel), we have

$$\frac{\mathrm{vol}(\ell^{-1}(P))}{\mathrm{vol}(\ell^{-1}(Q))} = \frac{\mathrm{vol}(P)}{\mathrm{vol}(Q)} = \pm \det(\log |\varepsilon_i|_{\mathfrak{p}}) = R$$

so we only need to show $\mathrm{vol}(\ell^{-1}(Q)) = \dfrac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\operatorname{disc} k|}}$.

$\ell^{-1}(Q)$ consists of $x \in (\mathbb{A}_k^\times)^1_{S_\infty}$ with $1 \leqslant |x|_{\mathfrak{p}} < e$ for all $\mathfrak{p} \in S'_\infty$ (where e is the Euler number). Let Q^* be the set of all $x \in (\mathbb{A}_k^\times)_{S_\infty}$ with $1 \leqslant |x|_{\mathfrak{p}} < e$ for all $\mathfrak{p} \in S_\infty$. Then

$$\mathrm{vol}(Q^*) = \int_{(\mathbb{A}_k^\times)^1} \left(\int_{tx \in Q^*} \frac{dt}{t} \right) d^1x = \int_{\ell^{-1}(Q)} \left(\int_{|x|_{\mathfrak{p}_0}^{-1}}^{e|x|_{\mathfrak{p}_0}^{-1}} \frac{dt}{t} \right) d^1x = \int_{\ell^{-1}(Q)} d^1x = \mathrm{vol}(\ell^{-1}(Q))$$

because $tx \in Q^*$ if and only if $x \in \ell^{-1}(Q)$ and $1 \leqslant |tx|_{\mathfrak{p}_0} < e$. Thus it suffices to show $\mathrm{vol}(Q^*) = \dfrac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\operatorname{disc} k|}}$.

Write $Q^* = \prod\limits_{\mathfrak{p} \in S_\infty} Q_{\mathfrak{p}} \times (\mathbb{A}_k^\times)^{S_\infty}$, where $Q^*_{\mathfrak{p}} := \left\{ r \in k_{\mathfrak{p}}^\times \mid 1 \leqslant |r|_{\mathfrak{p}} < e \right\}$ ($\mathfrak{p} \in S_\infty$). By nature of the measure $d^\times x$, it suffices to compute the volume of each component with respect to the local measure. For $\mathfrak{p}$ real,

$$\mathrm{vol}(Q_{\mathfrak{p}}) = 2 \int_1^e \frac{dt}{t} = 2$$

for $\mathfrak{p}$ complex,

$$\mathrm{vol}(Q_{\mathfrak{p}}) = \int_0^{2\pi} \int_1^{\sqrt{r}} \frac{2 dr d\theta}{r} = 2\pi$$

and by Lemma 7.11

$$\mathrm{vol}((\mathbb{A}_k^\times)^{S_\infty}) = \prod_{\mathfrak{p} \notin S_\infty} \mathrm{vol}(\mathfrak{o}_{\mathfrak{p}}^\times) = \prod_{\mathfrak{p} \notin S_\infty} (N_{\mathfrak{p}} \mathfrak{d}_p)^{-\frac{1}{2}} = \frac{1}{\sqrt{|\operatorname{disc} k|}}$$

The last equality is explained in Theorem 7.27. □

Let $h = \#\,\mathrm{Cl}(k)$ be the class number of k, and choose $x^{(1)}, \ldots, x^{(h)} \in (\mathbb{A}_k^\times)^1$ such that the corresponding ideals $\varphi(x^{(1)}), \ldots, \varphi(x^{(h)})$ represent the different ideal classes. Let w be the number of roots of unity in k. Let

$$E_0 := \left\{ x \in \ell^{-1}(P) \mid 0 \leqslant \operatorname{Arg} b_{\mathfrak{p}_0} < \frac{2\pi}{w} \right\}$$

We define the **multiplicative fundamental domain** E for $(\mathbb{A}_k^\times)^1$ mod $k^\times$ to be

$$E = E_0 x^{(1)} \cup \cdots \cup E_0 x^{(h)}$$

Theorem 7.39.

1. $(\mathbb{A}_k^\times)^1 = \bigsqcup_{r \in k^\times} rE$, so E deserves its name.

2. $\operatorname{vol}(E, d^1x) = \dfrac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|\operatorname{disc} k|}}$.

Proof.

1. Let $x \in (\mathbb{A}_k^\times)^1$. There is a unique $x^{(i)}$ such that $\varphi(x/x^{(i)})$ represents a principal ideal; say $\varphi(x/x^{(i)}) = \alpha\mathfrak{o}$ (α is unique modulo units). Then $\varphi(\alpha^{-1}x/x^{(i)}) = \mathfrak{o}$, so $\alpha^{-1}x/x^{(i)} \in (\mathbb{A}_k^\times)^1_{S_\infty}$. Up to a unique product of fundamental units ε_j, we may assume $\alpha^{-1}x/x^{(i)} \in \ell^{-1}(P)$. Multiplication by a root of unity in k we can further assume $\alpha^{-1}x/x^{(i)} \in E_0$, or $x \in \alpha x^{(i)} E_0$.

2. By $E = \bigsqcup_{i=1}^{h} x^{(i)} E_0$ and $\ell^{-1}(P) = \bigsqcup_{\zeta \in \mu(k)} \zeta E_0$, we have

$$\operatorname{vol}(E) = h \operatorname{vol}(E_0) = \frac{h}{w}\operatorname{vol}(\ell^{-1}(P)) = \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|\operatorname{disc} k|}}$$

□

Corollary 7.39.1. $k^\times$ is a discrete subgroup of $(\mathbb{A}_k^\times)^1$ (hence of $\mathbb{A}_k^\times$), and the quotient $(\mathbb{A}_k^\times)^1/k^\times$ is compact.

