KURODA'S CLASS NUMBER FORMULA

A THESIS
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE

By
Hatice Şahinoğlu
June, 2007

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Associate Prof. Dr. Franz Lemmermeyer (Supervisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Alexander Klyachko

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Ali Aydın Selçuk

Approved for the Institute of Engineering and Science:

Prof. Dr. Mehmet B. Baray
Director of the Institute Engineering and Science

ABSTRACT

KURODA'S CLASS NUMBER FORMULA

Hatice Şahinoğlu
M.S. in Mathematics
Supervisor: Associate Prof. Dr. Franz Lemmermeyer
June, 2007

In number theory theory, the class number of a field is a significant invariant. All over the time, people have come up with formulas for some cases and in this thesis I will discuss a proof of a class number formula for V_4-extensions.

Keywords: Class Field Theory, Class number.

ÖZET

KURODA NIN SINIF SAYISI FORMÜLÜ

Hatice Şahinoğlu
Matematik, Yüksek Lisans
Tez Yöneticisi: Associate Prof. Dr. Franz Lemmermeyer
Haziran, 2007

Sayı teorisinde bir cisimin sınıf sayısı önemli bir sabittir. Zaman içinde bazi cisim genişlemeleri için sınıf sayısı hesaplandı. Bu tezde ise Klein -4 group cisim genişlemeleri için Kuroda tarzı sınıf sayısı formülünü ele alacağız.

Anahtar sözcükler: Sınıf sayısı, Sınıf cismi teorisi.

Acknowledgements

I would like to express my sincere gratitude to my supervisor Franz Lemmermeyer who showed an endless tolerance and patience to my always repeating questions and effort to help me have a thesis.

I would like to give my thanks to Murat Altunbulak who helped me a lot with the computer stuff.

I would like to mention about the financial support of TUBITAK during the formation of my thesis, and give my gratitude to TUBITAK.

Contents

Chapter 1

Introduction

Let k be a number field and K/k a V_4-extension, i.e., a normal extension with Galois Group $\mathrm{Gal}(K/k) = V_4$, where $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. K/k has three intermediate fields, say k_1, k_2, and k_3. We will use the symbol N^i (resp. N_i) to denote the norm of K/k_i (resp. k_i/k), and by a common abuse of notation we will apply N^i and N_i not only to numbers, but also to ideals and ideal classes. The unit groups (groups of roots of unity, groups of fractional ideals, class numbers) in these fields will be denoted by E_k, E_1, E_2, E_3, E_K (W_k, W_1, ..., J_K, J_1, ..., h_k, h_1, ...) respectively, and the (finite) index $q(K) = (E_K : E_1E_2E_3)$ is called the *unit index* of K/k.

When we look at the literature, we see for $k = \mathbb{Q}$, $k_1 = \mathbb{Q}(\sqrt{-1})$ and $k_2 = \mathbb{Q}(\sqrt{m})$ Dirichlet knew that $h_K = \frac{1}{2}q(K)h_2h_3$. Bachmann [2], Amberg [1] and Herglotz [6] generalized this class number formula to multi-quadratic extensions of $\mathbb{Q}$. Varmon proved a class number formula for extensions with $\mathrm{Gal}(K/k)$ an elementary abelian p-group;

Kuroda [8] later gave a formula in case there is no ramification at the infinite primes. Wada stated a formula for 2-extensions of $k = \mathbb{Q}$ without any restriction on the ramification, and finally Walter [13], by using Brauer's class number relations, deduced the most general Kuroda-type formula.

The proofs mentioned above are all analytic; however, for V_4-extensions $K/\mathbb{Q}$, there exist algebraic proofs given by Hilbert (if $\sqrt{-1} \in K$), Kuroda [9] (if $\sqrt{-1} \in K$), Halter-Koch [4] (if K is imaginary), and Kubota [10, 11].

In this project I will follow Lemmermeyer's paper[12] in which he shows how Kubota's [10, 11] proof can be generalized. The proof consists of two parts; in the first part, where we measure the extent to which $\mathrm{Cl}(K)$ is generated by classes coming from the $\mathrm{Cl}(k_i)$. We will be using class field theory in its ideal-theoretic formulation. The second part of the proof is an extremely lengthy index computation. My thesis will start with listing the results from class field theory and group theory that we will be needed, then I will present Lemmermeyer's[12] proof in my words and organization.

Chapter 2

Preliminaries

2.1 Class Field Theory

First we will explain some notions from class field theory and then state the theorems we will need.

Artin map $\varphi_{L/K}$ maps the group $\mathbf{I}_K^{\mathfrak{m}}$ of ideals in $\mathcal{O}_K$ coprime to $\mathfrak{m}$ onto $\mathrm{Gal}(L/K)$.

Definition 1. A subgroup $\mathbf{H}$ of $\mathbf{I}_K$ is called a congruence subgroup if there is a modulus $\mathfrak{m}$ for K such that

$$\iota(K_{\mathfrak{m},1}) \subseteq \mathbf{H} \subseteq \mathbf{I}_K^{\mathfrak{m}}$$

where $\iota(K_{\mathfrak{m},1})$ *is the principal ideals in* $\mathbf{I}_K^{\mathfrak{m}}$ *which are generated by elements congruent to* 1 *modulo* $\mathfrak{m}$.

Now we can define an equivalence relation on the set of congruence subgroups. Two congruence subgroups $\mathbf{H}_1$ and $\mathbf{H}_2$ are said to be equivalent if they have a common restriction, that is if there is a modulus $\mathfrak{m}$ such that,

$$\mathbf{H}_1 \cap \mathbf{I}^{\mathfrak{m}} = \mathbf{H}_2 \cap \mathbf{I}^{\mathfrak{m}}.$$

Since for any $\mathfrak{m} \mid \mathfrak{m}'$ we get $\mathbf{I}^{\mathfrak{m}'} \subseteq \mathbf{I}^{\mathfrak{m}}$, this helps us to show transitivity. Given $\mathbf{H}_1 \sim \mathbf{H}_2$ modulo $\mathfrak{m}$ so is true for any multiple of $\mathfrak{m}$. Hence for $\mathbf{H}_1 \sim \mathbf{H}_2$ modulo $\mathfrak{m}$ and $\mathbf{H}_2 \sim \mathbf{H}_3$ modulo $\mathfrak{m}'$ we get $\mathbf{H}_1 \sim \mathbf{H}_3$ modulo $\mathrm{lcm}(\mathfrak{m}, \mathfrak{m}')$. Also we need the following lemma from Janusz [7].

Lemma 1. *Let* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *be congruence subgroups defined modulo* $\mathfrak{m}_1$ *and* $\mathfrak{m}_2$ *respectively, which have a common restriction* $\mathbf{H}_3 = \mathbf{H}_1 \cap \mathbf{I}^{\mathfrak{m}_3} = \mathbf{H}_2 \cap \mathbf{I}^{\mathfrak{m}_3}$. *Letting* $\mathfrak{m}$ *be the greatest common divisor of* $\mathfrak{m}_1$ *and* $\mathfrak{m}_2$. *Then there is a congruence subgroup* $\mathbf{H}$ *defined modulo* $\mathfrak{m}$ *such that* $\mathbf{H} \cap \mathbf{I}^{\mathfrak{m}_i} = \mathbf{H}_i$ *for* $i = 1, 2$.

An equivalence class of congruence subgroups is called an ideal group. If $\mathbf{H}$ denotes an ideal group and if $\mathfrak{m}$ is a modulus such that there is some congruence subgroup defined mod $\mathfrak{m}$ which belongs to $\mathbf{H}$, then there is only one subgroup in $\mathbf{H}$ defined modulo $\mathfrak{m}$ and denoted as $\mathbf{H}^{\mathfrak{m}}$. By the lemma above, whenever $\mathbf{H}^{\mathfrak{m}}$ and $\mathbf{H}^{\mathfrak{n}}$ belong to the ideal group $\mathbf{H}$ so does the $\mathbf{H}^{\mathfrak{m}'}$ for $\mathfrak{m}'$ equal to the greatest common divisor of $\mathfrak{m}$ and $\mathfrak{m}'$. So we should have a unique modulus $\mathbf{f}$ such that

$$\mathbf{H}^{\mathbf{f}} \in \mathbf{H}, \quad \textit{and} \quad \mathbf{H}^{\mathfrak{m}} \in \mathbf{H} \Rightarrow \mathbf{f} \mid \mathfrak{m}$$

It is easy to see that $\mathbf{f}$ is greatest common divisor of all $\mathfrak{m}$ such that $\mathbf{H}^{\mathfrak{m}} \in \mathbf{H}$. This $\mathbf{f}$ is called the *conductor* of the ideal group $\mathbf{H}$.

