ACTA ARITHMETICA
XXX (1976)

Conspectus materiae tomi XXX, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

Ranks of 3-class groups of non-Galois cubic fields*

by

FRANK GERTH III (Austin, Tex.)

1. Introduction. In this paper we describe how to compute the ranks of the 3-class groups of non-Galois cubic extension fields of the rational numbers $\boldsymbol{Q}$. The results of this paper may be considered as generalizations of the results in [5] on pure cubic fields and as analogs of classical results on 2-class groups of quadratic fields.

Some other mathematicians who have recently investigated 3-class groups of non-Galois cubic fields are G. Gras, S. Kobayashi, and T. Callahan. In [6] Gras finds upper and lower bounds for the ranks of the 3-class groups of non-Galois cubic fields, and the results of our paper are extensions of his results. In [10] and [11] Kobayashi treats the pure cubic case, and in [3] Callahan considers non-Galois cubic fields whose normal closure is unramified over the quadratic subfield of the normal closure. We thank these mathematicians for sending us preprints of their work.

We conclude this section with some remarks on notation. In general we use multiplicative notation for groups and modules, and the action of a group or a ring on a module is expressed by exponentiation. Furthermore $(x^\sigma)^\tau = x^{\sigma\tau}$. Results from class field theory that are quoted without references can be found in [1], [4], or [12].

2. Preliminary results and first main theorem. Let $\boldsymbol{Q}$ denote the field of rational numbers; let L be a non-Galois cubic extension field of $\boldsymbol{Q}$; let K be the normal closure of L; and let F be the quadratic field contained in K. Let σ be the generator of $\mathrm{Gal}(K/L)$, and let τ be a generator of $\mathrm{Gal}(K/F)$. Then $\mathrm{Gal}(K/\boldsymbol{Q})$ is generated by $\{\sigma, \tau\}$ subject to the relations $\sigma^2 = 1$, $\tau^3 = 1$, $\sigma\tau = \tau^2\sigma$. Note that $\sigma|F$ generates $\mathrm{Gal}(F/\boldsymbol{Q})$. We shall abbreviate $\mathrm{Gal}(K/L)$ by $\langle\sigma\rangle$, $\mathrm{Gal}(K/F)$ by $\langle\tau\rangle$, and $\mathrm{Gal}(K/\boldsymbol{Q})$ by $\langle\sigma, \tau\rangle$.

Let H be an abelian 3-group. Then H may be viewed as a module over $\boldsymbol{Z}_3$, where $\boldsymbol{Z}_3$ denotes the ring of 3-adic integers. We define

$$\mathrm{rank}\, H = \dim_{\boldsymbol{F}_3} H \otimes_{\boldsymbol{Z}_3} \boldsymbol{F}_3$$

* This research was supported by NSF Grant GP-28488A3.

where $\boldsymbol{F}_3$ is the finite field of three elements. If H is also a $\boldsymbol{Z}_3[\langle\sigma\rangle]$ module, we define $H^+ = \{a \in H \mid a^\sigma = a\}$ and $H^- = \{a \in H \mid a^\sigma = a^{-1}\}$. Then $H \cong H^+ \times H^-$ (cf. [5], proof of Lemma 2.1).

If M is any finite algebraic extension field of $\boldsymbol{Q}$, we let C_M denote the ideal class group of M, S_M denote the 3-class group of M (i.e., the Sylow 3-subgroup of C_M), and $A_M = \{a \in S_M \mid a^3 = 1\}$. Our goal is to compute rank S_L, where L is a non-Galois cubic extension of $\boldsymbol{Q}$. Since $\operatorname{rank} A_L = \operatorname{rank} S_L$, it suffices to compute $\operatorname{rank} A_L$.

We note that the natural map $S_L \to S_K$, which is induced by the inclusion mapping of ideals of L into ideals of K, is injective since 3 is relatively prime to $[K : L] = 2$. So we may consider S_L as a subgroup of S_K. Furthermore $S_K \cong S_K^+ \times S_K^-$ and $S_L \cong S_K^+$ (cf. [5], proofs of Lemmas 2.1 and 2.2). Similarly $A_K \cong A_K^+ \times A_K^-$ and $A_L \cong A_K^+$.

Let $N_\tau\colon S_K \to S_F$ (resp., $N_\sigma\colon S_K \to S_L$; resp., $N_{\sigma,\tau}\colon S_K \to S_{\boldsymbol{Q}}$) be the map induced by the norm map from ideals of K to ideals of F (resp. L, resp. $\boldsymbol{Q}$).

LEMMA 2.1. $N_\tau(S_K^+) = \{1\}$.

Proof. Let $a \in S_K^+$. Since S_K^+ is an abelian 3-group, there is an element $b \in S_K^+$ such that $b^2 = a$. Then

$$N_\tau(a) = a^{1+\tau+\tau^2} = (b^2)^{1+\tau+\tau^2} = (b^{1+\sigma})^{1+\tau+\tau^2} = b^{1+\tau+\tau^2+\sigma+\sigma\tau+\sigma\tau^2} = N_{\sigma,\tau}(b) \in S_{\boldsymbol{Q}} = \{1\}.$$

So $N_\tau(S_K^+) = \{1\}$.

LEMMA 2.2. *$S_F \subseteq S_K^-$, and hence $A_F \subseteq A_K^-$.*

Proof. If $a \in S_F$, then $a^{1+\sigma} = N_\sigma(a) \in S_{\boldsymbol{Q}} = \{1\}$ since $N_\sigma | S_F\colon S_F \to S_{\boldsymbol{Q}}$. So $a^\sigma = a^{-1}$, and hence $a \in S_K^-$.

Let $B = \{a \in A_K \mid a^{(1-\tau)^2} = 1\}$. If $a \in B$, then

$$(a^\sigma)^{(1-\tau)^2} = (a^\sigma)^{1-2\tau+\tau^2} = a^{\sigma-2\sigma\tau+\sigma\tau^2} = a^{\sigma-2\tau^2\sigma+\tau\sigma} = a^{(1-2\tau^2+\tau)\sigma} = a^{[(1-\tau)^2+3\tau-3\tau^2]\sigma} = 1$$

since $a^{(1-\tau)^2} = 1$ and $a^3 = 1$. So $a^\sigma \in B$, and B is a $\boldsymbol{Z}_3[\langle\sigma\rangle]$ module. So $B \cong B^+ \times B^-$.

LEMMA 2.3. $A_K^+ = B^+$.

Proof. Clearly $B^+ \subseteq A_K^+$. Now let $a \in A_K^+$. Since $a^\sigma = a$, it suffices to show that $a \in B$. Now

$$a^{(1-\tau)^2} = a^{1-2\tau+\tau^2} = a^{1+\tau+\tau^2-3\tau} = a^{1+\tau+\tau^2}$$

since $a^3 = 1$. Also $a^{1+\tau+\tau^2} = N_\tau(a) \in S_F \subseteq S_K^-$ (by Lemma 2.2). So $a^{(1-\tau)^2} \in S_K^-$. On the other hand,

$$(a^{(1-\tau)^2})^\sigma = a^{\sigma-2\tau\sigma+\tau^2\sigma} = a^{\sigma-2\sigma\tau^2+\sigma\tau} = (a^\sigma)^{1-2\tau^2+\tau} = a^{1-2\tau^2+\tau} = a^{(1-\tau)^2+3\tau-3\tau^2} = a^{(1-\tau)^2},$$

which implies $a^{(1-\tau)^2} \in S_K^+$. Hence $a^{(1-\tau)^2} \in S_K^+ \cap S_K^- = \{1\}$, which implies that $a \in B$.

Remark. We now have

$$\operatorname{rank} S_L = \operatorname{rank} A_L = \operatorname{rank} A_K^+ = \operatorname{rank} B^+ \tag{2.1}$$

and

$$B^+ = \{a \in S_K \mid a^3 = 1,\ a^{(1-\tau)^2} = 1, \text{ and } a^\sigma = a\}.$$

Let $\omega\colon B \to B$ be defined by $\omega(a) = a^{1-\tau}$ for $a \in B$. Let $a \in B^+$. Then

$$(a^{1-\tau})^\sigma = a^{\sigma-\tau\sigma} = a^{\sigma-\sigma\tau^2} = (a^\sigma)^{1-\tau^2} = a^{1-\tau^2} = (a^{1-\tau})^{1+\tau}.$$

Now

$$a^{(1-\tau)^2} = 1 \Rightarrow (a^{1-\tau})^{1-\tau} = 1 \Rightarrow a^{1-\tau} = (a^{1-\tau})^\tau.$$

So

$$(a^{1-\tau})^{1+\tau} = (a^{1-\tau})^2 = (a^{1-\tau})^{-1} \quad \text{since} \quad (a^{1-\tau})^3 = 1.$$

Hence for $a \in B^+$, $(a^{1-\tau})^\sigma = (a^{1-\tau})^{-1}$, which implies that $\omega(B^+) \subseteq B^-$. A similar argument shows that $\omega(B^-) \subseteq B^+$. Let $D = \ker\omega$. It is easy to see that D is a $\boldsymbol{Z}_3[\langle\sigma\rangle]$ module; hence $D = D^+ \times D^-$. Then we have an exact sequence

$$1 \to D^+ \to B^+ \to \omega(B^+) \to 1.$$

Since these groups are elementary abelian 3-groups,

$$\operatorname{rank} B^+ = \operatorname{rank} D^+ + \operatorname{rank} \omega(B^+). \tag{2.2}$$

We note that $\omega\big(\omega(B^+)\big) = (B^+)^{(1-\tau)^2} = \{1\}$ and $\omega(B^+) \subseteq B^-$, which imply that $\omega(B^+) \subseteq D^-$.

