AN EFFECTIVE VERSION OF THE GRUNWALD–WANG THEOREM

Thesis by

Song Wang

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2002

(Submitted September 13, 2001)

Acknowledgements

I would like to express to my advisor Dinakar Ramakrishnan my great appreciation for his suggestion of this topic, and for the continued help during my graduate study and the preparation of this thesis. Thanks are also made to E. Goins and D. Prasad who read the manuscript carefully and made helpful comments. Finally, I would like to thank Caltech for providing me a friendly environment in which to live in and learn.

Abstract

The main purpose of my thesis is to establish an effective version of the Grunwald–Wang Theorem, which asserts that given a family of local characters χ_v of K_v^* of exponent m where $v \in S$ for a finite set S of primes of K, there exists a global character χ of exponent m (unless some special case occurs, when it is $2m$) whose component at v is χ_v. The effectivity problem for this theorem is to bound the norm $N(\chi)$ of the conductor of χ in terms of K, m, S and $N(\chi_v)$. This problem was encountered in 1995 in the work of Hoffstein and Ramakrishnan ([H-Ra95]), where they needed it in a particular case when $K \supset \mu_m$ **AND** m is a prime. In this thesis, we solve this problem completely, and show in the general case that $N(\chi)$ is bounded by $A\prod_{v\in S} N(\chi_v)^B$ with $A = (A_0 N_S)^{C_1|S|}$. In the special cases when $K \supset \mu_m$ **OR** m is a prime, we can give a better bound for $N(\chi)$ with $A = A_0 N_S^{C_2}$, where A_0, B, C_1 and C_2 are independent of S. The later bound improves the result of [H-Ra95]. We get an even more precise bound, namely $N(\chi) \leqq 4\prod_{p\in S} NpN(\chi_p)$, when $K = \mathbb{Q}$ and $m = 2$.

In this thesis, we develop three different approaches, dealing with the quadratic extension case, the Kummer or the general l–extension case, and the general case respectively. In addition to class field theory, we use a reduction process to the unramified case and certain modified effective versions of the Chebotarev Density Theorem. Also, in the general case, we transport to this problem some techniques from Algebra involving essential subgroups and

essential closures.

To check the maximal range of our method, we also consider the problem with GRH, and get $A = (A_0 \log N_S)^{C_0|S|}$ in the general case where A_0 and C_0 are independent of S. When $K = \mathbb{Q}$ and $m = 2$, we do even better with $A << (2^{|S|} \log N_S)^2$. To get these results, we use yet another modification of the effective version of the Chebotarev Density Theorem (with GRH).

These effective results have some interesting applications in concrete situations. To give a simple example, if we fix p and l, one gets a good least upper bound for N such that p is not an l–th power mod N. One also gets the least upper bound for N such that $l^r \mid \phi(N)$ and p is not an l–th power mod N. The table 3.1 describes the best least upper bound we get this way for quadratic Dirichlet characters on $C_{\mathbb{Q}}$ having desired local behavior at some p and/or infinity.

Contents

List of Tables

Introduction

In 1933, W. Grunwald ([Gr33]) stated a striking theorem asserting that, given a number field K, a finite set S of places, and a family of characters χ_v, $v \in S$, of $K_v^\times$ of orders m_v, there exists a global character χ of finite order of K whose local components at $v \in S$ are χ_v. Furthermore, the order of χ is the least common multiple m of the m_v, unless a special case occurs when it is $2m$ (cf. Theorem 0.2– 0.4).

However, Grunwald's original statement and proof had a flaw, which occured when he discussed the special case. The gap was filled by Sh. Wang ([Wa48], [Wa50]), who also gave a precise criterion for the special case and showed that the order of χ can be taken to be m under an additional condition (see Chapter 10, [A-T68]). So this theorem is appropriately called the *Grunwald-Wang theorem*. For a detailed discussion of this theorem, see [Lo-Ro2000].

Given the local datum $\{ \chi_v \mid v \in S \}$, there are infinitely many global characters χ with local components χ_v. They can be highly ramified in general. Indeed, some additional ramification has to be allowed as seen for example when all the χ_v are unramified and K has class number 1. However, the natural question which arises is whether we can control the ramification of χ in terms of K, S, m and the norms $N(\chi_v)$ of the conductors of χ_v for v in S. To be precise, one would like a bound on the norm $N(\chi)$ of the conductor of χ,

of the form $A\prod_{v\in S}(N(\chi_v))^B$ for some constants A, B only depending on K, S and m.

This effectivity problem was encountered in 1995 in the work of J. Hoffstein and D. Ramakrishnan on Siegel zeros ([H-Ra95]), where they needed it in a particular case when $K \supset \mu_m$ **and** m a prime, bounding $N(\chi)$ by $\prod_{v\in S}(A + N(\chi_v))^B$.

In this thesis, we solve this problem completely. In the general case, we bound $N(\chi)$ by $A\prod_{v\in S}(N(\chi_v))^B$, with $A = (A_0 \cdot N_S)^{C_1|S|}$, where B, A_0 and C_1 depend only on K and m and N_S is the product of the norm of S.

If K contains μ_m (Kummer case) **or** if m is a prime l (l–extension case), we get a bound of the form $A\prod_{v\in S}(N(\chi_v))^B$ with $A = A_0 N_S^{C_2}$ where B, A_0 and C_2 depend only on K and m. So our bound is stronger and more precise than the bound in [H-Ra95]. And if $K = \mathbb{Q}$ and $m = 2$, we can, by using a different method, even show that $N(\chi) \leq C N_S \prod_{v\in S} N(\chi_v)$ for some constant C. For a precise statement of the theorems, see the next section.

To understand the problem, let us look at the the simplest case, which occurs when $K = \mathbb{Q}$, $m = 2$, with $S = \{p\}$ or $\{p, \infty\}$, and χ_p unramified. A quadratic Dirichlet character χ_D, $(D, p) = 1$, is nontrivial at p if and only if p is inert in $\mathbb{Q}(\sqrt{D})$, i.e., $\left(\frac{D}{p}\right) = -1$ if $p \neq 2$ and $\left(\frac{2}{D}\right) = -1$ if $p = 2$. It is nontrivial at ∞ if and only if $D < 0$. Thus this problem is exactly the one of finding a bound for the least nonquadratic residue mod p.

In this thesis we develop three different approaches dealing separately with

the following cases: (i) Quadratic extensions over $\mathbb{Q}$ (Chapter 3), (iia) Kummer extensions with m arbitrary, (iib) Non-Kummer extensions with m a prime (Chapter 4), and (iii) the general case (Chapter 5).

Let us begin with some things which will be used in some or all the approaches.

By class field theory ([Lang70]), there is a natural surjective map from the set of characters χ of order m to the set of cyclic extensions of degree m, with the fibers being of the form $\{\chi^j \mid 1 \leq j \leq m-1, (j,m) = 1\}$. Thus the problem reduces to the construction of minimally ramified cyclic extensions with given local behavior.

In cases (i), (iia) and (iib) we make a reduction to the"unramified" case, which means that in the given datum, all local characters are unramified. The main idea of this reduction process is to find a minimally ramified global character μ with the given local ramification behavior so that by twisting with this character, one eliminates the ramification at the given places. But the choice of μ is critical and we pick it carefully. In cases (i) and (iib) when $K = \mathbb{Q}$, we choose at any prime p, a Dirichlet character $\mu^{(p)}$ which is unramified outside p such that $(\mu^{(p)})^{-1}|_{\mathbb{Q}_p^\times} \cdot \chi_p$ is unramified and set $\mu = \prod_{p \in S} \mu^{(p)}$ (See Lemma 3.5 and Proposition 1.7). In case (iia), since the characters of order m are given by $K^\times / K^{\times m}$, the problem reduces to finding $u \in \mathcal{O}_K$ of minimal norm with $v(u) = v(u_v)$ for any $v \in S$, where $u_v \in \mathcal{O}_{K_v}$ corresponds to χ_v. For more details, see below. Finally, we get a bound which is a product of an expression coming from the unramified case and a power of the product of the

norms of the conductors of the given local characters.

In cases (i) and (iii), we use suitable effective versions of the Chebotarev Density Theorem. We need only the standard ones ([L-M-O79], [KM94]) in case (i) while we need a modification (see Theorem 2–C, Chapter 2) in case (iii). This modified version of the Chebotarev Density Theorem for a Galois extension L/K gives a least bound for a prime of K **outside** the given S which is unramified in L and does not split or corresponds to a certain conjugacy class under the Artin symbol. The main idea to prove this modified version is the same as the classical version in [L-O77], [L-M-O79], [KM94]. The only difference is to estimate a certain sum over the primes in S. For details, see Chapter 2.

Let us briefly discuss the cases (i), (iia) and (iib), and then describe in greater detail the difficult general case (iii).

The approach in case (i) (Chapter 3), dealing with quadratic extensions of $\mathbb{Q}$, is the following. After the reduction to the unramified case, we further reduce the problem to the construction of a minimally ramified quadratic extension $\mathbb{Q}(\sqrt{D})$ over $\mathbb{Q}$ with given local behavior. Note that for any D not divisible by p, the restriction of χ_D to $\mathbb{Q}_p^\times$ is nontrivial iff $\left(\frac{D}{p}\right) = -1$ (resp. $\left(\frac{2}{D}\right) = -1$) when $p \neq 2$ (resp. $p = 2$). Thus by the quadratic reciprocity law of Gauss, each local condition corresponds a condition on $\left(\frac{p}{D}\right)$ or the sign of D. Hence, the problem is then reduced to a question (Question Z in Chapter 3, see Section 1.5) related to the Chebotarev Density Theorem for $L/\mathbb{Q}$ where L is the extension of $\mathbb{Q}(\sqrt{-1})$ obtained by attaching $\sqrt{p}$ for all p in S. We

answer this question unconditionally with only elementary methods.

The second approach deals with cases (iia) and (iib). In case (iia), by the Kummer theory (see [Ne91], [Lang70], and also Chapter 1 below), we have a bijection between characters of exponent m and the elements of the field modulo m-th powers, and such bijection is compatible with localization. Thus one reduces the problem to finding a $b \in \mathcal{O}_K$ with $b \equiv b_v \pmod{(K_v^\times)^m}$ (See Corollary 4.2). Reducing to the unramified case, where each b_v is a unit in $\mathcal{O}_{K_v}$, the equations becomes $b \equiv b_v \mod \mathfrak{p}_v$. So we can we apply an effective version of the Chinese Remainder Theorem (Theorem 4.1) which is stated and proved in this chapter. This method does not work in the general case.

In case (iib), we lift the local characters to $K_v(\zeta_l)^\times$ and proceed as in case (iia), and then pull back the global character. More explicitly, let $\tilde{\chi}_\omega = \chi_v \circ N_{K_{1\omega}/K_v}$ for $\omega \in \tilde{S}$, where $\tilde{S}$ is the set of places of $K_1 = K(\zeta_l)$ above S. First we find a global character $\tilde{\chi}$ of K_1 with the given localization by using (iia). We need to pull back $\tilde{\chi}$ on C_{K_1} to χ on C_K through $N_{K_1/K}$. To do this we use $(\prod_\sigma \tilde{\chi} \circ \sigma)^{1/[K_1:K]}$ instead of $\tilde{\chi}$ while σ runs over $Gal(K_1/K)$. This is possible since $[K_1 : K]$ divides $l - 1$ which is prime to l.

The third approach (Chapter 5) treats the general case. Without loss of generality, we may just consider the case when $m = l^r$ is a prime power. The idea for this case is complicated. In fact, we consider a stronger problem which comes from another formulation of the Grunwald–Wang Theorem. Given $P = \prod_{\varphi \in S} K_\varphi^\times \hookrightarrow \mathbb{I}_K$ and subgroup $P_0 \leq P$ with $P^m \subseteq P_0$, there exists a standard open subgroup V of $\mathbb{I}_K$ such that $V\mathbb{I}_K^n K^\times$ separates P/P_0. i.e.,

$P \cap V\mathbb{I}_K^n K^\times \subseteq P_0$ where $n = m$, or $2m$ if the special case occurs. The problem is to find a least bound of the norm of such V. To achieve this, we transport to this problem some techniques from Algebra involving essential subgroups and essential closures.

To make our explanation understandable, let us discuss here only the generic case. One crucial step is that if S' is a set of primes of K containing S such that $\#C\ell(K, S')$ is not divisible by l, then $V\mathbb{I}_K^n K^\times = V\mathbb{I}_K^n K^{S'} = V\mathbb{I}_K^n W$ for some subgroup W in $K^{S'}$ of finite rank which is computable (See Prop 5.8). If a set Σ of $\mathfrak{p} \notin S$ is chosen such that for any representative $a \in W/W^{l^r} - 1$, there is some $\mathfrak{p}$ in Σ which does not have a lift splitting in $K(\zeta_{l^r}, \sqrt[l]{a})/K(\zeta_{l^r})$, i.e., $K_\upsilon(\zeta_{l^r}, \sqrt[l]{a}) \neq K_\upsilon(\zeta_{l^r})$, or is inert in $K(\zeta_{l^r})$, then by Prop 5.6, the standard open subgroup $V_\mathfrak{c}$, corresponding to the cycle $\mathfrak{c}$ which is the formal product of the primes in Σ, separates $\mathbb{I}_K^{l^r} \cdot W/\mathbb{I}_K^{l^r}$. Thus take $V = V_\mathfrak{c} \cap V_\mathfrak{f}$ where $\mathfrak{f}$ is the conductor of P_0 in P (for definition, see Section 5.4). V is what we need.

When a special case occurs, however, some changes in the statements and the proof are needed, but the main idea is the same. For a definition of the special case, see Chapter 0.

Now let us describe the contents of all the chapters. In the ensuing section, we will list out all the main results we get in this thesis. Chapter 0 consists of the background material for the Grunwald-Wang Theorem, and some notations which will be used in this thesis. Chapter 1 involves the preliminaries to the later chapters. Chapters 3, 4, 5 deal with and solve this problem in various cases via the three different approaches. Then Chapter 2 focuses on

the statement and the proof of a modified version of the Chebotarev Density Theorem.

Finally, it may be of some interest to know how much better we can do in terms of finding the best possible constants A and B. To this end, we show (see Chapter 6) that if assumes GRH, one can get $A = (A_0 \log N_S)^{C_0|S|}$ in the general case, where A_0 and C_0 depend only on K and m. For case (i), one can do even better with $A << (2^{|S|} \log N_S)^2$. To get these results, we use two S–versions of the Chebotarev Density Theorem (with GRH), proved in Chapter 6, which is a small improvement of Theorem 2.6 in [Se81] by J.-P. Serre.

Main Results

Here we state the main results of this thesis. First, we list out all the unconditional results. In fact, we solve the problem in general, and also find stronger bounds for various particular cases.

We begin with an effective version in the **quadratic case** $K = \mathbb{Q}$ and $m = 2$.

Theorem A. *Let S be a finite set of primes of $\mathbb{Q}$, χ_p be either a quadratic charatcer or a trivial character of $\mathbb{Q}_p^\times$ for each $p \in S$. Then there exists a global quadratic character χ with $\chi|_{\mathbb{Q}_p^\times} = \chi_p$ such that*

$$N(\chi) \leqq C N_S \prod_{p \in S} N(\chi_p)$$

$C = 2$ if $\infty \in S$, $C = 4$ if $\infty \notin S$, where $N_S = \prod_{p \in S} Np$.

This is Proposition 3.6.

Theorem B. *Let p be a rational prime and χ_p be a quadratic character on $\mathbb{Q}_p^\times$. Then there exists a global quadratic character χ on $C_\mathbb{Q}$ such that*

(i) $\chi|_{\mathbb{Q}_p^\times} = \chi_p$;

(ii)

$$N(\chi) \leqq \begin{cases} N(\chi_p)(p+3) & \text{if } p \equiv 1 \pmod 4; \\ 8N(\chi_p) & \text{if } p \equiv 3 \pmod 4; \\ 10N(\chi_p) & \text{if } p = 2. \end{cases}$$

If we also require that χ is even/odd, then condition (ii) is replaced by

(ii′)

$$N(\chi) \leqq \begin{cases} CN(\chi_p)(p+3) & \text{if } p \equiv 1 \pmod 4; \\ 2CN(\chi_p)(p+1) & \text{if } p \equiv 3 \pmod 4; \\ 7CN(\chi_p) & \text{if } p = 2 \end{cases}$$

where $C = 1$ if χ is even, and $C = 2$ if χ is odd.

This is Proposition 3.7.

For a more precise result when $S = \{p\}$ or $\{p, \infty\}$, see Tables 3.1 and 3.2.

Now we turn to the **general Kummer case** $\mu_m \subset K$.

Theorem C. *Let $m \geqq 1$, K a number field which contains the group μ_m of m-th roots of unity, S a finite set of finite primes of K, and χ_v a local character of exponent m on $K_v^\times$ for each $v \in S$. Then there exists a global character χ on C_K of exponent m with $\chi|_{K_v^\times} = \chi_v$ such that*

$$N(\chi) \leqq ((m^2/2) \prod_{p|m} p^3)^{n_K} \cdot B(\Omega) \cdot {N_S}^{n_K} \cdot \prod_{v \in S} N(\chi_v)^{(m-1)n_K} \cdot 2^{c_1}$$

where $\Omega = \{\omega_1, \omega_2, \ldots, \omega_{n_K}\}$ *is an integral basis for* K, $n_K := [K : \mathbb{Q}]$,

$$B(\Omega) := \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_K} |\sigma(\omega_i)|,$$

$N_S = \prod_{v \in S} N\mathfrak{p}_v$, *and* $c_1 = r_1(K)$ *(resp. 1) if* $m = 2$ *(resp.* $m > 2$*).*

This is Theorem 4–A.

For any finite set T of places of a number field K, we will write $C\ell_{K,T}$ for the T–class group of K (see the end of Section 0.1 for a precise definition).

Here is another version in the Kummer case.

Theorem D. *Let* S *be a finite set of finite primes of* K *which contains* μ_m, *where* m *is a positive integer greater than* 1, χ_v *a local character of exponent* m *on* $K_v^\times$ *for each* $v \in S$. *Assume that* S^* *is a finite set of finite primes disjoint from* S, $S_m = \{v \mid m\}$ *and* S_∞ *with* $C\ell_{K, S^* \cup S_\infty \cup (S_m - S)} = 1$. *Then there exists a global character* χ *on* C_K *of exponent* m *with* $\chi|_{K_v^\times} = \chi_v$ *such that*

$$N(\chi) \leqq ((m^2/2) \prod_{p \mid m} p^3)^{n_K} \cdot B(\Omega) \cdot {N_S}^{n_K} \cdot \prod_{v \in S^*} N\mathfrak{p}_v \cdot \prod_{v \in S, v \nmid m} N(\chi_v) \cdot 2^{c_1}$$

where $B(\Omega)$, c_1, N_S *and* n_K *are as defined in the previous theorem.*

This is Theorem 4–B.

Next we get a precise result for the l–**extension case**, i.e., with $m = l$, an odd prime, and K arbitrary.

Theorem E. *Let* S *be a finite set of finite primes of* K, *and* $m = l$ *is an odd rational prime,* χ_v *a local character of exponent* m *on* $K_v^\times$ *for each* $v \in S$. *Then there exists a global character* χ *on* C_K *of exponent* m *with* $\chi|_{K_v^\times} = \chi_v$

such that

$$N(\chi) \leqq (\frac{l^{3n_K+2n_Kd}}{2^{n_Kd}}) \cdot B(\Omega^*) \cdot {N_S}^{n_Kd^2} \cdot \prod_{v \in S} N(\chi_v)^{(l-1)n_Kd^2}$$

where $K_1 = K(\zeta_l)$, $n_K = [K : \mathbb{Q}]$, $d = [K_1 : K]$, $\Omega^* = \{\omega_1, \omega_2, \ldots, \omega_{n_Kd}\}$ *is an integral basis for* K_1, *and*

$$B(\Omega^*) := \prod_{\sigma : K \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_Kd} |\sigma(\omega_i)|.$$

This is Theorem 4–C.

Here is a more precise result for $K = \mathbb{Q}$ and $m = l$ an odd prime. Note that this is not merely a corollary of Theorem E..

Theorem F. *Let* S *be a finite set of finite primes of* $\mathbb{Q}$, *and* χ_p *a local character on* $\mathbb{Q}_p^\times$ *of exponent* l *for each* $p \in S$ *while* l *is an odd rational prime. Then there exists a global character* χ *on* $C_\mathbb{Q}$ *of exponent* l *with* $\chi|_{\mathbb{Q}_p^\times} = \chi_p$ *such that*

$$N(\chi) \leqq 2^{-(l-1)} l^{2l+1} (l-1)^{l-1} \cdot N_S^{l-1} \cdot \prod_{p \in S, p \neq l} N(\chi_p).$$

This is Theorem 4–D.

Here is the **general case**. Without loss of generality, we may assume that m is a prime power l^r.

Theorem G. *Let* K *be a number field,* $m = l^r$ *a prime power,* S *a finite set of primes of* K, χ_v *a local character on* $K_v^\times$ *of exponent* m *for each* $v \in S$. *Assume* $K(\zeta_{l^r})/K$ *is cyclic, or the special case occurs with some specified condition holds. There is a global character* χ *on* C_K *of exponent* m *with*

$\chi|_{K_v^\times} = \chi_v$ *such that*

$$N(\chi) \leqq (d_K l^{(r+1)\, n_K} N_{S'})^{C(r_W+1)l[K(\zeta_{l^r}):K]} \cdot \prod_{v \in S} N(\chi_v)$$

for some absolute, positive, effectively computable constant C *where* S' *is a finite set of* finite *primes containing all the finite primes in* S *and satisfying* $l \nmid \# C\ell_{K,S' \cup S_\infty}$, *and*

$$r_W = \gamma_l(C\ell_{K,S \cup S_\infty}) + \#(S \cup S_\infty) - 1.$$

Here $\gamma_l(G)$ denotes the minimal cardinality of the generating set of the Sylow-l subgroup of G. For a more explicit version, see Chapter 5.

Corollary H. *Let* $m = l^r$ *a prime power,* S *a finite set of primes of* $\mathbb{Q}$, χ_p *a local character on* $\mathbb{Q}_p^\times$ *of exponent* m *for each* $p \in S$. *There is a global character* χ *on* $C_\mathbb{Q}$ *of exponent* m *with* $\chi|_{\mathbb{Q}_p^\times} = \chi_p$ *such that*

$$N(\chi) \leqq (l^{r+1} N_{S_f})^{C(|S_f|+1)l^{r+1}} \cdot \prod_{p \in S} N(\chi_p)$$

for some absolute, positive, effectively computable constant C *where* S_f *consists of all the finite primes in* S.

Finally we turn to a result with GRH for the general case.

Theorem I. *Preserve all the hypothesis of Theorem G with the same* r_W *and* S', *and assume* GRH. *Then There is a global character* χ *on* C_K *of exponent*

m with $\chi|_{K_v^\times} = \chi_v$ *such that*

$$N(\chi) \leq C'^{2r_W+3}(E_1 + (r+1)E_2 + E_3)^{2r_W+2}\left((E_1 + rE_2)^2 + E_3\right)\prod_v N(\chi_v)$$

for some absolute positive constant C'*, where*

$$E_1 = [K_1 : K]\log d_K$$

$$E_2 = [K_1 : K]\, n_K \log l$$

$$E_3 = [K_1 : K]\log N_{S'}$$

The following theorem provides a bound for $m = 2$ and $K = \mathbb{Q}$ assuming GRH, which is stronger than what is implied by the previous theorem.

Theorem J. *Let* S *be a finite set of primes of* $\mathbb{Q}$*,* χ_p *a charatcer of exponent* 2 *of* $\mathbb{Q}_p^\times$ *for each* $p \in S$*. Assuming* GRH*, there exists a global quadratic character* χ *with* $\chi|_{\mathbb{Q}_p^\times} = \chi_p$ *such that*

$$N(\chi) << \left(2^{|S|}\log_2 N_S\right)^2 \prod_{p\in S} N(\chi_p).$$

Besides these results, we also get three modified versions of the effective version of the Cheborarev Density Theorem (Theorem 6–A, 6–B and 2–C). The first one is a small improvement of Theorem 2.6 in [Se81].

Chapter 0 Notations and Statement of the Problem

0.1 Notations and Background

Let K be a number field, v a place of K, and $\mathfrak{p}$ the prime corresponding to v. In the non–Archimedean case, $\mathfrak{p}$ has the natural meaning — a prime ideal of K.

Let K_v or $K_\mathfrak{p}$ denote the completion of K at v (or $\mathfrak{p}$), and let $\mathcal{O}_K$ denote the ring of integers of K, where K is a local or global field (e.g. a number field). If $K = \mathbb{R}$ or $\mathbb{C}$, then $\mathcal{O}_K = K$.

Let $\mathcal{U}_K$ or $\mathcal{O}_K^\times$ denote the group of invertible elements in $\mathcal{O}_K$.

If K is an ultramedian local field, denote π a uniformizer, and $\mathfrak{p} = (\pi)$ the prime ideal of K. Also denote

$$V_{\mathfrak{p}^n} = \mathcal{U}_K^{(n)} = \{x : v_\mathfrak{p}(x-1) \geq n\} = 1 + \mathfrak{p}^n$$

where $v_\mathfrak{p}$ is the valuation corresponding to $\mathfrak{p}$. If $K = \mathbb{R}$, denote $\mathfrak{p}$ the corresponding infinite prime of K. Denote

$$V_1 = V_{\mathfrak{p}^0} = \mathbb{R}^\times$$

$$V_{\mathfrak{p}^1} = \mathbb{R}_+^\times = \left\{a \in \mathbb{R}^\times \mid a \gneqq 0\right\}.$$

If $K = \mathbb{C}$, then $V_1 = \mathbb{C}^\times$.

In the above case, we use the notation $V_{\mathfrak{p}^n}$ where $\mathfrak{p}^n$ is a formal prime power which is called a *cycle*. Such $V_{\mathfrak{p}^n}$ is called *the standard open subgroup (of the multiplicative group $\mathcal{O}_K^\times$ of level n)*. Also we denote the unit group as the following: (Compare with the group of the invertibles.)

$$U_K = \begin{cases} \mathcal{U}_K & \text{if } K \text{ is non–Archimedean} \\ \{\pm 1\} & \text{if } K = \mathbb{R} \\ S^1 \text{ if } K = \mathbb{C} \end{cases}$$

If K is a global field (for example, a number field or a function field over a finite field), denote $\mathbb{A}_K$ as the ring of adeles of K, i.e., the restricted product of K_v rel. to $\mathcal{O}_v$; $\mathbb{I}_K$ the ring of ideles of K, i.e., the restricted product of $K_v^\times$ rel. to $\mathcal{U}_v$ where $\mathcal{U}_v = \mathcal{U}_{K_v}$. i.e.,

$$\begin{aligned} \mathbb{A}_K &:= \{(x_v) \mid x_v \in K_v, x_v \in \mathcal{O}_v \qquad \text{for almost all primes } v.\} \\ &= \prod{}' K_v \end{aligned}$$

and also we have

$$\begin{aligned} \mathbb{I}_K &:= \left\{(x_v) \mid x_v \in K_v^\times, x_v \in \mathcal{O}_v^\times \qquad \text{for almost all primes } v.\right\} \\ &= \prod{}' K_v^\times \end{aligned}$$

K embeds into $\mathbb{A}_K$, and $K^\times$ embeds into $\mathbb{I}_K$ in a natural way: $K \hookrightarrow \mathbb{A}_K : a \to (\dots, a, \dots, a, \dots)$, and $K^\times \hookrightarrow \mathbb{I}_K : a \to (\dots, a, \dots, a, \dots)$.

Let $C_K = \mathbb{I}_K / K^\times =$ the group of idele classes of K.

Let $\mathfrak{c} = \prod \mathfrak{p}^{n_\mathfrak{p}}$ denote a cycle, i.e., a formal product of primes. If $\mathfrak{p}$ is real, $n_\mathfrak{p} = 0$ or 1; if $\mathfrak{p}$ is complex, $n_\mathfrak{p} = 0$; if $\mathfrak{p}$ is a finite prime, $n_\mathfrak{p} = 0, 1, \ldots$. Note that $n_\mathfrak{p}$ is 0 for almost all $\mathfrak{p}$.

An idele $\mathbf{a} = (a_v) \in \mathbb{I}_K$ is said to be 1 *modulo* $\mathfrak{c}$, if the following hold:

(1) $a_v \equiv 1 (\mod \mathfrak{p}^{n_\mathfrak{p}})$ if $\mathfrak{p}$ is non–Archimedean. This condition is equivalent to $v_\mathfrak{p}(a_v - 1) \geq n_\mathfrak{p}$.

(2) $a_v \gneqq 0$, if $\mathfrak{p}$ is real and $n_\mathfrak{p} = 1$.

(3) $a_v \in \mathcal{O}_{K_v}^\times = \mathcal{O}_v^\times$ if $n_\mathfrak{p} = 0$, for any case.

Denote the above $\mathbf{a} \equiv 1 \pmod{\mathfrak{c}}$.

Put $\mathbb{I}_K^\mathfrak{c} = \{ \mathbf{a} \in \mathbb{I}_K \mid \mathbf{a} \equiv 1 \pmod{\mathfrak{c}} \}$. Note that $\mathbb{I}_K^1 = \{ \mathbf{a} \in \mathbb{I}_K \mid a_v \in \mathcal{O}_{K_v}^\times \}$.

Denote $V_\mathfrak{c} = \mathbb{I}_K^\mathfrak{c}$ the *standard open subgroup of* $\mathbb{I}_K$ *of the cycle* $\mathfrak{c}$. Also denote

$$C_K^\mathfrak{c} = \frac{\mathbb{I}_K^\mathfrak{c} \cdot K^\times}{K^\times}$$

the *Ray* idele class group of K of the cycle $\mathfrak{c}$.

For a global field K, denote U_K the unit group of K as before.

$$U_K := \{ a \in K^\times, a \in \mathcal{O}_{K_v}^\times \text{ for all non–Archimedean } v \}$$

$$\mu(K) := \text{the group of roots of unity in K}$$

$$= \{ \omega \in K^\times \mid \omega^N = 1 \text{ for some } N \}$$

$$\mu_n(K) = \{ \omega \in K^\times \mid \omega^n = 1 \}$$

A *local character* χ *on/of* $K^\times$ (sometime we say of K) where K is a local

field is a homomorphism: $\chi : K^\times \to S^1$.

A character χ is said to be *of exponent* n if χ factors through $K^\times/(K^\times)^n \to \mu_n(K) \hookrightarrow S^1 \hookrightarrow \mathbb{C}^\times$. If n is the smallest positive integer such that χ factors through $K^\times/K^{\times n}$, we also say that χ is of order n. (Denote here $Ord\,\chi = n$.)

A *global character* χ on/of C_K (We also call such χ a *Grossencharacter* on C_K or on K.) is a continuous homomorphism:

$$\chi : C_K = \mathbb{I}_K/K^\times \to S^1$$

with $Ker\,\chi$ contains $C_K^{\mathfrak{c}} = V_{\mathfrak{c}} \circ K^\times/K^\times$ for some cycle $\mathfrak{c}$. (Note that $C_K^{\mathfrak{c}}$ form a basis of open neighborhood of 1 in C_K.) Also, χ is said to be *of exponent* n if χ factors through $C_K/C_K^n \to \mu_n(\mathbb{C}) \hookrightarrow S^1 \hookrightarrow \mathbb{C}^\times$.

χ is said to be of *order* n if such n is the minimal exponent of χ.

Also, the natural embedding $K_v^\times \to \mathbb{I}_K$ induces a natural embedding $K_v^\times \to C_K$.

Compose χ with such embedding, we get $\chi|_{K_v^\times}$, the *local component* χ *at* v. Also we denote it $\chi|_v$.

The *conductor* $\mathfrak{f}_\chi$ of χ is defined as the following:

If χ is a local character χ_v on $K_{\mathfrak{p}}^\times = K_v^\times$ where $\mathfrak{p}$ is the corresponding prime. (It is a real ideal if v is non–Archimedean.)

$\mathfrak{f}_\chi = \mathfrak{p}^f$ where f is the minimal nonnegative integer satisfying $\mathcal{U}_{K_v}^{(f)} \subseteq Ker\,\chi$.

In fact, if v is non–Archimedean, it means that χ_v factors through $K^\times/(1+\mathfrak{p}^f)$, and $\chi_v|_{1+\mathfrak{p}^{f-1}}$ is nontrivial.

If v is complex, $\mathfrak{f}_\chi = 1$.

If v is real, then $\mathfrak{f}_\chi = 1$ or $\mathfrak{p}$, and it depends on the sign of $\chi(-1)$. $\mathfrak{f}_\chi = 1$ iff $\chi(-1) = 1$; $\mathfrak{f}_\chi = \mathfrak{p}$ iff $\chi(-1) = -1$.

Next, if χ is a global character, then $\mathfrak{f}_\chi = \mathfrak{c}$ where $\mathfrak{c}$ is the smallest cycle such that $\chi|_{C_K^{\mathfrak{c}}} \equiv 1$. i.e., Let $\tilde{\chi}$ be the composition the natural map $\mathbb{I}_K \to C_K$ and χ, Then $\mathfrak{c}$ is the cycle such that $\tilde{\chi}|_{V_\mathfrak{c}} = 1$ and if $\tilde{\chi}|_{V_{\mathfrak{c}'}} = 1$ for some $\mathfrak{c}'|\mathfrak{c}$ then $\mathfrak{c}' = \mathfrak{c}$.

If $\mathfrak{f}_\chi = \mathfrak{c} = \mathfrak{c}_{inf}\mathfrak{c}_f$ where $\mathfrak{c}_{inf}$ is the infinite part of $\mathfrak{c}$ and $\mathfrak{c}_f$ is the finite part of $\mathfrak{c}$, then we also call $\mathfrak{c}_f$ the *finite conductor* of χ, which appears in the functional equation of $L(s, \chi)$.

Theorem 0.1. *If χ is a global character, then the conductor of χ is the product of the conductor of its local components. i.e.,*

$$\mathfrak{f}_\chi = \prod_v \mathfrak{f}_{\chi_v}$$

where $\chi_v = \chi|_v$.

Proof. See [Lang70] or [Ne86]. □

A local character χ on $K^\times$ is said to be *unramified* if $\mathfrak{f}_\chi = 1$. A global character χ is said to be *unramified* at v if $\chi|_v$ is unramified (otherwise we say it *ramified*), i.e., $\mathfrak{f}_\chi$ does not involve $\mathfrak{p}$ – the corresponding prime to $fVfV$.

Let $\mathfrak{p}$ be a prime of K (local or global). $N\mathfrak{p}$ is defined as (1) $N\mathfrak{p} = [\mathcal{O}_K : \mathfrak{p}]$ if $\mathfrak{p}$ is a finite prime of K; (2) $N\mathfrak{p} = 2$, if $\mathfrak{p}$ is real.

Remark: If K is a global field, v is non–Archimedean, $\mathfrak{p}$ the corresponding prime ideal, then $[\mathcal{O}_{K_v} : \mathfrak{p}\mathcal{O}_{K_v}] = [\mathcal{O}_K : \mathfrak{p}]$; thus (1) is compatible with localization.

If $\mathfrak{c} = \prod \mathfrak{p}^{n_\mathfrak{p}}$, then define the norm $N\mathfrak{c} = \prod (N\mathfrak{p})^{n_\mathfrak{p}}$.

The *norm* of the conductor of χ (local or global) is denoted $N(\chi) := N(\mathfrak{f}_\chi)$. By the definition and Theorem 0.1,

$$N(\chi) = N(\mathfrak{f}_\chi) = \prod_v N(\chi_v) = \prod_v N(\mathfrak{f}_{\chi_v})$$

To end, let us explain the concept of a *T–class group* here.

For any finite set T of places of a number field K, we will write $C\ell_{K,T}$ for the T–class group of K. It is well known that T–class group has two interpretations (see [Lang70] , [Ne91]).

