BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 3, May 1973

RANKS OF SYLOW 3-SUBGROUPS OF IDEAL CLASS GROUPS OF CERTAIN CUBIC FIELDS[1]

BY FRANK GERTH III

Communicated by Oscar Goldman, November 20, 1972

1. **Introduction.** Let Q denote the field of rational numbers, and let l be a prime number. Let S be a finite abelian l-group. We define

$$\text{rank } S = \dim_{F_l}(S \otimes_{Z_l} F_l),$$

where Z_l is the ring of the l-adic integers, and F_l is the finite field of l elements.

The following classical theorem can be proved using the genus theory of Gauss.

THEOREM 1.1 (Cf. [**5**, THEOREM 4]). *Let $H = Q(D^{1/2})$ be a quadratic extension of Q with discriminant D, and let d denote the number of distinct rational primes dividing D. Let S_H denote the Sylow 2-subgroup of the ideal class group of H (in the wide sense). Then*

(i) *if H is imaginary quadratic,* rank $S_H = d - 1$,

(ii) *if H is real quadratic,*

$$\text{rank } S_H = d - 1 \quad \text{if no prime } p \equiv -1 \pmod 4 \text{ divides } D,$$

$$= d - 2 \quad \text{if some prime } p \equiv -1 \pmod 4 \text{ divides } D.$$

In this paper we present analogous results for the ranks of the Sylow 3-subgroups of the ideal class groups of the following fields:

(i) cyclic cubic extensions of $Q(\zeta)$, where ζ is a primitive cube root of unity,

(ii) pure cubic extensions of Q (cf. [**1**] and [**2**]),

(iii) cyclic cubic extensions of Q.

2. **Cyclic cubic extensions of $Q(\zeta)$.** Let $F = Q(\zeta)$, where ζ is a primitive cube root of unity. Let K/F be a cyclic cubic extension. By Kummer theory $K = F(x^{1/3})$ for some $x \in F$. Let M be the maximal abelian unramified extension of K (i.e., the Hilbert class field of K), and let M_1 be the maximal abelian extension of F contained in M. (M_1 is called the genus field of K/F.) Let C_K denote the ideal class group of K, and let S_K

AMS (MOS) subject classifications (1970). Primary 12A30, 12A35, 12A65; Secondary 12A25, 12A50.

[1] The results announced here are contained in the author's Ph.D. thesis, written under the supervision of Professor Kenkichi Iwasawa at Princeton University.

denote the Sylow 3-subgroup of C_K. Let τ be a generator of the cyclic group $\mathrm{Gal}(K/F)$. Let $C_K^{1-\tau} = \{a^{1-\tau} | a \in C_K\}$ and $C_K^{(\tau)} = \{a \in C_K | a^\tau = a\}$. ($C_K^{1-\tau}$ is called the principal genus of K/F, and $C_K^{(\tau)}$ is called the group of ambiguous ideal classes of K/F.) Define $S_K^{1-\tau} = \{a^{1-\tau} | a \in S_K\}$ and $S_K^{(\tau)} = \{a \in S_K | a^\tau = a\}$.

Class field theory shows that $\mathrm{Gal}(M/K) \cong C_K$. The following results are also known (cf. [**3**, p. 24] and [**5**, pp. VII-3, VII-13]).

LEMMA 2.1. $\mathrm{Gal}(M/M_1) \cong C_K^{1-\tau}$, $\mathrm{Gal}(M_1/K) \cong C_K/C_K^{1-\tau} \cong S_K/S_K^{1-\tau}$, *and* $\mathrm{rank}\, S_K^{(\tau)} = \mathrm{rank}\, S_K/S_K^{1-\tau}$.

Now

$$\mathrm{rank}\, S_K = \mathrm{rank}\, S_K/S_K^3 = \mathrm{rank}\, S_K/S_K^{1-\tau} + \mathrm{rank}\, S_K^{1-\tau}/S_K^3.$$

(*Note.* For $K = F(x^{1/3})$, it can be shown that $S_K^3 \subseteq S_K^{1-\tau}$; hence the above groups are well defined.) The next result is a consequence of [**4**, p. 274].

LEMMA 2.2. *Let* $t = \mathrm{rank}\, S_K^{(\tau)} = \mathrm{rank}\, S_K/S_K^{1-\tau}$. *Then* $t = d + q - 2$, *where*

$$d = \textit{number of ramified primes in } K/F,$$

$$q = 1 \quad \textit{if } \zeta \in N_{K/F}K,$$

$$= 0 \quad \textit{if } \zeta \notin N_{K/F}K$$

and $N_{K/F}$ *is the norm map from* K *to* F.