Proof. It is clear that E has nonempty interior and is contained in some compact set. □

Definition. A **Hecke character** is a quasi-character $\chi : \mathbb{A}_k^\times/k^\times \to \mathbb{C}^\times$ of the idele class group of k.

- Since $(\mathbb{A}_k^\times)^1/k^\times$ is compact, the restriction of a Hecke character to $(\mathbb{A}_k^\times)^1$ is a (unitary) character.

- A Hecke character that is trivial on $(\mathbb{A}_k^\times)^1$ has the form $x \mapsto |x|^s$ for some complex number s. Indeed, if $c : \mathbb{A}_k^\times \to \mathbb{C}^\times$ is such a map, then $c(x) = c(|x|(x/|x|)) = c(|x|)$ for each $x \in \mathbb{A}_k^\times$. Since every continuous homomorphism from $\mathbb{R}_{>0}$ to $\mathbb{C}^\times$ is of the form $t \mapsto t^s$, so $c(|x|) = |x|^s$ for some $s \in \mathbb{C}$.

- To each Hecke character $c : \mathbb{A}_k^\times \to \mathbb{C}^\times$ there exists a unique real number σ such that $|c(\cdot)| = |\cdot|^\sigma$. The number $\operatorname{wt}(c) := \sigma$ is called the **exponent / weight** of c. A quasi-character is a character if and only if its exponent is 0.

7.3.4 The ζ-function; Functional Equation

As in the local case, denote by $\mathfrak{z}$ the class of all functions $f : \mathbb{A}_k \to \mathbb{C}$ satisfying the following three conditions.

$\mathfrak{z}_1$) $f \in \operatorname{inv}(\mathbb{A}_k)$ (as in Theorem 7.8);

$\mathfrak{z}_2$) The series $\sum_{r\in k} f(\alpha(x+r))$ and $\sum_{r\in k} \widehat{f}(\alpha(x+r))$ are both uniformly convergent for $(\alpha, x) \in K \times D$, where D is the additive fundamental domain of $\mathbb{A}_k/k$ and K is some fixed compact subset of $\mathbb{A}_k^\times$.

$\mathfrak{z}_3$) $f(x)|x|^\sigma$ and $\hat{f}(x)|x|^\sigma$ are in $L^1(\mathbb{A}_k^\times)$ for $\sigma > 1$.

Note that if $f : \mathbb{A}_k \to \mathbb{C}$ is continuous, its restriction to the idele group $\mathbb{A}_k^\times$ is still continuous, for the topology we have adopted in $\mathbb{A}_k^\times$ is stronger than the subspace topology on $\mathbb{A}_k^\times$ induced from $\mathbb{A}_k$.

In view of ($\mathfrak{z}_1$) and ($\mathfrak{z}_2$), the Riemann-Roch theorem is valid for functions in $\mathfrak{z}$. The purpose of ($\mathfrak{z}_3$) is the following.

Definition. For each $f \in \mathfrak{z}$ and Hecke character c of k with exponent greater than 1, we define the **ζ-integral**

$$\zeta(f, c) := \int_{\mathbb{A}_k^\times} f(x)c(x)d^\times x$$

Two Hecke-characters are called equivalent if they coincide on $(\mathbb{A}_k^\times)^1$. Then an equivalence class consists of all Hecke characters of the form $c(x) = c_0(x)|x|^s$, where c_0 is a fixed representative from the class and s is a complex number. As in the local case, the parametrization by $s \in \mathbb{C}$ lets us think of a class as a Riemann surface, and we can show by ($\mathfrak{z}_3$) that for each Hecke character c of exponent > 1, the integral

$$\int_{\mathbb{A}^\times} f(x)c(x)|x|^s d^\times x$$

defines a holomorphic function of s near $s = 0$.

Theorem 7.40. A ζ-function $\zeta(f, c)$ has an analytic continuation to the domain of all Hecke characters which is entire except at $c = \mathbf{1}$ and $c = |\cdot|$, where it has simple poles with residue $-\kappa f(0)$ and $\kappa \widehat{f}(0)$, respectively, where κ is the volume of the multiplicative fundamental domain (c.f. Theorem 7.39).

The function $\zeta(f, c)$ satisfies the functional equation

$$\zeta(f, c) = \zeta(\widehat{f}, \widehat{c})$$

where $\widehat{c}(x) := |x|c^{-1}(x)$ is defined as in the local theory.

Proof. Let c be a Hecke character of exponent > 1. We have

$$\zeta(f, c) = \int_{\mathbb{A}_k^\times} f(x)c(x)d^\times x = \int_0^\infty \left(\int_{(\mathbb{A}_k^\times)^1} f(tx)c(tx)d^1 x \right) \frac{dt}{t} \overset{\text{say}}{=} \int_0^\infty \zeta_t(f, c)\frac{dt}{t}$$

Here for almost all t the integral

$$\zeta_t(f, c) = \int_{(\mathbb{A}_k^\times)^1} f(tx)c(tx)d^1 x$$

is absolute convergent for c of all exponents, because it is convergent for some c and $|c(tx)| = t^{\mathrm{wt}(c)}$ is constant for $x \in (\mathbb{A}_k^\times)^1$. □

Lemma 7.41. For all Hecke characters c we have

$$\zeta_t(f,c) + f(0)\int_E c(tx)d^\times x = \zeta_{1/t}(\widehat{f},\widehat{c}) + \widehat{f}(0)\int_E \widehat{c}\left(\frac{x}{t}\right)d^\times x$$

where E is the multiplicative fundamental domain.

