Notes on Number Theory

Philip Fan

2024/1/2

Contents

Preface

This is a note on number theory. The note covers many aspects on number theory, like class field theory, analytic number theory and so on. The reference books are listed in the bibliography. This note is written in LaTeX, and the source code is available on https://github.com/fanyf22/Notes-on-Number-Theory. This note is still under construction, and I will update it from time to time. If you find any mistakes, please contact me at fanyf22@mails.tsinghua.edu.cn. I will be very grateful for your help.

Philip Fan

2023.11.23

Notations

Basic Notations

$\mathbb{C}$	the field of complex numbers
C_n	the cyclic group of order n
$\mathbb{F}_q$	the finite field with q elements
$\mathbb{N}$	the set of non-negative integers
$\mathbb{P}$	the set of prime numbers
$\mathbb{Q}$	the field of rational numbers
$\mathbb{R}$	the field of real numbers
$\mathbb{Z}$	the ring of integers

Set Operation

$\#A$	the cardinality of A
$A - B$	the set difference of A and B
$A \cup B$	the union of A and B
$A \sqcup B$	the disjoint union of A and B
$A \cap B$	the intersection of A and B
$A \times B$	the Cartesian product of A and B
$\bigcup_{i\in I} A_i$	the union of A_i for $i \in I$
$\bigsqcup_{i\in I} A_i$	the disjoint union of A_i for $i \in I$
$\bigcap_{i\in I} A_i$	the intersection of A_i for $i \in I$
$\prod_{i\in I} A_i$	the Cartesian product of A_i for $i \in I$

Commutative Algebra

R, S	usually a commutative ring
$I, J, \mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$	usually an ideal of a ring
$\mathfrak{m}$	usually a maximal ideal of a ring
$\mathfrak{p}, \mathfrak{q}$	usually a prime ideal of a ring
$I + J$	the ideal generated by I and J
IJ	the product of I and J
$\sum_{i \in I} I_i$	the ideal generated by I_i for $i \in I$
$(a_1, \cdots, a_n)$	the ideal generated by $a_1, \cdots, a_n$
R/I	the quotient ring of R by I
$S^{-1}R$	the ring of fractions of R at S
R_f	the ring of fractions of R at f
$R_{\mathfrak{p}}$	the localization of R at $\mathfrak{p}$
$R[x_1, \cdots, x_n]$	the polynomial ring in $x_1, \cdots, x_n$ over R
$R[[x_1, \cdots, x_n]]$	the power series ring in $x_1, \cdots, x_n$ over R
$R \times S$	the direct product of R and S
$\prod_{i \in I} R_i$	the direct product of R_i for $i \in I$
A, B, C, M, N	usually a module
$M \oplus N$	the direct sum of M and N
$M \otimes_R N, M \otimes N$	the tensor product of M and N over R
$\bigoplus_{i \in I} M_i$	the direct sum of M_i for $i \in I$
$\prod_{i \in I} M_i$	the direct product of M_i for $i \in I$
$\bigotimes_{i \in I} M_i$	the tensor product of M_i for $i \in I$
$\cdots \to A \to B \to C \to \cdots$	an exact sequence

Field Theory

E, F, K, L	usually a field
L/K	a field extension
$[L : K]$	the degree of L/K
$\mathrm{Gal}(L/K)$	the Galois group of L/K
K^{al}	the algebraic closure of K
K^{sep}	the separable closure of K
$K(\alpha_1, \cdots, \alpha_n)$	the field generated by K and $\alpha_1, \cdots, \alpha_n$
$K(t_1, \cdots, t_n)$	the field of rational functions in $t_1, \cdots, t_n$ over K

$K((t_1,\cdots,t_n))$	the field of formal Laurent series in $t_1,\cdots,t_n$ over K

Group Theory

G,H	usually a group
$H \le G$	H is a subgroup of G
$H \trianglelefteq G$	H is a normal subgroup of G
$(G:H)$	the index of H in G
G/H	the quotient group or the left cosets of G by H
$H\backslash G$	the right cosets of G by H
$G\times H$	the direct product of G and H
$\bigoplus_{i\in I} G_i$	the direct sum of G_i for $i\in I$
$\prod_{i\in I} G_i$	the direct product of G_i for $i\in I$
$\langle g_1,\cdots,g_n\rangle$	the subgroup generated by $g_1,\cdots,g_n$
$\langle g_1,\cdots,g_n \vert \cdots\rangle$	the group presented by generators and relations
$G \curvearrowright X$	G acts on X
$\mathrm{Stab}_G(x), \mathrm{Stab}(x)$	the stabilizer of x under G
$\mathrm{Orb}_G(x), \mathrm{Orb}(x)$	the orbit of x under G
X/G	the set of orbits of X under G
$[G]$	the set of conjugacy classes of G
G^{ab}	the abelianization of G

Part I

Class Field Theory

Chapter 1

Group Extension

1.1 *Group Extension and Second Cohomology Group*

Analysis 1.1. Let $0 \to A \xrightarrow{i} U \xrightarrow{j} G \to 0$ be a short exact sequence of groups, with G finite and A abelian. We take any elements $u_\sigma \in U$ for each $\sigma \in G$, such that $j(u_\tau) = \tau$. We define an action of G over A by $a^\sigma = u_\sigma a u_\sigma^{-1}$. We claim that this action is well-defined, and independent on the choice of u_σ.

