

A CAPITULATION PROBLEM AND GREENBERG'S CONJECTURE ON REAL QUADRATIC FIELDS

T. FUKUDA AND K. KOMATSU

ABSTRACT. We give a sufficient condition in order that an ideal of a real quadratic field F capitulates in the cyclotomic \mathbb{Z}_3 -extension of F by using a unit of an intermediate field. Moreover, we give new examples of F 's for which Greenberg's conjecture holds by calculating units of fields of degree 6, 18, 54 and 162.

1. INTRODUCTION

Let p be a prime number, F a totally real number field, F_∞ the cyclotomic \mathbb{Z}_p -extension of F and F_n the n th layer of F_∞/F . Let A_n be the p -part of the ideal class group of F_n . In [1], Greenberg showed the following:

Proposition . *Assume that only one prime of F lies over p and that this prime is totally ramified in F_∞/F . Then the following two statements are equivalent.*

- (1) *Every ideal class of A_0 becomes trivial in A_n for some n .*
- (2) *The order of A_n is bounded as $n \rightarrow \infty$.*

In this paper, we treat the case that F is a real quadratic field and $p = 3$. In §2 we give a sufficient condition for (1) by using a unit in F_n . In §3 we give a method of finding the above unit.

2. THEOREM

We put $\zeta_{3^n} = e^{2\pi\sqrt{-1}/3^n}$ for a positive integer n . Our main purpose of this section is to prove the following theorem which plays a fundamental role in the next section.

Theorem . *Let F be a real quadratic field. Let $F_n = F(\zeta_{3^{n+1}}) \cap \mathbb{R}$, $G(F_n/\mathbb{Q}) = \langle \sigma \rangle$ the Galois group F_n over \mathbb{Q} , ε a fundamental unit of F and A_n the 3-part of the ideal class group of F_n . We assume that 3 divides the class number h_F of F and that 3 does not split in F/\mathbb{Q} . If there exists a unit η of F_n such that $\eta^{1+\sigma}$ is a cube of an element of F_n and that neither η nor $\eta\varepsilon$ nor $\eta\varepsilon^2$ is a cube of an element of F_n , then the natural mapping of A_0 to A_n is not injective.*

Let $F_n^* = F(\zeta_{3^{n+1}})$ and F' be the imaginary quadratic field contained in F_0^* such that $F' \cap \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}$. Let M be the maximal abelian 3-extension of F_0^* unramified outside 3, $X = G(M/F')$ and ρ the complex conjugation. We put

Received by the editor September 26, 1994 and, in revised form, February 11, 1995.
1991 *Mathematics Subject Classification*. Primary 11R30, 11R22, 11Y40.

Key words and phrases. Iwasawa invariants, real quadratic fields, unit groups, computation.

$X^+ = \{x \in X \mid \rho^{-1}x\rho = x\}$. Let M^- be the intermediate field between F_0^* and M corresponding to X^+ . For a real number α , we denote by $\sqrt[3]{\alpha}$ the real number whose cube is α . Even though the following Lemma 2.1 is well known, for completeness we give a proof.

Lemma 2.1. *Let α be an element of F . If $F_0^*(\sqrt[3]{\alpha}) \subset M$, then $F_0^*(\sqrt[3]{\alpha}) \subset M^-$.*

Proof. Let σ be an element of X^+ with $\sqrt[3]{\alpha}^\sigma = \sqrt[3]{\alpha}\zeta$, where ζ is a cubic root of unity. Then we have $\sqrt[3]{\alpha}^{\rho\sigma\rho^{-1}} = (\sqrt[3]{\alpha}\zeta)^{\rho^{-1}} = \sqrt[3]{\alpha}\zeta^{-1} = \sqrt[3]{\alpha}^\sigma = \sqrt[3]{\alpha}\zeta$. Hence we have $\zeta = 1$. This shows $\sqrt[3]{\alpha} \in M^-$. \square

For an ideal \mathfrak{A} of F , we denote by $\bar{\mathfrak{A}}$ the ideal class of F which contains \mathfrak{A} . Let $\bar{\mathfrak{A}}_1, \dots, \bar{\mathfrak{A}}_r$ be a basis of $\{a \in A_0 \mid a^3 = 1\}$, $\mathfrak{A}_i^3 = (\alpha_i)$ and k the intermediate field between F_0^* and M corresponding to $X^3 = \{x^3 \mid x \in X\}$. Then under the assumption that 3 does not split in F/\mathbb{Q} we have by Lemma 2.1 the following result.