Proof. Since $(\mathbb{A}_k^\times)^1 = \bigsqcup_{\alpha\in k^\times} \alpha E$, we have

$$\begin{aligned}\zeta_t(f,c) + f(0)\int_E c(tx)d^\times x &= \sum_{\alpha\in k^\times}\int_{\alpha E} f(tx)c(tx)d^1x + f(0)\int_E c(tx)d^1x \\ &= \sum_{\alpha\in k^\times}\int_{E} f(\alpha tx)c(tx)d^1x + f(0)\int_E c(tx)d^1x\end{aligned}$$

By $(\mathfrak{z}_2)$ for f, the sum $\sum_{\alpha\in k^\times} f(\alpha tx)$ converges compactly in E, and a similar argument to Lemma 7.32 says we can interchange the sum and the integral. Thus

$$\begin{aligned}\zeta_t(f,c) &= \int_E\left(\sum_{\alpha\in k^\times} f(\alpha tx)\right)c(tx)d^1x + f(0)\int_E c(tx)d^1x \\ &= \int_E\left(\sum_{\alpha\in k} f(\alpha tx)\right)c(tx)d^1x \\ \text{(Riemann-Roch)} &= \int_E\left(\sum_{\alpha\in k}\widehat{f}\left(\frac{\alpha}{tx}\right)\right)\frac{1}{|tx|}c(tx)d^1x \overset{x\mapsto x^{-1}}{=} \int_E\left(\sum_{\alpha\in k}\widehat{f}\left(\frac{\alpha x}{t}\right)\right)\widehat{c}\left(\frac{x}{t}\right)d^1x\end{aligned}$$

Reversing the steps completes the proof. □

Lemma 7.42.

$$\int_E c(tx)d^1x = \begin{cases}\kappa t^s & \text{, if } c(x) = |x|^s \\ 0 & \text{, if } c|_{(\mathbb{A}_k^\times)^1} \neq \mathbf{1}\end{cases}$$

Proof. This is clear since integration of $c(x)$ over E is the same as integration over of $c(x)$ the compact group $(\mathbb{A}_k^\times)^1/k^\times$, and $c(t) = |t|^s = t^s$. □

To prove the theorem, for c of exponent > 1 write

$$\zeta(f,c) = \int_0^\infty \zeta_t(f,c)\frac{dt}{t} = \int_0^1 \zeta_t(f,c)\frac{dt}{t} + \int_1^\infty \zeta_t(f,c)\frac{dt}{t}$$

The latter term

$$\int_1^\infty \zeta_t(f,c)\frac{dt}{t} = \int_{|x|\geqslant 1} f(x)c(x)d^\times x$$

converges absolutely for all Hecke characters c, for we already know it converges for those of exponent > 1, and the less the exponent is, the better it converges. For the former term, we use the lemmas.

$$\int_0^1 \zeta_t(f,c)\frac{dt}{t} = \int_0^1 \zeta_{1/t}(\widehat{f},\widehat{c})\frac{dt}{t} + \left\{\int_0^1 \kappa\widehat{f}(0)\left(\frac{1}{t}\right)^{1-s}\frac{dt}{t} - \int_0^1 \kappa f(0)t^s\frac{dt}{t}\right\}$$

The curly bracket term appears only when c is trivial on $(\mathbb{A}_k^\times)^1$, in which case we assume $c(x) = |x|^s$. Since we are assuming $\mathrm{wt}(c) > 1$, that term makes sense, and equals

$$\frac{\kappa\widehat{f}(0)}{s-1} - \frac{\kappa f(0)}{s}$$

Making the substitute $t \mapsto 1/t$ in the main part, we obtain

$$\int_0^1 \zeta_t(f,c)\frac{dt}{t} = \int_1^\infty \zeta_t(\widehat{f},\widehat{c})\frac{dt}{t} + \left\{\frac{\kappa\widehat{f}(0)}{s-1} - \frac{\kappa f(0)}{s}\right\}$$

whence

$$\begin{aligned}\zeta(f,c) &= \int_1^\infty \zeta_t(f,c)\frac{dt}{t} + \int_1^\infty \zeta_t(\widehat{f},\widehat{c})\frac{dt}{t} + \left\{\frac{\kappa\widehat{f}(0)}{s-1} - \frac{\kappa f(0)}{s}\right\} \\ &= \int_{|x|>1} f(x)c(x)d^\times x + \int_{|x|>1} \widehat{f}(x)c^{-1}(x)|x|d^\times x + \left\{\frac{\kappa\widehat{f}(0)}{s-1} - \frac{\kappa f(0)}{s}\right\}\end{aligned}$$

The two integrals converge absolutely for all Hecke characters c (of arbitrary exponent), so it gives an analytic continuation of $\zeta(f,c)$, and from which we can directly read off the poles and residues. Observe also that this expression remains unchanged if we replace (f,c) by $(\widehat{f},\widehat{c})$, so the functional equation holds.

7.3.5 Comparison with the Classical Theory

In this subsection we shall exhibit for each equivalence class C of Hecke characters an explicit function $f \in \mathfrak{z}$ such that the corresponding ζ-function is nontrivial on C. These special ζ-functions will turn out to be, essentially, the classical ζ-functions and L-series. The analytic continuation and the functional equation for our ζ-functions will yield the same for the classical functions.