First, if T is a finite set of primes of K, the T–ideal class group $C\ell_{K,T}$ is defined as $J_K/J_K^T P_K$ where J_K is the ideal group of K, J_K^T the subgroup of J_K generated by all primes in T, and P_K the subgroup of J_K generated by all principal ideals of $\mathcal{O}_K$. It is clear that $C\ell_{K,\emptyset}$ is exactly the class group of K, and as T gets larger, $C\ell_{K,T}$ shrinks.

Furthermore, if T contains all infinite primes of K, then $C\ell_{K,T}$ is defined as $\mathbb{I}_K/\mathbb{I}_K^T K^\times$, where $\mathbb{I}_K^T$ denotes the group of ideles Z with local component $Z_\varphi \in \mathcal{U}_{K_\varphi}$ for $\varphi \notin T$. Also, it is clear that $C\ell_{K,S_\infty}$ is isomorphic to the class group of K, and that $C\ell_{K,T}$ shrinks as T gets larger, where S_∞ is the set consisting of all the infinite primes of K.

The two definitions are compatible with each other since for any finite set of finite primes S, the first $C\ell_{K,S}$ is isomorphic to $C\ell_{K,S\cup S_\infty}$ defined in the second way. So we can define $C\ell_{K,T}$, for arbitrary set T of primes of K, finite or infinite, using either definition.

0.2 The Grunwald–Wang Theorem and the Effective Version

Here we state the main theorem — Grunwald's Theorem. This theorem was first stated and proved (not completely) by Grunwald. However, the proof appeared in [A-T68] was first due to Sh. Wang (see Chapter 10 of [A-T68], and [Wa50]).

Theorem 0.2. *Let S be a finite set of primes and $\{\chi_v, v \in S\}$ a set of local characters of K. (χ_v on $K_v^\times$ for each $v \in S$) of exponent m.*

Then there exists a global character χ on C_K such that

(a) $\chi|_v = \chi_v$.

(b) *χ is of exponent m, unless the special case occurs (which we will define below), when such χ be found of exponent $2m$.*

Theorem 0.3 (Characterization of the special case). *Let S be a finite set of primes of K, $P(m,S) := \{x \in K^\times, x$ is an m-th power in $K_v^\times$ for all $v \notin S\}$.*

Then $P(m,S) = K^{\times m}$ except if the following conditions hold. (If they hold, we say that the special case of Wang *occurs.)*

(a) *K is a number field.*

(b) *$-1, \pm(2+\eta_{2^s})$ are nonsquares in $K^\times$ where s is the integer such that $\eta_{2^s} \in K^\times$, $\eta_{2^{s+1}} \notin K^\times$.*

(c) *$m = 2^t m'$, $2 \nmid m'$, $t \gneqq s$,*

(d) *$S_0 \subseteq S$, where $S_0 :=$ the set of primes $\varphi|2$ such that $-1, \pm(2+\eta_{2^s})$ are nonsquares in K_φ.*

In the special case, $P(m,S) = K^{\times m} \cup a_0 K^{\times m}$, *where* $a_0 = (1+\zeta_{2^s})^m = \eta_{2^{s+1}}^m = (i\eta_{2^{s+1}})^m = [\pm(2+\eta_{2^s})]^{m/2}$.

Notation: $\zeta_n :=$ a primitive n-th of root of unity. $\eta_n := 2\,Re\,\zeta_n = \zeta_n + \frac{1}{\zeta_n}$

Theorem 0.2 and Theorem 0.3 are proved in [A-T68]. Also in Chapter 1, the sketch of proof will be contained.

Remark. The simplest of the special case occurs when $m = 8$, $K = \mathbb{Q}$, $S_0 = \{2\}$, $16 \in P(m,S)$, but $16 \notin \mathbb{Q}_2^8$, $a_0 = (2+\eta^4)^4 = 16$.

Theorem 0.4. *Keep the notations as in Theorem 0.2 and Theorem 0.3.*

If the special case occurs, then such χ *can be found of exponent* $n = lcm(|\chi_v|)$ *if*

$$\prod_{v \in S_0} \chi_v(a_0) = 1$$

Otherwise, we can only reach the exponent $2n$.

Remark. The simplest of the special case for $S_0 = \phi$ occurs when $m = 8$, $K = \mathbb{Q}(\sqrt{-7})$, $a_0 = 16$, and $K(\zeta_8) = K(\sqrt{2}, i)/K$ collapses at 2 since $\sqrt{7} = i\sqrt{-7}$ and -7 is a square in $\mathbb{Q}_2$.

In [H-Ra95], Lemma 2.10 asserts that for $K \supseteq \mu_l$, where l – a rational prime, given S a finite set of finite primes, $\chi_v, v \in S$ global characters are given of exponent l. By Theorem 0.2 and Theorem 0.3, note that $\eta_2 = \eta_4 = 0$, the special case can't occur. So we can find a global character χ satisfying

Theorem 0.2, $\chi \mid l$. And furthermore, we can find such χ with

$$N(\chi) \leq \prod_{v \in S} (A + N(\chi_v))^B$$

where A, B depend on l, K and S.

In fact, we will see in next chapters that such bound can be strengthened to the form

$$N(\chi) \leq A(\prod_{v \in S} N(\chi_v))^B$$

A depends on K, S and l, and B depends on K and l.

This is the simplest case of what we call an effective version of the Grunwald–Wang theorem.

Of course, there is a natural way to generalize this theorem. One may ask how the bound will depend on the various parameters, when the condition that m is a prime or that $\zeta_m \in K$ is dropped.

Problem I K is a number field, S, m given and $\{ \chi_v, v \in S \}$ given as in Theorem 0.2. All notations are the same as in Theorem 0.2 and Theorem 0.3. Find a (effective) bound for $N(\chi)$ in terms of K, S, m and $N(\chi_v)$ for a solution χ in Theorem 0.2.

Or, restating it.

Problem I′ K is a number field, S a finite set of primes, m a positive integer, and χ_v a local character on $K_v^\times$ for each $v \in S$. Assume that χ_v are of exponent m, find a global character χ which is a solution of the Grunwald–

Wang Theorem, such that $N(\chi)$ can be bounded by an effective expression in terms of K, S, $N(\chi_v)$.

Remark: Of course, **Problem I** also has an obvious analog when K is a function field over a finite field.

By the local and global class field theory, there is a surjective map from the set of local characters on $K_v^\times$ (global characters on C_K) of finite order, to the set of cyclic extensions of K_v (K) of finite order. Also there's a one–to–one corresponding between the set of open subgroups of $K_v^\times$ (C_K).

Another version of the Grunwald–Wang theorem and the precise form is as follows.

Theorem 0.5. *S is a finite set of primes of K, and for each K_v for $v \in S$, a local cyclic extension L_v/K_v is given. $[L_v : K_v]|m$. Then there exists a cyclic global field extension L/K such that*

(a) *L_ω/K_v, the localization of L/K at a prime ω/v, is the same as L_v/K_v* (Up to a K_v-isomorphism).

(b) *$[L : K]$ divides m, unless the special case occurs; if the special case occurs, we can find such L with the following "a_0" constraint:*

$$S_1 \subseteq S_0 \subseteq S,$$

where

$$S_1 := \{\varphi \in S_0, a_0 \text{ is a norm of } L_\beta/K_\varphi, \beta|\varphi\}$$

Otherwise, we can only find L with $[L : K] = 2m$.

Notation: If L/K is cyclic corresponding to a character χ (local or global), then denote $\mathfrak{f}|_{L/K} = \mathfrak{f}|_{\chi}$.

Thus, we state the following problem:

Problem II S, L_v/K_v are given above in Theorem 0.5. Find a global extension L/K satisfying Theorem 0.5 and find the least bound of $N(\mathfrak{f}_{L/K})$ in terms of K, S, m, $N\mathfrak{f}_{L_v/K_v}$.

Remark 1: Such bound for **Problem I** or **Problem II** should exist, since for each local field K_v, $K_v^{\times n}$ is of finite index in $K_v^{\times}$, thus the set of local characters on $K_v^{\times}$ of exponent m is finite. Thus the character family $\{\chi_v, v \in S\}$ is from a finitely many choice. For each choice of $\{\chi_v, v \in S\}$, there is a solution χ satisfying Theorem 0.2. Choose the maximal of such $N(\chi)$ for χ obtained through all choices of $\{\chi_v, v \in S\}$.

Remark 2: **Problem I** and **Problem II** are not equivalent unless $\#S = 1$ or $m = 2$, and Theorem 0.2 and Theorem 0.5 are not equivalent unless $\#S = 1$ or $m = 2$.

Here we introduce the notation **BP1** and **BP2**, the least bounds obtained from **Problem I** and **Problem II**. If an expression E is found for such bound, we write **BP1** $\leqq E$ or **BP2** $\leqq E$, respectively.

Chapter 1 Preliminaries

1.1 Reciprocity Law and Properties

First recall some important properties of characters of finite order both in the global and local settings.

Let $K_\mathfrak{p}$ be a local field, $\mathfrak{p}$ be its maximal ideal, and assume that $\zeta_m \in K_\mathfrak{p}$, thus via the local class field theory, each subgroup of $K_\mathfrak{p}^\times$ of index M and exponent m corresponds to an abelian extension of $K_\mathfrak{p}$ of degree M and exponent m. Here, "*exponent* m" means that the Galois group of this abelian extension has exponent m. This correspondence is set up by the local reciprocity law. See [Ne86], [Ne91].

Consider a local field $L_\mathfrak{q} = K_\mathfrak{p}(\sqrt[m]{K_\mathfrak{p}^\times})$. By Kummer theory, $N_{L_\mathfrak{q}/K_\mathfrak{p}} L_\mathfrak{q}^\times = K_\mathfrak{p}^{\times m}$

and $Gal(L_\mathfrak{q}/K_\mathfrak{p}) = K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times m}$ is finite.

Consider the following reciprocity map $\tilde{\Phi}_\mathfrak{p}$:

$$\begin{aligned} \tilde{\Phi}_\mathfrak{p} : K_\mathfrak{p}^\times &\to K_\mathfrak{p}^{\times\wedge} \\ b &\to \chi_{b,\mathfrak{p}} = \left(\frac{*, b}{\mathfrak{p}}\right) \\ &= \frac{(*, L_\mathfrak{q}/K_\mathfrak{p})\sqrt[m]{b}}{\sqrt[m]{b}} \end{aligned}$$

where $\left(\frac{*,b}{\mathfrak{p}}\right)$ is the local Hilbert symbol, and $K_\mathfrak{p}^{*\wedge} = Hom(K_\mathfrak{p}^*, \mu(K))$.

By the local class field theory (See [A-T68], [Ne86] and [Ne91]), $\tilde{\Phi}_\mathfrak{p}$ induces

a homomorphism:

$$\Phi_{\mathfrak{p}} : K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times m} \to (K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times m})^{\wedge}$$

$$[b] \to \chi_{b,\mathfrak{p}}$$

$$\chi_{b,\mathfrak{p}}([a]) = \chi_{b,\mathfrak{p}}(a) = \left(\frac{a,b}{\mathfrak{p}}\right) \qquad \forall [a] \in K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times m},$$

Proposition 1.1. *$\Phi_{\mathfrak{p}}$ is an isomorphism.*

□

Proposition 1.2. *Let χ be a local character of exponent m of $K_{\mathfrak{p}}^{\times}$,*

(1) *If $\mathfrak{p} \nmid m$, then $\mathfrak{f}_{\chi} = 1$ iff χ is unramified, and $\mathfrak{f}_{\chi} = \mathfrak{p}$ iff χ is ramified. Say $\chi = \chi_{b,\mathfrak{p}}$ for some $b \in K_{\mathfrak{p}}$ Then $\mathfrak{f}_{\chi_{b,\mathfrak{p}}} = 1$ iff $b \in \mathcal{U}_{K_{\mathfrak{p}}} \cdot K_{\mathfrak{p}}^{\times m}$, $\mathfrak{f}_{\chi_{b,\mathfrak{p}}} = \mathfrak{p}$ otherwise.*

(2) *In general, if $\zeta_m \in K_{\mathfrak{p}}$ is* NOT *assumed, then $\mathfrak{f}_{\chi} \mid \mathfrak{p}^{\lambda_{\mathfrak{p}}+1}$, where*

$$\lambda_{\mathfrak{p}} = \begin{cases} 0, & \text{if } \mathfrak{p} \nmid m \\ \left[\upsilon_{\mathfrak{p}}(m) + \frac{e_{\mathfrak{p}/p}}{p-1}\right] & \text{if } \mathfrak{p} \mid m \end{cases}$$

where p is the rational prime lying under $\mathfrak{p}$, and $e_{\mathfrak{p}/p}$ is the ramification index of $\mathfrak{p}$ over p.

In particular, if $m = p^{\gamma}v$ and $p \nmid v$, then $\lambda_{\mathfrak{p}} = \left[e_{\mathfrak{p}/p}(\gamma + \frac{1}{p-1})\right]$ when $\mathfrak{p} \mid m$.

Remark. Here $[x]$ denotes the integral part of x, i.e., the largest integer not exceeding x.

Proof.

(1) See Prop 3.4 and Lemma 5.3 in [Ne86] and [Ne91].

(2) It suffices to show that:

If $v_{\mathfrak{p}}(x) \gneqq v_{\mathfrak{p}}(m) + e_{\mathfrak{p}/p}/(p-1)$,

then $y = \sum_{\alpha=0}^{\infty} \binom{\frac{1}{m}}{\alpha} x^{\alpha}$ converges, and $y^m = 1 + x$.

Since

$$\begin{aligned} v_{\mathfrak{p}}\left(\binom{\frac{1}{m}}{\alpha} x^{\alpha}\right) &= \alpha v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}\left(\frac{\frac{1}{m}(\frac{1}{m}+1)(\frac{1}{m}+2)\cdots(\frac{1}{m}+\alpha-1)}{\alpha!}\right) \\ &= \alpha[v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(m)] - v_{\mathfrak{p}}(\alpha) \\ &\geqq \alpha[v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(m)] - \sum_{\gamma=1}^{\infty} \frac{\alpha}{p^{\gamma}} v_{\mathfrak{p}}(p) \\ &= \alpha(v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(m) - \frac{e_{\mathfrak{p}/p}}{p-1}) \to 0 \end{aligned}$$

as $v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(m) - \frac{e_{\mathfrak{p}/p}}{p-1}$ is positive. Thus as a formal series, $y = (1+x)^{\frac{1}{m}}$ $\square$

Now we come to global characters. Let K be a number field with $\zeta_m \in K$. Consider the following map:

$$\tilde{\Phi} : K^{\times} \to {C_K}^{\wedge}$$

$$b \to \chi_b$$

$$\forall a \in C_K, \chi_b(a) := \frac{(a, K(\sqrt[m]{b})/K)\sqrt[m]{b}}{\sqrt[m]{b}}$$

where $(a, K(\sqrt[m]{b})/K)$ is the global reciprocity law symbol.

The main assertion about the global characters is the following Proposition.

Proposition 1.3. (The interconnection between the global and local reciprocity laws of exponent m)

(1) $\tilde{\Phi}$ *induces an isomorphism* Φ *between* $K^{\times}/K^{\times m}$ *and the group of con-*

tinuous characters on C_K of exponent m.

(2) *For $b \in K^\times$, $\mathfrak{p}$ a prime ideal of K, we have*

$$\chi_b|_{\mathfrak{p}} = \left(\frac{*, b}{\mathfrak{p}}\right) = \chi_{b,\mathfrak{p}}$$

where $\chi_{b,\mathfrak{p}} = \left(\frac{\cdot, b}{\mathfrak{p}}\right)$ is the m-th power Hilbert symbol on $K_{\mathfrak{p}}$.

This is standard. See [Ne86] and [Ne91].

Next, we consider $\lambda_{\mathfrak{p}}$ appeared in Prop 1.2, and state and prove some results, which will be useful to us in the later chapters.

Lemma 1.4. *Let K be a number field, m an integer. (Here ζ_m is not assumed to be in K.)*

(1) *$\prod_{\mathfrak{p}} \mathfrak{p}^{\lambda_{\mathfrak{p}}}$ divides $\prod_{\mathfrak{p}|m} \mathfrak{p}$ which in turn divides $(m)\prod_{p|m}(p)$.*

(2)

$$\prod_{\mathfrak{p}} (N\mathfrak{p})^{\lambda_{\mathfrak{p}}} \leqq \left\{ m \prod_{p|m} p \right\}^{n_K}$$

(3) *For any global character χ of exponent m, put $\mathfrak{f}_\chi = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ and $\chi_v = \chi|_v$. Then, $\prod_{v|m} \mathfrak{f}_{\chi_v}$ divides $(m)\prod_{p|m}(p)^2$, and $\mathfrak{f}_\chi$ divides*

$$\prod_{\mathfrak{p} \, real.} \mathfrak{p}(m) \prod_{p|m} (p)^2 \prod_{\mathfrak{p} \nmid m, \, ram.} \mathfrak{p}.$$

Hence,

$$N(\chi) \leqq \left\{ (m) \prod_{p|m} (p)^2 \right\}^{n_K} \prod_{\mathfrak{p} \nmid m, \, ram.} N(\mathfrak{p}).$$

Proof.

(1) As $\lambda_{\mathfrak{p}} \leqq v_{\mathfrak{p}}(m)+1$, then (1) immediately holds.

(2) Directly from (1).

(3) From Proposition 1.2, we have

$$\prod_{v|m} \mathfrak{f}_{\chi_v} \quad \text{divides} \quad \prod_{\mathfrak{p}|m} \mathfrak{p}^{1+\lambda_{\mathfrak{p}}} \quad \text{divides} \quad \prod_{\mathfrak{p}|m} \mathfrak{p}^{1+v_{\mathfrak{p}}(m)+e_{\mathfrak{p}/p}}$$

$$\text{divides} \quad \left\{ (m) \cdot \prod_{\mathfrak{p}|m} \mathfrak{p} \cdot \prod_{p|m} p \right\}$$

$$\text{divides} \quad (m) \cdot \prod_{p|m} (p)^2$$

and

$$\prod_{v\nmid m,\ \text{finite}} \mathfrak{f}_{\chi_v} \quad \text{divides} \quad \prod_{\mathfrak{p}|m, \chi|_{\mathfrak{p}}\ \text{ram.}} \mathfrak{p}$$

using $\mathfrak{f} = \prod_{v\ \text{finite}} \mathfrak{f}_v \cdot \prod_{\mathfrak{p}\ \text{real}} \mathfrak{p}$.

Thus all assertions in (3) hold. Done. □

The following corollary can be easily drawn from Lemma 1.4 and Proposition 1.2, together with the Kummer theory.

Corollary 1.5. *Assume that* $\zeta_m \in K$, K *a number field,* $\chi = \chi_b$, *and* $(b) = \prod_{\mathfrak{p}|m} \mathfrak{p}^{n_{\mathfrak{p}}(b)} \cdot \mathfrak{c}$, *and* $b \in \mathcal{O}_K \backslash \{0\}$, $\mathfrak{c}$ *being some cycle not involving those primes* $\mathfrak{p} \mid m$.

Then

$$\mathfrak{f}_\chi \quad \text{divides} \quad \mathfrak{c}_1(m) \prod_{p|m} (p)^2 N\mathfrak{c}$$

and

$$N(\chi) \leqq \left\{ m \prod_{p|m} p^2 \right\}^{n_K} N\mathfrak{c} \cdot 2^{c_1}$$

where $\mathfrak{c}_1$ *is the cycle which is the formal product of all real primes in* K*, and* c_1 *denotes the numbers of all real places* v *of* K *where* χ_v *is ramified.*

Proof.

Note that for $\mathfrak{p} \nmid m$, $\chi|_{\mathfrak{p}}$ is ramified iff $\mathfrak{f}_{\chi|_{\mathfrak{p}}} = \mathfrak{p}$, iff $m|v_{\mathfrak{p}}(\mathfrak{c})$. □

1.2 l-extensions

Next we want to say something about *l–extensions*, by which we mean cyclic field extensions of degree a prime number l.

Assume that K is a number field, $m = l$, an odd rational prime, let χ a global character of K of exponent l. $K_1 = K(\zeta_l)$, and $\tilde{\chi} = \chi \circ N_{K_1/K}$.

For each prime tower ω/v in K_1/K, we have the following commutative diagram:

$$\begin{array}{ccc} (K_1)_\omega & \longrightarrow & C_{K_1} \\ \downarrow{\scriptstyle N_{(K_1)_\omega/K_v}} & & \downarrow{\scriptstyle N_{K_1/K}} \\ K_v & \longrightarrow & C_K \end{array}$$

such that:

$$\tilde{\chi}|_\omega = \chi_v \circ N_{(K_1)_\omega/K_v}$$

i.e., the localization commutes with the norm.

The following is easy but crucial. It will be used in the Chapter 4.

Lemma 1.6. *Let* $\chi_v = \chi|_v$, *and* $\tilde{\chi}_\omega = \chi_v \circ N_{(K_1)_\omega/K_v}$. *Then* $\tilde{\chi}|_\omega = \tilde{\chi}_\omega$ *and*

$$\prod_{\omega|v} \mathfrak{f}_{\tilde{\chi}_\omega} \mid \mathfrak{f}_{\chi_v},$$

equality holds if $v \nmid l$. *Hence,*

$$\prod_{\omega|v} N(\tilde{\chi}_\omega) \mid N(\chi_v)^{[K_1:K]},$$

equality holds if $v \nmid l$. *Here, given a formal cycle* $\mathfrak{c}$ *of product of finite primes in* K, *we identify it with the cycle represented by the ideal* $\mathfrak{c}\mathcal{O}_{K_1}$ *in* K_1.

Proof.

It suffices to show (2) by all the discussion above.

For any $\alpha \in 1 + \mathfrak{p}_v^{n_v}$ in $K_v^\times$ where $\mathfrak{f}_{\chi_v} = \mathfrak{p}_v^{n_v}$,

$$N_{(K_1)_\omega/K_v}(\alpha) \subseteq 1 + \mathfrak{p}_v^{n_v}$$

Thus $\tilde{\chi}_\omega(\alpha) = \chi_v(N_{(K_1)_\omega/K_v}(\alpha)) = 1$, thus $\mathfrak{f}_{\tilde{\chi}_\omega} \mid \mathfrak{f}_{\chi_v}$, thus $\prod_{\omega|v} \mathfrak{f}_{\tilde{\chi}_\omega} \mid \mathfrak{f}_{\chi_v}$.

Furthermore, if $v \nmid l$, and $\omega \mid v$, then $\omega \nmid l$, and $\mathfrak{p}_v = \prod_{\omega|v} \mathfrak{p}_\omega$ since $(K_1)_\omega/K_v$ is unramified as $K_1 = K(\zeta_l)$.

And by Prop 1.2 $\mathfrak{f}_{\chi_v} = 1$ or $\mathfrak{p}_v$, and $\mathfrak{f}_{\tilde{\chi}_\omega} = 1$ or $\mathfrak{p}_\omega$.

Thus it suffices to show that $\tilde{\chi}_\omega$ is unramified iff χ_v is.

Due to the following diagram,

$$\begin{array}{ccc} F_1 & \xrightarrow{N_{F_1/F}} & F \\ \Big\downarrow{\scriptstyle N_{F_1/(K_1)_\omega}} & & \Big\downarrow{\scriptstyle N_{F/K_v}} \\ (K_1)_\omega & \xrightarrow[N_{(K_1)_\omega/K_v}]{} & K_v \end{array}$$

By the global reciprocity law, say χ_v corresponds to F/K_v for some cyclic extension field F, and $F_1 = F(\zeta_l)$ thus by the functorality and lemma 1.6, $F_1/K_{1\omega}$ is the field extension corresponding to $\tilde{\chi}_\omega$.

Note that $l \nmid [(K_1)_\omega : K_v]$ and $[F : K_v]$ and $[F_1 : K_{1\omega}]$ are 1 or l, thus they are equal. And also, $F_1/K_{1\omega}$ is unramified if F/K_v is unramified; $F_1/K_{1\omega}$ is totally ramified if F/K_v is totally ramified.

Thus (2) is true.

For (3), although we have identified the cycles of K with the corresponding ones in K_1 in the sense of Lemma 1.6, the norms mean different. They differ by a factor of $[K_1 : K]$ at the power index. □

More details will be discussed in later parts.

We conclude this section by the following proposition which is a direct consequence of the decomposition $\mathbb{I}_\mathbb{Q} = \mathbb{Q}^\times \times \mathbb{R}^+ \times \prod_p \mathcal{U}_{\mathbb{Q}_p}$. See [Lang70], [Ne91], [Ra-Va97].

Proposition 1.7. *Let p be a rational prime and χ_p a given local character on $\mathbb{Q}_p^\times$. Then there exists a global character χ of $C_\mathbb{Q}$ of the order dividing that of χ_p satisfying the following:*

(1) *χ is unramified at all rational primes $q \neq p$,*

(2) *$\chi|_p|_{\mathcal{U}_{\mathbb{Q}_p}} = \chi_p|_{\mathcal{U}_{\mathbb{Q}_p}}$. i.e., $\chi_p^{-1} \cdot \chi|_p$ is unramified.*

□

1.3 Local and Global m-th Powers

In this part we discuss the local and global m-th powers and the interconnection between them. More importantly, we go through a proof of the Grunwald–Wang Theorem, because we will later need to use both the notations and some ideas in the proof.

Recall that for any finite set S of primes of K, $C\ell_{K,S}$ denotes the S–class group of K.

For each number field K, and S some set of finite primes in K, we introduce the following notations.

$$
\begin{aligned}
I_K^*(m,S) &= I^*(m,S) \\
&:= \{\, c \in \mathbb{I}_K, v_\varphi(c_\varphi) \text{ is divisible by } m \text{ for all } \varphi \notin S \,\} \\
I_K(m,S) &= I(m,S) \\
&:= \{\, c \in \mathbb{I}_K, c_\varphi \in K_\varphi^{\times m} \text{ for all } \varphi \notin S \,\} \\
P^*(m,S) &= I^*(m,S) \cap K^\times \\
&:= \{\, a \in K^\times, v_\varphi(a) \text{ is divisible by } m \text{ for all } \varphi \notin S \,\} \\
P(m,S) &= I(m,S) \cap K^\times \\
&:= \{\, a \in K^\times, a \in K_\varphi^{\times m} \text{ for all } \varphi \notin S \,\}
\end{aligned}
$$

Lemma 1.8. *If $C\ell_{K,S} = 1$, i.e., $\mathbb{I}_K = \mathbb{I}_K^S \cdot K^\times$, then $P^*(m,S) = K^S \cdot K^{\times m}$.*

Remark. K^S denotes the set of S-units of K.

Proof. See [Lang70] or [Ne86]. □

Proposition 1.9. *Let K be a number field and S a finite set of primes, $P(m,S)$ defined as above. Thus $P(m,S) = K^{\times m}$ if $K(\zeta_{2^t})/K$ is cyclic, where $m = 2^t m'$ where m' is an odd integer. In general, $P(m,S) \supseteq K^{\times m/2}$.*

Proof. We proceed this into several steps.

Also see the Chapter 9 and 10 in [A-T68].

Step 1. Reduce to the prime power case

If we know that Proposition 1.9 is true when m a prime power, then

$$\begin{aligned} P(m,S) &= \bigcap_{p^\alpha | m} P(p^\alpha, S) \\ &= \bigcap_{p^\alpha | m, p \neq 2} K^{\times p^\alpha} \cap P(2^t, S) \\ &= K^{\times m'} \cap P(2^t, S) \end{aligned}$$

If $K(\zeta_{2^t})/K$ is cyclic, then

$$\begin{aligned} (\text{LHS}) &= K^{\times m'} \cap K^{\times 2^t} \\ &= K^{\times m} \end{aligned}$$

else

$$\begin{aligned} (\text{LHS}) &= K^{\times m'} \cap K^{\times 2^t/2} \\ &= K^{\times m/2} \end{aligned}$$

Here we used a fact that if $(a,b)=1$ for a, b positive integers, then $K^{\times a} \cap K^{\times b} = K^{\times ab}$.

In fact, say $ua+vb=1$, $u,v \in \mathbb{Z}$ then if $x \in K^{\times a} \cap K^{\times b}$ then $x = x^{ua+vb} \in K^{\times ab}$.

Remark: In fact

$$\begin{aligned}[P(m,S) : K^{\times m}] &= [K^{\times m'} \cap P(2^t, S) : K^{\times m}] \\ &= [P(2^t, S) : K^{\times 2^t}]\end{aligned}$$

by the following lemma and that $K^{\times m'} \cdot K^{\times 2^t} = K^{\times}$.

Lemma 1.10. *Let $H \subsetneqq G \subsetneqq W$ be abelian groups, $C \subsetneqq W$ another subgroup. Then $[C \cap G : C \cap H]$ divides $[G:H]$. In fact, $[G:H] = [GC:HC] \cdot [C \cap G : C \cap H]$. Then $[G:H] = [C \cap G : C \cap H]$ iff $GC = HC$.*

Proof.

$$[G : C \cap G] = [GC : C] = [GC : HC][HC : C] = [GC : HC][H : C \cap H]$$

Thus

$$[G:H] = [GC:HC] \cdot [C \cap G : C \cap H]$$

□

Continuation of the Proof of Prop 1.9.

Step 2: Kummer case, $m = p^r$, and $\zeta_m \in K$

Assume that $\zeta_{p^r} \in K$, need to show that $P(m,S) = K^{\times p^r}$.

$\forall \alpha \in P(m,S), \alpha \in K_\varphi^{\times m}$ for any $\varphi \in S$. Thus the Kummer extension $K(\sqrt[p^r]{\alpha})/K$ collapses completely outside S, i.e., $K_\varphi(\sqrt[p^r]{\alpha})/K_\varphi$ is a trivial extension. Thus by Theorem 5.2 in [A-T68] or Corollary 3.9 in [Ne86] which asserts that a Galois extension is trivial if all but finite primes split completely. We conclude that $K(\sqrt[p^r]{\alpha})/K$ is also trivial. i.e., $\alpha \in K^{\times p^r}$.

Step 3: $K(\zeta_{p^r})/K$ is cyclic of the degree of a prime power. $m = p^r$

Note that if p is an odd prime, then $K(\zeta_{p^r})/K$ is cyclic.

For each $\alpha \in P(m,S)$, let $S' = \{\varphi' | \varphi \in S,\ \varphi' \text{ primes in } K_1\}$, thus $\alpha \in K_\varphi^{\times m} \in K(\zeta_{p^r})_{\varphi'}^{\times p^r}$ for $\varphi' \mid \varphi$, $\varphi' \notin S'$.

Thus by step 2, we may assume that $\alpha = {\beta_0}^m$, $\beta_0 \in K(\zeta_{p^r})^\times$, $\beta_i = \beta_0 {\zeta_{p^r}}^i$. Thus $K(\beta_i)/K$ is a subextension of $K(\zeta_{p^r})/K$. Since $K(\zeta_{p^r})/K$ is cyclic of degree of p power, then all subextensions can be totally ordered by inclusion. If $\alpha \notin K^{\times m}$ then $\beta_i \notin K$, then select a minimal subextension $K(\beta_{i_0})/K$ which is contained in $K(\beta_i)/K$ for other K.

Note that $\varphi \notin S$ splits completely in $K(\beta_i)/K$ for some i since $\alpha = \beta^i$, thus $\varphi \notin S$ splits completely in $K(\beta_{i_0})/K$.

By Theorem 5.2 in [A-T68] we just mentioned, $K(\beta_{i_0}) = K$, $\beta_{i_0} \in K^\times$ contradicts the assumption that $\alpha = {\beta_{i_0}}^m \notin K^{\times m}$.

Step 4. $m = p^r$, p is odd

$\forall x \in P(m,S)$, let $K_1 = K(\zeta_p)$, $S' = \{\varphi' \mid \varphi \in S,\ \varphi' \text{ primes of } K_1.\}$, thus $\forall \varphi' \notin S'$, $\varphi' \mid \varphi$, $x \in K_\varphi^{\times m} \subseteq {K_1}_{\varphi'}^{\times m}$.

Note that $K_1(\zeta_{p^r})/K_1$ is cyclic of degree of power of p, from the last step, $x \in {K_1}^{\times m}$, thus $x = y^m$ for some $y \in {K_1}^\times$.

Let $\lambda = [K_1 : K] \mid p-1$, then

$$x^\lambda = N_{K_1/K}(x) = N_{K_1/K}(y^m) = (N_{K_1/K}(y))^m$$

Thus $x^\lambda \in K^{\times m}$.

Note that $(\lambda, m) = (\lambda, p^r) = 1$ as $\lambda \mid p-1$, we get $x \in K^{\times m}$.

Step 5. $m = 2^t$, $K(\zeta_m)/K$ is cyclic

$K(\zeta_{2^t})/K$ is cyclic of degree dividing 2^{t-1}; thus from the step 3, the proposition is true in this case.

Step 6. $m = 2^t$, $t \geqq 3$, then $P(m, S) \subsetneqq K^{\times m/2}$

Note that $K(\zeta_4)/K = K(\sqrt{-1})/K$ is cyclic. Thus if $K(\zeta_{2^t})/K$ is not cyclic, $t \geqq 3$.

Now we prove that $P(m, S) \subsetneqq K^{\times m/2}$. In fact, let $K_1 = K(\sqrt{-1})$, $\tilde{S} = \{\tilde{\varphi} \mid \varphi,\ \tilde{\varphi} \text{ primes of } K_1\}$. $\forall \tilde{\varphi} \in \tilde{S}$, $\tilde{\varphi} \mid \varphi$, $x \in K_\varphi^{\times m} \subset K_{1\tilde{\varphi}}^{\times m}$.

Note that $K_1(\zeta_{2^t})/K_1$ is cyclic. Thus by the step 5, $x \in {K_1}^{\times 2^t}$.

Say $x = y^{2^t}$, for some $y \in K_1 = K(\sqrt{-1})$, thus

$$x^2 = N_{K(\sqrt{-1})/K}(x) = \left(N_{K(\sqrt{-1})/K}(y)\right)^{2^t}$$

Hence $x = \pm y^{2^{t-1}}$. If $x = -y^{2^{t-1}}$, then $-x \in K_\varphi^{\times 4}$ for all $\varphi \notin S$ as $t \geqq 3$, then $-1 \in K_\varphi^{\times 4}$ for all $\varphi \notin S$. Thus by the step 5, $-1 \in K^{\times 4}$, thus $\pm\sqrt{-1} \in K^{\times 2}$, thus $K_1 = K(\sqrt{-1})/K$, thus $x \in K^{\times m}$.

Otherwise $x \in K^{\times m/2}$.

Combining up the last 6 steps, we get the proposition. □

Proposition 1.11 (Description of the special case). *If K is a number field, $K(2^t)/K$ is not cyclic. $m = 2^t m', 2 \nmid m'$*

Here

$$\begin{aligned} a_0 &= (1+\zeta_{2^s})^m \\ &= (2+\eta_{2^s})^{m/2} = (\sqrt{-1}(2+\eta_{2^s}))^{m/2} \end{aligned}$$

where s is the integer such that $\eta_{2^s} \in K$ and $\eta_{2^{s+1}} \notin K$.

Then

(1) *$P(m,S) \subsetneqq K^{\times m} \cup a_0 K^{\times m}$, and $8 \mid m$.*

(2) *If $-(2+\eta_{2^s})$ is a nonsquare in $K^\times$.*

Let

$$S_0 := \{\, \varphi|2, \quad -1,\ \pm(2+\eta_{2^s}) \text{ are nonsquares in } K_\varphi^\times \,\}$$

then $P(m,S) = K^{\times m}$ if $S_0 \subsetneqq S$;

$$P(m,S) = K^{\times m} \cup^* a_0 K^{\times m} \text{ if } S_0 \subsetneqq S.$$

(3) *If $-(2+\eta_{2^s})$ is a square in $K^\times$ then $a_0 = (1+\zeta_{2^s})^m \in K^{\times m}$.*

Remark: Here we explain why Prop 1.9 and Prop 1.11 lead to Theorem 0.3. Note that if $K(\zeta_{2^t})/K$ is not cyclic, then we rule out the possibility that K is a function field. Also -1 is not a square of K since $Gal(K(\zeta_{2^t})/K(\sqrt{-1}))$ is a subgroup of $Gal(\mathbb{Q}(\zeta_{2^t})/\mathbb{Q}(\sqrt{-1}))$ which is cyclic. Here $\pm\sqrt{-1}^2 = -1$.