Firstly, since A is a normal subgroup of U, we see $u_\sigma a u_\sigma^{-1} \in A$. Since A is abelian, and distinct choices of u_σ only differ by A, the choice of u_σ does not affect the value of a^σ. Since $j(u_\sigma u_\tau) = j(u_{\sigma\tau})$, we have

$$a^{\sigma\tau} = u_{\sigma\tau} a u_{\sigma\tau}^{-1} = u_\sigma u_\tau a u_\tau^{-1} u_\sigma^{-1} = (a^\tau)^\sigma$$

$$a^\sigma b^\sigma = u_\sigma a u_\sigma^{-1} \cdot u_\sigma b u_\sigma^{-1} = u_\sigma ab u_\sigma^{-1} = (ab)^\sigma$$

Thus it is indeed a group action. We call it the induced action by $U/A \approx G$.

Definition 1.2. Let A be a G-module. A *group extension* of A is a short exact sequence $0 \to A \to E \to G \to 0$ (or $U/A \approx G$ for short) such that G acts on A by the induced action.

Analysis 1.3. In fact, we can describe U by A and a map $(\sigma, \tau) \mapsto a_{\sigma,\tau}$ explicitly. Given a group extension $U/A \approx G$, we take $a_{\sigma,\tau} = u_\sigma u_\tau u_{\sigma\tau}^{-1}$. First, each element in U can be uniquely written in the form au_σ for some $a \in A$ and $\sigma \in G$. Thus it suffices to tell its multiplication:

$$au_\sigma b u_\tau = ab^\sigma u_\sigma u_\tau = ab^\sigma a_{\sigma,\tau} u_{\sigma\tau}$$

where $ab^\sigma a_{\sigma,\tau} \in A$ and $\sigma\tau \in G$. Thus we see a group extension of A can be constructed by $U = A \times G$ as a set and $(a,\sigma)\cdot(b,\tau) = (ab^\sigma a_{\sigma,\tau}, \sigma\tau)$ for some map $(\sigma,\tau) \mapsto a_{\sigma,\tau}$. Therefore, we wish to decribe what $a_{\sigma,\tau}$ induces a group extension, and what $a_{\sigma,\tau}$ induces the same group extension.

Firstly, we try to give a condition of $a_{\sigma,\tau}$ to induce a group extension. We start from associative law:

$$((a,\sigma)(b,\tau))(c,\gamma) = (a,\sigma)((b,\tau)(c,\gamma))$$

From the multiplication we obtained above, we see

$$((a,\sigma)(b,\tau))(c,\gamma) = (ab^\sigma a_{\sigma,\tau},\sigma\tau)(c,\gamma) = (ab^\sigma c^{\sigma\tau} a_{\sigma,\tau} a_{\sigma\tau,\gamma},\sigma\tau\gamma)$$

$$(a,\sigma)((b,\tau)(c,\gamma)) = (a,\sigma)(bc^\tau a_{\tau,\gamma},\tau\gamma) = (ab^\sigma c^{\sigma\tau} a^\sigma_{\tau,\gamma} a_{\sigma,\tau\gamma},\sigma\tau\gamma)$$

Thus we see $a_{\sigma,\tau}a_{\sigma\tau,\gamma} = a^\sigma_{\tau,\gamma}a_{\sigma,\tau\gamma}$. Conversely, if this condition is satisfied, then we can define a multiplication on U by $au_\sigma bu_\tau = ab^\sigma a_{\sigma,\tau}u_{\sigma\tau}$, and it is associative. The identity is $(a^{-1}_{1,1},1)$, and the inverse is $(b,\tau)^{-1} = (a^{-1}_{1,1}a^{-1}_{\tau^{-1},\tau}b^{-\tau^{-1}},\tau^{-1})$. In conclusion, the condition is $a^\sigma_{\tau,\gamma} = a_{\sigma,\tau}a_{\sigma\tau,\gamma}a^{-1}_{\sigma,\tau\gamma}$, or $\sigma a_{\tau,\gamma} = a_{\sigma,\tau} - a_{\sigma,\tau\gamma} + a_{\sigma\tau,\gamma}$ additively.