Each class of Hecke characters can be represented by a unitary Hecke character. To describe this in detail, we fix a finite set of primes S containing all archimedean primes, and discuss the characters which are unramified outside S. A character of this type is nothing more nor less than a product

$$c(x) = \prod_{\mathfrak{p}} c_{\mathfrak{p}}(x_{\mathfrak{p}})$$

of local characters $c_{\mathfrak{p}}$ satisfying the two conditions

(1) $c_{\mathfrak{p}}$ unramified outside S (i.e. $\mathfrak{c}_{\mathfrak{p}}|_{\mathfrak{o}_{\mathfrak{p}}^\times} = \mathbf{1}$).

(2) $\prod_{\mathfrak{p}} c_{\mathfrak{p}}(\alpha) = 1$ for all $\alpha \in k^\times$.

To construct such characters and express them in more concrete terms, we write for $\mathfrak{p} \in S$:

$$c_{\mathfrak{p}}(x_{\mathfrak{p}}) = \widetilde{c}_{\mathfrak{p}}(\widetilde{x}_{\mathfrak{p}})|x_{\mathfrak{p}}|_{\mathfrak{p}}^{it_{\mathfrak{p}}}$$

$\widetilde{c}_{\mathfrak{p}}$ being a character of $\mathfrak{o}_{\mathfrak{p}}^\times$, $t_{\mathfrak{p}}$ a real number (c.f. Theorem 7.10). For $\mathfrak{p} \notin S$ we throw all the local characters together into a single character, say

$$c^*(x) = \prod_{\mathfrak{p} \notin S} c_{\mathfrak{p}}(x_{\mathfrak{p}})$$

and interpret c^* as coming from an ideal character. Namely: The map

$$x \mapsto \varphi_S(x) := \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} x}$$

is a homomorphism of the idele group onto the multiplicative group of ideals prime to S. Its kernel is $(\mathbb{A}^\times)_S$. Since $c^*(x)$ is identity on $(\mathbb{A}^\times)_S$, we have

$$c^*(x) = \chi(\varphi_S(x))$$

for some character χ of the group of ideals prime to S. Our character $c(x)$ is now written in the form

$$c(x) = \prod_{\mathfrak{p} \in S} \widetilde{c}_{\mathfrak{p}}(\widetilde{x}_{\mathfrak{p}}) \cdot \prod_{\mathfrak{p} \in S} |x_{\mathfrak{p}}|_{\mathfrak{p}}^{it_{\mathfrak{p}}} \cdot \chi(\varphi_S(x))$$

To construct such characters we must select our $\widetilde{c}_{\mathfrak{p}}$, $t_{\mathfrak{p}}$ and χ such that $c(x) = 1$ for all $x \in k^\times$. For this purpose we first look at the S-units ε of k, i.e., the elements of $k^\times \cap (\mathbb{A}^\times)_S$ for which $\varphi_S(\varepsilon) = \mathfrak{o}$. Assume S contains $m+1$ primes; let ε_0 be a primitive root of unity in k and let $\{\varepsilon_1, \dots, \varepsilon_m\}$ be a basis for the free abelian group of S-units modulo roots of unity. For c to be trivial on the S-units it is then necessary and sufficient that $c(\varepsilon_\nu) = 1$, $0 \leqslant \nu \leqslant m$. The requirement $c(\varepsilon_0) = 1$ is simply a condition on the $\widetilde{c}_{\mathfrak{p}}$:

$$\prod_{\mathfrak{p}} \widetilde{c}_{\mathfrak{p}}(\varepsilon_0) = 1 \tag{A}$$

We therefore first select a set of $\widetilde{c}_{\mathfrak{p}}$ for $\mathfrak{p}$ which satisfies (A). The requirements $c(\varepsilon_\nu) = 1$, $1 \leqslant \nu \leqslant m$ gives the conditions on the $t_{\mathfrak{p}}$:

$$\prod_{\mathfrak{p} \in S} |\varepsilon_\nu|_{\mathfrak{p}}^{it_{\mathfrak{p}}} = \prod_{\mathfrak{p} \in S} \widetilde{c}_{\mathfrak{p}}^{-1}(\widetilde{\varepsilon}_{\nu\mathfrak{p}}), \qquad 1 \leqslant \nu \leqslant m$$

which will be satisfied if and only if the numbers $t_{\mathfrak{p}}$ solve the real linear equations

$$\sum_{\mathfrak{p} \in S} t_{\mathfrak{p}} \log |\varepsilon_\nu|_{\mathfrak{p}} = i \log \left(\prod_{\mathfrak{p} \in S} \widetilde{c}_{\mathfrak{p}}(\widetilde{\varepsilon}_{\nu\mathfrak{p}}) \right), \qquad 1 \leqslant \nu \leqslant m \tag{B}$$

for some value of the logarithms on the right hand side. We now select a set of values for those logarithms and a set of numbers $t_{\mathfrak{p}}$ solving the resulting equation (B). It is well-known that the rank of the matrix $(\log|\varepsilon_\nu|_{\mathfrak{p}})$ is m, so there always exist solutions $t_{\mathfrak{p}}$. And since $\sum\limits_{\mathfrak{p}\in S} \log|\varepsilon_\nu|_{\mathfrak{p}} = 0$ for all ν, the most general solution is then $t_{\mathfrak{p}} + t$ for any t. Having selected the $\widetilde{c}_{\mathfrak{p}}$ and $t_{\mathfrak{p}}$, the requirement $c(\alpha) = 1$ for all $\alpha \in k^\times$ means that χ must satisfy the condition

$$\chi(\varphi_S(\alpha)) = \prod_{\mathfrak{p}\in S} \widetilde{c}^{-1}(\widetilde{\alpha}_{\mathfrak{p}})|\alpha|_{\mathfrak{p}}^{-it_{\mathfrak{p}}} \tag{C}$$

for all ideals of the form $\varphi_S(\alpha)$, the ideals obtained from principal ideals by cancelling the powers of primes in S from their factorization. These ideals form a subgroup of finite index h_S in the group of all ideals prime to S. Since the multiplicative function of α on the right hand side of condition (C) has been fixed up to be trivial on the S-units, it amounts to a character of this subgroup of ideals of the form $\varphi_S(\alpha)$. We then must select χ to be one of the finite number h_S of extensions of this character to the group of all ideals prime to S.