REMARK. The t in Lemma 2.2 is analogous to $\mathrm{rank}\, S_H$ in Theorem 1.1 since $\mathrm{rank}\, S_H = \mathrm{rank}\, S_H/S_H^2 = \mathrm{rank}\, S_H/S_H^{1-\sigma}$, where σ is a generator of $\mathrm{Gal}(H/\boldsymbol{Q})$. Thus the cyclic cubic case K/F is more complicated than the quadratic case $H/\boldsymbol{Q}$ because we must also consider $\mathrm{rank}\, S_K^{1-\tau}/S_K^3$.

Our problem then is to compute $\mathrm{rank}\, S_K^{1-\tau}/S_K^3$. Let

$$\delta: S_K/S_K^{1-\tau} \to S_K^{1-\tau}/S_K^3,$$

$$a \bmod S_K^{1-\tau} \mapsto a^{1-\tau} \bmod S_K^3.$$

This map is surjective, and $\ker \delta = (S_K^{(\tau)} \cdot S_K^{1-\tau})/S_K^{1-\tau}$. Let

$$s = \mathrm{rank}(S_K^{(\tau)} \cdot S_K^{1-\tau})/S_K^{1-\tau}.$$

Then $\mathrm{rank}\, S_K^{1-\tau}/S_K^3 = t - s$. So we have established the following result.

PROPOSITION 2.3. $\mathrm{rank}\, S_K = 2t - s$, *where* t *is given by Lemma* 2.2, *and* $s = \mathrm{rank}(S_K^{(\tau)} \cdot S_K^{1-\tau})/S_K^{1-\tau}$.

The computation of s requires further discussion. We recall that $\mathrm{Gal}(M_1/K) \cong S_K/S_K^{1-\tau}$, which is an elementary abelian 3-group of rank t. Then by Kummer theory $M_1 = K(x_1^{1/3}, \ldots, x_t^{1/3})$, $x_i \in K$. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ be ideals of K whose ideal classes $\mathrm{cl}(\mathfrak{a}_1), \ldots, \mathrm{cl}(\mathfrak{a}_t)$ form a basis for $S_K^{(\tau)}$. (Note that $S_K^{(\tau)}$ is also an elementary abelian 3-group of rank t.)

PROPOSITION 2.4. *s = rank of the matrix (α_{ij}), where $\alpha_{ij} \in \boldsymbol{F}_3$ = finite field of 3 elements, $1 \leqq i \leqq t$, $1 \leqq j \leqq t$; $\zeta^{\alpha_{ij}} = (x_i^{1/3})^{\mu_{ij}-1}$ (power residue symbol); μ_{ij} = Artin symbol $(\mathfrak{P}_j, K(x_i^{1/3})/K)$.*

PROOF. Let $\psi : S_K^{(\tau)} \to \boldsymbol{F}_3^t$ be the composite map

$$S_K^{(\tau)} \to S_K \to S_K/S_K^{1-\tau} \xrightarrow{\sim} \mathrm{Gal}(M_1/K)$$

$$\xrightarrow{\sim} \mathrm{Gal}(K(x_1^{1/3})/K) \times \cdots \times \mathrm{Gal}(K(x_t^{1/3})/K) \cong \boldsymbol{F}_3^t,$$

where the first map is the natural inclusion; the second map is the natural projection; and the last three maps are isomorphisms. ($\boldsymbol{F}_3^t$ denotes a vector space of dimension t over $\boldsymbol{F}_3$.) Then $s = \mathrm{rank}(S_K^{(\tau)} \cdot S_K^{1-\tau})/S_K^{1-\tau} = \mathrm{rank}\,\psi = \mathrm{rank}(\alpha_{ij})$, since (α_{ij}) is the matrix of ψ with respect to the bases $\{\mathrm{cl}(\mathfrak{a}_1), \ldots, \mathrm{cl}(\mathfrak{a}_t)\}$ and $\{x_1, \ldots, x_t\}$.

THEOREM 2.5. *$\mathrm{rank}\, S_K = 2t - s$, where t is given by Lemma 2.2, and s is specified by Proposition 2.4.*

To apply Theorem 2.5, we must find $x_1, \ldots, x_t$, $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ and then compute the appropriate power residue symbols. [7] shows how to find $x_1, \ldots, x_t$. On the other hand, finding a basis $\{\mathrm{cl}(\mathfrak{a}_1), \ldots, \mathrm{cl}(\mathfrak{a}_t)\}$ of $S_K^{(\tau)}$ can be very difficult. However it can be shown that a set of generators of $S_K^{(\tau)}$ is sufficient for the calculations, and the ideal classes of the prime ideals that ramify in K/F frequently comprise such a generating set. Furthermore it can be shown that the power residue symbol calculations, which involve arithmetic in K, can be replaced by cubic Hilbert symbol computations that involve only arithmetic in F.