Remark 1.4. Readers might take it for granted that $A \hookrightarrow U$ via the map $a \mapsto (a,1)$, but it is in fact not true, since $(a,1) \leftrightarrow au_1$. Thus, a actually corresponds to $(au_1^{-1},1) = (aa^{-1}_{1,1},1)$.

Proposition 1.5. *Let A be a G-module. Then the map $(\sigma,\tau) \mapsto a_{\sigma,\tau}$ induces a group extention if and only if $\sigma a_{\tau,\gamma} = a_{\sigma,\tau} - a_{\sigma,\tau\gamma} + a_{\sigma\tau,\gamma}$ for any $\sigma,\tau,\gamma \in G$.*

Lemma 1.6. *If $a_{\sigma,\tau}$ induces a group extension, then $a_{1,\sigma} = a_{1,1}$ and $\sigma a_{\tau,1} = a_{\sigma\tau,1}$ for any $\sigma,\tau \in G$.*

Proof. Take $\tau = 1$, then $\sigma a_{1,\gamma} = a_{\sigma,1}$, hence $a_{1,\gamma} = a_{1,1}$. Take $\gamma = 1$, then $\sigma a_{\tau,1} = a_{\sigma\tau,1}$. □

Proposition 1.7. *If $a_{\sigma,\tau}$ induces $U/A \approx G$, then there exists $u_\sigma \in G$ such that $j(u_\sigma) = \sigma$ and $a_{\sigma,\tau} = u_\sigma u_\tau u^{-1}_{\sigma\tau}$.*

Proof. Let $u_\sigma = (x_\sigma,\sigma)$ for some $x_\sigma \in A$. Then we see

$$u_\sigma u_\tau u^{-1}_{\sigma\tau} = (x_\sigma + \sigma x_\tau + a_{\sigma,\tau},\sigma\tau)(-\tau^{-1}\sigma^{-1}x_{\sigma\tau} - a_{1,1} - a_{\tau^{-1}\sigma^{-1},\sigma\tau},\tau^{-1}\sigma^{-1})$$

$$= (x_\sigma + \sigma x_\tau + a_{\sigma,\tau} - x_{\sigma\tau} - \sigma\tau a_{\tau^{-1}\sigma^{-1},\sigma\tau} + a_{\sigma\tau,\tau^{-1}\sigma^{-1}} - \sigma\tau a_{1,1},1)$$

Apply Proposition 1.5 with $(\sigma,\tau,\gamma) \to (\sigma\tau,\tau^{-1}\sigma^{-1},\sigma\tau)$, we see

$$\sigma\tau a_{\tau^{-1}\sigma^{-1},\sigma\tau} = a_{\sigma\tau,\tau^{-1}\sigma^{-1}} - a_{\sigma\tau,1} + a_{1,\sigma\tau}$$

Therefore, we have

$$u_\sigma u_\tau u^{-1}_{\sigma\tau} = (x_\sigma + \sigma x_\tau - x_{\sigma\tau} + a_{\sigma,\tau} + a_{\sigma\tau,1} - a_{1,\sigma\tau} - \sigma\tau a_{1,1},1)$$

$$= (x_\sigma + \sigma x_\tau - x_{\sigma\tau} + a_{\sigma\tau,1} + a_{\sigma,\tau} - a_{1,1} - a_{\sigma\tau,1},1)$$

$$= (x_\sigma + \sigma x_\tau - x_{\sigma\tau} + a_{\sigma,\tau} - a_{1,1},1)$$

As we've remarked, the embedding $A \hookrightarrow U$ if given by $a \mapsto (a - a_{1,1},1)$, hence our goal is to find x_σ such that $x_\sigma + \sigma x_\tau - x_{\sigma\tau} = 0$. Take $x_\sigma = 0$ and we finish the proof. □

Definition 1.8. Two group extensions U,U' of G-module A are said to be *isomorphic*, if there exists a group isomorphism $f : U_1 \to U_2$ such that the following diagram is commutative:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & U & \longrightarrow & G & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & A & \longrightarrow & U' & \longrightarrow & G & \longrightarrow & 0
\end{array}$$

Analysis 1.9. Now we study on the problem of what $a_{\sigma,\tau}$ induces isomorphic group extensions. Let $f : U' \to U$ be an isomorphism of group extensions induced by $a'_{\sigma,\tau}$ and $a_{\sigma,\tau}$ respectively. We've already shown that there exists a lifting $u_\sigma \in U$ (and $u'_\sigma \in U'$ respectively) such that $a_{\sigma,\tau} = u_\sigma u_\tau u_{\sigma\tau}^{-1}$ (and $a'_{\sigma,\tau} = u'_\sigma u'_\tau u'^{-1}_{\sigma\tau}$ respectively). Since $j' \circ f = j$, we may write $f(u'_\sigma) = x_\sigma u_\sigma$ with $x_\sigma \in A$. Therefore,

$$a'_{\sigma,\tau} = f(a'_{\sigma,\tau}) = f(u'_\sigma u'_\tau u'^{-1}_{\sigma\tau}) = (x_\sigma,\sigma)(x_\tau,\tau)(x_{\sigma\tau},\sigma\tau)^{-1} = (x_\sigma + \sigma x_\tau - x_{\sigma\tau} + a_{\sigma,\tau} - a_{1,1}, 1) = x_\sigma x_\tau^\sigma x_{\sigma\tau}^{-1} a_{\sigma,\tau}$$