LEMMA 2.4. $\omega(B^+) = \{a \in D^- \mid a = b^{1-\tau}$ *for some* $b \in S_K\}$.

Proof. Suppose $a \in D^-$ and $a = b^{1-\tau}$ for some $b \in S_K$. Let $b_1 = b^{\frac{1}{3}(1+\sigma)} \in S_K^+$. It suffices to show that $a = b_1^{1-\tau}$ and $b_1 \in B^+$, since then $a = \omega(b_1)$. Now

$$b_1^{1-\tau} = b^{\frac{1}{3}(1+\sigma)(1-\tau)} = b^{(1-\tau+\sigma-\sigma\tau)\frac{1}{3}} = b^{(1-\tau+\sigma-\tau^2\sigma)\frac{1}{3}} = b^{[1-\tau+(1-\tau^2)\sigma]\frac{1}{3}} = b^{(1-\tau)[1+(1+\tau)\sigma]\frac{1}{3}} = a^{[1+(1+\tau)\sigma]\frac{1}{3}}.$$

Since $a \in D^-$, then $a^\tau = a$, $a^3 = 1$, and $a^\sigma = a^{-1}$. So

$$a^{(1+\tau)\sigma} = a^{2\sigma} = a^{-2} = a.$$

Then $b_1^{1-\tau} = a^{[1+1]\frac{1}{3}} = a$. It remains to show that $b_1 \in B^+$. Since $b_1 \in S_K^+$ and $B^+ = A_K^+$ (by Lemma 2.3), it suffices to show that $b_1^3 = 1$ (i.e., $b_1 \in A_K$). Now

$$1 = a^{1-\tau} = b_1^{(1-\tau)^2} = b_1^{1-2\tau+\tau^2} = b_1^{1+\tau+\tau^2-3\tau}.$$

Since $b_1 \in S_K^+$, Lemma 2.1 implies $b_1^{1+\tau+\tau^2} = N_\tau(b_1) = 1$. So $1 = b_1^{3\tau}$, which implies $b_1^3 = 1$.

Let ${}_ND = \{a \in D \mid N_\tau(a) = 1\}$. Since

$$N_\tau(a^\sigma) = (a^\sigma)^{1+\tau+\tau^2} = a^{(1+\tau^2+\tau)\sigma} = \big(N_\tau(a)\big)^\sigma = 1^\sigma = 1$$

for each $a \in {}_ND$, then ${}_ND$ is a $\boldsymbol{Z}_3[\langle\sigma\rangle]$ module. So ${}_ND = {}_ND^+ \times {}_ND^-$.

LEMMA 2.5. *$D^+ = {}_ND^+$ and $\omega(B^+) \subseteq {}_ND^-$.*

Proof. By definition ${}_ND^+ \subseteq D^+$. Now let $a \in D^+ \subseteq S_K^+$. By Lemma 2.1, $N_\tau(a) = 1$. So $a \in {}_ND^+$, and hence $D^+ \subseteq {}_ND^+$. So $D^+ = {}_ND^+$. Now we prove that $\omega(B^+) \subseteq {}_ND^-$. Since $\omega(B^+) \subseteq D^-$, it suffices to show that $N_\tau(a) = 1$ for each $a \in \omega(B^+)$. So suppose $a \in \omega(B^+)$. Then $a = b^{1-\tau}$ for some $b \in B^+$, and

$$N_\tau(a) = a^{1+\tau+\tau^2} = (b^{1-\tau})^{1+\tau+\tau^2} = b^{1-\tau^3} = 1 \quad \text{since} \quad \tau^3 = 1.$$

PROPOSITION 2.6.

$$\operatorname{rank} S_L = \operatorname{rank}_N D - \operatorname{rank}_N D^- / ({}_ND^- \cap S_K^{1-\tau}).$$

Proof.

$$\begin{aligned}\operatorname{rank} S_L &= \operatorname{rank} B^+ \quad \text{(by equation (2.1))}\\ &= \operatorname{rank} D^+ + \operatorname{rank} \omega(B^+) \quad \text{(by equation (2.2))}\\ &= \operatorname{rank}_N D^+ + \operatorname{rank} \omega(B^+) \quad \text{(by Lemma 2.5).}\end{aligned}$$

Since ${}_ND^-$ is an elementary abelian 3-group, the exact sequence

$$1 \to \omega(B^+) \to {}_ND^- \to {}_ND^-/\omega(B^+) \to 1$$

implies that

$$\operatorname{rank} \omega(B^+) = \operatorname{rank}_N D^- - \operatorname{rank}_N D^-/\omega(B^+).$$

So $\operatorname{rank} S_L = \operatorname{rank}_N D^+ + \operatorname{rank}_N D^- - \operatorname{rank}_N D^-/\omega(B^+)$. Since ${}_ND = {}_ND^+ \times {}_ND^-$, then

$$\operatorname{rank}_N D = \operatorname{rank}_N D^+ + \operatorname{rank}_N D^-.$$

Also $\omega(B^+) = {}_ND^- \cap S_K^{1-\tau}$ by Lemmas 2.4 and 2.5. Hence

$$\operatorname{rank} S_L = \operatorname{rank}_N D - \operatorname{rank}_N D^- / ({}_ND^- \cap S_K^{1-\tau}).$$

Previously we have defined a map $N_\tau\colon S_K \to S_F$, and we now define $N_\tau\colon C_K \to C_F$ in the same way, namely the map induced by the norm map from ideals of K to ideals of F. Let

$${}_NC_K = \{a \in C_K \mid N_\tau(a) = 1\} \quad \text{and} \quad {}_NS_K = \{a \in S_K \mid N_\tau(a) = 1\}.$$

It is easy to see that $C_K^{1-\tau} \subseteq {}_NC_K$ and $S_K^{1-\tau} \subseteq {}_NS_K$. Let t denote the number of primes of F which ramify in K. By [7], Section 1, ${}_NC_K/C_K^{1-\tau} = \{1\}$ if $t = 0$ or 1. Similarly ${}_NS_K/S_K^{1-\tau} = \{1\}$ if $t = 0$ or 1. If $t \geqslant 2$, we let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ be the primes of F which ramify in K. Let $G = \operatorname{Gal}(K/F)$, and let $X = G \times \dots \times G$ (a product of $t-1$ copies of G). For $1 \leqslant i \leqslant t-1$, we define a map $\psi_i\colon F^x \to G$ (where $F^x = F - \{0\}$) by

$$\psi_i(z) = (z, K/F)_{\mathfrak{p}_i} \tag{2.3}$$

where $(\ , K/F)_{\mathfrak{p}_i}$ is the norm residue symbol. Then we define $\psi\colon F^x \to X$ by

$$\psi(z) = \big(\psi_1(z), \dots, \psi_{t-1}(z)\big). \tag{2.4}$$

Let

$$Y = X/\psi(E_F) \tag{2.5}$$

where E_F denotes the group of units of F. Let P_F denote the group of principal fractional ideals of F. Then ψ induces a homomorphism $\psi'\colon P_F \to Y$. Let $\mathfrak{N}_{K/F}\colon I_K \to I_F$ be the norm map from the group of ideals I_K of K to the group of ideals I_F of F. Let ${}_NI_K = \{\mathfrak{A} \in I_K \mid \mathfrak{N}_{K/F}\mathfrak{A} \in P_F\}$. Then we have a map

$$\psi' \circ \mathfrak{N}_{K/F}\colon {}_NI_K \to Y \tag{2.6}$$

which induces a homomorphism $\lambda\colon {}_NC_K \to Y$. Furthermore λ induces an isomorphism $\lambda'\colon {}_NC_K/C_K^{1-\tau} \xrightarrow{\sim} Y$ (cf. [7], Theorem 1). Now Y is an elementary abelian 3-group. So ${}_NC_K/C_K^{1-\tau}$ is an elementary abelian 3-group. Since ${}_NS_K/S_K^{1-\tau}$ is the Sylow 3-subgroup of ${}_NC_K/C_K^{1-\tau}$, then ${}_NS_K/S_K^{1-\tau}$ is canonically isomorphic to ${}_NC_K/C_K^{1-\tau}$. So $\lambda'\colon {}_NS_K/S_K^{1-\tau} \xrightarrow{\sim} Y$ is an isomorphism. Since ${}_NS_K/S_K^{1-\tau}$ and Y are elementary abelian 3-groups, they may be viewed as vector spaces over the finite field $\boldsymbol{F}_3$. Then the map λ' is a vector space isomorphism which is induced by norm residue symbols.