Lemma 2.2 (cf. [1, p. 281]). *Let k^- be the field $k \cap M^-$. Then we have $k^- = F_0^*(\sqrt[3]{3}, \sqrt[3]{\varepsilon}, \sqrt[3]{\alpha_1}, \dots, \sqrt[3]{\alpha_r})$.*

The following is well known (cf. [1, p. 280]):

Lemma 2.3. *Let σ be a generator of the Galois group $G(F_n^*/F')$ and α be a non-zero element of F_n^* such that there exists an element β with $\alpha^\sigma = \alpha^{-1}\beta^3$. Then $F_n^*(\sqrt[3]{\alpha})$ is an abelian extension of F' .*

Proof of the Theorem. Since $\eta^{1-\sigma^2} = (\eta^{1+\sigma})^{1-\sigma}$, there exists an element β of F_n with $\eta^{1-\sigma^2} = \beta^3$. Hence we have $N_{F_n/F_0}(\beta^3) = 1$, which means $N_{F_n/F_0}(\beta) = 1$. Hence there exists an element γ of F_n with $\beta = \gamma^{1-\sigma^2}$, which shows $\eta\gamma^{-3} \in F_0$. This shows $F_n^*(\sqrt[3]{\eta}) = F_n^*(\sqrt[3]{\eta\gamma^{-3}}) = F_n^*F_0^*(\sqrt[3]{\eta\gamma^{-3}})$. Since $F_n^*(\sqrt[3]{\eta})$ is an abelian 3-extension of F_0^* unramified outside 3 by Lemma 2.3 and since $\eta\gamma^{-3} \in F_0^*$, we have $F_0^*(\sqrt[3]{\eta\gamma^{-3}}) \subset k^- = F_0^*(\sqrt[3]{3}, \sqrt[3]{\varepsilon}, \sqrt[3]{\alpha_1}, \dots, \sqrt[3]{\alpha_r})$ by Lemmas 2.1 and 2.2. Hence there exist integers n_1, n_2, \dots, n_r, n and an element δ of F_0 with $\eta\gamma^{-3} = \alpha_1^{n_1} \dots \alpha_r^{n_r} \varepsilon^n \delta^3$ by Lemma 2.2. This shows by the assumption on η that $\mathfrak{A}_1^{n_1} \dots \mathfrak{A}_r^{n_r}$ is not principal in F_0 but principal in F_n . \square

3. METHOD OF FINDING η

In this section, we explain how to compute and find a unit η in the theorem. Let E_n be the unit group of F_n and $r = 2 \cdot 3^n - 1$. If a basis $\{\varepsilon_1 E_n^3, \dots, \varepsilon_r E_n^3\}$ of E_n/E_n^3 is obtained, without loss of generality, η can be written in the form $\eta = \varepsilon_1^{e_1} \dots \varepsilon_r^{e_r}$ with $0 \leq e_i \leq 2$. Therefore, we can decide whether or not such an η exists by examining all the combinations of $\{e_1, \dots, e_r\}$. If $n = 1$, we can obtain fundamental units of F_1 (cf. [3]) and can use this direct algorithm. But it is hard to obtain a basis of E_n/E_n^3 for $n \geq 2$. So we proceed as follows.