Hence, two $a_{\sigma,\tau}$ induce ismorphic group extensions if and only if they differ by $(\sigma,\tau) \mapsto x_\sigma x_\tau^\sigma x_{\sigma\tau}^{-1}$.

Analysis 1.10. Now we've already given the condition of $a_{\sigma,\tau}$ to induce a group extension, and also given the condition of when two induced group extensions are isomorphic. Let Z be the set of $a_{\sigma,\tau}$ inducing a group extension, i.e., $C = \left\{(\sigma,\tau) \mapsto a_{\sigma,\tau} : \sigma a_{\tau,\gamma} = a_{\sigma,\tau} - a_{\sigma,\tau\gamma} + a_{\sigma\tau,\gamma}\right\}$. If both $a_{\sigma,\tau}$ and $a'_{\sigma,\tau}$ belongs to C, we see $a_{\sigma,\tau} + a'_{\sigma,\tau}$ and $-a_{\sigma,\tau}$ belongs to C. Hence C has an abelian group structure. Moreover, two $a_{\sigma,\tau}$ induce isomorphic group extensions if and only if they differ by $(\sigma,\tau) \mapsto x_\sigma + \sigma x_\tau - x_{\sigma\tau}$. We denote by B the set of such maps. It is easy to verify B is a subgroup of C. Hence we have:

Proposition 1.11. *Isomorphism classes of group extensions corresponds one-to-one to elements of C/B.*

Analysis 1.12. Let $P_n = \mathbb{Z}[G^{n+1}]$, the free abelian group with basis G^{n+1} equipped with the group action $s(g_0,\cdots,g_n) = (sg_0,\cdots,sg_n)$. Define a map $\varepsilon : P_0 \to \mathbb{Z}$ by $g \mapsto 0$ and $d : P_n \to P_{n-1}$ by

$$d(g_0,\cdots,g_n) = \sum_{i=0}^{n} (-1)^i (g_0,\cdots,\hat{g}_i,\cdots,g_n)$$

where $\hat{g}_i$ means excluding the term. We already know that

$$\cdots \to P_n \to \cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

is an exact sequence, hence it is a free resolution of $\mathbb{Z}$. We take the functor $\mathrm{Hom}_G(\cdot,A)$, and obtain a complex $K = \mathrm{Hom}_G(P,A)$. Therefore, $H^n(G,A) = H^n(K)$.

Now given $f \in K^n = \mathrm{Hom}_G(\mathbb{Z}[G^{n+1}],A)$, we define a map $\varphi : G^n \to A$ by

$$\varphi(g_1,\cdots,g_n) = f(1,g_1,g_1g_2,\cdots,g_1\cdots g_n)$$

Since f is a G-homomorphism, it is uniquely determined by φ. By definition,

$$(df)(g_0,\cdots,g_{n+1}) = \sum_{i=0}^{n+1} f(g_0,\cdots,\hat{g}_i,\cdots,g_{n+1})$$

Therefore, under its correspondence with φ, we have

$$(d\varphi)(g_1,\cdots,g_{n+1}) = g_1 \cdot \varphi(g_2,\cdots,g_{n+1}) + \sum_{i=1}^{n} (-1)^i \varphi(g_1,\cdots,g_ig_{i+1},\cdots,g_{n+1}) + (-1)^{n+1}\varphi(g_1,\cdots,g_n)$$

We call φ an *n-cochain* (of G in A). If $\varphi \in \ker d$, i.e., $d\varphi = 0$, we call φ an *n-cocycle*, and if $\varphi \in \operatorname{im} d$, we call φ an *n-coboundary*. Thus the cohomology group is the quotient group of cocycles by coboundaries.

