6-2020

On the Divisor Class Group and Special Units of Multiquadratic Real Fields

John E. Basias
The Graduate Center, City University of New York

On the divisor class group and special units of multiquadratic real fields.

by

John Basias

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2020

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirements for the degree of Doctor of Philosophy.

Victor Kolyvagin

_____ _____

Date Chair of Examining Committee

Ara Basmajian

_____ _____

Date Executive Officer

Victor Kolyvagin

_____

Kenneth Kramer

_____

Alexander Gamburd

_____

_____

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

On the divisor class group and special units of multiquadratic real fields.

by

John Basias

Advisor: Victor Kolyvagin

We study the 2-primary component $Cl_{K,2^\infty}$ of the divisor class group of multiquadratic real extension K of $\mathbb{Q}$ under the assumption that for all quadratic subextensions k of K 2-primary components of their divisor class groups are generated by ramified prime divisors. Then $Cl_{K,2^\infty} = Cl_{K,2^n}$, where $2^n = [K:\mathbb{Q}]$, and we study $r_K = dim_{\mathbb{Z}/2\mathbb{Z}}(2^{n-1}Cl_{K,2^n})$.

We show that $r_K \leq r_K^+ \leq r_K^{++}$, where r_K^+, r_K^{++} are non-negative integers explicitly described in much by means of values of Legendre symbols $(\frac{a}{b})$, where $(a,b) = 1$ a,b are square-free divisors of the product of discriminants of the fields k. We obtain sufficient conditions for equality $r_K = r_K^+$ to hold.

In the case $n = 3$ ($r_K = r_K^+$ if $n = 2$) we prove that $r_K - r_K^+ \leq 2$ with further estimates under additional conditions on K.

We also study the special units of K which play an important role in our study of r_K.

Acknowledgements

I want to especially thank professor Victor Kolyvagin for all his guidance and patience with my research. I also thank the teachers who showed me the joy and intrigue of mathematics as well as introducing mathematical problem solving and research, which include: my high school math teachers Larry Zimmerman and Dr Brandler, all the graduate school professors that teach Modern Algebra, Number Theory, Differential Geometry, Algorithms and Matrix Multiplication, Complex Analysis and Topology. Each of these graduate classes were in their own way intriguing and forged a foundation from which emanated my further mathematical endeavors. These professors included (in relative order) Lucien Schpiro, Petche, Dan Lee and Scott Wilson, Victor Pan, Jun Hu and Linda Keen, Rob Thompson as well as Alexander Gamburd (who also teaches Number Theory). I also extend my thanks to the defense committee. Above all, I am grateful to my immediate family, who prayed and supported me, while I was working for my PHD in Mathematics. In particular, I sincerely thank my mother Evanthia, father Emmanuel and sister Christina for encouraging me through the bad times and the good . My debt to you could never be fully repaid.

Thank you once more.

Introduction

Let K be a multiquadratic extension of $\mathbb{Q}$: K is an abelian extension of $\mathbb{Q}$ with $Gal(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^n$, $n \geq 2$. Let for a finite extension $L/\mathbb{Q}$, Cl_L denote the divisor class group of L. Let $\psi : \prod_k Cl_k \to Cl_K$, where the product is taken over all quadratic subfield k of K, is the product of natural homomorphisms $Cl_k \to Cl_K$, induced by inclusions $k \subset K$. If $n = 2$, Kubota [2] showed that the kernel and the cokernel of ψ are 2-elementary groups, in particular , if ℓ is an odd prime, ψ induced an isomorphism of the product of ℓ-primary components of Cl_k to the ℓ-primary component of Cl_K. The result of Kubota is compatible with a previous result of Herglotz [3], according to which $[Cl_K] = m\prod_k [Cl_k]$ where $m =$ 1,2 or 4, if $n = 2$ and K is real. In the case $n = 2$, K is real, the relationship between the 2-primary components of Cl_k and the 2-primary component of Cl_K was further studied in the work [1] of Sime. The work [1] inspired our study.

In general, see the proposition 1.2, $2^{n-1}ker(\psi) = 2^{n-1}coker(\psi) = 0$. Suppose that for each quadratic subextension k of K 2-primary component $Cl_{k,2^\infty}$ of Cl_k is 2-periodic: $Cl_{k,2^\infty} = Cl_{k,2}$. Then $2^n Cl_{K,2^\infty} = 0$. Hence $Cl_{K,2^\infty} = Cl_{K,2^n}$ and $Z_K = 2^{n-1}Cl_{K,2^n}$ is a 2-

periodic group.

Let r_K be the dimension (over $\mathbb{Z}/2\mathbb{Z}$) of Z_K, we call it 2^n-rank of Cl_K: it is the number of copies of $\mathbb{Z}/2^n\mathbb{Z}$ in the decomposition of $Cl_{k,2^\infty}$ into the sums of cyclic groups: $Cl_{K,2^\infty} \xrightarrow{\sim} (\mathbb{Z}/2^n\mathbb{Z})^{r_K} \oplus (2^{n-1}$-periodic group).

Our goal is the study of r_K for the multiquadratic real field K under the assumption (like in [1]) that for each k the ramified prime divisors of k generate $Cl_{k,2^\infty}$ (we call this condition the ramified divisors condition for K). The work [1] studied the case $n = 2$. We study the case $n \geq 2$, with more detail consideration of the case $n = 3$, where complications in the comparison with the case $n = 2$ are already presented.

The proposition 1.1, inspired by lemma 3.3 in [1], and results from algebraic number theory imply the proposition 1.4 according to which $Z_K = \rho(A)$, where A is the subgroup in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by odd primes splitting in K, and $\rho(p)$= the projection to $Cl_{K,2^\infty}$ of $\prod_k p_k$, where p_k is a prime divisor of k dividing p ($\rho(p)$ does not depend on the choices of p_k).

Let SF be the group of positive square-free integers with the group operation induced by the bijection $SF \to \mathbb{Q}_+^*/(\mathbb{Q}_+^*)^2$. Let R be the subgroup in SF generated by primes ramified in K (primes dividing the product of the discriminants $D(k)$ of the fields k). Let V be the subgroup of SF such that $K = \mathbb{Q}(\sqrt{V})$. Consider the homomorphism $\gamma : R/V \to Cl_{K,2}$: $\gamma(c)$ = the divisor class of the divisor $(c)^{1/2}$ of K. Then $Im(\psi_2) = \gamma(R/V)$, where ψ_2 is

the restriction of ψ to $\prod_k Cl_{k,2}$ (see the proposition 1.2 for more details).

And $\rho = \psi_2 \circ \alpha$, $\alpha : A \to \prod_k Cl_{k,2}$, where k-component of $\alpha(p)$ is the projection of p_k to $Cl_{k,2} = Cl_{k,2^\infty}$ (see the section 1.2 for more details).

Our way to determine r_K is to construct an explicit space (subspace in $(\mathbb{Z}/2\mathbb{Z})$-vector space) $X \subset R/V$ such that $\gamma(X) = Z_K$. Then $r_K = dim(X/(X \cap ker(\gamma))$ and the problem of explicit description of $ker(\gamma)$ arises as another ingredient of our study.

Here the special units of K enter the scene. Namely a unit u of K is called special for K if $\exists c \in \mathbb{Q}$ such that $u/c \in K^2$. Then $C_K(u) \stackrel{def}{=}$ the set of square free integers c such that $u/c \in K^2$. If $u > 0$ (we consider K to be a subfield of $\mathbb{R}$), $C_K(u)$ is a coset of V in R, so the homomorphism $\eta : S(K) \to R/V$ is defined, where $S(K)$ is the group of positive special units of K, $\eta(u) = C_K(u)$. Actually, $\eta(E_K^2) = 1$, where E_K is the group of units of K, so η induces the homomorphism $\eta : S(K)/E_K^2 \to R/V$.

Importance of special units for our study is because of the proposition 2.2: $Ker(\gamma) = Im(\eta)$, so $r_k = dim(X/(X \cap \eta(S(K))))$, and the problem of effective computation of $\eta(S(K))$ arises along with the problem of the construction of the space X.

The chapter 2 of our work is about the special units. Let ε_d be a fixed positive fundamental unit of $k = \mathbb{Q}(\sqrt{d})$. Let $S_0(K)$ be the subgroup of $S(K)$ of special units of K being the product of units of k: $u \in S_0(K) \Leftrightarrow u = \varepsilon_\Sigma \varepsilon^2$ is special, where $\Sigma \subset W = V \setminus \{1\}$, $\varepsilon_\Sigma = \prod_{d \in \Sigma} \varepsilon_d, \varepsilon \in \prod_k E_k$. It is well known that ε_d is special for k if the norm $N(\varepsilon_d)$ is equal

to 1, with explicit description of the set $C_k(\varepsilon_d)$, see, for example, [1]. We also present this information in the section 2.2 for convenience of the reader and consistency with further exposition. So $\varepsilon_\Sigma \in S_0(K)\ \forall \Sigma \subset W_+$, where $W_\pm \stackrel{def}{=} \{d \in W : N(\varepsilon_d) = \pm 1\}$.

If $N(\varepsilon_d) = -1$, then the special units of k are trivial: $S(k) = E_k^2$, however ε_Σ could be special for K if $\Sigma \subset W_-, |\Sigma| > 1$. In the case $n = 2$, the only possibility for $\varepsilon_\Sigma \in S_0(K), \Sigma \subset W_-$ is the case when $W = W_-$ and $\Sigma = W$. However the way to determine $C_K(\varepsilon_W)$ in this case is not presented in [1], this is the reason that r_K is determined in [1] in this case with error ≤ 1. Another simplification in the case $n = 2$ is that $S(K) = S_0(K)$, while for $n \geq 3$ apriory $S(K)^{2^{n-2}} \subset S_0(K)$, see the consequence 2.2, so one could encounter special units of K not belonging to $S_0(K)$.

In the section 2.3 we describe all special units $\varepsilon_\Sigma \in S_0(K), \Sigma \subset W_-$ and determine explicitly the sets $C_K(\varepsilon_\Sigma)$: see proposition 2.7. In particular, ε_Σ, with $\Sigma \subset W_-$, is special $\Leftrightarrow \prod_{d\in\Sigma} d$ is a square. The method to get these results is to extend the field $k = \mathbb{Q}(\sqrt{d})$, with $N(\varepsilon_d) = -1$, to the field $F = k(i)$, $i = \sqrt{-1}$. Then ε_d become special for F relative to $\mathbb{Q}(i)$: $\varepsilon_d/c \in F^2$ with $c \in \mathbb{Q}(i)$. This allows us to make analysis parallel to the computations in the section 2.2.

In the section 2.4 we study the relationship of special units of K with units in $S_0(K)$ by analyzing the effect of action of $Gal(K/\mathbb{Q})$ on special units. In particular, we obtain in the propositions 2.11, 2.12, 2.13 sufficient conditions to have $S(K) = S_0(K)$.

In the chapter 3, which is the joint work with professor V. Kolyvagin, we introduce the concept of an unoid and a m-unoid which model the sets $\Sigma \subset W_+$ with associated sets $C_k(\varepsilon_d)$. This is helpful to study the necessary conditions to have $u^2 = \varepsilon_\Sigma \varepsilon^2$, where $\Sigma \subset W_+$, $\varepsilon \in \prod_k E_k$, $u \in S(K)$. In particular, we introduce the 2-periodic group $ms(U_K)$ which is computable and such that the group $S(K)/S_0(K)$ injects in $ms(U_K)$, if $n = 3, W_+ \neq \emptyset$. We show, among other results, that $t_K = dim(ms(U_K)) \leq 2$ and describe all cases when $t_K = 2$, see the proposition 3.25.

In the chapter 4 we construct the explicit space X mentioned above. Like in the work [1] we use the duality between Cl_k/Cl_k^2 and the "primary" group $\Delta_d \subset k^*/k^{*2}$. This duality follows from the Kummer theory and the class field theory. The classical genus theory allows describe Δ_d explicitly (see the proposition 4.2). Under the ramified divisors condition the natural homomorphism $Cl_{k,2} \to Cl_k/Cl_k^2$ is an isomorphism, so an element a of $Cl_{k,2}$ is determined by values (a,e), where e generate Δ_d and $(,)$ is a pairing which produce the duality mentioned above. This allows for a prime $p \in A$ to describe $\alpha(p)$ in terms of Legendre symbols $(\frac{q}{p})$, where q runs through odd primes ramified in K. This allows to describe the group $H = \alpha(A)$, then $r_K = dim(H/H')$, where $H' = H \cap ker(\psi_2)$. Let $Y = \{\prod_k($ the divisor class of $\sqrt{a_k})$, $a_k \in SF, a_k | D(k)$, $\prod_k a_k$ is a square $\}$. Obviously, $Y \subset ker(\psi_2)$. In the case $n = 2$, $W \neq W_-$, $ker(\psi_2) = Y$. In the case $n = 2$, $W = W_-$ $dim(ker(\psi_2)/Y) \leq 1$.

Let $H'' = H \cap Y$, $r'_K = dim(H/H'')$. So Sime in [1] in the case $n = 2$ showed that $r_K = r'_K$ if $W \neq W_-$ and showed that $r_K = r'_K$ or $r_K = r'_K - 1$ if $W = W_-$.

In the chapter 4 we developed the use of the above duality to construct the space $X \subset R/V$, described in terms of matrices which entries are determined by values $(\frac{a}{b})$, where $(a,b) = 1$, $a,b \in R$. More precisely, according to the proposition 4.9

$$r_K = 2^n\text{-rank of } Cl_K = dim(\mathbb{L}/\mathbb{U}),$$

where $\mathbb{L} \subset B_{D''}, \mathbb{L} = Im(J), J : B_{D'} \to B_{D''}$ is a linear mapping defined by an explicit matrix $\mathbb{J}$. Here $R/V \overset{\omega}{\tilde{\to}} B_{D''}$, ω is an explicit isomorphism. Respectively homomorphisms γ, η carried to $B_{D''}$ become the homomorphisms $\gamma' : B_{D''} \to Cl_{K,2}$, $\eta' : S(K) \to B_{D''}$. $\mathbb{U} = \eta'(S(K)) \cap \mathbb{L}$.

We define $r_K^{++} = rank(\mathbb{J}) = dim(\mathbb{L})$. According to the consequence 4.2

$$r_K \leq r_K^{++} \leq m - e,$$

where $m = dim(B_{D'})$ =(the number of primes dividing at least one $d \in W$) - n, $e = 0$ or 1 (see the consequence 4.2). We note that $m' = dim(B_{D''}) = dim(R/V) = m + 1$ if all $d \in W$ are odd and $\exists d \in W, d \equiv 3 \pmod 4$, otherwise $m' = m$.

We define $\mathbb{U}_0$ to be $\mathbb{L} \cap \eta'(S_0(K))$, $r_K^+ = dim(\mathbb{L}/\mathbb{U}_0)$. So

$$r_k \leq r_K^+ \leq r_K^{++}$$

The numbers $r_K^{++} \geq r_K^+$ appear (under the ramified divisors condition for K) as upper

bounds for r_K explicitly determined and computable in result of our study. The checking the ramified divisors condition for $k = \mathbb{Q}(\sqrt{d}) \subset K$ and determination of r_K^{++} both require just finding the ranks of explicit matrices which entries are composed from the Legendre symbols, mentioned above.

To determine $\eta'(S_0(K))$ one can use (2.3) and the proposition 2.7. Note that in the case $d \in W_+$ the alternative way to determine $\eta'(\varepsilon_d)$, also solely dependable on values of Legendre symbols, is given by the proposition 4.3. Determinations of $\eta'(\varepsilon_\Sigma), \Sigma \subset W_-$, described in the proposition 2.7, requires to work with Gaussian integers.

We recall that if $n = 2$, then $\mathbb{U} = \mathbb{U}_0$, so $r_K = r_K^+$ is completely determined, in [1] it was done except for the case $W = W_-$, where r_K was determined up to an error ≤ 1.

In general, we have the rough bound

$$r_K - r_K^+ \leq 2^n - 1 - dim(\mathbb{U}_0),$$

where the right hand side is not smaller than $n_- = dim(W_- \cup \{1\})$, see (4.22). However, the propositions 2.11, 2.13 give sufficient conditions for the equality $r_K = r_K^+$.

In the case $n = 3$, if $W = W_-$ the proposition 4.12 gives a sufficient condition for the equality $r_K = r_K^+$ and proves that if this condition fails than $r_K = r_K^{++}$ or $r_K = r_K^{++} - 1$.

In the case $n = 3$, if $|W_+| > 0$, then the above bound for $r_K - r_K^+$ was significantly refined because of results in the chapter 3, which is the joint work with professor V. Kolyva-

gin. Namely, according to the proposition 3.2 the group $S(K)/S_0(K)$ injects in the computable 2-periodic group $ms(U_K)$ which is studied and described in details in the chapter 3, as an application of the general theory of unoids developed in this chapter. Let $t_K = dim(ms(U_K))$. Let $W_1 = \{d \in W, d \equiv 1 \pmod 4\}$, W_1 is a p-subspace (a space without 1) of W, always $|W_1| \geq 1$ (see the section 3.3). According to the proposition 3.24 $t_K \leq 2$ and $t_K \leq 1$ if $|W_1| > 1$. Hence if $n = 3, |W_+| > 0$, than

$$r_K - r_K^+ \leq 2$$

$$r_K - r_K^+ \leq 1 \text{ if } |W_1| > 1$$

$$r_K = r_K^+ \text{ if } t_K = 0$$

Computations with abstract unoids in the section 3.3 suggest that the proportion of cases when $t_K > 0$ decreases rapidly when $\tau(W)$ grows. Here $\tau(W)$ = the number of primes dividing at least one element of W. In the section 3.6 this suggestion got more evidence by more close watching the special cases (rather than abstract unoids) of unoids U_K (see the definition of U_K in the section 3.1) because of the propositions 3.26, 3.27 and computations followed. In particular, the case $t_K = 0$ appears to be a frequent case, in this case (under the ramified divisors condition for K) $r_K = r_K^+$ is fully determined by result of our work.

Contents

Chapter 1

Kubota-type relations and their applications

1.1 Kubota-type relations and their consequences

Let M be a finite extension of $\mathbb{Q}, q$ be a rational prime, K/M be an abelian extension with $G = Gal(K/M) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^n$. The following proposition 1.1 is inspired by lemma 3.3 in [1] (in which, in particular, $q = 2, n = 2$)

Proposition 1.1. *Let a be a divisor or an element of K. Then*

$$\prod_{H \subset G. [G/H]=q} N_{K/K^H}(a) = a^{q^{n-1}} N_{K/M}(a)^{\frac{q^{n-1}-1}{q-1}} \tag{1.1}$$

proof: Let $m \geq 1, f(m) =$ the number of subgroups of index q in $(\mathbb{Z}/q\mathbb{Z})^m$. Let $1 \neq g \in G, X(g) =$ the set of subgroups of index q in G containing g. Let $< g >$ be the subgroup of G generated by g. The map $H \to (H+ < g >)/ < g >$ induces the bijection of $X(g)$ and the set of subgroups in $G/ < g >$ of index q. Hence $|X(g)| = f(n-1)$. We have

$$\prod_{H \subset G, [G/H]=q} \prod_{g \in H} g(a) = a^{f(n)} \prod_{g \neq 1} g(a)^{f(n-1)} = a^{f(n)-f(n-1)} (N_{K/M}(a))^{f(n-1)}.$$

We prove (1.1) if show that

$$f(m) = \frac{q^m - 1}{q-1} \tag{1.2}$$

Let $\phi : V = (\mathbb{Z}/q\mathbb{Z})^m \to \mathbb{Z}/q\mathbb{Z}$ be a non-zero homomorphism. $ker(\phi)$ is a subgroup of index q, and for subgroup H of V of index q, and for a subgroup H of V of index q, there are $q-1$ homomorphisms ϕ such that $\ker(\phi) = H$ (they correspond to the isomorphisms of $V/H \xrightarrow{\sim} \mathbb{Z}/q\mathbb{Z}$). So $(q-1)f(m) =$ the number of nonzero homomorphisms $=q^m - 1$ and (1.2) follows.

Let L be a finite extension of M, ${Cl_L}'$ be the factor-group of the divisor class group Cl_L of L by the natural image of Cl_M in Cl_L. Let

$\psi : \prod_{H \subset G, [G/H]=q} Cl'_{K^H} \to Cl'_K$ be the homomorphisms induced by the natural homomor-

phisms $Cl'_{K^H} \to Cl'_K$.

Proposition 1.2. *$ker(\psi)$ and $coker(\psi)$ are groups annihilating by q^{n-1}.*

proof: If $n = 1$, then ψ is just the identity map $Cl'_K \to Cl'_K$ and the proposition 1.2 follows. Suppose $n \geq 2$. The statement about $coker(\psi)$ follows immediately from (1.1). Suppose for each $H \subset G$, with $[G/H] = q$, x_H is a divisor of K^H and $\prod_H x_H = (b)c$ where $b \in K^*$ and c is a divisor of M.

Let $H_0 \subset G, [G/H_0] = q$, Let $L = K^{H_0}$. Taking $N_{K/L}$ from the above equality we obtain

$(\prod_{H \neq H_0} N_{K^H/M}(x_H))^{q^{n-2}} x_{H_0}^{q^{n-1}} = N_{K/L}(b)c^{q^{n-1}}$

This is because if $H \neq H_0$, the natural homomorphism $H_0 \to G/H$ is surjective because the image is equal to the image of $H_0 + H = G$. Also, counting cardinalities, we conclude that $|ker(H_0 \to G/H)| = q^{n-2}$. The relation proved shows $x_{H_0}^{q^{n-1}} = 1$ in Cl'_L. Hence $q^{n-1} ker(\psi) = 0$.

Consequence 1.1. *The homomorphism ψ is an isomorphism on ℓ-primary components if $\ell \neq q$.*

So the consequence 1.1 solves completely the problem of the description of Cl'_K in terms of the groups Cl'_{K^H} in ℓ-primary components for $\ell \neq q$.

The situation for $\ell = q$ is more delicate and is the subject of study in this work (with detail consideration of the case $M = \mathbb{Q}, q = 2, n = 3$).

The proposition 1.2, at least in the case when $M = \mathbb{Q}, q = 2, n = 2$ is due to Kubota (see [1]), taking into account the proposition 1.1 the generalizations above are straightforward.

1.2 Applications of Kubota-type relations for q-primary component of Cl'_K.

Proposition 1.3. *The group $Cl_{K,st}$ of classes of strictly equivalent divisors of K is generated by p_K where p runs through the set of all divisors of M coprime to a fixed integral divisor and splitting completely in K.*

proof: We recall that p_K denotes a prime divisor of K, $p_K|p$. In the proposition 1.3 we mean that for p all possible p_K are included in the generating set. Let K^{unr} be the maximal abelian unramified extension of K . By the class field theory K^{unr}/K is finite and the map $\theta : \pi \mapsto Fr_{\pi'}$, where π is a prime divisor of K and $Fr_{\pi'}$ is the frobenius automorphism in $Gal(K^{unr}/K)$ corresponding to a prime divisor π' of K^{unr}, $\pi'|\pi$ ($Fr_{\pi'}$ is independent of the choice of π'), induces an isomorphism $Cl_{K,st} \xrightarrow{\sim} Gal(K^{unr}/K)$. Let $C \in Cl_{K,st}$ be a divisor class, $g = \theta(c)$. By the Chebotarev density theorem there exist infinitely many prime divisors p of M such that p is unramified in K^{unr} and for some prime divisor π' of K^{unr} dividing p $f_{\pi'} \overset{def}{=}$(the frobenius automorphism corresponding to the Galois extension K^{unr}/M and π')=g. Then p splits completely in K because $f_{\pi'}|_K = g|_K = id$. In particular, $Fr_{\pi'} = f_{\pi'}$. Let π be the prime divisor of K such that $\pi'|\pi$. Then $\theta(\pi) = Fr_{\pi'} = f_{\pi'} = g = \theta(c) \Rightarrow \pi \in C$. We can satisfy the condition that $p \not|$(a fixed integral divisor of M) by

sorting away finitely many prime divisors.

Let $q = 2$ and $Cl'_{L,2^\infty}$ denotes the 2-primary component of the group Cl'_L, it is canonically defined as a subgroup and a factor group of Cl'_L. If a is a divisor of L, $(a)_2$ denotes the natural image of a in $Cl'_{L,2^\infty}$. We will denote by k quadratic extensions of M inside of K. Assume that $\forall k$ the group $Cl'_{k,2^\infty} = Cl'_{k,2} \stackrel{def}{=}$ subgroup of all elements of Cl'_k of order 2. If p is a prime divisor of M splitting in k, $(p) = \pi\lambda$, then $(\pi)_2(\lambda)_2 = (p)_2 = 1$, also $(\pi)_2^{-1} = (\pi)_2$ because $Cl'_{k,2^\infty}$ is 2-periodic by the condition. Hence $(\pi)_2 = (\lambda)_2$ and $(p_k)_2$ depends only on p and not on the choice of p_k.

Let ψ_2 be the homomorphism ψ, defined above, restricted to the 2-primary component, so

$\psi_2 : \prod_k Cl'_{k,2} \to Cl'_{K,2}$.

Let A be the subgroup in $I(M)/I(M)^2$ generated by prime divisors splitting in K ($\Leftrightarrow$ splitting in all k) and coprime to 2. We recall that $I(M)$ denotes the group of divisors of M. We have a well defined homomorphism $\alpha : A \mapsto \prod_k Cl'_{k,2}$ such thatα(the coset of p)$= \prod_k (p_k)_2$.

Let $\rho : A \mapsto Cl'_{K,2^\infty}, \rho = \psi_2 \circ \alpha$.

If we choose p_K and put $a = p_K, p_k = N_{K/k}(p_K)$ (1.1) implies that

$$\rho(p(\mathrm{mod}\ I(M)^2)) = (p_K)_2^{2^{n-1}} \tag{1.3}$$

The left hand side of (1.3) is 2-periodic and the proposition 1.3 implies that p_K generate $Cl'_{K,2^\infty}$(being the factor group of Cl_K).