Also $2+\eta_{2^s} = (\pm\eta_{2^{s+1}})^2$, and $\eta_{2^{s+1}} \notin K^\times$, thus $2+\eta_{2^s}$ is not a square.

Also $t \geqq 3$ since $K(\zeta_{2^r})/K$ is cyclic if $t \leq 3$.

Also check that

$$a_0 = (1+\zeta_{2^s})^m = {\eta_{2^{s+1}}}^m = \left(\sqrt{-1}\eta_{2^{s+1}}\right)^m$$
$$= [\pm(2+\eta_{2^s})]^{m/2}$$

Thus all assertions can be easily deduced from these two propositions.

Proof of Proposition 1.11.

Let $K_1 = K(\sqrt{-1}) = K(\sqrt{-1})$, then $K_1(\zeta_{2^t})/K_1$ is cyclic. By the remark $8 \mid m$ and $t \geqq 3$.

Thus by Prop 1.9,

$$P(m,S) = {K_1}^{\times m} \subsetneqq {K_1}^{\times 2^t}$$

$\forall x \in P(m,S)$, say $x = y^{2^t}$, $y \in K_1$.

Let σ be the nontrivial element of $Gal(K_1/K)$, i.e., the nontrivial automorphism of K_1, then $x = \sigma(y)^{2^t}$.

Thus

$$\left(\frac{y}{\sigma(y)}\right)^{2^t} = 1$$

$$\frac{y}{\sigma(y)} = {\zeta_{2^t}}^r$$

for some r, and ${\zeta_{2^t}}^r \in K_1$. Also

$${\zeta_{2^t}}^{-r} = \frac{\sigma(y)}{y} = \sigma\left(\frac{y}{\sigma(y)}\right) = \sigma({\zeta_{2^t}}^r)$$

Let $r = 2^{t-\lambda} \cdot \mu$ for some integer λ and some odd integer μ.

Say $\mu A + 2^t B = 1$ for some integer A and B, thus ${\zeta_{2^t}}^{-rA} = \sigma\left({\zeta_{2^t}}^{rA}\right)$.

However,

$$\begin{aligned} {\zeta_{2^t}}^{rA} &= {\zeta_{2^t}}^{2^{t-\lambda}\mu A} = {\zeta_{2^t}}^{2^{t-\lambda}(1-2^t B)} \\ &= {\zeta_{2^t}}^{2^{t-\lambda}} = \zeta_{2^\lambda} \end{aligned}$$

and

$$\underset{K_1/K}{Trace}(\zeta_{2^\lambda}) = \zeta_{2^\lambda} + {\zeta_{2^\lambda}}^{-1} = \eta_{2^\lambda} \in K$$

By the assumption of s, $\lambda \leqq s$.

Thus

$$\frac{y}{\sigma(y)} = {\zeta_{2^s}}^{\mu_0}$$

for some μ_0.

Note that

$$\zeta_{2^s} \in \mathbb{Q}(\eta_{2^s}, \sqrt{-1}) \subseteq K(\sqrt{-1}) = K_1$$

and $\sigma\zeta_{2^s} = {\zeta_{2^s}}^{-1}$ since $Im\,\zeta_{2^s} \in \mathbb{Q}(\eta_{2^s})$, and

$$\begin{aligned} \sigma(\zeta_{2^s}) &= \sigma(\zeta_{2^s}) + \sigma(\sqrt{-1})\sigma(Im\,\zeta_{2^s}) \\ &= \eta_{2^s} - \sqrt{-1}\,Im\,\zeta_{2^s} = {\zeta_{2^s}}^{-1} \end{aligned}$$

Thus $\sigma(1 + \zeta_{2^s}) = 1 + {\zeta_{2^s}}^{-1}$

and

$$\frac{1+\zeta_{2^s}}{\sigma(1+\zeta_{2^s})} = \zeta_{2^s}$$

Thus let $y' = y/(1+\zeta_{2^s})^{\mu_0} \in K_1$.

Check that

$$y'/\sigma(y') = y/\sigma(y) \Big/ ([1+\zeta_{2^s}]/[1+\zeta_{2^s}{}^{-1}])^{\mu_0} = 1$$

Thus $y' \in K$.

Thus $x = (1+\zeta_{2^s})^{2^t\mu_0} \in K^{\times 2^t}$.

Note that

$$(1+\zeta_{2^s})^{2^{t+1}} = (2+\eta_{2^s})^{2^t} \in K^{\times 2^t}$$

and

$$a_0 = (1+\zeta_{2^s})^m = (1+\zeta_{2^s})^{2^t m'} = (2+\eta_{2^s})^{2^{t-1}m'}$$

Thus

$$x \in K^{\times 2^t} \cup a_0 K^{\times 2^t}$$

As x and $a_0 \in K^{\times m'}$.

Thus

$$x \in (K^{\times 2^t} \cap K^{\times m'}) \cup a_0(K^{\times 2^t} \cap K^{\times m'})$$
$$= K^{\times m} \cup a_0 K^{\times m}$$

Thus (1) holds.

Now Prove (2).

If $-(2+\eta_s)$ is a nonsquare in $K^\times$, i.e, $\pm\sqrt{-1}\eta_{2^{s+1}} \notin K$, we have that $F = K(\zeta_{2^{s+1}}) = K(\sqrt{-1}, \eta_{2^{s+1}})$ over K a four-group subextension of $K(\zeta_{2^t})/K$.

Thus by the definition of S_0, F/K collapses at φ iff $\varphi \notin S_0$ since $-1 = \sqrt{-1}^2$, $(\pm\eta_{2^{s+1}})^2 = 2 + \eta_{2^s}$ and $(\pm\sqrt{-1}\eta_{2^{s+1}})^2 = -(2+\eta_{2^s})$.

Note that if $\sqrt{-1} \in K_\varphi^\times$ then $\zeta_{2^s} \in \mathbb{Q}(\eta_{2^s}, \sqrt{-1}) \subset K_\varphi^\times$. Thus if F/K collapses and $\sqrt{-1}$, $\eta_{2^{s+1}}$ or $\sqrt{-1}\eta_{2^{s+1}} \in K_\varphi^\times$, then

$$a_0 = (1+\zeta_{2^s})^m = {\eta_{2^{s+1}}}^m = (\sqrt{-1}\eta_{2^{s+1}})^m \in K_\varphi^{\times m}$$

Next, we will prove that $a_0 \notin K_\varphi^{\times m}$ for $\varphi \in S_0$.

Assume that

$$a_0 \in K_\varphi^{\times m} \qquad (*)$$

Then $a_0 \in K_\varphi^{\times 2^t}$. In $K(\zeta_{2^t})/K$,

$$x^{2^t} - a_0 = \prod_{r=0}^{2^t-1} (x - {\zeta_{2^t}}^r (1+\zeta_{2^s})^{m'})$$

Thus say $b_r = {\zeta_{2^t}}^r (1+\zeta_{2^s})^{m'}$, thus $K(b_r)/K$ is a subextension of $K(\zeta_{2^t})/K$ for

each r, thus it is abelian.

Since F/K does not collapse at φ as $\varphi \in S_0$, thus neither does $K(\zeta_{2^t})/K$. Thus for each r, if b_r is not in $K^\times$, then $K(b_r)/K$ will not collapse at φ, thus $b_r \in K_\varphi^\times$. Thus by the assumption (*) we claim that one of the b_r should be in $K^\times$.

Thus for some r

$$\zeta_{2^t}{}^r \cdot (1+\zeta_{2^s})^{m'} \in K^\times$$

Thus

$$\zeta_{2^t}{}^{2r} \cdot (1+\zeta_{2^s})^{2m'} = \zeta_{2^t}{}^{2r+2^{t-s}m'} \cdot (2+\eta_{2^s})^{m'} \in K^{\times 2} \subset K^\times$$

As $2+\eta_{2^s} \in K^\times$, thus $\zeta_{2^t}{}^{2r+2^{t-s}m'} \in K$.

Since $\sqrt{-1} \notin K$ we have $\zeta_{2^{2r'+2^{t-s}m'}} = \pm 1$, then $\pm(2+\eta_{2^s})^{m'} \in K^{\times 2}$, thus $\pm(2+\eta_{2^s}) \in K^{\times 2}$, which contradicts the assumption of (2) stated in Prop 1.9.

So (*) is not true.

(3) is easy since $\left(\sqrt{-1}\eta_{2^{s+1}}\right)^2 = -(2+\eta_{2^s})$ and $a_0 = \left(\sqrt{-1}\eta_{2^{s+1}}\right)^m$ □

Given S, let $\tilde{P} = \prod_{\varphi \in S} K_\varphi^\times$ and endow it with the product topology, thus via the natural embedding $K_\varphi^\times \hookrightarrow \mathbb{I}_K$ and $K_\varphi^\times \hookrightarrow C_K$, we get the two injective homomorphisms: $\tilde{P} \hookrightarrow \mathbb{I}_K$ and $\tilde{P} \hookrightarrow C_K$.

Throughout this part and Chapter 5, P be the image of $\tilde{P}$ in C_K via the natural map. Note that the natural map $\tilde{P} \to P \hookrightarrow C_K$ is continuous, but in general not a homeomorphism unless $\#S = 1$. See [A-T68], [Lang70], [Ra-Va97].

1.4 Local and Global m-th Powers (II)

A problem arises: how can we characterize open subgroups of P of finite index?

Proposition 1.12. *Let $P_0 \subset P \hookrightarrow C_K$ be a subgroup with its pre-image $\tilde{P}_0$ via the natural map $\tilde{P} \to P \hookrightarrow C_K$.*

Then P_0 is open in P of finite index iff $\tilde{P}_0$ is open in $\tilde{P}$ of finite index, i.e., if $[P : P_0] < \infty$, P_0 is open in P.

Remark. Since $\tilde{P} \to P \hookrightarrow C_K$ is continuous, then "P_0 open in P" implies "$\tilde{P}_0$ is open $\tilde{P}$". The converse is not true in general, but $[P : P_0] < \infty$ implies that $\tilde{P}_0$ is open in $\tilde{P}$ of finite index, as $K_\varphi^{\times m}$ is open in $K_\varphi^\times$ for all φ and m.

Proof. Assume that $[P : P_0] < \infty$ need to show that P_0 is open P.

Note that $P_0 \supseteq P^{[P:P_0]}$, and P^n is of finite index in P. Thus it suffices to show that P^n is open in P as P_0 is the union of some cosets of P^n. Since any closed subgroup of a topological group of finite index is open, it suffices to show that P^n is closed in P.

We claim that P^n contains $P \cap {C_K}^{2n}$. Since C_K^{2n} is closed in C_K thus $P \cap {C_K}^{2n}$ is closed in P. Also, the index of $P \cap {C_K}^{2n}$ in P is less than or equal to the one of P^{2n} in P which is finite as $P \cap {C_K}^{2n} \supseteq P^{2n}$, thus $P \cap {C_K}^{2n}$ is open in P, thus so is P^n in P. Done.

Now we prove the claim. In fact, for any $[x] \in P \cap {C_K}^{2n}$ for some $x \in \mathbb{I}_K$ while $(x)_\varphi = 1$ for $\varphi \notin S$. Thus for some $b \in K^\times$, $b^{-1}x \in {\mathbb{I}_K}^{2n}$, thus $b^{-1} \in K_\varphi^{\times 2n}$ for all $\varphi \notin S$, thus by Proposition 1.9. $b^{-1} \in K^{\times n}$, thus $x \in \mathbb{I}_K^n$ and $[x] \in P^n$. □

Proposition 1.13. (1)*: $P \cap {C_K}^n = P^n$ unless we're in the special case.*

Let a_0^* be the idele class represented by the idele: a_0 at $\varphi \in S_0$, and 1 outside. Then if the special case occur, $P \cap {C_K}^n = P^n \cup a_0 P^n$, where $a_0 = (2 + \eta_{2^s})^{m/2}$ and s is the largest integer such that $\eta_{2^s} \in K$.

(2): ${C_K}^n$ is closed in C_K.

Proof. First prove (1).

Abuse the notation. Also denote P the image of $\tilde{P}$ in $\mathbb{I}_K$. If $x \in P \cap K^\times \mathbb{I}_K^n$. Say $x = az^n$ where $z \in \mathbb{I}_K$ and $a \in K^\times$. Thus $a \in P(n, S) = K^{\times n}$ unless the special case occurs, whence $a \in P(n, S) = K^{\times n} \cup a_0 K^{\times n}$. Note that $a_0 \in K_\varphi^{\times n}$ for all $\varphi \notin S_0$ from Proposition 1.11, we prove (1).

(2) (Also see [A-T68], [Ra-Va97] and [Ne86]). Let S^* be sufficiently large containing all infinite primes such that $C\ell_{K,S^*} = 1$.

Let $\mathbb{I}_K = \cup_{T \supset S^*} \mathbb{I}_{K,T}$ where $\mathbb{I}_{K,T} := \left\{ i \in \mathbb{I}_K, (i)_\varphi \in \mathcal{U}_{K_\varphi} \text{ for } \varphi \notin T \right\}$.

$\mathbb{I}_{K,T}$ is open in $\mathbb{I}_K$ for each T, thus it suffices to show that

$K^\times \mathbb{I}_K^n \cap \mathbb{I}_{K,T}$ is closed in $\mathbb{I}_{K,T}$.

(Thus $K^\times \mathbb{I}_K^n$ is closed in $\mathbb{I}_K$, thus ${C_K}^n$ is closed in C_K.)

$$\forall x \in K^\times \mathbb{I}_K^n \cap \mathbb{I}_{K,T}$$

$$x = a \cdot i^n, \qquad i \in \mathbb{I}_K, \qquad a \in K^\times$$

thus $a \cdot {(i)_\varphi}^n \in \mathcal{U}_{K_\varphi}$ for $\varphi \notin T$, thus $n \mid v_\varphi(a)$ where v_φ be the valuation corresponding to φ.

Let $\beta = \prod_{\varphi \notin T} \varphi^{\frac{v_\varphi(a)}{n}}$, since $C\ell_{K,T} = 1$ then

$\alpha \in J_{K,T}$ such that $\alpha\beta$ is principal.

Say $\alpha\beta = (\gamma)$, and let $a' = a \cdot \gamma^{-n}$.

Check that $v_\varphi(a') = 0$ for $\varphi \notin T$. Thus $a' \in K^T$ and $i' = \gamma i \in \mathbb{I}_{K,T}$, thus $K^\times \mathbb{I}_K^n \cap \mathbb{I}_{K,T} = K^T {\mathbb{I}_{K,T}}^n$.

Note that ${\mathbb{I}_{K,T}}^n$ is closed in $\mathbb{I}_{K,T}$, and $K^T : {K^T}^n$ is finite,

thus $[K^T {\mathbb{I}_{K,T}}^n : (K^T)^n {\mathbb{I}_{K,T}}^n = {\mathbb{I}_{K,T}}^n] < \infty$, thus $K^T \cdot {\mathbb{I}_{K,T}}^n$ is also closed in $\mathbb{I}_{K,T}$, Done. □

Remark: K^T denote the set of T-units in $K^\times$. i.e, the set of elements in K^T which is a unit in K_φ outside T.

The next thing is as follows: Say $P \cap C^n \subsetneqq P_0$, can we find an open subgroup V in $C = C_K$ such that $V \supsetneqq C^n$ and $P \cap V = P_0$.

Similar to the case of global characters, we can also introduce the conception of a *conductor* an open subgroup of C_K.

Let V be any open subgroup of C_K^1. Define $\mathfrak{f}_V$ the least cycle $\mathfrak{m}$ such that $C_K^{\mathfrak{m}} \subsetneqq V$.

Definition W a topological abelian group, $H \leqq G \leqq W$ is a tower of subgroups of W.

We say that an open subgroup V (of e—which is the identity element of W) *separates* G/H iff $G \cap V \subsetneqq H$.

Remark. It's easy to show that: if $G \cap V \subsetneqq H$ then $G \cap VH = H$.

Lemma 1.14. *$H \leqq G$ open subgroup, $G \subsetneqq W$ abelian, $W^n \leqq H$, then the following are equivalent:*

(a) $\exists$ *an open subgroup* V *such that* $G \cap W^n V \subsetneqq H$.

(b) $\exists$ *an open subgroup* V *such that* $GW^n \cap V \subsetneqq HW^n = H$, *i.e.,* V *separates* GW^n/H.

(c) $\exists$ *an open subgroup* V_H *such that* $V_H \supsetneqq HW^n$ *and* $G \cap V_H = H$.

Proof.

(a) $\Rightarrow$ (b): If $G \cap W^n V \subsetneqq H$, then $\forall x \in GW^n \cap V$, say $x = g\omega^n$ where $g \in G$, $\omega \in W$, then $g = x\omega^{-n} \in VW^n \cap G \subsetneqq H$, then $x \in HW^n = H$.

(b) $\Rightarrow$ (a): If $GW^n \cap V \subsetneqq HW^n$. Let $g \in G \cap W^n V$, $g = \omega^{-n} v$ for some $v \in V$ and $\omega \in W$, thus $v = g\omega^n \in V \cap GW^n \subsetneqq HW^n \in H$, thus $g \in HW^n = H$.

(a) $\Leftrightarrow$ (c): See the remark above. $\square$

From Lemma 1.14, to prove that there is a open subgroup V in $C = C_K$ such that $V \supset C^n$ and $P \cap V = P_0$ while P/P_0 is of exponent n, it suffices to find a open subgroup V of C_K such that $PC^n \cap V \subset P_0 C^n$, i.e., V separates PC^n/P_0C^n. If V separates PC^n/P_0C^n, then VC^n separates P/P_0 and VC^n contains C^n.

Since $[PC^n : P_0C^n] \mid [P : P_0]$ is finite, thus P_0C^n is open in PC^n if it is closed.

Lemma 1.15. (1) P_0C^n *is closed thus open in* PC^n *where* n *is an arbitrary positive integer.*

(2) C/C^n *is compact.*

Proof. From Prop 1.13, C^n is closed in C. Consider the following natural

homomorphism:

$$\Psi : \tilde{P} \to P \hookrightarrow C_K \to C/C^n$$

Of course Ψ is continuous, and is a group homomorphism.

Note that $P^n \subset C^n$ then Ψ factors through

$$\psi : \tilde{P}/\tilde{P}^n \to C/C^n$$

Note that

$$\tilde{P}/\tilde{P}^n = \prod_{\varphi \in S} K_\varphi^\times / K_\varphi^{\times n}$$

is compact.

In fact,

$$K_\varphi^\times / K_\varphi^{\times n} = \begin{cases} 1 \text{ or } \mathbb{Z}/2\mathbb{Z}, & \text{if } \varphi \text{ is real.} \\ 1, & \text{if } \varphi \text{ is complex.} \\ \mathbb{Z}/n\mathbb{Z} \times \mathcal{U}_{K_\varphi}/\mathcal{U}_{K_\varphi}^{(n)}, & \text{if } \varphi \text{ is non-Archimedean.} \end{cases}$$

The image of $\tilde{P}_0\tilde{P}^n/\tilde{P}^n$ in C/C^n is P_0C^n/C^n. Of course, $\tilde{P}_0\tilde{P}^n$ is open and closed in $\tilde{P}$ thus $\tilde{P}_0\tilde{P}^n/\tilde{P}^n$ is open and closed in $\tilde{P}/\tilde{P}^n$.

By the compactness of $\tilde{P}/\tilde{P}^n$ we get that P_0C^n/C^n is open and closed in PC^n/C^n. Thus P_0C^n is closed in PC^n.

Furthermore,

$$C/C^n = \mathbb{R}_+^\times / \mathbb{R}_+^{\times n} \times C_K^1 / {C_K^1}^n$$

and C_K^1 which consists of elements of norm 1 in C_K is compact (see [Ra-Va97]).

□

The following proposition and lemma will lead to a proof of the Grunwald–Wang theorem. In fact, if P/P_0 is cyclic and there is an open subgroup V such that $P \cap V = P_0$ and $V \supset C^n$, then we get a global character on PV/P_0V which can be extended to a character of the same order on C/P_0V which is finite.

Proposition 1.16. (the Grunwald–Wang Theorem, a "pre-formal" version)

(1) *Let P be the canonical image of $\prod_{v\in S} K_v^*$ in C_K with a subgroup P_0 such that $P \cap C^n \subset P_0$, Then there exists an open subgroup N_0 of C containing C^n such that*

$$PN_0/N_0 \cong P/P_0 = P/P \cap N_0$$

(2) *If P/P_0 is cyclic of order m, then there exists an open subgroup N such that C/N is cyclic of order m and $P \cap N_0 = P_0$, unless the special case occurs.*

If the special case occurs, and $P_0 \supsetneqq P \cap C^m$ then C/N can be made of order m otherwise C/N is of order $2m$.

Recall Theorem 0.3 for the definition of the special case.

Lemma 1.17. *Let $H \leqq G$ be a subgroup of finite index and G an abelian group, χ_H a character of H of exponent n, and $Ker\,\chi_H \supseteq G^n$. Then χ_H can be extended to a character χ_G on G of exponent n.*

Proof. Using the induction, we may assume that G/H is cyclic of a prime order, since in general, any subgroup tower of an abelian group is contained in a tower in which any two consecutive terms have their factor group cyclic of prime order.

Assume $Ker\,\chi_H = 1$ without loss of generation since $Ker\,\chi_H$ is also a normal subgroup of G.

Thus $H \cong \mathbb{Z}/a\mathbb{Z}$ where $a \mid n$, and G is of exponent n. Say $\#[G : H] = p$ for some prime number $p|n$.

If H has a complement N, i.e., $G = HN$ and $H \cap N = 1$, thus define χ_G as the following way:

$\chi_G(hn) = \chi_H(h)$ for $h \in H$ and $n \in N$.

Thus $Ker\,\chi_G = N$ and $\chi_G|_H = \chi_H$. Thus χ_G is what we need.

So we complete the cases when H has a complement.

If H has no complement, by the structure theory of abelian groups of finite order, the Sylow p-subgroup W of G which is also abelian should be cyclic. In fact, say $a = p^\alpha u$ where $p \nmid u$, if W is not cyclic, then W must be of type (p^α, p), and $W \cap H$ must have a complement Y which is a p group, and thus Y is a complement of H in G.

Note that $G = W \times M$ for some cyclic group M in H of order u, W is cyclic of order $p^{\alpha+1}$ and $H = (W \cap H) \times M$, thus it is easy to extend χ_H to χ_G of order $ap = \#G$ as G is cyclic, while G is of exponent n.

Done. □

Proof of Proposition 1.16.

(1) From Lemma 1.15, P_0C^n is open and closed in PC^n.

Assume that V separates PC^n/P_0C^n, i.e., $PC^n \cap V \subsetneqq P_0C^n$.

Let $N_0 = P_0C^nV$.

Then $P \cap N_0 = P \cap P_0C^nV \subsetneqq P_0C^n(P \cap V) = P_0C^n$.

Then $P \cap N_0 \subsetneqq P \cap P_0C^n \subsetneqq P_0(P \cap C^n) \subsetneqq P_0$.

Then $P \cap N_0 = P_0$ as $P_0 \subset P_0C^nV$.

Thus $PN_0/N_0 \cong P/P \cap N_0 = P/P_0$.

(2) $n = m$, or $2m$ is the special case occurs and $P \cap C^m \subsetneqq P_0$. We have $P \cap C^n \subset P_0$ from Prop 1.13. Applying (1), we find such N_0 and note that C/N_0 is of exponent n. Apply Lemma 1.17 and extend the character on $PN_0/N_0 \cong P/P_0$ to C/N_0 of exponent n, and let N be the kernel of such character, then N is what we need. Done. □

1.5 Quadratic Characters

This part is a preliminary part for Chapter 3. Here we list some well lemmas.

As $\mathbb{Q} \supsetneqq \mu_2 = \{\pm 1\}$, each quadratic extension over $\mathbb{Q}$ should be a Kummer extension.

Lemma 1.18. *Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic extension for some square free integer d, then we have*

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \pmod 4; \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Furthermore,

$$d_L = Disc\,\mathcal{O}_L = \begin{cases} 4d, & \text{if } d \equiv 2,3 \pmod 4; \\ d, & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Proposition 1.19. (Characterization of the local quadratic extension over $\mathbb{Q}_p$ or $\mathbb{R}$)

Let $K = \mathbb{Q}_p$ or $\mathbb{R}$ a local field of $\mathbb{Q}$, and L/K a quadratic extension. Then

(i) *If $K = \mathbb{R}$ then $L = \mathbb{C}$.*

(ii) *If $p \neq 2$ and $K = \mathbb{Q}_p$, then either*

(a) *L/K is unramified, $L = K(\sqrt{c})$, $c \in \mathcal{U}_{\mathbb{Q}_p}$ is not a square; or*

(b) *L/K is ramified, $L = K(\sqrt{p})$; or*

(c) *L/K is unramified, $L = K(\sqrt{pc})$, $c \in \mathcal{U}_{\mathbb{Q}_p}$ is not a square.*

(iii) *If $p = 2$, $K = \mathbb{Q}_2$ then*

(a) *L/K is unramified, $L = K(\sqrt{5})$; or*

(b) *L/K is ramified, $L = K(\sqrt{\lambda})$, $\lambda = \pm 2, -1, -5, \pm 10$.*

Remark. See Lemma 1.21.

Proposition 1.20. *If $L = \mathbb{Q}(\sqrt{d})$, d a square free integer, then*

(i) *∞ ramifies iff $d < 0$.*

(ii) *$p \neq 2$, a rational prime, ramifies iff $p \mid d$.*

If $p \mid d$, and $\frac{d}{p}$ is a square mod p, then case is (ii)(b) *in the last proposition; If $p \mid d$, and $\frac{d}{p}$ is not a square mod p, then the case is* (ii)(c).

If $p \nmid d$, then if d is not a square mod p, then the case is (ii)(a) *and p is inert; If d is a square mod p then p splits.*

(iii) *$p = 2$, ramifies iff $d \equiv 2,3 \pmod 4$;*

If $d \equiv 1 \pmod 8$ *then* 2 *splits, if* $d \equiv 5 \pmod 8$ *then* 2 *is inert.*

Lemma 1.21. *Let* $\chi_{K,d}$ *denote the local or global quadratic character, corresponding to* $K(\sqrt{d})/K$*, where the character is local if* K *is a local field, global if* K *is a global field.*

Then

$$\chi_{K,d\cdot d'} = \chi_{K,d} \cdot \chi_{K,d'}$$

i.e.,

$$\chi_{K,*} : \begin{cases} (K^\times/K^{\times 2})^\wedge \to \{\pm 1\}, & \text{if } K \text{ is local} \\ (C_K/{C_K}^2)^\wedge \to \{\pm 1\}, & \text{if } K \text{ is global} \end{cases}$$

is a continuous homomorphism.

Remark: Proof of Prop 1.20 and Lemma 1.21 can be found in many textbooks, for example in [Lang70], [Ne86], [Ne91]

Proof of Prop 1.19.

(i) is clear. We will prove (ii) and (iii) because we will need the explicit statements later.

(ii) Let p be an odd prime.

If L/K is unramified, then $L = K(\sqrt{c})$ for some $c \in \mathcal{U}_{\mathbb{Q}_p}$, where c is a non-square.

Note that if c_1 and c_2 are two non-squares in $\mathcal{U}_{\mathbb{Q}_p}$, then $c_1 {c_2}^{-1}$ is a square, then

$\chi_{\mathbb{Q}_p,c_1} = \chi_{\mathbb{Q}_p,c_2}$.

If L/K is ramified, then the corresponding character χ is not trivial on $\mathcal{U}_{\mathbb{Q}_p}$.

Note that $\chi_{\mathbb{Q},p}$ is not trivial on $\mathcal{U}_{\mathbb{Q}_p}$, and furthermore,

$(1+p\mathbb{Z}_p)^2 = 1+p\mathbb{Z}_p$ for p odd, thus χ and $\chi_{\mathbb{Q}_p,p}$ factor through $\mathcal{U}_{\mathbb{Q}_p}/1+p\mathbb{Z}_p \cong (\mathbb{Z}/p\mathbb{Z})^\times$ thus they both agree with quadratic symbol on $(\mathbb{Z}/p\mathbb{Z})^\times$.

Thus $\chi|_{\mathcal{U}_{\mathbb{Q}_p}} = \chi_{\mathbb{Q}_p,p}|_{\mathcal{U}_{\mathbb{Q}_p}}$, thus $\chi \cdot {\chi_{\chi_p,p}}^{-1}$ is unramified,

thus $\chi = \chi_{\mathbb{Q}_p,p}$ or $\chi_{\mathbb{Q}_p,p} \cdot \chi_{\mathbb{Q}_p,c} = \chi_{\mathbb{Q}_p,pc}$ for some nonsquare c in $\mathcal{U}_{\mathbb{Q}_p}$.

(iii) $\chi \in (\mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2)^\wedge$.

Note that $\mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$,

and $\chi_{\mathbb{Q}_2,-1}$, $\chi_{\mathbb{Q}_2,2}$ and $\chi_{\mathbb{Q}_2,5}$ are "linearly independent" in $(\mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2)^\wedge$, and also they generate $(\mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2)^\wedge$.

In fact, we have the following:

$$\chi_{\mathbb{Q}_2,-1}(-1) = -1 \qquad \chi_{\mathbb{Q}_2,-1}(5) = 1 \qquad \chi_{\mathbb{Q}_2,-1}(2) = 1$$

$$\chi_{\mathbb{Q}_2,2}(-1) = 1 \qquad \chi_{\mathbb{Q}_2,2}(5) = -1 \qquad \chi_{\mathbb{Q}_2,2}(2) = 1$$

$$\chi_{\mathbb{Q}_2,5}(-1) = 1 \qquad \chi_{\mathbb{Q}_2,5}(5) = 1 \qquad \chi_{\mathbb{Q}_2,5}(2) = -1$$

□

Chapter 2 A modified Version of the Chebotarev Density Theorem

In this chapter, we will prove an S–effective analog of the result in [L-M-O79].

By class field theory, idele class characters χ of finite order correspond in a canonical way to characters of $Gal(\bar{K}/K)$ of finite order. By abuse of notation, we will still use the letter χ to denote this Galois character. Moreover, there is a canonically associated finite abelian extension L/K such that the kernel of χ as an idele class character is the norm from C_L.

Throughout this section, for any number field L, d_L denotes the discriminant of L, and $d_{L/K}$ denotes the relative discriminant of L over a subfield K.

Theorem 2–C. *Let L/K be a Galois extension of number fields of degree n, S a finite set of primes of K, and C a conjugacy class in $Gal(L/K)$. Then there is a prime ideal $\mathfrak{p}$ of K such that* (1) *$\mathfrak{p}$ is unramified in L, and $\mathfrak{p}$ is of degree* 1 *over* $\mathbb{Q}$. (2) $\mathfrak{p} \notin S$. (3)

$$\left(\frac{L/K}{\mathfrak{p}}\right) = C$$

(4)

$$N_{K/\mathbb{Q}}\mathfrak{p} \leqq d_L^{A_2(\varepsilon)}(n \log N_S + 1)^{c+\varepsilon}$$

where ε is any positive number, $A_2(\varepsilon)$ is some constant only depending on ε. $c = 1$ *if ζ_L has no exceptional zero,* $c = 3/2$ *otherwise.*

An *exceptional zero* of $\zeta_L(s)$ is a real zero near $s = 1$. For details, see Lemma 2.3.

We note that by Stark ([Stk74]), there is no exceptional zero if the Galois closure $\tilde{L}$ of L over $\mathbb{Q}$ contains no quadratic extension, in particular, when $[\tilde{L} : \mathbb{Q}]$ is odd.

This theorem gives a strengthening of Theorem 1.1 in [L-M-O79]. The difference is the presence of condition (2) in our result. The basic method is as in [L-M-O79]; however, there are some delicate points to be resolved. We will accomplish this in Section 2.3 after some preliminaries in Sections 2.1 and 2.2.

In Chapter 6, (see Section 6.1), we also give such S–versions of two distinct results of this kind under GRH. But note that this is not the case for Theorem 2–C above, and indeed, every result till the end of Chapter 5 is unconditional.

2.1 Some Estimations, Preparations for the Main Argument

In this section, we will describe several things we plan to use in our proof.

First we introduce two kernel functions used in the classical analytic method, which was also used by Lagarias, Odlyzko, Montgomery and K. Murty (cf. [L-O77], [L-M-O79], [KM94] and [Se81]). The use of these two different

kernel functions is related to the *Explicit formulas* of A.P. Guinand ([Gu48]) and A. Weil ([We52]).

Let

$$k_1(s) = k_1(s; x, y) = \left(\frac{y^{s-1} - x^{s-1}}{s-1}\right)^2$$
$$k_2(s) = k_2(s; x) = x^{s^2+s}$$

Thus

$$k_1(1) = \left(\log \frac{y}{x}\right)^2$$
$$k_2(1) = x^2$$

For each smooth function $k(s)$, denote $\hat{k}(u)$ the inverse Mellin transform, defined as

$$\hat{k}(u) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} k(s) u^{-s} ds$$

where a is a sufficiently large number.

Thus for $a > 1$, we have

$$\hat{k}_1(u) = \hat{k}_1(u; x, y) = \begin{cases} 0, & \text{if } u \geq y^2 \text{ or } u \leq x^2; \\ \frac{1}{u} \log \frac{y^2}{u} & \text{if } xy \leq u \leq y^2; \\ \frac{1}{u} \log \frac{u}{x^2} & \text{if } x^2 \leq u \leq xy. \end{cases}$$

$$\hat{k}_2(u) = \hat{k}_2(u; x) = (4\pi \log x)^{-\frac{1}{2}} \exp\left\{-\frac{\left(\log \frac{u}{x}\right)^2}{4 \log x}\right\}$$

Note that for each j and u, $\hat{k}_j(u) \geq 0$, and for large u, $\hat{k}_j(u)$ is small.

Lemma 2.1. (1) *Let Σ^R denote the summation over the prime ideals of K that ramify in L, then*

$$\sum_{\mathfrak{p}}^{R} \sum_{m\geq 1} \log(N\mathfrak{p})\hat{k}_1(N\mathfrak{p}^m) << \frac{1}{n}\frac{\log\frac{y}{x}}{x^2}\log d_L$$

$$\sum_{\mathfrak{p}}^{R} \sum_{m\geq 1, N\mathfrak{p}^m \leq x^{10}} \log(N\mathfrak{p})\hat{k}_2(N\mathfrak{p}^m) << \frac{1}{n}(\log x)^{\frac{1}{2}}\log d_L$$

(2) *Let Σ^S denote the summation over the prime ideals of K in S, then*

$$\sum_{\mathfrak{p}}^{S} \sum_{m\geq 1} \log(N\mathfrak{p})\hat{k}_1(N\mathfrak{p}^m) << \frac{\log\frac{y}{x}}{x^2}\log N_S$$

$$\sum_{\mathfrak{p}}^{S} \sum_{m\geq 1, N\mathfrak{p}^m \leq x^{10}} \log(N\mathfrak{p})\hat{k}_2(N\mathfrak{p}^m) << (\log x)^{\frac{1}{2}}\log N_S$$

(3) *Let Σ^P denote the summation over the pairs $(\mathfrak{p}, m)$ for which $N\mathfrak{p}^m$ is not a rational prime, then*

$$\sum_{\mathfrak{p},m}^{P} \log(N\mathfrak{p})\hat{k}_1(N\mathfrak{p}^m) << n_K\frac{(\log\frac{y}{x})(\log y)}{x(\log x)}$$

$$\sum_{\mathfrak{p}}^{R} \log(N\mathfrak{p})\hat{k}_2(N\mathfrak{p}^m) << n_K x^{7/4}$$

(4)

$$\sum_{\mathfrak{p},m}^{R} \sum_{m\geq 1, N\mathfrak{p}^m > x^{3+\delta}} \log(N\mathfrak{p})\hat{k}_2(N\mathfrak{p}^m) << n_K x^{2-\frac{\delta^2}{4}}(\log x)$$

where δ is any positive number.