Now we consider the case when $n = 2$. The 2-cochains are maps $\varphi : G \times G \to A$.

$$(d\varphi)(g_1, g_2, g_3) = g_1 \cdot \varphi(g_2, g_3) - \varphi(g_1 g_2, g_3) + \varphi(g_1, g_2 g_3) - \varphi(g_1, g_2)$$

A 2-cocycle if a 2-cochain φ satisfying $d\varphi = 0$, i.e., $g_1 \cdot \varphi(g_2, g_3) = \varphi(g_1 g_2, g_3) - \varphi(g_1, g_2 g_3) + \varphi(g_1, g_2)$. Surprisingly, it coincides with the condition of $a_{\sigma,\tau}$ to induce a group extension. Moreover, let $\psi : G \to A$ be a 1-cochain, and we have

$$(d\psi)(g_1, g_2) = g_1 \cdot \psi(g_2) - \psi(g_1 g_2) + \psi(g_1)$$

A 2-coboundary is a 2-cochain of the form $d\psi$, and it also coincides with the condition of $a_{\sigma,\tau}$ to induce the same group extension. Therefore, $a_{\sigma,\tau}$ is in fact a 2-cochain: the condition of it to induce a group extension is to be a 2-cocycle, and the condition of it to induce the same group extension is to differ by a 2-coboundary. Hence, we have the following theorem:

Theorem 1.13. *Let A be a G-module. Then isomorphism classes of group extensions of A are in a natural one-to-one correspondence with the elements of the second cohomology group $H^2(G, A)$.*

Remark 1.14. Given a 2-cocycle $a_{\sigma,\tau}$, we can construct a group extension $U = A \times G$ with

$$(a, \sigma) \cdot (b, \tau) = (a + b^\sigma + a_{\sigma,\tau}, \sigma\tau)$$

However, this extension is not simple enough since the way A is embedded into U is by $a \mapsto (a - a_{1,1}, 1)$. Hence we wish $a_{1,1} = 0$, which leads us to prove the following proposition:

Proposition 1.15. *Let $\alpha \in H^2(G, A)$. Then there exists a 2-cocycle $a_{\sigma,\tau}$ of class α such that $a_{1,\sigma} = a_{\sigma,1} = 0$.*

Proof. Let $b_{\sigma,\tau}$ be a 2-cocycle of α. We define $c_{\sigma,\tau} = \sigma b_{1,1}$. It is easy to verify that $c_{\sigma,\tau}$ is actually a 2-coboundary. Hence $a_{\sigma,\tau} = b_{\sigma,\tau} - c_{\sigma,\tau}$ is also of class α. $b_{1,\sigma} = b_{1,1}$ and $b_{\sigma,1} = \sigma b_{1,1}$, so proof. $\square$

1.2 *Homomorphism of Group Extensions and Tranfer*

Definition 1.16. Let $U/A \approx G$ and $U'/A' \approx G'$ be two group extensions, with two given group homomorphisms $f : A \to A'$ and $\varphi : G \to G'$, then a *group extension homomorphism* is a group homomorphism $F : U \to U'$ such that the following diagram is commutative:

$$\begin{array}{ccccc} A & \longrightarrow & U & \longrightarrow & G \\ {\scriptstyle f}\big\downarrow & & {\scriptstyle F}\big\downarrow & & {\scriptstyle \varphi}\big\downarrow \\ A' & \longrightarrow & U' & \longrightarrow & G' \end{array}$$

Analysis 1.17. We wish to find a condition of f and φ being able to extend to F. First we take a 2-cocycle of U satisfying the condition of Proposition 1.15, say $a_{\sigma,\tau}$ and $a'_{\sigma,\tau} \in U'$ similarly. Firstly,

$$f(a^\sigma) = f(u_\sigma a u_\sigma^{-1}) = F(u_\sigma) f(a) F(u_\sigma)^{-1} = f(a)^{F(u_\sigma)} = f(a)^{\varphi(\sigma)}$$

Hence the f is a G-homomorphism with A' regarded as a G-module via φ. Secondly, we see $F(0, \sigma) = (x_\sigma, \varphi(\sigma))$

Chapter 2

Global Class Field Theory

2.1 *Artin Map and Reciprocity Law*

NOTATION. *We denote by K a global field and $\mathfrak{M}_K$ its set of places. S is often a finite set of places of K containing all the archimedean places. We denote by I^S the free abelian group generated by $\mathfrak{M}_K - S$.*

L is often a finite Galois extension of K, and in such cases, S is often required to contain the ramified primes.

ANALYSIS 2.1. Let L/K be a finite Galois extension of global fields. For any unramified prime $\mathfrak{p}$ in K, let $\mathfrak{P}$ be a prime in L above $\mathfrak{p}$. Since $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified, we see $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is cyclic of order $f(\mathfrak{P}/\mathfrak{p})$, and we let $\sigma_{\mathfrak{P}}$ be the Frobenius map in $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. We know that the local Galois group can be embedded naturally into the global one, hence $\sigma_{\mathfrak{P}}$ can be regarded as an element of $\mathrm{Gal}(L/K)$.