If M is any number field and $\mathfrak{A}$ is an ideal of M, we define $\operatorname{cl}_M(\mathfrak{A})$ to be the ideal class of $\mathfrak{A}$ in the ideal class group C_M. Now let $\mathfrak{A}_1, \dots, \mathfrak{A}_s$ be ideals of K such that the subgroup of C_K generated by $\operatorname{cl}_K(\mathfrak{A}_1), \dots, \operatorname{cl}_K(\mathfrak{A}_s)$ is ${}_ND^-$. Then $\operatorname{cl}_K(\mathfrak{A}_i)^3 = 1$ for $1 \leqslant i \leqslant s$. Let R_K be the free abelian group generated by $\mathfrak{A}_1, \dots, \mathfrak{A}_s$ in I_K, and let $V_K = R_K/R_K^3$. Then the map $V_K \to {}_ND^-$ defined by $\mathfrak{A} \to \operatorname{cl}_K(\mathfrak{A})$ is surjective. We now consider the maps

$$V_K \to {}_ND^- \to {}_NS_K \to {}_NS_K/S_K^{1-\tau} \xrightarrow{\lambda'} Y,$$

where the first map is surjective; the second map is the natural inclusion; the third map is the natural projection; and the last map is the isomorphism λ'. We let $\mu\colon V_K \to Y$ denote the composition of these maps. Then μ is a vector space homomorphism over $\boldsymbol{F}_3$, and with an appropriate choice of bases, the matrix of μ is

$$[(\mathfrak{N}_{K/F}\mathfrak{A}_j, K/F)_{\mathfrak{p}_i}] \bmod \psi(E_F), \qquad 1 \leqslant i \leqslant t-1,\ 1 \leqslant j \leqslant s$$

(cf. equations (2.3) through (2.6)). We note that the image of μ in Y is isomorphic to $({}_ND^- \cdot S_K^{1-\tau})/S_K^{1-\tau} \cong {}_ND^-/({}_ND^- \cap S_K^{1-\tau})$. So

$$\operatorname{rank}_N D^-/({}_ND^- \cap S_K^{1-\tau}) = \text{rank of the matrix } [(\mathfrak{N}_{K/F}\mathfrak{A}_j, K/F)_{\mathfrak{p}_i}] \bmod \psi(E_F)$$
$$\text{for } 1 \leqslant i \leqslant t-1,\ 1 \leqslant j \leqslant s.$$

We also note that

$${}_ND^-/({}_ND^- \cap S_K^{1-\tau}) \cong ({}_ND^- \cdot S_K^{1-\tau})/S_K^{1-\tau} \subseteq {}_NS_K/S_K^{1-\tau} = \{1\} \quad \text{when} \quad t = 0 \text{ or } 1.$$

So

$$\operatorname{rank}_N D^-/({}_ND^- \cap S_K^{1-\tau}) = 0 \quad \text{if} \quad t = 0 \text{ or } 1.$$

We summarize the results of this section in the following theorem.

THEOREM 2.7. *Let L be a non-Galois cubic extension of $\boldsymbol{Q}$. Let K be the normal closure of L, and let F be the quadratic subfield of K. Let τ be a generator of the cyclic group $\operatorname{Gal}(K/F)$, and let σ be the generator of $\operatorname{Gal}(K/L)$. Let S_K (resp. S_L, resp. S_F) be the 3-class group of K (resp. L, resp. F). Let $N_\tau: S_K \to S_F$ be the map induced by the norm map $\mathfrak{N}_{K/F}$ from ideals of K to ideals of F. Let*

$${}_ND = \{a \in S_K \mid a^\tau = a \text{ and } N_\tau(a) = 1\} \quad \text{and} \quad {}_ND^- = \{a \in {}_ND \mid a^\sigma = a^{-1}\}.$$

Then

$$\operatorname{rank} S_L = \operatorname{rank}_N D - \operatorname{rank}_N D^-/({}_ND^- \cap S_K^{1-\tau}).$$

Now let t denote the number of ramified primes in K/F. If $t = 0$ or 1, $\operatorname{rank}_N D^-/({}_ND^- \cap S_K^{1-\tau}) = 0$. If $t \geqslant 2$, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the prime ideals of F which ramify in K, and let $\mathfrak{A}_1, \ldots, \mathfrak{A}_s$ be ideals of K whose ideal classes generate ${}_ND^-$. Let $\mathfrak{N}_{K/F}\mathfrak{A}_j = (x_j)$, where $x_j \in F$ for $1 \leqslant i \leqslant s$. Let E_F be the group of units of F, and ψ be the map defined by equations (2.3) and (2.4). Then

$$\operatorname{rank}_N D^-/({}_ND^- \cap S_K^{1-\tau}) \doteq \operatorname{rank}\{[(x_j, K/F)_{\mathfrak{p}_i}] \bmod \psi(E_F)\}$$

where $[(x_j, K/F)_{\mathfrak{p}_i}]$ is the $(t-1) \times s$ matrix (over the finite field $\boldsymbol{F}_3$) whose ij-th element is the norm residue symbol $(x_j, K/F)_{\mathfrak{p}_i}$.

3. Other main theorems. Let notations be the same as in Section 2. We want to describe how to compute $\operatorname{rank}_N D$ and find a set of ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_s$ whose ideal classes generate ${}_ND^-$. Let $S_K^{(\tau)} = \{a \in S_K \mid a^\tau = a\}$. Then ${}_ND \subseteq S_K^{(\tau)}$. If H is a finite group, we let $|H|$ denote the number of elements in H. It is known (cf. [8], Theorem 13) that

$$|S_K^{(\tau)}| = |S_F| \cdot 3^{t-2+q} \tag{3.1}$$

where

$$q = \begin{cases} 1 & \text{if} \quad e \in N_{K/F}K^x, \\ 0 & \text{if} \quad e \notin N_{K/F}K^x \end{cases} \tag{3.2}$$

where $N_{K/F}$ is the norm map from K^x to F^x, and where e is specified as follows:

(i) if F is an imaginary quadratic field $\neq \boldsymbol{Q}(\sqrt{-3})$, then $e = 1$;

(ii) if $F = \boldsymbol{Q}(\sqrt{-3})$, then $e = \zeta$, where ζ is a primitive cube root of unity (e.g., $\zeta = \frac{1}{2}(-1+\sqrt{-3})$);

(iii) if F is a real quadratic field, then e is the fundamental unit of F.

Let $h = |C_F/S_F|$, and let T be the subgroup of $S_K^{(\tau)}$ generated by S_F and $\operatorname{cl}_K(\mathfrak{P}_1^h), \ldots, \operatorname{cl}_K(\mathfrak{P}_t^h)$, where $\mathfrak{P}_i$ is the unique prime ideal of K such that $\mathfrak{P}_i^3 = \mathfrak{p}_i$, $1 \leqslant i \leqslant t$. Then (cf. [8], proof of Theorem 13),

$$|T| = |S_F| \cdot 3^{t-2+q_1} \tag{3.3}$$

where

$$q_1 = \begin{cases} 1 & \text{if} \quad e \in N_{K/F}E_K, \\ 0 & \text{if} \quad e \notin N_{K/F}E_K \end{cases} \tag{3.4}$$

and where E_K is the group of units of K. So $T = S_K^{(\tau)}$ unless $e \in N_{K/F}K^x$ and $e \notin N_{K/F}E_K$, in which case $|S_K^{(\tau)}| = 3 \cdot |T|$, since then $q = q_1 + 1$.

It is easy to see that T is a $\boldsymbol{Z}_3[\langle\sigma\rangle]$ module, and hence $T \cong T^+ \times T^-$. We shall now find generators for T^+ and T^-. Let $p_1, \ldots, p_u, p_{u+1}, \ldots, p_{u+v}$ be the rational primes which ramify totally in $L/\boldsymbol{Q}$, and suppose $p_1, \ldots, p_u$ decompose in F and $p_{u+1}, \ldots, p_{u+v}$ either remain prime or ramify in F. (We remark that 3 is the only prime which can ramify totally in $L/\boldsymbol{Q}$ and also ramify in $F/\boldsymbol{Q}$.) We order the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ of F so that $(p_i) = \mathfrak{p}_{2i-1}\mathfrak{p}_{2i}$ for $1 \leqslant i \leqslant u$ and so that $\mathfrak{p}_{2u+j}$ is the unique prime of F above (p_{u+j}) for $1 \leqslant j \leqslant v$. (We note that $t = 2u+v$.)