The close relation between the Artin map and ideal groups leads us to deeper analysis. Actually for an abelian extension L of the number field K such that reciprocity law modulo $\mathfrak{m}$ holds, the kernel of the Artin map $\varphi_{L/K}$ on $\mathbf{I}_K^{\mathfrak{m}}$ is also a congruence subgroup and denoted as $\mathbf{H}^{\mathfrak{m}}(L/K)$.

Definition 2. Let L be an abelian extension of the number field K. The ideal group $\mathbf{H}(L/K)$ containing all congruence subgroups $\mathbf{H}^{\mathfrak{m}}(L/K)$ such that reciprocity law holds, is called the *class group* of the extension L of K and L is called the *class field* for the ideal group $\mathbf{H}(L/K)$. The conductor of $\mathbf{H}(L/K)$ is denoted by $\mathbf{f}(L/K)$.

We now list the basic theorems of class field theory.

Theorem 1 (Artin's Reciprocity Law). *For an unramified and abelian extension of number fields* K/F, *the Artin map,* $I \to \mathrm{Gal}(K/F)$, *is surjective and*

its kernel consists of the group of principal ideals. In particular, the Artin symbol $(\frac{K/F}{\mathfrak{p}})$ *only depends on the ideal class* $[\mathfrak{p}]$ *of* $\mathfrak{p}$*, and induces an isomorphism* $Cl(F) \simeq \mathrm{Gal}(K/F)$

Theorem 2 (The Classification Theorem). *Let* L *be any algebraic number field, the correspondence* $L \leftrightarrow \mathbf{H}(L/K)$ *is a one to one, inclusion reversing correspondence between finite dimensional abelian extensions* L *of* K *and the ideal groups of* K*.*

Theorem 3 (Translation Theorem). *Having an abelian extension* L/K *Let* F *be any finite dimensional extension of* K *and* $\mathfrak{m}$ *be a modulus divisible by conductor of the extension* L/K *. Then the ideal group to the abelian extension* FL/F *is the ideal group which contains the congruence subgroup*

$$\{\mathfrak{A} \in \mathbf{I}_F^{\mathfrak{m}} : N_{LF/F}(\mathfrak{A}) \in \mathbf{H}^{\mathfrak{m}}(L/K)\}$$

where $I_F^{\mathfrak{m}}$ *denotes the ideals of* F *coprime to* $\mathfrak{m}$

Note that $\iota(K^*)$ is a congruence subgroup defined modulus $\mathfrak{m} = 1$. The class field to the ideal group containing $\iota(K^*)$ is called the Hilbert class field of K. Given K/k a normal extension of number fields, if F is the Hilbert class field of K/k it turns out that F is the maximal, abelian and unramified extension of K. Here we will list some theorems from Hilbert class field theory that will be used in the thesis.

Theorem 4. *Every number field* F *has a unique Hilbert class field* K*.*

Theorem 5. *Let* k/F *be an unramified abelian extension. Then*

$$(\mathrm{Cl}(F) : N_{k/F}\mathrm{Cl}(k)) = (k : F).$$

In particular $N_{k/F}\mathrm{Cl}(k) = 1$ *for the Hilbert class field* K *of* F

Another term we will be using is the genus field. We will mention what it is and add some properties without proof.

Definition 3. Given an abelian extension K/k the genus field of K is the maximal extension of K contained in Hilbert Class field of K that is abelian over k. It is denoted by K_{gen}.

Theorem 6. *If K is a class field of F, then for each field L with $F \subseteq L \subseteq K$, L is a class field of F, and K is a class field of L.*

Using the theorem above, since K_{gen} is a subfield of a class field it is also a class field over K. The property of K_{gen} is that it is class field of k for the ideal group $N_{K/k}H_K^{(\mathfrak{m})}.H_{\mathfrak{m}}^{(1)}$ where $\mathfrak{m}$ is a multiple of the conductor of $\mathbf{f}(K/k)$.

We next explain norm residues and Hilbert symbols for quadratic extensions.

Definition 4. Given an extension K/k, $\alpha \in k^{\times}$ is said to be a norm residue mod $\mathfrak{p}^l$ if $\alpha \equiv N_k^K A \bmod \mathfrak{p}^l$ for some $A \in K^{\times}$. Moreover α is said to be a norm residue at $\mathfrak{p}$ if the above relation holds for all $l \geq 0$.

Now let us see some properties of quadratic Hilbert symbols. Having a quadratic extension $K = k(\sqrt{\mu})$ for $\mu \in \theta_k$ and not a square. We denote Hilbert symbol over this extension as follows:

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right)_2 = \begin{cases} +1 \text{ if } \nu \text{ is a norm residue at } \mathfrak{p} in \text{K/k} \\ -1 \text{ if } \nu \text{ is a norm non-residue at } \mathfrak{p} \end{cases}$$

But Hasse and Hilbert symbols are connected in the sense that $\left(\frac{\nu,K}{\mathfrak{p}}\right) = \left(\frac{\nu,\mu}{\mathfrak{p}}\right)_2$ for $K = k(\sqrt{\mu})$ So we attain the following property of Hasse symbols that will be needed for our thesis.

$$\left(\frac{\nu, K_1K_2}{\mathfrak{p}}\right) = \left(\frac{\nu, K_1}{\mathfrak{p}}\right)_2 \left(\frac{\nu, K_2}{\mathfrak{p}}\right)_2$$

for two quadratic extensions K_1, and K_2.

Now we will state Hasse's Norm Theorem the proof of which can be found in Janusz[7].

Theorem 7 (Hasse's Norm Theorem). *Let L be a cyclic extension of the number field K, an element of K is a norm from L if and only if it is a norm residue at every prime of K.*

2.2 Group Theory

Now we will state and prove the Snake Lemma which we will make use of.

Theorem 8.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & a & \xrightarrow{f} & b & \xrightarrow{g} & c & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & a' & \longrightarrow & b' & \longrightarrow & c' & \longrightarrow & 1 \end{array}$$

Having two exact sequences located as above and connected with homomorphisms, give us the exact sequence below,

$$1 \to \ker\alpha \to \ker\beta \to \ker\gamma \to \mathrm{cok}\alpha \to \mathrm{cok}\beta \to \mathrm{cok}\gamma \to 1,$$

Proof. For short call $\ker\alpha$ as a_k $\ker\beta$ as b_k $\ker\gamma$ as c_k obviously these lie in a, b, c. Let's denote the images of α, β, γ as a_i, b_i, c_i respectively.
First denoting $\mathrm{cok}\alpha$ as a_q $\mathrm{cok}\beta$ as b_q $\mathrm{cok}\gamma$ as c_q,while these lie in a', b', c' we also get that $a_q = a'/a_i, b_q = b'/b_i, c_q = c'/c_i$.
Hence with these notations we will prove the exactness of

$$1 \to a_k \to b_k \to c_k \to a_q \to b_q \to c_q \to 1.$$

First observe that a_k is mapped into b_k and b_k is mapped into c_k since the diagram is commutative a_k is mapped to zero by α if we apply f' to this it becomes same as applying first f and then β to it. Since it is zero we get that f maps a_k into b_k. Similarly b_k is mapped into c_k by g.

Since f maps a_k into b_k this shows exactness at a_k.

Now we will show exactness at b_k. For any element in a, say x such that $g(f(x)) = 0$, So it is true for the restriction on a_k. Hence image is mapped into the kernel. For the converse, take $y \in b_k$ such that $g(b_k) = 0$ in c_k. If x is the preimage of y in a with respect to f. Since $\beta(y) = 0$, we get $\alpha(x) = 0$. So $x \in b_k$; we get that kernel is in the image. This completes the proof of exactness at b_k.

Observe that each $y \in a_i$ comes from some $x \in a$. Taking the two paths from x to b' we see a_i is mapped into b_i, so we can map each coset of $a_i \in a'$ into a

coset of $b_i \in b'$. That is f' defines a well defined map from a_q into b_q. Similarly g' defines a well defined map from b_q into c_q.