Now let $\sigma \in \mathrm{Gal}(L/K)$, then $\mathfrak{P}^{\sigma}$ is also a prime in L above $\mathfrak{p}$. We have a natural isomorphism between $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ and $\mathrm{Gal}(L_{\mathfrak{P}^{\sigma}}/K_{\mathfrak{p}})$ as subgroups of $\mathrm{Gal}(L/K)$ by mapping τ to $\sigma\tau\sigma^{-1}$. Thus $\sigma_{\mathfrak{P}^{\sigma}} = \sigma\sigma_{\mathfrak{P}}\sigma^{-1}$. Therefore, we see fixed a prime $\mathfrak{p}$ in K, $\sigma_{\mathfrak{P}}$ falls into the same conjugacy class in $\mathrm{Gal}(L/K)$ for all primes $\mathfrak{P}$ above $\mathfrak{p}$. Thus we can define the map $F_{L/K} : \mathfrak{M}_K - S \to [\mathrm{Gal}(L/K)]$ by mapping $\mathfrak{p}$ to the conjugacy class of $\sigma_{\mathfrak{P}}$. Since a conjugacy class is mapped to a single element in the abelianization, we induces $\mathrm{Art}_{L/K} : \mathfrak{M}_K - S \to \mathrm{Gal}(L/K)^{ab}$. By definition of I^S, we may extend to the *Artin map* $\mathrm{Art}_{L/K} : I^S \to \mathrm{Gal}(L/K)^{ab}$.

PROPOSITION 2.2. *Let L'/K' be a Galois extension such that $K \subseteq K'$ and $L \subseteq L'$. Let S' be a finite set of places of K' containing all the archimedean places, the primes ramified in L' and all primes above S. Then we have*

$$\begin{array}{ccc} I^{S'} & \xrightarrow{\mathrm{Art}_{K'}} & \mathrm{Gal}(L'/K')^{ab} \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle \theta} \\ I^S & \xrightarrow{\mathrm{Art}_{L/K}} & \mathrm{Gal}(L/K)^{ab} \end{array}$$

where θ is induced by the restriction map $\mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$.

Proof. Let $v' \in \mathfrak{M}_{K'} - S'$, and $v \in \mathfrak{M}_K$ below v'. Let w' be a place in L' above v', and w be the place in L below w'. Thus $\mathrm{Art}_{L/K}(v)$ (and $\mathrm{Art}_{L'/K'}(v')$ respectively) is the Frobenius map σ_w of L_w/K_v (and $\sigma_{w'}$ of

$L_{w'}/K_{v'}$ respectively). We see the Frobenius map is a power map of the cardinality of the residue field of the ground field, hence we have $\sigma_{w'} = \sigma_w^{[\kappa(v'):\kappa(v)]} = \sigma_w^{f(v'/v)}$. We see $N_{K'/K}v' = f(v'/v)\cdot v$, so proof. $\square$

Notation. *For $a \in K^\times$, we denote by $(a)^S$ the element in I^S: $(a)^S = \sum_{v\notin S} v(a)\cdot v$*

Theorem 2.3 (Reciprocity Law in the Crude Form). *Let L/K be a finite abelian extension of global fields, and S be a set of places in K consisting of the archimedean ones and those ramified in L. Then there exists $\varepsilon > 0$ such that if $a \in K^\times$ and $|a-1|_v < \varepsilon$ for all $v \in S$, then $\mathrm{Art}_{L/K}((a)^S) = 1$.*

Definition 2.4. Let K be a global field and $S \subseteq \mathfrak{M}_K$ consisting of all archimedean places, and let G be a abelian topological group. Then a homomorphism $\phi : I^S \to G$ is said to be *admissible* if for each open neighbourhood N of the identity element 1 of G, there exists $\varepsilon > 0$ such that $\phi((a)^S) \in N$ whenever $a \in K^\times$ and $|a-1|_v < \varepsilon$ for all $v \in S$.

Remark 2.5. When G is discrete, we simply take $N = 1$, thus we have:

Theorem 2.6 (Reciprocity Law). *Let L/K be an abelian extension of global fields, then $\mathrm{Art}_{L/K}$ is admissible.*

2.2 *Chevalley's Interpretation by Idèles*

Notation. *We first review the notations of idèles. Let K be a global field, and S be any finite subset of $\mathfrak{M}_K$ consisting of achimedean places, we denote by $J_{K,S} = \prod_{v\in S} K_v^\times \times \prod_{v\notin S} U_v$, equipped with the product topology. For $S \subseteq S'$, we have a natural continuous homomorphism $J_{K,S} \to J_{K,S'}$, and it induces a direct system $(J_{K,S})_S$. We define the group of idèles to be $J_K = \varinjlim_S J_{K,S}$, and denote by J_K^S the idèles that have coordinate 1 at S.*

Notation. *Let $x = (x_v)$ be an idèle, we denote by $(x)^S = \sum_{v\notin S} v(a_v)\cdot v$.*

Proposition 2.7. *Let G be a complete abelian topological group and $\phi : I^S \to G$ admissible. Then there exists a unique continuous homomorphism $\psi : J_K \to G$ such that*

1. *$\psi(K^\times) = 1$;*
2. *$\psi(x) = \phi((x)^S)$ for $x \in J_K^S$.*

Conversely, if ψ is a continuous homomorphism $J_K \to G$ such that $\psi(K^\times) = 1$, then ψ comes from some admissible pair (ϕ, S) as defined above, provided there exists an open neighbourhood of 1 in G in which 0 is the only subgroup.