We have proved

Proposition 1.4. *Suppose $Cl'_{k,2^\infty} = Cl'_{k,2}$ for all k. Then $Cl'_{K,2^\infty}$ is 2^n-periodic. Let $Z_K = (Cl'_{K,2^\infty})^{2^{n-1}} \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^m$. Then $Z_K = \rho(A)$.*

We define r_K to be the number m from the proposition 1.4 and call it 2^n-rank of Cl'_K : $Cl'_{K,2^\infty} \xrightarrow{\sim} (\mathbb{Z}/2^n\mathbb{Z})^{r_K} \oplus (2^{n-1} - \text{periodic group})$.

r_K in the case $M = \mathbb{Q}$(then $Cl'_L = Cl_L$), $n = 2$, K is real was studied in [1], our goal is to study r_K in the case $M = \mathbb{Q}, n \geq 3, K$ is real.

The proposition 1.4 is the starting point for this study.

Let $G' = G \setminus \{1\}$. Let $K(g)$ be the subfield of K fixed by $g \in G$. Let $\Sigma = \{g_1, g_2, g_1g_2\} \subset G'$. The relation $(1+g_1)+(1+g_2)+(1+g_1g_2) = 2+(1+g+1+g_2+g_1g_2)$ in $\mathbb{Z}[G]$ implies that if $r_{K(g)} = 0$, $\forall g \in \Sigma$, then $r_K = 0$. Hence we proved the following necessary condition for r_K to be bigger than 0:

Proposition 1.5. *Suppose $Cl'_{k,2^\infty} = Cl'_{k,2}$ for all k. For r_K to be bigger than 0 it is necessary that $\forall g_1, g_2 \in G$ such that $\Sigma = \{g_1, g_2, g_1g_2\} \subset G'$, $r_{K(g)} > 0$ for some $g \in \Sigma$.*

Chapter 2

The special units

2.1 The special units and ramified divisors.

We will assume further in the paper that $M = \mathbb{Q}, q = 2$ and K is real. By the Kummer theory such fields are in one-to-one correspondence with $\mathbb{Z}/2\mathbb{Z}$-subspaces of $\mathbb{Q}_+/{\mathbb{Q}_+}^2$ of dimension n ($\mathbb{Q}_+$ is the multiplicative group of positive rational numbers). Namely $K \mapsto V$ where $V = ((K^*)^2 \cap \mathbb{Q}^*)/{\mathbb{Q}_*}^2$ and the opposite map is $V \mapsto \mathbb{Q}(\sqrt[2]{V'})$ where V' is any full set of representatives of V in $\mathbb{Q}_+$. Let SF denote the set of positive square-free rational integers. Then $SF \mapsto \mathbb{Q}_+/{\mathbb{Q}_+}^2$ is the bijection and SF becomes canonicaly isomorphic to $\mathbb{Q}_+/{\mathbb{Q}_+}^2$ if we carry from it to SF the multiplication which we will denote by $\cdot$. Explicitly , if $a,b \in SF$, then $a \cdot b = ab/(a,b)$, where (a,b) is the $m.c.d(a,b)$. In the following we will mean by $V = V(K)$ the corresponding subspace of SF, so $K = \mathbb{Q}(\sqrt{V(K)})$. We will denote by $W = W(K)$ the set $V(K) \setminus \{1\}$, again $K = \mathbb{Q}(\sqrt{W(K)})$ and the quadratic subfields $k \subset K$ are the fields $\mathbb{Q}(\sqrt{d})$, $d \in W$. So we have $2^n - 1$ such subfields, this also

follows from $(1,2)$ and Galois theory.

The primes ramified in a quadratic extension $k = \mathbb{Q}(\sqrt{d})$ are those which divide the discriminant $D(k)$ of k which is equal to d if $d = 1 \pmod 4$ and is equal to $4d$, if $d \equiv 2,3 \pmod 4$ ([4], Ch 2, Sec7, Th .1). If $p|D(k)$ then p_k is the unique prime divisor of k such that $(p) = {p_k}^2$. The 2-elementary condition for k ($Cl_{k,2^\infty} = Cl_{k,2}$)is satisfied if $(p_k)_2$ generate $Cl_{k,2^\infty}$ when p runs through the prime divisors of $D(k)$. We will prove later in proposition 4.3 that it is equivalent to 2-elementary condition for k if d is divisible by a prime $\equiv 3 \pmod 4$ and is equivlent to 2-elementary condition for k together with the condition that the norm of a fundamental unit of k is equal to -1 if d is not divisible by a prime $\equiv 3 \pmod 4$. So if 2-elementary condition holds for k we can use $p_k, p|D(k)$, as generators for $Cl_{k,2}$.

Let R be the subspace in SF generated by primes ramified in K
(primes dividing $\prod_k D(k)$). If $c \in R$, then (c) is a square in $I(K)$. If the 2-elementary condition holds for K, what means that is holds for every $k \subset K$, then $Im(\psi_2)$ consists of divisor classes of $(c)^{1/2}$, where c runs through R, so the natural question arsing is if $c \in R$ when $(c)^{1/2}$ is a principal divisor of K.

Proposition 2.1. *For $c \in R, (c)^{1/2}$ is a principal divisor of $K \Leftrightarrow \exists$ a positive unit ε of K such that $\varepsilon = ca^2$, where $a \in K^*$.*

proof: If $\varepsilon = ca^2$, then $(1) = (c)(a)^2 \Rightarrow (c)^{1/2} = (a)^{-1}$ is principal. Suppose $(c)^{1/2} = (b)$, where $b \in K^*$. Then $(c) = (b)^2 \Rightarrow c = \varepsilon b^2$ for a positive unit ε of $K \Rightarrow \varepsilon = ca^2$, where

$a = b^{-1}$.

Let ε be a unit of K. We define the set $C_K(\varepsilon)$ to be the set of square-free integers c (not necessarily positive) such that $\varepsilon/c \in (K^*)^2$. We call a unit ε a special unit for K if $C_K(\varepsilon)$ is non-empty, then $C_K(\varepsilon)$ is the $V(K)$-orbit(a coset of $V(K)$) in the group of square free integers(by the Kummer theory): $C_K(\varepsilon) = V(K) \cdot c$ for any $c \in C_K(\varepsilon)$.

If $\varepsilon > 0$, then $C_K(\varepsilon)$ is $V(K)$-orbit in R, because if $\varepsilon = ca^2 \Rightarrow c > 0$ and (c) is a square in $I(K) \Rightarrow$ if a prime $p|c$, then p is ramified in K.

Obviously, the product of two special units is a special unit. Let $S(K)$ be the group of positive special units for K. Consider the homomorphism $\gamma : R \to Cl_{K,2}$ such that $\gamma(c) =$ the divisor class of $(c)^{1/2}$. The subspace $V = V(K) \subset ker(\gamma)$, so we have the induced homomorphism $\gamma : R/V \to Cl_{K,2}$. Let us define the homomorphism $\eta : S(K) \to R/V$ by $\eta(\varepsilon) =$ the coset $C_K(\varepsilon)$. The proposition 2.1 implies

Proposition 2.2. *$Ker(\gamma) = Im(\eta)$, so $Im(\psi_2) = \gamma(R/V) \xrightarrow{\sim} (R/V)/\eta(S(K))$*

The proposition 2.2 shows the importance of special units for our study: in order to determine r_K we must determine explicitly the group $\eta(S(K))$, another necessary ingredient is to identify explicitly the subset $X \subset (R/V)/\eta(S(K))$ corresponding(via the above isomorphism) to the subspace $\psi_2(\alpha(A)) \subset Im(\psi_2)$. Then $r_k = dim(X)$.

Solving these two problems will constitute the following content of our work.

2.2 Special units for quadratic real fields

The simplest source of special units for K would be special units for its quadratic subfields, so we start our study of special units with determination of special units for k and the sets $C_k(\varepsilon)$.

The content of this section is well known, we present it for the convenience of the reader and for further references and consequences. For a subfield $L \subset K$ the group $S(L)$ trivially contains the group E_L^2, where E_L is the group of units of L, and for a unit ε of L the set $C_L(\varepsilon)$ depends only on $\varepsilon(\bmod {E_L}^2)$.

It is known that for the real quadratic field $k = \mathbb{Q}(\sqrt{d})$ the group of positive units of k is isomorphic to $\mathbb{Z}$, its generators are called fundamental units of k, there are two of them, they are equal mod $({E_k}^2)$, as one is the inverse of the other one. So it is enough for a fixed fundamental unit ε of k to answer if it is a special unit of k and if it is to determine the set $C_k(\varepsilon)$, what means to describe explicitly a single $c \in C_k(\varepsilon)$, because then $C_k(\varepsilon) = \{c, c \cdot d\}$ by the above.

It is obvious that the necessary condition for a unit $u \in k$ to be a special is that $N_{k/\mathbb{Q}}(u) = 1$. So if a fundamental unit of k has norm -1, then there are no non-trivial special units for $k : S(k) = {E_k}^2$ (note that the homomorphism η is trivial on ${E_k}^2$). So we suppose now that ε is a positive unit of $k = \mathbb{Q}(\sqrt{d})$, $d \in SF, d \neq 1$, and the norm of ε is equal to 1.

Let $\varepsilon = a + b\sqrt{d}$, where $a, b \in \mathbb{Q}$. Note that $a, b \in \mathbb{Z}$ if $d \equiv 2,3$ (mod 4); $a, b \in \frac{1}{2}\mathbb{Z}$ if $d \equiv 1$(mod 4). ([2],Ch 2, Sec 7.1,Th 1). The unit ε has norm $1 \Rightarrow a^2 - b^2 d = 1 \Rightarrow (a-1)(a+1) = b^2 d$. Let $\delta = (2(a-1), 2(a+1))$. Then $\delta = 1, 2$ or 4 when a is half an integer, even integer or odd integer respectively. Then

$$(\frac{2(a-1)}{\delta})(\frac{2(a+1)}{\delta}) = \frac{4b^2 d}{\delta^2} \tag{2.1}$$

with 2 coprime factors on the left hand side. If $\delta = 1$ then $a = \alpha/2$ where α is an odd integer, then the left hand side of (2.1) is equal to $\alpha^2 - 4$, we conclude that $b = \beta/2$ where β is an odd integer.

So $d = (\alpha^2 - 4)/\beta^2 \equiv 1$ (mod 4). If $\delta = 2$, then $a = 2\alpha, \alpha \in \mathbb{Z}$, so that the left hand side of (2.1) is equal to $(2\alpha - 1)(2\alpha + 1) = -1 + 4\alpha^2$, we conclude from (2.1) that b is an odd integer. so $d = (-1 + 4\alpha^2)/b^2 \equiv 3$ (mod 4). We showed that if $\delta = 1, 2$ then $d \equiv 1, 3$ (mod 4) respectively.

Taking into account that d is square-free integer and representing factors of the left hand side of (2.1) as products of square free integers and a square, we get uniquely defined square-free integers r, s and integers m, n (m, n defined up to sign change for both) such that

$$(\frac{2(a-1)}{\delta}) = m^2 r, (\frac{2(a+1)}{\delta}) = n^2 s, rs = d, mn = \frac{2b}{\delta} \tag{2.2}$$

(2.2) implies that $\frac{4a}{\delta} = m^2 r + n^2 s$. Now $\frac{4\varepsilon}{\delta} r = \frac{4}{\delta}(a + b\sqrt{d})r = m^2 r^2 + n^2 sr + 2mnr\sqrt{d} = (mr + n\sqrt{d})^2$.

We proved that if $\delta = 1$ or 4 then $\varepsilon/r \in k^{*2}$, in particular, $r > 0$ and $r = 1$ or $d \Leftrightarrow \varepsilon$ is a square in k. If $\delta = 2$ (then $d \equiv 3 \pmod 4$) $\varepsilon/(2r) \in k^{*2}$, in particular, $r > 0$ and ε is not a square in k, because $2r \neq 1$ or d. Let $\alpha = \frac{2(a-1)}{\delta}, 0 < r' = m.c.d(\alpha, d)$. Then $r = r'$.

Really, (2.2) $\Rightarrow r|r'$. Now, if p is a prime, $p|r'$, then $p|\alpha$, so (2.1) $\Rightarrow p|r$ (the factors on the left hand side of (2.1) are coprime). Hence $r'|r$ (r' is square-free), so $r' = r$. We summarize the above in

Proposition 2.3. *Let $\varepsilon = a + b\sqrt{d}$ is a positive unit of $k = \mathbb{Q}(\sqrt{d})$ with norm = 1. Let $\alpha = 2(a-1), (a-1)/2, a-1$, when a is half an integer, odd integer, even integer respectively. Then $d \equiv 1$ (mod 4), 3(mod 4) is the first, third cases respectively.*

Let $0 < r = mcd(\alpha, d)$. Then ε is a special unit for k with

$$C_k(\varepsilon) = \{r, d/r\}, C_k(\varepsilon) = \{2r, 2(d/r)\} \tag{2.3}$$

In the first and second, in the third cases respectively

Consequence 2.1. *In the notations of proposition 2.3 ε is not a square in k iff the first and second case happens with $r \neq 1$ or d or the third case happens.*

Then a fundamental unit ε_d of k has norm = 1 and $C_k(\varepsilon_d)$ is described by (2.3).

In [2],Ch 2, Sec 7.3 an algorithm to determine a fundamental unit ε_d using the theory of continued fractions is presented. Then (2.3) for $\varepsilon = \varepsilon_d$ determine $C_k(\varepsilon_d)$ in the case $N(\varepsilon_d) = 1$. Also one can try units ε of k with norm 1 and if the condition of consequence 2.1 is satisfied then a fundamental unit ε_d of k has norm 1 and $C_k(\varepsilon_d) = C_k(\varepsilon)$ explicitly described by (2.3).

2.3 The description of the group $S_0(K)$.

Let the group $S_0(K)$ be the subgroup of the group $S(K)$ of units being the product of units of quadratic subfields of K. Up to squares any $\varepsilon \in S_0(K)$ is represented as $\varepsilon_\Sigma = \prod_{d\in\Sigma} \varepsilon_d$, where ε_d is a fixed fundamental unit of $\mathbb{Q}(\sqrt{d})$ (positive) and Σ is a subset of $W = W(K)$. We know (see section 2.2) that each ε_d with $N(\varepsilon_d) = 1$ is special, so it is enough to find out which ε_Σ with $\Sigma \subset W_-$ are special for K and determine explicitly the set $C_K(\varepsilon_\Sigma)$ for them. Here Σ_+, Σ_- are subsets of Σ consisting of all d such that $N(\varepsilon_d) = 1, -1$ respectively.

We know that ε_d with $d \in \Sigma_-$ is not special for $k = \mathbb{Q}(\sqrt{d})$, it is also not special for K. Really if $\varepsilon_d \in ca^2, a \in K$, then $a^2 \in k$ and $a^2 \in W(k^*)^2$ by the Kummer duality. Hence ε_d

is special for k which is impossible. But for $\Sigma \subset W_-, |\Sigma| > 1$ ε_Σ could be special for some Σ and this is what we are going to study in this section.

The useful idea is to consider the field $F = F_d = k(i)$. Then $-1 = N(\varepsilon_d) \Rightarrow -1 = a^2 - b^2 d$ if $\varepsilon = \varepsilon_d = a + b\sqrt{d}$ with $a, b \in (\frac{1}{2})\mathbb{Z}$. Then

$$(2a - 2i)(2a + 2i) = 4b^2 d \tag{2.4}$$

and we can make analysis parallel to the computations of section 2.2 with the ring $\mathbb{Z}$ replaced with the ring $\mathbb{Z}[i]$ of integers of the field $g = \mathbb{Q}(i)$. We will find that ε is special for the extension F/g, namely $\varepsilon \in \mathbb{Z}[i]F^2$ and this will help to determine for which $\Sigma \subset W_-$ ε_Σ is special and how the set $C_K(\varepsilon_\Sigma)$ can be effectively computed.

Note that $2a \mp 2i$ is not divisible by any odd rational prime. If $p \equiv 3 \pmod 4$, then p remains a prime in g, hence p does not divide l.h.s of (2.4)$\Rightarrow$ p does not divide r.h.s (2.4). In particular, any odd prime p dividing d must be equal to 1 (mod 4). We proved

Proposition 2.4. *The necessary condition for $N(\varepsilon_d) = -1$ is that all odd prime divisors of d are equal to 1 (mod 4).*

The prime 2 ramifies in $g : 2i = (1+i)^2$, and $1+i$ represents the unique prime divisor of

g dividing 2.

Let δ represents $m.c.d(2a-2i, 2a+2i)$. Then $\delta|4$. Now $4 \not| (2a-2i)$, and also if $(1+i)|(2a-2i)$, then $(1+i)|2a \Rightarrow 2|2a \Rightarrow 2|\delta$. So δ can be chosen to be 1 or 2 or $2(1+i)$.

Proposition 2.5. *$\delta = 1 \Leftrightarrow a$ is a half integer (and not an integer), $\delta = 2 \Leftrightarrow a$ is an even integer. $\delta = 1$ or $2 \Leftrightarrow d \equiv 1$ (mod 4). $\delta = 2(1+i) \Leftrightarrow a$ is an odd integer $\Leftrightarrow d \equiv 2$ (mod 4). $\beta \stackrel{def}{=} (2a-2i)/\delta \equiv 1$ (mod 2) $\Leftrightarrow \delta = 1$ or $\delta = 2(1+i)$ and $a \equiv 3$ (mod 4).*

proof: If a is an integer, $2|\delta$. So $\delta = 1 \Rightarrow a$ is a strict half integer: $a = \alpha/2$, where α is an odd integer. Then $\beta = \alpha - 2i \equiv 1$ (mod 2), in particular, $\delta = 1$ if a is a strict half integer. Suppose a is an integer. Then $a - i \equiv i$ (mod 2) $\not\equiv 1$ (mod 2), if a is even, so $\delta = 2$ in this case and $\beta \not\equiv 1$ (mod 2). If a is an odd integer, then $a - i = a + 1 - (1+i) = (1+i)(-1 + \frac{a+1}{2}(1-i)) \Rightarrow \delta = 2(1+i)$ and $\beta \equiv 1$ (mod 2) $\Leftrightarrow a \equiv 3$ (mod 4). Now (2.4) implies that $\delta = 1 \Leftrightarrow b$ is a strict half integer and d is odd, $\delta = 2 \Leftrightarrow b$ is an odd integer and d is odd, $\delta = 2(1+i) \Leftrightarrow b$ is an odd integer and $2|d$. The proposition 2.4 is proved.

Let $T = T(\Sigma)$ be the set of primes dividing at least one $d \in \Sigma$. Let odd $p \in T$. By the proposition 2.4 $p \equiv 1$ (mod 4). Let $n_p, m_p \in \mathbb{N}, n_p^2 + m_p^2 = p$. Assume that m_p is even and put $p(g) = n_p + m_p i$ - the prime of g, $p(g)\overline{p(g)} = p$ ($\bar{x}$ denotes the complex conjugate of x)

Let $d' = d$ if d is odd, $d' = d/2$ if d is even. (2.4) implies that

$$\beta\overline{\beta} = ((2b)^2/(\delta\overline{\delta}))d \tag{2.5}$$

where $\beta = \frac{2a-2i}{\delta} \in \mathbb{Z}[i]$ is not divisible by $1+i$, $(\beta, \overline{\beta}) = 1$. Hence $\forall p|d\ \beta$ is divisible by one and only one prime from the set $\{p(g), \overline{p(g)}\}$. We define $\sigma(p(d) \in Gal(\mathbb{C}/\mathbb{R})$ to be id if $p(g)|\beta$, to be the complex conjugation if $\overline{p(g)}|\beta$. Let

$t_g = t_g(d) = \prod_{odd\ p|d} p(g)^{\sigma(p,d)}$

Then $t_g\overline{t_g} = d'$ and $\delta\overline{\delta}(d/d')$ is even power of 2, so (2.5) $\Rightarrow (\beta/t_g)(\overline{\beta/t_g})$ is a square in $\mathbb{Z}[i]$, so the divisor of β/t_g is a square because the factors in the product are coprime.

So we can choose $m \in \mathbb{Z}[i], i(d) \in \{1, i\}$ such that $\beta = i(d)t_g m^2$ (the units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$ and $-1 = i^2$). Taking into account that $i(d) = 1 \Leftrightarrow i(d) \equiv 1 \pmod 2, t_d \equiv 1 \pmod 2, m^2 \equiv 1 \pmod 2$ ($(1+i) \not| m$) and the proposition 2.5 we conclude that $i(d) = 1$ if $\delta = 1$ or $\delta = 2(1+i)$ ($\Leftrightarrow d$ is even) and $a \equiv 3$ (mod 4), otherwise $i(d) = i$. We have $(m\overline{m})^2 = \beta\overline{\beta}/(t_g\overline{t_g}) = \frac{(2b)^2}{\delta\overline{\delta}}(d/d')$. Let $f_g = i(d)t_g$.

Now if $\delta = 1$ or 2, so d is odd, we have $\frac{4a}{\delta} = \beta + \overline{\beta} = f_g m^2 + \overline{f_g}\overline{m}^2, (m\overline{m})^2 = (\frac{2b}{\delta})^2$, so $\frac{4\varepsilon}{\delta} = (\frac{4a}{\delta} + \frac{4b}{\delta}\sqrt{d})f_g = f_g^2 m^2 + f_g\overline{f_g}\overline{m}^2 \pm 2m\overline{m}\sqrt{d}f_g = (f_g m \pm \overline{m}\sqrt{d})^2$ because $f_g\overline{f_g} = t_g\overline{t_g} = d' = d$.

If $\delta = 2(1+i)$ so d is even, then $\beta = \frac{2a-2i}{\delta} \Rightarrow a-i = \beta(1+i) \Rightarrow 2a = (1+i)\beta + (1-i)\overline{\beta} = (1+i)f_g m^2 + (1-i)\overline{f_g}\overline{m}^2, (m\overline{m})^2 = b^2$, so $b = \pm m\overline{m}$ and $2\varepsilon(1+i)f_g = (2a+2b\sqrt{d})(1+i)f_g = (1+i)^2 f_g^2 m^2 + (1+i)(1-i)f_g\overline{f_g}\overline{m}^2 \pm 2m\overline{m}(1+i)f_g\sqrt{d} = ((1+i)f_g m \pm \overline{m}\sqrt{d})^2$ because $(1+i)(1-i)f_g\overline{f_g} = 2d' = d$

Let $2(g) = 1+i$, if $2|d$ $\sigma(2,d) = id$

Proposition 2.6. *Let* $c_g(d) = \prod_{p|d} p(g)^{\sigma(p,d)}$ *Then*

$\varepsilon_d / c_g(d) \in F_d^2$ *if* d *is odd,*

$\varepsilon_d(j(d)c_g(d)) \in F_d^2$ *is* d *is even, where*

$j(d) = 1,2$ *if* $a \equiv 1$ *(mod 4),* $\equiv 3$ *(mod 4) respectively, where* $\varepsilon_d = a + b\sqrt{d}$.

proof: If $\delta = 1, c_g = t_g = f_g$ because $i(d) = 1$. If $\delta = 2, c_g = t_g$, $f_g = it_g$ and $2i = (1+i)^2 \in F_d^2$.

In these cases $\frac{\varepsilon f_g}{\delta} \in F_d^2$ as was proved above and so $\varepsilon_d / c_g(d) \in F_d^2$.

If $\delta = (1+i)2$ we proved that $2\varepsilon(1+i)f_g \in F_d^2$ and $c_g = (1+i)t_g, f_g = i(d)t_g, 2i(d)j(d) \in F_d^2$ so $\varepsilon_d/(j_d c_g(d)) \in F_d^2$.

We are ready to prove

Proposition 2.7. *Let for* $d \in W_-$ $\varepsilon_d = a_d + b_d\sqrt{d}$ *is a fundamental unit (positive) of* $k_d = \mathbb{Q}(\sqrt{d})$. *Let* $\Sigma \subset W_-$, *for an odd prime* $p \in T(\Sigma) = \{$ *the set of all primes divid-*

ing at least one $d \in \Sigma\}$ $p(g) = n_p + im_p$, *where* $n_p, m_p \in \mathbb{Z}$, $n_p^2 + m_p^2 = p$ *and let* $N_\Sigma(p) =$ $\{$ *the number of* $d \in \Sigma : p|d$ *and* $p(g)|2(a_d + i)\}$. *If* $2 \in \Sigma$ *let* $N_\Sigma(2) = \{$ *the number of* $d \in \Sigma : 2|d$ *and* $a_d \equiv 3$ *(mod 4) (*a_d *is an integer, if* d *is even). Let*

$$c_\Sigma = \prod_{p \in T(\Sigma), N_\Sigma(p) \text{ is odd}} p \tag{2.6}$$

The unit $\varepsilon_\Sigma = \prod_{d \in \Sigma} \varepsilon_d$ *is special for the multiquadratic field* $L, V(L) \supset \Sigma$ *(in particular, for the field* K*) if and only if* $\prod_{d \in \Sigma} d$ *is a square in* $\mathbb{Z}$. *In this case* $C_L(\varepsilon_\Sigma)$ *is the* $V(L)$*-coset of* c_Σ *defined by (2.6).*

proof: We can assume that m_p are even. Taking into account the proposition 2.6 and that $\overline{p(g)} = p(g)p/p(g)^2$, we see that (we recall $2(g) = 1 + i$)

$\varepsilon_\Sigma = c_\Sigma \prod_{d \in \Sigma} (\prod_{p|d} p(g)) y^2$, where $y \in L(i)$.

Now $\prod_{d \in \Sigma} \prod_{p|d} p(g)) = \prod_{p \in T(\Sigma)} (\prod_{d \in \Sigma, p|d} p(g)) = \prod_{p \in T(\Sigma)} p(g)^{\ell_p}$,

where $\ell_p = ord_p(\prod_{d \in \Sigma} d)$.