To prove exactness at b_q, consider that everything in a' becomes zero in c'. So every coset of a_i in a' becomes zero in c'. So the image of f' is contained in kernel ofg'. Conversely every y' in b' act as a coset representative for b_q, and suppose it becomes 0 in in c_q. In other words $g'(y')$ lies in c_i. Pull this up to something in c, and pull this back to some y in b. If $\beta(y)$ differs from y', the difference lies in the kernel of g'. Call this difference z. Now z and y', represent the same coset of b_i, so we may as well use z. Since z becomes 0, in c', let w in a', map to z. Now the coset $w + a_i$ map to the coset $z + b_i$. The kernel equals the image, and b_q is exact.

Now we should find a map from c_k to a_q. Given an element y in c_k, pull it back to some $x \in b$, and afterwards down to b'. This moves forward to 0, so lies in the image of a'. Pull it back to a', thus defining a coset of a_i, or an element a_q. To check well-definedness observe that if we had selected a different x in the preimage of a_q, the difference would map to 0 in c, and would come from some $w \in a$. Since $\alpha(w) \in a_i$, the coset has not changed. After proving the well-definedness we can call this map h.

Apply h, and then g', and reach up in b_i. The image of h lies in the kernel of g'. Conversely, let $w \in a'$ and $b_i \in b'$. Going up to b and over to c and find y. Now $\gamma(y) = g'(f'(w))$, which is 0, hence $y \in c_k$, and is a valid preimage under h. The kernel equals the image, and a_q is exact.

We will be done after showing the exactness of c_k. Letting $x \in b_k$ mapped to $y \in c_k$, applying h, the result becomes 0, hence the image lies the kernel. Conversely, let $y \in c_k$ pull back to $x \in b$, and down and back to something in a_i. We lift this to $w \in a$, and subtract $f(w)$ from x. Note that $g(x)$ still equals y, and now, $\beta(x) = 0$. Thus $x \in b_k$, the kernel equals the image, and c_k is exact. Hence this completes the proof of Snake Lemma. □

In addition, we will state and prove the following group theoretical lemma which will help us to find the proper index values.

Lemma 2. *Let G be a group and assume that H is a subgroup of finite index in G. If f is a homomorphism from G to another group, then*

$$(G : H) = (G^f : H^f)(G_f H : H),$$

where $G^f = \mathrm{im} f$, $G_f = \ker f$, and H^f is the image of the restriction of f to H.

Proof. Consider the map from (G/H) to (G^f/H^f) where $gH \to f((g)f(H)$ This map is well defined and surjective. the kernel is the cosets $(G_f H/H)$ and this gives the index relation $(G : H) = (G^f : H^f)(G_f H : H)$. □

Finally we will state and prove a particular case of $Hilbert's \quad Theorem \quad 90$.

Theorem 9. *For a quadratic extension $E = F(\sqrt{d})/F$ of characteristic zero, if given $\alpha \in E$ has the property that $N_{E/F}(\alpha) = 1$. Then there exists $b \in E^\star$ such that $\alpha = b^\sigma/b$, where σ is the non-trivial automorphism of E/F.*

Proof. If for $\alpha = -1$, we take $b = \sqrt{d}$. Otherwise given $b = (1 + \alpha)^{-1}$, then $\frac{1+\alpha}{1+\alpha^\sigma} = \frac{(1+\alpha)\alpha}{(1+\alpha^\sigma)\alpha} = \frac{(1+\alpha)\alpha}{\alpha+\alpha\alpha^\sigma} = \frac{(1+\alpha)\alpha}{1+\alpha} = \alpha$. □

Chapter 3

Kuroda's Formula

Our aim is to prove that for a V_4 extension K/k:

$$h(K) = 2^{d-\kappa-2-v} q(K) h_1 h_2 h_3 / h_k^2. \tag{3.1}$$

where

- d is the number of infinite places ramified in K/k;
- κ is the Z-rank of E_k;
- $v = 1$ if $K = k(\sqrt{\varepsilon}, \sqrt{\eta}\,)$ with units $\varepsilon, \eta \in E_k$, and $v = 0$ otherwise.

To show 3.1 we will first show that

$$h(K) = \frac{\mathrm{cok} j}{\ker j} \cdot h_1 h_2 h_3. \tag{3.2}$$

Considering the homomorphism,

$$j : \mathrm{Cl}(k_1) \times \mathrm{Cl}(k_2) \times \mathrm{Cl}(k_3) \longrightarrow \mathrm{Cl}(K)$$

where $c_i = [\mathfrak{a}_i]$ is the ideal class in k_i generated by $\mathfrak{a}_i$; and $j(c_1, c_2, c_3) = [\mathfrak{a}_1 \mathfrak{a}_2 \mathfrak{a}_3 \mathcal{O}_K]$ where $\mathcal{O}_K$ is the ring of integers in K, we get

$$h(K) = \frac{\mathrm{cok} j}{\ker j} \cdot h_1 h_2 h_3.$$

Since the aim is to compute $h(K)$ one has to compute the orders of the groups $\ker j$ and $\mathrm{cok}j = \mathrm{Cl}(K)/\mathrm{im}j$. To do this construct the subgroup

$$\widehat{C} = \{(c_1, c_2, c_3) \mid N_1 c_1 N_2 c_2 N_3 c_3 = 1\}$$

of

$$\mathrm{Cl}(k_1) \times \mathrm{Cl}(k_2) \times \mathrm{Cl}(k_3)$$

and denote the restriction of j on this subgroup as $\widehat{j}$.

We will try to show that

$$h_k \cdot \frac{\mathrm{cok}j}{\ker j} = \frac{\mathrm{cok}\widehat{j}}{\ker \widehat{j}}. \tag{3.3}$$

and by means of this we will be able to find $h(K)$ in terms of $\mathrm{cok}\widehat{j}$ and $\ker \widehat{j}$, which will be determined soon.

To show this consider the following map:

Let

$$\nu : C = \mathrm{Cl}(k_1) \times \mathrm{Cl}(k_2) \times \mathrm{Cl}(k_3) \longrightarrow \mathrm{Cl}(k), \quad \nu(c_1, c_2, c_3) = N_1 c_1 N_2 c_2 N_3 c_3.$$

If there exists a ramified extension k_i/k is we get $N_i\mathrm{Cl}(k_i) = \mathrm{Cl}(k)$ by class field theory. But when all the k_i/k are unramified, the groups $N_i\mathrm{Cl}(k_i)$ will have index $2 = (k_i : k)$ in $\mathrm{Cl}(k)$, and they will be different from each other as by the Artin map there is a correspondence among

$$k_i/k \text{ and } N_i\mathrm{Cl}(k_i)$$

But ν is onto in any case. In addition, we observe $\widehat{C} = \ker \nu$ and obtain the exact sequence

$$1 \longrightarrow \widehat{C} \longrightarrow C \longrightarrow \mathrm{Cl}(k) \longrightarrow 1.$$

Let $\widehat{j}$ be the restriction of j to $\widehat{C}$; then the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \widehat{C} & \longrightarrow & C & \longrightarrow & \mathrm{Cl}(k) & \xrightarrow[\nu]{} & 1 \\ & & \downarrow{\scriptstyle \widehat{j}} & & \downarrow{\scriptstyle j} & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{Cl}(L) & \longrightarrow & \mathrm{Cl}(L) & \longrightarrow & 1 & & \end{array}$$

is exact and commutative. The snake lemma gives us an exact sequence

$$1 \longrightarrow \ker\widehat{j} \longrightarrow \ker j \longrightarrow \mathrm{Cl}(k) \longrightarrow \mathrm{cok}\widehat{j} \longrightarrow \mathrm{cok}j \longrightarrow 1,$$

and this gives that:

$$h_k \cdot \frac{\mathrm{cok}j}{\ker j} = \frac{\mathrm{cok}\widehat{j}}{\ker\widehat{j}}. \tag{3.4}$$

Next we will be calculating $\mathrm{cok}\widehat{j}$. Before this we will prove the following proposition which will be needed in the proof

Proposition 1. *For V_4-extensions K/k, the following assertions are equivalent:*

(i) $r \in k^\times$ is a norm residue in K/k at every place of k;

(ii) $r \in k^\times$ is a (global) norm from k_1/k and k_2/k;

(iii) there exist $\alpha \in K^\times$ and $a \in k^\times$ such that $r = a^2 \cdot N_{K/k}\alpha$.