Remark 2.8. It is clear that if such a ψ exists for a given ϕ and S, then it induces a continuous homomorphism of the idèle class group $C_K \approx J_K/K^\times$ to G. We also denote by ϕ ths induced homomorphism.

Remark 2.9. If ϕ and S induce such a homomorphism ψ, then ϕ and S' also induce a homomorphism ψ' for any $S' \supseteq S$. By the uniqueness, we have $\psi = \psi'$. In particular, if two ϕ's on I^S coincide with $I^{S'}$ for some finite $S' \supseteq S$, they are actually equal on I^S.

Corollary 2.10. *The reciprocity law holds for a finite abelian extension L/K of global fields, if and only if there exists a continuous homomorphism $\psi : J_K \to \mathrm{Gal}(L/K)^{ab}$ such that $\psi(K^\times) = 1$ and $\psi(x) = \mathrm{Art}_{L/K}((x)^S)$ for $x \in J_K^S$, where S consists of the archimedean places and the primes ramified in L.*

Notation. *Let L/K be a finite extension of global fields, then for each $w \in \mathfrak{M}_L$ and $v \in \mathfrak{M}_K$ below w, L_w/K_v is a finite extension of local fields. Let $a_w \in L_w$, then we have the local norm $N_{L_w/K_v} a_w$. For any $(a_w) \in J_L$, we define its norm to be given by $(N_{L/K}(a_w))_v = \prod_{w/v} N_{L_w/K_v} a_w \in J_K$.*

Proposition 2.11. *If the reciprocity law holds for L/K and L'/K', then the following diagram is commutative:*

$$\begin{tikzcd} J_{K'} \arrow[r, "\psi_{L'/K'}"] \arrow[d, "N_{L/K}"'] & \mathrm{Gal}(L'/K')^{ab} \arrow[d, "\theta"] \\ J_K \arrow[r, "\psi_{L/K}"] & \mathrm{Gal}(L/K)^{ab} \end{tikzcd}$$

Corollary 2.12. *If the reciprocity law holds for L/K, then $\psi_{L/K}(N_{L/K} J_L) = 1$.*

2.3 *Statements of Main Theorems*

Chapter 3

Hilbert Class Field

Part II

Analytic Number Theory

Chapter 4

Dirichlet Characters

4.1 *Group Characters of Integers*

Notation. *In this section, G is a finite abelian group.*

Definition 4.1. A *character* of G is a homomorphism $\chi : G \to \mathbb{C}^\times$. Such characters form a group under multiplication defined by $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. We call this group the *character group* of G, or the *dual* of G and denote it by G^*. We usually denote the identity element of G^* by χ_0, called the *principal character*.

Proposition 4.2. *$G \simeq G^*$ non-canonically.*

Proposition 4.3. *$G \simeq G^{**}$ canonically by mapping g to $\chi \mapsto \chi(g)$.*

Proposition 4.4. *$(\cdot)^*$ is an exact functor.*

Proof. Because $(\cdot)^* = \mathrm{Hom}(\cdot, \mathbb{Q}/\mathbb{Z})$ and $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module. ☐

Notation. *From now on, we identify G^{**} with G.*

Definition 4.5. Let H be a subgroup of G. The *orthogonal complement* of H is defined by

$$H^\perp := \{\chi \in G^* : \chi(h) = 1 \text{ for any } h \in H\}$$

Proposition 4.6. *Let H be a subgroup of G, then $H^{\perp\perp} = H$.*

Proof. Since $(\cdot)^*$ is an exact functor, $(G/H)^*$ is indeed a subgroup of G, and by the definition of $H^\perp$ we see $H^\perp = (G/H)^*$. Thus we have $H^{\perp\perp} = (G^*/(G/H)^*)^*$. By the exactness of dual functor again we see $G^*/(G/H)^* = H^*$, hence $H^{\perp\perp} = H^{**} = H$. So proof. ☐

Proposition 4.7. *For any $\chi, \chi' \in G^*$, we have*

$$\frac{1}{\#G}\sum_{g\in G}\chi(g)\bar{\chi}'(g) = \begin{cases} 1 & \chi = \chi' \\ 0 & \chi \neq \chi' \end{cases}$$