Having selected a character

$$c(x) = \prod_{\mathfrak{p}} c(x_{\mathfrak{p}}) = \prod_{\mathfrak{p}\in S} \widetilde{c}_{\mathfrak{p}}(\widetilde{x}_{\mathfrak{p}}) \cdot \prod_{\mathfrak{p}\in S} |x_{\mathfrak{p}}|_{\mathfrak{p}}^{it_{\mathfrak{p}}} \cdot \chi(\varphi_S(x))$$

unramified outside S, we wish to find a simple function $f \in \mathfrak{z}$ whose ζ-function is nontrivial on the surface on which $c(x)$ lies. To this effect we choose for each $\mathfrak{p} \in S$ some function $f_{\mathfrak{p}} \in \mathfrak{z}_{\mathfrak{p}}$ whose (local) ζ-function is nontrivial on the surface on which $c_{\mathfrak{p}}$ lies (for instance select $f_{\mathfrak{p}}$ to be the function used to compute $\rho_{\mathfrak{p}}(c_{\mathfrak{p}}|\cdot|^s)$ previously). For $\mathfrak{p} \notin S$, we choose $f_{\mathfrak{p}} = \mathbf{1}_{\mathfrak{o}_{\mathfrak{p}}}$. We then put

$$f(x) = \prod_{\mathfrak{p}} f_{\mathfrak{p}}(x_{\mathfrak{p}})$$

We will show in the course of our computations that the function f is in the class $\mathfrak{z}$.

Chapter 8

Exercise

8.1 The Power Residue Symbol

Let m be a fixed natural number and K a fixed global field containing the group μ_m of m-th roots of unity. Let S denote the set of primes of K consisting of the archimedean ones and those dividing m. For $a_1, \ldots, a_r \in K^\times$, put

$$S(a_1, \ldots, a_r) = S \cup \{\nu \in M_K \mid |a_i|_\nu \neq 1 \text{ for some } i = 1, \ldots, r\}$$

Definition. For $a \in K^\times$ and $\mathfrak{b} \in I^{S(a)}$, the symbol $\left(\frac{a}{\mathfrak{b}}\right)$ is defined by the equation

$$(\sqrt[m]{a})^{\mathrm{Frob}_{L/K}(\mathfrak{b})} = \left(\frac{a}{\mathfrak{b}}\right) \sqrt[m]{a}$$

where $L = K(\sqrt[m]{a})$.

Lemma 8.1. $\left(\frac{a}{\mathfrak{b}}\right) \in \mu_m$ and is independent of the choice of $\sqrt[m]{a}$.

Proof. Since $\mathrm{Frob}_{L/K}(\mathfrak{b}) \in \mathrm{Gal}(L/K)$, it sends $\sqrt[m]{a}$ to one of its conjugates. Every conjugate of $\sqrt[m]{a}$ takes the form $\zeta \sqrt[m]{a}$ with $\zeta \in \mu_m$; this proves the first assertion. For the second, if we take $\xi \sqrt[m]{a}$ instead, where $\xi \in \mu_m$, since $\mu_m \subseteq K$, ξ is fixed by $\mathrm{Frob}_{L/K}(\mathfrak{b})$; hence

$$\frac{(\xi \sqrt[m]{a})^{\mathrm{Frob}_{L/K}(\mathfrak{b})}}{\xi \sqrt[m]{a}} = \frac{\xi(\sqrt[m]{a})^{\mathrm{Frob}_{L/K}(\mathfrak{b})}}{\xi \sqrt[m]{a}} = \frac{(\sqrt[m]{a})^{\mathrm{Frob}_{L/K}(\mathfrak{b})}}{\sqrt[m]{a}}$$

□

Lemma 8.2.

1. For $a, a' \in K^\times$ and $\mathfrak{b} \in I^{S(a,a')}$, one has $\left(\frac{aa'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a'}{\mathfrak{b}}\right)$.

2. For $a \in K^\times$ and $\mathfrak{b}, \mathfrak{b}' \in I^{S(a)}$, one has $\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a}{\mathfrak{b}'}\right)$.

Proof.

1. Recall that if $L \subseteq M \subseteq N$ are abelian extensions with $\nu \in M_L$ unramified in N, then $F_{N/L}(\nu)|_M = F_{M/L}(\nu)$. Hence to compute $\left(\dfrac{aa'}{\mathfrak{b}}\right)$, we can work in the field $L' = K(\sqrt[m]{a}, \sqrt[m]{a'})$ instead of $K(\sqrt[m]{aa'})$. By the same reason, we have
$$\left(\frac{aa'}{\mathfrak{b}}\right) \sqrt[m]{aa'} = (\sqrt[m]{aa'})^{\mathrm{Frob}_{L'/K}(\mathfrak{b})} = (\sqrt[m]{a'})^{\mathrm{Frob}_{K(\sqrt[m]{a})/K}(\mathfrak{b})}(\sqrt[m]{a'})^{\mathrm{Frob}_{K(\sqrt[m]{a'})/K}(\mathfrak{b})} = \left(\frac{a}{\mathfrak{b}}\right) \sqrt[m]{a} \left(\frac{a'}{\mathfrak{b}}\right) \sqrt[m]{a'}$$

2. This is clear since $F_{L/K}$ is a homomorphism.

□

Corollary 8.2.1. For $a \in K^\times$ and $\mathfrak{b} = \sum n_\nu \nu \in I^{S(a)}$, one has
$$\left(\frac{a}{\mathfrak{b}}\right) = \prod_{\nu \notin S(a)} \left(\frac{a}{\nu}\right)^{n_\nu}$$

Lemma 8.3. If $\nu \notin S$, then the map
$$\begin{aligned} \alpha : \mu_m(K) &\longrightarrow \mu_m(\kappa(\nu)) \\ \zeta &\longmapsto \zeta \mod \mathfrak{p}_\nu \end{aligned}$$
is an isomorphism of groups.