Suppose $z = \prod_{p \in T(\Sigma)} p(g)^{\ell_p} = c' x^2, c' \in \mathbb{Q}, x \in L(i)$. We claim this happens iff all ℓ_p are even.

By the Kummer theory ($L(i) = g(\sqrt{V(L)})$) z/c' is a square in $L(i) \Leftrightarrow z/c' \in V(L)g^2$. But

then $z = c''w^2$ with $c'' \in \mathbb{Q}, w \in g$. Let $\pi = \overline{p(g)}$, p odd.

Then $0 = ord_\pi(z) = ord_p(c'') + 2ord_\pi(w) \Rightarrow ord_p(c'')$ is even.

So $\ell_p = ord_{\overline{\pi}}(z) = ord_p(c'')$ (mod 2) $\equiv 0$ (mod 2).

Also, if $2 \in T(\Sigma)$, $\ell_2 = ord_{2(g)}(z) = 2ord_2(c'')$ (mod 2) $\equiv 0$ (mod 2).

We proved that $\varepsilon_\Sigma/c_\Sigma \in \mathbb{Q}L(i)^2 \Leftrightarrow \prod_{d\in\Sigma} d$ is a square in $\mathbb{Z} \Leftrightarrow \varepsilon_\Sigma/c_\Sigma \in L(i)^2$.

But $\varepsilon_\Sigma/c_\Sigma \in L(i)^2 \Leftrightarrow \varepsilon_\Sigma/c_\Sigma \in \pm L^2$ (because $L(i) = L(\sqrt{-1})$), then apply Kummer theory again). And so $\varepsilon_\Sigma/c_\Sigma \in L^2$ because ε_Σ and c_Σ are positive. The proposition 2.7 is proved.

Taking into account the section 2.2 we conclude that for $\Sigma \subset W$ $\varepsilon_\Sigma = \prod_{d\in\Sigma} \varepsilon_d$ is special for $K \Leftrightarrow \prod_{d\in\Sigma\cap W_-} d$ is square. Then $C_K(\varepsilon)$ is $V(K)$-coset of

$c_\Sigma = (\prod_{d\in W\cap\Sigma_+} c_d)c_{\Sigma\cap W_-}$ (the product is in SF) , where for $d \in W \cap \Sigma_+$ c_d is representative of $C_{k_d}(\varepsilon_d)$, determined effectively by proposition 2.3 (see (2.3)) and $c_{\Sigma\cap W_-}$ is determined effectively by the proposition 2.7 (see (2.6)). So the study of the group $S_0(K)$ is completed, it is generated mod$(\prod_k {E_k}^2)$ by the special units ε_Σ just mentioned above.

In particular, if K is biquadratic real over $\mathbb{Q}$ and $W(K) = \{d_0, d_1, d_0d_1\} = W_-(K)$, then proposition 2.7 allows to compute c_Σ for the special unit ε_Σ with $\Sigma = W(K)$, what, in particular, resolves an ambiguity in [1], where the way to compute c_Σ is not presented. This completes in this case the determination of the 4-rank r_K (see the definition in 1.2) studied in [1].

In the case of the biquadratic field $K = \mathbb{Q}(\sqrt{d_0}, \sqrt{d_1})$, $W = \{d_0, d_1, d_0d_1\}$ and the only

possibility that $\Sigma \subset W$ and $\prod_{d\in W} d$ is a square is the case $\Sigma = W$. So if there $\exists d \in W$: $N(\varepsilon_d) = 1$, then $S(K) = S_0(K)$ (it is proved in the section 2.4 that $S(K)^{2^{n-2}} \subset S_0(K)$ for $[K/\mathbb{Q}] = 2^n$) is generated (mod ${E_K}^2$) by ε_d with $N(\varepsilon_d) = 1$. If $\Sigma = \Sigma_-$ then $S(K)$ is generated by ε_W which $\in {E_K}^2 \Leftrightarrow c_W \in V(K)$, where c_W is defined by (2.6) with $\Sigma = W$. If we move to the threequadratic real field ($n = 3$) or field with $n > 3$, the situation with special units becomes more complicated: there are more possibilities for $\Sigma \subset W$ to satisfy the condition $\prod_{d\in W} d$ is a square and so if $\Sigma \subset W_-$ for ε_Σ to be special, also the special units of K which are not in $S_0(K)$ could exist.

Let $W' \subset W$. Let us consider $\mathbb{Z}/2\mathbb{Z}$-vector space $\mathbb{X} = \mathbb{X}(W')$ consisting of subsets $\Sigma \subset W'$ with addition $\Sigma_1 \cdot \Sigma_2 = (\Sigma_1 \setminus \Sigma_2) \cup (\Sigma_2 \setminus \Sigma_1)$. $\mathbb{X}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$-vector space with basis $e_d, d \in W'$ under the mapping $\Sigma \mapsto \sum_{d\in\Sigma} e_d$ (the empty set goes to 0).

We have a linear mapping $\mathbb{X} \stackrel{\ell}{\to} V(W') \stackrel{def}{=} \mathbb{Z}/2\mathbb{Z}$-vector subspace of SF generated by $d \in W'$, where $\ell(\Sigma) = \prod_{d\in\Sigma} d$. And $ker(\ell) \cap (W_-)$ surjects onto a subspace in $S_0(K)/(\prod_k E_k)^2$ generated by $\varepsilon_\Sigma \in S_0(K)$, $\Sigma \in W'_-$, via the mapping $\Sigma \mapsto$ the coset of ε_Σ .So

$$dim(ker(\ell)) = |W'| - dim(V(W')) \tag{2.7}$$

is the upper bound for the dimension of this subspace, if $W' = W_-$.

Proposition 2.8. *Let $V' \subset V, dim(V') = 3, W' = V' \setminus \{1\}$. Then $dim(ker(\ell)) = 4, ker(\ell)$ is the direct sum of $(\mathbb{Z}/2\mathbb{Z})W'$ and the subspace $\mathbb{X}_h$ of $\mathbb{X}$ consisting of the sets $W' \setminus H$, H is a p-hyperplane in W'. The set $\{W' \setminus H_i, i = 1,2,3\}$ is a basis of $\mathbb{X}_h \Leftrightarrow \bigcap H_i = \emptyset$*

proof: $dim(ker(\ell)) = 4$ by (2.7) because $|W'| = 7$ and $dimV(W') = dim(V') = 3$. Suppose $\Sigma \in ker(\ell)$, If $|\Sigma| \geq 4$, $|\Sigma \cdot W'| = |W' \setminus \Sigma| \leq 3$. If $|\Sigma| \leq 3$, the only way for $\Sigma \in ker(\ell)$ is to be a p-hyperplane. So $ker(\ell)$ is generated by W' and the set $\mathbb{X}_h$.

Any two distinct p-hyperplanes H_1 and H_2 have $|H_1 \cap H_2| = 1$, because if $H_1 \cap H_2 = \{x, y\}$, then $H_1 = H_2 = \{x, y, x \cdot y\}$, and if $H_1 \cap H_2 = \emptyset$, then V contains the direct sum of two hyperplanes $H_1 \cup \{0\}$ and $H_2 \cup \{0\}$, $dim(V) \geq 4$ while $dim(V) = 3$.

Suppose $H_1 \cap H_2 = \{x\}$ and $H_1 = \{x, y, x \cdot y\}$, $H_2 = \{x, z, x \cdot z\}$. Then $z \neq x \cdot y$, so $\{x, y, z\}$ is a basis of V' and $W' = \{x, y, z, x \cdot y, x \cdot z, y \cdot z, x \cdot y \cdot z\}$. So $(W' \setminus H_1) \cdot (W' \setminus H_2) = \{z, x \cdot z, y \cdot z, x \cdot y \cdot z\} \cdot \{y, x \cdot y, y \cdot z, x \cdot y \cdot z\} = \{z, x \cdot z, y, x \cdot y\} = W' \setminus \{x, y \cdot z, x \cdot y \cdot z\}$ and $\{x, y \cdot z, x \cdot y \cdot z\}$ is the unique p-hyperplane H_3 distinct from H_1 and H_2 such that $H_1 \cap H_2 \cap H_3$ is non-empty.

2.4 Special units and Galois action

In this section we study the special units of K analyzing the effect of action of $Gal(K/\mathbb{Q})$ on them with applications to the study of the group $S(K)/S_0(K)$.

We begin with a general result in the setting where q is a prime number, M a finite extension of $\mathbb{Q}$,K is an abelian extension of M with Galois group $G(K/M) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^n$, $n \geq 2$.

We recall that for a number field L E_L denotes the group of units of L.

Proposition 2.9. ${E_K}^{q^{n-1}} \subset \prod_k E_k$. $(E_K \cap (MK^q))^{q^{n-2}} \subset \prod_k E_k$.

In both cases k runs through all subfields $M \subset k \subset K$ such that $Gal(k/M) \xrightarrow{\sim} \mathbb{Z}/q\mathbb{Z}$

proof: The first inclusion follows immidiately from (1.1) with $a = u \in E_K$. Let $u = cb^q \in E_K$, where $c \in M, b \in K$.

Then $N_{K/k}(u) = c^{q^{n-1}}(N_{K/k}(b))^q = {u_k}^q$ with $u_k \in E_k$. Also $N_{K/M}(u) = (u_M)^q$ with $u_M \in E_M$, so (1.1) with $a = u$ implies that $u^{q^{n-2}} \in \mu_q(K)\prod_k E_k$, where $\mu_q(K) =$ the group of q-th roots of unity in K. It is enough to show that $\mu_q(K) \subset M$. If $\mu_q(K) \neq 1$ then $\mu_q \xrightarrow{\sim} \mathbb{Z}/q\mathbb{Z}$ and the action of $G(K/M)$ on $\mu_q = \mu_q(K)$ induces a homomorphism $G(K/M) \to Aut(\mu_q) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^* \xrightarrow{\sim} \mathbb{Z}/(q-1)\mathbb{Z}$ which can only be trivial because

$G(K/M) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^n$. Hence $\mu_q \subset$the subfied of K on which $G(K/M)$ acts trivially = the field M by the Galois theory.

Let us now return to the case $q = 2, M = \mathbb{Q}, K$ is real. Proposition 2.9 implies

Consequence 2.2. ${S(K)}^{2^{n-2}} \subset S_0(K)$*, in particular,* $S(K) = S_0(K)$*, if* $n = 2$.

Let $1 \neq \sigma \in Gal(K/\mathbb{Q}), H_\sigma$ is the hyperplane in $V = V(K)$ such that $Q(\sqrt{H_\sigma})$ is the field fixed by σ. If $\sigma = id$ we let $H_\sigma = V$.

Suppose $\Sigma \subset W, \varepsilon_\Sigma = \prod_{d\in\Sigma} \varepsilon_d \in S(K)$, that is $\varepsilon_\Sigma = cb^2$, where $c \in \mathbb{Q}, b \in K$. Taking into account that $\varepsilon_d {\varepsilon_d}^\sigma = {\varepsilon_d}^2$ if $d \in \Sigma \cap H_\sigma$, $= N_{k/\mathbb{Q}}(\varepsilon_d) = \pm 1$ if $d \in \Sigma_\pm \setminus H_\sigma$, where $k = \mathbb{Q}(\sqrt{d}), \Sigma_\pm = \Sigma \cap W_\pm$, we obtain

$c^2(bb^\sigma)^2 = \varepsilon_\Sigma \varepsilon_\Sigma{}^\sigma = (\prod_{d\in\Sigma\cap H_\sigma} \varepsilon_d{}^2)(-1)^{|\Sigma_- \setminus H_\sigma|}$

Comparing signs of the l.h.s and r.h.s we conclude that $|\Sigma_- \setminus H_\sigma|$ is even $\forall\sigma$, hence $|\Sigma- \setminus H|$ is even for every hyperplane $H \subset V$.

Proposition 2.10. *Let X be a subset of W. Then*

$$|X \setminus H| \text{ is even } \forall \text{ hyperplane } H \text{ of } V \Leftrightarrow \prod_{d\in X} d \text{ is a square} \tag{2.8}$$

proof: Let $x = \prod_{d\in X} d$ (mod squares) $\in V$. Let $\phi_H : V \to \mathbb{Z}/2\mathbb{Z}$, $ker\phi_H = H$. Then $\phi_H(x) = \sum_{d\in X} \phi_H(d) = \sum_{d\in X\setminus H} 1 = |X \setminus H|$ (mod 2).

So the contradiction $|X \setminus H|$ is even means that $\phi_H(x) = 0$ and it holds for $\forall H \Leftrightarrow x = 1$.

So we reproved that for ε_Σ to be special for K it is necessary that $\prod_{d\in\Sigma_-} d$ is square. We recall that in the section 2.3 it is proved that it is a sufficient condition also.

Now suppose u is special for $K : u = cb^2$, where $c \in \mathbb{Q}, b \in K$, and suppose that $u^2 \in S_0(K)$ what is always the case is $n = 3$ by the consequence 2.2. So

$$u^2 = \varepsilon_\Sigma \varepsilon^2, \text{ where } \Sigma \subset W, \varepsilon \in \prod_k E_k \tag{2.9}$$

We have for $\sigma \in Gal(K/\mathbb{Q})$ $(c^2(bb^\sigma)^2)^2 = (uu^\sigma)^2 = \varepsilon_\Sigma \varepsilon_\Sigma^\sigma (\varepsilon\varepsilon^\sigma)^2 =$

$\varepsilon_{\Sigma_+\cap H_\sigma}^2 \varepsilon_{\Sigma_-\cap H_\sigma}^2 (-1)^{|\Sigma_-\setminus H_\sigma|}(\varepsilon\varepsilon^\sigma)^2$. Note that ε_Σ is special for K (being a square in K), so $(-1)^{|\Sigma_-\setminus H_\sigma|} = 1$ by the above. Also $(\varepsilon\varepsilon^\sigma)^2 = (\varepsilon')^4$ for some $\varepsilon' \in \prod_k E_k$, where k runs through the quadratic subfields of $\mathbb{Q}(\sqrt{H^\sigma})$. Taking into account that bb^σ is also in the latter field, we conclude that $\varepsilon_{\Sigma_+\cap H_\sigma}\varepsilon_{\Sigma_-\cap H_\sigma}$ is a square in $\mathbb{Q}(\sqrt{H_\sigma})$ (we recall that $\varepsilon_d > 0$ by definition)

In paticular $\varepsilon_{\Sigma_-\cap H_\sigma}$ is special for K, because ε_d are special $\forall d \in W_+$ by the section 2.2. Hence by the above

$$\prod_{d\in\Sigma_-\cap H} \text{ is a square if } H = V \text{ or a hyperplane of } V \tag{2.10}$$

Proposition 2.11. *Let K be real multiquadratic extension of $\mathbb{Q}$. Then for $\varepsilon_\Sigma\varepsilon^2 = u^2$, where $\emptyset \neq \Sigma \subset W, \varepsilon \in \prod_k E_k, u$ is a special unit for K, it is necessary that for $H = V$ or a hyperplane of V $\prod_{d\in\Sigma_-\cap H}$ is a square in $\mathbb{Z}$ and $c_{W\cap H} = (\prod_{d\in\Sigma_+\cap H} c_d)\cdot c_{W_-\cap H} \in H$ (the product is in SF), where c_d is any element of the set $C_k(\varepsilon_d), k = \mathbb{Q}(\sqrt{d})$ defined by (2.3) and $c_{W_-\cap H}$ is defined by (2.7). If no such sets Σ exist, then $S(K) = S_0(K)$.*

proof: We have proved that for (2.9) to hold it is necessary that (2.10) must hold and $\varepsilon_{\Sigma\cap H}$ must be a square in $\mathbb{Q}(\sqrt{H})$. The latter condition is equivalent to the condition that $c_{\Sigma\cap H} \in$

H because $\varepsilon_{\Sigma\cap H} \in c_{\Sigma\cap H}(\mathbb{Q}(\sqrt{H}))^2$ by proposition 2.3 and 2.7 and $SF \cap (\mathbb{Q}(\sqrt{H}))^2 = H$ by the Kummer theory. Now if $S(K) \neq S_0(K)$, then $\exists$ a special unit u of K such that $u^2 = \varepsilon_\Sigma \varepsilon^2$, but $u \notin S_0(K)$, so $\Sigma \neq \emptyset$.

Let us prove that the condition (2.10) in the case $W_- \subset V' \subset V, dim(V') = 3$ is satisfied iff $\Sigma_- = W_- = W' = V' \setminus \{1\}$, if $\Sigma_- \neq \emptyset$. In the section 2.3 (see the description of $ker(\ell)$ at the end of section 2.3) it is proved a non-empty $X \subset W'$ is satisfied to the condtition $\prod_{d\in X} d$ is a square iff X is either W' or a p-hyperplane, or $W'\setminus$(a p-hyperplane). So $(2.10)'$ $\stackrel{def}{=}$ (2.10) with V replaced by V'(it is equivalent to (2.10) if $\Sigma_- \in V'$) holds for $X = W'$, otherwise it does not hold: if X is a p-hyperplane than for a hyperplane $H_2 \neq X \cup \{1\}$, $|X \cap X_2| = 1$, and if $X = W \setminus H_1$, where H_1 is a hyperplane, then for a hyperplane $H_2 \neq H_1$ $|X \cap H_2| = |H_2 \setminus H_1| = 2$.

Proposition 2.12. *Let K be a real threequadratic extension of $\mathbb{Q}$ with $W = W_-$ ($\Leftrightarrow$ all the fundamental units of ε_d have norm= -1). Then $|S(K)/S_0(K)| \leq 2$ and $S(K) = S_0(K)$ if $\exists H = V$ or a hyperplane of V such that $c_{W\cap H}$ defined by (2.6) does not belong to H. If $|S(K)/S_0(K)| = 2$, then $\eta(S(K)) \subset R/V$ is at most one dimensional, where η is defined at the end of section 2*

proof: If $S(K) \neq S_0(K)$, $u_1, u_2 \in S(K) \setminus S_0(K)$, then $u_i^2 \in S_0(K)$, because $S(K)^2 \in S_0(K)$ by the consequence 2.2, so $u_1^2 = \varepsilon_\Sigma \varepsilon_1^2$, $u_2^2 = \varepsilon_\Sigma \varepsilon_2^2$, where $\varepsilon_i \in \prod_k E_k$, $\Sigma = W$ by the above, so $u_1/u_2 \in S_0(K) \Rightarrow |S(K)/S_0(K)| = 2$. And $S_0(K)$ is generated by $\varepsilon_{W\cap H}$ by the proposition

2.8, so $\eta(S_0(K))$ is generated by $\eta(\varepsilon_{W\cap H})$ = the coset of $c_{W\cap H} = V$, because $c_{W\cap H} \in H \subset V$. So $\eta(S(K))$ is generated by $\eta(u_1)$.

Note that in the case $n > 3$ the condition (2.10) may hold for sets Σ_- distinct from W, for example, if Σ_- = a p-hyperplane of W. Really, if H_1, H_2 are distinct hyperplanes of V, then the exact sequence

$$0 \mapsto H_1 \cap H_2 \mapsto H_1 \oplus H_2 \mapsto V \mapsto 0$$

implies that $dim(H_1 \cap H_2) = 2(n-1) - n = n-2 > 1$, so the condition (2.10) holds for any p-hyperplane of W because $\sum_{x\in Y} x = 0$ for a subspace $Y \subset (\mathbb{Z}/2\mathbb{Z})^n$ of dimension > 1, what can be proved by induction on the dimension of Y: the property holds, if $dim(Y) = 2$ by direct computation, if $dim(Y) \geq 3$, then $Y = Z \cup (y+Z)$ for $y \in Y$ and a subspace $Z \subset Y$ of dimension = $dim(Y) - 1 > 1$, $y \notin Z$.

Now if $n \geq 3$ and $dim(V(W_-)) \leq 3, |W_-| < 7$,in particular, if $n = 3$ and $W_+ \neq \emptyset$, then in (2.9) $\emptyset \neq \Sigma = \Sigma_+$ by the above and the proposition 2.11 implies

Proposition 2.13. *Let $n \geq 3$ and $dim(V(W_-)) \leq 3, |W_-| < 7$,in particular, $n = 3$ and $W_+ \neq \emptyset$. Then for $\varepsilon_\Sigma \varepsilon^2 = u^2$, where $\emptyset \neq \Sigma \subset W, \varepsilon \in \prod_k E_k, u$ is special for K, it is necessary that $\Sigma \subset W_+$ and*

$$\prod_{d\in\Sigma\cap H} c(d) \in_2 H \tag{2.11}$$

where $c(d)$ is any element of the set $C_k(\varepsilon_d), k = \mathbb{Q}(\sqrt{d})$ defined by (2.3). If no such sets $\Sigma \subset W_+$ exist, then $S(K) = S_0(K)$.

Chapter 3

The theory of Unoids

The chapter 3 is the joint work with professor V. Kolyvagin.

Explanation of Notations

Let SF = the set of positive square free integers.

SF is the group with operation $x \cdot y = xy/(x,y)^2$.

$\mathrm{SF} \mapsto \mathbb{Q}^+/\mathbb{Q}^2$ is an isomorphism.

If $K/\mathbb{Q}$ is a real multiquadratic extension i.e $(G(K/\mathbb{Q}) = [\mathbb{Z}/2\mathbb{Z}]^n)$ then

$V = V(K) = \{d \in \mathrm{SF}, \sqrt{d} \in K\}$.

$V \mapsto V(K)$ defines a one to one correspondence

(Kummer Theory) of K of degree 2^n and a n- dimensional $\mathbb{Z}/2\mathbb{Z}$ subspaces of SF.

$W = V \setminus \{1\}$.

Our main case $n = 3$, so $|W| = 7$.

If d_0, d_1, d_2 is a basis for W (i.e a basis for V) then $d_{01}, d_{02}, d_{12}, d_{012}$ denotes $d_0 \cdot d_1, d_0 \cdot d_2, d_1 \cdot d_2$, $d_0 \cdot d_1 \cdot d_2$ respectively.

A hyperplane of V is a subspace of V of co-dimension 1.

A p-hyperplane (punctured hyperplane)= a hyperplane $/\{1\}$.

$N =_2 M \Leftrightarrow NM$ is a square.

3.1 Definition of unoids and m-unoids

To study the necessary conditions (see the proposition 2.11 and (2.11)) for a product of fundamental units with norm 1 to be the square of a special unit we introduce the concept of a unoid which models sets of fundamental units e_d with norm 1 and associated to them the sets $C_k(e_d)$, where $k = \mathbb{Q}(\sqrt{d})$.

We recall that SF denotes the set of square free natural numbers. The subgroup $\{1, d\}, d \in W$, act on SF naturally.

We call a preunoid U associated to W a collection $\{C(d) \subset \mathrm{SF}, d \in W\}$ such that $C(d)$ is an orbit of $\{1, d\}$ We call the base $X = X(U)$ of a preunoid U the set $\{d \in W : C(d) \neq \{1, d\}\}$. A section c of U is a collection $\{c(d) \in C(d), d \in W\}$. A preunoid U can be recovered by

any of its section c if because $C(d) = \{1,d\}c(d)$.

We call a preunoid U an unoid if $C(d)$ consists of divisors of d if $d \equiv 1,2(\text{ mod } 4)$ of divisors of $2d$ if $d \equiv 3$ (mod 4).

We have the following unoid U_K, associated to the field K: the base X_K of U_K is the set of all $d \in W$ such that the fundamental unit e_d of $\mathbb{Q}(\sqrt{d})$ has norm 1. And $C(d) = C_k(e_d)$, where $k = \mathbb{Q}(\sqrt{d})$, if $d \in X_K$ (so $C(d) = \{1,d\}$ if $d \notin X_K$)

This important example links the following theory of unoids to the study of arithmetic of K.

We call a preunoid U_1 a subpreunoid of a preunoid U_2 if $X_1 \subset X_2$ and $C_1(d) = C_2(d)$ for $d \in X(U_1)$

We call a preunoid U a m-preunoid if the following condition holds: If $Y = V$ or is a hyperplane of V, c is a section of U, then.

$$\prod_{d \in Y \setminus \{1\}} c(d) \in_2 Y \tag{3.1}$$

It is clear from the definitions that the condition 3.1 holds for some $c \Leftrightarrow$ it holds for every c. A m-unoid is a m-preunoid which is a unoid.

It follows from chapter 2, proposition 2.11 that if $X \subset X_K$ and $(\prod_{d\in X} e_d))e^2 = u^2$, where u is a special unit of K and e is the product of units from the quadratic subfields of K, then it is necessary that the subunoid of U_K with base = X is a m-unoid. This makes important to study the properties and classifications of m-unoids.

The following proposition will be crucial for the study of m-unoids (and will explain their calling)

We call a section c of a preunoid U multiplicative if for $x, y \in W$ $x \neq y, c(x\cdot y) = c(x)\cdot c(y)$. If we put $c_1 = 1$, it is equivalent that $c : U \mapsto SF$ is a linear mapping of $\mathbb{Z}/2\mathbb{Z}$ vector spaces. We will abbreviate saying that c is a multiplicative section by saying that c is a m-section.

Proposition 3.1. *Let $n \geq 3$ .A preunoid U is m-preunoid if $\exists$ m-section of U. In this case there are precisely two distinct m-sections c and c' and $c(d)\cdot c'(d) = d$ ($\Leftrightarrow c(d) = c'(d)\cdot d$). If $n = 3$ the existence of a m-section is also necessary for U to be a m-preunoid.*

Consequence 3.1. *Let $n \geq 3$. A preunoid U is a m-preunoid $\Leftrightarrow$ if $d \in W, x \in C(d)$ then $\exists!$ m-section of U such that $c(d) = x$*

Proof of consequence 3.1: The sufficiency of the condition is immediate from the proposition 3.1. Suppose U is a m-preunoid and c' is a m-section of U existed by the proposition 3.1. If $c'(d) = x$ we are done. Otherwise $c'(d) = x\cdot d$ and $c(d) = x$ for the second m-section of U described in the proposition

Proof of proposition 3.1: Suppose c is m-section of U. Let $Y = V$ or a hyperplane of V. We assume $c(1) = 1$. Y is the disjoint union of cosets $x \cdot H$, where H is a hyperplane of V, Hence:

$\prod_{d\in Y} c(d) = \prod_x \prod_{d\in H} c(x\cdot d) =_2 \prod_x c(x)^{|H|} \prod_{d\in H} c(d)$ and it is enough to show that

$\prod_{d\in H} c(d) =_2 1$, but $H = \{1, y, z, y\cdot z\}$ if $n = 3$, so we have that

$\prod_{d\in H} c(d) =_2 c(1)c(y)c(z)c(y\cdot z) =_2 1$. If $n \geq 3$, the claim can be proved by induction on n.

