J. Math. Soc. Japan
Vol. 47, No. 1, 1995

Algebraic number fields with the discriminant equal to that of a quadratic number field

By Takeshi KONDO

(Received May 12, 1993)

§ 1. Introduction.

The purpose of the present paper is to prove the following Theorem 1 and Theorem 2.

THEOREM 1. *Let F be an algebraic number field of degree n and $d(F)$ be the discriminant of F. Let K be the Galois closure of F over $\boldsymbol{Q}$, the field of rational numbers. If $d(F)$ is equal to the discriminant of a quadratic number field, i.e., $d(F)$ is not a square and equals the discriminant of the field $\boldsymbol{Q}(\sqrt{d(F)})$, then the following hold*:

(a) *the Galois group of K over $\boldsymbol{Q}$ is isomorphic to Σ_n, the symmetric group of degree n, and*

(b) *the extension $K/\boldsymbol{Q}(\sqrt{d(F)})$ is unramified (at all finite primes of $\boldsymbol{Q}(\sqrt{d(F)})$).*

This is a generalization of theorems which were proved by several authors (cf. [**K**], [**N**], [**O**], [**Y1**] and [**Y2**]) under the assumption that $d(F)$ is square free.

COROLLARY. *Let $f(t)$ be a monic irreducible polynomial of degree n with rational integral coefficients and $d(f)$ be the discriminant of $f(t)$. Let $K=\boldsymbol{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)$, the splitting field of $f(t)$ over $\boldsymbol{Q}$, where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are the roots of an equation $f(t)=0$. If $d(f)$ is equal to the discriminant of a quadratic number field $\boldsymbol{Q}(\sqrt{d(f)})$, then*

(a) *the Galois group of K over $\boldsymbol{Q}$ is isomorphic to Σ_n,*

(b) *the extension $K/\boldsymbol{Q}(\sqrt{d(f)})$ is unramified,*

(c) *$\mathcal{O}_K=\boldsymbol{Z}[\alpha_1, \alpha_2, \cdots, \alpha_n]$, where $\mathcal{O}_K$ is the ring of integers in K.*

(a) and (b) of Corollary are immediate from Th. 1, and (c) follows from a result of E. Maus [**M**].

THEOREM 2. *Let F and $d(F)$ be as in Theorem 1. Then the following statements* (A) *and* (B) *are equivalent*:

(A) *$d(F)$ is equal to the discriminant of a quadratic number field $\boldsymbol{Q}(\sqrt{d(F)})$.*

(B) *For every prime p of $d(F)$, p has exactly one ramified prime divisor in F and its ramification index (resp. residue class degree) is two (resp. one).*

REMARK. If $p \| d(F)$, i.e., $d(F)$ is divisible by exactly the first power of p, p satisfies the condition in (B) of Th. 2 (cf. the proof of Case 1 in § 3). Also see Lemma 4 in § 4.

In an interesting paper of Yamamura [**Y2**, p. 107], it is stated that, under the assumption (B), (a) and (b) of Th. 1 hold, although the proof is omitted. So it can be said that Th. 1 is a consequence of Th. 2. But, in the present paper, Th. 1 and Th. 2 will be proved at the same time.

§ 2. Some Lemmas.

The following two lemmas are well known in algebraic number theory.

LEMMA 1 (Dedekind). *Let F be an algebraic number field and $\mathfrak{D}$ be the different of F over $\boldsymbol{Q}$. Let $\mathfrak{P}$ be a prime divisor in F of a prime number p, and $\mathfrak{P}^d \| \mathfrak{D}$ and $\mathfrak{P}^e \| p$. Then*

(a) *if $p \nmid e$, then $d=e-1$,*

(b) *if $p^v \| e$ $(v>0)$, then $e \leqq d \leqq ev+e-1$.*

See [**F2**] for the proof.