LEMMA 3.1. *T^+ is generated by*

$$\operatorname{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^h), \ldots, \operatorname{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^h), \operatorname{cl}_K(\mathfrak{P}_{2u+1}^h), \ldots, \operatorname{cl}_K(\mathfrak{P}_{2u+v}^h).$$

T^- is generated by

$$S_F \quad \text{and} \quad \operatorname{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^{2h}), \ldots, \operatorname{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^{2h}).$$

Here $h = |C_F/S_F|$.

Proof. With our ordering of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, we see that

$$\mathfrak{p}_{2i-1}^\sigma = \mathfrak{p}_{2i} \quad \text{and} \quad \mathfrak{p}_{2i}^\sigma = \mathfrak{p}_{2i-1} \quad \text{for} \quad 1 \leqslant i \leqslant u,$$

and

$$\mathfrak{p}_{2u+j}^\sigma = \mathfrak{p}_{2u+j} \quad \text{for} \quad 1 \leqslant j \leqslant v.$$

Then $\mathfrak{P}_{2i-1}^\sigma = \mathfrak{P}_{2i}$ and $\mathfrak{P}_{2i}^\sigma = \mathfrak{P}_{2i-1}$ for $1 \leqslant i \leqslant u$, and $\mathfrak{P}_{2u+j}^\sigma = \mathfrak{P}_{2u+j}$ for $1 \leqslant j \leqslant v$. So

$$(\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^h)^\sigma = \mathfrak{P}_{2i}^h\mathfrak{P}_{2i-1}^h = \mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^h \quad \text{for} \quad 1 \leqslant i \leqslant u,$$

and

$$(\mathfrak{P}_{2u+j}^h)^\sigma = \mathfrak{P}_{2u+j}^h \quad \text{for} \quad 1 \leqslant j \leqslant v.$$

Hence

$$\mathrm{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^h), \ldots, \mathrm{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^h), \mathrm{cl}_K(\mathfrak{P}_{2u+1}^h), \ldots, \mathrm{cl}_K(\mathfrak{P}_{2u+v}^h) \in T^+.$$

Now Lemma 2.2 implies $S_F \subseteq T^-$. Also

$$\begin{aligned}(\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^{2h})^\sigma &= \mathfrak{P}_{2i}^h\mathfrak{P}_{2i-1}^{2h} = (\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^{2h})^{-1}\mathfrak{P}_{2i-1}^{3h}\mathfrak{P}_{2i}^{3h} \\ &= (\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^{2h})^{-1}\mathfrak{p}_{2i-1}^h\mathfrak{p}_{2i}^h = (\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^{2h})^{-1}(p_i)^h\end{aligned}$$

for $1 \leqslant i \leqslant u$. Since (p_i) is a principal ideal,

$$\mathrm{cl}_K(\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^{2h})^\sigma = \mathrm{cl}_K(\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^{2h})^{-1},$$

and hence

$$\mathrm{cl}_K(\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^{2h}) \in T^- \quad \text{for} \quad 1 \leqslant i \leqslant u.$$

Since S_F and $\mathrm{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^h), \mathrm{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^{2h}), \ldots, \mathrm{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^h), \mathrm{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^{2h}), \mathrm{cl}_K(\mathfrak{P}_{2u+1}^h), \ldots, \mathrm{cl}_K(\mathfrak{P}_{2u+v}^h)$ generate T, then our calculations show that $\mathrm{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^h), \ldots, \mathrm{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^h), \mathrm{cl}_K(\mathfrak{P}_{2u+1}^h), \ldots, \mathrm{cl}_K(\mathfrak{P}_{2u+v}^h)$ generate T^+, and S_F and $\mathrm{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^{2h}), \ldots, \mathrm{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^{2h})$ generate T^-.

We recall that $S_K^{(\tau)} = T$ unless $e \in N_{K/F}K^\times$ and $e \notin N_{K/F}E_K$, in which case $|S_K^{(\tau)}| = 3 \cdot |T|$ and $q = q_1 + 1$ (cf. equations (3.1) through (3.4)). We first consider the case $S_K^{(\tau)} = T$. (So $q_1 = q$.) Then ${}_ND = \{a \in T \mid N_\tau(a) = 1\}$. The map $N_\tau|T\colon T \to S_F$ produces an exact sequence

$$1 \to {}_ND \to T \to N_\tau(T) \to 1,$$

and hence

$$|{}_ND| = |T|/|N_\tau(T)|. \tag{3.5}$$

Equation (3.3) specifies $|T|$, but we still need to compute $|N_\tau(T)|$. By Lemma 2.1, $N_\tau(T^+) = \{1\}$. So $N_\tau(T) = N_\tau(T^-)$. We note that $N_\tau(S_F) = S_F^3$, and

$$N_\tau[\mathrm{cl}_K(\mathfrak{P}_{2i-1}^h\mathfrak{P}_{2i}^{2h})] = \mathrm{cl}_F(\mathfrak{p}_{2i-1}^h\mathfrak{p}_{2i}^{2h}) \quad \text{for} \quad 1 \leqslant i \leqslant u.$$

We let

$$Z = \text{subgroup of } S_F \text{ generated by } \mathrm{cl}_F(\mathfrak{p}_1^h\mathfrak{p}_2^{2h}), \ldots, \mathrm{cl}_F(\mathfrak{p}_{2u-1}^h\mathfrak{p}_{2u}^{2h}). \tag{3.6}$$

Then

$$|N_\tau(T)| = |S_F^3 \cdot Z| = |(S_F^3 \cdot Z)/S_F^3| \cdot |S_F^3| = |Z/(Z \cap S_F^3)| \cdot |S_F^3|.$$

Using this result, equation (3.3) with $q_1 = q$, and equation (3.5), we get

$$|{}_ND| = \frac{|S_F| \cdot 3^{t-2+q}}{|Z/(Z \cap S_F^3)| \cdot |S_F^3|}.$$

Let $r = \mathrm{rank}\, S_F = \mathrm{rank}\, S_F/S_F^3$, and $z = \mathrm{rank}\, Z/(Z \cap S_F^3)$. Since S_F/S_F^3 and $Z/(Z \cap S_F^3)$ are elementary abelian 3-groups, $|S_F/S_F^3| = 3^r$ and $|Z/(Z \cap S_F^3)| = 3^z$. We also note that $0 \leqslant z \leqslant \min(r, u)$. Then $|{}_ND| = 3^{r+t+q-z-2}$. Since ${}_ND$ is an elementary abelian 3-group, $\mathrm{rank}\ {}_ND = r+t+q-z-2$.

In the case $|S_K^{(\tau)}| = 3 \cdot |T|$, we can repeat the above arguments with ${}_ND \cap T$ replacing ${}_ND$ and with $q_1 = q-1$. Then $\mathrm{rank}({}_ND \cap T) = r+t+q-z-3$. Now $S_K^{(\tau)}/T$ is a cyclic group of order 3 generated by the image in $S_K^{(\tau)}/T$ of some ideal class $b \in S_K^{(\tau)}$. By [6], proof of Proposition 2, b can be chosen from $(S_K^{(\tau)})^+ = \{a \in S_K^{(\tau)} \mid a^\sigma = a\}$. But then $N_\tau(b) = 1$ by Lemma 2.1, and hence $b \in {}_ND$. So $\mathrm{rank}\ {}_ND = 1 + \mathrm{rank}({}_ND \cap T)$, and we again obtain the formula

$$\mathrm{rank}_N D = r+t+q-z-2.$$

We summarize our results in the following

PROPOSITION 3.2. *Let notations be as in Theorem 2.7. Then*

$$\mathrm{rank}_N D = r+t+q-z-2,$$

where $r = \mathrm{rank}\, S_F$; $t =$ *number of ramified primes in* K/F; $q = 0$ *or* 1 *as specified by equation* (3.2); *and* $z = \mathrm{rank}\, Z/(Z \cap S_F^3)$, *where* Z *is defined by equation* (3.6). *Furthermore* $0 \leqslant z \leqslant \min(r, u)$, *where* u *is the number of rational primes which ramify totally in* $L/\boldsymbol{Q}$ *and decompose in* $F/\boldsymbol{Q}$.

COROLLARY 3.3. *If* K/F *is unramified, then* $\mathrm{rank}_N D = r+q-2$.