Now we prove that for $n = 3$ the existence of a m-section in necessary for U to be a m-preunoid.

Let $\{d_0, d_1, d_2\}$ be a basis for U. For a section c if U

we will denote by $c_0, c_1, c_2, c_{01}, c_{02}, c_{12}, c_{012}$ the value of c on $d_0, d_1, d_2, d_{01}, d_{02}, d_{12}, d_{012}$ respectively.

We know that $c_{01} =_2 c_0 c_1 d_0^x d_1^y$ with $x, y \in \{0, 1\}$ (by the condition 3.1 for c and the hyperplane $\{1, d_0, d_1, d_{01}\}^2$).

Let $c'_{01} =_2 c_{01}(d_0 d_1)^x, c'_0 = c_0, c'_1 =_2 c_1 d_1^{x+y}$

Then $c'_{01} =_2 c'_0 c'_1$ and c'_0, c'_1, c'_{01} may be values of a section of U on d_0, d_1, d_{01} respectively.

Now $c_{02} =_2 c_0 c_2 d_0^z d_2^w$. with $z, w \in \{0, 1\}$.

Similarly as before we put $c'_{02} =_2 c_{02}(d_0d_2)^z, c'_2 = c_2d_2^{z+w}$ to get $c'_{02} =_2 c'_0 \cdot c'_2$.

Now consider the condition (3.1) for c and the p-hyperplane $\{d_{01}, d_{02}, d_{12}\}$ and the section $\{c'_0, c'_1, c'_{01}, c'_2, c'_{02}, c_{12}, c_{012}\}$. We have

$c'_{01}c'_{02}c_{12} =_2 (d_0 \cdot d_1)^t(d_1 \cdot d_2)^r$ for $t, r \in \{0,1\}$. On the other hand the left hand side$=_2$ $c'_0c'_1c'_0c'_2c_{12} =_2 d_1^v d_2^u$ for $v, u \in \{0,1\}$ (taking into account the condition 3.1 for p-hyperplane $\{d_1, d_2, d_{12}\}$). We conclude $t = 0$ and $u = v = r$. Now let $c'_{12} =_2 c_{12} \cdot (d_1 \cdot d_2)^r$. We see that $c'_{12} =_2 c'_1c'_2$

We have the remaining p-hyperplanes $\{d_i, d_{012}, d_{jk}\}$ where $j \neq k \neq i$ to apply the condition 3.1. So

$c_{012} =_2 c'_ic'_{jk}d_i^{x_i}(d_0d_1d_2d_i)^{y_i} =_2 c'_0c'_1c'_2(d_i)^{x_i+y_i}(d_0d_1d_2)^{y_i}$.

This implies $x_i = y_i$ and $y_i = y$ is independent on i.

We put $c'_{012} =_2 c_{012}(d_0d_1d_2)^y$ to have $c'_{012} = c'_0c'_1c'_2$ and the section c' is m-section.

Before proving the remaining part of the proposition 3.1 we introduce multiplication of subpreunoids of a preunoid U. Let U_1, U_2 be subpreunoids of U with bases X_1, X_2 respectively.

Then the product $U_1 \cdot U_2$ of U_1 and U_2 is the subpreunoid of U with the base $X_1 \cdot X_2$ where $X_1 \cdot X_2$ is the product of the subsets of W introduced above: $X_1 \cdot X_2 = \{X_1 \setminus X_2\} \cup \{X_2 \setminus X_1\}$.

It follows if a, b are sections of U_1, U_2 then the product $a \cdot b$ is a section of $U_1 \cdot U_2$ and

$U_1 \cdot U_2$ is determined by this.

In particular the set $ms(U)$ of m-subpreunoids of U is the subgroup of the group $s(U)$ of subpreunoids of U because if a,b are m-sections of U_1, U_2 the product $a \cdot b$ is a m-section.

Now suppose that a,b are m-sections of a preunoid U. Then $a \cdot b$ is a m-section of the unoid $U_0 = U \cdot U$ which is the trivial unoid - the unoid with the base being the empty set.

So to complete the proof of the proposition it is enough to show that if c is a m-section of U_0 then either $c(d) = 1$ for all $d \in W$ or $c(d) = d$ for all $d \in W$.

Let c be a m-section of U_0, suppose $\exists x \in W$ such that $c(x) = 1$. Let $y \in W, y \neq x$.

Then $c(x \cdot y) = c(x) \cdot c(y) = c(y)$, if $c(y) \neq 1$ we get a contradiction because $c(x \cdot y) \neq 1$, so $c(y) = y, c(x \cdot y) = x \cdot y$ $(c(d) \in \{1, d\})$.

So $c(y) = 1 \Rightarrow c(z) = 1 \forall z \in W$. The proposition 3.1 is proved.

In the rest of chapter 3 we are going to determine in the case $n = 3$ the structure of the group $ms(U)$ of m-subunoids of a unoid U. In particular, we will show that $dim_{\mathbb{Z}/2\mathbb{Z}} ms(U) \leq 2$ and describe explicitly when non-triviality of $ms(U)$ can happen. It is important for the study of the arithmetic of the field K, because of the following:

Proposition 3.2. *Let $n = 3$. Let $S(K), S_0(K)$ be the group of special units of K , the group of special units of K being the product of units in quadratic subfieds of K respectively.*

If there exists a quadratic subfield of K with fundamental unit of norm 1, the group

$S(K)/S_0(K)$ injects in the group $ms(U_K)$.

Proof: Let u be a special unit of K, $u \notin S_0(K)$ It follows from chapter 2, that

$u^2 = \prod_{d \in X} e_d e^2$, e is the product of units in quadratic subfields of K.

Then as was mentioned above, the subunoid of U_K with basis X is in $ms(U_K)$.

If there exists $X' \neq X$ such that the identity for u^2 holds, then we obtain non-trivial relations between the fundamental units of quadratic subfields of K which is impossible, because the subgroup generated by fundamental units is a free abelian group of rank 7.

This follows because the rank of the group of positive units of K is equal to 7 (by the Dirchlet theorem about units) and $u^4 \in$ the subgroup of units generated by e_d what follows from (1.1) if we put $a = v$.

Now let $i : S(K) \mapsto ms(U_K)$ is such that $i(U) =$ the sub unoid of U_K with the base X, then obviously i is an injection.

We recall that if all fundamental units e_d have norm = -1, we already proved in chapter 2 that $dim_{\mathbb{Z}/2\mathbb{Z}} S(K)/S_0(K) \leq 1$ and $S(K) = S_0(K)$ if $\prod_d e_d$ is not a square in $K \Leftrightarrow$ the set $C(\prod_d e_d)$ computed as described in Chapter 2, is not in the set V.

3.2 Factorization of $Hom(V,\mathbf{SF})$

In this section we will prove some useful results about linear mappings $\phi : V \mapsto$ SF. For a moment V will be an n - dimensional $\mathbb{Z}/2\mathbb{Z}$ vector space.

Proposition 3.3. *Let p be a prime number, $H_p = \{x \in V : p \not| \phi(x)\}$, then $H_p = V$ or H_p is a hyperplane of U*

Proof: Suppose $H_p \neq V$, then H_p is a proper subspace of V. Let $y,z \notin H_p$. Then $\phi(x), \phi(y)$ are square free numbers divisible by p. Hence $\phi(y \cdot z) = \phi(y) \cdot \phi(z)$ is not divisible by p, so $y \cdot z \in H_p \Rightarrow y \equiv z^{-1} \equiv z \pmod{H_p} \Rightarrow |V/H_p| = 2 \Rightarrow H_p$ s a hyperplane.

Consequence 3.2. *If p divides $\phi(x)$ for at least one $x \in V$, H_p is a hyperplane and $\{x \in V : p|\phi(x)\} = V \setminus H_p$*

Let H be a hyperplane in V,

$$a_H(\phi) := m.c.d(\phi(y) : y \notin H) \tag{3.2}$$

Proposition 3.4. *The numbers $a_H(\phi) \in$SF are pairwise co prime . Also $\forall x \in V$:*

$$\phi(x) = \prod_{H:x\notin H} a_H(\phi) \tag{3.3}$$

The mapping $\phi \mapsto \{a_H(\phi)\}$ is the bijection between $Hom(V,SF)$ and the set of pairwise coprime elements of SF enumerated by hyperplanes of V, with the inverse mapping defined by (3.3).

Proof: Let H be a hyperplane of V, p be a prime number. If $p|a_H(\phi)$ then consequence 3.2 $\Rightarrow H_p$ is a hyperplane and $V \setminus H \subset V \setminus H_p \Rightarrow H \supset H_p \Rightarrow H = H_p$. Hence for distinct H_1, H_2, neither prime divides both $a_{H_1}(\phi), a_{H_2}(\phi)$, so the numbers are coprime, It follows from definition (3.2) that if $x \notin H$, then $a_H(\phi)$ divides $\phi(x)$. Hence the right hand side of (3.3) divides $\phi(x)$.

Now suppose a prime $p|\phi(x)$. Then H_p is a hyperplane and $x \notin H_p \Rightarrow p|a_{H_p}(\phi) \Rightarrow \phi(x)$ divides right hand side of (3.3).

($\phi(x)$ is square free) $\Rightarrow$ (3.3) follows. It is clear that (3.2), (3.3) define inverse mappings, we need only check that the mapping defined by (3.3) is a linear mapping. Let $y, z \in V \setminus \{1\}, y \neq z$. It is enough to check that $\phi(y \cdot z) = \phi(y) \cdot \phi(z)$.

It follows from (3.3) that then $\phi(y) \cdot \phi(z) = \prod a_H(\phi)$, where the product is by hyperplanes $H : y \notin H, z \in H$,or $y \in H, z \notin H$, But these hyperplanes are exactly that do not contain

$y \cdot z$ because $y \cdot z \in H \Leftrightarrow y,z \in H$ or $y,z \notin H$. So the product exactly equals $\phi(y \cdot z)$

Now let V be a three dimensional subspace of SF and $\{d_0, d_1, d_2\}$ be a basis of V. For a linear map $\phi : V \mapsto$SF we will denote by $a(\phi), a_{ij}(\phi), b_i(\phi)$, where $0 \leq i, j \leq 2, i \neq j$ the numbers $a_H(\phi)$ corresponding to the following hyperplanes respectively:

$\{1, d_{01}, d_{02}, d_{12}\}, \{1, d_{ij}, d_{012}, d_k : k \neq i, j\}, \{1, d_k, d_j, d_{kj} : k, j \neq i\}$. Explicitly we have :

$$\begin{aligned} a(\phi) &= m.c.d(\phi(d_0), \phi(d_1), \phi(d_2), \phi(d_{012})) \\ a_{ij}(\phi) &= m.c.d(\phi(d_i), \phi(d_j), \phi(d_{ik}), \phi(d_{jk})) \text{ where } \quad k \neq i, j \\ b_i(\phi) &= m.c.d(\phi(d_i), \phi(d_{ij}), \phi(d_{ik}), \phi(d_{012})) \text{ where } \quad j, k \neq i \end{aligned} \tag{3.4}$$

Then (3.3) implies the following decompositions: for $d \in W = V \setminus \{1\}, \phi(d)$ is the product of the numbers appearing in (3.4), for which d appears in the brackets on the right hand side.

$$\begin{aligned} \phi(d_i) &= a(\phi) a_{ij}(\phi) a_{ik}(\phi) b_i \\ \phi(d_{ij}) &= a_{ik}(\phi) a_{jk} b_i b_j \text{ where } k \neq i, j \\ \phi(d_{012}) &= a_(\phi) b_0 b_1 b_2 \end{aligned} \tag{3.5}$$

Note that because the numbers in the left hand side of (3.4) are pairwise co prime, (3.5)

implies they can be defined also as follows:

$$\begin{aligned} a(\phi) &= m.c.d(\phi(d_0), \phi(d_1), \phi(d_2)) \\ a_{ij}(\phi) &= m.c.d(\phi(d_i)/a(\phi), \phi(d_j)/a(\phi)) \\ b_i(\phi) &= \phi(d_i)/(a(\phi)a_{ij}(\phi)a_{ik}(\phi)), \text{ where } j,k \neq i, j \neq k \end{aligned} \tag{3.6}$$

We note that if we take into account that $\phi(d_0), \phi(d_1), \phi(d_2) \in$ SF, $a(\phi).a_{ij}(\phi)$ defined by (3.6) can be easily seen to be pairwise co prime, so $b_i(\phi)$ can be defined as in (3.6) and again, it is easy to see directly that $a(\phi).a_{ij}(\phi), b_j$ are pairwise co prime . Then the decomposition (3.5) follows by direct computations. The more general approach above shows that the numbers in the right hand side of (3.4) appear actually as invariants, defined by ϕ and hyperplanes in V, while their indexation depends on the chosen basis of V.

3.3 Structure of m-Unoids

We suppose $n = 3$ in the sections 3.3 - 3.5

The following proposition gives explicit parametrization of m - sections of unoids, and so by proposition 3.1, of m-unoids themselves.

Proposition 3.5. *Let $\{d_0, d_1, d_2\}$be a basis of W an a, a_{ij}, b_i are the numbers defined by (3.6) (or (3.4)) for $\phi : V \mapsto V, \phi = id$. Let $\alpha, \alpha_{ij} = \alpha_{ji}, \beta_i$ where $0 \leq i, j \leq 2, i \neq j$ are*

numbers such that $\alpha|a', \alpha_{ij}|a'_{ij}, \beta_i|b'_i$, *where* N' *the largest odd factor of* N. *Let* $x_i \in \{0,1\}$ *for* $0 \leq i \leq 2$.

Let $c(d_i) = \alpha \cdot \alpha_{ij} \cdot \alpha_{ik} \cdot \beta_i \cdot 2^{x_i}$, *where* $0 \leq i \leq 2, j \neq k, j,k \neq i$. *Let* $c : W \mapsto SF$ *extends* c *to a multiplicative function (so* $c(d_{ij}), c(d_{012})$ *are defined by (3.5) with* $\alpha, \alpha_{ij}, \beta_i 2^{x_i}$ *in the right hand side).*

Suppose c satisfies the parity condition: $c(d)$ *is odd if* $d \equiv 1$*(mod 4).*

Then the preunoid $U = U(c)$ *determined by the condition that c is its section, that is* $C(d) = \{c(d), d \cdot c(d)\}$ *is an m-unoid and c is its m-section. If U is m-unoid c is its section (existing in proposition 3.1) then c is described as above.*

Proof: If U is an m-unoid, c its m-section, let $\phi : V \mapsto$ SF is the linear mapping such that $\phi(d) = c(d)'$ if $d \in W$, Let $\alpha = a(\phi), \alpha_{ij} = a_{ij}(\phi), \beta_i = b_i(\phi)$. Taking into account that $c(d)'|d'$, the definition (3.2) (see 3.4) implies that $\alpha|a, \alpha_{ij}|a_{ij}, \beta_i|b_i$
and hence $\alpha|a', \alpha_{ij}|a'_{ij}, \beta_i|b_i{}'$ since $\alpha, \alpha_{ij}, \beta_i$ are odd.

The equality (3.5) for ϕ implies that $c(d_i) = c(d_i)' \cdot 2^{x_i} = \alpha \cdot \alpha_{ij} \cdot \alpha_{jk} \cdot \beta_i \cdot 2^{x_i}$ and of course c must satisfy the parity condition in the proposition 3.5, by the definition of a unoid. So c is as described in proposition 3.5.

Now let c be as described in proposition 3.5. Then $c(d)'$ is given as in (3.5) with $\alpha, \alpha_{ij}, \beta_i$ in the right hand side respectively. So $c(d)'|d$ because d is given by (3.5) with a, a_{ij}, b_i in

the right hand side respectively.

Hence $c(d)|d, 2d$ if $d \equiv 2,3(\text{ mod } 4)$ respectively and $c(d)'|d$ if $d \equiv 1(\text{ mod } 4)$ by the parity condition. Hence $U = U(c)$ is a unoid, and of course , c is its m-section, so U is an m-unoid

Next we want to count the numbers $N(W), N_m(W)$ of unoids, m-unoid respectively, associated with the set W. Let W_n for $n = 1,2,3$ be the subsets of all elements of W equal to $n(\text{ mod } 4)$, $m_n = |W_n|$. Note that $\{1\} \cup W_1$ is a subspace of V and always $m_1 \geq 1$. Really $m_2 \leq 4$ by the consequence 3.2 for $p = 2, \phi : V \mapsto V, \phi = id$ Hence $m_1 + m_3 \geq 3$. Also if $x, y \in W_3, x \cdot y \in W_1$ so $m_1 \geq 1$.

Now if $m_2 = 0$, then either $W = W_1$ and then the numbers x_i in the proposition 3.5 are forced to be 0 by the parity condition, or W_1 is a p-hyperplane so one can choose $d_0 \equiv d_1 \equiv 1(\text{ mod } 4)$, $d_2 \equiv 3(\text{ mod } 4)$. Then $x_0 = x_1 = 0$ while x_2 equals 0 or 1 to satisfy the parity condition.

If $m_2 > 0$, then $m_2 = 4$ by the consequence 3.2 so one can choose $d_2 \equiv 0$ (mod 2) and there are two options: $m_1 = 3$so one can choose $d_0 \equiv d_1 \equiv 1(\text{ mod } 4)$, or $m_1 = 1$ so one can choose $d_0 \equiv 1(\text{ mod } 4)$, $d_3 \equiv 3(\text{ mod } 4)$.

Then $x_0, x_1 = 0, x_2 = 0$ or 1; $x_0 = 0, x_1, x_2 = 0$ or 1 respectively.

The number of all triples $(\alpha, \alpha_{ij}, \beta_i)$ in the proposition 3.5 is equal to the number of odd

divisors of $a \cdot a_{01} \cdot a_{02} \cdot a_{12} \cdot b_1 \cdot b_2 \cdot b_3$ which is equal to $2^{\tau(W)-1}, 2^{\tau(W)}$, when $m_2 = 4, 0$ respectively. (a prime $p \mid$ one of $\alpha, \alpha_{ij}, \beta_i \Leftrightarrow p|d$ for some $d \in W$) and $\tau(W) =$ the number of primes dividing at least one element of W.

The number of possible combinations of x_0, x_1, x_2 satisfying the parity condition is equal(as follows from the above when corresponding basis chosen) to 1, if $m_1 = 7$ to 2 if $m_1 = 3, m_2 = 0$ or $m_1 = 3, m_2 = 4$, to 4 if $m_1 = 1, m_2 = 4$.

Because each m-unoid has precisely 2 m-sections (proposition 3.1), the total number $N_m(W)$ of m-unoids is equal to $2^{\tau(W)-1}$ if $m_1 = 7$; $2^{\tau(W)-1} \cdot 2$ if $m_1 = 3, m_2 = 0$; $2^{\tau(W)-2} \cdot 2$ if $m_1 = 3, m_2 = 4$, $2^{\tau(W)-2} \cdot 4$ if $m_1 = 1, m_2 = 4$. On the other hand, the total number $N(W)$ of all unoids is equal to

$\prod_{d \in W \setminus W_3} 2^{\tau(d)-1} \prod_{d \in W_3} 2^{\tau(2d)-1} = (\prod_{d \in W} 2^{\tau(d)}) 2^{-m_1-m_2}$

Because, by the consequence 3.2, each prime dividing at least one element of W, divides precisely four elements of $W, \prod_{d \in W} 2^{\tau(d)} = 2^{4 \cdot \tau(W)}$. Hence the ratio $N_m(W)/N(W)$ is equal to:

$$\frac{2^{m(W)}}{2^{3\tau(W)}}$$

where $m(W) = 6$ if $m_1 = 7$; 3 if $m_1 = 3, m_2 = 0$; 6 if $m_1 = 3, m_2 = 4$;

5 if $m_1 = 1, m_2 = 4$. Equally one can say $m(W) = 6$ if $m_3 = 0 = 7 - m_3$ if $m_3 = 4, 2$.

We see that the density of m-unoids goes to 0 extremely fast when $\tau(W) \mapsto \infty$. This suggests that the threequadratic fields with some fundamental units of norm $= 1$ and special units that are not the product of units from quadratic subfields (that is the group $ms(U_K)$ is not trivial) are rare when $\tau(W)$ is big.

More precise statements in this direction, of course, require further study.

3.4 Structure of m-unoids of a given rank

We define the rank $r = r(U)$ of a preunoid U to be the cardinality of the base X of U. We denote by $MP_r(W), M_r(W)$ the set of m-preunoids, m-unoids (associated to W) of rank r , respectively. $MP_0(W) = M_0(W) = \{U_0\}$, where U_0 - the trivial unoid = the unoid with base equal to the empty set, or equivalently being defined by the section $c \equiv 1$. We shall show that there are no m-preunoids (and hence no m-unoids) of rank 1,2 and will present explicit descriptions of the sets $MP_r(W), M_r(W)$ for $r \geq 3$. Note that the proposition 3.5 already gives explicit description of m-unoids but without emphasis on their ranks. In this section we will see what the condition that an m-preunoid has a given rank means and , in the case of an m-unoid, adds to the previous analysis.

Note that the rank of the unoid U_K is equal to the number of quadratic subfields of K with fundamental units of norm = 1 (which under the ramification condition) may be equal to 0 , 4 , 6 or 7. And of course the group $ms(U_K)$ consists of m-unoids of rank $\leq r(U_k)$. So to know how the restriction on rank affects m-unoids is, in particular, important for the

application to the study of special units of K.

We recall that a m-function $c : W \mapsto \mathrm{SF}$ is the restriction to W of a linear map ℓ of V in SF. $ker(c) = ker(\ell) \setminus \{1\}$. The preunoid $U(c)$ is the preunoid for which c is a section. If the $ker(c) = H$ is a p-hyperplane, then c is constant on $W \setminus H$ because $W \setminus H$ is the unique non trivial coset of V by $H \cup \{1\}$.

Proposition 3.6. *There is no m-preunoids of rank 1 or 2. The map $c \mapsto U(c)$ induces one to one correspondence of the sets of m-functions*

$c : W \mapsto SF$ such that $H = ker(c) =$ a p-hyperplane and $c(W \setminus H) \in W \setminus H, \notin W \setminus H$ and the sets $MP_3(W), MP_4(W)$ respectively.

Proof: Let U be a m-preunoid of rank ≤ 4. Then, if X is the base of U, $W \setminus X$ contains at least 3 elements.

We claim $\exists!$ m-section c of U such that $|ker(c)| \geq 3$. Really let e be an m-section of U. Then $e(d) \in \{1, d\}$,if $d \in W \setminus X$, if $e(d) = 1$ for two elements we are done because $|ker(c)| = 0, 1, 3, 7$. If not then $e(d) = d$ for two or more elements of $W \setminus X$ and $e' = e \cdot i$, where $i(d) = d$ solves the problem. Now if $c \equiv 1$, then $U = U_0$ has rank 0. Otherwise $ker(c) = 3$ so $H = ker(c)$ is a p-hyperplane.

Now if $c(W \setminus H) \in W \setminus H$ then $r(U) = 3$ because $c(d) \in \{1, d\} \Leftrightarrow d \in H \cup \{c(W \setminus H)\}$. If $c(W \setminus H) \notin W \setminus H$, then obviously $r(U) = 4$. In particular, there is no room for m-preunoids

of rank 1 or 2.

Also uniqueness of c follows because the only other m-section of U is $c \cdot i$ (the proposition 3.1), but if $H' = ker(c \cdot i)$ is a p-hyperplane then obviously $H' \cap H = \emptyset$ what contradicts to the fact that the intersection of two p-hyperplanes is non-empty.

Consequence 3.3. *Let $X = \{d_0, d_1, d_2\}$ be a basis of W and c_X be the m function defined by $c_X(d_i) = d_{012}$ for $i = 0, 1, 2$.*

Then $X \rightleftarrows U(c_X)$ defines a one to one correspondence of the set $B(W)$ of basises of W and the set $MP_3(W)$ with opposite map $U \mapsto X$ =(the base of U)

Proof: $W \setminus X = \{d_{01}, d_{02}, d_{12}, d_{012}\} = H \cup \{d_{012}\}$, where H is the unique hyperplane in W/X. And if H is a hyperplane with $x \in W/H$, then $X = W \setminus (H \cup (x))$ is a basis. So bases are in one to one correspondence to pairs $(H, x \in W/H)$.

And the m-function $c|c(H) = 1, c(W \setminus H) = x$ is exactly such that $c(d_i) = x = d_{012}$ for $i = 0, 1, 2$ and the base $U(c) = W \setminus (H \cup \{x\})$

Consequence 3.4. $|MP_3(W)| = 28$

Proof: There are $C_7^3 = 35$ triples $x, y, z \in W$ and there are 7 p-hyperplanes among them. The rest are basises of W. We see that the lower rank there are more restrictions on $U \in MP_r(W)$.

Proposition 3.7. *Let $\{d_0, d_1, d_2\}$ be a basis for W. $c : W \mapsto SF$ an m-function such that*

$c_0 = 1, c_1 = d_1, c_2 \notin \{1, d_2, d_{01}, d_1, d_{02}\}$.

Then $U(c) \in MP_5(W)$ and $c \mapsto U(c)$ defines a surjection of the set of such m-functions to the set $MP_5(W)$.

Proof: The section c has values $c_2, c_{01} = d_1, c_{02} = c_2, c_{12} = d_1 \cdot c_2, c_{012} = d_1 \cdot c_2$. So $r(U(c)) = 5 \Leftrightarrow c_2 \notin \{1, d_2, d_{01}, d_1, d_{02}\}$.