For an element ξ of F_n , we denote ξ^{σ^i} by ξ_i . Let C_n be the cyclotomic unit group of F_n . First we assume that there exists an element $\xi \in C_n$ such that $C_n = \langle -1, \xi_0, \dots, \xi_{r-1} \rangle$. Moreover, we assume that the 3-Sylow subgroup $(E_n/C_n)_3$ of E_n/C_n is cyclic of order 3^n . Under these assumptions, we determine the form of $\alpha \in E_n$ which satisfies $(E_n/C_n)_3 = \langle \alpha C_n \rangle$ and $\alpha^{1+\sigma} \in E_n^3$. From the assumption $A_0 \neq 1$, there exists $\gamma \in E_0$ such that

$$\gamma^3 = \prod_{i=0}^{3^n-1} \xi_{2i}.$$

Assume that $(E_n/C_n)_3 = \langle \alpha C_n \rangle$ and $\alpha^{1+\sigma} = \beta^3$ for some $\beta \in E_n$. Since the order of $(E_n/C_n)_3$ is 3^n , we see that $\alpha^{3^{n-1}} = \gamma u$, $\beta = \alpha^e v$ for some $u, v \in C_n$ and $e \in \mathbb{N}$. Then

$$u^{1+\sigma} = \pm(\alpha^{3^{n-1}})^{1+\sigma} = \pm\beta^{3^n} = \pm\alpha^{e3^n} v^{3^n} \equiv (\gamma u)^{3e} = \prod_{i=0}^{3^n-1} \xi_{2^i}^e u^{3e} \pmod{C_n^{3^n}}.$$

We write $u = \xi_0^{e_0} \cdots \xi_{r-1}^{e_{r-1}}$ with $e_i \in \mathbb{Z}$ and substitute this in both sides of the above congruence relation. Since $\xi_r = \pm(\xi_0 \cdots \xi_{r-1})^{-1}$, we obtain the following system of simultaneous equations:

$$e_{i-1} + e_i - e_{r-1} \equiv \begin{cases} e + 3ee_i & \text{if } i \text{ is even,} \\ 3ee_i & \text{if } i \text{ is odd.} \end{cases}$$

Here the congruence is modulo 3^n and $e_{-1} = 0$. This equation is easily solved. In fact, if we put $x = e_{r-1}$ and $y = e$, then we can represent all e_i by x and y . Now, we fix x to be 0 and vary y from 0 to $3^n - 1$. If we find that γu is contained in $E_n^{3^{n-1}}$ for some y , then we put $\eta = (\gamma u)^{1/3^{n-1}}$. It is easy to check whether η , $\eta\varepsilon$ or $\eta\varepsilon^2$ is a cube in E_n .

A Galois generator ξ of C_n is hard to find. But we know the cyclotomic unit of Hasse (cf. [2]) which generates a fairly large subgroup of C_n . So, we execute the above procedure by letting ξ to be Hasse's unit. We will be able to find η by this method with some luck.

4. EXAMPLES

Let $F = \mathbb{Q}(\sqrt{m})$ where m is a positive square-free integer congruent to 2 modulo 3. There are 207 m 's less than 10000 which satisfy $|A_0| = 3$. We denote $\text{Ker}(A_0 \rightarrow A_n)$ by H_n . We used a computer to implement the above method for these F 's and fortunately found η and conclude that $H_n \neq 1$ for many F 's. We show the results of our computation in Table 1 (next page). The proposition in §1 implies that if $m \equiv 2 \pmod{3}$, $|A_0| = 3$, and $H_n \neq 1$ for some $n \geq 1$, then the order of A_n is bounded, namely, Greenberg's conjecture is valid for F , and the Iwasawa invariant $\lambda_3(F)$ is zero. A question mark in the table means that we do not know the value. For example, we got $|H_1| = 1$ when $m = 899$ (cf. the remark below). So we searched $\eta \in F_2$ with the method of §3 but could not find it. We cannot conclude whether $|H_2|$ is 1 or 3. Next we pursued a calculation in F_3 and found $\eta \in F_3$. Therefore $|H_3| = 3$ and $\lambda_3(F) = 0$.

Remark . Since $|H_1| = (E_0 : N_{E_1/F_0}(E_1))$, we can obtain the exact value of $|H_1|$ by computing E_1 (cf. [3]). We note that $|H_1| = 1$ for all m 's in Table 1 for which we could not find $\eta \in E_1$.