Proof. Since K/F is unramified, then $t = 0$. Furthermore, $0 \leqslant z \leqslant u \leqslant t$, which implies $z = 0$. So Proposition 3.2 gives $\mathrm{rank}_N D = r+q-2$.

THEOREM 3.4. *Let notations be as in Theorem 2.7. If* K/F *is unramified, then* $\mathrm{rank}\, S_L = \mathrm{rank}\, S_F - 1$.

Proof. By Corollary 3.3, $\mathrm{rank}_N D = r+q-2$. By Theorem 2.7, $\mathrm{rank}_N D^-/({}_ND^- \cap S_K^{1-\tau}) = 0$ since $t = 0$. Hence Theorem 2.7 and Corollary 3.3 imply that $\mathrm{rank}\, S_L = r+q-2 = \mathrm{rank}\, S_F + q - 2$. So it suffices to show that $q = 1$. From equation (3.2), we must show that $e \in N_{K/F}K^\times$, where e is the unit of F that is specified immediately after equation (3.2). Let $\mathfrak{p}$ be any prime of F and $\mathfrak{P}$ a prime of K above $\mathfrak{p}$. Let $F_\mathfrak{p}$ (resp. $K_\mathfrak{P}$) be the completion of F at $\mathfrak{p}$ (resp. of K at $\mathfrak{P}$). Then $K_\mathfrak{P}/F_\mathfrak{p}$ is unramified. It is well known that if e is a unit of $F_\mathfrak{p}$ and $K_\mathfrak{P}/F_\mathfrak{p}$ is unramified, then e is the norm of a unit of $K_\mathfrak{P}$. So e is a "local norm" at each prime $\mathfrak{p}$ of F. Since K/F is a cyclic extension, then e is a "global norm"; that is, $e \in N_{K/F}K^\times$, which is what we wanted to prove.

Remark. Theorem 3.4 proves a conjecture of Callahan [3].

We now return to the general case (Theorem 2.7) and describe how to find ideals $\mathfrak{A}_1, \dots, \mathfrak{A}_s$ of K whose ideal classes generate ${}_ND^-$. We note that ${}_ND^- = \{a \in T^- \mid N_\tau(a) = 1\}$, and Lemma 3.1 shows that T^- is generated by S_F and $\mathrm{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^{2h}), \dots, \mathrm{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^{2h})$. Let ${}_NS_F = \{a \in S_F \mid N_\tau(a) = 1\}$. Since $N_\tau(a) = a^{1+\tau+\tau^2} = a^3$ for $a \in S_F$, then ${}_NS_F = \{a \in S_F \mid a^3 = 1\}$, and hence ${}_NS_F$ is an elementary abelian 3-group with $\mathrm{rank}_N S_F = \mathrm{rank}\, S_F = r$. We let $\mathfrak{A}_1, \dots, \mathfrak{A}_r$ be ideals of F whose ideal classes generate ${}_NS_F$. Next we let A be the subgroup of T^- generated by $\mathrm{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^{2h}), \dots, \mathrm{cl}_K(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^{2h})$, and we let $\Gamma = \{b \in A \mid N_\tau(b) \in S_F^3\}$. From these definitions $A^3 \subseteq \Gamma$. Also since $\mathfrak{P}_i^3 = \mathfrak{p}_i$ for each i, then A^3 is generated by ideal classes arising from S_F. Furthermore $N_\tau(A) = Z$ (which is defined by equation (3.6)), $N_\tau(\Gamma) = Z \cap S_F^3$, and $|A/\Gamma| = |Z/(Z \cap S_F^3)| = 3^z$. We let $\mathfrak{b}_1, \dots, \mathfrak{b}_\gamma$ be ideals of K whose ideal classes belong to Γ and whose images in Γ/A^3 generate Γ/A^3. (Note that we may choose the ideals so that $\gamma = u - z$.) Since $N_\tau[\mathrm{cl}_K(\mathfrak{b}_i)] \in S_F^3$, there exists an ideal $\mathfrak{c}_i$ of F such that $N_\tau[\mathrm{cl}_K(\mathfrak{b}_i)] = \mathrm{cl}_F(\mathfrak{c}_i^3) = N_\tau[\mathrm{cl}_K(\mathfrak{c}_i)]$. Then $N_\tau[\mathrm{cl}_K(\mathfrak{b}_i\mathfrak{c}_i^{-1})] = 1$ for $1 \leqslant i \leqslant \gamma$. We let $\mathfrak{A}_{r+i} = \mathfrak{b}_i\mathfrak{c}_i^{-1}$ for $1 \leqslant i \leqslant \gamma$, and we let $s = r + \gamma$. Then $\mathfrak{A}_1, \dots, \mathfrak{A}_r, \mathfrak{A}_{r+1}, \dots, \mathfrak{A}_s$ are ideals such that $\mathrm{cl}_K(\mathfrak{A}_1), \dots, \mathrm{cl}_K(\mathfrak{A}_s)$ generate ${}_ND^-$, and they can be used in Theorem 2.7. In Section 4 we shall use this procedure for finding $\mathfrak{A}_1, \dots, \mathfrak{A}_s$.

Next we describe how to compute q in the general case (cf. Proposition 3.2). From equation (3.2), $q = 1$ if $e \in N_{K/F}K^x$, and $q = 0$ if $e \notin N_{K/F}K^x$, where e is the unit of F specified immediately after equation (3.2). So $q = 1 \Leftrightarrow e$ is a global norm $\Leftrightarrow e$ is a local norm at each prime of F (since K/F is cyclic) $\Leftrightarrow e$ is a local norm at each prime $\mathfrak{p}_i$ of F which ramifies in K (since local units are local norms at unramified primes) $\Leftrightarrow$ each norm residue symbol $(e, K/F)_{\mathfrak{p}_i}$ is trivial, $1 \leqslant i \leqslant t$. (Also the "product formula" for norm residue symbols allows us to drop one prime.) So

$$q = 1 - \mathrm{rank}\,[(e, K/F)_{\mathfrak{p}_i}],$$

where $[(e, K/F)_{\mathfrak{p}_i}]$ is a $(t-1) \times 1$ matrix. Since $\psi(E_F) = \psi(e)$ (see equations (2.3) and (2.4) for the definition of ψ), then we can combine Theorem 2.7 and Proposition 3.2 as follows.

THEOREM 3.5. *With the notations of Theorem 2.7 and Proposition 3.2,*

$$\mathrm{rank}\, S_L = r + t - 1 - z - \mathrm{rank}\,[(x_j, K/F)_{\mathfrak{p}_i}], \quad 1 \leqslant i \leqslant t-1,\ 0 \leqslant j \leqslant s,$$

where $x_0 = e$ (which is specified immediately after equation (3.2)).

We now consider the special case $S_F = \{1\}$. Then in Theorem 3.5, $r = 0$ and $z = 0$ (cf. Proposition 3.2). For generators of ${}_ND^-$, we may take $\mathrm{cl}_K(\mathfrak{P}_1^h\mathfrak{P}_2^{2h}), \dots, \mathrm{cl}(\mathfrak{P}_{2u-1}^h\mathfrak{P}_{2u}^{2h})$. Then $s = u$, $\mathfrak{A}_j = \mathfrak{P}_{2j-1}^h\mathfrak{P}_{2j}^{2h}$, and $(x_j) = \mathfrak{N}_{K/F}\mathfrak{A}_j$ for $1 \leqslant j \leqslant s$. Hence we obtain the following

THEOREM 3.6. *Let notations be as in Theorems 2.7 and 3.5. If* $S_F = \{1\}$, *then*

$$\mathrm{rank}\, S_L = t - 1 - \mathrm{rank}\,[(x_j, K/F)_{\mathfrak{p}_i}], \quad 1 \leqslant i \leqslant t-1,\ 0 \leqslant j \leqslant s.$$

Remark. Theorem 3.6 can be used for pure cubic extensions $L/\boldsymbol{Q}$ since then $F = \boldsymbol{Q}(\sqrt{-3})$ and $S_F = \{1\}$. In [5], Theorem 4.5, we presented another algorithm for computing $\mathrm{rank}\, S_L$. Although that algorithm is somewhat different from the algorithm in this paper, we point out that the t in [5] corresponds to

$$t - 1 - \mathrm{rank}\,[(x_0, K/F)_{\mathfrak{p}_i}], \quad 1 \leqslant i \leqslant t-1,$$

in Theorem 3.6; and the s_1 in [5] corresponds to

$$\mathrm{rank}\,\{[(x_j, K/F)_{\mathfrak{p}_i}] \bmod \psi(x_0)\}, \quad 1 \leqslant i \leqslant t-1,\ 1 \leqslant j \leqslant s$$

(see Theorem 2.7). We also remark that as a consequence of [6], proof of Proposition 2, we may omit the column of the matrix in [5], Theorem 4.5, that involves the prime (π).