Proof. (i) $\Longrightarrow$ (ii) If $r \in k^\times$ is a norm residue in K/k at every place of k, then it is a norm residue in k_1/k and k_2/k for every place of k but k_1/k and k_2/k are cyclic extensions. Therefore by Hasse's norm residue theorem, which says that for cyclic extensions an element is a global norm if and only if its a local norm for all primes, we get that $r \in k^\times$ is a (global) norm from k_1/k and k_2/k.

(ii) $\Longrightarrow$ (iii).Having $r \in k^\times$ is a (global) norm from k_1/k and k_2/k, there exist $\alpha_1 \in k_1$ and $\alpha_2 \in k_2$ such that $N_1\alpha_1 = N_2\alpha_2 = r$. But then we get that $(\alpha_1/\alpha_2) \in K$ and $(\alpha_1/\alpha_2)^{1+\sigma\tau} = 1$. Since K/k_3 is a cyclic extension we can use $Hilbert's \quad Theorem \quad 90$, this says that there exists $\alpha \in K^\times$ such that $\alpha_1/\alpha_2 = \alpha^{1-\sigma\tau}$. But

$$\alpha^{1-\sigma\tau} = \alpha^{1+\sigma}(\alpha^{1+\tau})^{-\sigma} \quad \text{this implies} \quad \alpha^{1+\sigma}/\alpha_1 = (\alpha^{1+\tau})^\sigma/\alpha_2$$

Since

$\alpha^{1+\sigma}/\alpha_1 \in k_1$ and$(\alpha^{1+\tau})^\sigma/\alpha_2 \in k_2$ it is also in the intersection which is k.

Assigning $a = \alpha^{1+\sigma}/\alpha_1$ we have

$$N_{K/k}\alpha = (\alpha^{1+\sigma})^{1+\tau} = (\alpha_1 a)^{1+\tau} = N_1(\alpha^1)a^2 = a^2 r \tag{3.5}$$

where $a, r \in k^\times$.

(iii) $\Longrightarrow$ (i) As $r = N_i(N^i\alpha)/a)$ for $i = 1, 2$ so it is norm residue at every place of k_1 and k_2 hence using the relation which says,

$$\Big(\frac{\beta\,,\, k_1k_2}{\mathfrak{p}}\Big) \;=\; \Big(\frac{\beta\,,\, k_1}{\mathfrak{p}}\Big)\Big(\frac{\beta\,,\, k_2}{\mathfrak{p}}\Big).$$

we see that r is a norm residue in $k_1k_2 = K$ at every place.

□

We define $K^{(2)}$ to be the maximal subextension of K_{gen}/k such that $\text{Gal}(K^{(2)}/k)$ is an elementary abelian 2-group. Moreover, we let J_K (resp. H_K) denote the group of (fractional) ideals (resp. principal ideals) of K. Then we have the following theorem.

Proposition 2. *To every subfield F of the Hilbert class field K^1 of K there is a unique ideal group $\mathfrak{h}_F$ such that $H_K \subseteq \mathfrak{h}_F \subseteq J_K$ and F is class fied for $\mathfrak{h}_F$. Under this correspondence,*

$$\text{Gal}(K^1/F) \simeq \text{Cl}(K)/(J_K/\mathfrak{h}_F) \simeq \mathfrak{h}_F/H_K,$$

and we find the following diagram of subextensions F/k of K/k and corresponding Galois groups $\text{Gal}(K^1/F)$*:*

$$\begin{array}{ccc}
K^1 & \longleftrightarrow & 1 \\
| & & | \\
K_{\text{gen}} & \longleftrightarrow & \text{im}\widehat{j} \\
| & & | \\
K^{(2)} & \longleftrightarrow & \text{im}j \\
| & & | \\
K & \longleftrightarrow & \text{Cl}(K)
\end{array}$$

Proof. We need to show $K_{\text{gen}} \longleftrightarrow \text{im}\widehat{j}$. We know that K_{gen} is the class field of k for the ideal group $N_{K/k}H_K^{(\mathfrak{m})} \cdot H_{\mathfrak{m}}^{(1)}$, where the defining modulus $\mathfrak{m}$ is a

multiple of the conductor $\mathfrak{f}(K/k)$. But any element of this ideal group is of form $N_{K/k}(A)\cdot(\alpha)$ where $\alpha \equiv 1 \mod \mathfrak{m}$ and $(A)+\mathfrak{m}=(1)$ so we get that it has the form $N_{K/k}(A) \mod \mathfrak{m}$. This ideal class consists of norm residues modulo $\mathfrak{m}$. So elements of ideal class group become norm residue in K/k for every place of k. Using Proposition 1 we see that elements of the ideal class group have the form $a^2 \cdot N_{K/k}\alpha$ where $a \in k$, $\alpha \in K$, and $(\alpha)+\mathfrak{m}=(1)$. Using the translation theorem we derive that the ideal group corresponding to K_{gen}/K is:

$$\mathfrak{h}_{\text{gen}} = \{\mathfrak{a} \in J_K \,|\, \mathfrak{a}+\mathfrak{m}=(1), N_{K/k}\mathfrak{a} \in N_{K/k}H_K^{(\mathfrak{m})}\cdot H_{\mathfrak{m}}^{(1)}\}.$$

Having $N_{K/k}\mathfrak{a} = a^2 \cdot N_{K/k}\alpha$ we get $N_{K/k}(\mathfrak{a}/\alpha) = (a)^2$. Set $\mathfrak{b} = \mathfrak{a}/\alpha$. Our aim is to show that $\mathfrak{b} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$ for $\mathfrak{a}_i$ in k_i. Without loss of generality we can assume that no ideal in k_i divides $\mathfrak{b}$. So any $\mathfrak{P} \mid \mathfrak{b}$ can not have inertia degree greater than 1 and can not have a conjugate dividing $\mathfrak{b}$. Therefore given that $\mathfrak{P}^m \parallel \mathfrak{b}$ this implies that

$$N_{K/k}\mathfrak{P}^m \parallel N_{K/k}\mathfrak{b} = (a^2),$$

hence this says that $2 \mid m$. But

$$2 = 1+\sigma+\tau+\sigma\tau-(1+\sigma\tau)\sigma$$

where $\sigma, \tau, \sigma\tau$ are non-trivial elements of $\text{Gal}(K/k)$ fixing k_1, k_2, k_3 respectively. This means any element in square form say $\mathfrak{P}^2$ is of form $\mathfrak{P}^2 = N^1\mathfrak{P}\cdot N^2\mathfrak{P}\cdot(N^3\mathfrak{P})^{-\sigma}$. So $(a^2) = N_{K/k}\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 = (N_1\mathfrak{a}_1\cdot N_2\mathfrak{a}_2\cdot N_3\mathfrak{a}_3)^2$ hence we get that $(a) = N_1\mathfrak{a}_1\cdot N_2\mathfrak{a}_2\cdot N_3\mathfrak{a}_3$.

The identity 3 shows $\mathfrak{P}^2 = N^1\mathfrak{P}\cdot N^2\mathfrak{P}\cdot(N^3\mathfrak{P})^{-\sigma}$, and we are done with the claim.

On the other hand any ideal $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$ with $\mathfrak{a}+\mathfrak{m}=(1)$ and $(a) = N_1\mathfrak{a}_1\cdot N_2\mathfrak{a}_2\cdot N_3\mathfrak{a}_3$ lies in $\mathfrak{h}_{\text{gen}}$. In addition, $H_K^{(\mathfrak{m})} \subseteq \mathfrak{h}_{\text{gen}}$. So we get that

$$\mathfrak{h}_{\text{gen}} = \{\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \,|\, \mathfrak{a}+\mathfrak{m}=(1),\ N_1\mathfrak{a}_1\cdot N_2\mathfrak{a}_2\cdot N_3\mathfrak{a}_3 = (a) \text{ for some } a \in k\}\cdot H_K^{(\mathfrak{m})},$$

We can remove the condition $\mathfrak{a}+\mathfrak{m}=(1)$ (because $\mathfrak{h}_{\text{gen}}$ can be defined modulo (1)) and get an equivalent ideal group which is:

$$\mathfrak{h}_{\text{gen}} = \{\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \,|\, N_1\mathfrak{a}_1\cdot N_2\mathfrak{a}_2\cdot N_3\mathfrak{a}_3 = (a) \text{ for some } a \in k\}\cdot H_K.$$

The corresponding class group is $\mathfrak{h}_{\text{gen}}/H_K$, and

$$\text{Gal}(K^1/K) \simeq \mathfrak{h}_{\text{gen}}/H_K = \{c = c_1c_2c_3 \,|\, N_1c_1N_2c_2N_3c_3 = 1\} = im\widehat{j}.$$

□

Hence this was all we needed,

$$\#\text{cok}\widehat{j} = (\text{Cl}(K) : \text{im}\widehat{j}) = (K_{\text{gen}} : K). \tag{3.6}$$

But Furuta's [3] formula says,

$$(K_{\text{gen}} : K) = 2^{d-2}h_k\frac{\prod e(\mathfrak{p})}{(E_k : H)}.$$

Hence it gives that

$$\#\text{cok}\widehat{j} = 2^{d-2}h_k\frac{\prod e(\mathfrak{p})}{(E_k : H)}. \tag{3.7}$$

The derivation of $\#\ker\widehat{j}$ requires a lengthy index computation which will be done in several steps. For this we must introduce some new notions.