TABLE 1. All m 's satisfying $m \equiv 2 \pmod{3}$ and $|A_0| = 3$ ($m < 10000$)

m	$ H_1 $	$ H_2 $	$ H_3 $	$ H_4 $	$\lambda_3(F)$	m	$ H_1 $	$ H_2 $	$ H_3 $	$ H_4 $	$\lambda_3(F)$
254	1	?	?	?	?	3221	3	3	3	3	0
257	3	3	3	3	0	3281	3	3	3	3	0
326	3	3	3	3	0	3287	3	3	3	3	0
359	3	3	3	3	0	3305	1	?	?	?	?
443	1	3	3	3	0	3419	3	3	3	3	0
473	1	?	?	?	?	3422	1	3	3	3	0
506	3	3	3	3	0	3482	3	3	3	3	0
659	3	3	3	3	0	3569	1	?	3	3	0
761	3	3	3	3	0	3590	3	3	3	3	0
785	1	?	3	3	0	3602	3	3	3	3	0
839	3	3	3	3	0	3803	3	3	3	3	0
842	3	3	3	3	0	3941	3	3	3	3	0
899	1	?	3	3	0	3962	3	3	3	3	0
1091	3	3	3	3	0	4001	3	3	3	3	0
1211	3	3	3	3	0	4094	3	3	3	3	0
1223	3	3	3	3	0	4106	3	3	3	3	0
1229	3	3	3	3	0	4151	3	3	3	3	0
1367	3	3	3	3	0	4193	3	3	3	3	0
1373	3	3	3	3	0	4238	1	3	3	3	0
1406	3	3	3	3	0	4283	3	3	3	3	0
1478	3	3	3	3	0	4286	1	?	3	3	0
1523	3	3	3	3	0	4355	3	3	3	3	0
1646	1	?	?	?	?	4367	3	3	3	3	0
1787	3	3	3	3	0	4481	1	3	3	3	0
1811	1	3	3	3	0	4493	3	3	3	3	0
1847	3	3	3	3	0	4511	1	3	3	3	0
1901	3	3	3	3	0	4649	3	3	3	3	0
1907	3	3	3	3	0	4670	3	3	3	3	0
1937	1	?	?	?	?	4706	3	3	3	3	0
2021	1	?	3	3	0	4778	3	3	3	3	0
2099	1	3	3	3	0	4841	3	3	3	3	0
2177	3	3	3	3	0	4853	3	3	3	3	0
2207	3	3	3	3	0	4886	3	3	3	3	0
2213	3	3	3	3	0	4907	1	3	3	3	0
2429	1	?	3	3	0	4910	3	3	3	3	0
2459	3	3	3	3	0	4934	3	3	3	3	0
2495	3	3	3	3	0	4970	3	3	3	3	0
2510	1	?	3	3	0	4982	3	3	3	3	0
2543	3	3	3	3	0	4994	3	3	3	3	0
2666	1	?	?	?	?	5042	3	3	3	3	0
2678	1	3	3	3	0	5063	1	?	?	?	?
2711	3	3	3	3	0	5081	1	?	?	3	0
2726	3	3	3	3	0	5099	3	3	3	3	0
2777	1	3	3	3	0	5102	3	3	3	3	0
2831	3	3	3	3	0	5255	3	3	3	3	0
2894	3	3	3	3	0	5261	3	3	3	3	0
2918	1	?	3	3	0	5297	1	?	?	3	0
2981	3	3	3	3	0	5303	3	3	3	3	0
2993	3	3	3	3	0	5327	3	3	3	3	0
3023	3	3	3	3	0	5333	3	3	3	3	0
3035	3	3	3	3	0	5369	3	3	3	3	0
3047	1	?	?	3	0	5477	3	3	3	3	0
3062	3	3	3	3	0	5621	3	3	3	3	0
3071	3	3	3	3	0	5738	3	3	3	3	0
3158	1	?	3	3	0	5741	3	3	3	3	0
3173	3	3	3	3	0	5798	3	3	3	3	0