Again we assume $S_F = \{1\}$. Suppose no rational prime decomposes in $F/\boldsymbol{Q}$ if it ramifies totally in $L/\boldsymbol{Q}$. Then $s = u = 0$, and hence we obtain the following result (cf. [5], Theorem 5.1 and Corollary 5.2, [6], Corollary 6, and [10]).

COROLLARY 3.7. *With the assumptions of Theorem 3.6, suppose that no rational prime decomposes in* $F/\boldsymbol{Q}$ *if it ramifies totally in* $L/\boldsymbol{Q}$. *Then*

$$\mathrm{rank}\, S_L = t - 1 - \mathrm{rank}\,[(x_0, K/F)_{\mathfrak{p}_i}], \quad 1 \leqslant i \leqslant t-1.$$

4. Some examples. In this section we illustrate Theorems 3.4, 3.5, and 3.6 with examples. We let notations be the same as in Sections 2 and 3. First we claim that the norm residue symbols $(x_j, K/F)_{\mathfrak{p}_i}$ can be replaced by cubic Hilbert symbols, which are easy to compute (see [1], Chapter 12 or [4], pp. 348–354). This is clear if $F = \boldsymbol{Q}(\sqrt{-3})$, for then F contains the cube roots of unity, and hence $K = F(\sqrt[3]{x})$ for some $x \in F$. Then we can replace the norm residue symbol $(x_j, K/F)_{\mathfrak{p}_i}$ by the cubic Hilbert symbol $(x_j, x)_{\mathfrak{p}_i}$. (Here we are using the notation of [1].) Now suppose $F \neq \boldsymbol{Q}(\sqrt{-3})$. Suppose $\mathfrak{p}$ is a prime of F above a rational prime $p \neq 3$, and suppose $\mathfrak{p}$ ramifies in K/F (hence p ramifies totally in $L/\boldsymbol{Q}$). Then [9], Section 3, shows that p decomposes in F if $p \equiv 1 \pmod 3$ and remains prime in F if $p \equiv -1 \pmod 3$. For $p \equiv 1 \pmod 3$, the multiplicative group of the residue class field of F at $\mathfrak{p}$ contains $p-1$ elements, and $3 \mid (p-1)$. For $p \equiv -1 \pmod 3$, the multiplicative group of the residue class field of F at $\mathfrak{p}$ contains p^2-1 elements, and $3 \mid (p^2-1)$. So in both cases the completion $F_\mathfrak{p}$ of F at $\mathfrak{p}$ contains the cube roots of unity. If $\mathfrak{P}$

is the unique prime of K above $\mathfrak{p}$, then the completion $K_{\mathfrak{P}}$ of K at $\mathfrak{P}$ satisfies $K_{\mathfrak{P}} = F_{\mathfrak{p}}(\sqrt[3]{x_{\mathfrak{p}}})$ for some $x_{\mathfrak{p}} \in F_{\mathfrak{p}}$. (Actually $x_{\mathfrak{p}}$ can be chosen from F.) So we can replace the norm residue symbol $(x_j, K/F)_{\mathfrak{p}}$ by the cubic Hilbert symbol $(x_j, x_{\mathfrak{p}})_{\mathfrak{p}}$. Finally we suppose that the prime $\mathfrak{p}$ of F is above 3 and that $\mathfrak{p}$ ramifies in K/F. If $\mathfrak{p}$ is the only prime of F above 3 (i.e., if 3 ramifies or remains prime in $F/\boldsymbol{Q}$), then we may take $\mathfrak{p}_t = \mathfrak{p}$, and $\mathfrak{p}$ will not enter into the calculations in Theorems 3.5 and 3.6. If 3 decomposes in F, then $F_{\mathfrak{p}} = \boldsymbol{Q}_3$, the field of 3-adic numbers. We adjoin a primitive cube root of unity ζ to $F_{\mathfrak{p}}$. If $\mathfrak{P}$ is the unique prime of K above $\mathfrak{p}$, then $K_{\mathfrak{P}}(\zeta) = F_{\mathfrak{p}}(\zeta, \sqrt[3]{x_{\mathfrak{p}}})$ for some $x_{\mathfrak{p}} \in F_{\mathfrak{p}}(\zeta)$. Then we may replace $(x_j, K/F)_{\mathfrak{p}}$ by $(x_j, x_{\mathfrak{p}})_{\mathfrak{l}}$, where $\mathfrak{l}$ is the unique prime of $F_{\mathfrak{p}}(\zeta) = \boldsymbol{Q}_3(\zeta)$ above $\mathfrak{p}$. We note that [1], Chapter 12, and [4], pp. 353–354, show explicitly how to compute cubic Hilbert symbols in $\boldsymbol{Q}_3(\zeta)$.

Thus from Theorems 3.5 and 3.6, we see that we can compute $\operatorname{rank} S_L$ if we know the arithmetic of the quadratic field F. More precisely, r and z are determined by examining the 3-class group of F; t is the number of primes of F which ramify in K; and the elements of the matrix can be determined by cubic Hilbert symbol calculations in F (with perhaps some cubic Hilbert symbol calculations in $\boldsymbol{Q}_3(\zeta)$).

In the examples that follow, we make use of the results on cubic fields that appear in [9] and [13]. As our first example we let L be a cubic extension of $\boldsymbol{Q}$ obtained by adjoining a root of $x^3+10x+1 = 0$ to $\boldsymbol{Q}$. Since the discriminant of the polynomial x^3-ax+b is $D = 4a^3-27b^2$, then $D = 4(-10)^3-27(1)^2 = -4027$ for the polynomial $x^3+10x+1$. It follows that $F = \boldsymbol{Q}(\sqrt{-4027})$ and that K/F is unramified (since D is square free). From Theorem 3.4, $\operatorname{rank} S_L = S_F - 1$. By [14], Table 1, $\operatorname{rank} S_F = 2$. So $\operatorname{rank} S_L = 1$.

For our next example we let L be a cubic extension of $\boldsymbol{Q}$ obtained by adjoining a root of $x^3-3\cdot 13x+2\cdot 13\cdot 17 = 0$ to $\boldsymbol{Q}$. The discriminant of this polynomial is $D = 2^4\cdot 3^4\cdot 13^2\cdot(-23)$. Then $F = \boldsymbol{Q}(\sqrt{-23})$. The rational primes which ramify totally in $L/\boldsymbol{Q}$ are 3 and 13 (here we are using results from [9] and [13]). In F, both 3 and 13 decompose. We write $(13) = \mathfrak{p}_1\mathfrak{p}_2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_4$, where $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ are distinct prime ideals of F. Furthermore $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ are the prime ideals of F which ramify in K/F. So $t = 4$. Now S_F is a cyclic group of order 3 (see [2], Table 4). In fact the ideal class group C_F is cyclic of order 3. So $r = \operatorname{rank} S_F = 1$, and $h = |C_F/S_F| = 1$. Now let Z be the subgroup of S_F generated by $\operatorname{cl}_F(\mathfrak{p}_1^h\mathfrak{p}_2^{2h})$ and $\operatorname{cl}_F(\mathfrak{p}_3^h\mathfrak{p}_4^{2h})$; i.e., by $\operatorname{cl}_F(\mathfrak{p}_1\mathfrak{p}_2^2)$ and $\operatorname{cl}_F(\mathfrak{p}_3\mathfrak{p}_4^2)$ since $h = 1$. We claim that $Z = S_F$. It suffices to show that either $\operatorname{cl}_F(\mathfrak{p}_1\mathfrak{p}_2^2) \neq 1$ or $\operatorname{cl}_F(\mathfrak{p}_3\mathfrak{p}_4^2) \neq 1$ since S_F is cyclic of order 3. Suppose $\operatorname{cl}_F(\mathfrak{p}_1\mathfrak{p}_2^2) = 1$. Since $\mathfrak{p}_1\mathfrak{p}_2 = (13)$, which is principal, then $\operatorname{cl}_F(\mathfrak{p}_1\mathfrak{p}_2^2) = 1$ implies $\operatorname{cl}_F(\mathfrak{p}_2) = 1$.