We call an ideal $\mathfrak{a}_i$ in k_i *ambiguous* when we have $\mathfrak{a}_i^\tau = \mathfrak{a}_i$ for any $\tau \in \text{Gal}(K/k)$. Similarly we call an ideal class $c \in \text{Cl}(k_i)$ *ambiguous* if $c^\tau = c$ for any $\tau \in \text{Gal}(K/k)$, and *strongly ambiguous* if $c = [\mathfrak{a}_i]$ for some ambiguous ideal $\mathfrak{a}_i \in k_i (i = 1, 2, 3)$. Letting A_i denote the group of strongly ambiguous ideal classes in k_i $(i = 1, 2, 3)$, $A = A_1 \times A_2 \times A_3$ turns out to be a subgroup of C, and $\widehat{A} = \widehat{C} \cap A$ becomes a subgroup of $\widehat{C}$. Having already the formula for $\#A_i$'s we get $\#A$ and one can try to calculate $\#\ker\widehat{j}$ by restricting the map to $\widehat{j}$ to $\widehat{A}$, finding the kernel of this restricted map and index relation between the kernels of the original map and restricted map.

H, which was defined earlier as group of units in E_k that are norm residues in K/k at every place of k turns out to be the following:

$$H = \{\eta \in E_k \,|\, \eta = N_i\alpha_i \text{ for some } \alpha_i \in k_i, i = 1, 2, 3\}.$$

Then we form $H_0 = E_1^N \cap E_2^N \cap E_3^N$ that's the subgroup of H consisting of the units in H that are norm residues of units in k_i/k, for every i. Now we can start

the computations. We will continue by doing a series of claims and then prove them and get the result we want by combining derived results.

Claim 1. *Let's call restriction of the map $\widehat{j}$ to $\widehat{A}$ as j^* , then*

$$\#\ker\widehat{j} = (H : H_0) \cdot \#\ker j^*. \tag{3.8}$$

Proof. Let $([\mathfrak{a}_1], [\mathfrak{a}_2], [\mathfrak{a}_3]) \in \ker\widehat{j}$; then $\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 = (\alpha)$ for some $\alpha \in K^\times$. $([\mathfrak{a}_1], [\mathfrak{a}_2], [\mathfrak{a}_3]) \in \widehat{C}$, so $(N_{K/k}\alpha) = (N_1\mathfrak{a}_1 \cdot N_2\mathfrak{a}_2 \cdot N_3\mathfrak{a}_3)^2 = (a)^2$ for some $a \in k$. Therefore $\eta = (N_{K/k}\alpha)/a^2$ is a unit in E_k which is unique mod $NE_K \cdot E_k^2$. So we can define the following well defined homomorphism.

$$\theta_0 : \ker\widehat{j} \longrightarrow H/NE_K \cdot E_k^2, \quad ([\mathfrak{a}_1], [\mathfrak{a}_2], [\mathfrak{a}_3]) \longmapsto \eta NE_K \cdot E_k^2,$$

We intend to get an isomorphism, by showing our map is onto and finding the kernel of it. To show θ_0 is onto, take $\eta \in H$, by theorem1 we have $b \in k^\times, \alpha \in K^*$ such that, $\eta = b^2 N_{K/k}\alpha$, letting $b = a^{-1}$ we get $a^2\eta = N_{K/k}\alpha$. We have seen that an equation $N_{K/k}\mathfrak{a} = (a)^2$ implies the existence of ideals $\mathfrak{a}_i$ in k_i such that $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$. This gives that $(\alpha) = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$. We get Now $(N_1\mathfrak{a}_1 \cdot N_2\mathfrak{a}_2 \cdot N_3\mathfrak{a}_3)^2 = (N_{K/k}\alpha) = (a)^2$ means $(a) = (N_1\mathfrak{a}_1 \cdot N_2\mathfrak{a}_2 \cdot N_3\mathfrak{a}_3)$, so the triple $([\mathfrak{a}_1], [\mathfrak{a}_2], [\mathfrak{a}_3])$ is in $\ker\widehat{j}$ given η we could find a triple in $\ker\widehat{j}$, this proves surjectivity. Now we will a bit modify the image set, to achieve a relation between $\#\ker\widehat{j}$ and $\#\ker j^*$. As $\theta_0 : \ker\widehat{j} \longrightarrow H/NE_K \cdot E_k^2$ is onto, we will again get a onto map by replacing $NE_K \cdot E_k^2/$ with a larger group including it. Hence $H_0 = E_1^N \cap E_2^N \cap E_3^N$ is such a group.

We construct $\rho_i = (N^i\alpha)/a$; then $N_i\rho_i = \eta \in H_0$. Also we observe that $\mathfrak{a}_1^{1-\tau} = (\rho_1)$ as $\rho_1 = (N^1\alpha)/a$ and

$$(N^1\alpha)/a = \mathfrak{a}_1^{1+\sigma}\mathfrak{a}_2^{1+\sigma}\mathfrak{a}_3^{1+\sigma}/\mathfrak{a}_1^{1+\tau}\mathfrak{a}_2^{1+\sigma}\mathfrak{a}_3^{1+\sigma\tau} = \mathfrak{a}_1^{2-(1+\tau)} = \mathfrak{a}_1^{1-\tau} \tag{3.9}$$

Similarly $\mathfrak{a}_2^{1-\sigma\tau} = (N^2\alpha)/a = (\rho_2)$ and

$\mathfrak{a}_3^{1-\sigma} = (N^3\alpha)/a = (\rho_3)$

Writing $\eta = N_i\varepsilon_i$, where $\varepsilon_i \in E_i$, and replacing ρ_i by ρ_i/ε_i, we modify ρ_i 's such that $N_i\rho_i = 1$. Since k_i/k's are cyclic extensions we apply Hilbert's

Theorem 90 and get $\rho_2 = \beta_2^{1-\sigma\tau}$, and $\rho_3 = \beta_3^{1-\sigma}$ for some $\beta_i \in k_i$. But then the ideals $fb_i = \mathfrak{a}_i\beta_i^{-1}$ become ambiguous; to see this, consider $\mathfrak{b}_1 = \mathfrak{a}_1\beta_1^{-1}$. Then τ acts as follows:

$$\mathfrak{b}_1^\tau = \mathfrak{a}_1^\tau\beta_1^{-\tau} = \mathfrak{a}_1^\tau\rho_1\beta_1^{-1} = \mathfrak{a}_1\beta_1^{-1} \tag{3.10}$$

But $[\mathfrak{b}_i] = [\mathfrak{a}_i]$ so $[\mathfrak{a}_i]$ turn out to be strongly ambiguous. Hence we get

$$\ker\theta \subseteq \ker\widehat{j} \cap A_1 \times A_2 \times A_3 = \ker j^*.$$

And for $([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) \in \ker j^*$ $\rho_i = (N^i\alpha)/a$ become units, moreover

$$\eta = \theta([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) = N_i\rho_i \in E_1^N \cap E_2^N \cap E_3^N = H_0.$$

So $\ker\theta = \ker j^*$. Using this fact we construct the following exact sequence

$$1 \longrightarrow \ker j^* \longrightarrow \ker\widehat{j} \xrightarrow{\theta} H/H_0 \longrightarrow 1$$

This gives the index relation: $\#\ker\widehat{j} = (H : H_0)\cdot\#\ker j^*$, and proves claim1. □