Proof.

For (1), see Lemma 3.1 in [L-M-O79]. For (2), the proof is almost the same as (1) except that we need to estimate $\sum^S \log(N\mathfrak{p})$ instead of $\sum^R \log(N\mathfrak{p})$.

For (3), see Lemma 3.2 in [L-M-O79]. However, a step in the original proof of the first estimation of that lemma needs to be slightly corrected as follows. Use the fact that the number of pairs $(\mathfrak{p}, m)$ such that $N\mathfrak{p}^m = q$ is at most n_K, and get

$$\begin{aligned}\sum_{\mathfrak{p},m}^{P} \log(N\mathfrak{p})\hat{k}_1(N\mathfrak{p}^m) &<< n_K(\log\frac{y}{x}) \sum_{x^2\le p^h\le y^2, h\ge 2} p^{-h}\log p^h \\ &<< n_K(\log\frac{y}{x})(\log y) \sum_{n=p^a, a\ge 2, n\ge x^2} n^{-1} \\ &<< n_K(\log\frac{y}{x})(\log y)\frac{1}{x\log x}\end{aligned}$$

where the last bound uses the prime number theorem.

For the second estimation, let $S(u)$ denote the number of prime power integers p^h in the interval $[1, u]$. It is easy to see that $S(u) << u^{1/2}$. Thus

$$\begin{aligned}\sum_{\mathfrak{p}}^{P} \log(N\mathfrak{p})\hat{k}_2(N\mathfrak{p}^m) &<< n_K \sum_{p,h\ge 2} \log(p^h)\hat{k}_2(p^h) \\ &<< n_K \int_3^\infty (\log u)\,\hat{k}_2(u)\,dS(u) << n_K x^{\frac{7}{4}}\end{aligned}$$

where the last bound uses the integration by part as in [L-M-O79].

For (4),

$$\begin{aligned}
\sum_{N\mathfrak{p}^m > x^{3+\delta}} \log(N\mathfrak{p})\hat{k}_2(N\mathfrak{p}^m) &<< n_K \sum_{q > x^{3+\delta}} (\log q)\hat{k}_2(q) \\
&<< n_K \int_{x^{3+\delta}}^{+\infty} (\log u)\hat{k}_2(u)du \\
&<< n_K (\log x)^{-\frac{1}{2}} \int_{(3+\delta)\log x}^{+\infty} t \exp\left(-\frac{(t-\log x)^2}{4\log x}\right) e^t dt \\
&<< n_K x^2 (\log x)^{-\frac{1}{2}} \int_{(3+\delta)\log x}^{+\infty} t \exp\left(-\frac{(t-3\log x)^2}{4\log x}\right) dt \\
&<< n_K x^2 (\log x)^{-\frac{1}{2}} \Big\{ \int_{\delta \log x}^{+\infty} 3\log x \exp\left(-\frac{t^2}{4\log x}\right) dt \\
&\quad + (\log x) \int_{\delta\sqrt{\log x}}^{+\infty} t \exp\left(-\frac{t^2}{4}\right) dt \Big\} \\
&<< n_K x^2 (\log x)^{-\frac{1}{2}} \Big\{ 3(\log x)^{3/2} \int_{\delta\sqrt{\log x}}^{+\infty} \exp\left(-\frac{t^2}{4}\right) dt \\
&\quad + (\log x) \exp\left(-\frac{\delta^2}{4}\log x\right) \Big\} \\
&<< n_k x^{2-\frac{\delta^2}{4}} (\log x)
\end{aligned}$$

where we use the well known estimate $\int_T^{+\infty} e^{-t^2/4} dt << e^{-T^2/4}$.

□

Recall that for any global character χ of K, $A(\chi)$ is defined as

$$d_K N_{K/\mathbb{Q}}(\mathfrak{f}_0(\chi))$$

where $\mathfrak{f}_0(\chi)$ is the finite part of the conductor of χ. For the definition, see Section 0.1.

Lemma 2.2. *Let χ be a global character of K.*

(1) *If $N(t) = N_L(t)$ denotes the number of zeros $\rho = \beta + i\gamma$, of $\zeta_K(s)$ with*

$0 < \beta < 1$ *and* $|\gamma - t| \leq 1$, *then we have*

$$N(t) << \log d_K + n_K \log(|t| + 2)$$

(2) *If* $n(r; s) = n_K(r; s)$ *denotes the number of zeros* ρ, *of* $\zeta_K(s)$ *with* $|\rho - s| \leq r$, *then we have*

$$n(r; s) << 1 + r(\log d_K + n_K \log(|s| + 2))$$

(3) *If* $N_\chi(t)$ *denotes the number of zeros* $\rho = \beta + i\gamma$, *of* $L(s, \chi, K)$ *with* $0 < \beta < 1$ *and* $|\gamma - t| \leq 1$, *then we have*

$$N_\chi(t) << \log A(\chi) + n_K \log(|t| + 2)$$

(4) *If* $n_\chi(r; s)$ *denotes the number of zeros* ρ *of* $L(s, \chi, K)$ *with* $|\rho - s| \leq r$, *then we have*

$$n_\chi(r; s) << 1 + r(\log A(\chi) + n_K \log(|s| + 2))$$

Proof. See [L-O77] and Lemma 2.2 in [L-M-O79]. □

Lemma 2.3. *Let* χ *be a global character of* K. *There is a positive, absolute, effectively computable constant* c_2 *such that*

(1) $L(s, \chi, K)$ *has no zero* $\rho = \beta + i\gamma$ *in the region*

$$\beta \geq 1 - {c_2}^{-1}(\log A(\chi) + n_K \log(|\gamma| + 2))^{-1}$$

$$\gamma \geq (1 + c_2 \log A(\chi))^{-1}$$

(2) $L(s,\chi,K)$ *has at most one zero in the region*

$$\beta \geq 1 - (c_2 \log A(\chi))^{-1}$$

$$\gamma \leq c_2 \log A(\chi))^{-1}$$

If such a zero exists, it must be simple and real, and χ *must be trivial or quadratic.*

In the last statement of the lemma, such zero is called the *exceptional zero* of $L(s,\chi,K)$. Again, by Stark ([Stk74]), if the Galois closure $\tilde{K}$ of K over $\mathbb{Q}$ contains no quadratic extension of $\mathbb{Q}$, χ must be quadratic.

Proof. See [L-O77], or [Lang70] and [Ne91]. □

Before finishing this part, we quote the Deuring–Heilbronn phenomenon here, a discussion of which can be found in Section 5 in [L-M-O79].

Lemma 2.4. [Deuring–Heilbronn Phenomenon]

There are positive, absolute, effectively computable constants c_7 *and* c_8 *such that if* $\zeta_L(s)$ *has a real zero* β_0*, then* $\zeta_L(\sigma+it) \neq 0$ *for*

$$\sigma \geq 1 - c_8 \cdot \frac{\log\left(\frac{c_7}{(1-\beta_0)\log(d_L\tau^{n_L})}\right)}{\log(d_L\tau^{n_L})}$$

where $\tau = |t|+2$ *with the single exception* $\sigma+it=\beta_0$.

□

Corollary 2.5. *There is a positive, absolute, effectively computable constant*

c_{10} such that any real zero β_0 of $\zeta_L(s)$ satisfies

$$1 - \beta_0 \geq {d_L}^{-c_{10}}$$

Proof. See Corollary 5.2 in [L-M-O79]. □

2.2 The Standard Model

In this part, we will recall the main model of [L-M-O79] for our method here. We have included the relevant details for the convenience of the readers.

We need to consider the Artin L–series $L(s, \phi, L/K)$ (cf. [Lang70], [Ne91], [L-O77], [L-M-O79]) where ϕ is the character of an irreducible representation of $G = G(L/K)$. We have

$$-\frac{L'}{L}(s, \phi, L/K) = \sum_{\mathfrak{p}} \sum_{m \geq 1} \Phi_K(\mathfrak{p}^m) \log(N\mathfrak{p})(N\mathfrak{p})^{-ms}$$

where

$$\Phi_K(\mathfrak{p}^m) = \frac{1}{e_{\mathfrak{p}}(L/K)} \sum_{\alpha \in I_{\mathfrak{p}}(L/K)} \phi(\tau^m \alpha)$$

where $\tau = \left(\frac{L/K}{\mathfrak{p}}\right)$ is one representative of the Frobenius element corresponding to $\mathfrak{p}$, $I_{\mathfrak{p}} = I_{\mathfrak{p}}(L/K)$ is the inertial subgroup of the decomposition group $G_{\mathfrak{p}} = G(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ and $e_{\mathfrak{p}}(L/K) = |I_{\mathfrak{p}}|$ is the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$.

If $\mathfrak{p}$ is unramified in L then $\Phi_K(\mathfrak{p}^m) = \phi(\alpha^m)$. If L/K is abelian, then all irreducible ϕ are characters.

Lemma 2.6. *Let C be a conjugacy class of G and g a representative of C, $H =< g >$ and $E = L^H$ the fixed field of g. Then we have*

(1)

$$F_C(s) := -\frac{|C|}{|G|} \sum_{\phi \text{ irreducible}} \bar{\phi}(g) \frac{L'}{L}(s, \phi, L/K) = -\frac{|C|}{|G|} \sum_{\chi \in \hat{G}(L/E)} \bar{\phi}(g) \frac{L'}{L}(s, \chi, E)$$

where $\hat{G}(L/E)$ denotes the group of characters of $G(L/E)$, and (2)

$$F_C(s) = \sum_{\mathfrak{p}} \sum_{m \geq 1} \theta(\mathfrak{p}^m) \log(N\mathfrak{p})(N\mathfrak{p})^{-s},$$

where

$$\theta(\mathfrak{p}^m) = \begin{cases} 1 & \text{if } \left(\frac{L/K}{\mathfrak{p}}\right)^m = C \\ 0 & \text{if } \left(\frac{L/K}{\mathfrak{p}}\right)^m \neq C \end{cases}$$

and $|\theta(\mathfrak{p}^m)| \leq 1$ if $\mathfrak{p}$ ramifies in L.

Proof. See Section 5, [L-O77]. □

The previous lemma allows us to reduce the density problem to the case of a cyclic extension, for which we can use just the abelian L–series of Hecke.

The following lemma (cf. [Lang70], [L-O77]) describes a functional equation that $L(s, \chi, E)$ satisfies.

Lemma 2.7. *Let $L(s, \chi) = L(s, \chi, E)$ be the L–series associated to $\chi \in \hat{G}(L/E)$.*

$$A(\chi) = d_E N_{E/\mathbb{Q}}(\mathfrak{f}_0(\chi))$$

where $\mathfrak{f}_0(\chi)$ *denotes the finite conductor of* χ.

$$\delta(\chi) = \begin{cases} 1 & \text{if } \chi \text{ is principal;} \\ 0 & \text{otherwise.} \end{cases}$$

There are nonnegative integers $a = a(\chi)$ *and* $b = b(\chi)$ *such that*

$$a(\chi) + b(\chi) = n_E$$

Set

$$\gamma_\chi(s) = \left\{\pi^{-\frac{s+1}{2}}\Gamma(\frac{s+1}{2})\right\}^b \left\{\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\right\}^a$$

and

$$\Lambda(s,\chi) = (s(s-1))^{\delta(\chi)} A(\chi)^{s/2} \gamma_\chi(s) L(s,\chi)$$

Then $\Lambda(s,\chi)$ *satisfies the functional equation*

$$\Lambda(1-s,\bar{\chi}) = W(\chi)\Lambda(s,\chi)$$

where $W(\chi)$ *is a certain constant of absolute* 1.

Furthermore, $\Lambda(s,\chi)$ *is entire of order* 1 *and does not vanish at* $s = 0$.

□

Let

$$J_j(\chi) \triangleq -\frac{1}{2\pi i}\int_{2-i\infty}^{2+\infty} \frac{L'}{L}(s,\chi) k_j(s) ds$$

and

$$I_j = -\frac{1}{2\pi i}\int_{2-i\infty}^{2+\infty} F_C(s)k_j(s)ds$$

where $F_C(s)$ is defined in Lemma 2.6.

By this lemma, we have

$$I_j = \frac{|C|}{|G|}\sum_{\chi\in\hat{G}(L/E)} \bar{\chi}(g)J_j(\chi) \tag{2-2-1}$$

where g is a representative of C.

We have two ways to express I_j. One way is using the inverse Mellin transform and the other is using the residue theorem.

By the inverse Mellin transform, and we have

$$J_j(\chi) = \sum_{\mathfrak{p}}\sum_{m\geq 1} \chi(\mathfrak{p}^m)\log(N\mathfrak{p})\hat{k}_j(N\mathfrak{p}^m)$$

since

$$-\frac{L'}{L}(s,\chi,E) = \sum_{\mathfrak{p}}\sum_{m\geq 1} \chi(\mathfrak{p}^m)\log(N\mathfrak{p})(N\mathfrak{p})^{-ms}$$

Also, by Lemma 2.6,

$$\begin{aligned} I_j &= \frac{|C|}{|G|}\sum_{\chi\in\hat{G}(L/E)} \bar{\chi}\sum_{\mathfrak{p}}\sum_{m\geq 1} \chi(\mathfrak{p}^m)\log(N\mathfrak{p})\hat{k}_j(N\mathfrak{p}^m) \\ &= \sum_{\mathfrak{p}}\sum_{m\geq 1} \theta(\mathfrak{p}^m)\log(N\mathfrak{p})\hat{k}_j(N\mathfrak{p}^m) \end{aligned}$$

Lemma 2.8. (1)

$$J_j(\chi) = \delta(\chi)k_j(1) - \sum_{\rho} k_j(\rho) + O(n_E k_j(0))$$
$$+ O(k_j(-\frac{1}{2})(\log A(\chi) + n_E))$$

where the sum runs over all the nontrivial zeros of $L(s, \chi, E)$, *and all the implied constants are absolute and effectively computable.*

(2)

$$\frac{|G|}{|C|} I_j \geq k_j(1) - \sum_{\rho} k_j(\rho)$$
$$- c_6\{n_L k_j(0) + k_j(-\frac{1}{2}) \log d_L\}$$

where the sum runs over all the nontrivial zeros of $\zeta_L(s)$ *and* c_6 *is positive, absolute and effectively computable.*

For the proof we need the following

Proposition 2.9. (the Conductor–Discriminant Formula)

$$\prod_{\chi \in \hat{G}(L/E)} A(\chi) = d_L$$

□

For a proof, see [L-O77], [Od77].

Proof of Lemma 2.8.

For (1), see [L-O77]. The basic idea is to consider the following integral

$$J_j(\chi,T) \triangleq -\frac{1}{2\pi i}\int_{\partial B(T)} \frac{L'}{L}(s,\chi,E)k_j(s)ds$$
$$= \delta(\chi)k_j(1) - a_\chi k_j(0) - \sum_{|\gamma|<T} k_j(\rho)$$

where the sum runs over all the zeros $\rho = \beta + i\gamma$ of $L(s,\chi,E)$ within the rectangle $B(T)$: $[-\frac{1}{2},2]\times[-T,T]$. Estimate the integral on each line segment and let T go to the infinity as in [L-O77]. In fact, on the line segment from $-\frac{1}{2}+iT$ to $-\frac{1}{2}-iT$,

$$\left|\frac{L'}{L}(s,\chi,E)\right| << \log A(\chi) + n_E(\log(|s|+2))$$

(see Lemma 6.2, [L-O77]). Thus,

$$\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}-iT}^{-\frac{1}{2}+iT} \frac{L'}{L}(s,\chi E)k_j(s)ds\right| << k_j(-\frac{1}{2})\{\log A(\chi) + n_E\}$$

as

$$k_1(-\frac{1}{2}+it) << k_1(-\frac{1}{2})\frac{1}{1+t^2} \quad \text{if } y >> x$$
$$k_2(-\frac{1}{2}+it) << k_1(-\frac{1}{2})\exp(-t^2\log x) \quad \text{if } x >> 1$$

To estimate the integral $I_\pm(T)$ on the horizontal line segments from $2\pm iT$ to $-\frac{1}{2}\pm iT$, one uses the method of Landau (Section 6 of [L-O77], Section 3 of [L-M-O79], [Land27]), obtaining the estimate

$$I_\pm(T) << k_j(iT)(\log A(\chi) + n_E \log T).$$

Combining these estimates with Proposition 2.9, we obtain (1).

Now (2) is easy to get from (1) since

$$I_j = \frac{|C|}{|G|} \sum_{\chi \in \hat{G}(L/E)} J_j(\chi)$$

and

$$\zeta_L(s) = \prod_{\chi \in \hat{G}(L/E)} L(s, \chi, E)$$

and we can use Proposition 2.9.

□

Now we are ready to explain how we plan to use the standard model for our purposes.

From the rest of this chapter, assume that $y >> x$ if we apply the first kernel function $k_1(s)$ and $x >> 1$ if we apply the second one $k_2(s)$. Let $n = n_L/n_K$ which is not less than $|G|/|C|$.

Thus, by Lemma 2.8 (2), we have

$$I_j \geq \frac{1}{n}(k_j(1) - \sum_{\rho} |k_j(\rho)|) - c_6 \left\{ n_K k_j(0) + k_j(-\frac{1}{2}) \left(\frac{1}{n} \log d_L \right) \right\}$$

Note that

$$k_1(0) = \left(\frac{x^{-1} - y^{-1}}{-1}\right)^2 << x^{-2}$$

$$k_1(-\frac{1}{2}) = \left(\frac{x^{-\frac{3}{2}} - y^{-\frac{3}{2}}}{-\frac{3}{2}}\right)^2 << x^{-3}$$

$$k_2(0) = 1$$

$$k_2(-\frac{1}{2}) = x^{-\frac{1}{4}}$$

Thus, the $c_6\{\ \}$ term is bounded by some multiple of

$$T_j = \begin{cases} \frac{x^{-2}}{n} \log d_L, & \text{if } j = 1; \\ \frac{1}{n} \log d_L, & \text{if } j = 2. \end{cases}$$

Furthermore, we have

$$I_j = \sum_{\mathfrak{p}} \sum_{m \geq 1} \theta(\mathfrak{p}^m) \log(N\mathfrak{p}) \hat{k}_j(N\mathfrak{p}^m)$$

Thus,

$$I_1 = S_{1,1} + S_{1,2} + S_{1,3} + \tilde{I}_1$$

$$I_2 = S_{2,1} + S_{2,2} + S_{2,3} + S_{2,4} + \tilde{I}_2$$

where the symbols mean the following:

$\tilde{I}_j$ denotes the sum over the primes outside S, unramifying in L, of degree 1 over K and the Artin symbol of $\mathfrak{p}$ under L/K being C such that $N\mathfrak{p} \leq y^2$ or $x^{3+\delta}$ when $j = 1$ or 2 respectively.

$S_{1,1}$ denotes the sum over $(\mathfrak{p}, m)$ with $\mathfrak{p}$ ramifying in L. $S_{2,1}$ denotes the sum over $(\mathfrak{p}, m)$ with $\mathfrak{p}$ ramifying in L and $N\mathfrak{p}^m \leq x^{10}$.

$S_{1,2}$ denotes the sum over $(\mathfrak{p}, m)$ with $\mathfrak{p}$ in S. $S_{2,2}$ denotes the sum over $(\mathfrak{p}, m)$ with $\mathfrak{p}$ in S and $N\mathfrak{p}^m \leq x^{10}$.

$S_{j,3}$ denotes the sum over $(\mathfrak{p}, m)$ with $N\mathfrak{p}^m$ not a rational prime.

$S_{2,4}$ denotes the sum over $(\mathfrak{p}, m)$ with $N\mathfrak{p}^m > x^{3+\delta}$.

Applying Lemma 2.1, we have

$$S_{1,1} << \frac{1}{n}\frac{\log(y/x)}{x^2}\log d_L$$

$$S_{2,1} << \frac{1}{n}(\log x)^{\frac{1}{2}}\log d_L$$

$$S_{1,2} << \frac{\log(y/x)}{x^2}\log N_S$$

$$S_{2,2} << (\log x)^{\frac{1}{2}}\log N_S$$

$$S_{1,3} << n_K\frac{(\log(y/x))(\log y)}{x(\log x)}$$

$$S_{2,3} << n_K x^{7/4}$$

$$S_{2,4} << n_K x^{2-\frac{\delta^2}{4}}\log x$$

Then the main idea of this model is the following: Pick x, y appropriately. If we assume that for any $\mathfrak{p}$ unramifying in L, of degree 1 over K and the Artin symbol of $\mathfrak{p}$ under L/K being C such that either $N\mathfrak{p} > y^2$ or $x^{3+\delta}$ when $j = 1$ or 2 respectively, or $\mathfrak{p} \in S$ or $\mathfrak{p}$ ramifies in L, then $\tilde{I}_j = 0$ and

$$\frac{1}{n}\left(k_j(1) - \sum_{\rho}|k_j(\rho)|\right) \leq c_6' T_j + \sum_{v} S_{j,v}$$

However, if the left–hand side dominates over $c_6' T_j$ and $S_{j,v}$ by a sufficiently large constant factor, then one gets a contradiction.

So the key component of this model is to find a better lower bound for

$$k_j(1) - \sum_{\rho} |k_j(\rho)|$$

2.3 Proof of Theorem 2–C.

In this part we will prove Theorem 2–C. Let $P_1(C, S)$ be the set of primes of K satisfying (1) to (3) in Theorem 2–C.

From last section we've already seen that the quality of the effective bound depends on the lower bound of $k_j(1) - \sum_{\rho} |k_j(\rho)|$. However, the possible exceptional zero β_0 will cause difficulty. In general, one will be forced to use the Deuring–Heilbronn. Fortunately, there is nothing new here compared with the classical case where $S = \emptyset$.

To simplify our notation, we define β_0 to be the exceptional zero of $\zeta_L(s)$ if it exists, and $\beta_0 = 1 - (c_2 \log d_L)^{-1}$ otherwise, where c_2 is the constant defined in Lemma 2.3, so that $\zeta_L(s)$ has at most one zero in the interval $(1 - (c_2 \log d_L)^{-1}, 1)$.

In either case,

$$k_j(1) - \sum_{\rho} |k_j(\rho)| \geq k_j(1) - k_j(\beta_0) - \sum_{\rho \neq \beta_0} |k_j(\rho)|$$

By using the mean value theorem, we have

$$\begin{aligned} k_1(1) - k_1(\beta_0) &= \left(\log \frac{y}{x}\right)^2 - \left(\frac{y^{\beta_0-1} - x^{\beta_0-1}}{\beta_0 - 1}\right)^2 \\ &\geq \frac{1}{10}\left(\log \frac{y}{x}\right)^2 \min\left\{1, (1-\beta_0)\log \frac{y}{x}\right\} \\ k_2(1) - k_2(\beta_0) &= x^2 - x^{\beta_0+\beta_0{}^2} \geq \frac{x^2}{10} \min\left\{1, (1-\beta_0)\log \frac{y}{x}\right\} \end{aligned}$$

First suppose

$$1 - \beta_0 \geq {c_7}^2 (\log d_L 3^{n_L})^2$$

where c_7 is the constant defined in Lemma 2.4. In this case, we use the kernel $k_1(s)$.

The contribution of the zeros ρ of $\zeta_L(s)$ with $|\rho - 1| \geq 1$ is bounded by

$$\sum_{|\rho-1|\geq 1} |k_1(\rho)| \leq \int_1^\infty \frac{2}{t^2} dn(t;1) << \log d_L$$

where $n(t;1)$ is the number of the nontrivial zeros of ζ_L with $|\rho - 1| \geq t$ (See Lemma 2.2).

Next, assume that $|\rho - 1| \leq 1$ for a nontrivial zero $\rho = \beta + i\gamma \neq \beta_0$ of ζ_L.

If β_0 as an exceptional zero exists with

$$1 - \beta_0 \leq \frac{1}{18} c_2 {c_7}^2 (\log d_L)^{-1},$$

then since $d_L \geq 3^{n_L/2}$ for $n_L \geq 2$, we have

$$\frac{c_7}{(1-\beta_0)\log(d_L 3^{n_L})} \geq \left\{(\frac{1}{2}c_2)(1-\beta_0)\log d_L\right\}^{-\frac{1}{2}},$$

and therefore by the Deuring–Heilbronn (Lemma 2.4)

$$\beta \leq 1 - c_8 \frac{\log\left\{\frac{c_7}{(1-\beta_0)\log(d_L 3^{n_L})}\right\}}{\log(d_L 3^{n_L})} \leq 1 - c_{11}\frac{\log\left\{(\frac{1}{2}c_2)(1-\beta_0)\log d_L\right\}^{-1}}{\log d_L}$$

On the other hand, if

$$1 - \beta_0 \geq \frac{1}{18} c_2 {c_7}^2 (\log d_L)^{-1}$$

then by the zero–free region given by Lemma 2.3,

$$\beta \leq (3c_2 \log d_L)^{-1}$$

Hence we have

$$\beta \leq 1 - c_{12}\frac{\log\left\{(\frac{1}{2}c_2)(1-\beta_0)\log d_L\right\}^{-1}}{\log d_L} \qquad (*)$$

for some $0 < c_{12} < c_{11}$.

Thus (*) holds for all the cases.

Let

$$B = c_{12}\frac{\log\left\{(\frac{1}{2}c_2)(1-\beta_0)\log d_L\right\}^{-1}}{\log d_L}$$

From (*), we have

$$|k_1(\rho)| << x^{2(\beta-1)}|\rho - 1|^{-2} << x^{-2B}|\rho - 1|^{-2}$$

Thus, by Lemma 2.2,

$$\sum_{|\rho-1|<1,\rho\neq\beta_0} |k_1(\rho)| \leq x^{-2B}\int_B^1 \frac{1}{t^2}dn(t;1)$$

$$<< x^{-2B}(B^{-2}+B^{-1}\log d_L)$$

$$<< x^{-2B}B^{-1}\log d_L$$

As $B >> (\log d_L)^{-1}$, using the expression of B, we have

$$\sum_{|\rho-1|<1,\rho\neq\beta_0} |k_1(\rho)| << (\log d_L)^2\left\{(\frac{1}{2}c_2)(1-\beta_0)\log d_L\right\}^{2c_{12}\frac{\log x}{\log d_L}}$$

Thus we have shown that

$$k_1(1)-\sum_\rho |k_1(\rho)| \geq \frac{1}{10}\Big(\log\frac{y}{x}\Big)^2 \min\Big\{1,(1-\beta_0)\log\frac{y}{x}\Big\} \qquad \text{(4A-1)}$$

$$-c_{13}\log d_L$$

$$-c_{14}(\log d_L)^2\left\{(\frac{1}{2}c_2)(1-\beta_0)\log d_L\right\}^{2c_{12}\frac{\log x}{\log d_L}}$$

for some positive constants c_{13} and c_{14}.

We now complete the proof of Theorem 2–C in the case

$$1-\beta_0 \geq {c_7}^2(\log d_L 3^{n_L})^2.$$

Assume that for any $\mathfrak{p}$ in $P_1(C,S)$, $N\mathfrak{p} > y^2$. Then

$$
\begin{aligned}
0 = \tilde{I}_1 &= \sum_{\mathfrak{p}\in P_1(C,S)} (\log N\mathfrak{p})\hat{k}_1(N\mathfrak{p}) \\
&\geq \frac{1}{10n}\Big(\log\frac{y}{x}\Big)^2 \min\Big\{1, (1-\beta_0)\log\frac{y}{x}\Big\} \\
&- c_{13}\frac{1}{n}\log d_L \\
&- c_{14}\frac{1}{n}(\log d_L)^2\Big\{(\frac{1}{2}c_2)(1-\beta_0)\log d_L\Big\}^{2c_{12}\frac{\log x}{\log d_L}} \\
&- c_{15,1}\left\{\frac{1}{n}\frac{1}{x^2}\log\left(\frac{y}{x}\right)\log d_L\right\} \\
&- c_{15,2}\left\{\frac{1}{x^2}\log\left(\frac{y}{x}\right)\log N_S\right\} \\
&- c_{15,3}\left\{n_K\frac{\left(\log\frac{y}{x}\right)(\log y)}{x\log x}\right\} \\
&- c_6'\frac{x^{-2}}{n}\log d_L
\end{aligned}
$$

where $c_{15,v}\{\dots\}$ comes from $S_{1,v}$ and $c_6'\{\dots\}$ comes from T_1.

Fix any positive constant ϵ, and set $y = x^{1+\epsilon}$, $x = {d_L}^{C(\epsilon)}(1+n\log N_S)^{\frac{1+\epsilon}{2}}$ for sufficiently large $C(\epsilon)$, one gets that the first term dominates over the other terms by a large constant factor. Let us check this.

The $c_{14}\{\dots\}$ term is bounded by some multiple of

$$\frac{1}{n}(\log d_L)^2 4^{-c_{12}C(\epsilon)} = o\left(\frac{(\log x)^2}{n}\right)$$

as $C(\epsilon)$ goes to ∞, thus it is dominated over by $\frac{1}{n}\big(\log\frac{y}{x}\big)^2$ by a large constant factor. Also, this term is bounded by some multiple of

$$\frac{1}{n}(\log d_L)^2 4^{1-c_{12}C(\epsilon)}\cdot(1-\beta_0)\log d_L$$

which is $o(\frac{(\log x)^3}{n}(1-\beta_0))$ as $C(\epsilon)$ goes to ∞, thus it is dominated over by $\frac{1}{n}\left(\log \frac{y}{x}\right)^3(1-\beta_0)$ by a large constant factor. From the discussion above one can verify this assertion for the $c_{14}\{\dots\}$ term.

Since

$$\frac{1}{x^2}\log\frac{y}{x}\log N_S << \frac{1}{d_L^{2C(\epsilon)}}\log\frac{y}{x} << \frac{1}{n}\log\frac{y}{x}$$

thus one can verify this assertion for the $c_{15,2}\{\dots\}$ term.

Other terms are easy to check. So one draws a contradiction, and we get Theorem 2–C in this case.

Furthermore, we consider the case

$$1-\beta_0 \le {c_7}^2(\log d_L 3^{n_L})^{-2},$$

where we will use the second kernel function $k_2(s)$. In this case

$$\log\frac{c_7}{(1-\beta_0)\log d_L 3^{n_L}} \ge \frac{1}{2}\log(1-\beta_0)^{-1}$$

If $\rho = \beta + i\gamma$ is a zero of $\zeta_L(s)$ with $|\gamma| \le 1$, and $\rho \ne \beta_0$, then by the Deuring–Heilbronn,

$$\begin{aligned}|k_2(\rho)| &<< x^{\beta^2+\beta} << x^{1+\beta}\\ &= x^2\exp\left\{-c_{19}\frac{\log x\log(1-\beta_0)^{-1}}{\log d_L}\right\}x^2(1-\beta_0)^{c_{19}\frac{\log x}{\log d_L}}\end{aligned}$$

for some positive absolute constant c_{19}. Thus

$$\sum_{|\gamma|\leq 1, \rho\neq\beta_0} |k_2(\rho)| << x^2(1-\beta_0)^{c_{19}\frac{\log x}{\log d_L}} \log d_L$$

If $\rho = \beta + i\gamma$ is a zero of $\zeta_L(s)$ with $|\gamma| \geq 1$, and $\rho \neq \beta_0$, we have

$$|k_2(\rho)| \leq x^{2-\gamma^2} << x$$

Thus assume $x > 2$. Applying Lemma 2.2, we have

$$\begin{aligned}\sum_{|\gamma|>1} |k_2(\rho)| &<< \sum_{n\geq 1} N(|2n|)\, x^{1+4n-4n^2} \\ &<< x \log d_L \sum_{n\geq 1} 2^{4n-4n^2} + x\, n_L \sum_{n\geq 1} 2^{4n-4n^2} \log(2n+1) \\ &<< x \log d_L\end{aligned}$$

where $N(T)$ is the number of zeros of $\zeta_L(s)$ in the region $[0,1]\times[T-1, T+1]$.

Thus

$$\begin{aligned}k_2(1) - \sum_{\rho} k_2(\rho) \geq \frac{x^2}{10} \min\{1, (1-\beta_0)\log x\} \\ - c_{20} x \log d_L - c_{21} x^2 (1-\beta_0)^{c_{19}\frac{\log x}{\log d_L}} \cdot \log d_L\end{aligned} \tag{4A-2}$$

for some absolute positive constants c_{20} and c_{21}.

We now complete the proof of Theorem 2–C in the case

$$1 - \beta_0 \leq {c_7}^2 (\log d_L 3^{n_L})^2.$$

Assume that for any $\mathfrak{p}$ in $P_1(C,S)$, $N\mathfrak{p} > x^{3+\delta}$. Then

$$
\begin{aligned}
0 = \tilde{I}_2 = & \sum_{\mathfrak{p}\in P_1(C,S), N\mathfrak{p}\le x^{3+\delta}} (\log N\mathfrak{p})\hat{k}_2(N\mathfrak{p}) \\
& \geq \frac{x^2}{10n}\min\{1,(1-\beta_0)\log x\} \\
& - c_{20}\frac{1}{n}\log d_L \\
& - c_{21}\frac{1}{n}x^2(1-\beta_0)^{c_{19}\frac{\log x}{\log d_L}}\cdot\log d_L \\
& - c_{22,1}\left\{\frac{1}{n}(\log x)^{\frac{1}{2}}\log d_L\right\} \\
& - c_{22,2}\left\{(\log x)^{\frac{1}{2}}\log N_S\right\} \\
& - c_{22,3}\left\{n_K x^{\frac{7}{4}}\right\} \\
& - c_{22,4}\left\{n_K x^{2-\frac{\delta^2}{4}}(\log x)\right\} \\
& - c_6'\log d_L
\end{aligned}
$$

where $c_{22,v}\{\dots\}$ comes from $S_{2,v}$ and $c_6'\{\dots\}$ comes from T_1.

Fix any positive constant ϵ', and set $x = {d_L}^{C(\epsilon')}(1+n\log N_S)^{\frac{1+\epsilon'}{2}}$ for sufficiently large $C(\epsilon)$. One gets that the first term dominates over the other terms by a large constant factor. Let us check this.

First be aware that by the Deuring–Heilbronn (Corollary 2.5), and the fact that $d_L^{\varepsilon} >> \log d_L >> n_L$ for any $\varepsilon > 0$, the first term dominates over $n_K x^{2-\alpha}$ for $C(\epsilon')$ sufficiently large for any $\alpha > 0$.

The $c_{21}\{\dots\}$ term is bounded by some multiple of

$$\frac{1}{n}x^2(1-\beta_0)^{c_{19}C(\epsilon')}\log d_L$$

as $C(\epsilon)$ goes to ∞, and thus it is dominated over by the first term.

Since

$$(\log x)^2 \log N_S << x^{\frac{2}{1+\epsilon'}}$$

thus one can verify this assertion for the $c_{22,2}\{\dots\}$ term.

Other terms are easy to check now. So one draws a contradiction, and we prove Theorem 2–C in this case.

2.4 Computations of $B_l(K(\zeta_{l^r}), \tilde{S})$ and $C_{l^r(K,S)}$

In this part, we will apply Theorem 2–C to compute two types of constants we will need in Chapter 5.

Let l^r be a prime power, K a number field, S a finite set of (finite) primes, $\tilde{S}$ the set of primes of $K_1 = K(\zeta_{l^r})$ over the primes in S. It is easy to check that $N_{\tilde{S}} = N_S^{[K_1:K]}$.