So $\mathfrak{p}_2 = \left(\dfrac{x+y\sqrt{-23}}{2}\right)$ for some $x, y \in \boldsymbol{Z}$. But then

$$\left(\frac{x^2+23y^2}{4}\right) = \mathfrak{N}_{F/\boldsymbol{Q}}\left(\frac{x+y\sqrt{-23}}{2}\right) = \mathfrak{N}_{F/\boldsymbol{Q}}(\mathfrak{p}_2) = (13),$$

which implies that $x^2+23y^2 = 52$. However this equation has no solutions $x, y \in \boldsymbol{Z}$. Hence we must have $\operatorname{cl}_F(\mathfrak{p}_2) \neq 1$, which implies $\operatorname{cl}_F(\mathfrak{p}_1\mathfrak{p}_2^2) \neq 1$, and then $Z = S_F$. So

$$z = \operatorname{rank} Z/(Z\cap S_F^3) = \operatorname{rank} S_F/(S_F\cap S_F^3) = \operatorname{rank} S_F/S_F^3 = 1.$$

We remark that the same procedure we used on $\mathfrak{p}_2$ can be used on $\mathfrak{p}_1$, $\mathfrak{p}_3$, and $\mathfrak{p}_4$ to show that $\operatorname{cl}_F(\mathfrak{p}_1) \neq 1$, $\operatorname{cl}_F(\mathfrak{p}_3) \neq 1$, and $\operatorname{cl}_F(\mathfrak{p}_4) \neq 1$. Thus far we have determined that $r = 1$, $t = 4$, and $z = 1$. In Theorem 3.5 we must still compute $\operatorname{rank}[(x_j, K/F)_{\mathfrak{p}_i}]$, $1 \leqslant i \leqslant t-1$, $0 \leqslant j \leqslant s$. Now $x_0 = e = 1$ since F is imaginary quadratic and $\neq \boldsymbol{Q}(\sqrt{-3})$. For $1 \leqslant j \leqslant s$, $(x_j) = \mathfrak{N}_{K/F}\mathfrak{A}_j$, where the $\mathfrak{A}_j$ can be found using the procedure that is given in Section 3 (see the discussion following the proof of Theorem 3.4). In that procedure we first find ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ of F whose ideal classes generate

$$_NS_F = \{a \in S_F \mid N_r(a) = 1\} = \{a \in S_F \mid a^3 = 1\}.$$

Since $r = 1$ and S_F is cyclic of order 3, we may take $\mathfrak{A}_1$ to be any ideal of F whose ideal class is a nontrivial element of S_F. For convenience, we take $\mathfrak{A}_1 = \mathfrak{p}_3$. Since $\mathfrak{N}_{K/F}\mathfrak{p}_3 = \mathfrak{p}_3^3 = \left(\dfrac{x+y\sqrt{-23}}{2}\right)$ for some $x, y \in \boldsymbol{Z}$, and

$$\left(\frac{x^2+23y^2}{4}\right) = \mathfrak{N}_{F/\boldsymbol{Q}}\left(\frac{x+y\sqrt{-23}}{2}\right) = \mathfrak{N}_{F/\boldsymbol{Q}}\mathfrak{p}_3^3 = (3^3),$$

we may take $x = 4$ and $y = 2$. So if we let $x_1 = \dfrac{4+2\sqrt{-23}}{2} = 2+\sqrt{-23}$, we get $(x_1) = \mathfrak{N}_{K/F}\mathfrak{p}_3$. Next we let $\mathfrak{P}_i$ be the unique prime of K above $\mathfrak{p}_i$, $1 \leqslant i \leqslant 4$, and we consider $\operatorname{cl}_K(\mathfrak{P}_1\mathfrak{P}_2^2)$ and $\operatorname{cl}_K(\mathfrak{P}_3\mathfrak{P}_4^2)$. We note that

$$N_r[\operatorname{cl}_K(\mathfrak{P}_1\mathfrak{P}_2^2)] = \operatorname{cl}_F(\mathfrak{p}_1\mathfrak{p}_2^2) \notin S_F^3 = \{1\},$$

and

$$N_r[\operatorname{cl}_K(\mathfrak{P}_3\mathfrak{P}_4^2)] = \operatorname{cl}_F(\mathfrak{p}_3\mathfrak{p}_4^2) \notin S_F^3 = \{1\}.$$

However, by interchanging $\mathfrak{p}_1$ and $\mathfrak{p}_2$ if necessary, we may assume $\operatorname{cl}_F(\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_4^2) = 1$, and then $N_r[\operatorname{cl}_K(\mathfrak{P}_1\mathfrak{P}_2^2\mathfrak{P}_3\mathfrak{P}_4^2)] = 1 \in S_F^3$. So we may take $\mathfrak{A}_2 = \mathfrak{P}_1\mathfrak{P}_2^2\mathfrak{P}_3\mathfrak{P}_4^2$, and it is easy to check that $(x_2) = \mathfrak{N}_{K/F}\mathfrak{A}_2$ if $x_2 = 3\cdot 13\cdot(4+\sqrt{-23})$. We recall that we want to compute rank

$[(x_j, K/F)_{\mathfrak{p}_i}]$, $1 \leqslant i \leqslant 3$, $0 \leqslant j \leqslant 2$, and we have found x_0, x_1, and x_2. As we pointed out at the start of this section, we may actually use cubic Hilbert symbols. To do this, we must find $x_{\mathfrak{p}_i} \in F_{\mathfrak{p}_i}$ such that $K_{\mathfrak{P}_i} = F_{\mathfrak{p}_i}(\sqrt[3]{x_{\mathfrak{p}_i}})$ for $i = 1, 2$ and $x_{\mathfrak{p}_3} \in F_{\mathfrak{p}_3}(\zeta)$ such that $K_{\mathfrak{P}_3}(\zeta) = F_{\mathfrak{p}_3}(\zeta, \sqrt[3]{x_{\mathfrak{p}_3}})$. Since $K_{\mathfrak{P}_i}$ is generated over $F_{\mathfrak{p}_i}$ by a root of $x^3 - 3 \cdot 13x + 2 \cdot 13 \cdot 17 = 0$ for each i, then it can be proved that we may take $x_{\mathfrak{p}_i} = -\frac{b}{2} + \left(\frac{b^2}{4} - \frac{a^3}{27}\right)^{1/2}$ with $a = 3 \cdot 13$ and $b = 2 \cdot 13 \cdot 17$. Furthermore it can be proved that $x_{\mathfrak{p}_1} = 13y_1^3$ for some $y_1 \in F_{\mathfrak{p}_1}$; $x_{\mathfrak{p}_2} = 13y_2^3$ for some $y_2 \in F_{\mathfrak{p}_2}$; and $x_{\mathfrak{p}_3} = \eta_1 \eta_3^2 y_3^3$, where $\eta_1 = 1 - (1 - \zeta) = \zeta$, $\eta_3 = 1 - (1 - \zeta)^3$, and $y_3 \in F_{\mathfrak{p}_3}(\zeta)$. Then our matrix elements can be computed as follows (cf. [1] or [4]):

$$(1, 13)_{\mathfrak{p}_1} = 1 \quad (2 + \sqrt{-23}, 13)_{\mathfrak{p}_1} = \zeta^2 \quad (3 \cdot 13 \cdot (4 + \sqrt{-23}), 13)_{\mathfrak{p}_1} = \zeta$$
$$(1, 13)_{\mathfrak{p}_2} = 1 \quad (2 + \sqrt{-23}, 13)_{\mathfrak{p}_2} = \zeta^2 \quad (3 \cdot 13 \cdot (4 + \sqrt{-23}), 13)_{\mathfrak{p}_2} = \zeta$$
$$(1, \eta_1 \eta_3^2)_{\mathfrak{l}} = 1 \quad (2 + \sqrt{-23}, \eta_1 \eta_3^2)_{\mathfrak{l}} = \zeta^2 \quad (3 \cdot 13 \cdot (4 + \sqrt{-23}), \eta_1 \eta_3^2)_{\mathfrak{l}} = \zeta$$

where ζ is a primitive cube root of unity, and $\mathfrak{l}$ is the unique prime idea of $F_{\mathfrak{p}_3}(\zeta)$ above $\mathfrak{p}_3$. So $\operatorname{rank}[(x_j, K/F)_{\mathfrak{p}_i}] = 1$. Then

$$\begin{aligned} \operatorname{rank} S_L &= r + t - 1 - z - \operatorname{rank}[(x_j, K/F)_{\mathfrak{p}_i}] \\ &= 1 + 4 - 1 - 1 - 1 = 2. \end{aligned}$$