Let $U \in MP_5(W)$. Let $\{d_0, d_1\} = W \setminus X(U), d_2 \in X(U), d_2 \neq d_{01}$. By the consequence 3.1 there exists a unique m-section c of U such that $c_0 = 1$. Then $c_1 = d_1$ otherwise $c_1 = 1 \Rightarrow c_{01} = 1$ - a contradiction, because $d_{01} \in X(U)$. And the value $c_2 = c(d_2)$ must satisfy the restrictions in the proposition 3.7 as we have seen above

Now we want to describe explicitly the sets $M_r(W)$ for $r \geq 3$ taking into account that $M_r(W) = MP_r(W) \cap M(W)$, where $M(W)$ is the set of all unoids associated to W, the proposition 3.5 and the analysis of the sets $MP_r(W)$ above.

Proposition 3.8. *Under the bijection of the consequence 3.2 the set $M_3(W)$ corresponds to the basises $\{d_0, d_1, d_2\}$ of W such that either $b_0 = b_1 = b_2 = 1$ or $b_i = 2$ for unique i , $0 \leq i \leq 2$, for $0 \leq j \leq 2$ $j \neq i$, $d_j \equiv 3 \pmod 4$ and $b_j = 1$. Respectively, $d_{012} = a$ or a is odd and $d_{012} = 2a$.*

Proof: We could refer to the proposition 3.5 but in this case it is easy to show this directly also. Let $U \in MP_3(W)$. For the m-section c such that $c_0 = c_1 = c_2 = d_{012}a \cdot b_0 \cdot b_1 \cdot b_2$ (see

(3.5) with $\phi = i$)

$U \in MP_3(W)$ iff for $0 \leq i \leq 2$ either d_{012} divides d_i or $d_i \equiv 3 \pmod 4$ and $d_{012}$is even and $d_{012}/2$ divides d_i. The case when $d_{012}|d_i$ for $0 \leq i \leq 2$ is the case when $a \cdot b_0 \cdot b_1 \cdot b_2|(mcd(d_0,d_1,d_2) = a) \Leftrightarrow b_0 = b_1 = b_2 = 1$, The other case means that d_{012} is even, $d_{012}/2$ divides a with a being odd$\Leftrightarrow d_{012} = 2a \Leftrightarrow b_0 \cdot b_1 \cdot b_2 = 2 \Leftrightarrow$ one of the b_i is equal to 2 and the others equal 1.

Also if $b_j = 1$ then $d_j \equiv 3 \pmod 4$, by the parity condition.

Proposition 3.9. *Let (H,γ) be a pair such that H is a p-hyperplane of W*

and if $b = mcd(d : d \in X)$, where $X = W \setminus H$, then either $\gamma|b, \gamma \neq 1, \gamma \neq b$ if $b \in X$ or b is odd, odd $d \in X \equiv 3 \pmod 4$, $\gamma = 2\beta$, where $\beta|b$, $\beta \neq b$ if $2b \in X$.

Then the map $(H,\gamma) \mapsto U(c)$, where c is an m function such that $c(d) = 1$ if $d \in H$, $c(d) = \gamma$ if $d \in X$, defines the bijection of such pairs and $M_4(W)$.

The set X is the base of $U(c)$,

Proof: Taking into account the proposition 3.6 for a preunoid $U \in MP_4(W)$ and the corresponding m function $c; H = ker(c), \gamma = c(X)$ we have to satisfy the condition that for $d \in X$ either $\gamma|d$ or $d \equiv 3 \pmod 4$, $\gamma = 2\beta, \beta|d$ Then either $\gamma|\beta$, or otherwise b is odd, $\gamma = 2\beta$ where $\beta|b$ and if $d \in X$, d is odd, then $d \equiv 3 \pmod 4$.

Of course the base of $U(c) = \{d \in W : c(d) \notin \{1,d\}\} = X$.

Proposition 3.10. *Let $d_0, d_1 \in W, d_0 \neq d_1$, be such that $(d_0, d_1) = 1$ or $(d_0, d_1) = 2$ and $x = d_{01} \equiv 3 \pmod 4$ if $(d_0, d_1) = 2$.*

Let $X = W \setminus \{d_0, d_1\}$. If $\exists d \in X, d \neq x, d \equiv 1 \pmod 4$ let d_2 be any such d; otherwise let $d_2 \in X, d_2 \neq x$. Let β be a divisor of b'_2(N' is the greatest odd divisor of N; a, a_{ij}, b_j are the numbers associated to the basis $\{d_0, d_1, d_2\}$ as described above).

Let $c_2 = a'_{12} \cdot \beta \cdot 2^y$, where $y = 0$ in the first case ($d_2 \equiv 1 \pmod 4$), $y = 0$ or 1 in the second case($d_2 \not\equiv 1 \pmod 4$).

Assume $c_2 \notin \{1, d_2, d_1, d_{01}, d_{02}\}$. Let c be the m function on W such that $c_0 = 1, c_1 = d_1, c_2$ defined above. Then the preunoid $U(c) \in MP_5(W)$ and $MP_5(W) = \{U(c), c$ runs through all m functions described above $\}$

Proof: Let $U \in MP_5(W), X = X(U)$, Let $W \setminus X = \{d_0, d_1\}$, $d_2 \in X$ is such as in the proposition 3.10. By the proposition 3.7. U has a m-section c such that $c_0 = 1, c_1 = d_1, c_2 \notin \{1, d_1, d_2, d_{01}, d_{02}\}$. $U \in M_5(W)$ iff the m-section c satisfies the condition of the proposition 3.5. Namely the conditions are: $\exists \alpha, \alpha_{ij}, \beta_j$ - odd divisors of a, a_{ij}, b_j respectively such that:

$$\begin{aligned} 1 = c'_0 = \alpha \cdot \alpha_{01} \cdot \alpha_{02} \cdot \beta_0, a' \cdot a'_{01} \cdot a'_{12} \cdot b'_1 = d'_1 \\ = c'_1 = \alpha \cdot \alpha_{01} \cdot \alpha_{12} \cdot \beta_1, c'_2 = \alpha \cdot \alpha_{02} \cdot \alpha_{12} \cdot \beta_2 \end{aligned} \tag{3.7}$$

and the parity condition: if $d \equiv 1 \pmod 4$ then $c(d)$ is odd must hold.

(3.7) holds iff $\alpha = 1, \alpha_{01} = \alpha_{02} = \beta_0 = 1, a' = 1, a'_{01} = 1, \alpha_{12} = a'_{12}, \beta_1 = b'_1, \beta_2 | b'_2$.

In particular, $(d_0, d_1) = a \cdot a_{01} \Rightarrow (d_0, d_1)' = a'_0 \cdot a'_{01} = 1$ and if $(d_0, d_1) = 2$ then $c(d_{01}) = d_1$ is even, so odd d_{01} must be 3 (mod 4).

To finish the proof of the proposition 3.10 we have to check that the parity condition for the m function c from the proposition:

If $d \equiv 1 \pmod 4$, then $c(d)$ is odd. Let us check that the parity condition holds. It holds for d_0, d_1 because $c_1 = 1, c_1 = d_1$.

Now suppose $d_{01} \equiv 1 \pmod 4$. Then $(d_0, d_1) = 1$ by the condition of proposition 3.10. Hence $c_{01} = d_1$ is odd because otherwise d_1 is even$\Rightarrow$ d_0 is even because $d_{01} = d_0 \cdot d_1$ and d_{01} is odd. Then $(d_0, d_1) = 2$ - contradiction.

So the parity condition holds for d_{01} also.

In the second case there are no $d \equiv 1 \pmod 4$, $d \in W \setminus \{d_0, d_1, d_{01}\}$, so the parity condition holds. In the first case, we have to check the parity condition for $d \in \{d_2, d_{02}, d_{12}, d_{012}\}$ with $c(d) = c_2, c_2, c_2 \cdot d_1, c_2 \cdot d_1$ respectively. Now $d_2 \equiv 1$ (mod 4) and c_2 is odd by the conditions of proposition 3.10. If $c_2 \cdot d_1$ is even, then d_1 is even, so d_{12} is even. Also $d_{01} \not\equiv 1 \pmod 4$ because d_1 is odd if $d_{01} \equiv 1 \pmod 4$ as was proved above. Hence $d_{012} \equiv d_{01} \not\equiv 1 \pmod 4$.

Proposition 3.11. *Let $d_0 \in W, U \in M_6(W)$ with $X(U) = W \setminus \{d_0\}$ iff for a basis $\{d_0, d_1, d_2\}$ $U = U(c)$, where c is a m function as in the proposition 3.5 with $c_0 = 1$, so $\alpha = \alpha_{01} = \alpha_{02} = \beta_0 = x = 1$ and $c(d) \notin \{1, d\}$ for $d \in X(U)$.*

Proof: Follows from proposition 3.5 and existence of m-section of U such that $c_0 = 1$ consequence 3.1 taking into account the definition of the rank of U.

Proposition 3.12. *$U \in M_7(W) \Leftrightarrow U = U(c)$, where c is as in the proposition 3.5 and $c(d) \notin \{1, d\}$ for all $d \in W$.*

Proof: Follows from proposition 3.5 and the definition of the rank of U.

3.5 The structure of the group $ms(U)$

Let U be a unoid associated to W. The group $ms(U)$ of m-subunoids of U is 2-periodic, so it is a $\mathbb{Z}/2\mathbb{Z}$ - vector space. We will show that $dim(ms(U)) \leq 2$ and describe explicitly the cases when $dim(ms(U)) = 2$.

We call preunoids when U_1 and U_2 compatible if $C_1(d) = C_2(d)$ for $d \in X_1 \cap X_2$, where $X_i =$ base of U_i.

It follows from the definition that U_1, U_2 are subpreunoids of a preunoid U iff U_1, U_2 are compatible.

Also let for compatible U_1, U_2, $U_1 \cup U_2$ be the preunoid with the base $X_1 \cup X_2$ and for $d \in X_i$ $C(d) = C_i(d)$.

Then $U_1 \cup U_2$ is the smallest U such that $U_i \in s(U)$. More precisely $U_1, U_2 \in s(U) \Leftrightarrow U_1 \cup U_2 \in s(U)$.

Let U_1, U_2 are compatible preunoids of rank r_1, r_2 respectively. Let $r_{12} = |X_1 \cap X_2|$, where X_i is the base of U_i. Let $U_3 = U_1 \cdot U_2$. The base X_3 of U_3 is $[X_1 \setminus (X_1 \cap X_2)] \cup [X_2 \setminus (X_1 \cap X_2)]$

$r_3 = rank(U_3) = r_1 + r_2 - 2r_{12}$ So for permutation (i, j, k) of $(1, 2, 3)$, if $X_{ij} = X_i \cap X_j, r_{ij} = |X_{ij}|$

$$r_i = r_j + r_k - 2r_{jk} \tag{3.8}$$

because $U_i = U_j \cdot U_k$

Proposition 3.13. *Let $U_1 \in MP_7(W)$. Then if $U_2 \in MP(W)$ is compatible with U_1,then $U_2 = U_0$ or U_1.*

Proof: Suppose $U_2 \neq U_1, U_0$ is compatible with U_1.

Let $U_3 = U_1 \cdot U_2$: Then $r_{12} = r_2$ so $r_3 = 7 - r_2$ by (3.8).

$U_3 \neq U_0$, so by the proposition 3.6($U \in MP(W), U \neq U_0 \Rightarrow r(U) \geq 3) r_2 \geq 3, 7 - r_2 \geq 3 \Rightarrow$ $r_2 = 3$ or 4 and then $r_3 = 4$ or 3 respectively.

It follows from proposition 3.6 and consequence 3.3 that if $U \in MP_3(W)$ then $X(U)$ is a basis of W and if $U \in MP_4(W)$ then $W \setminus X(U)$ is a p-hyperplane.

Now $X_3 = W \setminus X_2$, so X_2, X_3 is a basis and p-hyperplane simultaneously if $r_2 = 3,4$ respectively. What is impossible.

Now if $U_1, U_2 \in MP(W)$ are compatible, $U_1 \neq U_2$, then $U_3 \in MP(W), U_3 \neq U_0$, so

$$r_1 + r_2 - 2r_{12} \geq 3 \tag{3.9}$$

Also

$$r_1 + r_2 - r_{12} \leq 7 \tag{3.10}$$

because $W \supset X_1 \cup X_2 =$ disjoint union of $X_1 \setminus (X_1 \cap X_2), X_1 \cap X_2$ and $X_2 \setminus (X_1 \cap X_2)$. In particular,

$r_1 + r_2 - 7 \leq r_{12} \leq \frac{r_1+r_2}{2} - \frac{3}{2} \Rightarrow \frac{r_1+r_2}{2} \leq 7 - \frac{3}{2} \Rightarrow r_1 + r_2 \leq 11,$

Hence $U_1, U_2 \in MP_6(W), U_1 \neq U_2$, cannot be possible. Taking into account the proposition

3.13 we have

Consequence 3.5. *Let U_1, U_2 be distinct non trivial compatible m-preunoids. Then $r_i \leq 6$ and one of r_i is less than or equal to* 5.

Proposition 3.14. *There is no compatible $U_1 \in M_5(W), U_2 \in M_6(W)$.*

Proof: Suppose $U_1 \in M_5(W), U_2 \in M_6(W)$ are compatible.

Then (3.9),(3.10) $\Rightarrow r_{12} = 4$, hence $U_3 \in M_3(W)$ by (3.8).

Again (3.8)$\Rightarrow r_{13} = 1$. Let $X_1 \cap X_3 = \{d_2\}$ and $X_3 = \{d_0, d_1, d_2\}$, so $\{d_0.d_1\} = W \setminus X_1$. Then $(d_0, d_1)|2$ by the proposition 3.10, so $a = (d_0, d_1, d_2)|2$.

On the other hand $d_{012} = a \cdot b_0 \cdot b_1 \cdot b_2$ and $b_0 \cdot b_1 \cdot b_2|2$ by the proposition 3.8. Hence $d_{012}|2^2 \Rightarrow d_{012} = 2$ being square free. But $d_{012} \in X_1$ and we come to a contradiction taking into account:

Proposition 3.15. *Let U be a unoid, X is the base of U, then $2 \notin X$.*

Proof: Let an even $d \in X$, $a \in C(d)$. Then by definition of a unoid $a \neq 1, d, a|d$ hence $d \neq 2$.

Proposition 3.16. *There is no compatible $U_1 \in MP_5(W), U_2 \in MP_5(W)$, $U_1 \neq U_2$.*

Proof: Suppose such U_1, U_2 exist. Then (3.9)(3.10) $\Rightarrow r_{12} = 3$, so $U_3 \in MP_4(W)$. Then $r_{13} = 2$. Let $X_3 \setminus X_{13} = \{d_0, d_1\}$ and $d_2 \in X_{13}$. We know (Proposition 3.6) that X_3 is

the complement to a p-hyperplane, so d_0, d_1, d_2 is a basis and $X_{13} = \{d_2, d_{012}\}$. By the Proposition 3.6. U_3 has an m-section e such that $e(x) = \gamma \, \forall x \in X_3$. Let c be the m-section of U_1 such that $c_0 = 1, c_1 = d_1$ (see Proposition 3.7).

The sets $C_1(d)$ and $C_3(d)$ coincide if $d \in X_{13}$ (because U_1 and U_3 are compatible). Hence $c_2 = \gamma$ or $\gamma \cdot d_2$ and $c_{012} = d_1 \cdot c_2 = \gamma$ or $\gamma \cdot d_{012}$. If $c_2 = \gamma, d_1 \cdot \gamma \neq \gamma, \gamma \cdot d_{012}$ If $c_2 =_2 \gamma \cdot d_2$, $d_1 \cdot d_2 \gamma \neq \gamma, \gamma \cdot d_{012}$ which is a contradiction.

Proposition 3.17. *There is no compatible $U_1 \in MP_4(W), U_2 \in MP_6(W)$.*

Proof: Suppose such U_1, U_2 exist. Then (3.9)(3.10) $\Rightarrow r_{12} = 3$. Hence $U_3 \in M_4(W), U_3 \neq U_1, U_1 \cdot U_3 = U_2$. On the other hand the product of the two distinct compatible m pre-unoids of rank 4 has rank 4, because their bases are complements to p-hyperplanes $\Rightarrow$ contradiction.

Proposition 3.18. *There is no compatible $U_1 \in M_3(W), U_2 \in M_6(W)$.*

Proof: Suppose such U_1, U_2 exist. Then (3.9)(3.10) $\Rightarrow r_{12} = 2$ or 3. If $r_{12} = 2$ then $U_3 \in M_5(W), U_3 \neq U_2$ is compatible with U_2. What contradicts to Proposition 3.14, hence $r_{12} = 3$, which means $\cdot \, X_1 \subset X_2$. So $X_3 = X_2 \setminus X_1$ and both X_1, X_3 are basis of W by Consequence 3.2. Let $X_1 = \{d_0, d_1, d_2\}$. Then $W \setminus X = \{d_{01}, d_{02}, d_{12}, d_{012}\}$ and X_3 necessarily contains d_{012}, because $\{d_{01}, d_{02}, d_{12}\}$ is a p-hyperplane. Any two elements of it together with d_{012} is a basis. Say $X_3 = \{d_{01}, d_{02}, d_{012}\}$, other cases are symmetrical. By the Proposition 3.8 $b_0 = 1$ or 2. Also (3.5) with $\phi(d) = d$ imply that $mcd(x : x \in X_3) = b_0$. By

Proposition 3.8 applied to U_3 $d_0 = d_{01} \cdot d_{02} \cdot d_{012} = b_0$ or $2 \cdot b_0 \Rightarrow d_0 = 2$ which contradicts Proposition 3.15.

Proposition 3.19. *Let $U_1 \in MP_5(W), U_2 \in MP_4(W)$ are compatible.*

Then $U_3 \in MP_3(W)$ and $r_{12} = 3, r_{13} = 2, r_{23} = 1$. Let $U_1 \in M_5(W), U_2 \in M_3(W)$. Then $U_3 \in M_4(W)$ and $r_{12} = 2, r_{13} = 3, r_{23} = 1$.

Proof: In the first case (3.9),(3.10) $\Rightarrow r_{12} = 2$ or 3 . If $r_{12} = 2$, then $U_3 \in MP_5(W)$ which contradicts the proposition 3.16. Hence $r_{12} = 3$ and the other statements follow. In the second case (3.9)(3.10) $\Rightarrow r_{12} = 1$ or 2. If $r_{12} = 1$ then $U_3 \in MP_6(W)$ which contradicts proposition 3.14. Hence $r_{12} = 2$ and the statements follow.

We have proved so far that $U \in M_7(W) \cup M_6(W)$ has not compatible m-unoids distinct from U or U_0, while $U \in M_5(W)$ is compatible to a m-unoid $U' \neq U, U_0$ if and only if $\exists$ compatible $U_1 \in M_3(W), U_2 \in M_4(W) : U = U_1 \cdot U_2$ and $U' = U_1$ or U_2.

So we have reduced the study of compatible m-unoids U_1, U_2 to the cases when $r_1 = r_2 = 3; r_1 = 3, r_2 = 4$ or $r_1 = 4, r_2 = 3; r_1 = r_2 = 4$.

Proposition 3.20. *$U_1, U_2 \in M_4(W), U_1 \neq U_2$, are compatible if and only if $|W_1| = 1$, say $W_1 = \{x\}, 2 \notin W$ and if J be the set of cosets of $W/\{x\}$ by $\{1, x\}$, then X_1, X_2 are the unions of cosets from two distinct pairs of cosets, while X_3 is the union of cosets from the remaining pair of cosets, and U_i all have m-sections equal to 2 on X_i.*

Proof: The set J consists of three elements, so the statement about $X_3 := (X_1 \setminus X_{12}) \cup (X_2 \setminus X_{12})$ follows.

$W \setminus X_i = \{x\} \cup Y_i$ is a p-hyperplane because $Y_i \in J$. By the proposition 3.9, U_i with the base X_i, and m-section equal to 2 on X_i is an m-unoid of rank 4 and U_i, U_j are obviously compatible.

Suppose $U_1, U_2 \in M_4(W), U_1 \neq U_2$ are compatible. Then $r_{12} = 2$ as was discussed above, so $U_3 \in MP_4(W)$. By the proposition 3.9 each U_i has an m-section equal to γ_i on X_i. If $\gamma_1 \neq \gamma_2$ then $\gamma_1 \cdot \gamma_2 = d$ for $d \in X_1 \cap X_2$(because $C_1(d) = C_2(d)$ for such d by the compatibility of U_1 and U_2) which is impossible, hence $\gamma_1 = \gamma_2$. If an odd prime $p|\gamma$ then by proposition 3.9 $p|d$ for $d \in X_1 \cup X_2$, but $|X_1 \cup X_2| = 6$, while p can divide no more than 4 of the elements of W by the proposition 3.3. Hence $\gamma = \gamma_1 = \gamma_2 = 2$. The elements of X_1, X_2 cannot be $\equiv 1 \pmod 4$ by the Proposition 3.9, hence $W_1 \subset W/\{X_1 \cup X_2\}$, and $|W_1| = 1$ because always $|W_1| \geq 1$, as was shown in section 4. Let $W_1 = \{x\}$. If $y \neq x, y \notin X_i$, then the coset $\{y, y \cdot x\} \not\subset X_i$ because $W \setminus X_i$ is a p-hyperplane. So X_i is the union of the two remaining cosets of $\{1, x\}$ in W, not equal to $\{y, y \cdot x\}$. Also U_3 has m-section equal to 2 on X_3. This follows because U_3 has an m-section equal to the product of the m-sections for U_1, U_2 or by considering the pair U_1, U_3 like the pair U_1, U_2 above.

Proposition 3.21. *$U_1, U_2 \in M_3(W), U_1 \neq U_2$, are compatible if and only if $|W_1| = 1$, say $W_1 = \{x\}$, $2 \in W$, the bases X_i of U_i are the unions of $\{2x\}$ and distinct cosets of $\{1, x\}$ in*

$X_3 = W \setminus \{x, 2, 2x\}$, U_i corresponds to the basis of X_i of W via the correspondence of the consequence 3.3, so U_i has the m-section equal to 2 on X_i. The unoid $U_3 = U_1 \cdot U_2 \in M_4(W)$ has the base X_3 and m-section equal to 2 on X_3.

Proof: If $\{y, yx\}$ is a coset of $\{1, x\}$ in X_3, then $X = \{2x, y, yx\}$ is a basis of W, so for $i = 1, 2$ $U_i \in MP_3(W)$ and has an m-section equal to $2 =_2 \prod_{x \in X_i} x$ by the consequence 3.3. Then $U_i \in M_3(W)$ because X_i does not contain any elements $\equiv 1 \pmod 4$. This also follows from proposition 3.8. U_1, U_2 are compatible because they have sections equal on $X_1 \cap X_2$. The statements on U_3 follow from the definition of the product $U_1 \cdot U_2$.

Now suppose $U_1, U_2 \in M_3(W), U_1 \neq U_2$, are compatible. Then $r_{12} = 0$ or 1 by (3.9). If $r_{12} = 0$ then $U_3 \in M_6(W)$ is compatible with U_1 and U_2 which contradicts proposition 3.18. We conclude that $r_{12} = 1$. Let $X_{12} = \{d_2\}$, $X_1 = \{d_0, d_1, d_2\}$ - the basis of W by the consequence 3.3. Let $U_3 = U_1 \cdot U_2 \in MP_4(W)$ by (3.7), $X_3 =$ the base of U_3.

Then $d_0, d_1 \in X_3$ while $d_2 \notin X_3$ because $X_3 = (X_1 \setminus \{d_2\}) \cup (X_2 \setminus \{d_2\})$, If $d_0 \cdot d_2 \notin X_3$ then $d_0 = (d_0 \cdot d_2) \cdot d_2 \notin X_3$ because W/X_3 is a p-hyperplane, - contradiction. Hence $d_{02} \in X_3$.

Similarly $d_{12} \in X_3$. We conclude that $X_3 = \{d_0, d_1, d_{02}, d_{12}\}$. Both U_1, U_3 have m-sections constant, say equal to γ_1, γ_3, respectively on their bases by proposition $(\cdot)$ and the consequence 3.3. We claim that $\gamma_1 = \gamma_3 = \gamma$ Otherwise $\gamma_1 \cdot \gamma_2 = d$ for $d \in X_{13} = \{d_0, d_1\}$. because U_1, U_3 are compatible, what is impossible.

Now $\gamma' = a'$ by the proposition 3.8 (we recall that N' is the largest odd factor of N and

a, a_{ij}, b_i are numbers associated to the basis $\{d_0, d_1, d_2\}$ and $\phi(d) = d$ by (3.4)).

Now $mcd(d : d \in X_3) = a_{01}$ by (3.4). So $\gamma' | a'_{01}$ by the proposition 3.9. We conclude that $\gamma' = 1$ because $(a, a_{01}) = 1$. Hence $\gamma = 2$ being a square free natural integer.

Now $d_{012} = \gamma_1 = 2$ and $W_1 = \{d_{01}\}$ because $|W_1| \geq 1$ and $(X_1 \cup X_3) \cap W_1 = \emptyset$ by the parity condition. Let $x = d_{01} \equiv 1 \pmod 4$.

Then $d_2 = d_{012} \cdot d_{01} = 2x$, $X_1 = \{2x\} \cup \{d_0, d_0 \cdot x\}$, $X_2 = X(U_1 \cdot U_3) = \{d_2, d_{02}, d_{12}\} = \{2x\} \cup \{d_{02}, d_{02} \cdot x\}$.

Also U_2 has m-section equal to 2 on X_2, because 2 is the product in SF of $x \in X_3$, or by considering U_2 instead of U_1. The proposition 3.21 is proved.