If $\zeta_l \in K$,

$$B_l(K,S,\alpha) := \begin{cases} \text{the least bound for } N\mathfrak{q} \text{ such that} \\ \text{(i) } \mathfrak{q} \text{ a prime of } K \text{ not splitting in } K(\sqrt[l]{\alpha}); \\ \text{(ii) } \mathfrak{q} \nmid l \text{ and } \mathfrak{q} \notin S. \end{cases}$$

$$B_l(K,S) := \max_{\alpha \in K^S, \alpha \notin (K^S)^l} B_l(K,S,\alpha).$$

The next symbol has multiple meaning:

If $K(\zeta_{l^r})/K$ is cyclic, then

$$C_{l^r}(K,S) := \begin{cases} \text{the least bound for } N\mathfrak{q} \text{ such that} \\ \text{(i) } \mathfrak{q}, \text{ a prime of } K \text{ inert in } K(\zeta_{p^r}); \\ \text{(ii) } \mathfrak{q} \nmid p \text{ and } \mathfrak{q} \notin S. \end{cases}$$

If $K(\zeta_{l^r})/K$ is not cyclic, so that $l = 2$ and $r \geq 3$.

$$C_{2^r}(K,S) := \begin{cases} \text{the least bound for } N\mathfrak{q}' \text{ such that} \\ \text{(i) } \mathfrak{q}', \text{ a prime of } K_1 = K(\sqrt{-1}) \text{ inert in } K(\zeta_{2^r}); \\ \text{(ii) } \mathfrak{q}' \nmid 2 \text{ and } \mathfrak{q}' \notin S' \text{ while } S' = \{\, \mathfrak{p}' \mid \mathfrak{p} \in S \,\}. \end{cases}$$

Now we explain how we apply Theorem 2–C to calculate these quantities.

(1) Calculation of $B_l(K(\zeta_{l^r}), \tilde{S})$.

Set $K_1 = K(\zeta_{l^r})$, it is easy to check that $d_{K_1} = {d_K}^{[K_1:K]} d_{K_1/K}$ where the relative discriminant $d_{K_1/K}$ divides ${l^r}^{[K_1:K]n_K}$. This is because l^r belongs to the relative different $\mathcal{D}_{K_1/K}$.

For any $\alpha \in K_1^{\tilde{S}} - {K_1^{\tilde{S}}}^l$, we consider $L_1 = K_1(\sqrt[l]{\alpha})$. Without loss of generality, one may assume that $\alpha \in \mathcal{O}_{K_1}$ and $0 \leq v_{\tilde{\mathfrak{p}}}(\alpha) \leq l-1$ for each $\tilde{\mathfrak{p}} \in \tilde{S}$.

Let $\tilde{T}_1$ be the set of primes $\tilde{\mathfrak{p}}$ dividing α, $\tilde{T}_2 = \tilde{S} - \tilde{T}_1$. Also, we denote $\tilde{T}_0$ as the set of primes of K_1 dividing l which does not ramify in $L_1 = K_1(\sqrt[l]{\alpha})$.

Lemma 2.10.

$$d_{L_1/K_1} N_{\tilde{T}_0}^l \quad \text{divides} \quad {l^{n_K l[K_1:K]}} {N_{\tilde{T}_1}}^{l-1}$$

Proof.

Let $\pi = \pi_{\tilde{\mathfrak{p}}}$ be a uniformizer of the local field $(K_1)_{\tilde{\mathfrak{p}}}$ for any $\tilde{\mathfrak{p}} \in \tilde{T}_1$. Thus

there exists integers m_1 and m_2 with $-m_1 l + m_2 v_{\tilde{\mathfrak{p}}}(\alpha) = 1$. So $v_{\tilde{\mathfrak{p}}}(\pi^{-m_1 l}\alpha^{m_2}) = 1$.

Let $\alpha' = \pi^{-m_1 l}\alpha^{m_2}$, then $L_1 = K_1(\sqrt[l]{\alpha'})$. Let ω be the (finite) prime of L_1 over $\tilde{\mathfrak{p}}$. Then $\mathcal{D}_{(L_1)_\omega/(K_1)_{\tilde{\mathfrak{p}}}}$ contains $l\omega^{l-1}$. Thus $\mathcal{D}_{L_1/K_1}$ divides $(l)\prod_{\tilde{\mathfrak{p}}\in\tilde{T}_1}\omega^{l-1}$.

Since each prime in $\tilde{T}_0$ is unramified in L_1, we have $\mathcal{D}_{L_1/K_1}\prod_{\mathfrak{p}'\in\tilde{T}_0}(\mathfrak{p}')$ divides $(l)\prod_{\tilde{\mathfrak{p}}\in\tilde{T}_1}\omega^{l-1}$.

Thus $d_{L_1/K_1}{N_{\tilde{T}_0}}^l$ divides $l^{l[K_1:K]n_K}{N_{\tilde{T}_1}}^{l-1}$. □

Since all primes in $\tilde{T}_1$ ramify in L_1, so applying Theorem 2–C, we have

$$\begin{aligned} B_l(K_1,\tilde{S},\alpha) &= B_l(K_1,\tilde{T}_2\cup\tilde{T}_0,\alpha) \\ &\le \left({N_{\tilde{T}_0}}^{-l}{d_{K_1}}^l l^{n_K l[K_1:K]}{N_{\tilde{T}_1}}^{l-1}\right)^{A_2}(1+l\log N_{\tilde{T}_2}+l\log N_{\tilde{T}_0})^2 \\ &\le \left({d_{K_1}}^l l^{n_K l[K_1:K]}{N_{\tilde{S}}}^{l-1}\right)^{A_2} \end{aligned}$$

while the last inequality holds since we can choose $A_2 > 2$.

Thus

$$\begin{aligned} B_l(K_1,\tilde{S}) &\le \left({d_{K_1}}^l l^{l n_{K_1}}{N_{\tilde{S}}}^{l-1}\right)^{A_2} \\ &\le \left({d_K}^l l^{l(1+r)n_K}{N_S}^{l-1}\right)^{A_2[K_1:K]} \end{aligned} \tag{2-4-1}$$

(2) Calculation of $C_{l^r}(K,S)$.

First, if K_1/K is not cyclic and $l=2$, $r\ge 3$, then assume $\mathfrak{p}$ is the rational prime of K whose lift in $K(i)$ is inert in K_1 and of degree 1 over $\mathbb{Q}$, then $\mathfrak{p}$ is also of degree 1 over $\mathbb{Q}$. Also, let $\eta = \zeta_{2^r} + \zeta_{2^r}^{-1}$. Then $K_1 = K(\eta)K(i)$ and $K(\eta)\cap K(i) = K$, and thus $Gal(K_1/K) \cong Gal(K_1/K(i)) \times \mathbb{Z}/2\mathbb{Z} \cong$

$Gal(K(\eta)/K) \times \mathbb{Z}/2\mathbb{Z}$. Thus if the lift of $\mathfrak{p}$ in $K(i)$ is inert in K_1, then $\mathfrak{p}$ is inert in $K(\eta)$ and $\left(\frac{K_1/K}{\mathfrak{p}}\right) = \sigma$ for some generator σ of $G(K_1/K(i))$. Conversely, if $\left(\frac{K_1/K}{\mathfrak{p}}\right) = \sigma$ for some generator σ of $G(K_1/K(i))$, and $\mathfrak{p}$ is of degree 1 over $\mathbb{Q}$, then the lift of $\mathfrak{p}$ in $K(i)$ is inert in K_1, and it is of degree 1 over $\mathbb{Q}$.

Note that every prime of K dividing l is totally ramified in K_1, so that we may apply Theorem 2–C in all cases to get

$$\begin{aligned} C_{l^r}(K,S) &\leq (d_K\, l^{r\, n_K})^{A_2[K_1:K]}(1 + [K_1 : K] \log N_S)^2 \qquad (2\text{-}4\text{-}2) \\ &\leq (d_K\, l^{r\, n_K}\, N_S)^{A_2[K_1:K]} \end{aligned}$$

where we have used the identity $d_{K_1} = (d_K\, l^{r\, n_K})^{[K_1:K]}$.

Chapter 3 Quadratic Dirichlet Characters

This chapter is to solve the Grunwald's problem in the case $K = \mathbb{Q}$ and $m = l = 2$.

As $\mathbb{Q} \supseteq \mu_2 = \{ \pm 1 \}$, each quadratic extension over $\mathbb{Q}$ is a Kummer extension.

Note that if $m = 2$, **Problem I** and **Problem II** described in Section 0.2 are equivalent.

3.1 Main Results of This Chapter

Question Z Let $S = \{ p_1, p_2, \ldots, p_M \}$ be a finite set of finite primes.

Find α, such that $p_1, p_2, \ldots, p_M \nmid \alpha$, and 4 divides $\alpha - 1$ if $p_i = 2$ for some i, and

$$\left(\frac{\alpha}{p_i} \right) = (-1)^{\epsilon_i}$$

$\epsilon_i = 0$ or 1 given.

Define $\left(\frac{\alpha}{2} \right) = (-1)^{\frac{\alpha^2 - 1}{2}}$ be the quadratic residue symbol of α in $\mathbb{Q}_2$,

Thus

$$\left(\frac{\alpha}{2} \right) = \begin{cases} 1 & \text{if } \alpha \equiv 1 \pmod 8 \\ -1 & \text{if } \alpha \equiv 5 \pmod 8 \end{cases}$$

Also find the least bound of such $|\alpha|$.

Remark: $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ is unramified at p_i iff $p_i \nmid \alpha$ (for odd p_i) or $4|\alpha - 1$ (for $p_i = 2$).

Answer: We can find this α such that

(1) $\alpha \gneqq 0$,

$|\alpha| \leqq 4N_S$ if $2 \in S$, $|\alpha| \leqq N_S$ if $2 \notin S$;

(2) $\alpha \lneqq 0$,

$|\alpha| \leqq 4N_S$ if $2 \in S$, $|\alpha| \leqq N_S$ if $2 \notin S$;

(3) any sign for α,

$|\alpha| \leqq 2N_S$ if $2 \in S$, $|\alpha| \leqq N_S/2$ if $2 \notin S$;

where $N_S := \prod_{p \in S} Np$, define $N\infty = 2$.

Lemma 3.1. (1) *Let L_1 and L_2 are finite extensions over $\mathbb{Q}$, $L_1 \cap L_2 = \mathbb{Q}$ and $L = L_1 L_2$. Then the discriminant of L satisfying*

$$d_L \leqq {d_{L_1}}^{n_{L_2}} {d_{L_2}}^{n_{L_1}}$$

and

$$\frac{\log_2 d_L}{n_L} \leqq \frac{\log_2 d_{L_1}}{n_{L_1}} + \frac{\log_2 d_{L_2}}{n_{L_2}}$$

where $n_K = [K : \mathbb{Q}]$.

(2) *Let L_1, L_2, ... and L_s are finite extensions over $\mathbb{Q}$, and $L_i \cap L_1 \cdots \hat{L_i} \cdot L_s = \mathbb{Q}$ and $L = L_1 \cdots L_s$. Then*

$$\frac{\log_2 d_L}{n_L} \leqq \sum_{i=1}^{s} \frac{\log_2 d_{L_i}}{n_{L_i}}.$$

Remark. In fact, if $L_1 \cap L_2 = K$, then we can prove

$$(d_{L/K}) \quad \text{divides} \quad (d_{L_1/K})^{n_{L_2/K}} (d_{L_2/K})^{n_{L_1/K}}$$

where $(d_{L/K}) = N_{L/K}\mathcal{D}_{L/K}$ = the ideal of $\mathcal{O}_L$ generated by $Disc_{L/K}(V)$ for all free $\mathcal{O}_K$-submodule V in $\mathcal{O}_L$.

Proposition 3.2. *Let d is a square free integer. Let $D = d$ if $d \equiv 1 \pmod 4$, $4d$ if $d \equiv 2, 3 \pmod 4$ be the discriminant of $\mathbb{Q}(\sqrt{d})$. If $\chi_{\mathbb{Q},d}$ be the quadratic character corresponding to $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, then*

$$\mathfrak{f}_\chi = \begin{cases} |D| & \text{if } d > 0 \\ |D|\infty & \text{if } d < 0 \end{cases}$$

and

$$N(\chi) = N\mathfrak{f}_\chi = \begin{cases} |D| & \text{if } d > 0 \\ 2|D| & \text{if } d < 0 \end{cases}$$

Proposition 3.3. *For $m = 2$, $K = \mathbb{Q}$, all χ_v for $v \in S$ finite, are unramified, then*

$$\textbf{\textit{BP1}}, \textbf{\textit{BP2}} \leqq \begin{cases} 2N_S & \text{(if } \infty \in S, \ \chi_\infty \text{ is trivial;)} \\ 4N_S & \text{(if } \infty \notin S \text{ or } \infty \in S, \ \chi_\infty \text{ is nontrivial.)} \end{cases}$$

Proposition 3.4 (Ramified Factors).

$$N(\chi_{\mathbb{Q},p}) = \begin{cases} p & \text{if } p \equiv 1 \pmod 4 \\ 4p & \text{if } p \equiv 3 \pmod 4 \end{cases} \tag{i}$$

$$\mathfrak{f}_{\chi_{\mathbb{Q},p}} = \begin{cases} p & \text{if } p \equiv 1 \pmod 4 \\ 4p & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$$N(\chi_{\mathbb{Q},-p}) = \begin{cases} 2p & \text{if } p \equiv 1 \pmod 4 \\ 8p & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$$\mathfrak{f}_{\chi_{\mathbb{Q},-p}} = \begin{cases} p\infty & \text{if } p \equiv 1 \pmod 4 \\ 4p\infty & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$$N(\chi_{\mathbb{Q},2}) = 8 \qquad \mathfrak{f}_{\chi_{\mathbb{Q},2}} = 8 \tag{ii}$$

$$N(\chi_{\mathbb{Q},-1}) = 8 \qquad \mathfrak{f}_{\chi_{\mathbb{Q},-1}} = 4 \cdot \infty$$

$$N(\chi_{\mathbb{Q},-2}) = 16 \qquad \mathfrak{f}_{\chi_{\mathbb{Q},-2}} = 8 \cdot \infty$$

Proof. This can be easily verify. □

Lemma 3.5. (Reduction to the unramified case)

(1) *Given any quadratic character on* $\mathbb{Q}_2^\times$, *one can select one of* $\lambda = \pm 1$ *or* ± 2 *such that* $\chi_{\mathbb{Q}_2,\lambda}|_{\mathcal{U}_{\mathbb{Q}_2}}$ *agrees with this character on* $\mathcal{U}_{\mathbb{Q}_2}$.

(2) *For* ***Problem I****,* $m = 2$ *and* $K = \mathbb{Q}$, *the following way is used to find a global quadratic (or trivial)* χ_1 *such that* $\chi_1|_p = \chi_p$.

Let $(\chi^*)_p$ *be a local character defined as below:*

$$(\chi^*)_p = \begin{cases} \chi_{\mathbb{Q},p} & \text{if } p \equiv 1 \pmod 4 \\ \chi_{\mathbb{Q},-p} & \text{if } p \equiv -1 \pmod 4 \\ \chi_{\mathbb{Q},\lambda} & \text{if } p = 2 \end{cases}$$

while $\chi_{\mathbb{Q}_2,\lambda}|_{U_{\mathbb{Q}_2}} = (\chi^*)_2|_{U_{\mathbb{Q}_2}}$.

Then let

$$\chi_0 = \prod_{\substack{p\nmid\infty, p\in S \\ \chi_p \text{ ramified}}} (\chi^*)_p$$

then $\chi_p \cdot \chi_0|_p^{-1}$ *are unramified for all finite* $p \in S$.

Thus the ***Problem I*** *is reduced to the problem:* $(m = 2, K = \mathbb{Q})$, *find* $\tilde{\chi}$ *such that* $\tilde{\chi}_p = \chi_p \cdot \chi_0|_p^{-1}$ *for all finite* $p \in S$.

Thus $\chi_1 = \tilde{\chi} \cdot \chi_0$ *is a solution, and* $\chi_1|_p = \chi_p$ *for all* $p \in S$.

(3) *If* $\infty \in S$ *and* $2 \notin S$, *the following way is used to find a global quadratic (or trivial)* χ_1 *such that* $\chi_1|_p = \chi_p$.

Let $(\chi^*)_p$ *be a local character defined as below:*

$$(\chi^*)_p = \begin{cases} \chi_{\mathbb{Q},p} & \text{if } p \text{ is odd} \\ \chi_{\mathbb{Q},-1} & \text{if } p = \infty \end{cases}$$

Then let

$$\chi_0 = \prod_{\substack{p\nmid\infty, p\in S \\ \chi_p \text{ramified}}} (\chi^*)_p$$

then $chi_p \cdot \chi_0|_p^{-1}$ *are unramified for all finite* $p \in S$.

Thus the ***Problem I*** *is reduced to the problem:* $(m = 2, K = \mathbb{Q})$, *find* $\tilde{\chi}$ *such that* $\tilde{\chi}_p = \chi_p \cdot \chi_0|_p^{-1}$ *for all finite* $p \in S$.

Thus $\chi_1 = \tilde{\chi} \cdot \chi_0$ *is a solution, and* $\chi_1|_p = \chi_p$ *for all* $p \in S$.

Proposition 3.6. $m = 2$ *and* $K = \mathbb{Q}$, *then*

$$\textbf{\textit{BP1}}, \textbf{\textit{BP2}} << CN_S \cdot \prod_p N(\chi_p)$$

$C = 2$ *if* $\infty \in S$; $C = 4$ *if* $\infty \notin S$.

This is Theorem A.

For $\#S = 1$, $S = \{p\}$, p a finite prime, a stronger version of Prop 3.6 holds.

Proposition 3.7. *If* p *is a rational prime,* $S = \{p\}$, $m = 2$, $K = \mathbb{Q}$, *then*

$$\textbf{\textit{BP1}}, \textbf{\textit{BP2}} \leqq \begin{cases} N(\chi_p)(p+3) & \text{if } p \equiv 1 \pmod 4; \\ 8N(\chi_p) & \text{if } p \equiv 3 \pmod 4; \\ 10N(\chi_p) & \text{if } p = 2. \end{cases}$$

This is Theorem B.

Remark. (1) Proof of Prop 3.7, using a varied version of Prop 3.3, for $S = \{p\}$ will be given.

Also, we can list out all representatives of global characters, when localized at a given prime, we get a given local character.

Remark. (2) From Table 3.1, Prop 3.7 can be justified to

$$\mathbf{BP1}, \mathbf{BP2} \leqq N(\chi_p)(p+3), \quad \text{if } p \equiv 1 \pmod 4;$$

$$\mathbf{BP1}, \mathbf{BP2} \leqq 8N(\chi_p) \qquad \text{if } p \equiv 3 \pmod 4.$$

3.2 Proofs

Proof of the Question Z

Select α such that $\alpha \equiv u_i \pmod{p_i}$ for odd p_i, where $\left(\frac{u_i}{p_i}\right) = (-1)^{\epsilon_i}$ for some $u_i \in (\mathbb{Z}/p_i\mathbb{Z})^\times$,

$\alpha \equiv v_i \pmod 8$ for $p_i = 2$,

$v_i = 1$ if $\epsilon_i = 0$, $v_i = 5$ if $\epsilon_i = 1$.

Then we can find

$$\begin{aligned}
\text{Such } \alpha \gneqq 0, \text{ and } |\alpha| &\leqq 4N_S && \text{if } 2 \in S,\\
|\alpha| &\leqq N_S && \text{if } 2 \notin S;\\
\text{Such } \alpha \lneqq 0, \text{ and } |\alpha| &\leqq 4N_S && \text{if } 2 \in S,\\
|\alpha| &\leqq N_S && \text{if } 2 \notin S;\\
\text{Such } \alpha, \text{ and } |\alpha| &\leqq 2N_S && \text{if } 2 \in S,\\
|\alpha| &\leqq N_S/2 && \text{if } 2 \notin S.
\end{aligned}$$

□

Proof of Lemma 3.1. We prove a stronger version. Also see [Lang70].

p	Representatives			localized at p
	$L = \mathbb{Q}(\sqrt{d})$	D	$N(\chi)$	
$p \equiv 3 \pmod 4$	$\mathbb{Q}$	1	1	splits
	$\mathbb{Q}(\sqrt{-d'})$ $1 \leqq d' \leqq \frac{p+1}{2}$ d' not a square mod p	d' or $4d'$	$2d'$ or $8d'$	
	$\mathbb{Q}(\sqrt{-1})$	4	8	unram., inert
	$\mathbb{Q}(\sqrt{d'})$ $1 \leqq d' \leqq \frac{p+1}{2}$ d' not a square mod p	d' or $4d'$	d' or $4d'$	
	$\mathbb{Q}(\sqrt{p})$	$4p$	$4p$	ram., p is a norm
	$\mathbb{Q}(\sqrt{-pd'})$ $1 \leqq d' \leqq \frac{p+1}{2}$ d' not a square mod p	pd' or $4pd'$	$2pd'$ or $8pd'$	
	$\mathbb{Q}(\sqrt{-p})$	p	$2p$	ram., p is not a norm
	$\mathbb{Q}(\sqrt{pd'})$ $1 \leqq d' \leqq \frac{p+1}{2}$ d' not a square mod p	pd' or $4pd'$	pd' or $4pd'$	
$p \equiv 1 \pmod 4$	$\mathbb{Q}$	1	1	splits
	$\mathbb{Q}(\sqrt{-1})$	4	8	
	$\mathbb{Q}(\sqrt{\pm d'})$ $1 \leqq d' \leqq \frac{p+3}{4}$ d' not a square mod p	d' or $4d'$	d' / $2d'$ or $4d'$ / $8d'$	unram., inert
	$\mathbb{Q}(\sqrt{p})$	p	p	ram., p is a norm
	$\mathbb{Q}(\sqrt{-p})$	$4p$	$8p$	
	$\mathbb{Q}(\sqrt{\pm pd'})$ $1 \leqq d' \leqq \frac{p+3}{4}$ d' not a square mod p	pd' or $4pd'$	pd' / $2pd'$ or $4pd'$ / $8pd'$	ram., p is not a norm
$p = 2$	$\mathbb{Q}$	1	1	splits
	$\mathbb{Q}(\sqrt{-7})$	7	14	
	$\mathbb{Q}(\sqrt{5})$	5	5	unramified, inert
	$\mathbb{Q}(\sqrt{-3})$	3	6	
	$\mathbb{Q}(\sqrt{-1})$	4	8	type $\chi_{\mathbb{Q}_2,-1}$
	$\mathbb{Q}(\sqrt{7})$	28	28	
	$\mathbb{Q}(\sqrt{-5})$	20	40	type $\chi_{\mathbb{Q}_2,-5}$
	$\mathbb{Q}(\sqrt{3})$	12	12	
	$\mathbb{Q}(\sqrt{2})$	8	8	type $\chi_{\mathbb{Q}_2,2}$
	$\mathbb{Q}(\sqrt{-14})$	56	112	
	$\mathbb{Q}(\sqrt{10})$	40	40	type $\chi_{\mathbb{Q}_2,10}$
	$\mathbb{Q}(\sqrt{-6})$	24	48	
	$\mathbb{Q}(\sqrt{-2})$	8	16	type $\chi_{\mathbb{Q}_2,-2}$
	$\mathbb{Q}(\sqrt{14})$	56	56	
	$\mathbb{Q}(\sqrt{-10})$	40	80	type $\chi_{\mathbb{Q}_2,-10}$
	$\mathbb{Q}(\sqrt{6})$	24	24	

Table 3.1: Representatives of Global Characters over $\mathbb{Q}$ with Given Local Behavior at p and/or ∞

Lemma 3.8. *If $L_1 \cap L_2 = K$, then*

$$(d_{L/K}) \quad \text{divides} \quad (d_{L_1/K})^{n_{L_2/K}} (d_{L_2/K})^{n_{L_1/K}}.$$

Proof. Note that $\mathcal{O}_{L_1 L_2} \supseteq \mathcal{O}_{L_1} \mathcal{O}_{L_2}$

and for any K-bases Ω_1 and Ω_2 in $\mathcal{O}_{L_1}$ and $\mathcal{O}_{L_2}$ respectively,

$$\Omega = \Omega_1 \Omega_2 = \{ \omega_1 \cdot \omega_2 \mid \omega_1 \in \Omega_1, \omega_2 \in \Omega_2 \}$$

is a K-basis of L in $\mathcal{O}_{L_1 L_2}$.

Thus, direct computation leads to

$$\underset{K}{Disc}(\Omega) = \underset{K}{Disc}(\Omega_1)^{n_{L_2/K}} \cdot \underset{K}{Disc}(\Omega_2)^{n_{L_1/K}}$$

Therefore,

$$\underset{K}{Disc}(\mathcal{O}_{L_1 L_2}) \quad \text{divides} \quad \underset{K}{Disc}(\Omega) = \underset{K}{Disc}(\Omega_1)^{n_{L_2/K}} \cdot \underset{K}{Disc}(\Omega_2)^{n_{L_1/K}}$$

Then,

$$\underset{K}{Disc}(\mathcal{O}_{L_1 L_2}) \quad \text{divides} \quad \underset{K}{Disc}(\mathcal{O}_{L_1})^{n_{L_2/K}} \cdot \underset{K}{Disc}(\mathcal{O}_{L_2})^{n_{L_1/K}}$$

Done. □

Proof of Prop 3.2.

$$\mathfrak{f}(\chi_{\mathbb{Q},d}|_p) = \begin{cases} p & \text{if } p \text{ is odd and } p \mid d; \\ 1 & \text{if } p \text{ is odd and } p \nmid d; \\ 8 & \text{if } p = 2 \mid d; \\ 4 & \text{if } p = 2 \text{ and } d \equiv 2, 3 \pmod 4; \\ 1 & \text{if } p = 2 \text{ and } d \equiv 1 \pmod 4; \\ \infty & \text{if } p = \infty \text{ and } d \leq 0; \\ 1 & \text{if } p = \infty \text{ and } d \geq 0. \end{cases}$$

and verify that

$$\prod_{p \nmid \infty} = \begin{cases} \prod_{p|d} p = |d| & \text{if } d \equiv 1 \pmod 4; \\ \prod_{p|d} p \cdot 4 = 4|d| & \text{otherwise.} \end{cases}$$

and $N(\chi_{\mathbb{Q},d}) = N(\chi_{\mathbb{Q},d}|_\infty)|D|$. □

Proof of Prop 3.3.

First assume that $\infty \in S$,

Let $S' = S - \{\infty\}$. We want to find α such that

$\forall p_i \in S'$, $\left(\frac{\alpha}{p_i}\right) = (\alpha)^{\epsilon_i}$,

where $\epsilon_i = 1$ if χ_{p_i} is trivial and -1 otherwise, and $p_i \nmid \alpha$ for all finite primes; if $p_i = 2$ then $\alpha \equiv 1 \pmod 4$,

and furthermore from the Question Z, we can find such α, in addition, satisfying,

(1) If $\infty \in S$, $|\alpha| \leqq 4N_{S'}$ and $\alpha \equiv 1 \pmod 4$ if $2 \in S'$; $|\alpha| \leqq N_{S'}$ if $2 \notin S'$, no matter whether χ_∞ is trivial.

If $\infty \notin S$, $|\alpha| \leqq 2N_{S'}$ and $\alpha \equiv 1 \pmod 4$ if $2 \in S'$; $|\alpha| \leqq N_{S'}/2$ if $2 \notin S'$, no matter whether χ_∞ is trivial.

(2)

$$\left(\frac{\alpha}{p_i}\right) = (-1)^{\epsilon_i}$$

where

$$\epsilon_i = \begin{cases} 0 & \text{if } \chi_{p_i} \text{ is trivial;} \\ 1 & \text{if } \chi_{p_i} \text{ is not trivial.} \end{cases}$$

(3) If $\infty \in S$, then $\alpha \geq 0$ if χ_∞ is trivial; $\alpha \leq 0$ if χ_∞ is not trivial.

Thus by some arguments, (2) and (3) lead to that $\chi_{\mathbb{Q},\alpha}|_{p_i} = \chi_{p_i}$;

and from (1), the absolute value of the discriminant of $\mathbb{Q}(\sqrt{\alpha})$ is

$$|D| \leqq \begin{cases} 4N_{S'} & \text{if } \infty \in S; \\ 2N_S & \text{if } \infty \notin S. \end{cases}$$

Hence

$$N(\chi_{\mathbb{Q},\alpha}) \leqq \begin{cases} 4N_S & \text{if } \infty \notin S \text{ or } \chi_\infty \text{ is nontrivial;} \\ 2N_S & \text{if } \infty \in S \text{ and } \chi_\infty \text{ is trivial.} \end{cases}$$

□

Proof of Prop 3.6.

From Prop 3.3, we know, if χ_v are unramified for all finite $v \in S$ we have

$$\textbf{BP1}, \textbf{BP2} \leqq \begin{cases} 2N_S \prod_p N(\chi_p) = 2N_S N(\chi_\infty) & \text{if } \infty \in S; \\ 4N_S & \text{if } \infty \notin S. \end{cases}$$

(i) If $\infty \notin S$, use the reduction process (2) in Lemma 3.5.

By Prop 3.3, we can find $\tilde{\chi}$ such that

$\tilde{\chi}|_p = \chi_p \cdot \chi_{0|_p^{-1}}$ for all $p \in S$

and $N(\tilde{\chi}) \leqq 4N_S$ and $\mathfrak{f}_{\tilde{\chi}}$ divides $\infty \cdot c$ where $N(c) = |c| \leqq 2N_S$.

Note that $\mathfrak{f}_{\chi_0}$ divides $\infty \prod_{p \in S} \mathfrak{f}(\chi_p)$,

thus

$$\begin{aligned} \mathfrak{f}_{\chi_1} = \mathfrak{f}_{\tilde{\chi}} \mathfrak{f}_{\chi_0} \quad & \text{divides} \quad lcm(\mathfrak{f}_{\tilde{\chi}}, \mathfrak{f}_{\chi_0}) \\ & \text{divides} \quad \infty \cdot c \cdot \prod_{p \in S} \mathfrak{f}(\chi_p) \end{aligned}$$

$$\Rightarrow N(\chi_1) \leqq 2 \cdot 2N_S \cdot \cdot \prod_{p \in S} N(\chi_p) = 4N_S \cdot \prod_{p \in S} N(\chi_p)$$

(ii) If $\infty \in S$, use the reduction process (2) in Lemma 3.5.

By Prop 3.3, we can find $\tilde{\chi}$ such that

$\tilde{\chi}|_p = \chi_p \cdot \chi_{0|_p^{-1}}$ for all $p \in S$

and $N(\tilde{\chi}) \leqq 2N_S N(\chi_\infty \cdot \chi_0|_\infty^{-1})$ and $\mathfrak{f}_{\tilde{\chi}}$ divides $\mathfrak{f}_{\tilde{\chi}|_\infty} \cdot c$ where $N(c) = |c| \leqq 2N_S$.

Note that $\mathfrak{f}_{\chi_0}$ divides $\infty \prod_{p \in S} \mathfrak{f}(\chi_p)$,

thus

$$\begin{aligned} \mathfrak{f}_{\chi_1} = \mathfrak{f}_{\tilde{\chi}}\mathfrak{f}_{\chi_0} \quad &\text{divides} \quad lcm(\mathfrak{f}_{\tilde{\chi}}, \mathfrak{f}_{\chi_0}) \\ &\text{divides} \quad \infty \cdot c \cdot \prod_{p \in S - \{\infty\}} \mathfrak{f}(\chi_p) \end{aligned}$$

and

$$\chi_1|_\infty = \tilde{\chi}|_\infty \cdot \chi_0|_\infty = \chi_\infty \cdot \chi_0|_\infty^{-1} \cdot \chi_0|_\infty = \chi_\infty$$

Therefore,

$$\mathfrak{f}_{\chi_1} \quad \text{divides} \quad c \cdot \prod_{p \in S} \mathfrak{f}(\chi_p)$$

Thus

$$N(\chi_1) \leqq 2N_S \cdot \prod_p N(\chi_p)$$

□

Proof of Prop 3.7.

Study the proof of Prop 3.6 above, case $S = \{p\}$, we have

$$\mathfrak{f}_{\chi_1} \quad \text{divides} \quad \infty \cdot c \cdot \mathfrak{f}(\chi_p)$$

where c is the finite part of the conductor of $\tilde{\chi}$.

Say $\tilde{\chi} = \chi_{\mathbb{Q},d}$ thus $c = |D|$ while D is the discriminant of $\mathbb{Q}(\sqrt{d})$.

Therefore,

$$N(\chi_1) \leqq 2N(\chi_p)|D| \leqq \begin{cases} 2|d|N(\chi_p) & \text{if } d \equiv 1 \pmod 4; \\ 8|d|N(\chi_p) & \text{if } d \equiv 2,3 \pmod 4; \end{cases}$$

Assume that $\chi_p \neq 1$, note that $d \pmod p$ is a square residue iff

$$\tilde{\chi}|_p = (\chi^*)_p = \chi_p \cdot \chi_0|_p^{-1}$$

Thus if $p \equiv 3 \pmod 4$ take $d = \pm 1$ and $|D| = 1$ or 4.

If $p \equiv 1 \pmod 4$, thus we can find d satisfying $|d| \leqq \frac{p+3}{4}$ which is a non-square mod p and $|D| \leqq p+3$. Such d exists as the # of square residues mod p is $\frac{p-1}{2}$, or $d = 1$ and $D = 1$.

If $p = 2$ take $d = 1$ or 5 thus $|D| = 1$ or 5.

□

Chapter 4 Kummer Extensions and General l–Extensions

4.1 Statement of the Main Theorem

This chapter is to describe and discuss **Problem I** and **Problem II** in the Kummer extension case (case (iia)) and the l–extension case (case (iib)). Note that in the case (iib), $\zeta_m \in K$ will not be needed.

Condition (A): K is a number field, S is a finite set of finite primes, m a rational integer great than 1. For each $v \in S$, χ_v a local character of exponent m on $K_v^\times$ is given.

Kummer case Condition (B): $\zeta_m \in K$.

The assertion of the Grunwald–Wang Theorem:

Given condition (A), there exists a global character χ of exponent m ($2m$ if the special case occurs. See page 7.) on C_K such that $\chi|_v = \chi|_{K_v^\times \hookrightarrow C_K} = \chi_v$ for each $v \in S$.

What is **BP1**: Recall that, the effective version of the Grunwald–Wang theorem is that: Not only such χ exists, but also, we can find such χ with the norm $N(\chi)$ is bounded by **BP1**.

Now state the four main theorems of this chapter. These four main theorems complete Theorem C to F, as the later ones are the **Problem I** part of the

following four theorems.

Theorem 4–A. *For **Problem I** and **Problem II**, assume the condition (A) and the Kummer case Condition (B) hold. Then*

$$\boldsymbol{BP1}, \boldsymbol{BP2} \leqq \left(\frac{m^2}{2} \prod_{p|m} p^3 \right)^{n_K} B(\Omega)\, {N_S}^{n_K} \prod_{v \in S} N(\chi_v)^{(m-1)\, n_K}$$

where Ω is an integral basis for K, $\Omega = \{ \omega_1, \omega_2, \cdots, \omega_{n_K} \}$, $n_K := [K : \mathbb{Q}]$,

$$B(\Omega) := \prod_{\sigma : K \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_K} |\sigma(\omega_i)|$$

and $N_S = \prod_{v \in S} N\mathfrak{p}_v$ where $||$ denotes the absolute value in $\mathbb{R}$ or $\mathbb{C}$.

This theorem leads to Theorem C.

Theorem 4–B. *For **Problem I** and **Problem II**, assume the condition (A) and the Kummer case Condition (B) hold, and assume that S^* is a set of finite primes disjoint from S_m and S, where*

$$S_m = \{ v,\ \textit{finite primes in } K \textit{ dividing } m \}$$

such that

$$C\ell_{K, S^* \cup S_\infty \cup (S_m - S)} = 1,$$

i.e.,

$$K^{S^* \cup S_\infty \cup (S_m - S)} := \left\{ x \in K^\times, v_\varphi(x) \geqq 0 \quad \forall \varphi \notin S^* \cup S_\infty \cup (S_m - S) \right\}$$

is a PID.

Then

$$\textbf{\textit{BP1}}, \textbf{\textit{BP2}} \leqq \left(\frac{m^2}{2} \prod_{p|m} p^3 \right)^{n_K} \cdot B(\Omega) \cdot {N_S}^{n_K} \cdot \prod_{v \in S^*} N\mathfrak{p}_v \cdot \prod_{v \in S, v \nmid m} N(\chi_v)$$

where $B(\Omega)$, n_K and N_S are defined in Theorem 4–A.