For our final example we let L be a cubic extension of $\boldsymbol{Q}$ generated over $\boldsymbol{Q}$ by a root of $x^3 - 2 \cdot 5 \cdot 7x + 2 \cdot 3 \cdot 5 \cdot 7 = 0$. The discriminant of this polynomial is $D = 2^2 \cdot 5^2 \cdot 7^2 \cdot 37$. So $F = \boldsymbol{Q}(\sqrt{37})$. The rational primes which ramify totally in $L/\boldsymbol{Q}$ are 2, 5, and 7. In F, 2 and 5 remain prime, and 7 decomposes. We let $(7) = \mathfrak{p}_1\mathfrak{p}_2$, $(5) = \mathfrak{p}_3$, and $(2) = \mathfrak{p}_4$, where $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ are distinct prime ideals of F, and they are the prime ideals of F which ramify in K/F. So $t = 4$. By [2], Table 1, the ideal class group C_F is trivial. So S_F is trivial, and Theorem 3.6 applies. We need to compute rank $[(x_j, K/F)_{\mathfrak{p}_i}]$. Now $x_0 = 6 + \sqrt{37}$, the fundamental unit of F. Since $h = |C_F/S_F| = 1$ and $S_F = \{1\}$, we may take $\mathfrak{A}_1 = \mathfrak{P}_1\mathfrak{P}_2^2$, where $\mathfrak{P}_i$ is the unique prime ideal of K above $\mathfrak{p}_i$ for each i. Then it is easy to show that $\mathfrak{N}_{K/F}\mathfrak{A}_1 = (x_1)$ if $x_1 = \frac{1}{2} \cdot 7 \cdot (19 - 3\sqrt{37})$. So we have $x_0 = 6 + \sqrt{37}$ and $x_1 = \frac{1}{2} \cdot 7 \cdot (19 - 3\sqrt{37})$. Next we want to find $x_{\mathfrak{p}_i} \in F_{\mathfrak{p}_i}$ such that $K_{\mathfrak{P}_i} = F_{\mathfrak{p}_i}(\sqrt[3]{x_{\mathfrak{p}_i}})$, $1 \leqslant i \leqslant 3$. For our polynomial equation $x^3 - 2 \cdot 5 \cdot 7x + 2 \cdot 3 \cdot 5 \cdot 7 = 0$, we may take $x_{\mathfrak{p}_i} = -\frac{b}{2} + \left(\frac{b^2}{4} - \frac{a^3}{27}\right)^{1/2}$ with $a = 2 \cdot 5 \cdot 7$ and $b = 2 \cdot 3 \cdot 5 \cdot 7$. It can be proved that $x_{\mathfrak{p}_1} = 14y_1^3$ for some $y_1 \in F_{\mathfrak{p}_1}$;

$x_{\mathfrak{p}_2} = 14y_2^3$ for some $y_2 \in F_{\mathfrak{p}_2}$; and $x_{\mathfrak{p}_3} = 5y_3^3$ for some $y_3 \in F_{\mathfrak{p}_3}$. Then our matrix elements can be computed as follows:

$$(6 + \sqrt{37}, 14)_{\mathfrak{p}_1} = \zeta^2 \quad \left(\tfrac{1}{2} \cdot 7 \cdot (19 - 3\sqrt{37}), 14\right)_{\mathfrak{p}_1} = 1$$
$$(6 + \sqrt{37}, 14)_{\mathfrak{p}_2} = \zeta^2 \quad \left(\tfrac{1}{2} \cdot 7 \cdot (19 - 3\sqrt{37}), 14\right)_{\mathfrak{p}_2} = 1$$
$$(6 + \sqrt{37}, 5)_{\mathfrak{p}_3} = \zeta \quad \left(\tfrac{1}{2} \cdot 7 \cdot (19 - 3\sqrt{37}), 5\right)_{\mathfrak{p}_3} = \zeta$$

where ζ is a primitive cube root of unity. So $\operatorname{rank}[(x_j, K/F)_{\mathfrak{p}_i}] = 2$, and by Theorem 3.6

$$\operatorname{rank} S_L = t - 1 - \operatorname{rank}[(x_j, K/F)_{\mathfrak{p}_i}] = 4 - 1 - 2 = 1.$$

Remark. In a sequel to [3], Callahan has obtained results which provide lower and upper bounds for the ranks of the 3-class groups of all non-Galois cubic extensions of the rational numbers.

Remark. In the paper *On l-class groups of certain number fields* (to appear), Gerth has obtained lower and upper bounds for the ranks of the l-class groups of certain number fields, where l is an odd prime. Those results can be considered as generalizations of some of the results on the 3-class groups of cubic fields that are given in this paper. For the special fields considered in that paper, the ranks of the l-class groups depend upon certain groups B_1, B_2/B_1, ..., B_{l-1}/B_{l-2}. For $l = 3$, only B_1 and B_2/B_1 are needed. (B_1 corresponds to ${}_ND$ and B_2 corresponds to $B \cap {}_NS_K$ in this paper.) For $l > 3$, it is usually very difficult to determine B_3/B_2, ..., B_{l-1}/B_{l-2} explicitly.

References

[1] E. Artin and J. Tate, *Class Field Theory*, Benjamin, New York 1967.

[2] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York 1966.

[3] T. Callahan, *The 3-class groups of non-Galois cubic fields I*, Mathematika 21 (1974), pp. 72–89.

[4] J. W. Cassels and A. Fröhlich, *Algebraic Number Theory*, Thompson Book Company, Washington, D. C., 1967.

[5] F. Gerth, *On 3-class groups of pure cubic fields*, to appear in Journ. Reine Angew. Math.

[6] G. Gras, *Sur les l-classes d'idéaux des extensions non galoisiennes de Q de degré premier impair l a clôture galoisienne diédrale de degré 2l*, J. Math. Soc. Japan 26 (1974), pp. 677–685.

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

[8] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Ia*, Jber. Deutsch. Math.-Verein 36 (1927), pp. 233–311.

[9] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf Klassenkörpertheoretischer Grundlage*, Math. Zeitschr. 31 (1930), pp. 565–582.
[10] S. Kobayashi, *On the 3-rank of the ideal class groups of certain pure cubic fields*, J. Fac. Sci. Univ. Tokyo, Sec. IA 20 (1973), p. 209–216.
[11] — *On the 3-rank of the ideal class groups of certain pure cubic fields II*, to appear.
[12] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970.
[13] H. Reichardt, *Arithmetische Theorie der kubischen Körper als Radikalkörper*, Monatshefte Math. Phys. 40 (1933), pp. 323–350.
[14] D. Shanks, *On Gauss's class number problems*, Math. Comp. 23 (1969), pp. 151–163.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TEXAS
Austin, Texas, U.S.A.

Received on 25. 9. 1974 (623)

ACTA ARITHMETICA
XXX (1976)

Filtration de K^*/K^{*p} et ramification sauvage

par

THONG NGUYEN-QUANG-DO (Paris)

Si k est un corps local de caractéristique 0, de caractéristique résiduelle $p \neq 0$, le groupe multiplicatif k^*/k^{*p} est filtré de façon naturelle par les sous-groupes $U_k^i k^{*p}/k^{*p}$ (sections 1 et 2). L'objet principal de cet article est d'étudier comment cette filtration se transforme dans une extension galoisienne K/k, plus précisément via l'homomorphisme naturel η: $k^*/k^{*p} \to K^*/K^{*p}$ (section 3): la façon dont η transforme la fonction d'ordre de la filtration est décrite par une fonction $\delta_{K/k}$ attachée à la fonction classique $\psi_{K/k}$ et jouissant de propriétés analogues. Dans la section 4, nous appliquons les résultats obtenus à la construction de p-extensions cycliques de k ayant des nombres de ramification donnés.

0. Notations générales. Dans toute la suite, sauf mention expresse du contraire, nous entendrons par „corps local" k, un corps k qui est complet pour une valuation discrète, qui est de caractéristique 0, et dont le corps résiduel $\bar{k}$ est *parfait*, de caractéristique $p \neq 0$.

Nous noterons ord_k la valuation additive normalisée de k, i.e. telle que $\mathrm{ord}_k k = \mathbf{Z} \cup \{\infty\}$.

Nous poserons $e_k = \mathrm{ord}_k p$ et $e'_k = e_k/(p-1)$ (c'est un entier si k contient les racines p-ièmes de l'unité). Pour tout $x \in k^*$, il sera commode de noter: $d_k(x) = \mathrm{ord}_k(1-x)$.

Comme d'habitude, nous introduisons les groupes multiplicatifs:

$U_k = U_k^0 = \{x \in k^*;\ \mathrm{ord}_k x = 0\}$,

$U_k^i = \{x \in k^*;\ d_k(x) \geqslant i\}$ pour tout entier $i \geqslant 1$.

Enfin, pour tout entier $i \geqslant 0$, nous noterons $\overline{U}_k^i = U_k^i/U_k^{i+1}$. On sait que $\overline{U}_k^0 \cong \bar{k}^*$ (groupe multiplicatif de $\bar{k}$) et que, pour tout entier $i \geqslant 1$, $\overline{U}_k^i$ est isomorphe au groupe additif de $\bar{k}$ (de façon non canonique, par le choix d'une uniformisante).

Dans la suite, lorsqu'il n'y aura pas d'ambiguïté possible, on sous-entendra l'indice k, et l'on écrira: $\mathrm{ord}(x)$, $d(x)$, e, e', etc... au lieu de $\mathrm{ord}_k(x)$, $d_k(x)$, e_k, e'_k, etc...