Claim 2. *Let* $R = \{\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \mid \mathfrak{a}_i \in I_i$ *is ambiguous in* $k_i/k\}$ *and* $R_\pi = R \cap H_K$*; then*

$$\#\ker j^* = \#A/(R : R_\pi). \tag{3.11}$$

Proof. Let

$$\begin{aligned} R &= \{\mathfrak{A} \mid \mathfrak{A} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3, \mathfrak{a}_i \in J_i \text{ ambiguous}\}, \\ \widehat{R} &= \{\mathfrak{A} \mid \mathfrak{A} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3, \mathfrak{a}_i \in J_i \text{ ambiguous}, \ \nu([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) = 1\}, \end{aligned}$$

and define a homomorphism π mapping $\mathfrak{A} \in \widehat{R} \subseteq J_K$ to $[\mathfrak{A}] \in \mathrm{Cl}(K)$. Then $\pi : \widehat{R} \longrightarrow \mathrm{im}j^*$ is onto as the map is defined similarly on the same set with j^*. It is easily seen that $\ker\pi = \widehat{R} \cap H_K$. On the other hand if $\rho \in K$ and $(\rho) = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \in \widehat{R}$, then

$$(\rho)^2 = (\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3)^2 = (N\mathfrak{a}_1 \cdot N\mathfrak{a}_2 \cdot N\mathfrak{a}_3) = (r)$$

for some $r \in k$. So

$$\ker\pi = \{(\rho) \mid \rho \in K, (\rho)^2 = (r) \text{ for some } r \in k\} = R_\pi,$$

and

$$(\widehat{R} : R_\pi) = \#\mathrm{im}\pi = \#\mathrm{im}j^* = (\widehat{A} : \ker j^*),$$

which says

$$\#\ker j^* = \frac{\#\widehat{A}}{(\widehat{R} : R_\pi)}. \tag{3.12}$$

Now we will try to see a relation between $(A : \widehat{A})$ and$(R : \widehat{R})$. For this examine the homomorphism below: $\nu : C \longrightarrow \mathrm{Cl}(k)$ defined previously sends $([\mathfrak{a}_1], [\mathfrak{a}_2], [\mathfrak{a}_3]) \in A = A_1 \times A_2 \times A_3 \subseteq C$ to $[\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3]^2 \in \mathrm{Cl}(k)$, and we get the following exact sequence.

$$1 \longrightarrow \widehat{A} \longrightarrow A \xrightarrow{\nu} A_1^2A_2^2A_3^2 \longrightarrow 1$$

We construct another exact sequence as follows:

$$1 \longrightarrow \widehat{R} \longrightarrow R \xrightarrow{\overline{\nu}} A_1^2A_2^2A_3^2 \longrightarrow 1,$$

where $\overline{\nu}(\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3) = \nu([\mathfrak{a}_1], [\mathfrak{a}_2], [\mathfrak{a}_3]) = [\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3]^2$. From these sequences one can conclude that $(A : \widehat{A}) = (R : \widehat{R})$, and substituting this in the equation above we get:

$$\#\ker j^* = \frac{\#\widehat{A}}{(\widehat{R} : R_\pi)} = \frac{(A : \widehat{A}) \cdot \#\widehat{A}}{(R : \widehat{R})(\widehat{R} : R_\pi)} = \frac{\#A}{(R : R_\pi)}.$$

which proves the claim2. □

Now we will compute $(R : R_\pi)$. To do this, take $(\rho) \in R_\pi$. Since $(\rho)^2 = (r)$ for some $r \in k^\times$, construct $\eta = \rho^2/r$ is a unit in $\mathcal{O}_K$. As the ideal (ρ) is fixed by $\mathrm{Gal}(K/k)$, $\eta_i = (N^i\rho)/r$ is a unit in E_i since $N_i(\eta_i) = \rho^4/r^2 \in \mathcal{O}_k$.

Picking $\sigma \in \mathrm{Gal}(K/k)$, the automorphism that acts nontrivially on k_3/k, we observe that $\eta = \eta_1\eta_2\eta_3^{-\sigma} \in E_1E_2E_3$, and

$$N_1\eta_1 = N_2\eta_2 = N_3(\eta_3^{-\sigma}) = (N_{K/k}\rho)/r^2.$$

Because of the way the unit η is constructed it is determined up to a factor in E_kE^2, where E is used as short of the unit group E_K, Therefore we can define a homomorphism $\varphi : R_\pi \longrightarrow E/E_kE^2$ by assigning the ideal $(\rho) \in R_\pi$ that satisfies $(\rho)^2 = (r)$, $r \in k^\times$ to the class of the unit $\eta = \rho^2/r$. Since we had $\eta = \eta_1\eta_2\eta_3^{-\sigma}$ and $N_i(\eta_1) = N_2(\eta_2) = N_3(\eta_3)$, we can restrict the image set to the following;

$$E^* = \{e_1e_2e_3 \,|\, e_i \in E_i, N_1e_1 \equiv N_2e_2 \equiv N_3e_3 \bmod E_k^2\}$$

Thus we get that $\mathrm{im}\varphi \subseteq E^*/E_kE^2$. And the lemma below will tell about the surjectivity of the map.

Lemma 3. *Having $\eta = e_1e_2e_3 \in E^*$, $K(\sqrt{\eta})/k$ is a normal extension with an elementary abelian Galois group and for η , there are $\rho \in K^\times$ and $r \in k^\times$ such that $\eta = \rho^2/r$.*

Proof. We know that an extension $K(\sqrt{\eta})/k$ is normal if and only if for every $\sigma \in \mathrm{Gal}(K/k)$ there exists an $\alpha_\sigma \in K^\times$ such that $\eta^{1-\sigma} = \alpha_\sigma^2$. For a V_4 extension with galois group $\mathrm{Gal}(K/k) = \{1, \sigma, \tau, \sigma\tau\}$, say σ fixes k_1; then

$$\eta^{1-\sigma} = (e_1e_2e_3)^{1-\sigma} = (e_2e_3)^{1-\sigma} = (e_2e_3)^2/(N_2e_2 \cdot N_3e_3),$$

and this is a square in $K^\times$ as $N_2e_2 \equiv N_3e_3 \bmod E_k^2$.
We take it known that $\mathrm{Gal}(K(\sqrt{\eta})/k)$ is elementary abelian if and only if $\alpha_\sigma^{1+\sigma} = \alpha_\tau^{1+\tau} = \alpha_{\sigma\tau}^{1+\sigma\tau} = +1$. Picking $\alpha_\sigma = e_2e_3/e$ where $e \in E_k$ and $e^2 = N_2e_2 \cdot N_3e_3$, we get $\alpha_\sigma^{1+\sigma} = (N_2e_2 \cdot N_3e_3)/e^2 = +1)$.

Since $K(\sqrt{\eta})/k$ is elementary abelian, $k(\sqrt{\eta}) = k(\sqrt{r})$ for some $r \in k^\times$. But then there must exist $\rho \in k^\times$ such that $\rho^2 = \eta r$. □

Given η we could find (ρ, r) giving $\rho^2 = \eta r$ therefore $\varphi : R_\pi \longrightarrow E^*/E_kE^2$ is onto. And,

$$\begin{aligned}
\ker\varphi &= \{(\rho) \in R_\pi \,|\, \rho^2/r = ue^2, u \in E_k, e \in E\} \\
&= \{(\rho) \in R_\pi \,|\, \exists\ r \in k^\times, e \in E : (\rho/e)^2 = r\} \\
&= \{(\rho) \in R_\pi \,|\, \rho^2 = r \text{ for } r \in k^\times\} = R_0.
\end{aligned}$$

Just, we defined $R_0 = \ker\varphi$; the group of principal ideals H_k is a subgroup of R_0, and we will calculate the index $(R_0 : H_k)$

Claim 3. *$(R_0 : H_k) = 2^{2-u}$, where $2^u = (E^{(2)} : E_k)$ and $E^{(2)} = \{e \in E : e^2 \in E_k\}$.*

Proof. let $\Lambda = \{\rho \in K^\times \mid \rho^2 \in k^\times\}$ and map $\Lambda/k^\times$ onto R_0/H_k by sending $\rho \cdot k^\times$ to $(\rho) \cdot H_k$.