This theorem leads to Theorem D.

Remark. Theorem 4–B applies especially when $\mathcal{O}_K$ is a PID, and $S^* = \emptyset$.

The following are the two main results for the case when condition (A) remains and (B) drops, and $m = l$ an odd rational prime.

Theorem 4–C. *For **Problem I** and **Problem II**, $m = l$, an odd rational prime, (A) holds. Then*

$$\textbf{\textit{BP1}}, \textbf{\textit{BP2}} \leqq \left(\frac{l^{3\,n_K + 2\,n_K d}}{2^{n_K d}} \right) N_S^{n_K d^2} \cdot B(\Omega^*) \prod_{v \in S} N(\chi_v)^{(l-1)\,n_K d^2}$$

where $K_1 = K(\zeta_l)$ and $d = [K_1 : K]$, and also Ω^* is an integral basis for K_1, $\Omega^* = \{\omega_1, \omega_2, \cdots, \omega_{n_K d}\}$,

$$B(\Omega^*) := \prod_{\sigma : K_1 \hookrightarrow \mathbb{C}} \sum_{i=1}^{n_K d} |\sigma(\omega_i)|$$

This theorem leads to Theorem E.

Theorem 4–D. *For **Problem I** and **Problem II**, $K = \mathbb{Q}$, $m = l$ an odd rational prime, condition (A) holds. Then*

$$\textbf{\textit{BP1}}, \textbf{\textit{BP2}} \leqq 2^{-(l-1)l^{2l+1}(l-1)^{l-1}} \cdot B(\Omega^*) \cdot {N_S}^{(l-1)^2} \prod_{v \in S, v \nmid l} N(\chi_v)$$

This theorem leads to Theorem F.

4.2 Main Approach: The Kummer Case

This section is to prove Theorem 4–A. The main idea is to apply the following theorem – the effective version of the Chinese Remainder's theorem.

Theorem 4.1. ***(Effective version of the remainder theorem)***

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$, K a number field, $B(\Omega)$ the same as in Theorem 4–A, Let $\lambda \in \mathbb{Z}^+$ a positive integer in $\mathfrak{a} \cap \mathbb{Z}$.

Thus, for each $c \in \mathcal{O}_K$, $\exists c' \in \mathcal{O}_K$, such that

(a) $c - c' \in \mathfrak{a}$,

(b) $Nc' = |N_{K/\mathbb{Q}}(c')| \leqq (\frac{\lambda}{2})^N B(\Omega)$. *where* $N = n_K = [K : \mathbb{Q}]$

Remark: Recall that

$$B(\Omega) := \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sum_{i=1}^{N} |\sigma(\omega_i)|$$

Proof. Say $c = \sum_{i=1}^{N} \alpha_i \omega_i$, then let $c' = \sum_{i=1}^{N} \alpha_i' \omega_i$ such that λ divides $\alpha_i - \alpha_i'$ and $|\alpha_i'| \leqq \frac{\lambda}{2}$, thus $c - c' \in \lambda \mathcal{O}_K \subseteqq \mathfrak{a}$ and

$$\begin{aligned} Nc' = \left|N_{K/\mathbb{Q}}(c')\right| &= \prod_{\sigma|\infty} |\sigma(c')| \\ &\leq \prod_{\sigma|\infty} \sum_{i} |\alpha_i' \sigma(\omega_i)| \leqq (\frac{\lambda}{2})^N \prod_{\sigma|\infty} \sum_{i=1}^{N} |\sigma(\omega_i)| \\ &= (\frac{\lambda}{2})^N \cdot B(\Omega) \end{aligned}$$

□

The following corollary is deduced from the theorem above.

Corollary 4.2. *Let S be a finite set of finite primes in K, and choose $b_v \in$*

$K_v^\times$ for each $v \in S$. Assume that $v(b_v) = E_v$, $0 \leqq E_v \lneqq m$. Then there exists $b \in \mathcal{O}_K$ such that

$$b \equiv b_v \pmod{K_v^{\times m}}, \tag{A}$$

i.e., $b_v^{-1} \cdot b \in K_v^{\times m}$,

$$Nb \leqq \left(\frac{m \cdot \prod_{p|m} p}{2}\right)^N \cdot \prod_{v \in S} (N\mathfrak{p}_v)^{E_v N} \cdot N_S^N \cdot B(\Omega) \tag{B}$$

Proof. Let $\mathfrak{a} = \prod_{v \in S} \mathfrak{p}^{\lambda_{\mathfrak{p}_v} + E_v + 1}$,

where $\lambda_{\mathfrak{p}_v}$ is defined in Prop 1.2.

Recall that

$$\lambda_{\mathfrak{p}} = \begin{cases} [v_{\mathfrak{p}}(m) + e(\mathfrak{p}/p)/(p-1)] \leqq v_{\mathfrak{p}}(m) + e_{\mathfrak{p}/p} & \text{if } \mathfrak{p} \text{ divides } p|m; \\ 0 & \text{if } \mathfrak{p} \nmid m. \end{cases}$$

where p is a rational prime divisible by $\mathfrak{p}$. Set $\lambda = m \cdot \prod_{p|m} p \cdot \prod_{fV \in S} (N\mathfrak{p}_v)^{E_v+1} \in \mathbb{Z}^+$.

Check that $\lambda \in \mathfrak{a}$, in fact, for any $v = v_{\mathfrak{p}} \in S$, $\mathfrak{p}$ be the corresponding prime ideal and lying above the rational prime p.

Thus, if $\mathfrak{p} \mid m$, then

$$\begin{aligned} v_{\mathfrak{p}}(\lambda) &= v_{\mathfrak{p}}(m) + v_{\mathfrak{p}}(p) + E_{v_{\mathfrak{p}}} + 1 \\ &= v_{\mathfrak{p}}(m) + e_{\mathfrak{p}/p} + E_{v_{\mathfrak{p}}} + 1 \geqq \lambda_{\mathfrak{p}} + E_{v_{\mathfrak{p}}} + 1 \end{aligned}$$

if $\mathfrak{p} \nmid m$, then

$$v_{\mathfrak{p}}(\lambda) = E_{v_{\mathfrak{p}}} + 1 = \lambda_{\mathfrak{p}} + E_{v_{\mathfrak{p}}} + 1$$

Next we can apply Theorem 4.1.

First by the remainder theorem, there exists $b_0 \in \mathcal{O}_K$, such that $v(b_0 - b_v) \geqq \lambda_{\mathfrak{p}_v} + E_v + 1$ for any $v \in S$. Applying Theorem 4.1, there exists b such that $b - b_0 \in \mathcal{O}_K$, thus satisfies (B).

Check (easily) that ${b_v}^{-1} \cdot b \in \mathcal{U}_{K_v}$ and $v({b_v}^{-1} \cdot b - 1) \geqq \lambda_{\mathfrak{p}_v} + 1$, thus by Prop 1.2, ${b_v}^{-1} \cdot b \in K_v^{\times m}$, thus (A) holds. □

Next, we combine all things above.

Proposition 4.3. *Preserve the hypotheses of Theorem 4-A, and assume that* $\chi_v = \chi_{b_v,\mathfrak{p}_v}$ *for each* $v \in S$, *and* $v(b_v) = E_v$, $0 \leqq E_v \lneqq m$.

Then, there exists a global character $\chi = \chi_b$ *of exponent* m, *such that*

$$\chi_b|_v = \chi_{b,\mathfrak{p}_v} = \chi_{b_v,\mathfrak{p}_v} \tag{A}$$

$$N(\chi) \leqq \left\{ m^2 \cdot \prod_{p|m} p^3 \right\}^{n_K} \cdot {N_S}^{n_K} \cdot B(\Omega) \cdot \prod_{v \in S} (N\mathfrak{p}_v)^{E_v n_K} \tag{B}$$

Prop 4.3 stands a crucial part for this chapter.

Corollary 4.4. *Keep the hypotheses of Prop 4.3. If* $b_v \in \mathcal{U}_{K_v}$, *i.e.*, $E_v = 0$ *for any* $v \in S$, *there exists a global character* $\chi = \chi_b$ *of exponent* m *satisfying*

(A) and the following

$$N(\chi) \leqq \left\{ m^2 \cdot \prod_{p|m} p^3 \right\}^{n_K} \cdot {N_S}^{n_K} \cdot B(\Omega) \qquad \text{(B')}$$

It is easy to get Corollary 4.4 from Prop 4.3.

Proof of Proposition 4.3.

By Corollary 4.2, there exists $b \in K^\times$ satisfying (A) and (B) in Corollary 4.2, then $\chi_b|_v = \chi_{b,\mathfrak{p}_v} = \chi_{b_v,\mathfrak{p}_v}$ as ${b_v}^{-1} \cdot b \in K_v^{\times m}$ holds for each $v \in S$. To verify (B) in Prop 4.3. Applying Lemma 1.4 (3) and note that (also applying Prop 1.2)

$$\left(\prod_{\mathfrak{p} \nmid m,\ \chi|_\mathfrak{p} \text{ ram.}} N\mathfrak{p} \right) \quad \text{divides} \quad Nb$$

Done. □

Proof of Theorem 4–A.

By observation, we need only to show that

$$\prod_{v \in S} (N\mathfrak{p}_v)^{E_v} \leqq \prod_{v \in S} N(\chi_v)^{m-1}$$

so that we can apply Prop 4.3.

Note that $\chi_v = \chi_{b_v,\mathfrak{p}_v}$ for some $b_v \in K_v^\times$, we can choose such b_v that $b_v \in \mathcal{O}_{K_v}$ and $v(b_v) \leqq m$, so Prop 4.3 can be applied.

Note that if $E_v \neq 0$, then $1 \leqq E_v \leqq m-1$, thus $K_v(\sqrt[m]{b_{b_v}})/K_v$ must be

ramified. Then $N(\chi_v) \geqq N\mathfrak{p}_v$, and eventually

$$\prod_{v\in S}(N\mathfrak{p}_v)^{E_v} \leqq \prod_{v\in S,\ \chi_v=\chi|_v \text{ ram.}} (N\mathfrak{p}_v)^{m-1} \leqq \prod_{v\in S} N(\chi_v)^{m-1}$$

Done. □

Proof of Theorem 4-B.

First assume that $\chi_v = \chi_{b_v,\mathfrak{p}_v}$ for each $v \in S$, $v(b_v) = E_v$, $0 \leqq E_v \lneqq m$.

Since $C\ell_{K,S^*\cup S_\infty\cup(S_m-S)} = 1$, we can find $c_v \in \mathcal{O}_K$ satisfying

(i) $v(c_v) = 1, \tilde{v}(c_v) = 0$ for any $\tilde{v} \neq v$ in S;

(ii) $\tilde{v}(c_v) = 0$ outside S^*, S_m and S_∞.

Let $c = \prod_{v\in S} {c_v}^{E_v}$

By the assumptions above, $v(c^{-1}\cdot b_v) = E_v - v(c) = 0$. Thus from Corollary 4.2, there exists $b_0 \in \mathcal{O}_K$ satisfying

$$b_0 \equiv c^{-1}\cdot b_v \pmod{K_v^{\times m}} \tag{AA}$$

$$Nb_0 \leqq \left(\frac{m\cdot\prod_{p|m}p}{2}\right)^{n_K}\cdot {N_S}^{n_K}\cdot B(\Omega) \tag{BB}$$

Check that $\chi_{b_0\cdot c}|_v = \chi_{b_v,\mathfrak{p}_v} = \chi_v$.

Furthermore, we want to estimate

$$\prod_{\mathfrak{p}\nmid m,\chi_{b_0\cdot c} \text{ ram. at } \mathfrak{p}.} N\mathfrak{p}$$

so that we can apply Lemma 1.4 (3).

Note that

$$\prod_{\mathfrak{p}\nmid m,\chi_{b_0\cdot c}\text{ ram. at }\mathfrak{p}.} N\mathfrak{p} \leqq \prod_{\mathfrak{p}\nmid m,\mathfrak{p}\mid b_0 c} N\mathfrak{p} \leqq Nb_0 \cdot \prod_{\mathfrak{p}\nmid m,\mathfrak{p}\mid c} N\mathfrak{p}$$

$$\leqq Nb_0 \cdot N_{S^*} \cdot \prod_{v\in S,\mathfrak{p}_v\nmid m,\mathfrak{p}_v\mid c} N\mathfrak{p}_v$$

$$= Nb_0 \cdot N_{S^*} \cdot \prod_{v\in S,v\nmid m,1\leqq E_v\leqq m-1} N\mathfrak{p}_v$$

Combine (BB) above, use Lemma 1.4 (3), and note that for $v \in S$, $v \nmid m$, $N(\chi_v) = 1$ if χ_v is unramified and $N(\chi_v) = N\mathfrak{p}_v$ if χ_v is ramified; and $E_v = 0$ iff χ_v is unramified. Done. □

4.3 Main Approach: Non–Kummer l-extensions

In this section, we will come to the case when (A) holds, and the Kummer extension case (B) is dropped. $m = l$ an odd rational prime.

We will prove Theorem 4–C and Theorem 4–D.

Here denote $K_1 = K(\zeta_l)$, $G = Gal(K_1/K)$, $N_1 = [K_1 : \mathbb{Q}]$, and $d = [K_1 : K] \mid l - 1$. G acts on K_1, $\mathbb{I}_{K_1}$ and C_{K_1} the natural way.

First, we sketch out the main idea of the proof.

Let $\tilde{S} := \{\omega \mid v \in S\}$, and $\tilde{\chi}_\omega = \chi_v \circ N_{(K_1)_\omega/K_v}$ for each $v \in S$, the point is, to construct a global character of exponent l: $\tilde{\chi}$, such that $\tilde{\chi}|_\omega = \chi_\omega$ and bound $N(\tilde{\chi})$.

Furthermore, by some trick, we need that $\tilde{\chi}$ can be pulled back, i.e., $\exists\chi$ a global character of exponent l, such that $\tilde{\chi} = \chi \circ N_{K_1/K}$, and thus $\chi|_v \circ N_{(K_1)_\omega/K_v} = (\chi \circ N_{K_1/K})|_\omega = \tilde{\chi}_\omega$, thus for $v \in S$, $\chi|_v = \chi_v$ on $N_{(K_1)_\omega/K_v}$, since

$[(K_1)_\omega : K_v] \mid d$, and $(l, d) = 1$, χ is of exponent l, hence

$$[K_v^\times : N_{(K_1)_\omega/K_v}(K_1)_\omega^\times] \quad \text{divides} \quad d \mid l-1$$

hence $\chi|_v = \chi_v$ on $K_v^\times$, so that we may apply Lemma 1.4 and Lemma 1.6.

Notice that, when we construct $\tilde{\chi}$ such that $\tilde{\chi}|_\omega = \tilde{\chi}_\omega$ for each $\omega \in \tilde{S}$, we don't necessarily have that $\tilde{\chi}$ factors through $C_{K_1}/\,Ker\, N_{K_1/K}$. However,

$$\tilde{\tilde{\chi}} = \left\{ \prod_{\sigma \in G} (\tilde{\chi} \circ \sigma) \right\}^{(d^{-1} \mod l)}$$

is what we need, since $\tilde{\tilde{\chi}} = \tilde{\tilde{\chi}} \circ \sigma, \forall \sigma \in G$.

Lemma 4.5. *If $\tilde{\chi}$ is a global character on C_{K_1} of exponent l, and $\tilde{\chi} = \tilde{\chi} \circ \sigma$ for any $\sigma \in G = Gal(K_1/K)$, then*

(1) *There exists a unique global character χ on C_K of exponent l satisfying $\tilde{\chi} = \chi \circ N_{K_1/K}$.*

(2) *Furthermore,*

$$\prod_{\tilde{\mathfrak{p}} \nmid l,\ \tilde{\chi}|_{\tilde{\mathfrak{p}}} \text{ unram.}} N\tilde{\mathfrak{p}} = \left(\prod_{\mathfrak{p} \nmid l,\ \chi|_{\mathfrak{p}} \text{ unram.}} N\mathfrak{p} \right)^d .$$

where $d = [K_1 : K]$.

Proof.

Step 1. $\tilde{\chi}$ factors through $C_K/\,Ker\, N_{K_1/K}$.

In fact, for each $\lambda \in Ker\, N_{K_1/K}$, $\lambda = a/\sigma(a)$ for some $a \in C_K$ and a generator σ of G which is a cyclic group since $H^{-1}(G, C_{K_1}) = 1$ by the global class field theory.

Step 2. Knowing that $N_{K_1/K}(Ker\,\tilde{\chi})$ is closed in C_K, (1) and (2) hold.

In fact, let $A_0 = N_{K_1/K}(Ker\,\tilde{\chi})$, $[N_{K_1/K}C_{K_1} : A_0] \mid l$, thus A_0 is of finite index and thus is open in C_K. Furthermore, from the step 1, we can get an algebraic character χ_0 (not assuming the continuity) on $N_{K_1/K}C_K$ of exponent l, which can be uniquely extended to an algebraic character χ on C_K of exponent l as $[C_K : N_{K_1/K}(C_{K_1})] = d \mid l-1$ relative prime to l. As $Ker\,\tilde{\chi} \supseteqq A_0$ is open, χ is continuous. It is easy to check (1). Applying Lemma 1.6 (3), (2) holds.

Step 3. $N_{K_1/K}(Ker\,\tilde{\chi})$ is closed in C_K.

Since $\tilde{\chi}$ is a global character on C_{K_1}, by the global class field theory, $Ker\,\tilde{\chi} = N_{L/K_1}C_L$ for some field extension L/K_1. Thus $N_{K_1/K}(Ker\,\tilde{\chi}) = N_{K_1/K}(N_{L/K_1}C_L) = N_{L/K}(K)$ which is closed. Done. □

Detailed Proof the Theorem 4–C.

Notations are the same as before. $K_1 = K(\zeta_l)$, $N_1 = n_{K_1} = [K_1 : \mathbb{Q}]$ $\tilde{\chi}_\omega = \chi_\upsilon \circ N_{(K_1)_\omega/K_\upsilon}$ for any finite prime ideal tower ω/υ in K_1/K where $\upsilon \in S$.

By Theorem 4–A, and its proof, and Corollary 4.2, we can find a global character $\tilde{\chi} = \tilde{\chi}_{\tilde{b}}$ of exponent l on C_{K_1}, such that $\tilde{\chi}|_\omega = \tilde{\chi}_\omega$, for any $\omega \in \tilde{S}$, and

$$\prod_{\tilde{\mathfrak{p}} \nmid l,\ \tilde{\chi}|_{\tilde{\mathfrak{p}}}} N\tilde{\mathfrak{p}} \leqq N\tilde{b} \leqq \left(\frac{l^2}{2}\right)^{N_1} \cdot \prod_{\omega \in \tilde{S}} (N\tilde{\mathfrak{p}}_\omega)^{E_{\tilde{\mathfrak{p}}_\omega} N_1} \cdot N_{\tilde{S}}^{N_1} \cdot B(\Omega^*)$$

Here we explain all the notations. $B(\Omega^*)$ is defined in Theorem 4–C, for

each ω, $\tilde{\mathfrak{p}}_\omega$ is the corresponding to ω, and $\tilde{\chi}_\omega = \tilde{\chi}_{\tilde{b}_\omega, \tilde{\mathfrak{p}}_\omega}$, for each $\omega \in \tilde{S}$, and $0 \leqq E_{\tilde{\mathfrak{p}}_\omega} := \omega(\tilde{b}_\omega) \lneqq l$, and note that if $E_{\tilde{\mathfrak{p}}_\omega} \neq 0$, $\tilde{\chi}_\omega$ is ramified.

Thus we have

$$\prod_{\omega \in \tilde{S}} (N\tilde{\mathfrak{p}}_\omega)^{E_{\tilde{\mathfrak{p}}_\omega} N_1} \leqq \prod_{\omega \in \tilde{S}} N(\tilde{\chi}_\omega)^{(l-1)N_1}$$

Thus we get

$$\prod_{\tilde{\mathfrak{p}} \nmid l,\ \tilde{\chi}_{\tilde{\mathfrak{p}}} \text{ ram.}} N\tilde{\mathfrak{p}} \leqq \left(\frac{l^2}{2}\right)^{N_1} \prod_{\omega \in \tilde{S}} N(\tilde{\chi}_\omega)^{(l-1)N_1} \cdot N_{\tilde{S}}^{N_1} \cdot B(\Omega^*) \qquad (\Delta\Delta)$$

Let $\tilde{\tilde{\chi}} = \left(\prod_{\sigma \in G} (\tilde{\chi} \circ \sigma\right)^{d^{-1} \pmod{l}}$

Thus $\tilde{\tilde{\chi}} = \tilde{\tilde{\chi}} \circ \sigma$, and

$$\prod_{\tilde{\mathfrak{p}} \nmid l,\ \tilde{\chi}|_{\tilde{\mathfrak{p}}} \text{ ram.}} N\tilde{\mathfrak{p}} \leqq (\text{RHS of } \Delta\Delta)^d$$

and by Lemma 4.5, $\tilde{\tilde{\chi}} = \chi \circ N_{K_1/K}$, χ a global character exponent l, and $\chi_v = \chi_v$ on $N_{(K_1)_\omega / K_v} K_{1\omega}^\times$, thus on $K^\times$ by the uniqueness of χ, and also,

$$\prod_{\mathfrak{p} \nmid l,\ \chi|_{\mathfrak{p}} \text{ ram.}} N\tilde{\mathfrak{p}} \leqq (\text{RHS of } \Delta\Delta)^d$$

and by Lemma 1.6 (1)–(3), we have

$$\prod_{\omega \in \tilde{S}} N(\tilde{\chi}_\omega) \leqq \prod_{v \in S} N(\chi_v)^d$$

and

$$\prod_{\omega\in\tilde{S}}\tilde{\mathfrak{p}}_\omega \;\Big|\; \prod_{v\in S}\mathfrak{p}_v\cdot\mathcal{O}_{K_1}$$

We get

$$\prod_{\mathfrak{p}\nmid l,\ \chi|_{\mathfrak{p}}\text{ ram.}} N\mathfrak{p} \leqq \left(\frac{l^2}{2}\right)^{n_K d} N_S^{n_K d^2} B(\Omega^*) \qquad (\star\star)$$
$$\cdot \prod_{v\in S} N(\chi_v)^{n_K d^2(l-1)}$$

Applying Lemma 1.4, we are done. □

Check the proof above. If additionally, we assume that $\chi_v, v \in S$ are unramified, thus so are $\tilde{\chi}_\omega$ for all $\omega \in S$ because of Lemma 1.6. Thus $E_{\mathfrak{p}_\omega} = 0$ for all $\omega \in \tilde{S}$, thus $(\Delta\Delta)$ is replaced by

$$\prod_{\tilde{\mathfrak{p}}\nmid l,\ \tilde{\chi}_{\tilde{\mathfrak{p}}}\text{ ram.}} N\tilde{\mathfrak{p}} \leqq \left(\frac{l^2}{2}\right)^{N_1}\cdot N_{\tilde{S}}^{N_1}\cdot B(\Omega^*) \qquad (\Delta\Delta')$$

and thus $(\star\star)$ is replaced by

$$\prod_{\mathfrak{p}\nmid l,\ \chi|_{\mathfrak{p}}\text{ ram.}} N\mathfrak{p} \leqq \left(\frac{l^2}{2}\right)^{n_K d} N_S^{n_K d^2} B(\Omega^*) \qquad (\star\star')$$

Especially, for $K = \mathbb{Q}$, $N = 1$, $d = l-1$ as we select the integral basis $\Omega^* = \{1, \zeta_l, \ldots, \zeta_l^{l-2}\}$, and $B(\Omega) = (l-1)^{(l-1)}$, we will get the following intermediate statement:

Proposition 4.6. *For **Problem I**: Let $K = \mathbb{Q}$, $m = l$ an odd prime, and S,*

a finite set of finite primes in $\mathbb{Q}$ *such that for each* $v \in S$, χ_v *is unramified. Then there exists a global character* χ *of exponent* l *such that*

$$\chi|_v = \chi_v \qquad (v \in S) \tag{A}$$

$$\prod_{p\nmid l,\ \chi|_p \text{ ram.}} Np \leqq \left(\frac{l^2}{2}\right)^{l-1} \cdot N_S^{(l-1)^2} \cdot (l-1)^{l-1} \tag{B}$$

□

Proof of Theorem 4–D.

For any given χ_v, $v \in S$, not necessarily assuming that χ_v is unramified for each χ_v, By Prop 1.7, for each p_v, the corresponding rational prime to v, there exists a global character Y_v such that Y_v is of exponent l, and $Y_v|_{p_v}$ and χ_v agree on $\mathcal{U}_{\mathbb{Q}_v}$, and Y_v is unramified at any other finite primes outside v.

Let $\chi_v^* = \prod_{u\in S}({Y_u}^{-1}|_v) \cdot \chi_v$, then χ_v^* is unramified for each $v \in S$, and χ_v^* is of exponent l.

Thus by Prop 4.6 there exists a global character χ^* of exponent l such that

$\chi^*|_v = \chi_v^* \qquad \forall v \in S$

and

$$\prod_{p\nmid l,\ \chi|_p \text{ ram.}} p \leqq \left(\frac{l^2}{2}\right)^{l-1} N_S^{(l-1)^2}(l-1)^{l-1}$$

Let $\chi = \chi^* \cdot \prod_{v\in S} Y_v$, then $\chi|_v = \chi_v (v \in S)$, and χ is of exponent l.

And by the construction of Y_v.

$$\prod_{p\nmid l,\ \chi|_p \text{ ram.}} p$$

$$\leqq \prod_{p\nmid l,\ \chi^*|_p \text{ ram.}} p \cdot \prod_{p\nmid l, v_p\in S} p$$

$$\leqq \left(\frac{l^2}{2}\right)^{l-1} N_S^{(l-1)^2}(l-1)^{l-1} \cdot \prod_{v\nmid l, v\in S} N(\chi_v)$$

Where v_p denotes the corresponding place to the prime p.

Applying Lemma 1.4, we are done. □

Chapter 5 General Case

In this chapter, we solve the general case using a different method. Since each character can be expressed uniquely as a product of characters of prime power order, we may easily reduce to the case when $m = l^r$ is a prime power. We will prove the following theorem.

Theorem 5–A. *Let K be a number field, $m = l^r$ a prime power, S a finite set of primes of K, χ_v a local character on K_v^* of exponent m for each v in S.*

Assume that $K(\zeta_{l^r})/K$ is cyclic. There is a global character χ on C_K of exponent m with its local component being χ_v at each $v \in S$, such that

$$N(\chi) \leq B_l(K(\zeta_{l^r}), \tilde{S}')^{rw+1} C_{l^r}(K, S') \prod_{v \in S} N(\chi_v)$$

where S' is a finite set of finite *primes containing all the* finite *primes in S and satisfying $l \nmid \#Cl_{K,S' \cup S_\infty}$, with*

$$r_W = \gamma_l(Cl_{K,S \cup S_\infty}) + |S \cup S_\infty| - 1$$

Here $\gamma_l(G)$ denotes the minimal cardinality of the generating set of the Sylow–l subgroup of G.

Definition 5–i. For each number field K, let s be the largest integer such

that $\eta_{2^s} \in K$. Define S_0 as the following.

$$S_0 = \{\mathfrak{p} \quad \text{divides} \quad 2, \quad -1, \pm(2+\eta_{2^s}) \text{ are not squares in } K_{\mathfrak{p}}^*.\}$$

Also, if $r > s$, define

$$a_0 = (1+\zeta_{2^s})^{2^r} = (i\eta_{2^{s+1}})^{2^r} = {\eta_{2^{s+1}}}^{2^r}$$

and a_0^* denotes the idele class in C_K with components a_0 at the primes in S_0 and 1 at other primes.

The next theorem deals with the case when $K(\zeta_{2^r})/K$ is *not cyclic.*

Theorem 5–B. *Preserve all the hypotheses of Theorem 5–A with $l = 2$ except to replace the condition about $K(\zeta_{l^r})/K$ by the following:*

(SS) $K(\zeta_{2^r})/K$ *is not cyclic,* $S_0 \subset S$ *and*

$$\prod_{v \in S_0} \chi_v(a_0) = 1$$

Then there is a global character χ on C_K of exponent m with its local component being χ_v at each $v \in S$, such that

$$N(\chi) \leq B_l(K(\zeta_{l^r}), \tilde{S}')^{r_W+1} C_{l^r}(K, S') \prod_{v \in S} N(\chi_v)$$

where S' and r_W are the same in Theorem 5–A.

Furthermore, if (SS) *is replaced by*

(SS′) $K(\zeta_{2^r})/K$ *is not cyclic,* $\mathfrak{p}_0 \in S_0 - S \neq \emptyset$,

then there is a global character χ on C_K of exponent m such that

$$N(\chi) \leq B_l(K(\zeta_{l^r}), \tilde{S}')^{rw+1} N\mathfrak{p}_0{}^{\lambda} \prod_{v \in S} N(\chi_v)$$

where λ is the smallest integer such that

$$1 + \mathfrak{p}_0{}^{\lambda} \subset \mathcal{U}^{2^r}_{K_{\mathfrak{p}_0}}.$$

Note that if both (SS) and (SS′) fail, then we are in the special case of Wang ([Wa50], [A-T68]), and such χ of exponent m might not exist. In such case, there will be a character χ of order $2m$ with desired local components, and the bound above will still apply with $m = 2^r$ replaced by 2^{r+1}.

Definition 5–ii. The *conductor* $\mathfrak{f}_V$ of an open subset V of $\mathbb{I}_K$ or C_K is the smallest cycle $\mathfrak{c}$ such that V contains $V_{\mathfrak{c}}$ which is the standard open subgroup in $\mathbb{I}_K$ or C_K corresponding to $\mathfrak{c}$. Also, when P_0 is open in P where P is a subgroup of $\mathbb{I}_K$ or C_K, the *conductor* $\mathfrak{f}$ of P_0 in P is the smallest cycle $\mathfrak{c}$ such that P_0 contains $P \cap V_{\mathfrak{c}}$.

In fact, we prove the following theorems which are stronger. For details, see Section 5.4.

Theorem 5–C. *Let K be a number field, $m = l^r$ a prime power, S a finite set of primes of K, $\tilde{P} = \prod_{v \in S} K_v^{\times}$, P the image of the natural embedding of $\tilde{P}$ into $\mathbb{I}_K$, and P_0 a subgroup of P such that P/P_0 is of exponent m.*

Assume that $K(\zeta_{l^r})/K$ is cyclic. There is a cycle $\mathfrak{c}$ such that

$$K^\times V_{\mathfrak{c}} \mathbb{I}_K^m \cap P \subseteq P_0$$

and

$$N\mathfrak{c} \leq B_l(K(\zeta_{l^r}), \tilde{S}')^{r_W+1} C_{l^r}(K, S') N\mathfrak{f}$$

where S' and r_W are the same in Theorem 5–A, and $\mathfrak{f}$ is the smallest cycle $\mathfrak{f}$ such that $P \cap V_{\mathfrak{f}} \subset P_0$.

Theorem 5–D. *Preserve all the hypotheses of Theorem 5–C with $l = 2$ except that the condition about $K(\zeta_{l^r})/K$ is replaced by the following.*

(SS) *$K(\zeta_{2^r})/K$ is not cyclic, $S_0 \subset S$ and $a_0^* \in P_0$,*

Then there is a cycle $\mathfrak{c}$ such that

$$K^\times V_{\mathfrak{c}} \mathbb{I}_K^m \cap P \subseteq P_0$$

and

$$N\mathfrak{c} \leq B_l(K(\zeta_{l^r}), \tilde{S}')^{r_W+1} C_{l^r}(K, S') N\mathfrak{f}$$

where S' and r_W are the same in Theorem 5–A, and $\mathfrak{f}$ is the smallest cycle $\mathfrak{f}$ such that $P \cap V_{\mathfrak{f}} \subset P_0$.

Furthermore, if (SS) *is replaced by*

(SS′) *$K(\zeta_{2^r})/K$ is not cyclic, $\mathfrak{p}_0 \in S_0 - S \neq \emptyset$,*

then there is a cycle $\mathfrak{c}$ *such that*

$$K^{\times} V_{\mathfrak{c}} \mathbb{I}_K^m \cap P \subseteq P_0$$

and

$$N\mathfrak{c} \leq B_l(K(\zeta_{l^r}), \tilde{S}')^{rw+1} N\mathfrak{p}_0{}^{\lambda} N\mathfrak{f}$$

where λ *is the smallest integer such that*

$$1 + \mathfrak{p}_0{}^{\lambda} \subset \mathcal{U}_{K_{\mathfrak{p}_0}}^{2^r}.$$

5.1 Formulation of Case (iii) & Problem V

Now we will find a weak bound for **Problem I** and **Problem II** in the general case. We do not assume that the ground field K contains ζ_m, $m = l^r$.

Here we still denote K as a number field, S a finite set of places (or primes) in K, and $\chi_v, v \in S$ given local characters of $K_v^{\times}$ of exponent m.

Let $\tilde{P} = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^{\times}$, $\tilde{P}$ injects into C_K in such a way that

$\forall (a_{\mathfrak{p}}) \in \tilde{P}$, there's an idele $c = (c_{\mathfrak{p}})$ such that

$$c_{\mathfrak{p}} = \begin{cases} a_{\mathfrak{p}}, & \text{if } \mathfrak{p} \in S \\ 1, & \text{otherwise} \end{cases}$$

and the following holds:

$$(c, K) = \prod_{\mathfrak{p} \in S} (a_{\mathfrak{p}}, K_{\mathfrak{p}})$$

Let $\tilde{P}_0 \subsetneqq \tilde{P}$ be a subgroup with quotient of exponent m, i.e., $\tilde{P}/\tilde{P}_0$ is of exponent m. Let P and P_0 be the images of $\tilde{P}$ and $\tilde{P}_0$ in C_K via the natural embedding $\tilde{P} \hookrightarrow C_K$. In general, $\tilde{P} \hookrightarrow C_K$ is not a topological embedding unless $\#S = 1$. However, by Proposition 1.12, there is a one–to–one correspondence between the set of open subgroups of finite index of $\tilde{P}$ and the set of open subgroups of P.

By Lemma 1.14 and Proposition 1.16, we can get the following reformulation of the Grunwald–Wang Theorem: ([A-T68])

Theorem 5.1. *Let P be the image of $\tilde{P} = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^{\times}$ via the the natural map:*

$$\prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^{\times} \hookrightarrow \mathbb{I}_K \to C = C_K$$

where S is a finite set of primes in K.

Let P_0 be the image of $\tilde{P}_0$ via the natural map above where $\tilde{P}_0$ is a subgroup of $\tilde{P}$ with the factor group $\tilde{P}/\tilde{P}_0$ being cyclic of order m.

Let $n = m$, or $2m$ if the special case occurs as in Theorem 0.3. Then we have the following:

(a) *There exists an open subgroup $\tilde{V}$ containing $P_0 C^n$, and $P \cap \tilde{V} = P_0$.*

(b) *There exists an open subgroup V separates PC^n/P_0C^n.*

(c) *There exists an open subgroup V such that $P \cap C^n V \subsetneqq P_0$.*

From Proposition 1.13, $n = m$, or $2m$ if the special case occurs. And

$P \cap C^n \subsetneqq P_0$.

In fact, when the special case occurs, $P \cap C^m \subsetneqq P_0 \cup a_0 P_0$ where $a_0 = (1+\zeta_{2^s})^m$ as in Theorem 0.2 and Theorem 0.3.

Note that (a) is exact Proposition 1.16, and in fact the main part of the Grunwald's Theorem, which was also proved [A-T68].

In Chapter 4, we get a weak least bound of $N(\chi)$ in terms of K, S and m where K is a number field and $\zeta_m \in K$, and S is a finite set of finite primes. Also, we get a least bound of $N(\chi)$ in terms of K, S and m where $m = l$ is an odd rational prime, and K be an arbitrary number field, and S a finite set of finite primes.