Proposition 3.22. *$U_1 \in M_3(W), U_2 \in M_4(W)$ are compatible with $U_3 = U_1 \cdot U_2 \in M_5(W)$ if and only if $|W_1| = 1, 2 \in W$ and if $\{z, y, x\}$ is a basis of W defined (up to permutations of y, z) by conditions $y \equiv z \equiv 3$ (mod 4) so $W_1 = \{x\}, x = y \cdot z$, then $(y, z) = 1$, $X_2 = W \setminus \{2, x, 2x\}$, U_2 has an m-section equal to 2 on X_2; $X_1 = \{x, 2x, 2y\}$ or $\{x, 2x, 2z\}$ and U_1 has an m-section equal to y, z respectively on X_1.*

U_3 has the base $W \setminus \{2, 2y\}, W \setminus \{2, 2z\}$ and m-section c such that $c(2) = 1, c(2y) = 2y$, $c(x) = y$; $c(2) = 1, c(2z) = 2z, c(x) = z$ respectively.

Proof: If $2 \in W$ then W contain 4 even and 3 odd elements (proposition 3.3). The condition $|W_1| = 1$ means W contains two elements $y, z \equiv 3 \pmod 4$, so $W_1 = \{y \cdot z\}$ and $2, y, z$ is a

basis for W. Preunoids U_1, U_2 defined in the proposition 3.22 belong to $M_3(W), M_4(W)$ by the propositions 3.8, 3.9 respectively, they are compatible because $X_{12} = \{d_2\}$ and U_1, U_2 have common $C(d_2) = \{2, 2 \cdot d_2\}$. Statements about U_3 follow directly from the definitions and the computation of the product of the m-sections of U_1, U_2 presented in the proposition 3.22.

Now suppose $U_1 \in M_3(W), U_2 \in M_4(W)$ are compatible. The condition U_3 is in $M_5(W)$ means that $r_{12} = 1$ by (3.8). Let $X_{12} = \{d_2\}$ and let $X_1 = \{d_0, d_1, d_2\}$ - a basis for W being the base of U_1. Now $W \setminus X_2$ is a p-hyperplane containing $\{d_0, d_1\}$, so $W \setminus X_2 = \{d_0, d_1, d_{01}\}$.

Then $mcd(d : d \in X_2) = b_2$ by (3.4) and U_2 has an m-section constant, say equal to γ, on X_2 such that $\gamma' | b_2$ according to the proposition 3.9. Also $b_2' = 1$ and U_1 has m-section equal to d_{012} on X_1 according to consequence 3.3 and the proposition 3.8.

We conclude that $\gamma' = 1 \Rightarrow \gamma = 2$. Compatibility of U_1, U_2 means that $\{d_{012}, d_{012} \cdot d_2\} = \{2, 2 \cdot d_2\}$ what implies that $d_{012} \cdot d_2 = d_{01} = 2$ because $d_{012} \in X_2$, but $2 \notin X_2$ by proposition 3.15. $W_1 \cap X_2 = \emptyset$ by the parity condition. We conclude that $W_1 = \{x\}$ where x is among d_0, d_1 which is odd, say $x = d_0$. Then $d_1 = d_{01} \cdot d_0 = 2x$. Because $x \equiv 1 \pmod 4$, $d_{012} = 2 \cdot d_2$, is odd by the parity condition. Let $d_2 = 2y$, where y is odd. Then $y = d_{012} \in X_2 \Rightarrow y \equiv 3 \pmod 4$. Also $y = a = mcd(d : d \in X_1)$ according to proposition 3.8. Hence $y | x$, let $z = x/y$. Then $(y, z) = 1$ and $z \equiv 3 \pmod 4$.

So $X_1 = \{x, 2x, 2y\}, X_2 = W \setminus \{x, 2x, 2\}$ and $\{2, y, z\}$ is a basis for W. Proposition 3.22 is

proved.

Let U_1, U_2, U_3 be a triple of pairwise compatible m-unoids such that $U_1 \cdot U_2 \cdot U_3 = U_0$ what is equivalent that $U_i \cdot U_j = U_k$ for i, j, k being a permutation of $(3, 1, 2)$.

We note that the pairwise compatibility is equivalent to the compatibility of any pair among the $\{U_i\}$, because if U_i and U_j are compatible $U_i, U_j \subset U_i \cup U_j$ (are subunoids) and $U_k = U_i \cdot U_j$ is also a sub-unoid of $U_i \cup U_j$. These inclusions also imply that $U_i \cup U_j$ coincide for all pairs (i, j).

Proposition 3.23. *The triples U_1, U_2, U_3 described in proposition 3.20 , 3.21 , 3.22 are the only triples (up to permutations of indices) of pairwise distinct, non trivial, compatible m-unoids with $U_1 \cdot U_2 \cdot U_3 = U_0$*

Proof: Consequence 3.5, Propositions 3.14 , 3.17, 3.18

imply that $U \in M_7(W)$ or $M_6(W)$ cannot appear in such a triple.

Proposition 3.19 implies that $U \in M_5(W)$ may appear only in the situation described in proposition 3.22.

The remaining cases are where all $U_i \in M_3(W)$ or $M_4(W)$. If two of them belong to $M_4(W)$ we are in a situation of the proposition 3.20, while if two belong to $M_3(W)$ we are in the situation of proposition 3.21.

Proposition 3.24. *Let U be a unoid associated to W. Then $dim_{\mathbb{Z}/2\mathbb{Z}}(ms(U)) \leq 2$. If*

$|W_1| > 1$, *then* $dim_{\mathbb{Z}/2\mathbb{Z}}(ms(U)) \leq 1$.

Proof: The condition $|W_1| = 1$ is a necessary condition for existence of triples of compatible m-unoids described in the propositions 3.20 - 3.22. Hence if $|W_1| \geq 1$ ($\Leftrightarrow |W_1| = 3$ or 7, then taking into account the proposition 3.23, the group $ms(U)$ contains at most 1 nontrivial m-unoid. So its order is≤ 2. Let $|W_1| = 1$ Suppose $\exists U$ such that $dim_{\mathbb{Z}/2\mathbb{Z}}(ms(U)) \geq 3$.

Any 3 dimensional $\mathbb{Z}/2\mathbb{Z}$ vector space contains 7 hyperplanes, so there are seven, at least, distinct triples (not - ordered), of pairwise distinct, non trivial compatible m-unoids associated with W. with the product of the unoids in the triples equal to U_0.

The condition $2 \in W$ is a necessary condition for the existence of such triples described in the propositions 3.21, 3.22. Hence if $2 \notin W$, then there is only one triple winch was described in proposition 3.20. Suppose $2 \in W$. Then there are not more than 3 such triples taking into account the propositions 3.21 , 3.22 and the proposition 3.23. We conclude that such U cannot exist so always $dim_{\mathbb{Z}/2\mathbb{Z}}(ms(U)) \leq 2$.

Now, taking into account the previous results, we want to summarize the description of $ms(U)$, in particular, to list explicitly these U for which $dim_{\mathbb{Z}/2\mathbb{Z}} ms(U) = 2$

Proposition 3.25. $dim_{\mathbb{Z}/2\mathbb{Z}}(ms(U)) = 2$ *if and only if* W *and* U *are as follows:* $|W_1| = 1$ *and*

if $2 \notin W$, *then* U *is an extension (has it as a sub unoid) of the unoid with the base* $X =$

$W \setminus \{2\}$ and the section equal to 2 on X. Then $ms(U) = \{U_0, U_1, U_2, U_3\}$, where $U_i \in M_4(W), i = 1,2,3$ are described as in proposition 3.20, if $2 \in W$, let $\{2, y, z\}$ be a basis for W such that $y \equiv z \equiv 3$ (mod 4)(defined up to permutation of y and z). Let $x = y \cdot z$.

If $(y,z) > 1$, then U is an extension of the unoid with the base $X = W/\{2,x\}$ and the section equal to 2 on X. Then $ms(U) = \{U_0, U_1, U_2, U_3\}$, where $U_1, U_2 \in M_3(W), U_3 \in M_4(W)$ are described in the proposition 3.21.

If $(y,z) = 1$, then U is either as above, or U is the unoid with the base $X = W/\{2\}$ and the section c such that $c(x) = c(2x) = y$, $c(d) = 2$ for $d \in W/\{2,x,2x\}$ or U is the unoid with the base $X = W/\{2\}$ and the section c such that $c(x) = c(2x) = z$, $c(d) = 2$ for $d \in W/\{2,x,2x\}$. In the last two cases $ms(U) = \{U_0, U_1, U_2, U_3\}$, where $U_1 \in M_3(W), U_2 \in M_4(W), U_3 \in M_5(W)$ are as described in proposition 3.22 when U_1 has the base $\{x, 2x, 2y\}, \{x, 2x, 2z\}$ respectively.

For all other U, in particular, if $|W_1| > 1$, $ms(U) = \{U_0, U_1\}$ if $\exists$ a m-unoid $U_1 \subset U$ and $ms(U) = \{U_0\}$ otherwise.

Proof: If $dim_{\mathbb{Z}/2\mathbb{Z}}(ms(U)) = 2$, then, taking into account the proposition 3.23), U contains a triple (U_1, U_2, U_3) described in one of the propositions 3.20 - 3.22. Then U is an extension of the unoid $U_1 \cup U_2$ and that is exactly the unoid described in proposition 3.25 in the cases 1 - 3 respectively ($2 \notin$ the base of U by the proposition 3.15). Then $ms(U) \supset \{U_0, U_1, U_2, U_3\}$ and so $ms(U) = \{U_0, U_1, U_2, U_3\}$ because $dim_{\mathbb{Z}/2\mathbb{Z}}(ms(U)) = 2$.

The final statement of the proposition 3.25 is obvious.

3.6 The structure of $ms(U_K)$ under the ramified divisors condition.

In this section we interpret some results about the group $ms(U_K)$, obtained earlier in chapter 3, supposing that the ramified divisors condition holds for K and taking into account some results of our work.

Let W_{+o} be the subset of $W = W(K)$ consisting of elements $d \in W$ such that d is divisible by a prime $\equiv 3 \pmod 4$.

The proposition 2.4 implies that $W_{+o} \subset W_+$. And the proposition 4.3 implies that under the ramified divisors condition for K $W_+ = W_{+o}$ and hence $W_- = W \setminus W_+$ is the p-subspace of V consisting of all elements $d \in W$ not divisible by primes $\equiv 3 \pmod 4$.

Let $1 \neq d \in SF$, $k = \mathbb{Q}(\sqrt{d})$, ε_d is a positive fundamental unit of k, a natural number c divides the discriminant of k , $c \neq 1, d$. Then $c \in C_k(\varepsilon_d)$ (and hence $N(\varepsilon_d) = 1$, because $C_k(\varepsilon_d)$ is empty if $N(\varepsilon_d) = -1$) $\Leftrightarrow \varepsilon_d = ca^2$, where $a \in k, \Leftrightarrow \varepsilon = c(a')^2$ for some ε of k and $a' \in k$ (because $\varepsilon/\varepsilon_d \in E_k^2 \Rightarrow C_k(\varepsilon_d) = C_k(\varepsilon)$) $\Leftrightarrow \sqrt{c}$ is a principal divisor $\Leftrightarrow$ the divisor class of $\sqrt{c} \in Cl_k^2$, if the ramified divisors condition holds for k, (because then the divisor class of $\sqrt{c} \in Cl_{k,2} \cap Cl_k^2 = 1$) $\Leftrightarrow \sqrt{c}$ is orthogonal to Δ_d under the pairing $(,)$ (see section 4.1) We suppose further in this section that $n = 3$.

Now we are going to interpret the results of the proposition 3.25 for $U = U_K$, taking into account the above and the proposition 4.2.

Note that under the ramified divisors condition for K, the case in proposition 2.25 when $2 \in W$ and U_K is the extension of the unoid with the base $X = W \setminus \{2,x\}$ and the section equal to 2 on X is actually the case when U_K has the base $W_+ = W \setminus \{2\}$, because $W_+ = W_{+o}$ is the supplement to W_- which is the p-subspace of U, so $|W_+| = 7,6,4,0$. Also $2 \notin W_+$ because $N(\varepsilon_2) = -1$. In the following proposition 3.26 we will mark this case as the case when $c(2x) = 2$. The other two cases in the proposition 3.25 when $2 \in W$ we will mark as the cases when $c(2x) = y,z$ if this is the case when $\exists$ a section $c \mid c(2x) = y,z$ respectively.

Let $t_K = dim(ms(U_K))$. We recall that $T(W)$ is the set of all primes which divide at least one element of W.

Proposition 3.26. *Suppose that $n = 3$ and the ramified divisors condition holds for K. If $2 \notin W$, the cases when $t_K = 2$, described in proposition 3.25 (that is all cases when $2 \notin W, t_K = 2$) happen iff $|W_1| = 1, W_{+o} \supset W \setminus W_1$ and all primes $p \equiv 1 \pmod 4 \in T(W)$ are equal to 1 (mod 8) and all primes $\equiv 3 \pmod 4 \in T(W)$ are equal (mod 8).*

If $2 \in W$, the cases when $t_K = 2$, described in the proposition 3.25 (that is all cases when $2 \in W, t_K = 2$) happen as follows. It is necessary that $|W_1| = 1 \Leftrightarrow W$ has a basis $\{2,y,z\}$, where $y \equiv z \equiv 3 \pmod 4$ (y,z are determined up to transposition) and both y,z are satisfied

the condition (4.2) with $\{3,7\} \ni i = i(y), i(z)$ *respectively, that is all primes* $\equiv$ *1 (mod 4) dividing* y,z *are* $\equiv$ *1 (mod 8) and all primes* $\equiv$ *3 (mod 4) dividing* y,z *are* $\equiv i(y), i(z)$ *(mod 8) respectively. Let* $x = y \cdot z$ *. Then the case when* $c(2x) = 2$ *happens iff additionaly* $\exists$ *a prime* $\equiv$ *3 (mod 4) dividing x (this condition holds automatically if* $(y,z) = 1$ *) and* $i(y) = i(z)$*. The cases when* $c(2x) = y,z$ *happen iff additionally (to the above necessary conditions)* $(y,z) = 1, i(y) \neq i(z), 7 = i(y), i(z)$ *respectively and the following common for both cases conditions hold:*

$$\begin{array}{c} (\frac{z}{p}) = 1 \forall \textit{ prime } p \equiv \textit{ 1 (mod 4), } p|y \\ (\frac{y}{p}) = 1 \forall \textit{ prime } p \equiv \textit{ 1 (mod 4), } p|z \\ (\frac{y}{p_1}) = (\frac{y}{p_2}) \forall \textit{ primes } p_1, p_2 \equiv \textit{ 3 (mod 4), } p_1, p_2|z \\ (\frac{z}{p_1}) = (\frac{z}{p_2}) \forall \textit{ primes } p_1, p_2 \equiv \textit{ 3 (mod 4), } p_1, p_2|y \\ (\frac{y}{p_2}) = -(\frac{z}{p_1}) \forall \textit{ primes } p_1, p_2 \equiv \textit{ 3 (mod 4), } p_2|z, p_1|y \end{array} \tag{3.11}$$

Proof: Suppose $2 \notin W$. We know (see above) that under the ramified divisors condition for K the base of U_K, which is always the set W_+, is equal to W_{+o}. And because of proposition 4.4 the subunoid of U_K with the base $X = W \setminus W_1$ has a section equal to 2 on X iff each $d \in X$ satisfies the condition (4.2) with $i = i(d) \in \{3,7\}$. We need only show that then $i(d)$ does not depend on d, that is that all primes $\equiv 3 \pmod 4 \in T(W)$ are equal (mod 8).

Let $p_1, p_2 \equiv 3 \pmod 4 \in T(W)$. Let $H'_{p_i} = \{x \in W : p_i \not| x\}$. Then H'_{p_i} is a p-hyperplane of V by proposition 3.3. Now $|H'_{p_1} \cup H'_{p_2}| \leq 5$ because $|H'_{p_1} \cap H'_{p_2}| \geq 1$ (see the end of section

4.2). Hence $\exists d \in X, d \notin H'_{p_1} \cup H'_{p_2}$ because $|X| = 6$, and so p_1, p_2 divide $d \Rightarrow p_1, p_2 \equiv i(d) \pmod 8 \Rightarrow p_1 \equiv p_2 \pmod 8$.

Suppose $2 \in W, |W_1| = 1, \{2, y, z\}$ - a corresponding basis of W, $x = y \cdot z$, so $W_1 = \{x\}$. In all cases when $t_K = 2$, according to the proposition 3.25, $W_{+o} = W_+ =$ the base of $U_K = W \setminus \{2\}$ (see the remark above that W_{+o} cannot be equal to $W \setminus \{2, x\}$). Hence it is necessary that $\exists$ a prime $p \equiv 3 \pmod 4$ dividing x , that automatically follows if $(y, z) = 1$. Also in all cases there exists a section c of U_K such that $c(y) = c(z) = 2$ what forces y, z to satisfy the condition (4.2) with $i = i(y), i(z)$ respectively, because of the proposition 4.4. Now the cases split as follows. The case $c(2x) = 2$ happens iff $i(y) = i(z)$ because this marks the case (according to our agreement) when $\exists$ a section of c of U_K equal to 2 on $X' = W \setminus \{2, x\}$, for what the condition $i(y) = i(z)$ is sufficient, because then all $d' \in X$ satisfy the condition (4.2). The condition $i(y) = i(z)$ is also necessary, because if $p_1, p_2 \equiv 3$ (mod 4) than it can be proved as above that $\exists d \in W \setminus \{2\}$ such that p_1, p_2 both divide d, hence such d can be chosen to be in X' (if p_1, p_2 both divide x, they both divide $2x$)$\Rightarrow p_1 \equiv i(d) \equiv p_2 \pmod 8 \Rightarrow i(y) = i(z)$.

The cases when $c(2x) = y$ or z differ from the case when $c(2x) = 2$, because in the latter case a section of U_K may take on $2x$ only values 2 and x which are different from both y and z . Hence $i(y) \neq i(z)$ for these cases, also $(y, z) = 1$ by the proposition 3.25.

The remaining conditions to satisfy for the cases when $c(2x) = y, z$ are the conditions that

$w \in C_{k_1}(\varepsilon_{d_1}), w \in C_{k_2}(\varepsilon_{d_2})$, where $k_i = \mathbb{Q}(\sqrt{d_i}), d_1 = x, d_2 = 2x$ and $w = y, z$ respectively .

For these are exactly the cases when $\exists$ a section c on U_K, as described in proposition 3.25, taking into account that c can already be chosen to be equal to 2 on $W \setminus \{2, x, 2x\}$ because y, z satisfy the condition (4.2). Hence we have to check when $\sqrt{w}$ is orthogonal to $\Delta_{d_i}, i = 1, 2$, under the corresponding paring $(,)$ as was discussed in the beginning of section 3.6.

Let us start with the case $d_1 = x$. Note that if $y \in C_{k_1}(\varepsilon_x) \Leftrightarrow z \in C_{k_1}(\varepsilon_x)$ because $y \cdot z = x$. It follows from proposition 4.2 that Δ_x is generated by cosets (mod $(k_1)^*$) of primes $p \equiv 1$ (mod 4) dividing x and by cosets of $p_1 p_2$, where $p_1 \equiv p_2 \equiv 3$ (mod 4) , p_1, p_2 divide x.

Suppose $p \equiv 1$ (mod 4) , $p|z$. Then $(\sqrt{y}, p) = 1 \Leftrightarrow (\frac{p}{y}) = 1 \Leftrightarrow (\frac{y}{p}) = 1$ (taking into account quadratic reciprocity law). Suppose $p \equiv 1$ (mod 4) , $p|y$. Then $(\sqrt{y}, p) = 1 \Leftrightarrow (\frac{p}{y/p})(\frac{p \cdot x}{p}) = (\frac{y/p}{p})(\frac{(y/p) \cdot z}{p}) \Leftrightarrow (\frac{z}{p}) = 1$. Suppose $p_1, p_2 \equiv 3$ (mod 4) , p_1, p_2 divide z. Then $(\sqrt{y}, p_1 p_2) = 1 \Leftrightarrow (\frac{p_1 p_2}{y}) = 1 \Leftrightarrow (\frac{y}{p_1 p_1}) = 1$ (By the quadratic reciprocity law) $\Leftrightarrow (\frac{y}{p_1}) = (\frac{y}{p_2})$. Suppose $p_1, p_2 \equiv 3$ (mod 4) , p_1, p_2 divide y. Then $(\sqrt{y}, p_1 p_2) = 1 \Leftrightarrow (\frac{p_1}{(y/p_1)})(\frac{p_1 \cdot x}{p_1})(\frac{p_2}{(y/p_2)})(\frac{p_2 \cdot x}{p_2}) = 1 \Leftrightarrow (\frac{p_1}{(y/p_1)})(\frac{y/p_1}{p_1})(\frac{z}{p_1})(\frac{p_2}{(y/p_2)})(\frac{y/p_2}{p_2})(\frac{z}{p_2}) = (\frac{z}{p_1})(\frac{z}{p_2}) = 1 \Leftrightarrow (\frac{z}{p_1}) = (\frac{z}{p_2})$ (taking into account the quadratic reciprocity law and that y/p_1 and y/p_2 have the same number of prime divisors $\equiv 3$ (mod 4)). Suppose $p_1, p_2 \equiv 3$ (mod 4) , $p_1|y$, $p_2|z$. Then $(\sqrt{y}, p_1 p_2) = 1 \Leftrightarrow (\frac{p_1}{(y/p_1)})(\frac{p_1 \cdot x}{p_1})(\frac{p_2}{y}) = (\frac{p_1}{(y/p_1)})(\frac{(y/p_1)}{p_1})(\frac{z}{p_1})(\frac{p_2}{y}) = -(\frac{z}{p_1})(\frac{y}{p_2}) = 1 \Leftrightarrow -(\frac{z}{p_1}) = (\frac{y}{p_2})$ (taking into account the quadratic reciprocity law and that the number of

prime divisors of y congruent to 3 (mod 4) exceeds by 1 the number of prime divisors of y/p_1 congruent to 3 (mod 4)) .

Hence the conditions for $y \in C_{k_1}(\varepsilon_x)$ ($\Leftrightarrow z \in C_{k_1}(\varepsilon_x)$) are exactly the conditions of (3.11). To complete the proof of proposition 3.26, we note that if $z' = 2z, x' = yz'$ then the orthogonality of $\sqrt{y}$ and $\Delta_{x'}$ means the above conditions of orthogonality of $\sqrt{y}$ and Δ_x (in terms of the Legendre symbols) with z replaced by z'. For $\Delta_{x'}$ is generated by the very same $p, p_1p_2 \pmod{(k_2{}^*)^2}$.

The first four conditions in (3.11) holds simultaneously for z and z', because y, z satisfy (4.2), hence $(\frac{2}{p}) = 1$ if $p \equiv 1 \pmod 4$, $p|y$ (then $p \equiv 1 \pmod 8$, and $(\frac{2}{p_1}) = (\frac{2}{p_2})$) if $p_1, p_2 \equiv 3 \pmod 4$, $p_1, p_2|y$ (then $p_1 \equiv p_2 \pmod 8$) (Also $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ by the reciprocity law).

And the last condition in (3.11) means that $(\frac{2}{p_1}) = 1$ $\forall p_1 \equiv 3 \pmod 4$, $p_1|y$ what means that $i(y) = 7$.

Similarly, the orthogonality of $\sqrt{z}$ and Δ_{2x} means that (3.11) holds with y replaced by $2y$ what happens iff $i(z) = 7$.

We see that the conditions for $t_K = 2$ are restrictive what confirms the suggestion in section 3.3 that the threequadratic real fields K with $|W_+| \geq 1$ and $S(K) \neq S_0(K)$ are relatively rare (see the next proposition also).

The next case, when we want to interpret the previous results in chapter 3, is the case

where $|W_1| = 3$, $W_{+o} = W \setminus W_1$. Equivalently, W has a basis $\{d_0, d_1, d_2\}$ such that d_0, d_1 are odd, divisible only by primes $\equiv 1 \pmod 4$ and $\tau_3(d_2) > 0$ where $\tau_3(d) =$ the number of primes $\equiv 3 \pmod 4$, dividing d.

Then $W_1 = \{d_0, d_1, d_0 \cdot d_1\}$. The proposition 3.25 implies that $t_K \leq 1$ in this case.

Proposition 3.27. *Suppose $|W_1| = 3$ $X = W_{+o} = W \setminus W_1$, $b_2 = m.c.d$ of elements of X. If the ramified divisors condition holds for K, $t_K = 1$ iff $\exists 0 < c = \gamma$, where $\gamma | b_2, \gamma \neq 1$, or , in the case when b_2 is odd ($\Leftrightarrow d_2$ is odd), $c = 2\gamma, \gamma | b_2$, such that the following conditions are satisfied:*

$$
\begin{gathered}
\forall \text{ prime } p \equiv 1 \pmod 4,\ p|\gamma\ (\tfrac{d_0}{p}) = (\tfrac{d_1}{p}) = (\tfrac{d_2/c}{p}) = 1 \\
\forall \text{ prime } p \equiv 1 \pmod 4,\ p|d_0 \text{ or } d_1 \text{ or } d_2/c\ (\tfrac{c}{p}) = 1 \\
\text{If } \tau_3(\gamma) = 0, \text{ then } \forall p_1, p_2 \equiv 3 \pmod 4,\ p_1, p_2 | b_2\ (\tfrac{c}{p_1}) = (\tfrac{c}{p_2}) \\
\text{If } \tau_3(\gamma) = \tau_3(b_2), \text{ then } \forall p_1, p_2 \equiv 3 \pmod 4,\ p_1, p_2 | b_2 \\
(\tfrac{d_0}{p_1}) = (\tfrac{d_0}{p_2}),\ (\tfrac{d_1}{p_1}) = (\tfrac{d_1}{p_2}),\ (\tfrac{d_2/c}{p_1}) = (\tfrac{d_2/c}{p_2}) \\
\text{If } 0 < \tau_3(\gamma) < \tau_3(b_2), \text{ then } \forall p \equiv 3 \pmod 4,\ p|\gamma\ (\tfrac{d_0}{p}) = (\tfrac{d_1}{p}) = 1 \\
\text{and } \forall p_1, p_2, p_3, p_4 \equiv 3 \pmod 4\ p_1, p_2 | (b_2/\gamma), p_3, p_4 | \gamma \\
(\tfrac{c}{p_1}) = (\tfrac{c}{p_2}) = -(\tfrac{d_2/c}{p_3}) = -(\tfrac{d_2/c}{p_4})
\end{gathered}
\tag{3.12}
$$

If such c exists, the only non-trivial m-subunoid of U_K has the base $X' \subset X$ (so (2.9) may

potentially hold only for $\Sigma = X'$) and a section equal to c on X', where $X' = X \setminus \{b_2\}$ if $b_2 \in X, c = b_2, X = X'$ otherwise. If such c does not exists, then $t_K = 0$.