The kernel of this map is $E^{(2)}k^\times/k^\times$ since it is a normal subgroup of $\Lambda/k^\times$ and elements of $E^{(2)}k^\times/k^\times$ corresponds to unit elements of $\Lambda/k^\times$ under the map defined. Hence we get the following exact sequence:

$$1 \longrightarrow E^{(2)}k^\times/k^\times \longrightarrow \Lambda/k^\times \longrightarrow R_0/H_k \longrightarrow 1$$

and $\Lambda/k^\times$ has order 4 as $(\Lambda/k^\times = \{k^\times, \sqrt{a} \cdot k^\times, \sqrt{b} \cdot k^\times, \sqrt{ab} \cdot k^\times\}$ for $K = k(\sqrt{a}, \sqrt{b}))$ and $E^{(2)}k^\times/k^\times \simeq E^{(2)}/E_k = 2^u$. So we really get that $(R_0 : H_k) = 2^{2-u}$. □

Claim 4. $(R : H_k) = (R : J_k)(J_k : H_k) = 2^t h_k$, *where* $t = \#\mathrm{Ram}(K/k)$.

Proof. It is already defined that that $(J_k : H_k) = h_k$, what about (R/J_k); This consists of the triples $\mathfrak{a} \cdot \mathfrak{b} \cdot \mathfrak{c}$ where $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are ramified primes in respectively k_1, k_2, k_3. This seems to give $2^{t_1} \cdot 2^{t_2} \cdot 2^{t_3}$ triples, where t_i denotes the number of finite primes ramified in k_i, but we should be careful since any ramified prime either ramifies in two of the subextensions or three of them. Hence we can use them only once. So any ramified can contribute only once therefore we should divide our number by 4 for totally ramified primes and by two for those ramifying in only two of the subextensions. But this gives exactly 2^t elements by claim4, which says $2^{t_1+t_2+t_3} = 2^t \prod e(\mathfrak{p})$, where t is the number of ramified primes in K. □

So we get

$$(R : R_\pi) = \frac{(R : H_k)}{(R_\pi : R_0)(R_0 : H_k)} = 2^{t-2} h_k \frac{(E^{(2)} : E_k)}{(E^* : E_k E^2)}.$$

Since

$$\begin{aligned}
(E : E_k E^2) &= \frac{(E : E^2)}{(E_k E^2 : E^2)}, \\
(E_k E^2 : E^2) &= (E_k : E^2 \cap E_k) = \frac{(E_k : E^2)}{(E^2 \cap E_k : E_k^2)} \quad \text{and} \\
(E^2 \cap E_k : E_k^2) &= (E^{(2)} : E_k),
\end{aligned}$$

we get $(E : E_k E^2) = 2^{\lambda-\kappa}(E^{(2)} : E_k)$, where λ and κ denote the $\mathbb{Z}$-ranks of E and E_k, respectively.

Putting all these together, we find

$$\begin{aligned}(R : R_\pi) &= 2^t h_k \frac{1}{(E^* : E_k E^2)(R_0 : H_k)} = 2^t h_k \frac{(E : E^*)(E^{(2)} : E_k)}{4(E : E_k E^2)} \\ &= 2^{t+\kappa-\lambda-2} h_k (E : E^*).\end{aligned}$$

Writing $(E : E^*) = (E : E_1E_2E_3)(E_1E_2E_3 : E^*)$, where the first factor is the unit index $q(K)$, we get

$$(R : R_\pi) = 2^{t+\kappa-\lambda-2} q(K) h_k (E_1E_2E_3 : E^*). \tag{3.13}$$

To calculate $(E_1E_2E_3 : E^*)$ we will find $(E_1E_2E_3 : E_1^*E_2^*E_3^*)$ and $(E^*/E_1^*E_2^*E_3^*)$ the ratio of whom will give the index desired and where E_i^* is defined as $E_i^* = \{e_i \in E_i \,|\, N_i e_i \in E_k^2\}$. After the construction we easily observe that;

Lemma 4. *We have*

$$E^*/E_1^*E_2^*E_3^* \simeq H_0/E_k^2. \tag{3.14}$$

Since E^* exactly consists of triples with each i^{th} component in E_i and all with the same norm mod E_k^2. We can define a map onto H_0/E_k^2 by assigning any i^{th} component to its norm modulo E_k^2. This is onto since for any $\alpha \in H_0$modulo E_k^2 there exists units in E_i ($i \in 1, 2, 3$) and we pick the product of these units which is already in E_k^2. The kernel of this map consists of tuples whose terms have norm in E_k^2. But this is exactly $E_1^*E_2^*E_3^*$. So we get the relation desired.

Now we will determine the index $(E_1E_2E_3 : E_1^*E_2^*E_3^*)$; so let us consider the homomorphism

$$\xi : E_1/E_1^* \times E_2/E_2^* \times E_3/E_3^* \longrightarrow E_1E_2E_3/E_1^*E_2^*E_3^*,$$

Letting $\overline{e}_1$ denote the coset $e_iE_i^*$ we find

$$\ker \xi = \{(\overline{e}_1, \overline{e}_2, \overline{e}_3) : e_1e_2e_3 = u_1u_2u_3 \text{ for some } u_i \in E_i^*\}.$$

If $(\overline{e}_1, \overline{e}_2, \overline{e}_3) \in \ker \xi$; then $e_1e_2e_3 = u_1u_2u_3$ for some $u_i \in E_i^*$. We replace the $\overline{e}_i = e_iE_i^*$ by $e_iu_i^{-1}E_i^*$, so get $e_1e_2e_3 = 1$. When σ is the element of Galois group

fixing $(e_1e_2e_3)^{1+\sigma} = e_1^2N_2e_2N_3e_3 = 1$, and this implies $e_2^2 \in E_k$; in a similar way we find that $e_2^2 \in E_k$ and $e_3^2 \in E_k$. If N_2e_2 were a square in E_k, so were N_3e_3, and e_1 would have to lie in E_k: but then $e_i \in E_i^*$ for $i = 1, 2, 3$, and $(\overline{e}_1, \overline{e}_2, \overline{e}_3)$ is trivial. So if $\ker\xi \neq 1$, we must have $e_i \in E_i \setminus E_k$ for $i = 2, 3$; but we have seen $e_i^2 =: \varepsilon_i \in E_k$, so we get $k_i = k(\sqrt{\varepsilon_i}\,)$ for $i = 2, 3$ and, therefore, $k_1 = k(\sqrt{\varepsilon_2\varepsilon_3}\,)$. Moreover,

$$\ker\xi = \{1, (\sqrt{\varepsilon_1}\cdot E_1^*, \sqrt{\varepsilon_2}\cdot E_2^*, \sqrt{\varepsilon_3}\cdot E_3^*)\}$$

in this case.

Thus we have shown that $\#\ker\xi \neq 1$ implies $u = 2$ and $\#\ker\xi = 2$, where the index $2^u = (E^{(2)} : E_k)$ was introduced above. If, on the other hand, $u = 2$, then $k_i = k(\sqrt{\varepsilon_i}\,)$ for units $\varepsilon_i \in E_k$, and $(\sqrt{\varepsilon_1}\cdot E_1^*, \sqrt{\varepsilon_2}\cdot E_2^*, \sqrt{\varepsilon_3}\cdot E_3^*)$ is a nontrivial element of $\ker\xi$. Therefore $\#\ker\xi = 2^v$ with $v = 2^u - u - 1$, and

$$(E_1E_2E_3 : E_1^*E_2^*E_3^*) = 2^{-v}\prod(E_i : E_i^*). \tag{3.15}$$

To determine $(E_i : E_i^*)$, we will use the group theoretical lemma which have been proved in preliminaries part:

Lemma 5. *Let G be a group and assume that H is a subgroup of finite index in G. If f is a homomorphism from G to another group, then*

$$(G : H) = (G^f : H^f)(G_fH : H),$$

where $G^f = \mathrm{im}f$, $G_f = \ker f$, and H^f is the image of the restriction of f to H.