However, the strategy used in Chapter 4 fails for the general case here. So we will develop another way.

In fact, given K, S, $\chi_v, v \in S$ as in Theorem 0.2, with $\tilde{P}_0$ determined as the kernel of $\prod \chi_v$ on $\tilde{P}$ and P_0 the image of $\tilde{P}_0$ via the natural map described on Page 30, if we find an open subgroup V of $C = C_K$ satisfying (c), we may let $\tilde{V} = P_0 C^n V$ then $\tilde{V}$ satisfies (a).

Denote **BP5** as the least bound for the **Problem V** or **Problem V′** given below. We have

$$\mathbf{BP2} \leq \mathbf{BP1} \leq \mathbf{BP5}$$

Problem V: *Let* $\tilde{P} = \prod_{v \in S} K_v^\times$ *where* S *is a finite set of places of a number field* K, $\tilde{P}_0$ *a subgroup of* $\tilde{P}$ *with the factor group* $\tilde{P}/\tilde{P}_0$ *being of exponent* $m > 1$, *and* P, P_0 *the respective images of* $\tilde{P}$, $\tilde{P}_0$ *via the natural injective*

homomorphism

$$\psi : \tilde{P} = \prod_{v \in S} K_v^{\times} \xrightarrow{\Psi} \mathbb{I}_K \to C_K.$$

Find a standard open subgroup $V = C_K^{\mathfrak{f}}$ *of* $C = C_K$ *for some cycle* $\mathfrak{f}$, *such that*

$$P \cap C^n V \subsetneqq P_0$$

and $N\mathfrak{f} \leq$ ***BP5***, *where* $n = m$, *or* $2m$ *if the special case occurs (see Theorem 0.3).*

Equivalently, we may work on the following **Problem V′**.

Problem V′: *Let* $\tilde{P} = \prod_{v \in S} K_v^{\times}$ *where* S *is a finite set of places of a number field* K, $\tilde{P}_0$ *a subgroup of* $\tilde{P}$ *with the factor group* $\tilde{P}/\tilde{P}_0$ *being of exponent* $m > 1$, *and* P, P_0 *the respective images of* $\tilde{P}$, $\tilde{P}_0$ *via the natural injective homomorphism*

$$\Psi : \tilde{P} = \prod_{v \in S} K_v^{\times} \to \mathbb{I}_K.$$

Find a standard open subgroup $V = V_{\mathfrak{f}}$ *of* $\mathbb{I}_K$ *for some cycle* $\mathfrak{f}$, *such that*

$$P \cap K^{\times} \mathbb{I}_K^n V \subsetneqq P_0$$

and $N\mathfrak{f} \leq$ ***BP5***, *where* $n = m$, *or* $2m$ *if the special case occurs (see Theorem 0.3).*

Recall that, we say the special case occurs, if $K(\zeta_{l^r})/K$ is not cyclic (hence

$l = 2$ and $r \geq 3$), $S_0 \subsetneqq S$ and $a_0^* \in P_0$. See the beginning of this chapter for the definition of S_0 and a_0^*.

5.2 Essential Closure

This part is to introduce the concept of "essential closure" which will be needed.

A *lattice* in $K^\times$ of rank h is a free abelian subgroup of $K^\times$ of rank h.

Let R be an integral domain and M an R–module. A submodule N is said to be *R–essential* or *R–divisibly closed in M* if for any $\sigma \neq 0 \in R$ and $n \in M$, we have $\sigma n \in N \Rightarrow n \in N$. Given any nonzero λ in R, N is said to be *λ–essential* or *λ–divisibly closed* if $\lambda n \in N \Rightarrow n \in N$.

For each nonzero λ in R, call the set

$$\{\, n \in M, \lambda^s n \in N \text{ for some } s \,\}$$

the *λ–essential closure* or *λ–divisible closure* of N in M. Of course a λ–essential R–submodule of M is the λ–essential closure of itself; and any λ–essential closure of a submodule of M is λ–essential.

Call the set

$$\{\, n \in M, rn \in N \text{ for some non–zero } r \text{ in } R \,\}$$

the *R–essential closure* or *R–divisible closure* of N in M. Of course any R–essential submodule is also λ–essential for any $\lambda \neq 0$ in R.

Also, when one says *essential* one means $\mathbb{Z}$*–essential.*

Example. The set K^S of S–units in K is $\mathbb{Z}$–essential in $K^\times$ for any finite set S of primes of K.

Now we recall some standard facts, and give proofs for completeness.

Proposition 5.2 (Basis of a sublattice in $\mathbb{Z}^n$). *Let $V \subsetneqq \mathbb{Z}^n$ be a sublattice of rank r, and let*

$$\begin{aligned} W_0 = 0 \subsetneqq W_1 = \mathbb{Z} \times 0^{n-1} \subsetneqq \dots \\ \subsetneqq W_i = \mathbb{Z}^i \times 0^{n-i} \subsetneqq \dots \\ \subsetneqq W_{n-1} = \mathbb{Z}^{n-1} \times 0^1 \subsetneqq W_n = \mathbb{Z}^n \end{aligned}$$

be a filtration of $\mathbb{Z}^n$, i.e.,

$$W_i = \{\, (a_1, \dots, a_n) \in \mathbb{Z}^n, \quad a_j = 0 \qquad \forall j \geqq i \,\}$$

Let $V_i = W_i \cap V$, $V_0 = 0$ and $V_n = V$, and α_i some element in V_i generating $V_i + W_{i-1}/W_{i-1} \subsetneqq W_i/W_{i-1} \cong \mathbb{Z}$ if $V_i \neq V_{i-1}$ and $\alpha_i = 0$ if $V_i = V_{i-1}$.

Thus the nonzero elements of $\alpha_1, \dots, \alpha_n$ form a $\mathbb{Z}$-basis for V.

Proof. First V is generated by $\alpha_1, \dots, \alpha_n$. This is true as we can inductively prove that $\langle \alpha_i \rangle + V_{i-1} = V_i$. In fact, for any $a \in V_i$, say $a = c_i \alpha_i + b$ where $c_i \in \mathbb{Z}$ and $b \in W_{i-1}$ thus $b \in W_{i-1} \cap V_i = V_{i-1}$, thus $\langle \alpha_i \rangle + V_{i-1} \supsetneqq V_i$.

Furthermore, we prove that only r elements in $\alpha_1, \dots, \alpha_n$ are not zero, so that we conclude V is free on r nonzero elements in $\alpha_1, \dots, \alpha_n$. In fact, if $V_i \neq V_{i-1}$ then $V_i/V_{i-1} \cong V_i + W_{i-1}/W_{i-1}\mathbb{Z}$. Thus $rk\, V_i = rk\, V_{i-1} + 1$. As

$rk\, V = r$, r of factors V_i/V_{i-1} are not zero, hence only r elements in $\alpha_1, \ldots, \alpha_n$ are not zero. □

Recall that J_K^S denotes the S–ideal group of K, i.e., the ideal group of K generated by (finite primes) $\mathfrak{p}$ in S; P_K^S denotes the principal S–ideal group, i.e., $P_K^S = P_K \cap J_K^S$. Also, let $r_1(K)$ and $r_2(K)$ denote the numbers of real and complex embeddings (up to conjugacy) of K respectively.

Lemma 5.3. *Let S be a finite set of finite primes. Then K^S is isomorphic to $\mu(K) \cdot M_0$, where $M_0 \subsetneq K^\times$ is free, with a basis of*

$$\{ \epsilon_1, \ldots, \epsilon_{r_1+r_2-1}, \pi_1, \ldots, \pi_{\#S} \}$$

where $\{ \epsilon_1, \ldots, \epsilon_{r_1+r_2-1} \}$ is a basis of units in $K^\times$.

Moreover, the images of π_i in J_K^S form a basis for P_K^S.

Proof. Let $\beta_1, \ldots, \beta_{M=|S|}$ be a basis for P_K^S in J_K^S. From Proposition 5.2, such basis exists, as P_K^S is a sublattice in $J_K^S \cong \mathbb{Z}^n$ of rank $M = |S|$.

Let π_i be an element of K^S which generates β_i for each i.

Thus we have

$$K^S = \langle \pi_1 \rangle \times \ldots \times \langle \pi_M \rangle \times U_K$$

Then by the Dirichlet's Unit Theorem (see [Lang70], [Ne86], [Ne91], [Ra-Va97], ...),

$$U_K = \mu(K) \times \langle \epsilon_1 \rangle \times \ldots \langle \epsilon_{r_1+r_2-1} \rangle$$

Combining the two formulas above, we get the assertion. Done. □

5.3 Effective Method (I)

Again, let l be a rational prime. The following is basic to our method.

Proposition 5.4. *Assume that $\zeta_{lr} \in K$. Let $W \leqq K^S$ is a $\mathbb{Z}$–essential subgroup containing $\mu(K)$, the group of the roots of unity in K, $rk\, W = r_W$, and S a finite set of finite primes*

Then there exists an open subgroup $V = V_{\mathfrak{q}_1} \cap \ldots \cap V_{\mathfrak{q}_\omega}$, $\omega \leqq r_W + 1$ of $\mathbb{I}_K$ separating $\mathbb{I}_K^{lr} W / \mathbb{I}_K^{lr}$, where $\mathfrak{q}_i$ are chosen via the following process:

***Step 1**: Set $A_0 = W$ and $i = 1$.*

***Step 2**: For each i, choose prime $\mathfrak{q}_i \notin S \cup S_l$ of K not splitting in $K(\sqrt[l]{\alpha})/K$ for some $\alpha \in A_{i-1} \subsetneqq W$, $\alpha \notin W^l$.*

***Step 3**: Set*

$$A_i = A_{i-1} \cap K_{\mathfrak{q}_i}^l$$

***Step 4**: If $A_i \neq W^l$, then increase i by 1 and go to Step 2. Otherwise set $\omega = i$.*

Corollary 5.5. *In Proposition 5.4, we can find such open $V_{\mathfrak{f}} = V_{\mathfrak{q}_1} \cap \ldots \cap V_{\mathfrak{q}_\omega}$, with*

$$N\mathfrak{f} \leqq B_l(K, S)^{r_W + 1}$$

where $B_l(K, S)$, defined in Chapter 2, denotes the upper bound of the least

norm of the prime in K outside S and S_l, which does not split completely in $K(\sqrt[l]{h})$ for $h \in K^S$.

Proof of Proposition 5.4. Assume that $\mathfrak{q}_1, \ldots, \mathfrak{q}_\omega$ is chosen as in this proposition, with $A_0 = W$, $A_\omega = W^l$. Later on we will prove that $\omega \leqq r_W + 1$.

First, we prove that $V = V_{\mathfrak{q}_1} \cap \ldots \cap V_{\mathfrak{q}_\omega}$ separates $\mathbb{I}^l W/\mathbb{I}^l$.

Assume that $Z^l \cdot a \in \mathbb{I}^l W \cap V$, where $a \in A_0 = W$ and $Z = Z_{\mathfrak{p}} \in \mathbb{I} = \mathbb{I}_K$. Thus $Z^l_{\mathfrak{q}_i} \cdot a \in V_{\mathfrak{q}_i}$.

If $a \in A_{i-1} \supseteqq W^l$, then

$$Z^l_{\mathfrak{q}_i} \cdot a \in 1 + \mathfrak{q}_i \subseteqq K^{\times l}_{\mathfrak{q}_i}$$

$$\Rightarrow a \in K^{\times l}_{\mathfrak{q}_i}$$

Thus the Kummer extension $K(\sqrt[l]{a})/K$ splits at $\mathfrak{q}_i$, hence $a \in A_i$. Note that $A_i \subsetneqq A_{i-1}$, and $A_\omega = W^l$. Thus, $a \in W^l$ and $Z^l \cdot a \in \mathbb{I}^l$.

Furthermore, $\omega \leqq rk_{\mathbb{Z}/l\mathbb{Z}}(W/W^l)$. In fact, $W \cong \mu(K) \cdot W'$ for some free W' of rank r_W. Therefore, $W/W^l \cong \mu(K)/\mu(K)^l \cdot W'/W'^l$ and $\zeta_l \in K$. Thus $\omega \leqq rk_{\mathbb{Z}/l\mathbb{Z}}(W/W^l) = 1 + r_W$.

In fact, from the discussion above, we see that $A_0 = W \supset A_1 \supset \ldots$ is a strictly descending series of subgroups of W containing W^l, and thus such a series is finite.

Next, prove that V separates $\mathbb{I}^{l^r} W/\mathbb{I}^{l^r}$.

We will prove inductively the following:

For any $0 \leq i \leqq r$

(1) V separates $\mathbb{I}^{l^i}W/\mathbb{I}^{l^i}$;

(2) $\mathbb{I}^{l^i}V$ separates W/W^{l^i}.

Clearly the assertion holds for $i = 0$.

Assume by induction that the assertions above hold for $i-1$, we will prove (1) and (2) for i.

If $x \in W \cap \mathbb{I}^{l^i}V \subset W^{l^{i-1}} = A_0^{l^{i-1}}$, we want to prove $x \in A_s^{l^{i-1}}$ for each $s \leq \omega$. By induction, we may assume that $x \in A_j^{l^{i-1}}$ for every $j < s$. We need to prove that $x \in A_s^{l^{i-1}}$.

Say $x = y^{l^{i-1}} \in \mathbb{I}^{l^i}V$.

Since $V_{\mathfrak{q}_s} \cap K_{\mathfrak{q}_s}^{\times} \subset K_{\mathfrak{q}_s}^{\times l^i}$ as $1 + \mathfrak{q}_s \subset K_{\mathfrak{q}_s}^{\times l^i}$ since $\mathfrak{q}_s \nmid l^i$, we have $y^{l^{i-1}} \in K_{\mathfrak{q}_s}^{\times l^i}$ hence $y\zeta_{l^{i-1}}^{m_0} \in K_{\mathfrak{q}_s}^{\times l}$ for some m_0.

Note that $i \leqq r$, $\zeta_{l^r} \in K$, $\zeta_{l^{i-1}} \in K_{\mathfrak{q}_s}^{\times l}$, $y \in K_{\mathfrak{q}_s}^{\times l}$, and $K(\sqrt[l]{y})/K$ splits at $\mathfrak{q}_s$. Thus $y \in A_s$ and $x \in {A_s}^{l^{i-1}}$.

Since this holds for all $s \leq \omega$, we have $x \in {A_\omega}^{l^{i-1}} = W^{l^i}$, and

$$\begin{aligned} \mathbb{I}^{l^i}W \cap V &\subseteqq \mathbb{I}^{l^i}(W \cap \mathbb{I}^{l^r}V) \\ &\subseteqq \mathbb{I}^{l^i}W^{l^i} = \mathbb{I}^{l^i} \end{aligned}$$

Thus (1) and (2) hold for each $i \leq r$, in particular hold for r. Done. □

In fact, from the process above, we can choose each $\mathfrak{q}_i$ with the norm not exceeding $B_l(K, S)$, So Corollary 5.5 follows.

Proposition 5.6. *Let K be a number field such that $K(\zeta_{l^r})/K$ cyclic, $W \leqq K^S$ a $\mathbb{Z}$–essential subgroup of rank r_W containing $\mu(K)$, the group of the roots of unity in K, and S a finite set of finite primes.*

Let $\mathfrak{q}$ *be an inert prime of* K *in* $K(\zeta_{l^r})$ *outside* S *and* S_l.

Let $V_1 = V_{\mathfrak{q}'_1} \cap \ldots \cap V_{\mathfrak{q}'_\omega}$ *be a standard open subgroup of* $\mathbb{I}_{K(\zeta_{l^r})}$ *that separates* $\mathbb{I}^{l^r}_{K(\zeta_{l^r})} \cdot \tilde{W}/\mathbb{I}^{l^r}_{K(\zeta_{l^r})}$, *while* $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_\omega$ *are selected as in Proposition 5.4 for* $K_1 = K(\zeta_{l^r})$, $\tilde{S} = \{\tilde{\mathfrak{p}}$ *a prime in* K_1, $\tilde{\mathfrak{p}}|\mathfrak{p} \in S\}$ *and* $\tilde{W}$ *is the* $\mathbb{Z}$*–essential closure of* W *in* $\mathbb{I}_{K_1}$.

Then $V = (V_1 \cap \mathbb{I}_K) \cap V_{\mathfrak{q}}$ *separates* $\mathbb{I}^{l^r}_K \cdot W/\mathbb{I}^{l^r}_K$, *and* $N\mathfrak{f}_V \leqq N\mathfrak{q} \cdot N\mathfrak{f}_{V_1}$.

Remark. $r_W = rk\, W = rk\, \tilde{W}$ as $\tilde{W}/W$ is torsion.

Also recall that S_l denotes the set of primes of K dividing l.

Recall that for each open subgroup V in $\mathbb{I}_K$, $\mathfrak{f}_V$ is the smallest cycle such that $V \supseteqq V_{\mathfrak{f}}$.

Corollary 5.7. *In Proposition 5.6, such* V *can be found as*

$$N\mathfrak{f}_V \leqq B_l(K_1, \tilde{S})^{rw+1} \cdot C_{l^r}(K, S)$$

where K_1 *and* $\tilde{S}$ *is as in Proposition 5.6 and* $B_l(K_1, \tilde{S})$ *is as in Corollary 5.5;* $C_{l^r}(K, S)$, *defined in Chapter 2, denotes the least norm of prime of* K *which is inert in the cyclic extension* $K(\zeta_{l^r})/K$ *outside* S *and* S_l.

We will prove Proposition 5.6 in the next section (see Proposition 5.12, Page 124). Similarly one can easily prove Corollary 5.7 from Proposition 5.6.

We conclude this part by a proposition. For the rest of this chapter, unless specified, S might contain infinite primes.

Proposition 5.8. *Let* $m = l^r$. *Let* S *be a finite set of primes,* S' *a finite set of* finite *primes containing* S_f *such that* $l \nmid \#Cl_{K,S'}$. *Then there exists a* $\mathbb{Z}$*-essential subgroup* W *of* $K^{S'}$ *such that*

(1) $W \cdot K^{\times m} \supseteqq P^*(m,S)$, $m = l^r$ *a prime power, where*

$$P^*(m,S) := \{\, x \in K^\times, m \mid v(x) \quad \forall v \text{ finite primes } \notin S \,\}$$

(2) $W \supseteqq K^S$.

(3)

$$\begin{aligned} rk\, W &\leqq rk\, K^S + \gamma_l(C\ell_{K,S}) \\ &= r_1(K) + r_2(K) - 1 + |S_f| + \gamma_l(C\ell_{K,S}) \end{aligned}$$

where

$S_f :=$ *the set consisting of all the finite primes in* S.

$\gamma_l(G) :=$ *the minimal number of generating elements Sylow* l*-subgroup of* G.

Especially, if $l \nmid \#C\ell_{K,S}$, *then* $W = K^S$.

Remark. If G is abelian then denote $\gamma_l(G)$ be the minimal number of generating elements of Sylow l subgroup of G.

For example, if $l = 3$, $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, then $\gamma_3(G) = 2$. If G is cyclic, then for any prime number l, $\gamma_l(G) = 1$; If $\#G$ is prime to l, then also $\gamma_l(G) = 1$.

Proof of the proposition.

Recall that J_K is the group generated by the ideals of $\mathcal{O}_K$ and P_K the subgroup of J_K generated by all principal ideals of $\mathcal{O}_K$. Also, J_K^S is the subgroup of J_K generated by the primes in S and P_K^S is $J_K^S \cap P_K$.

Let P'_K be the inverse image of the Sylow l–subgroup T of $C\ell_K$, i.e.,

$$P'_K = \left\{ \alpha \in J_K \mid \alpha^{l^A} \in P_K \ \texttt{for some} \ A \geq 0 \right\}$$

We can find a **minimal** subset of P'_K consisting of

$$i_1, i_2, \ldots, i_N$$

generating $P'_K J_K^S / P_K J_K^S$, i.e.,

$$\langle i_1 \rangle + \ldots + \langle i_N \rangle + J_K^S P_K \supseteq J_K^S P'_K$$

Note that

$$N = \gamma_l(P'_K J_K^S / P_K J_K^S) = \gamma_l(C\ell_{K,S})$$

since

$$P'_K J_K^S / P_K J_K^S \cong TC\ell_K^S / C\ell_K^S$$

is the Sylow l–subgroup of $C\ell_K / C\ell_K^S = C\ell_{K,S}$ where $C\ell_K^S = J_K^S / P_K^S$.

Furthermore, we can choose representatives i_s in $J_K^{S'} \cap P'_K$. The reason is the following: Since $l \nmid \#C\ell_{K,S'}$, we have

$$P'_K J_K^{S'} / P_K J_K^{S'} \cong TC\ell_K^{S'} / C\ell_K^{S'}$$

which is the Sylow–l subgroup of $C\ell_K / C\ell_K^S = C\ell_{K,S'}$, hence it is trivial. This

means

$$P'_K \subset P_K J_K^{S'} = P_K(P'_K \cap J_K^{S'}).$$

Let

$$J' = J_K^S \times \langle i_1 \rangle \times \langle i_2 \rangle \times \ldots \langle i_N \rangle \subset J_K^{S'}$$

and $E = J' \cap P_K$ a subgroup of J'. Then E admits a basis by Proposition 5.2.

Moreover, since $J'/E \cong J'P_K/P_K \leq C\ell_K$, then E and J' have the same rank $N + |S_f|$.

Hence we may find a basis of E formed by $(e_1), (e_2) \ldots (e_{N+|S_f|})$ with e_s in $K^{S'}$.

Let W_1 be the subgroup of $K^{S'}$ generated by U_K and $e_1, e_2 \ldots e_{N+|S_f|}$, and W the $\mathbb{Z}$–essential closure of W_1. It is easy to see that W_1 consists of those elements in $K^\times$ generating principal fractional ideals in E.

Note that $rk\, W = rk\, W_1 = N + |S_f| + r_1(K) + r_2(K) - 1$. Hence (3) holds.

Since E contains $J_K^S \cap P_K = P_K^S$, by the construction of W_1, W_1 and hence W contain K^S. Then (2) follows.

(1) holds from the following claim:

$$W_1 \cdot K^{\times m} \supseteq P^*(m, S)$$

Now we will prove this claim.

For any $a \in P^*(m, S)$, $m \mid v_\mathfrak{p}(a)$ for each finite prime $\mathfrak{p} \notin S$, and $v_\mathfrak{p}(a) = 0$

for all but a finite number $\mathfrak{p}$.

Define an ideal Λ by:

$$\Lambda := \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{\frac{v_{\mathfrak{p}}(a)}{m}}$$

Thus by the definition of P'_K, $\Lambda^h \in P'_K$ for some integer h not divisible by l.

Hence by the fact that the $i_s, 1 \leq s \leq N$, generate $P'_K J_K^S / P_K J_K^S$,

$$\Lambda^h = \Lambda_1 \cdot (b) \prod_{s=1}^{N} i_s^{\omega_s}$$

for some $\omega_s \in \mathbb{Z}$, $\Lambda_1 \in J_K^S$ and $b \in K^\times$.

Thus

$$(b)^{-1} \Lambda^h \in J_K^S J' = J',$$

and hence

$$(a^h)(b)^{-m} = (\Lambda^h (b)^{-1})^m \prod_{\mathfrak{p} \in S} \mathfrak{p}^{h v_{\mathfrak{p}}(a)} \in J_K^S J' = J'.$$

Thus

$$(a^h b^{-m}) \in J' \cap P_K = E.$$

So by the construction of W_1, we have

$$a^h b^{-m} \in W_1.$$

Hence $a^h \in W_1 K^{\times m}$.

Since h is not divisible by l and h is relative prime to m, we have

$$a \in a^h K^{\times m} \in W_1 K^{\times m} \subset W K^{\times m}.$$

Hence the claim and assertion (1) follow.

Done. □

5.4 Main Results and Proofs

In this section, we will prove the four main theorems in this chapter. After treating the case when $K(\zeta_{l^r})/K$ is cyclic (see Theorem 5.10 and Corollary 5.11, which are in fact Theorem 5–C and 5–A), we will focus on the case when $K(\zeta_{l^r})/K$ is not cyclic. We will state and prove Proposition 5.12 (see Page 124) which is an analog of Proposition 5.6 in this particular case. Finally we will finish proving Theorem 5–D and Theorem 5–B to conclude this section (see Theorem 5.15 and Corollary 5.16).

Before we start, recall that (see Section 1.3)

$$\begin{aligned} P^*(m,S) &= I^*(m,S) \cap K^\times \\ &:= \{\, a \in K^\times, v_{\mathfrak{p}}(a) \text{ is divisible by } m \text{ for all } \mathfrak{p} \notin S \,\} \\ P(m,S) &= I(m,S) \cap K^\times \\ &:= \{\, a \in K^\times, a \in K_{\mathfrak{p}}^{\times m} \text{ for all } \mathfrak{p} \notin S \,\} \end{aligned}$$

Let us begin sketching the main idea of our method.

Let K be a number field, S a finite set of (finite or infinite) primes, $\tilde{P} = \prod_{v \in S} K_v^\times$, P the image of $\tilde{P}$ via the natural embedding into $\mathbb{I}_K$, P_0 a subgroup of P with P/P_0 is of exponent $m = l^r$ which is a prime power.

Assumption 0: $P \cap K^\times \mathbb{I}^m \subsetneqq P_0$.

Note that this assumption holds when $K(\zeta_{l^r})/K$ is cyclic, in particular when l is odd.

Thus under the assumption above, we reduce the effectivity problem of the Grunwald–Wang Theorem to the one of finding an open subgroup V of $\mathbb{I}_K$ such that

$$P \cap K^\times \mathbb{I}^m V \subsetneqq P_0.$$

(see Section 5.1).

Let $x = (x_\mathfrak{p}) \in P \cap K^\times \mathbb{I}^m V$, $x_\mathfrak{p} = 1$ for $\mathfrak{p} \notin S$. Write $x = a \cdot Z^m \cdot R$, where $a \in K^\times$, $Z \in \mathbb{I}$ and $R = (R_\mathfrak{p}) \in V$.

Thus $1 = a \cdot Z_\mathfrak{p}^m \cdot R_\mathfrak{p}$ for $\mathfrak{p} \notin S$, and hence $a \in P^*(m, S)$.

So we want to choose V appropriately to force x to be in P_0.

Let S' be another finite set of finite primes containing S_f such that $\#C\ell_{K,S' \cup S_\infty}$ is not divisible by l. By Proposition 5.8, $a = a_1 \cdot c^m$ for some $c \in K^\times$ and $a_1 \in W \subsetneqq K^{S' \cup S_\infty}$ for some given W satisfying (1), (2) and (3) in Proposition 5.8. We still denote the rank of W as r_W.

Replacing a by a_1, and incorporating c into Z, we get

$$a \in W \subsetneqq K^{S'} = K^{S' \cup S_\infty}.$$

Consequently,

$$x = aZ^m R \in P \cap W\mathbb{I}^m V.$$

Now we prove the following

Lemma 5.9. *Assume that $K(\zeta_m)/K$ is cyclic where m is a prime power. If V_0 separates $W\mathbb{I}^m/\mathbb{I}^m$ where the conductor of V_0 does not involve any prime in S, then $V^* = V_0 \cap V_{\mathfrak{f}}$ separates P/P_0, where $\mathfrak{f}$ is the conductor of P_0 in P.*

Proof.

For any $x \in P \cap W\mathbb{I}^m V^*$, write

$$x = a \cdot Z^m \cdot R, \qquad a \in W,\ Z \in \mathbb{I},\ R \in V^*$$

Without loss of generality, assume that

$$x_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}} \qquad \mathfrak{p} \in S$$

It is clear that $x \in V_0$ since the conductor of V_0 does not involve the primes in S, and the component of x at each $\mathfrak{p} \notin S$ is 1.

Thus since $V_0 \supset V^*$ separates $\mathbb{I}^m W/\mathbb{I}^m$,

$$xR^{-1} = a\, Z^m \in V_0 \cap W\mathbb{I}^m \subset \mathbb{I}^m$$

Taking the local components on both sides at any $\mathfrak{p} \notin S$, and being aware that $x_{\mathfrak{p}} = 1$ outside S. We have $R_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times m}$ outside S.

Also, it is clear that $a \in \mathbb{I}^m$ as $a\, Z^m \in \mathbb{I}^m$, and thus $a \in K_{\mathfrak{p}}^{\times m}$ for any $\mathfrak{p}$.

So $a \in P(m, \emptyset)$. Since $K(\zeta_{l^r})/K$ is cyclic, $a \in K^{\times m}$ by Proposition 1.9 (see Section 1.3).

Set

$$\omega = \prod_{\mathfrak{p} \in S} R_{\mathfrak{p}} \in P$$

and $\omega' = R\omega^{-1}$.

As $R_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times m}$ for $\mathfrak{p} \notin S$, we have $\omega' \in \mathbb{I}^m$.

Note that

$$x\omega^{-1} = xR^{-1}\omega' \in \mathbb{I}^m \cap P \subset P_0$$

and

$$\omega \in V^* \cap P \subset V_{\mathfrak{f}} \cap P \subset P_0$$

Hence we have $x \in P_0$.

□

When $K(\zeta_{l^r})/K$ is cyclic, Assumption 0 holds, and thus we may choose V_0 as in Proposition 5.6 separating $W\mathbb{I}^m/\mathbb{I}^m$, so that

$$N\mathfrak{f}_{V^*} \leqq B_l(K(\zeta_{l^r}), \tilde{S}')^{rw+1} C_{l^r}(K, S') N\mathfrak{f}$$

Furthermore, $W\mathbb{I}^m V/\mathbb{I}^m = K^{\times}\mathbb{I}^m V/\mathbb{I}^m$ separates P/P_0 by the lemma above. We get the following

Theorem 5.10 (The First Main Result). *If $K(\zeta_{l^r})/K$ is cyclic, then*

$$\boldsymbol{BP5} \leqq B_l(K(\zeta_{l^r}), \tilde{S}')^{rw+1} C_{l^r}(K, S') N\mathfrak{f}$$

where $\tilde{S}'$ is the set of primes of $K(\zeta_{l^r})$ over primes in S', which is a given subset of primes of K containing all the finite primes in S and satisfying $l \nmid \#Cl_{K,S\cup S_\infty}$,

$$r_W := \gamma_l(Cl_{K,S\cup S_\infty}) + \#(S \cup S_\infty) - 1,$$

and $\mathfrak{f}$ is the conductor of P_0 in P.

This is Theorem 5–C.

Corollary 5.11. *Assume that $K(\zeta_{l^r})/K$ is cyclic. Then*

$$\boldsymbol{BP1}, \boldsymbol{BP2} \leqq B_l(K(\zeta_{l^r}), \tilde{S}')^{rw+1} C_{l^r}(K, S') \prod_{\mathfrak{p}\in S} N(\chi_{\mathfrak{p}})$$

The above theorem and corollary complete the proof of Theorem 5–A.

Next, consider the case when $m = 2^r$, $r \geq 3$ **and $K(\zeta_{2^r})/K$ is not cyclic.** We need a stronger statement than Proposition 5.6 and Corollary 5.7.

Recall that, s is the largest integer such that $\eta_{2^s} = 2\,Re(\zeta_{2^s})$ is in K,

$$S_0 = \{\, \mathfrak{p} \mid 2, -1, \pm(2 + \eta_{2^s}) \text{ are not squares in } K_{\mathfrak{p}}^{\times} \,\}$$

and

$$a_0 = (1 + \zeta_{2^s})^{2^r} = (\sqrt{-1}\eta_{2^{s+1}})^{2^r} = \eta_{2^{s+1}}^{2^r}$$

Proposition 5.12. *Let $l = 2$, $m = 2^r$. Assume that $K(\zeta_{2^r})/K$ is NOT cyclic.*

(1) *When $S_0 \not\subseteqq S$, Let $W \subseteqq K^{S'}$ a subgroup in $K^\times$ of rank r_W, and let $\tilde{W}$ be the $\mathbb{Z}$-essential closure of W in $K(\zeta_{2^r})$.*

Let $\mathfrak{q}$ be a prime of K in S_0, not in S and

$$V_1 = V_{\mathfrak{q}'_1} \cap \ldots \cap V_{\mathfrak{q}'_\omega}$$

separating $\mathbb{I}^{2^r}_{K(\zeta_{2^r})} \cdot \tilde{W}/\mathbb{I}^{2^r}_{K(\zeta_{2^r})}$, and V_1 is selected, as in Proposition 5.4, for $K_1 = K(\zeta_{2^r})$,

$$\tilde{S}' := \{\, \tilde{\mathfrak{p}} \text{ a prime in } K_1, \tilde{\mathfrak{p}} \text{ dividing } \mathfrak{p} \in S' \,\}$$

where S' be a given larger set of primes of K such that $\#Cl_{K,S'\cup S_\infty}$ is odd.

Then $V = (V \cap \mathbb{I}_K) \cap V_{\mathfrak{q}^\lambda}$ separates $\mathbb{I}^{2^r} \cdot W/\mathbb{I}^{2^r}$ and $N\mathfrak{f}_V \leqq N\mathfrak{f}_{V_1} N\mathfrak{q}^\lambda$, where λ is defined such that $1 + \mathfrak{q}^\lambda \leqq \mathcal{U}^{2^r}_{K_\mathfrak{q}}$.

(2) *When $S_0 \subseteqq S$, let V_1 be chosen above, and let $\mathfrak{q}$ be a prime with divisor $\mathfrak{q}_1$ in $K(\sqrt{-1})$ such that $\mathfrak{q}_1$ is inert in $K(\zeta_{2^r})$.*

Then $V = (V_1 \cap \mathbb{I}_K) \cap V_\mathfrak{q}$ separates $\mathbb{I}^{2^r} \cdot W/\mathbb{I}^{2^r} \cup a_0 \mathbb{I}^{2^r}$.

Propositions 5.6 and 5.12 play a crucial role for our method, and we will prove them together.

Proof of Prop 5.6 and Prop 5.12.

Keep the same notation as in Proposition 5.6 and Proposition 5.12.

We need to prove that $V = (V_1 \cap \mathbb{I}_K) \cap V_{\mathfrak{q}'}$ separates $\mathbb{I}^{l^r}_K W/\mathbb{I}^{l^r}_K$ or $\mathbb{I}^{2^r}_K W/\mathbb{I}^{2^r}_K \cup \mathbb{I}^{2^r}_K a_0^*$. Equivalently, it suffices that $\mathbb{I}^{l^r}_K V$ separates W/W^{l^r} or $W/W^{l^r} \cup a_0 W^{l^r}$ since W is $\mathbb{Z}$–essential. See Section 5.1.

Note that $W \subset K^{S'}$, and $\tilde{S}'$ is the set of primes of $K_1 = K(\zeta_{l^r})$ above the primes in S'. Here recall that S' is some given set of primes of K containing S_f such that $l \nmid \#C\ell_{K,S' \cup S_\infty}$.

Let $\tilde{W}$ be the $\mathbb{Z}$-essential closure of W in ${K_1}^{\tilde{S}'}$. Assume $a \in W \cap \mathbb{I}_K^{l^r} V$.

Then $a \in \mathbb{I}_K^{l^r} V_1 \subset \mathbb{I}_{K_1}{}^{l^r} V_1$. Thus by Proposition 5.4.

$$a \in \tilde{W} \cap \mathbb{I}_{K_1}{}^{l^r} V_1 \subset \tilde{W}^{l^r}$$

Write $a = b^{l^r}$ for some $b \in K(\zeta_{l^r})$,

$b_0 = b, b_1, b_2, \ldots, b_{l^r-1}$ are all l^r-th roots of a in $\tilde{W}$, and $b_i = b\zeta_{l^r}^i$ for all i.

Case (O): $K(\zeta_{l^r}) = K$. Here the assertion follows from Proposition 5.4.

Case (I): $K(\zeta_{l^r})/K$ is cyclic of degree > 1 and some prime $\mathfrak{q}$ of K is inert in $K(\zeta_{l^r})$.

