Notes on Number Theory

Philip Fan

2023/12/28

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
$\mathcal{G}al(L/K)$	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
$H \leq G$	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 $g_1,\cdots,g_n$
$\langle g_1,\cdots,g_n\|\cdots\rangle$	the group presented by generators and relations
$G \curvearrowright X$	G acts on X
$\mathcal{S}tab_G(x), \mathcal{S}tab(x)$	the stabilizer of x under G
$\mathcal{O}rb_G(x), \mathcal{O}rb(x)$	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 *Second Cohomology*

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

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

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

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 $a u_\sigma$ for some $a \in A$ and $\sigma \in G$. Thus it suffices to tell its multiplication:*

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

where $a b^\sigma a_{\sigma,\tau} \in A$ 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 $(a, \sigma) \cdot (b, \tau) = (a b^\sigma a_{\sigma,\tau}, \sigma\tau)$ 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 the associative law:

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

From the multiplication we obtained above, we see

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

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

Thus we see $a_{\sigma,\tau}a_{\sigma\tau,\gamma} = a_{\tau,\gamma}^{\sigma}a_{\sigma,\tau\gamma}$. *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 inverse is* $(b,\tau)^{-1} = (u_1^{-1}a_{\tau,\tau^{-1}}^{-1}b^{-\tau^{-1}},\tau^{-1})$. *In conclusion, the condition is* $a_{\tau,\gamma}^{\sigma} = a_{\sigma,\tau}a_{\sigma\tau,\gamma}a_{\sigma,\tau\gamma}^{-1}$, *or* $\sigma a_{\tau,\gamma} = a_{\sigma,\tau} - a_{\sigma,\tau\gamma} + a_{\sigma\tau,\gamma}$ *additively.*

PROPOSITION 1.4. *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* $\sigma,\tau,\gamma\in G$.

PROPOSITION 1.5. *If* $a_{\sigma,\tau}$ *induces* $U/A\approx G$, *then there exists a lifting* $u_{\sigma}\in U$ *such that* $a_{\sigma,\tau} = u_{\sigma}u_{\tau}u_{\sigma\tau}^{-1}$.

Proof. We have seen that $U = A\times G$ with $(a,\sigma)\cdot(b,\tau) = (ab^{\sigma}a_{\sigma,\tau},\sigma\tau)$. Take $u_{\sigma} = (a_{1,1},\sigma)$ □

DEFINITION 1.6. 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 1.7. *Now we study on the problem of what* $a_{\sigma,\tau}$ *induces isomorphic group extensions. Let* $a_{\sigma,\tau}$ *and* $a'_{\sigma,\tau}$ *be two maps that induce group extensions* U *and* U', *such that there exists isomorpism* $f : U\to U'$ *of group extensions. Clearly,* f *fixes* A, *and* $j'\circ f(u_{\sigma}) = \sigma$. *Thus we may write* $x_{\sigma} =$

Chapter 2

Global Class Field Theory

2.1 *Artin's 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 $Gal(L_\mathfrak{P}/K_\mathfrak{p})$ is cyclic of order $f(\mathfrak{P}/\mathfrak{p})$, and we let $\sigma_\mathfrak{P}$ be the Frobenius map in $Gal(L_\mathfrak{P}/K_\mathfrak{p})$. 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 $Gal(L/K)$.*

Now let $\sigma \in Gal(L/K)$, then $\mathfrak{P}^\sigma$ is also a prime in L above $\mathfrak{p}$. We have a natural isomorphism between $Gal(L_\mathfrak{P}/K_\mathfrak{p})$ and $Gal(L_{\mathfrak{P}^\sigma}/K_\mathfrak{p})$ as subgroups of $Gal(L/K)$ 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 $Gal(L/K)$ for all primes $\mathfrak{P}$ above $\mathfrak{p}$. Thus we can define the Artin map $Art_K : \mathfrak{M}_K - S \to [Gal(L/K)]$ by mapping $\mathfrak{p}$ to the conjugacy class of $\sigma_\mathfrak{P}$. Since a conjugacy class is mapped to a single element in the abeianization, we induces $Art_K : \mathfrak{M}_K - S \to Gal(L/K)^{ab}$. Since I^S has $\mathfrak{M}_K - S$ as its basis, we may extend Art_K to $Art_K : I^S \to Gal(L/K)^{ab}$.

NOTATION. *Let K'/K be a subextension of L/K, and $S' \subseteq \mathfrak{M}_{K'}$ be a finite set that only contains the primes above S. Then denote the norm map by $N_{K'/K} : I^{S'} \to I^S$, defined by*

$$N_{K'/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})} \text{ where } \mathfrak{P} \text{ lies above } \mathfrak{p}$$

PROPOSITION 2.2. *The following diagram is commutative:*

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

where θ is induced by the inclusion map $\mathcal{G}al(L/K) \to \mathcal{G}al(L/K')$.