Proof: Note that the product (in SF) of elements of X is equal to 1, so the product of the elements of any triple $\subset X$ is equal to the remaining element of X. This proves, in particular, that any triple $\subset X$ is a basis of V and $b_2 = m.c.d$ of elements of a triple $\subset X$. Taking this, that $W_+ = W_{+o}$ (by the above), consequence 3.3 and proposition 3.8 into account , we need only show that the divisor $\sqrt{c}$, where c is described in proposition 3.27 before (3.12), $\forall d \in X$ is orthogonal to Δ_d under the pairing $(,)$ corresponding to the field $k = \mathbb{Q}(\sqrt{d})$, what is equivalent that $c \in C_k(\varepsilon_d)$ under the ramified divisors condition for k (see above).

Let us in the following proof denote by $(,)_d$ the pairing $(,)$ associated to the field $\mathbb{Q}(\sqrt{d})$. In general Δ_d is generated by primes $\equiv 1 \pmod 4$, $p|d$ and products $p_1 p_2$, where primes $p_1, p_2 \equiv 3 \pmod 4$, $p_1, p_1|d$. In our case neither such p_1, p_2 may divide d_0 or d_1 , hence p_1, p_2 must divide b_2, if $d \in X$, also d_0, d_1 are coprime to b_2 (see (3.5)). Suppose a prime $p \equiv 1 \pmod 4$ divides γ. Then $p|d$ for all $d \in X$, hence $(\sqrt{c}, p)_d = (\frac{p}{c/p})(\frac{d/p}{p}) = 1 \Leftrightarrow (\frac{d/c}{p}) = 1$, taking into account QRL: quadratic reciprocity law. Because $X = \{d_2, d_0 \cdot d_2, d_1 \cdot d_2, d_0 \cdot d_1 \cdot d_2\}$, these conditions hold iff $(\frac{d_0}{p}) = (\frac{d_1}{p}) = (\frac{d_2/c}{p}) = 1$ for such p. Suppose prime $p \equiv 1 \pmod 4$ does not divide γ, but p divides some $d \in X$, that is $p|d_0$ or d_1 or (d_2/c).

Then $(\sqrt{c}, p)_d = (\frac{p}{c}) = 1 \Leftrightarrow (\frac{c}{p}) = 1$ by QRL. Let primes $p_1, p_2 \equiv 3 \pmod 4$ divide b_2/γ,

then for $d \in X$ $(\sqrt{c}, p_1p_2)_d = (\frac{p_1p_2}{c}) = 1 \Leftrightarrow (\frac{c}{p_1}) = (\frac{c}{p_2})$ by QRL.

Let primes $p_1, p_2 \equiv 3 \pmod 4$ divide γ. Then for $d \in X$,

$(\sqrt{c}, p_1p_2)_d = (\frac{p_1}{c/p_1})(\frac{d/p_1}{p_1})(\frac{p_2}{c/p_2})(\frac{d/p_2}{p_2}) = 1 \Leftrightarrow (\frac{d/c}{p_1}) = (\frac{d/c}{p_2})$ by QRL.

By the same reason as above, these conditions are equivalent that

$(\frac{d_2/c}{p_1}) = (\frac{d_2/c}{p_2}), (\frac{d_0}{p_1}) = (\frac{d_0}{p_2}), (\frac{d_1}{p_1}) = (\frac{d_2}{p_2})$

Suppose primes $p_1 \equiv 3$ (mod) divides b_2/γ, prime $p_2 \equiv 3 \pmod 4$ divides γ , so $0 < \tau_3(\gamma) < \tau_3(b_2)$. Then for $d \in X$ $(\sqrt{c}, p_1p_2)_d = (\frac{p_1}{c})(\frac{p_2}{c/p_2})(\frac{d/p_2}{p_2}) = 1 \Leftrightarrow (\frac{c}{p_1}) = -(\frac{d/c}{p_2})$ by QRL.

Again, this is equivalent that $(\frac{d_0}{p_2}) = (\frac{d_1}{p_2}) = 1$ and $(\frac{d_2/c}{p_2}) = -(\frac{c}{p_1})$. The proposition 3.27 is proved.

Let b_2 is fixed, $N =$ the number of prime divisors of $2b_2$. Let $Y =$ the set of primes dividing d_0 or d_1 (recall that all such primes $\equiv 1 \pmod 4$ and coprime to $2b_2$). Let us vary Y, supposing $|Y| = M$ is fixed. Let $Z = (\mathbb{Z}/2\mathbb{Z})^N$ and S be a hyperplane in Z. Then (3.12) implies that for $t_K = 1$ it is necessary that $\exists S$ (namely $S = \sum_{\text{primes } q|\gamma} x_q = 0$) such that $\forall p \in Y$ $((\frac{q}{p})', q|2b_2) \in S)$. This implies that the image of Y in Z^M (after ordering the set Y) must be contained in $T = \bigcup_S S^M \subset Z^M$. Taking into account that the density of the sets Y having fixed image in Z^M is equal to $1/|Z^M|$, we conclude that the density of sets Y such that (3.12) (even a part of it) holds for some K with V generated by $d_0, d_1, d_2 = b_2$, $Y(d_1, d_2) = Y$, is not greater than

$|T|/|Z^M| \leq min((2^N-1)(|Z|/2)^M/|Z^M|,1) \leq min(\frac{1}{2^{M-N}},1)$

which rapidly goes to 0 if $M \to \infty$.

This confirms, with more close watching the special cases of unoids U_K, rather than abstract unoids , the suggestion that the proportion of cases when $t_K > 0$ decreases rapidly when $\tau(W)$ = the number of primes dividing at least one element of W grows (the ramified divisors condition would not interfere significantly with this tendency, however its effect has to be taken into account for ultimate analysis). Respectively, say in the case $|W_1| = 3, W_{+o} = W \setminus W_1$, frequently $t_K = 0$, what means the full determination (see chapter 4) of r_K according to the approach in our work.

Chapter 4

Upper bounds for 2^n-rank of Cl_K and computation of it in certain cases

4.1 Genus theory and the 2-elementary condition

Let $1 \neq d \in SF$, $k = \mathbb{Q}(\sqrt{d})$-real quadratic extension of $\mathbb{Q}$. Let $Cl_{k,st}$ is the group of classes of strictly equivalent divisors of k: a is strictly equivalent to b if $a/b = (x)$, where $x \in k^*$ and $x > 0, x^\sigma > 0$, where σ is a generator of $Gal(k/\mathbb{Q})$.

The natural surjection $s : Cl_{k,st} \mapsto Cl_k$ is isomorphism iff $N(\varepsilon_d) = -1$, where ε_d is a fundamental unit of k, otherwise $ker(s) \tilde{\to} \mathbb{Z}/2\mathbb{Z}$. The important result of the genus theory is that $Cl_{k,st}/Cl_{k,st}^2 \tilde{\to} (\mathbb{Z}/2\mathbb{Z})^{m_d}$, where $m_d =$ #(of prime divisors of $D(k)$)-1 (see [4], Ch 3, Sec 8, Theorem 8).

Let $\Delta_{d,st}$ be the subgroup of k^*/k^{*2} of all elements x such that $k(\sqrt{x})$ is unramified extension of k. By Kummer duality the group $\Delta_{d,st}$ is dual to $G(k^{unr,2}/k)$ where $k^{unr,2}$ is the maximal 2-periodic abelian unramified extension of k. On the other hand, the reciprocity

map θ of the class field theory induces isomorphism $\theta : Cl_{k,st}/Cl_{k,st}^2 \xrightarrow{\sim} G(k^{unr,2}/k)$.

Combining Kummer duality and the isomorphism θ we obtain a non-degenerate pairing $(,) : Cl_{k,st}/Cl_{k,st}^2 \times \Delta_{k,st} \to \mu_2$ where $(a,x) = \prod_{\substack{\text{nonarch } v \\ v(a) \text{ is odd}}} (a,x)_v$, where $(,)_v$ is the quadratic Hilbert symbol for $k_v^*/(k_v^*)^2$.

Let for an odd prime $p|d$ $e(p) = p$, if $p \equiv 1 \pmod 4$, $e(p) = -p$ if $p \equiv 3 \pmod 4$

Proposition 4.1. *The group $\Delta_{d,st}$ is generated by $e(p)$, where p runs through odd prime divisors of d.*

proof: Let for a natural N $B_N = \sum_{\text{prime } p|N} \mathbb{Z}/2\mathbb{Z}\mathrm{v}(p)$- a $\mathbb{Z}/2\mathbb{Z}$ vector space with basis $\{\mathrm{v}(p)\}$. Note that $e(p) \in \Delta_{d,st}$, really $k(\sqrt{e(p)})$ is unramified over k at any prime divisor of k coprime to 2, it is also unramified at $w|2$, because $e(p) \equiv 1 \pmod 4$: then $e(p)/5 \equiv 1 \pmod 8$ and belongs to $(\mathbb{Q}^*)^2$, it is known that $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified.

So we have the homomorphism $h_{d,1} : B_{d_{\text{odd}}} \to \Delta_{d,st}$, $h_{d,1}(p) =$ the coset of $e(p)$, where $d_{odd} = d, d/2$ when d is odd, even respectively.

Now for odd $\delta|d$ $h_{d,1}(\sum_{\text{odd } p|d} ord_p(\delta)\mathrm{v}(p)) = e(\delta) \pmod{(k^*)^2}$, where $e(\delta) = \pm\delta, e(\delta) \equiv 1 \pmod 4$.

To have $e(\delta) \in (k^*)^2$ it is necessary that $e(\delta) = 1$ or d, because $k = \mathbb{Q}(\sqrt{d})$, both $e(\delta)$ and d are square-free. So if $d \equiv 2,3 \pmod 4$, then $e(\delta) = 1 \Rightarrow \delta = 1$, if $d \equiv 1 \pmod 4$ then $\delta = 1$ or d. In all cases, $dim(B_{d_{\text{odd}}}/ker(h_{d,1}) = m_d$, so $h_{d,1}$ is a surjection.

The group Cl_k/Cl_k^2 being the factor group of $Cl_{k,st}/Cl_{k,st}^2$ corresponds to the subextension

of $k^{unr,2}$ in which the archimedian primes of k split, so the subgroup Δ_d of $\Delta_{d,st}$ dual to Cl_k/Cl_k^2 is the kernel of the mapping $\Delta_{d,st} \to \mu_2 \times \mu_2 : x \mapsto (sgn(x), sgn(x^\sigma))$. Hence Δ_d consists of $e(\delta)(\text{mod } k^{*2})$, such that $\delta | d_{odd}, e(\delta) > 0$. Let $q(d)$ be a fixed prime dividing d, $q(d) = 2$ if d is even. Let $d' = d/q(d)$

Let p_d be a fixed prime $\equiv 3 \pmod 4$ dividing d', d when $d \equiv 1{,}2 \pmod 4$, $d \equiv 3 \pmod 4$ respectively, if such primes exist, otherwise let $p_d = 1$. Let $d'' = d'/p_d, d/p_d$ when $d \equiv 1{,}2 \pmod 4$, $d \equiv 3 \pmod 4$ respectively.

Define the homomorphism $h_{d,2} : B_{d''} \to \Delta_d$ as follows: $h_{d,2}(\mathrm{v}(p)) = p \pmod{(k^*)^2}$ if $p \equiv 1 \pmod 4$, = $pp_d \pmod{(k^*)^2}$, if $p \equiv 3 \pmod 4$.

Proposition 4.2. *The homomorphism $h_{d,2}$ is an isomorphism*

proof: It follows from the above that $\Delta_{k,st}$ is generated by $e(p)$ when $p|d'$, if $d \equiv 1{,}2 \pmod 4$, by $e(p)$ when $p|d$ $p \equiv 3 \pmod 4$. Let $x = \prod_{p\equiv 1(4)} p \prod_{p\equiv 3(4)} (pp_d) e(p_d)$. Then $x > 0 \Leftrightarrow x = \prod_{p\equiv 1(4)} p \prod_{p\equiv 3(4)} (pp_d)$, hence $h_{d,2}$ is surjective.

$h_{d,2}$ is also injective, because if $y \in B_{d''}$, $\mathrm{v}(p)$-coordinate of y is not zero ,where $p|d''$, then $h_{d,2}(y) = \delta \pmod{(k^*)^2}$, where $\delta \in \mathbb{N}, \delta \equiv 1 \pmod 4$, $p|\delta$, $\delta | d'; \delta | d$ if $d \equiv 1$,2 $\pmod 4$, $d \equiv 3 \pmod 4$ respectively. Hence $\delta \neq 1, d$ and δ ($\text{mod } (k^*)^2) \neq 1$.

Let $d''' = d'$ if $d \equiv 1,\ 2 \pmod 4$, $d''' = d'2$ if $d \equiv 3(4)$. We have a homomorphism $h_{d,3} : B_{d'''} \to Cl_{k,2}$, $h_{d,3}(\mathrm{v}(p))$ = the divisor class of $\sqrt{p}$ (the divisors of d''' ramify in k).

Then $h_{d,3}(B_{d'''})$ is the subgroup of $Cl_{k,2}$, generated by the ramified divisors (the divisor class of $\sqrt{q}$ is equivalent to the divisor class $\sqrt{d/q} = \sqrt{d'}$).

We define the pairing $(,) : B_{d'''} \times B_{d''} \to \mathbb{Z}/2\mathbb{Z}$ as $(y,x) = (h_{d,3}(y), h_{d,2}(x))'$, where $1' = 0, (-1)' = 1$ (mod 2). Note that $dim(B_{d'''}) = m_d$, while $n_d = dim(B_{d''}) = m_d$ if $d \equiv 1$, 2 (mod 4) and d' is not divisible by $p \equiv 3(4)$, otherwise $n_d = m_d - 1$.

The proposition 4.1 implies:

Consequence 4.1. *$Cl_{k,2} \xrightarrow{\sim} Cl_k/Cl_k^2 \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^{n_d}$. The 2-elementary condition for k that $Cl_{k,2^\infty} = Cl_{k,2}$ is equivalent to the condition that $Cl_{k,2^\infty} \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^{n_d}$ and is equivalent to the condition that $ord_2(h_d) = n_d$, where $h_d = |Cl_k|$- the class number of the field k.*

Let M^d be the matrix $(m^d_{p,q} = (\mathrm{v}(q), \mathrm{v}(p)), q|d''', p|d'')$ where explicitly:

$$\begin{aligned} m^d_{p,q} &= (\frac{p}{q})', \text{ if p} \equiv 1(\text{mod } 4),\ p \neq q \\ &= (\frac{d/q}{q})', \text{ if p} \equiv 1(\text{mod } 4),\ p = q \\ &= (\frac{pp_d}{q})', \text{ if p} \equiv 3(\text{mod } 4),\ p \neq q, p_d \neq q \\ &= (\frac{d \cdot p \cdot p_d}{q})', \text{ if p} \equiv 3(\text{mod } 4), \text{one of } p, p_d \text{ is } q. \end{aligned} \tag{4.1}$$

Here, $(\frac{a}{q})$ with $(a,q) = 1$ is the Legendre symbol, if $q = 2$, $a \equiv 1$ (mod 4) then $(\frac{a}{2}) = 1$ if $a \equiv 1$ (mod 8), $= -1$ if $a \not\equiv 1$ (mod 8).

In the case where $m_d = 0 (\Rightarrow n_d = 0) \Leftrightarrow d = 2$ or $d \equiv 1 \pmod 4$ is a prime we have $Cl_{k,st}/Cl_{k,st}^2 = 1$ and $N(\varepsilon_d) = -1$. In particular, $Cl_{k,2^\infty} = 1$ and 2-elementary condition for k is satisfied. In the case when $n_d = m_d - 1 = 0 \Leftrightarrow d \equiv 3 \pmod 4$ is a prime , or $d = 2p$, where p is a prime $\equiv 3 \pmod 4$, or $d = pq$ where p, q are distinct primes $\equiv 3 \pmod 4$ $Cl_{k,st}/Cl_{k,st}^2 \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$ while $Cl_k/Cl_k^2 = 1$, so $N(\varepsilon_d) = 1$ and 2-elementary condition again is trivially satisfied. Note that in these cases $C_k(\varepsilon_d) = \{2, 2d\}, \{2, p\}, \{p, q\}$ respectively because there is no room for $C_k(\varepsilon_d)$ to be something else. Suppose now that $n_d \geq 1$. If $n_d = m_d - 1$, prime r divides d''', we denote by M_r^d the minor of the matrix M^d obtained by deleting the r-th column. We say that for k the ramified divisors condition holds if $Cl_{k,rm} =$ the subgroup of $Cl_{k,2}$ generated by the ramified prime divisors of k is the group $Cl_{k,2^\infty}$.

Proposition 4.3. *If d is not divisible by a prime $\equiv 3 \pmod 4$, the ramified divisors condition holds for k iff the 2-elementary condition (that is $Cl_{k,2} = Cl_{k,2^\infty}$) holds for k and a fundamental unit ε_d of k has norm $= -1$. If d is divisible by a prime $\equiv 3 \pmod 4$ (in this case always $N(\varepsilon_d) = 1$, see proposition 2.4), the ramified divisors condition for k is equivalent to the 2-elementary condition for k. If d is not divisible by a prime $\equiv 3 \pmod 4$, then the ramified condition holds for $k \Leftrightarrow det(M^d) \neq 0$. If d is divisible by a prime $\equiv 3 \pmod 4$, then $n_d = m_d - 1$ and the ramified condition holds for $k \Leftrightarrow \exists$ a prime $r | d'''$ such that $det(M_r^d) \neq 0$. In this case the unique $c(d) \in C_k(\varepsilon_d)$ such that $q(d) \not| c(d)$ is equal to the product of all $r | d'''$ such that $det(M_r^d) \neq 0$.*

proof: Note that if we assume that $det(0 \times 0 \text{ matrix }) = 1$ then proposition 4.3 extends to the cases $m_d = 0$ or $n_d = 0$ and is proved taking into account the previous analysis of these cases. In general, $dim(Cl_{k,rm}) = m_d$ if $N(\varepsilon_d) = -1$, $= m_d - 1$ if $N(\varepsilon_d) = 1$. In the latter case $\exists!\ c(d) \in C_k(\varepsilon_d)$ such that $q(d) \not| c(d)$, so $\sqrt{c(d)}$ is principal divisor of k.

If d is not divisible by a prime $\equiv 3 \pmod 4$, then $m_d = dim(Cl_k/Cl_k^2) = dim(Cl_{k,2})$, so $Cl_{k,rm} = Cl_{k,2}$ iff $N(\varepsilon_d) = -1$ and the condition $Cl_{k,rm} = Cl_{k,2^\infty}$ is equivalent to the 2-elementary condition $Cl_{k,2} = Cl_{k,2^\infty}$ together with the condition that $N(\varepsilon_d) = -1$.

If d is divisible by a prime $\equiv 3 \pmod 4$, then $N(\varepsilon_d) = 1$ so $dim(Cl_{k,2}) = dim(Cl_k/Cl_k^2) = n_d = m_d - 1 = dim(Cl_{k,rm})$ so $Cl_{k,rm} = Cl_{k,2}$ and, of course, the ramified divisors condition coincides with 2-elementary condition.

Now the ramified divisors condition is equivalent to the condition that $Cl_{k,rm}$ surjects to Cl_k/Cl_k^2 because if it is the case than $Cl_{k,rm} = Cl_{k,2} = Cl_{k,2^\infty}$. Now $Cl_{k,rm}$ surjects to Cl_k/Cl_k^2 iff the pairing $B_{d'''} \times B_{d''}$ has trivial kernel on the right $\Leftrightarrow rank(M^d) = n_d$. If d is divisible by a prime $\equiv 3 \pmod 4$, then $N(\varepsilon_d) = 1, n_d = m_d - 1$. Let $c(d) \in C_k(\varepsilon_d)$,
$q(d) \not| c(d)$. Now a prime $r|d'''$ divides $c(d) \Leftrightarrow \sqrt{q}, q|d''', q \neq r$ generate $Cl_{k,rm}$ what in the case when the ramified divisors condition holds for k is equivalent to the condition that $det(M_r^d) \neq 0$, because the pairing $Cl_{k,rm} \times B_{d''}$ is non degenerate

Proposition 4.4. *Let $d = 2, 3 \pmod 4$, $d \neq 2$. The divisor class of $\sqrt{2}$ is in $Cl_k^2 \Leftrightarrow$ the following condition holds:*

$$\begin{gathered}\exists \text{ a unique } i \in \{3,7\} \text{ such that if the prime } p|d, \\ \text{then either } p \equiv 1 \pmod 8 \text{ or } p \equiv i \pmod 8.\end{gathered} \tag{4.2}$$

The condition (4.2) is necessary for $2 \in C_k(\varepsilon_d)$ *if* $N(\varepsilon_d) = 1$. *If d satisfies to(4.2) and is not divisible by a prime* $\equiv 3 \pmod 4$ *than the ramified divisors condition does not hold for k. If p is divisible by a prime* $\equiv 3 \pmod 4$ *, so* $N(\varepsilon_d) = 1$*, and the ramified condition holds for k, than the condition (4.2) is sufficient and necessary for* $2 \in C_k(\varepsilon_d)$

proof: The divisor class of $\sqrt{2}$ is in $Cl_k^2 \Leftrightarrow \sqrt{2}$ is orthogonal to $\Delta_d \Leftrightarrow$ (by the proposition 4.1) $\sqrt{2}$ is orthogonal to p, pp_d where $p|d'', p \equiv 1,3 \pmod 4$ respectively. This is exactly the property (4.2) because $(\sqrt{2}, \delta) = (\frac{\delta}{2})$ for $\delta \equiv 1 \pmod 4$.

If d is not divisible by a prime $\equiv 3 \pmod 4$ and the ramified divisors condition holds for k we know that $N(\varepsilon_d) = -1$ and if (4.2) holds than the divisor class of $\sqrt{2} \in Cl_k = 1 \Rightarrow \exists$ a unit $\varepsilon > 0$ of k with $2 \in C_k(\varepsilon)$ so $C_k(\varepsilon) \neq \{1, d\}$- contradiction. If d is divisible by a prime $\equiv 3 \pmod 4$ and if the ramified divisors condition holds for k than (4.2)$\Rightarrow \sqrt{2}$ is principal $\Rightarrow 2 \in C_k(\varepsilon_d)$.

4.2 The explicit matrix $\mathbb{J}$, upper bounds for r_K, its complete determination in the case when $S(K) = S_0(K)$.

Suppose that the ramified divisors condition holds for k, that is, according to the proposition 4.3, $det(M^d) \neq 0$, $det(M_r^d) \neq 0$, when d is not divisible by a prime $\equiv 3 \pmod 4$, is divisible by such a prime respectively. In the latter case we fix $r_d | d'''$ such that $det(M_{r_d}^d) \neq 0$, we choose r_d to be 2, if $d \equiv 3 \pmod 4$, and $det(M_2^d) \neq 0$. Let $d'''' = d''', d'''/r_d$, $\mathbb{M}_d = M^d, M_{r_d}^d$ respectively, so we have

$$det(\mathbb{M}_d) \neq 0 \tag{4.3}$$

The homomorphism $h_{d,3}$ restricted to $B_{d''''}$ is an isomorphism of $B_{d''''}$ and $Cl_{k,2}$, we also have isomorphism $h_{d,4} : Cl_{k,2} \xrightarrow{\sim} B_{d''}$, given by $h_{d,4}(a) = \sum_{p|d''}(a, h_{d,2}(\mathrm{v}(p)))\mathrm{v}(p)$. Let $h_{d,5} = h_{d,4} \circ h_{d,3}$ is an isomorphism of $B_{d''''}$ to $B_{d''}$, it is represented by the matrix $\mathbb{M}_d$: $Y = \mathbb{M}_d X$, where X is the column of coordinates of of $x \in B_{d''''}$ and Y is the column of coordinates of $y = h_{d,5}(x)$. The inverse isomorphism $h_{d,6} : B_{d''} \xrightarrow{\sim} B_{d''''}$ is represented by the matrix $\mathbb{G}_d = \mathbb{M}_d^{-1} = (g_{q,p}^d$, primes $q | d''''$, primes $p | d'')$. where

$$g^d_{q,p} = det(\mathbb{M}_{d;p,q}) \tag{4.4}$$

where $\mathbb{M}_{d;p,q}$ is the minor of the matrix $\mathbb{M}_d$ obtained by deleting p-th row and q-th column. (in practical computation of det it is enough to order primes q and to order primes p to get standard matrix with entries indexed by $(i,j)1 \leq i,j \leq n_d$). We have

$$h_{d,3} \circ h_{d,6} \circ h_{d,4} = id \text{ on } Cl_{k,2} \tag{4.5}$$

Really, by the definition of $h_{d,6}$ $h_{d,6} \circ h_{d,4} \circ h_{d,3} = id$ on $B_{d''}$. Hence $h_{d,3} \circ h_{d,6} \circ h_{d,4} \circ h_{d,3} = h_{d,3}$ what implies (4.5) because $h_{d,3}$ is isomorphism

We recall that for $\Sigma \subset W$ the set $T(W)$ is the set of all primes $q|\exists d \in W, q|d$. And $H_q = \{d \in W | q \not| d\}$. Let $W_{n-1} = W, q_{n-1}$ be any prime in $T(W_{n-1})$ (here $n = dim(V) = [K/\mathbb{Q}]$). Suppose we have the sequences of sets W_i and primes $q_i \in T(W_i), 0 \leq t \leq i \leq n-1$, such that $W_{n-1} = W, W_i = H_{q_{i+1}} \cap W_{i+1}$ for $t \leq i \leq n-2$, $W_i \cup \{1\}$ is a subspace of V of dimension $i+1, t \leq i \leq n-1$.