Since $a \in \mathbb{I}_K^{l^r} V \subset \mathbb{I}_K^{l^r} V_\mathfrak{q}$, we have $a \in K_\mathfrak{q}^{\times l^r}$ as $1 + \mathfrak{q} = (1 + \mathfrak{q})^{l^r}$ in $K_\mathfrak{q}^\times$ as $\mathfrak{q} \nmid l$. Thus one of b_i lies in $K_\mathfrak{q}^\times$.

However, for any i, $K(b_i)/K \subset K(\zeta_{l^r})/K$ and $\mathfrak{q}$ is inert in $K(\zeta_{l^r})/K$, thus $\mathfrak{q}$ is also inert in $K(b_i)/K$, and $b_i \notin K_\mathfrak{q}^\times$ if $b_i \notin K^\times$.

Since for some i, b_i is in $K_\mathfrak{q}^\times$, this b_i must be in $K^\times$. So $a \in K^{\times l^r}$. Hence $a \in W^{l^r}$ since W is $\mathbb{Z}$–essential in $K^\times$.

Case (II): $K(\zeta_{2^r})/K$ is not cyclic and $S_0 \not\subseteq S$. Let $\mathfrak{q} \in S_0 - S$ and λ an integer such that $1 + \mathfrak{q}^\lambda \subset \mathcal{U}_{K_\mathfrak{q}}^{2^r}$.

Since the 4-group subextension $K(\sqrt{-1}, \sqrt{2 + \eta_{2^s}})/K$ of K_1/K does not collapse when localized at $\mathfrak{q}$, the decomposition group $G_\mathfrak{q}(K_1/K)$ is the same as $G(K_1/K)$ (see Proposition 1.11 in Section 1.3).

Therefore, we have $a \in {K_{\mathfrak{q}}^{\times}}^{2^r}$ for $a \in \tilde{W}^{2^r} \cap \mathbb{I}_K^{2^r} V_{\mathfrak{q}^\lambda}$.

Then $a = {b_i}^{2^r}$ for some $b_i \in K_{\mathfrak{q}}^{\times}$.

However, $b_i \notin K^{\times} \Rightarrow b_i \notin K_{\mathfrak{q}}^{\times}$ as $G_{\mathfrak{q}} = G$. We conclude that some b_i must be in $K^{\times}$, So $a \in {K^{\times}}^{2^r}$. Hence $a \in W^{2^r}$.

Case (III): $K(\zeta_{2^r})/K$ is not cyclic, and $S_0 \subsetneqq S$.

We will prove:

$$W \cap \mathbb{I}_K^{2^r} \subsetneqq W^{2^r} \cup a_0 W^{2^r}.$$

As we have already had (from Case (I))

$$W \cap \mathbb{I}_K^{2^r} \subsetneqq W^* \cap \mathbb{I}_{K(\sqrt{-1})}^{2^r} V \subseteq W^{*2^r}$$

while W^* denotes the $\mathbb{Z}$-essential closure of W in $(K(\sqrt{-1}))^{\times}$. Thus the remaining is a result of the following lemma (also see Proposition 1.11), which in fact is proved in Chapter 1. □

Lemma 5.13. *Let K be a number field, and s the largest integer such that $\eta_{2^s} \in K$. Assume that $K(\zeta_{2^t}/K)$ is not cyclic.*

Put $a_0 = {\eta_{2^s}}^{2^{t-1}} = \left(\sqrt{-1}\eta_{2^s}\right)^{2^{t-1}} = (1+\zeta_{2^s})^{2^t}$ and assume that $a = b^{2^t}$ for $a \in K^{\times}$ and $b \in K(\sqrt{-1})^{\times}$. Then

$$a \in {K^{\times}}^{2^t} \cup a_0 {K^{\times}}^{2^t}$$

□

Now we work on **Problem V'** in the case when $K(\zeta_{l^r})/K$ is not cyclic.

Let us study the proof of Theorem 5.10. If we have found V separating $W\mathbb{I}^{2^r}/\mathbb{I}^{2^r}$, and $P(m,S) = K^{\times m}$ holds, then everything in the proof still works when $K(\zeta_{2^r})/K$ is **not** cyclic. This happens in the case $S_0 \not\subseteq S$, when we select $V^* = V_0 \cap V_{\mathfrak{f}}$ where $\mathfrak{f}$ is the conductor of P_0 in P, and V_0 is selected as in Proposition 5.12.

Note that in this case, the fact $P(m,S) = K^{\times}$ comes from Proposition 1.11.

Then it remains for us to consider the special case. Recall that in the special case, $S_0 \subseteq S$. Also, we need the condition $a_0^* \in P_0$.

Recall that a_0^* has local components a_0 at the primes in S_0 and 1 elsewhere. Also note that $a_0 \in K_{\mathfrak{p}}^{\times m}$ for $\mathfrak{p} \notin S_0$, hence $a_0 \cdot \mathbb{I}^{2^r} = a_0^* \cdot \mathbb{I}^{2^r}$.

Lemma 5.14. *Let $m = 2^r$. Assume that $K(\zeta_m)/K$ is* not *cyclic, $S_0 \subset S$ and $a_0^* \in P_0$. If V_0 separates $W\mathbb{I}^m/\mathbb{I}^m \cup a_0\mathbb{I}^m$, where the conductor of V_0 does not involve any prime in S, then $V^* = V_0 \cap V_{\mathfrak{f}}$ separates P/P_0, where $\mathfrak{f}$ is the conductor of P_0 in P.*

Proof.

The proof of this lemma is almost the same as the proof of Lemma 5.9.

Similarly, For any $x = (x_{\mathfrak{p}}) \in P \cap W\mathbb{I}^m V^*$, write

$$x = a \cdot Z^m \cdot R, \qquad a \in W,\ Z \in \mathbb{I},\ R = (R_{\mathfrak{p}}) \in V^*$$

Without loss of generality, assume that

$$x_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}} \qquad \mathfrak{p} \in S$$

It is clear that $x \in V_0$ by the same reason as in the proof of Lemma 5.9.

Thus since $V_0 \supset V^*$ separates $\mathbb{I}^m W/\mathbb{I}^m \cup a_0\mathbb{I}^m$,

$$xR^{-1} = a\,Z^m \in V_0 \cap W\mathbb{I}^m \subset \mathbb{I}^m \cup a_0\mathbb{I}^m$$

Taking the local components on both sides at any $\mathfrak{p} \notin S$, and being aware that $x_{\mathfrak{p}} = 1$ outside S and $a_0\mathbb{I}^m = a_0^*\mathbb{I}^m$. We have $R_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times m}$ outside S.

Also, it is clear that $a \in \mathbb{I}^m \cup a_0^*\mathbb{I}^m$ and thus $a \in K_{\mathfrak{p}}^{\times m}$ for any finite $\mathfrak{p} \notin S_0$.

So $a \in P(m, S_0)$, hence $a \in K^{\times m} \cup a_0 K^{\times m}$ by Proposition 1.11 (see Section 1.3).

Set

$$\omega = \prod_{\mathfrak{p} \in S} R_{\mathfrak{p}} \in P$$

and $\omega' = R\omega^{-1}$.

As $R_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times m}$ for $\mathfrak{p} \notin S$, we have $\omega' \in \mathbb{I}^m$.

Note that

$$x\omega^{-1} = xR^{-1}\omega' \in (\mathbb{I}^m \cup a_0^*\mathbb{I}^m) \cap P \subset P_0$$

and

$$\omega \in V^* \cap P \subset V_{\mathfrak{f}} \cap P \subset P_0$$

We have $x \in P_0$.

□

From this lemma, we have $P \cap K^{\times}\mathbb{I}^m V^* = P \cap W\mathbb{I}^m V^* \subsetneqq P_0$ where $V^* = V_0 \cap V_{\mathfrak{f}}$, V_0 is found via Proposition 5.12 such that V_0 does not involve primes in S and V_0 separating $W \cdot \mathbb{I}^{2^r}/a_0 \cdot \mathbb{I}^{2^r} \cup \mathbb{I}^{2^r}$, and $\mathfrak{f}$ is the conductor of P_0 in P.

Furthermore,

$$N\mathfrak{f}_{V^*} \leqq B_2(K(\zeta_{2^r}), \tilde{S}')^{rw+1} \cdot C_{2^r}(K, S') \cdot N\mathfrak{f}$$

Then we get the following main theorem of the special case. Here we abuse the notation; we denote $C_{2^r}(K, S)$ as the least bound of the norm of the finite prime in K (if $K(\zeta_{2^r})/K$ is cyclic) or $K(\sqrt{-1})$ (otherwise) which is not dividing any primes in S or 2, and is inert in $K(\zeta_{2^r})$.

Theorem 5.15. *If $m = 2^r$, $K(\zeta_{2^r})/K$ not cyclic, $S_0 \subsetneqq S$ and $a_0^* \in P_0$, then*

$$\boldsymbol{BP5} \leqq B_2(K(\zeta_{2^r}), \tilde{S}')^{rw+1} \cdot C_{2^r}(K, S') \cdot N\mathfrak{f}.$$

If $\mathfrak{p}_0 \in S_0 - S \neq \emptyset$, then

$$\boldsymbol{BP5} \leqq B_2(K(\zeta_{2^r}), \tilde{S}')^{rw+1} \cdot {\mathfrak{p}_0}^{\lambda} \cdot N\mathfrak{f},$$

where λ is the smallest integer such that $1 + {\mathfrak{p}_0}^{\lambda} \subset \mathcal{U}^{2^r}_{K_{\mathfrak{p}_0}}$.

This is Theorem 5–D.

Corollary 5.16. *If $K(\zeta_{2^r})/K$ is not cyclic, $S_0 \subsetneqq S$, and*

$$\prod_{v \in S_0} \chi_v(a_0) = 1,$$

then

$$\textbf{\textit{BP1}}, \textbf{\textit{BP2}} \leqq B_2(K(\zeta_{2^r}), \tilde{S}')^{r_W+1} \cdot C_{2^r}(K, S') \cdot N\mathfrak{f},$$

where $r_W = \gamma_2(C\ell_{K,S\cup S_\infty}) + \#(S \cup S_\infty) - 1$, and $\mathfrak{f}$ is the product of the conductors of χ_v.

If $\mathfrak{p}_0 \in S_0 - S \neq \emptyset$, then

$$\textbf{\textit{BP1}}, \textbf{\textit{BP2}} \leqq B_2(K(\zeta_{2^r}), \tilde{S}')^{r_W+1} \cdot {\mathfrak{p}_0}^{\lambda} \cdot N\mathfrak{f},$$

where λ is the smallest integer such that

$$1 + {\mathfrak{p}_0}^{\lambda} \subset \mathcal{U}^{2^r}_{K_{\mathfrak{p}_0}}.$$

The above theorem and corollary complete the proof of Theorem 5–B.

5.5 Proofs of Theorem G and Corollary H

In this part, we will plug in the results in Section 2.4 to prove Theorem G and Corollary H of page xvii.

Theorem G can be directly deduced from Theorem 5–A and 5–B. In fact, $C(K, S')$ is absorbed by $B(K_1, \tilde{S}')^{r_W+1}$. Also, note that if (SS′) holds, then

$\lambda \leq e(\mathfrak{p}_0/2)(r+1)$ $(r > 2)$ since

$$1 + \mathfrak{p}_0^{e(\mathfrak{p}_0/2)(r+1)} \subset \mathcal{U}_{K_{\mathfrak{p}_0}}^{2^r}$$

where $e(\mathfrak{p}_0/2)$ is the ramification index of $\mathfrak{p}_0$ over 2 (see Proposition 1.2 and its proof). Thus, ${N\mathfrak{p}_0}^{\lambda}$ is also absorbed by $B(K_1, \tilde{S}')^{rw+1}$.

Corollary H is easy to get from Theorem G as $\mathbb{Q}$ has class number 1 and $r_W + 1 = |S \cup S_\infty|$. It gives a good least bound of N such that p is not an l–th power and $l^r \mid \phi(N)$.

Chapter 6 Results assuming GRH

From now on, we assume GRH (Grand Riemann Hypothesis) which asserts that for a number field L, the Dedekind zeta function ζ_L has no nontrivial zeros beyond the critical line $Re\, s = \frac{1}{2}$ for a number field L. Proving such an assertion is of course far beyond reach at the moment.

We will prove Theorem I which answers the effectivity problem of the Grunwald–Wang Theorem in the general case assuming GRH.

Also, a sharp result for the quadratic extension case assuming GRH will also be given.

6.1 S–versions of the Chebotarev Density Theorem with GRH

In this section, we will prove two distinct results which are the S–effective versions of the Chebotarev Density Theorem with GRH. They are analogies to the results in [L-O77], [L-M-O79] and [KM94].

Throughout this section, for any number field L, d_L denotes the discriminant of L, and $d_{L/K}$ denotes the relative discriminant of L over a subfield K.

Theorem 6–A. *Let L/K be a Galois extension of number fields of degree n, S a finite set of primes of K. If we assume the* GRH, *then there is a prime*

ideal $\mathfrak{p}$ *of* K *such that* (1) $\mathfrak{p}$ *is unramified in* L, *and* $\mathfrak{p}$ *is of degree* 1 *over* $\mathbb{Q}$; (2) $\mathfrak{p} \notin S$; (3) $\mathfrak{p}$ *does not split in* L; *and* (4)

$$N_{K/\mathbb{Q}}\mathfrak{p} \leqq C_0 \left\{ \left(\frac{1}{n} \log d_L \right)^2 + \log N_S \right\}$$

where C_0 *is an absolute constant.*

This result is an S–analog to the main theorem in [KM94]. It is slightly stronger than the S–version (Theorem 2.6.) in the basic paper of Serre ([Se81]).

Theorem 6–B. *Let* L/K *be a Galois extension of number fields of degree* n, S *a finite set of primes of* K, *and* C *a conjugacy class in* $Gal(L/K)$. *Assuming the* GRH, *then there is a prime ideal* $\mathfrak{p}$ *of* K *such that* (1) $\mathfrak{p}$ *is unramified in* L, *and* $\mathfrak{p}$ *is of degree* 1 *over* $\mathbb{Q}$; (2) $\mathfrak{p} \notin S$; (3)

$$\left(\frac{L/K}{\mathfrak{p}} \right) = C$$

and (4)

$$N_{K/\mathbb{Q}}\mathfrak{p} \leqq C_0 \left\{ (\log d_L)^2 + n \log N_S \right\}$$

where C_0 *is an absolute constant.*

This theorem is an S–analog of the main theorem in [L-O77].

Now we prove Theorem 6–A and 6–B. Keep the notations as in Chapter 2. Assuming GRH, we need only to use the first kernel function $k_1(s)$.

Lemma 6.1. *Assuming* GRH, *we have*

$$k_1(\rho) - \sum_{\rho} |k_1(\rho)| = \left(\log \frac{y}{x}\right)^2 + O(x^{-1}) \log d_L$$

where the sum runs over all the nontrivial zeros ρ *of* $\zeta_L(s)$.

The proof is standard (see [KM94], [L-M-O79]). We give an argument for completeness.

Proof. Consider the sum over nontrivial $\rho = \beta + i\gamma$. Assume that $y >> x$, we have

$$\begin{aligned}
\sum_{\rho} |k_1(\rho)| = \sum_{\beta=\frac{1}{2}} |k_1(\rho)| &\leq \sum_{\beta=\frac{1}{2}} \frac{x^{-1}}{|\rho - 1|^2} \\
&<< \int_{1/2}^{\infty} \frac{x^{-1}}{r^2} dn(r;1) \\
&<< x^{-1}(4 + 2\log d_L) \\
&<< x^{-1} \log d_L
\end{aligned}$$

Done. □

Now we begin proving Theorem 6–B by applying the standard model in Section 2.2. From Lemma 2.8 and Lemma 6.1, we get

$$\begin{aligned}
nI_1 &\geq k_1(1) - \sum_{\rho} |k_1(\rho)| - c_6 \left\{ n_L k_1(0) + k_1(-\frac{1}{2}) \log d_L \right\} \\
&\geq \left(\log \frac{y}{x}\right)^2 + O(x^{-1}) \log d_L - c_6' x^{-2} \log d_L \\
&= \left(\log \frac{y}{x}\right)^2 + O(x^{-1}) \log d_L
\end{aligned}$$

Furthermore, $I_1 - \tilde{I}_1$ is bounded by the following:

$$\begin{aligned} I_1 - \tilde{I}_1 &= S_{1,1} + S_{1,2} + S_{1,3} \\ &= O\left(\frac{1}{nx^2}\left(\log\frac{y}{x}\right)\log d_L\right) \\ &+ O\left(\frac{1}{x^2}\left(\log\frac{y}{x}\right)\log N_S\right) \\ &+ O\left(n_K\frac{\left(\log\frac{y}{x}\right)(\log y)}{x\log x}\right) \end{aligned}$$

Here $n = [L : K]$.

If $N\mathfrak{p} > y^2$ for $\mathfrak{p} \in P_1(C, S)$, i.e., for $\mathfrak{p}$ satisfying (1)–(3) in Theorem 6–B, then $\tilde{I}_1 = 0$. Then set $x = \alpha\left(\log d_L + \sqrt{(n\log N_S)}\right)$ and $y = \beta x$ for sufficiently large β and $\alpha > (\log\beta)^2$.

Recall that $n = [L : K]$ and $n_L = [L : \mathbb{Q}]$, we have,

$$\begin{aligned} n|I_1| &= O\left(\frac{1}{\alpha^2(\log d_L)^2}(\log\beta)\log d_L\right) \\ &+ O\left(n\frac{1}{\alpha^2(n\log N_S)}(\log\beta)\log N_S\right) \\ &+ O\left(n_L\frac{(\log\beta)(\log\beta + \log x)}{x\log x}\right) \end{aligned}$$

is bounded as $n_L << \log d_L$. As β goes to infinity, we get $(\log\beta)^2 + o(1) = O(1)$ which also goes to infinity, contradiction.

So Theorem 6–B holds.

Next we will prove Theorem 6–A. We need to use a different model which is the same as in [KM94].

Let

$$J_K = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} -\frac{\zeta_K'}{\zeta_K}(s)k_1(s;x,y)ds$$

On one hand, by using Lemma 2.8,

$$J_K = \left(\log\frac{y}{x}\right)^2 - \sum_\rho k_1(\rho) + O(n_K k_1(0) + k_1(-\frac{1}{2})\log d_K)$$

where the sum runs over the zeros of $\zeta_K(s)$.

By Lemma 6.1, assuming GRH,

$$J_K = \left(\log\frac{y}{x}\right)^2 + O(x^{-1}\log d_K).$$

Furthermore,

$$J_K = \sum_{\mathfrak{p},m} \log(N\mathfrak{p})\hat{k}_1(N\mathfrak{p}^m;x,y).$$

Let

$$\tilde{J}_K = \sum_{\mathfrak{p}\notin S}{}' \log(N\mathfrak{p})\hat{k}_1(N\mathfrak{p};x,y),$$

where $\sum_{\mathfrak{p}\notin S}{}'$ runs over the primes unramified in L of degree 1 and outside S.

Thus

$$\begin{aligned} J_K - \tilde{J}_K &= S_{1,1} + S_{1,2} + S_{1,3} \\ &= O\left(\frac{1}{nx^2}\left(\log\frac{y}{x}\right)\log d_L\right) \\ &+ O\left(\frac{1}{x^2}\left(\log\frac{y}{x}\right)\log N_S\right) \\ &+ O\left(n_K\frac{\left(\log\frac{y}{x}\right)(\log y)}{x\log x}\right) \end{aligned}$$

Set $x = \alpha\left(\frac{1}{n}\log d_L + \sqrt{\log N_S}\right)^2$, $y = \beta x$ and assume that $\alpha \geq (\log\beta)^{2+\epsilon}$. Then it is easy to check that

$$J_K - \tilde{J}_K = O(\frac{1}{(\log\beta)^{\epsilon}})$$

If $N\mathfrak{p} > y^2$ for all $\mathfrak{p}$ satisfying (1) and (2) in Theorem 6–A, then

$$\tilde{J}_K - \frac{1}{n}J_L \leq 0$$

Thus

$$\left(\frac{n-1}{n}\right)(\log\beta)^2 + O((\log\beta)^{-2-\epsilon}) + O((\log\beta)^{-\epsilon}) \leq 0$$

as $\frac{x^{-1}}{n}\log d_L << \frac{1}{\alpha}$.

If β is large enough, this inequality will fail.

Thus, there is a $\mathfrak{p}$ satisfying (1) and (2) with

$$N\mathfrak{p} << y^2 << O\left(\left(\frac{1}{n}\log d_L\right)^2 + \log N_S\right).$$

Done. □

6.2 Results with GRH

First of all, we do some calculating. Throughout this part, $\tilde{S}$ denotes the set of primes of $K(\zeta_{l^r})$ over the primes in S.

Recall that If $\zeta_l \in K$,

$$B_l(K,S,\alpha) := \begin{cases} \text{the least bound for } N\mathfrak{q} \text{ such that} \\ \text{(i) } \mathfrak{q} \text{ a prime of } K \text{ not splitting in } K(\sqrt[l]{\alpha}); \\ \text{(ii) } \mathfrak{q} \nmid l \text{ and } \mathfrak{q} \notin S. \end{cases}$$

$$B_l(K,S) := \max_{\alpha \in K^S, \alpha \notin (K^S)^l} B_l(K,S,\alpha).$$

The next symbol has multiple meaning:

If $K(\zeta_{l^r})/K$ is cyclic, then

$$C_{l^r}(K,S) := \begin{cases} \text{the least bound for } N\mathfrak{q} \text{ such that} \\ \text{(i) } \mathfrak{q}, \text{ a prime of } K \text{ inert in } K(\zeta_{p^r}); \\ \text{(ii) } \mathfrak{q} \nmid p \text{ and } \mathfrak{q} \notin S. \end{cases}$$

If $K(\zeta_{l^r})/K$ is not cyclic, so that $l = 2$ and $r \geq 3$.

$$C_{2^r}(K,S) := \begin{cases} \text{the least bound for } N\mathfrak{q}' \text{ such that} \\ \text{(i) } \mathfrak{q}', \text{ a prime of } K_1 = K(\sqrt{-1}) \text{ inert in } K(\zeta_{2^r}); \\ \text{(ii) } \mathfrak{q}' \nmid 2 \text{ and } \mathfrak{q}' \notin S' \text{ while } S' = \{\, \mathfrak{p}' \mid \mathfrak{p} \in S \,\}. \end{cases}$$

(1) Calculation of $B_l(K(\zeta_{l^r}), \tilde{S})$ (with GRH).

Set $K_1 = K(\zeta_{l^r})$. For any $\alpha \in {K_1}^{\tilde{S}}$ which is not an l-th power in K_1. Let $L_1 = K_1(\sqrt[l]{\alpha})$. From Section 2.4 we know that $\log d_{K_1} \leq [K_1 : K] \log d_K +$

$r\, n_K[K_1 : K] \log l$ and, by Lemma 2.10 on Page 68,

$$\log d_{L_1} + l \log N_{\tilde{T}_0} \leq [K_1 : K] \{ l \log d_K + (l-1) \log N_{T_1} + (r+1) l\, n_K \log l \}$$

where $\tilde{T}_1 = \{ \tilde{\mathfrak{p}} \mid \quad l \nmid v_{\tilde{\mathfrak{p}}}(\alpha) \}$, $\tilde{T}_2 = \tilde{S} - \tilde{T}_1$, and $\tilde{T}_0$ the set of primes of K_1 dividing l which does not ramify in $L_1 = K_1(\sqrt[l]{\alpha})$.

Thus assuming GRH, and applying Theorem 6–A one gets

$$\begin{aligned} B_l(K_1,\tilde{S},\alpha) &= B_l(K_1, \tilde{T}_2 \cup \tilde{T}_0, \alpha) \\ &<< \left\{ [K_1 : K] \log d_K + \log N_{\tilde{T}_1} - \log N_{\tilde{T}_0} + (1+r)\, n_K [K_1 : K] \log l \right\}^2 \\ &\quad + l \log N_{\tilde{T}_2} + l \log N_{\tilde{T}_0} \\ &<< \{ [K_1 : K] \log d_K + \log N_{\tilde{S}} + (1+r)\, n_K [K_1 : K] \log l \}^2 \end{aligned}$$

Thus we have

$$B_l(K_1, \tilde{S}) << \{ [K_1 : K] (\log d_K + \log N_S + n_K (1+r) \log l) \}^2 \qquad (6\text{-}2\text{-}1)$$

(2) Calculation of $C_{l^r}(K, S)$ (with GRH).

From Section 2.4, in any case, we can apply Theorem 6–B for K_1/K. So we have

$$C_{l^r}(K, S) << \{ [K_1 : K] (\log d_K + r\, n_K \log l) \}^2 + [K_1 : K] \log N_S \qquad (6\text{-}2\text{-}2)$$

Plugging in the results above in Theorems 5–A and 5–B, one can easily get Theorem I. (Note that we assume that if $l = 2$ and $K(\zeta_{2^r})/K$ is not cyclic, then $S_0 \subset S$.)

6.3 The Quadratic Extension Case with GRH

First we recall Question Z (Section 3.1):

Let $S = \{ p_1, p_2, \ldots, p_M \}$ be a finite set of finite primes.

Find α, such that $p_1, p_2, \ldots, p_M \nmid \alpha$, and 4 divides $\alpha - 1$ if $p_i = 2$ for some i, and

$$\left(\frac{\alpha}{p_i} \right) = (-1)^{\epsilon_i}$$

$\epsilon_i = 0$ or 1 given.

Define $\left(\frac{\alpha}{2} \right) = (-1)^{\frac{\alpha^2-1}{2}}$ be the quadratic residue symbol of α in $\mathbb{Q}_2$.

Thus

$$\left(\frac{\alpha}{2} \right) = \begin{cases} 1 & \text{if } \alpha \equiv 1 \pmod 8 \\ -1 & \text{if } \alpha \equiv 5 \pmod 8 \end{cases}$$

Also find the least bound of such $|\alpha|$.

The **answer** to this question with GRH is the following:

Assuming GRH, we can find such prime α such that

$$\begin{aligned} |\alpha| &\leqq c'_{14}(2^{|S|} + 2^{|S|-1} \log_2 N_S)^2 \\ &<< (2^{|S|} \log_2 N_S)^2 \end{aligned}$$

We can also find such α with $-\alpha$ is a prime, and

$$|\alpha| << (2^{|S|} \log_2 N_S)^2$$

Proposition 6.2 (Assuming GRH**).** *For $m = 2$, $K = \mathbb{Q}$, all χ_v for $v \in S$ finite, are unramified. Then*

$$\boldsymbol{BP1}, \boldsymbol{BP2} << \left(2^{|S|} \log_2 N_S\right)^2$$

Proposition 6.3 (with GRH**).** *Let $m = 2$ and $K = \mathbb{Q}$. Then*

$$\boldsymbol{BP1}, \boldsymbol{BP2} << \left(2^{|S|} \log_2 N_S\right)^2 \cdot \prod_p N(\chi_p)$$

This is Theorem J.

Proof of Question Z and Prop 6.2., with GRH.

Let

$$L_i = \begin{cases} \mathbb{Q}(\sqrt{p_i}) & \text{if } p_i \equiv 1 \pmod 4 \text{ or } p_i = 2; \\ \mathbb{Q}(\sqrt{-p_i}) & \text{if } p_i \equiv 3 \pmod 4. \end{cases}$$

and $L_0 = \mathbb{Q}(\sqrt{-1})$

Put $L = \prod_{i=0}^{N} L_i$, so that Lemma 3.1 applies.

Note that

$$G(L/\mathbb{Q}) = \prod_i G(L_i/\mathbb{Q})$$

Thus, by [L-O77], there exists a prime number p corresponding to a given

element in $G(L/\mathbb{Q})$ under the Artin reciprocity map such that

$$\begin{aligned} p &\leqq c'_{14}(\log_2 d_L)^2 \\ &\leqq c'_{14}(2^{|S|} + 2^{|S|+1}\log_2 N_S)^2 \\ &<< (2^{|S|}\log_2 N_S)^2 \end{aligned}$$

where from Lemma 1.18 (see Section 1.5),

$$\frac{\log_2 d_L}{2^{|S|+1}} \leqq \prod_{i=0}^{|S|} \frac{\log_2 d_{L_i}}{2} \leqq 1 + \frac{1}{2}\log_2 N_S$$

as $d_{L_i} = p_i$ if $2 \mid p_i$, $d_{L_0} = 4$, $d_{L_i} = 8$ if $p_i = 2$.

Furthermore, we will describe below the conditions (2) and (2′), and prove that if (2) holds then $\left(\frac{p}{p_i}\right) = (-1)^{\epsilon}$, and that if (2′) holds then $\left(\frac{-p}{p_i}\right) = (-1)^{\epsilon}$. So that, by the discussion above, we can finish the proof of the answer to the Question Z with GRH.

Condition (2):

$$\left(\frac{L_i/K}{p}\right) = \begin{cases} \left(\frac{p_i}{p}\right) = (-1)^{\epsilon+1} & \text{if } p_i \equiv 3 \pmod 4; \\ \left(\frac{\pm p_i}{p}\right) = (-1)^{\epsilon} & \text{if } p_i \equiv 1 \pmod 4 \text{ or } p_i = 2. \end{cases}$$

$$\left(\frac{L_0/K}{p}\right) = \left(\frac{-1}{p}\right) = 1$$

Condition (2′):

$$\left(\frac{L_i/K}{p}\right) = \left(\frac{\pm p_i}{p}\right) = \begin{cases} (-1)^{\epsilon+1} & \text{if } p_i \equiv 3 \pmod 4; \\ (-1)^{\epsilon} & \text{if } p_i \equiv 1 \pmod 4 \text{ or } p_i = 2. \end{cases}$$

$$\left(\frac{L_0/K}{p}\right) = \left(\frac{-1}{p}\right) = -1$$

In fact, (2) implies $p \equiv 1 \pmod 4$.

Thus by Prop 1.20 on page 39, and the Gauss reciprocity formula, we have

$$\begin{aligned} \left(\frac{p}{p_i}\right) = \left(\frac{p_i}{p}\right) = \left(\frac{L_i/K}{p}\right) = (-1)^{\epsilon} \qquad & \text{if } p_i \equiv 1 \pmod 4; \\ \left(\frac{p}{p_i}\right) = \left(\frac{p_i}{p}\right) = \left(\frac{-p_i}{p}\right) & \\ = \left(\frac{L_i/K}{p}\right) = (-1)^{\epsilon} \qquad & \text{if } p_i \equiv 3 \pmod 4; \\ \left(\frac{p}{p_i}\right) = \left(\frac{2}{p}\right) = \left(\frac{L_i/K}{p}\right) = (-1)^{\epsilon} \qquad & \text{if } p_i = 2. \end{aligned}$$

Moreover, (2′) implies $p \equiv 3 \pmod 4$. Thus by Prop 1.20, and the Gauss reciprocity formula, we have

$$\begin{aligned} \left(\frac{-p}{p_i}\right) = \left(\frac{p}{p_i}\right) = \left(\frac{p_i}{p}\right) & \\ = \left(\frac{L_i/K}{p}\right) = (-1)^{\epsilon} \qquad & \text{if } p_i \equiv 1 \pmod 4; \\ \left(\frac{-p}{p_i}\right) = -\left(\frac{p}{p_i}\right) = \left(\frac{p_i}{p}\right) = -\left(\frac{-p_i}{p}\right) & \\ = -\left(\frac{L_i/K}{p}\right) = -(-1)^{\epsilon+1} = (-1)^{\epsilon} \qquad & \text{if } p_i \equiv 3 \pmod 4; \\ \left(\frac{-p}{p_i}\right) = \left(\frac{2}{p}\right) = \left(\frac{L_i/K}{p}\right) = (-1)^{\epsilon} \qquad & \text{if } p_i = 2. \end{aligned}$$

Now Prop 6.2 is clear. The proof is the same as Prop 3.3 (see page 73). □

Proof of Prop 6.3.

Without loss of generality, assume that $\infty \in S$. Use the reduction process (2) as in Lemma 3.5.

By Prop 6.2, we can find a quadratic character $\tilde{\chi}$ such that $\tilde{\chi}|_p = \chi_p \cdot \chi_0|_p^{-1}$ for all $p \in S$ and

$$N(\tilde{\chi}) = N\mathfrak{f}_{\tilde{\chi}} << (2^{|S|} \log_2 N_S)^2$$

Thus note that

$$\mathfrak{f}((\chi^*)_p) = \begin{cases} p & \text{if } p \neq 2, \infty; \\ 1, 4 \text{ or } 8 & \text{if } p = 2 \text{ or } \infty. \end{cases}$$

Thus

$$\mathfrak{f}(\chi_0) \quad \text{divides} \quad \infty \cdot \prod_{p \in S'} \mathfrak{f}(\chi_p)$$

Therefore,

$$\begin{aligned} N(\chi_1) &\leqq N(\tilde{\chi}) N(\chi_0) \\ &<< (2^{|S|} \log_2 N_S)^2 \cdot 8 \prod_{p \in S} N(\chi_p) \\ &<< (2^{|S|} \log_2 N_S)^2 \cdot \prod_{p \in S} N(\chi_p) \end{aligned}$$

□

Bibliography

[A-T68] E. Artin and J. Tate, *Class field theory*, Harvard University 1968

[Gr33] W. Grunwald, *Ein Allgemeines Existenztheorem für algebraicshe Zahlkörper*, Journ. f.d. reine u. angewante Math. **169**, (1933) 103–107

[Gu48] A.P. Guinand, *A summation formula in the theory of prime numbers*, Proc. London Math. Soc. (2) **50**, 107–119 (1948)

[H-Ra95] J. Hoffstein and D. Ramakrishnan, *Siegel Zeros and Cusp Forms*, IMRN(1995), No.**6**, 279–308

[KM94] V.K. Murty, *The least prime which does not split completely*, (Communicated by Dinakar Ramakrishnan) Forum Math.**6**(1994), 555–565

[L-O77] J.C. Lagarias, A.M. Odlyzko, *Effective Version of the Chebotarev Density Theorem* Algebraic Number Fields, L-functions and Galois Properties (edit by A.Frölich) 409–464 (1977)

[L-M-O79] J.C. Lagarias, H.L. Montgomery and A.M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Inventiones. Math. **54** 271–196

[Land27] E. Landau, *Algebraische Zahlen*, Göttingen 1927

[Lang70] S. Lang, *Algebraic number theory*, Springer-Verlag, 1970

[Lo-Ro2000] F. Lorenz and P. Roquette, *The Theorem of Grunwald–Wang in the setting of Valuation Theory*, Fields Institute Communication

[Ne86] J. Neukirch, *Class field theory*, Springer-Verlag, 1970

[Ne91] J. Neukirch, *Algebraic number theory*, Springer, 1991

[Od77] A.M. Odlyzko, *On conductors and discriminants*, Algebraic Number Fields, L-functions and Galois Properties (edit by A.Frölich) 377–407 (1977)

[Ra-Va97] D. Ramakrishnan, R.J. Valenza, *Fourier Analysis on Number Fields* Springer, 1999

[Se81] J.–P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ.Math. I.H.E.S., n **54** (1981) 123–201

[Se85] J.–P. Serre, *Œ UVRES Collected Papers*, Vol III, Springer Verlag. No.125. (563–641)

[Stk74] H. Stark, *Some effective cases of the Brauer–Siegel Theorem*, Inventiones Math. (**23**) 1974, 135–162

[Vo99] J. Voloch, *Chebyshev's method for number fields*, 1999

[Va-Vo99] J.D. Vaaler, J. Voloch, *The Least Nonsplit Prime in Galois extensions of* $\mathbb{Q}$, 1999

[Wa48] Sh. Wang, *A counter example to Grunwald's theorem*, Annals of Math. **49** (1948) 1008–1009

[Wa50] Sh. Wang, *On Grunwald's theorem*, Annals of Math. **51** (1950) 471–484

[We52] A. Weil *Sur les "formules explicites" de la théorie des nombres premiers*, Comm. Sem. Math. Lund, 252–265 (1952)

[Wh42] G. Whaples, *No-analytic class field theory and Gruenwald's Theorem*, Duke Math. J. **9** (1942) 455–473