We apply this lemma to $G = E_i$, $H = E_i^*$, and $f = N_i$. Then $G_f = \{\varepsilon \in E_i \,|\, N_i\varepsilon = 1\} \subseteq E_i^* = H$, $G^f = E_i^N = \{N_i\varepsilon \,|\, \varepsilon \in E_i\}$, and $H^f = E_k^2$; now Lemma 5 gives

$$(E_i : E_i^*) = (G : H) = (G^f : H^f) = (E_i^N : E_k^2). \tag{3.16}$$

Putting (3.13), (3.14), (3.15), (3.16) together, we find

$$\begin{aligned}(R : R_\pi) &= 2^{t+\kappa-\lambda-2}q(K)h_k(E_1E_2E_3 : E^*)\\ &= 2^{t+\kappa-\lambda-2}q(K)h_k\frac{(E_1E_2E_3 : E_1^*E_2^*E_3^*)}{(E^* : E_1^*E_2^*E_3^*)}\\ &= 2^{t+\kappa-\lambda-2-v}q(K)h_k\prod\frac{(E_i^N : E_k^2)}{(H_0 : E_k^2)},\end{aligned}$$

We have the following ambiguous class number formula for the quadratic extension k_i, the proof of which can be found among the lecture notes of Lemmermeyer's Global Class Field Theory course.

$$\#A_i = 2^{\delta_i-\kappa-2} h_k \cdot (E_i^N : E_k^2), \tag{3.17}$$

where δ_i denotes the number of (finite and infinite) places in k that are ramified in k_i/k.

Since $\#A = \prod \#A_i$, we obtain that

$$\#A = 2^{\delta_1+\delta_2+\delta_3-3\kappa-6} h_k^3 \cdot \prod (E_i^N : E_k^2);$$

by 3.11 dividing by 3.13 yields

$$\#\ker j^* = 2^{t_1+t_2+t_3-t+d_1+d_2+d_3+\lambda-4\kappa-4+v} h_k^2 \cdot (H_0 : E_k^2)/q(K), \tag{3.18}$$

Now we will show the following index relation for a neater formula.

Claim 5. *Let t_i be the finite part of δ_i and d_i be infinite part of δ_i where δ_i denotes the number of prime ideals in k ramified in k_i/k, then $\delta_i = t_i + d_i$ and*

$$2^{t_1+t_2+t_3} = 2^t \prod e(\mathfrak{p}), \quad 2d = d_1 + d_2 + d_3, \quad \textit{and} \quad \lambda - 4\kappa = 3 - 2d \tag{3.19}$$

where t denotes the number of ramified finite primes and d number of infinite primes in K/k also λ is the unit index of K and κ is the unit index of k.

Proof. For ramified finite primes $\mathfrak{p}$ it has either $e(\mathfrak{p}) = 4$, or $e(\mathfrak{p}) = 2$, if $e(\mathfrak{p}) = 4$ the inertia field becomes k so $\mathfrak{p}$ ramifies in all subextensions. On the other hand when $e(\mathfrak{p}) = 2$, we get that inertia field has index 2 over k, that is there exists only 2-extension in which $\mathfrak{p}$ is unramified. So it ramifies in two of the k_i's, this gives us the first relation. Now let κ be the map corresponding to an infinite prime. At this point we should note that this infinite prime ramifies in the extension $k\sqrt{m}$ if and only if $\kappa(\sqrt{m}) < 0$. Say $k_1 = k(\sqrt{m})$, $k_2 = k(\sqrt{n})$, $k_3 = k(\sqrt{mn})$. As $\kappa(\sqrt{mn}) = \kappa(\sqrt{m}).\kappa(\sqrt{n})$ we see that any infinite prime ramifies in two of the subextensions or does not ramify in any. This gives the second equation.

We have $n = (k : \mathbb{Q}) = r_k + 2s_k$ since $(K : k) = 4$ we get $4n = (K : Q) = r_K + 2s_K$ (where (r,s) refers to number of real and non-real infinite places). If none of the primes ramify we get $r_K = 4r_k, \quad s_K = 4s_k$, but if d of the infinite primes in k ramifies we get $r_K = 4(r_k - d)$ and $s_K = \frac{1}{2}(4n - 4(r_k - d)) = 4s_k + 2d$. Finally we calculate the unit index of k denoted as κ, $\kappa = r_k + s_k - 1 =$ and

$$\lambda = r_K + s_K - 1 = 4(r_k - d) + 4s_k + 2d - 1 = 4\kappa - 2d + 3.$$

This gives the relation $\lambda - 4\kappa = 3 - 2d$. □

Now we are ready to get the neat formula, for this we should remember what relations we have and do the proper substitutions:

We obtain from 3.19 and 3.18 that

$$\#\ker j^* = 2^{v-1} h_k^2 \prod e(\mathfrak{p}) \cdot (H_0 : E_k^2)/q(K).$$

by 3.8 , multiplying this with $(H : H_0)$, we get

$$\#\ker \widehat{j} = (H : H_0).\#\ker j^* = 2^{v-1} h_k^2 \prod e(\mathfrak{p}) \cdot (H : E_k^2)/q(K), \tag{3.20}$$

Having

$$h(K) = \frac{\mathrm{cok} j}{\ker j} \cdot h_1 h_2 h_3.$$

and the relation

$$h_k \cdot \frac{\mathrm{cok} j}{\ker j} = \frac{\mathrm{cok}\widehat{j}}{\ker \widehat{j}}. \tag{3.21}$$

knowing already $\mathrm{cok}\widehat{j}$ by 3.7 We get that

$$h(K) = 2^{d-\kappa-2-v} q(K) h_1 h_2 h_3 / h_k^2. \tag{3.22}$$

In particular,

$$h(K) = \begin{cases} \frac{1}{4} q(K) h_1 h_2 h_3 & \text{if } k = \mathbb{Q} \text{ and } K \text{ is real,} \\ \frac{1}{2} q(K) h_1 h_2 h_3 & \text{if } k = \mathbb{Q} \text{ and } K \text{ is complex,} \\ \frac{1}{4} q(K) h_1 h_2 h_3 / h_k^2 & \text{if } k \text{ is a complex quadratic extension of } \mathbb{Q}. \end{cases}$$

Example

Let us calculate the class number formula of the extension $K = \mathbb{Q}(\sqrt{-5}, \sqrt{6})$. Let $k_1 = \mathbb{Q}(\sqrt{-5})$, $k_2 = \mathbb{Q}(\sqrt{6})$, $k_3 = \mathbb{Q}(\sqrt{-30})$. Since K is complex we have the formula $h(K) = \frac{1}{2}q(K)h_1h_2h_3$. For quadratic number fields with small discriminants, it is not a big deal to calculate the class number. Actually we get that $h_1 = 1$, $h_2 = 2$ and $h_3 = 4$. The main task is to find $q(K)$. After finding the fundamental units, which is $\varepsilon = 5 + 2\sqrt{6}$ we test whether its square roots are also units. $\sqrt{\varepsilon} = \sqrt{2} + \sqrt{3}$, and $\sqrt{-\varepsilon} = i(\sqrt{2} + \sqrt{3})$. But these are not elements of K. Hence we see that every unit of K is included in one of the subextensions. That is $q(K) = 1$ and it turns out that $h(K) = 4$.

Bibliography

[1] E. J. Amberg, *Über den Körper, dessen Zahlen sich rational aus zwei Quadratwurzeln zusammensetzen*, Diss. Zurich, 1897

[2] P. Bachmann, *Zur Theorie der complexen Zahlen*, J. Reine Angew. Math. **67** (1867), 200–204

[3] Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. **29** (1967), 281–285

[4] F. Halter-Koch, *Ein Satz über die Geschlechter relativ-zyklischer Zahlkörper von Primzahlgrad und seine Anwendung auf biquadratisch-bizyklische Zahlkörper*, J. Number Theory **4** (1972), 144–156

[5] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, 2nd ed. Springer-Verlag 1985

[6] G. Herglotz, *Über einen Dirichletschen Satz*, Math. Z. **12** (1922), 255–261

[7] G.J. Janusz, *Algebraic Number Fields*,2nd ed. AMS 1996),

[8] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo Sec. I **4** (5) (1943), 383–406

[9] S. Kuroda, *Über die Klassenzahlen algebraischer Zahlkörper*, Nagoya Math. J. **1** (1950), 1–10

[10] T. Kubota, *Über die Beziehungen der Klassenzahlen der Unterkörper des bizyklischen biquadratischen Zahlkörpers*, Nagoya Math. J. **6** (1953), 119–127

[11] T. Kubota, *Über de bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65–85

[12] F.Lemmermeyer, *Kuroda's Class Number Formula*, Acta Arithmetica.LXVI.3 (1994),

[13] C. D. Walter, *Kuroda's class number relation*, Acta Arith. **35** (1979), 41–51