Proof. Since the image of χ' has absolute value 1, $\bar{\chi}' = \chi'^{-1}$, hence it suffices to show that

$$\frac{1}{\#G}\sum_{g\in G}\chi(g) = \begin{cases} 1 & \chi = 1 \\ 0 & \chi \neq 1 \end{cases}$$

The case $\chi = 1$ is trivial. When $\chi \neq 1$, we have $\chi(g_0) \neq 1$ for some $g_0 \in G$. Since

$$\chi(g_0)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(g_0 g) = \sum_{g\in G}\chi(g)$$

we prove the result. □

4.2 *Dirichlet Characters*

Definition 4.8. We call the group characters of $(\mathbb{Z}/n\mathbb{Z})^\times$ the *Dirichlet characters* modulo n.

Remark 4.9. Consider the natural homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ for $m \mid n$, it induces the natual homomorphism $(\widehat{\mathbb{Z}/m\mathbb{Z}})^\times \to (\widehat{\mathbb{Z}/n\mathbb{Z}})^\times$, i.e., a Dirichlet character modulo m can be regarded as a Dirichlet character modulo n. We say such two Dirichlet characters are equivalent. For each Dirichlet character χ, there exists a unique n such that it is equivalent to a Dirichlet character modulo n but not modulo m for any $m \mid n$. Such n is called the *conductor* of the Dirichlet character, denoted by f_χ. We see if χ is a Dirichlet character modulo n, then $f_\chi \mid n$. If $n = f_\chi$, we say χ is *primitive*. Thus, each Dirichlet character is equivalent to a primitive Dirichlet character, called the *primitive form*.

Remark 4.10. We may easily deduce that $\chi(-1)^2 = 1$, hence $\chi(-1) = \pm 1$. We call $\chi(-1)$ the *sign* of χ. If $\chi(-1) = 1$, we say χ is *even*, otherwise *odd*.

Now we give another form of Dirichlet character:

Definition 4.11. A *lifted Dirichlet character* modulo n is a map $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying the following conditions:

1. χ is periodic with period n, i.e., $\chi(x+n) = \chi(x)$ for any $x \in \mathbb{Z}$;
2. $\chi(x) = 0$ for all x such that $\gcd(x,n) \neq 1$;
3. χ is a group homomorphism from $(\mathbb{Z}/n\mathbb{Z})^\times$ to $\mathbb{C}^\times$.

Remark 4.12. We see that for any Dirichlet character χ modulo n, we may define $\tilde{\chi} : \mathbb{Z} \to \mathbb{C}$ by:

1. $\tilde{\chi}(x) = \chi(x)$ for $x \in \mathbb{Z}$ such that $\gcd(x,n) = 1$;
2. $\tilde{\chi}(x) = 0$ for $x \in \mathbb{Z}$ such that $\gcd(x,n) \neq 1$.

We see $\tilde{\chi}$ is a lifted Dirichlet character modulo n. We say $\tilde{\chi}$ is the *lifting* of χ.

Notation. *From now on, when we write $\chi(n)$, we always mean $\tilde{\chi}(n)$.*

Definition 4.13. We say the lifting of a primitive Dirichlet character is *primitive*.

Proposition 4.14. *Let χ be a Dirichlet character modulo n, then we have*

$$\sum_{k=1}^{n} \chi(k) = \begin{cases} \varphi(n) & \chi = \chi_0 \\ 0 & \chi \neq \chi_0 \end{cases}$$

Proposition 4.15. *Let x be an integer, then we have*

$$\sum_{\chi \bmod n} \chi(x) = \begin{cases} \varphi(n) & x \equiv 1 \pmod{n} \\ 0 & x \not\equiv 1 \pmod{n} \end{cases}$$

where χ runs over all Dirichlet characters modulo n.

Corollary 4.16. *Let r be an integer prime to n, then we have for all $x \in \mathbb{Z}$ that*

$$\sum_{\chi \bmod n} \chi(x)\bar{\chi}(r) = \begin{cases} \varphi(n) & x \equiv r \pmod{n} \\ 0 & x \not\equiv r \pmod{n} \end{cases}$$

where χ runs over all Dirichlet characters modulo n.

Remark 4.17. We see from the corollary that Dirichlet characters can tell whether an integer belongs to a residue class modulo n by an equation. That helps us study the properties of primes in arithmetic progressions.

4.3 *Dirichlet Characters of Ideals*

Notation. *In this section, K is a number field. $\mathfrak{M}_K$ is the set of prime ideals in K, and S is a finite subset of $\mathfrak{M}_K$. I^S is the free abelian group generated by primes in $\mathfrak{M}_K - S$.*

Definition 4.18. An element $\alpha \in K^\times$ is totally positive if $\sigma(\alpha) \in \mathbb{R}_{>0}$