Then we can extend such sequences by $W_{t-1} = H_{q_t} \cap W_t$, which by the proposition 3.3 is a

p-hyperplane of W_t, so $dim(W_{t-1} \cup \{1\}) = t$, and taking q_{t-1} to be any prime in $T(W_{t-1})$. So starting with any $q_{n-1} \in T(W)$, $W_{n-1} = W$ we can build as described above for $0 \leq i \leq n-1$ sequences of p-subspaces W_i of W of dimension $i+1$, and primes $q_i \in T(W_i)$, $W_{n-1} = W$, $W_{i-1} = H_{q_i} \cap W_i$ if $1 \leq i \leq n-1$. We will call such sequences an admissible collection for W.

Proposition 4.5. *Let $\{q_i, W_i\}$ be an admissible collection for W. Then $\exists$ a basis $\{d_i, 0 \leq i \leq n-1\}$ of V such that $q_i | d_i, q_i \not| d_j$ if $i \neq j$.*

proof: We will prove by induction on $n = dim(V)$. If $n = 1$ we are done taking $d_o \in W$ be the unique element of W. Suppose the proposition 4.5 is proved for $n \leq N$. Let $dim(V) = N+1$. Let $\{W_i\}, \{q_i\}$ $0 \leq i \leq N\}$ be an admissible collection for W.

Then $\{W_i\}, \{q_i\}$, $0 \leq i \leq N-1$ is an admissible collection for W_{N-1} and $dim(V') = N$, where $V' = W_{N-1} \cup \{1\}$. Let $\{d_i, 0 \leq i \leq N-1\}$ be a basis of V' such that $q_i | d_i, q_i \not| d_j$ if $0 \leq i \neq j \leq N-1$, existing by the induction hypothesis. Let d be any element of W such that $q_N | d$. Let $I = \{0 \leq i \leq N-1 | q_i | d\}$. Let $d_N = d \prod_{i \in I} q_i$ (the product is in SF). We claim that $\{d_i, 0 \leq i \leq N\}$ satisfies the requirements of proposition 4.5 . For $q_N \not| d_i$ if $0 \leq i \leq N-1$ because then $d_i \in W_i \subset W_{N-1} = H_{q_N} \cap W$ and obviously $q_i \not| d_N$ for $0 \leq i \leq N-1$ because the primes q_i, $0 \leq i \leq N$ are distinct: if $i < j$ $q_i \in W_i \subset W_j = H_{q_j} \cap W_j$. Also $q_N | d_N$.

In the following we choose primes q_i and a basis $\{d_i\}$ as in proposition 4.5, supposing that $q_{n-1} = 2$ if $2 \in T(W)$. For $d \in W$ we set $q(d) = 2$ if $2 | d$, otherwise $q(d) = q_t$, where

$t = max(i : q_i|d)$. In particular $q(d_i) = q_i$, $0 \leq i \leq n-1$. We recall that $d' = d/q(d)$, Let $D' =$ the product of all primes in $T(W)$ distinct from q_i, $0 \leq i \leq n-1$. So if $\tau(W) =$ the cardinality of $T(W)$, then D' is the product of $m = m_K = \tau(W) - n$ distinct primes. We define a homomorphism $\beta : A \to B_{D'}$ (see the definition of A in section 1.2) as follows:

$$\beta(\ell) = \sum_{q|D'} (\frac{q}{\ell})' \mathrm{v}(q) \tag{4.6}$$

Let $q|D', \ell(q)$ be an odd prime which splits in K and such that if a prime $q'|D'$, then $(\frac{q'}{\ell(q)}) = -1$ if $q = q'$, = 1 if $q \neq q'$. So $\beta(\ell(q)) = \mathrm{v}(q)$. Let us compute the element $x = (h_{d,4} \circ \alpha_d)(\ell(q)) \in B_{d''}$, where $\alpha_d(\ell) \in Cl_{(d),2}$ is the projection of ℓ_k in $Cl_{(d),2} = Cl_{k,2}$, where $k = \mathbb{Q}(\sqrt{d})$, and ℓ_k is a prime divisor of k dividing ℓ ($\alpha_d(\ell)$ does not depend on the choice of ℓ). If $p|d''$, then p-th coordinate of x is equal to $(\frac{p}{\ell(q)})'$, if $p \equiv 1 \pmod 4$, and is equal to $(\frac{pp_d}{\ell(q)})'$ if $p \equiv 3 \pmod 4$. Hence it is equal to

$$e^d_{p,q} = \begin{matrix} \xi(p,q), \text{ if } p \equiv 1 \pmod 4 \\ \xi(p,q) + \xi(p_d,q) \text{ if } p \equiv 3 \pmod 4 \end{matrix} \tag{4.7}$$

Here $\xi(p,q) = 1$ if $p = q$ or $p = q_i$ and $q|d'_i$, otherwise $\xi(p,q) = 0$. So if we define a linear mapping $\pi_d : B_{D'} \to B_{d''}$ to be represented by $n_d \times m$ matrix

$\mathbb{E}_d = \{e^d_{p,q}$, primes $p|d''$, primes $q|D'\}$, then $\phi_d(\ell(q)) = \pi_d(\beta(\ell(q)))$, where $\phi_d = h_{d,4} \circ \alpha_d$. Suppose $\ell(q)$ exists for any $q|D'$, Then $\ell(q)$ generate $A/ker(\phi_d)$ because $(\frac{p}{\ell})' = \sum_{q|D'}(\frac{q}{\ell})'(\frac{p}{\ell(q)})'$ for every odd prime $p \in T(W)$: if $p|D'$ this follows from the definition of $\ell(q)$, if $p = q_i$, $0 \le i \le n-1$, then $(\frac{d_i}{\ell}) = 1 \Rightarrow (\frac{p}{\ell}) = (\frac{d_i/p}{\ell})$. Hence $\phi_d(\ell) = \phi_d(y)$, where $y = \prod_{q|D'} \ell(q)^{i(q)}, i(q) = (\frac{q}{\ell})'$.

Proposition 4.6. *The linear mapping β is surjective and*

$$h_{d,4} \circ \alpha_d = \pi_d \circ \beta \tag{4.8}$$

proof: We need only prove the existence of $\ell(q)$. By Dirichlet's theorem about primes in arithmetic progressions, there exists a prime $\ell \equiv 1 \pmod 4$ and if $q'|D'$ then $(\frac{\ell}{q'})' = \delta_q^{q'}($ mod 2), and $(\frac{\ell}{q_i})' = \sum_{q'|d'_i} \delta_q^{q'}$. Taking into account that for prime $q \neq \ell$ $(\frac{q}{\ell}) = (\frac{\ell}{q})$ by the quadratic reciprocity law, we are done: ℓ has all properties of $\ell(q)$ ($(\frac{d_i}{\ell}) = 1 \; \forall 0 \le i \le n-1$ implies that $(\frac{d}{\ell}) = 1 \; \forall d \in W$ because $\{d_i\}$ is a basis of V).

Let $D'' = 2D'$, if all $d \in W$ are odd and $\exists d \in W, d \equiv 3 \pmod 4$, otherwise let $D'' = D'$. If δ, N are natural numbers $\mathrm{v}(\delta) \in B_N$, $\mathrm{v}(\delta) \stackrel{def}{=} \sum_{p|N} ord_p(\delta)\mathrm{v}(p)$. Let $\gamma' : B_{D''} \to Cl_{K,2}, \gamma'(\mathrm{v}(\delta)) =$ the divisor class of $\sqrt{\delta}$, where $\delta|D''$ (note that all primes dividing D'' are ramified in K).

Let $\pi^d : B_{d''''} \to B_{D''}$ be the linear mapping such that for a prime $q|d''''$ $\pi^d(\mathrm{v}(q)) = \mathrm{v}(q)$ if $q \neq q_i, 0 \leq i \leq n-1$, $\pi^d(\mathrm{v}(q)) = \mathrm{v}(d_i/q_i)$, if $q = q_i$.

We have:

$$\psi_{d,2} \circ h_{d,3} = \gamma' \circ \pi^d \tag{4.9}$$

where $\psi_{d,2} : Cl_{(d),2} \to Cl_{K,2}$ is induced by the inclusion $k = \mathbb{Q}(\sqrt{d}) \hookrightarrow K$

π^d is represented by $m' \times n_d$ matrix $\mathbb{F}_d = \{f^d_{p,q},$ primes $p|D'',$ primes $q|d''''\}$, where $m' = m$, if $D'' = D'$, $m' = m+1$ if $D'' = 2D'$,

$$f^d_{p,q} = \begin{array}{c} \delta^q_p, \text{ if } q \neq q_i, 0 \leq i \leq n-1 \\ 1, \text{ if } q = q_i, p|d'_i \\ 0, \text{ if } q = q_i, p \not| d'_i \end{array} \tag{4.10}$$

Let $J_d : B_{D'} \to B_{D''}$ be the linear mapping $\pi^d \circ h_{d,6} \circ \pi_d$ represented by the $m' \times m$ matrix

$$\mathbb{J}_d = \mathbb{F}_d \mathbb{G}_d \mathbb{E}_d \tag{4.11}$$

Let $\alpha_d : A \to Cl_{(d),2}$ be the d component of the homomorphism α, defined in section 1.2.

Proposition 4.7. $\gamma' \circ J_d \circ \beta = \psi_{d,2} \circ \alpha_d$

proof: Taking into account (4.5) (4.8) and (4.9) we have

$\psi_{d,2} \circ \alpha_d = \psi_{d,2} \circ h_{d,3} \circ h_{d,6} \circ h_{d,4} \circ \alpha_d = \gamma' \circ \pi^d \circ h_{d,6} \circ \pi_d \circ \beta = \gamma' \circ J_d \circ \beta.$

We recall that R is the subgroup in SF generated by the primes ramified in K, that is the primes dividing the product of the discriminants of the quadratic subfields in K. It follows from the previous definitions that this set of primes is the disjoint union of the set of prime divisors of D'' and the set $\{q_i, 0 \leq i \leq n-1\}$.

Proposition 4.8. *Let $x \in R/V$. There exists a unique representative $\delta(x) \in R$ such that $\delta(x)|D''$.*

proof: Let $y \in R$ be a representative of x. Then $\delta(x) = (y \cdot \prod_{q_i|y} d_i)|D''$ (the product in SF) . Let $d \in V, d|D''$. Then d is odd, otherwise $D'' = D'$ is odd so even d cannot divide D''. So $d|D'$. If $d \neq 1$, then $q_i = q(d)$ divides d but $q_i \not| D'$. So $d = 1$ and this proves uniqueness. If we define $R'' \subset R$ as the group generated by prime divisors of D'', then it follows from the proposition 4.8 that R is the direct sum of R'' and V (as a vector space over $\mathbb{Z}/2\mathbb{Z}$) and $\delta : R/V \to R''$ is the isomorphism induced by the projection of R to R''. Let $\omega : R/V \xrightarrow{\sim} B_{D''}$ be the isomorphism v $\circ \delta$. The homomorphism $\gamma : R/V \xrightarrow{\sim} Cl_{K,2}$ (see its definition in the section 2.1) is equal to $\gamma' \circ \omega$ and by proposition 2.2 $ker(\gamma) = Im(\eta)$, where $\eta : S(K) \to R/V$, $\eta(\varepsilon) =$ the coset $C_K(\varepsilon)$. Hence if we define $\eta' = \omega \circ \eta : S(K) \to$

$B_{D''}$, then

$$ker(\gamma') = Im(\eta') \tag{4.12}$$

Note that $\eta'(\varepsilon) = \mathrm{v}(c)$, where $c \in C_K(\varepsilon)$ is unique such that $c|D''$ ($\Leftrightarrow q_i \not| c, 0 \leq i \leq n-1$).

Let $J : B_{D'} \to B_{D''}, J = \sum_{d \in W} J_d$ where $W' = \{d \in W, n_d > 0\}$, so J is represented by the $m' \times m$ matrix

$$\mathbb{J} = \sum_{d \in W'} \mathbb{J}_d \tag{4.13}$$

Let $\mathbb{L} \subset B_{D''}, \mathbb{L} = Im(J)$. $\mathbb{U} = \mathbb{L} \cap \eta'(S(K))$.

We are ready to prove summarizing

Proposition 4.9. *Suppose that the ramified divisors condition holds for K. Then*

$$r_K = 2^n\text{- rank of } Cl_K = dim(\mathbb{L}/\mathbb{U}) \tag{4.14}$$

proof: By the proposition 1.4 $r_k = dim(Im(\rho))$ where $\rho = \psi_2 \circ \alpha$. $Im(\rho) = Im(\sum_{d\in W} \psi_{d,2} \circ \alpha_d) = Im(\sum_{d\in W'} \psi_{d,2} \circ \alpha_d)$ because if $n_d = 0$, then $Cl_{d,2} = 0$, $\psi_{d,2} = 0$. Taking into account the proposition 4.7, we have that $Im(\rho) = Im(\gamma' \circ J)$, because β is surjective by the proposition 4.6. (4.11) implies that $\gamma' : Im(J) \to Cl_{K,2}$ has the kernel = $\mathbb{U}$, so γ' induces isomorphism of $\mathbb{L}/\mathbb{U}$ to $Im(\gamma' \circ J)$.

Let $\mathbb{U}_0 = \mathbb{L} \cap \eta'(S_0(K)) \subset \mathbb{U}$.

$$r_K^{++} = rank(\mathbb{J}) = dim(\mathbb{L}) \tag{4.15}$$

$$r_K^{+} = dim(\mathbb{L}/\mathbb{U}_0) \tag{4.16}$$

Then

$$r_K \leq r_K^+ \leq r_K^{++} \tag{4.17}$$

and $r_k^{++} \geq r_K^+$ appear (under the ramified divisors condition for K) as upper bounds for r_K, explicitly determined and computable in result of our study.

The checking of the ramified divisors condition for $k = \mathbb{Q}(\sqrt{d}) \subset K$, namely that $det(M^d) \neq 0$ or $det(M_r^d) \neq 0$ (see the proposition 4.3) and determination of r_K^{++} both require just finding the ranks of explicit matrices which entries are sums of products of factors equal to $(\frac{p}{q})'$ or $(\frac{pr}{q})'$, where p,q,r are odd ramified prmes in K, $p \neq q$, $pr \equiv 1 \pmod 4$, $(\frac{p}{q})$ is the Legendre symbol, $(\frac{\delta}{2}) = 1,-1$ if $\delta \equiv 1{,}5 \pmod 8$ respectively and $1' = 0, (-1)' = 1$. $r_K^+ = r_K^{++} - dim(\mathbb{U}_0)$ and $\mathbb{U}_0 \subset B_{D''}$ is generated by $\eta'(c(\varepsilon_d))$, where $d \in W_+$, and $\eta'(c(\varepsilon_\Sigma)), \Sigma \subset W_-, \prod_{d\in\Sigma} d$ is a square. To determine $c(\varepsilon_d), c(\varepsilon_\Sigma)$, one can use (2.3), the proposition 2.7 respectively.

Note that in the case $d \in W_+$, the alternative way to determine $c(\varepsilon_d)$, also solely dependable on values of Legendre symbols, described above, is given by the proposition 4.3. Determination of $c(\varepsilon_\Sigma)$, as described in proposition 2.7, requires to work with the Gaussian integers.

We recall that if $n = 2$, then $\mathbb{U} = \mathbb{U}_0$(because $S(K) = S_0(K)$), so $r_K = r_K^+$ is completely

determined (it was done in [1] except for the case when $W = W_-$, where r_K was determined up to an error≤ 1)

We recall that m =(the number of primes dividing at least one element of W) - n. We have the inequality

$$r_K^{++} \leq m \tag{4.18}$$

because $r_K^{++} = rank(\mathbb{J})$, where J is $m' \times m$ matrix. The purpose of the next proposition is slightly improve (4.18) in certain cases. Let $\tau_3(d) =$ the number of primes $\equiv 3 \pmod 4$ dividing d.

Proposition 4.10. $\mathbb{K} = \bigcap_{d \in W} \ker(\pi_d) \neq 0 \Leftrightarrow \tau_3(d_i)$ *are even for odd* d_i *(in particular , if* $0 \leq i \leq n-2$*) and* $\exists$ *a prime* $\equiv 3$ *(mod 4)*$\subset T(W)$. *In this case the only* $0 \neq x \in \mathbb{K}$ *is* $x = \sum_{primes\ q \equiv 3\ (mod\ 4), q|D'} v(q)$.

Consequence 4.2.

$$r_K \leq r_K^{++} \leq m - e \tag{4.19}$$

where $e = 1$, if any odd $d \in W$ is divisible by an even number of primes $\equiv 3 \pmod 4$ and $\exists$ a prime $\equiv 3 \pmod 4$ dividing at least one of the $d \in W$, $e = 0$ otherwise.

Note that the condition in consequence 4.2 is equivalent to the corresponding condition in the proposition 4.10 because $\{d_i\}$ is a basis of V.

Proof of the proposition 4.10: Proposition 4.6 implies that $\mathbb{K} = \beta(\mathbb{K}')$, where $\mathbb{K}' = \bigcap_{d\in W} ker(\alpha_d) \subset A$. Now a $\ell \in \mathbb{K}' \Leftrightarrow \forall a \in \Delta_d, (\ell_k, a) = 1$, where $k = \mathbb{Q}(\sqrt{d})$. Δ_d is generated by q, q_1q_2, where q, q_1, q_2 are odd prime divisors of d, $q \equiv 1 \pmod 4$, $q_1 \equiv q_2 \equiv 3 \pmod 4$, (proposition 4.2). We have $(\ell_k, q) = (\frac{q}{\ell}), (\ell_k, q_1q_2) = (\frac{q_1q_2}{\ell})$. Hence for $\ell \in A$, if $(\frac{q}{\ell}) = 1 \ \forall$ prime $q \equiv 1 \pmod 4 \in T(W)$ and $(\frac{q_1}{\ell}) = (\frac{q_2}{\ell}) = 1 \ \forall$ prime $q_1, q_2 \equiv 3 \pmod 4$ $q_1, q_2 \in T(W)$, then $\ell \in \mathbb{K}'$. If a prime $q \equiv 1 \pmod 4 \in T(W)$, then $q|d$ for some $d \in W$, hence $(\frac{q}{\ell}) = 1$ is necessary for $\ell \in \mathbb{K}'$. Also if $q_1, q_2 \equiv 3 \pmod 4 \in T(W)$ than $\exists d \in T(W)$ such that $q_1|d, q_2|d$. For the sets $H'_{q_i} = \{d \in W : q_i \not| d\}$ are p-hyperplanes in V by the proposition 3.3, so $H'_{q_1} \cup H'_{q_2} \leq 2(2^{n-1} - 1) < 2^n - 1 = |W|$

So the above condition on ℓ is also necessary for $\ell \in \mathbb{K}'$. If $(\frac{\ell}{q}) = 1$ for $q \equiv 3(4), q \in T(W)$, or such q does not exist, then $\beta(\ell) = 0$ if $\ell \in \mathbb{K}'$. Hence the only possible non-zero $x \in \mathbb{K}$ is described in the proposition 4.10. Also the condition $(\frac{d_i}{\ell}) = 1, 0 \leq i \leq n-1$, must hold, hence the conditions in the proposition are necessary. They are also sufficient: let $\ell \in A$ is such that

$$\beta(\ell) = x \tag{4.20}$$

where x is described in the proposition, such that ℓ exists because β is surjective. Then (4.20)$\Rightarrow$ if a prime $q|D'$, $q \equiv 1 \pmod 4$, then $(\frac{q}{\ell}) = 1$, and if $q \equiv 3 \pmod 4$ is a prime dividing D',then $(\frac{q}{\ell}) = -1$. Now if $q_i, 0 \leq i \leq n-1$, is equal to 1 (mod 4), so then $q_i|d_i$, d_i is odd, so $(\frac{d_i}{\ell}) = 1 \Rightarrow (\frac{q_i}{\ell}) = 1$, because d_i/q_i divides D', so $(\frac{d_i/q_i}{\ell}) = (-1)^{\tau_3(d_i)} = 1$. Hence $(\frac{q}{\ell}) = 1 \ \forall q \in T(W), q \equiv 1 \pmod 4$.

Also, if q_i is equal to 3 (mod 4), then,

$(\frac{d_i}{\ell}) = 1 \Rightarrow (\frac{q_i}{\ell}) = (-1)^{\tau_3(d_i)-1} = -1$, so $\forall q \in T(W), q \equiv 3 \pmod 4$, $(\frac{q}{\ell}) = -1$. Hence $\ell \in \mathbb{K}'$ by the above and so $x \in \mathbb{K}$. Let $q \in T(W)$, $q \equiv 3 \pmod 4$, such q exists by the conditions. Then either $q|D'$ or $q = q_i$ and $\exists q' \in T(W), q' \equiv 3 \pmod 4$, $q'|D'$ because $\tau_3(d_i) - 1$ is odd so it is not smaller than 1. We see there is always a prime $\equiv 3 \pmod 4$ dividing D', hence $x \neq 0$.

It follows from the proposition 4.3 that under the ramified divisors condition for $k = \mathbb{Q}(\sqrt{d}), d \in W, d \in W_- \Leftrightarrow d$ is not divisible by a prime $\equiv 3 \pmod 4$. Hence W_- is a p-subspace of V, let $n_- = dim(W_- \cup \{1\}) \leq n$. It was proved in chapter 2 that $S_0(K)$ is generated $(mod \ \prod_k E_k^2)$ by $\varepsilon_d, d \in W_+$ and ε_Σ, $\Sigma \subset W_-, \prod_{d\in\Sigma} d$ is a square, and because of (2.7) the group $S_0(K)/(\prod_k E_k^2)$ has dimension $\leq |W_+| + |W_-| - n_- = 2^n - 1 - n_-$. Hence,

$$dim(\mathbb{U}_0) \leq 2^n - 1 - n_- \tag{4.21}$$

In general, for $n \geq 3$ we have for $dim(S(K)/E_K^2$, the rough bound $2^n - 1$= the rank of E_K (by the Dirichlet's theorem about units of K). Hence for $n \geq 3$

$$r_K - r_K^+ = dim(\mathbb{U}/\mathbb{U}_0) \leq dim(S(K)/(S_0(K)E_K^2)) \leq 2^n - 1 - dim(\mathbb{U}_0) \geq n_- \tag{4.22}$$

We recall that $r_K = r_K^+$, if $n = 2$. In particular, $r_K = r_K^+$ if $n_- = 0, dim(\mathbb{U}_0) = 2^n - 1$.

In general, the estimate (4.22) has to be improved, but

Proposition 4.11. *If the condition in the proposition 2.11 or in the proposition 2.13 for $S(K) = S_0(K)$ is satisfied, then $r_K = r_K^+$.*

In the case $n = 3$ the proposition 2.12 implies

Proposition 4.12. *Let $n = 3$, the ramified divisors condition holds for K, $W = W_-$ ($\Leftrightarrow$ $T(W)$ does not contain primes $\equiv 3$ (mod 4)). If $\exists H \subset W, H = W$ or is a p-hyperplane, such that $c_H \not\subset H \cup \{1\}$, then $r_K = r_K^+$ and $r_K^{++} - r_K^+ \leq 4$ by (4.21). Otherwise, $r_K = r_K^{++}$*

or $r_K = r_K^{++} - 1$

In the case $n = 3$, $W_+ \neq \emptyset$, the work done in chapter 3, which is the joint work with professor V. Kolyvagin, allows to significantly improve (4.22). Namely, according to the proposition 3.2 the group $S(K)/S_0(K)$ injects in the group $ms(U_K)$ which is described in details in the chapter 3. Let $t_K = dim(ms(U_K))$. Let $W_1 = \{d \in W, d \equiv 1 \pmod 4\}$, W_1 is a p-subspace of W, always $|W_1| \geq 1$ (see the section 3.3). According to the proposition 3.24 $t_K \leq 2$ and $t_K \leq 1$ if $|W_1| > 1$. Hence if $n = 3$

$$r_k - r_K^+ \leq 2 \tag{4.23}$$

$$r_K - r_K^+ \leq 1, \text{ if } |W_1| > 1 \tag{4.24}$$

$$r_K = r_K^+, \text{ if } t_K = 0 \tag{4.25}$$

Moreover, in the propositions 3.25, 3.26 the cases when $t_K = 2$ are described explicitly. Also the proposition 3.27 describes explicitly (in terms of the Legendre symbols) when $t_K = 1$ if the ramified divisors condition holds for K and $W_1 = W_-, |W_-| = 3$. In particular, in this case , the condition $t_K = 1$ put strong restraints on W, so $t_K = 0$ in many cases, what

means the complete determination of r_K according to (4.25).

Bibliography

[1] Sime, P.J, On the ideal class group of real quadratic fields. Transactions of the American Math Soc. Vol 347, n 12, (1995), 4855-4876.

[2] Kubota T., Uber den bizyklishcen biquadratischen Zahlkorper, Nagoya Math. J. 10 (1955), 65 - 85.

[3] Herglotz G. Uber einen Dirichletschen Satz, Math Z. 12(1922), 225-261.

[4] Borevich Z.I, Shafarevich I.R, Number Theory, Academic Press, 1966.

[5] Cassels J.W.S, Frohlich A, editors, Algebraic Number Theory, Second edition (2010), London math Soc.

[6] Lang S., Algebraic Number Theory, 2nd ed, Springer - Verlag, 1994.

[7] Hasse H., Number Theory, Springer-Verlag, Berlin-Heidelberg- New York. 1980.

[8] Marcus D. Number Fields, Springer Verlag, New York, Heidelberg and Berlin, 1977.

[9] Janusz G., Algebraic number fields, Academic Press, New York and London, 1973.