Proof. Suppose $\zeta \in \mu(K)$ is 1 modulo $\mathfrak{p}_\nu$, write $\zeta = 1 + \pi a$ for some $a \in \mathfrak{o}$ ($\mathfrak{o}$ denotes the ring of integers in K). Then
$$1 = \zeta^m = (1 + \pi a)^m = 1 + \sum_{k=1}^{m} \binom{m}{k} a^k \pi^k$$
so that $0 = m\pi a + \frac{m(m-1)}{2}\pi^2 a^2 + \cdots$; this gives $ma \in \mathfrak{p}_\nu$, and since $\mathfrak{p} \nmid m$, it forces $a \in \mathfrak{p}_\nu$. Write $a = \pi a_1$ for some $a_i \in \mathfrak{o}$ and consider $\zeta = 1 + \pi a = 1 + \pi^2 a_1$. Following the same procedure we obtain $a_1 \in \mathfrak{p}_v^2$. Continuing in this way we see $a \in \bigcap_{n \geqslant 1} \mathfrak{p}^n = 0$. Hence $\zeta = 1$, namely α is injective. Since the codomain is of size at most m, it follows that α is a bijection. □

Lemma 8.4. If $\nu \notin S(a)$, then $m \mid (N\nu - 1)$, where $N\nu = \#\kappa(\nu)$, and $\left(\frac{a}{\nu}\right)$ is the unique m-th root of unity such that
$$\left(\frac{a}{\nu}\right) \equiv a^{\frac{N\nu - 1}{m}} \pmod{\mathfrak{p}_\nu}$$

Proof. Note that $m \mid N\nu - 1$ is equivalent to $\mu_m \subseteq \kappa(\nu)$; the latter follows from 8.3, and hence $m \mid N\nu - 1$. For the last assertion, by definition
$$\left(\frac{a}{\nu}\right) = \frac{(a^{1/m})^{\mathrm{Frob}_{L/K}(\nu)}}{a^{1/m}} \equiv \frac{(a^{1/m})^{N\nu}}{a^{1/m}} = a^{\frac{N\nu-1}{m}} \pmod{\mathfrak{p}_\nu}$$
The uniqueness results from 8.3. □

Lemma 8.5. For $\nu \notin S(a)$, TFAE:

(i) $\left(\frac{a}{\nu}\right) = 1$.

(ii) The congruence $x^m \equiv a \pmod{\mathfrak{p}_\nu}$ is solvable with $x \in \mathfrak{o}_\nu$.

(iii) The equation $x^m = a$ is solvable with $x \in K_\nu$.

Proof. In the proof of 8.4 we see $\left(\frac{a}{\nu}\right) = 1$ if and only if $\left(\frac{a}{\nu}\right) \equiv 1 \pmod{\mathfrak{p}_\nu}$. Suppose (ii) holds; then 8.4 implies $\left(\frac{a}{\nu}\right) \equiv a^{\frac{Nv-1}{m}} \equiv x^{Nv-1} \equiv 1 \pmod{\mathfrak{p}_\nu}$, and hence (i). Suppose (i) holds. Since $\kappa(\nu)^\times$ is cyclic of order $N\nu - 1$, let γ be a generator of $\kappa(\nu)^\times$. Write $a = \gamma^n$ for some n. Then

$$1 = a^{\frac{Nv-1}{m}} = \gamma^{\frac{n(Nv-1)}{m}}$$

implies $Nv - 1 \mid \frac{n(Nv-1)}{m}$. Hence $m \mid n$, and thus $a = (\gamma^{n/m})^m$.

That (ii) ⇒ (iii) follows from Hensel's lemma. Now suppose (iii). Taking absolute value, we see $|x|_\nu^m = |a|_\nu \leqslant 1$, so that x lies in the ring of integers of K_ν. Then $x \mod \mathfrak{p}_\nu$ verifies (ii). $\square$

Lemma 8.6. If $\mathfrak{b}$ is an integral ideal prime to m, then

$$\left(\frac{\zeta}{\mathfrak{b}}\right) = \zeta^{\frac{N\mathfrak{b}-1}{m}} \text{ for } \zeta \in \mu_m$$

Proof. When $\mathfrak{b} = \nu$ is a prime, this follows from the uniqueness part of 8.4. For general $\mathfrak{b} = \sum n_\nu \nu$, putting $N\nu = 1 + mr_\nu$ we have

$$N\mathfrak{b} = \prod (1 + mr_\nu)^\nu \equiv 1 + m \sum n_\nu r_\nu \pmod{m^2}$$

Now by linearity

$$\left(\frac{\zeta}{\mathfrak{b}}\right) = \prod \left(\frac{\zeta}{\nu}\right)^{n_\nu} = \prod \zeta^{n_\nu \frac{N\nu-1}{m}} = \zeta^{\sum n_\nu r_\nu} = \zeta^{\frac{N\mathfrak{b}-1}{m}}$$