TABLE 1 (continued)

m	$ H_1 $	$ H_2 $	$ H_3 $	$ H_4 $	$\lambda_3(F)$	m	$ H_1 $	$ H_2 $	$ H_3 $	$ H_4 $	$\lambda_3(F)$
5903	3	3	3	3	0	8282	1	?	3	3	0
5918	3	3	3	3	0	8285	3	3	3	3	0
5930	3	3	3	3	0	8306	3	3	3	3	0
5954	1	?	3	3	0	8339	1	?	?	3	0
6026	3	3	3	3	0	8363	1	3	3	3	0
6053	3	3	3	3	0	8399	3	3	3	3	0
6185	3	3	3	3	0	8426	3	3	3	3	0
6209	3	3	3	3	0	8438	3	3	3	3	0
6311	3	3	3	3	0	8447	3	3	3	3	0
6401	3	3	3	3	0	8519	3	3	3	3	0
6515	3	3	3	3	0	8543	3	3	3	3	0
6557	3	3	3	3	0	8597	3	3	3	3	0
6623	3	3	3	3	0	8603	3	3	3	3	0
6686	3	3	3	3	0	8711	1	?	?	?	?
6770	3	3	3	3	0	8735	3	3	3	3	0
6782	3	3	3	3	0	8789	3	3	3	3	0
6791	1	3	3	3	0	8837	1	3	3	3	0
6806	1	?	?	?	?	8909	3	3	3	3	0
6887	3	3	3	3	0	8930	3	3	3	3	0
6995	1	?	?	?	?	8999	3	3	3	3	0
7019	3	3	3	3	0	9062	3	3	3	3	0
7055	3	3	3	3	0	9086	3	3	3	3	0
7058	3	3	3	3	0	9149	3	3	3	3	0
7235	3	3	3	3	0	9155	3	3	3	3	0
7259	3	3	3	3	0	9215	3	3	3	3	0
7262	3	3	3	3	0	9218	3	3	3	3	0
7310	3	3	3	3	0	9278	3	3	3	3	0
7319	3	3	3	3	0	9281	3	3	3	3	0
7415	3	3	3	3	0	9293	3	3	3	3	0
7481	3	3	3	3	0	9323	3	3	3	3	0
7598	1	?	3	3	0	9413	3	3	3	3	0
7601	1	?	3	3	0	9419	3	3	3	3	0
7643	1	3	3	3	0	9467	3	3	3	3	0
7655	3	3	3	3	0	9479	3	3	3	3	0
7658	1	?	?	3	0	9551	3	3	3	3	0
7673	3	3	3	3	0	9578	1	3	3	3	0
7694	3	3	3	3	0	9590	1	?	?	3	0
7709	1	3	3	3	0	9659	1	3	3	3	0
7721	3	3	3	3	0	9710	3	3	3	3	0
7745	3	3	3	3	0	9749	3	3	3	3	0
7883	1	3	3	3	0	9830	3	3	3	3	0
7994	3	3	3	3	0	9833	3	3	3	3	0
8051	3	3	3	3	0	9869	3	3	3	3	0
8057	3	3	3	3	0	9902	3	3	3	3	0
8069	1	3	3	3	0	9905	3	3	3	3	0
8255	3	3	3	3	0	9926	1	?	?	3	0
8267	3	3	3	3	0	9995	1	?	3	3	0
8279	1	3	3	3	0						

ACKNOWLEDGMENTS

The authors express their gratitude to the referee who pointed out that the Theorem is not correct without the assumption that 3 does not split in F/\mathbb{Q} . We also express our gratitude to Mr. H. Sumida. We could correct some errors in Table 1 by comparing our data with his computational results.

REFERENCES

1. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284. MR **53**:5529
2. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952. MR **14**:141
3. S. Mäki, *The determination of units in real cyclic sextic fields*, Lecture Notes in Math., vol. 797, Springer–Verlag, Berlin, Heidelberg, New York, 1980. MR **82a**:12004

DEPARTMENT OF MATHEMATICS, COLLEGE OF INDUSTRIAL TECHNOLOGY, NIHON UNIVERSITY,
2-11-1 SHIN-EI, NARASHINO, CHIBA, JAPAN

E-mail address: `fukuda@math.cit.nihon-u.ac.jp`

DEPARTMENT OF MATHEMATICS, TOKYO UNIVERSITY OF AGRICULTURE AND TECHNOLOGY,
FUCHU, TOKYO, JAPAN