At this point we could summarize the above results in a theorem which would explicitly state how to compute $\mathrm{rank}\, S_K$ for a cyclic cubic extension K of $\boldsymbol{Q}(\zeta)$; i.e., we could specify explicitly the x_i's, the generators of $S_K^{(\tau)}$, and the appropriate Hilbert symbols. However such a theorem would be very lengthy, and we defer its presentation to another time. In the remaining two sections of this paper, we present results analogous to Theorem 2.5 for pure cubic extensions of $\boldsymbol{Q}$ and for cyclic cubic extensions of $\boldsymbol{Q}$.

3. **Pure cubic fields.** Let k be a pure cubic field; i.e., $k = \boldsymbol{Q}(n^{1/3})$, where n is a rational integer. (Note that n can be chosen to be a positive, cube-free integer.) Let $K = k \cdot F$, where $F = \boldsymbol{Q}(\zeta)$. Then K is a cyclic cubic extension of F, and hence the results of §2 apply to K. So $\mathrm{rank}\, S_K = 2t - s$,

where t is given by Lemma 2.2, and s is given by Proposition 2.4. Let σ be a generator of $\mathrm{Gal}(K/k)$, and let S_k denote the Sylow 3-subgroup of the ideal class group of k. Then $S_k = \{a \in S_K | a^\sigma = a\}$, and furthermore $S_K \cong S_k \times S_K^-$, where $S_K^- = \{a \in S_K | a^\sigma = a^{-1}\}$. It is now possible to apply some tricks of Kummer duality theory (cf. [6]) to find rank S_k. The main result for pure cubic fields can be expressed as follows.

THEOREM 3.1. *Let $k = \boldsymbol{Q}(n^{1/3}) \neq \boldsymbol{Q}$, where n is a rational integer. Let $F = \boldsymbol{Q}(\zeta)$, where ζ is a primitive cube root of unity, and let $K = k \cdot F$. Then* rank $S_k = t - s_1$, *where t is given by Lemma* 2.2, *and s_1 is the rank of a certain matrix all of whose elements can be determined by Hilbert symbol computations in F.*

REMARK. It is possible to specify explicitly the elements in the matrix that is mentioned in Theorem 3.1. We shall do this in another paper.

The following theorem, which bears a striking resemblance to Theorem 1.1, is a special case of Theorem 3.1.

THEOREM 3.2. *Let $k = \boldsymbol{Q}(n^{1/3}) \neq \boldsymbol{Q}$, where $n = 3^{e_0} q_1^{e_1} \dots q_J^{e_J}$, each q_i is a rational prime $\equiv -1 \pmod 3$, and each e_i is a nonnegative rational integer. Let d denote the number of totally ramified primes in $k/\boldsymbol{Q}$. Then*

$$\begin{aligned} \text{rank } S_k &= d - 1 \quad \text{if each } q_i \equiv -1 \pmod 9 \\ &= d - 2 \quad \text{if some } q_i \equiv 2 \text{ or } 5 \pmod 9. \end{aligned}$$

4. **Cyclic cubic extensions of $\boldsymbol{Q}$.** Let k be a cyclic cubic extension of $\boldsymbol{Q}$. Let $F = \boldsymbol{Q}(\zeta)$ and $K = k \cdot F$. The results of §2 apply to K, and again certain tricks of Kummer duality theory can be used to find rank S_k. The main result is given below.

THEOREM 4.1. *Let k be a cyclic cubic extension of $\boldsymbol{Q}$. Then* rank $S_k = 2(d - 1) - s_2$, *where d is the number of ramified primes in $k/\boldsymbol{Q}$, and s_2 is the rank of a certain matrix all of whose elements can be determined by Hilbert symbol computations in $\boldsymbol{Q}(\zeta)$, where ζ is a primitive cube root of unity.*

REMARK. In another paper we shall specify explicitly the elements of the matrix that is mentioned in Theorem 4.1.

REFERENCES

1. P. Barrucand and H. Cohn, *A rational genus, class number divisibility, and unit theory for pure cubic fields*, J. Number Theory **2** (1970), 7–21. MR **40** #2643.

2. ———, *Remarks on principal factors in a relative cubic field*, J. Number Theory **3** (1971), 226–239. MR **43** #1945.

3. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. I, Jber. Deutsch. Math.-Verein. **35** (1926), 1–55.

4. ———, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. Ia, Jber. Deutsch. Math.-Verein. **36** (1927), 233–311.

5. C. S. Herz, *Construction of class fields*, Seminar on Complex Multiplication, Lecture Notes in Math., vol. 21, Springer-Verlag, Berlin and New York, 1966. MR **34** #1278.

6. H. W. Leopoldt, *Zur Struktur der l-Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199** (1958), 165–174. MR **20** #3116.

7. H. Wada, *On cubic Galois extensions of* $\boldsymbol{Q}(\sqrt{-3})$, Proc. Japan Acad. **46** (1970), 397–400.

Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104