$\square$

Lemma 8.7. If a and $\mathfrak{b} \in I^{S(a)}$ are integral, and if $a' \equiv a$ (mod)b, then

$$\left(\frac{a'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right)$$

Proof. We may assume $\mathfrak{b} = \nu$ is a prime. Since $a' \equiv a \pmod{\mathfrak{p}_\nu}$, $a^{\frac{N\nu-1}{m}} \equiv a'^{\frac{N\nu-1}{m}} \pmod{\mathfrak{p}_\nu}$, and the result follows from the uniqueness part of 8.4. $\square$

Lemma 8.8. Let $a \in K^\times$. If $\mathfrak{b}, \mathfrak{b}' \in I^{S(a)}$ are such that $\mathfrak{b}'\mathfrak{b}^{-1} = (c)$ is the principal ideal of an element $c \in K^\times$ such that $c \in (K_\nu^\times)^m$ for all $\nu \in S(a)$, then

$$\left(\frac{a}{\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right)$$

8.2 The Norm Residue Symbol

8.3 The Hilbert Class Field

Definition. Let L/K be a finite global field extension and $v \in M_K$ a place. v is said to **split completely** if there are precisely $[L : K]$ extensions of v to K.

(i) v real archimedean: this is equivalent to saying that $L_w = K_v = \mathbb{R}$ for each $M_L \ni w \mid v$.

(ii) v non-real archimedean: v splits completely automatically.

(iii) v non-archimedean: then v is unramified and $\mathrm{Gal}(L_w/K_v) = 1$ for each $M_L \ni w \mid v$.

For convenience, we say an archimedean place is **unramified** if it split completely.

§

Let L/K be a global abelian extension, $v \in M_K$, and $i_v : K_v^\times \to J_K$ the canonical extension.

Lemma 8.9. *v splits completely in L if and only if $i_v(K_v^\times) \subseteq K^\times N_{L/K} J_L$.*

Proof. we have the local Artin map given by

$$\psi_v : K_v^\times \xrightarrow{i_v} J_K \xrightarrow{\psi_{L/K}} \mathrm{Gal}(L/K)$$

From class field theory we know $\ker \psi_\nu = NL^{v\times} = i_v^{-1}(K^\times N_{L/K} J_L \cap i_v(K_v^\times))$ and $\psi_v : K_v^\times / NL^{v\times} \cong \mathrm{Gal}(L^v/K_v)$. Hence

$$\begin{aligned} v \text{ splits completely in } L &\Leftrightarrow v \text{ is unramified and } \mathrm{Gal}(L^v/K_v) = 1 \\ &\Rightarrow K_v^\times = NL^{v\times} \\ &\Leftrightarrow K_v^\times = i_v^{-1}(K^\times N_{L/K} J_L \cap i_v(K_v^\times)) \\ &\Leftrightarrow i_v(K_v^\times) \subseteq K^\times N_{L/K} J_L \end{aligned}$$

Suppose $i_v(K_v^\times) \subseteq K^\times N_{L/K} J_L$. Then Lemma 8.10 says v is unramified, and the second $\Rightarrow$ above can be replaced by $\Leftrightarrow$. □

Lemma 8.10. *v is unramified in L if and only if $i_v(U_v) \subseteq K^\times N_{L/K} J_L$. (Recall that $U_v = K_v^\times$ by definition when v is archimedean.)*

Proof. Let $w \in M_L$ lying above v. If v is unramified, then $N_{L_w/K_v} U_w = U_v$ so $i_v(U_v) \subseteq K^\times N_{L/K} J_L$. Conversely, suppose $i_v(U_v) \subseteq K^\times N_{L/K} J_L$. Then $i_v(U_v) \subseteq K^\times N_{L/K} J_L \cap i_v(K_v) = i_v(NL^{v\times})$ so that $U_v \subseteq NL^{v\times}$.

- For a non-archimedean prime, note that for an element $x \in L^{v\times}$ to satisfy $Nx \in U_v$, x must have absolute value 1, namely $x \in U_w$.

- Suppose v is archimedean. If v is non-real, then $U_v \subseteq NL^{v\times}$ means $\mathbb{C}^\times \subseteq \mathbb{R}_{>0}$, which is absurd. Hence v is real, and it must be the case $L^v = \mathbb{R}$, for otherwise $\mathbb{R}^\times \subseteq \mathbb{R}_{>0}$.

It suffices to deal with the non-archimedean prime; in this case we obtain $U_v = NU_w$. By Corollary 5.8.1 $U_v/(U_v \cap N_{L_w/K_v}L_w^\times) = U_v/NU_w$ is isomorphic to the inertia group of $\mathrm{Gal}(L_w/K_v)$; thus $U_v = NU_w$ implies $e_{w/v} = 1$, i.e. v is unramified. □

Lemma 8.11. Let S denote the set of archimedean primes. The class field to the group $K^\times J_{K,S}$ is the maximal abelian extension of K which is unramified at all primes (including archimedean primes).

Proof. By 8.10, it suffices to show that L/K is a unramified abelian extension, then $K^\times J_{K,S} \subseteq K^\times N_{L/K}J_L$. But this is clear, since the $i_v(U_v)$, $v \in M_K$ are precisely those "v-component" of $J_{K,S}$; precisely, $U_v = j_v(J_{K,S})$ for each v. □

Definition. Keep the notation above. The class field to $K^\times J_{K,S}$ is called the **Hilbert class field** of K; we will denote it by K'.

Lemma 8.12. The Frobenius homomorphism $\mathrm{Frob}_{K'/K}$ induces an isomorphism of the ideal class group $\mathrm{Cl}(K) = I_K/P_K$ of K onto the Galois group $\mathrm{Gal}(K'/K)$.

Proof. By global class field theory we have an isomorphism

$$\psi : J_K/K^\times J_{K,S} \longrightarrow \mathrm{Gal}(K'/K)$$

Notice that there is an surjective homomorphism

$$\begin{aligned} J_K &\longrightarrow I_K \\ (a_v)_v &\longmapsto \sum_{v\nmid\infty} \mathrm{ord}_v(a_v)v \end{aligned}$$

with kernel $J_{K,S}$, and under this map $K^\times$ can be identified with the group of principal fractional ideals; hence $J_K/K^\times J_{K,S} \cong I_K/P_K = \mathrm{Cl}(K)$.

Let us write the isomorphism more explicitly. For each ideal class C, choose a representative I and write I as a sum of finite primes $I = \sum_v a_v v$. Let π_v be a uniformizer of K_v for each v. Form an idele $(\pi_v^{a_v})$ whose infinite components are all 1. Then C is mapped to the element

$$\psi((\pi_v^{a_v})_v) = \mathrm{Frob}_{K'/K}((\pi_v^{a_v})^S) = \prod_v \mathrm{Frob}_{K'/K}(v)^{a_v}$$

Hence our isomorphism takes the form

$$\begin{aligned} \mathrm{Cl}(K) &\longrightarrow \mathrm{Gal}(K'/K) \\ \left[\sum_v a_v v\right] &\longmapsto \prod_v \mathrm{Frob}_{K'/K}(v)^{a_v} \end{aligned}$$

□

Corollary 8.12.1. Let H be a number field and H' be its Hilbert class field.

1. $h_K := \# \operatorname{Cl}(K) = [H' : H]$.
2. A prime ideal in K splits completely in K' if and only if it is a principal prime.
3. An arbitrary ideal I in K is principal if and only if $\operatorname{Frob}_{K'/K}(I) = 1$.

8.3.1 Hilbert class fields of imaginary quadratic fields

8.3.2 Big Hilbert class fields

Let J_S^+ denote the group of ideles which are positive at the real primes of K and are units at the non-archimedean primes. The class field over K with norm group $K^\times J_S^+$ is the maximal abelian extension which is unramified at all non-archimedean primes, but with no condition at the archimedean primes; let us denote it by K_1.

Definition. Let K be a number field. An element $a \in K$ is **totally positive** if for all real embedding $\sigma : K \to \mathbb{R}$ of K, $\sigma(a) > 0$.

Let P_K^+ denote the group of principal ideals of the form (a), where a is a totally positive element of K.

Lemma 8.13. The Frobenius homomorphism $\operatorname{Frob}_{K_1/K}$ gives an isomorphism $I_K/P_K^+ \cong \operatorname{Gal}(K_1/K)$.

Proof. We have the isomorphism

$$\psi : J_K/K^\times J_S^+ \longrightarrow \operatorname{Gal}(K_1/K)$$

Let $K_+^\times$ denote the set of totally positive elements in $K^\times$. We claim the equality $K_+^\times J_{K,S} = K^\times J_S^+$.

- Let $ax \in K^\times J_S^+$ with $a \in K^\times$, $x \in J_S^+$. Then $ax = a^2(a^{-1}x) \in K_+^\times J_{K,S}$.
- Let $ax \in K_+^\times J_{K,S}$ with $a \in K_+^\times$, $x \in J_{K,S}$. Let M be the set of all real embedding. Let $\varepsilon > 0$ be such that for all $\sigma \in M$ and for all $y \in K^\times$, if $|y - x_\sigma|_\sigma < \varepsilon$, then $\sigma(y)\sigma(x_\sigma) > 0$. By weak approximation there is an $y \in K^\times$ such that $|y - x_\sigma|_\sigma < \varepsilon$ for all $\sigma \in M$. Then $ax = ay^{-1}(yx) \in K^\times J_S^+$.

Now under the usual isomorphism $J_K/J_{K,S} \cong I_K$, P_K^+ is identified with the subgroup $K_+^\times J_{K,S}/J_{K,S}$, so that we have

$$J_K/K^\times J_S^+ = J_K/K_+^\times J_{K,S} \xrightarrow{\sim} I_K/P_K^+$$

□

Corollary 8.13.1. $\operatorname{Gal}(K_1/K') \cong P_K/P_K^+$ is an elementary abelian 2-group.

Proof. The isomorphism is clear from 8.12 and 8.13. For the last assertion, it is obviously that P_K/P_K^+ has exponent 2. □

Lemma 8.14. Let r be the number of real primes in K and $K_S^+ = K^\times \cap J_S^+$. Then

$$[P_K : P_K^+][K_S : K_S^+] = 2^{r_1}$$

Proof. We have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & K^\times \cap J_S^+ \arrow[r] \arrow[d] & K_+^\times \arrow[r] \arrow[d] & P_K^+ \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & K^\times \cap J_{K,S} \arrow[r] & K^\times \arrow[r] & P_K \arrow[r] & 0
\end{tikzcd}$$

where the horizontal maps are natural inclusions. Hence we have

$$[P_K : P_K^+][K_S : K_S^+] = [K^\times : K_+^\times]$$

It suffices to show $[K^\times : K_+^\times] = 2^r$. Let M be the set of real embeddings of K. For each $\sigma \in M$, we must find $a \in K^\times$ such that $\sigma(a) > 0$ but $\tau(a) < 0$ for any other $\tau \in M - \{\sigma\}$. But this follows from weak approximation. □

Bibliography

[CF68] JW Cassels and A Frohlich. *Algebraic Number Theory, Proceedings of the Brighton Conference.* 1968.

[Eis95] David Eisenbud. *Commutative algebra, volume 150 of Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995, pp. 185, 200–202.