LEMMA 2 (Van der Waerden). *Let F and K be as in Theorem 1, and Z and T be the decomposition group and the inertia group of a prime divisor in K of a prime number p respectively. Suppose that p has a decomposition in F*

$$p = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g} \qquad N_{L/\boldsymbol{Q}}(\mathfrak{P}_i) = p^{f_i} \quad (i=1, 2, \cdots, g)\,.$$

When the Galois group of K over $\boldsymbol{Q}$ is regarded as a permutation group of degree n (on the set of conjugates of F over $\boldsymbol{Q}$), Z has g orbits each of which is of length $e_i f_i$ and decomposes into f_i T-orbits of length e_i.

See [**W**] or [**F2**] for the proof.

LEMMA 3. *Let F be an algebraic number field. Assume that F has the discriminant equal to that of a quadratic number field $\boldsymbol{Q}(\sqrt{d(F)})$. Then F does not contain any proper intermediate field, i.e., a field L such that $\boldsymbol{Q} \subsetneqq L \subsetneqq F$.*

PROOF. $d(L)^{[F:L]} \mid d(F)$ by a transition property of discriminant, which is impossible unless $d(L)=1$, because $d(F)$ is a discriminant of a quadratic field. But $d(L)=1$ is also impossible by a theorem of Minkowski, unless $L=\boldsymbol{Q}$.

§ 3. The proof of Th. 1 and Th. 2.

3.1. The proof of Th. 1 and a part "(A)$\Rightarrow$(B)" of Th. 2.

Assume that $d(F)$ is equal to the discriminant of $\boldsymbol{Q}(\sqrt{d(F)})$ and $p \mid d(F)$. Suppose that we have factorizations

(1) $p=\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ $N_{L/\boldsymbol{Q}}(\mathfrak{P}_i)=p^{f_i}$ $(i=1, 2, \cdots, g)$,

(2) $\mathfrak{D}_p=\mathfrak{P}_1^{d_1}\mathfrak{P}_2^{d_2}\cdots\mathfrak{P}_g^{d_g}$ ($\mathfrak{D}_p$="p-part" of the different $\mathfrak{D}$ of $F/\boldsymbol{Q}$)

into prime divisors in F.

Case 1, where p is odd. Then $d(F)$ is divisible by exactly the first power of p. By taking norm $N_{F/\boldsymbol{Q}}$ of both sides of (2), we have

$$1=d_1f_1+d_2f_2+\cdots+d_gf_g\,.$$

Therefore we may assume

$$d_1=f_1=1\,,\qquad d_i=0\quad(i\geqq 2)$$

and so, by (a) of Lemma 1, $e_1=2$ and $e_i=1$ $(i\geqq 2)$. Thus in this case the condition (B) of Th. 2 holds. Moreover the inertia group T of a prime divisor in K of $\mathfrak{P}_1$ is a group of order 2 generated by a transposition by Lemma 2. In particular, any prime divisor in $\boldsymbol{Q}(\sqrt{d(F)})$ of p is unramified in K, since $|T|=2$ and p is already ramified in $\boldsymbol{Q}(\sqrt{d(F)})$.

Case 2, where $p=2$. Then $d(F)$ is divisible exactly by 4 or 8.

Subcase 2-1, where $4\| d(F)$. Then we have

$$2=d_1f_1+d_2f_2+\cdots+d_gf_g$$

and also, by (b) of Lemma 1, $d_i\geqq 2$ if $d_i\neq 0$. Thus we may assume

$$d_1=2,\quad f_1=1\ \text{ and }\ d_i=0\quad(i\geqq 2)$$

and then we see $e_1=2$ or 3 and $e_i=1$ $(i\geqq 2)$ from Lemma 1. We must show $e_1=2$. Suppose by way of contradiction that $e_1=3$. Then, by Lemma 2, the inertia group T is a subgroup of Σ_3. But since 2 is ramified in $\boldsymbol{Q}(\sqrt{d(F)})$, we must have $T=\Sigma_3$. This is impossible, because any inertia group has, in general, a normal Sylow p-subgroup ($p=2$ in the present case) while Σ_3 does not. Again we see from Lemma 2 that the inertia group T is a group of order 2 generated by a transposition, and so any prime divisor in $\boldsymbol{Q}(\sqrt{d(F)})$ of p is unramified in K.

Subcase 2-2, where $8\| d(F)$. Then we have

$$3=d_1f_1+d_2f_2+\cdots+d_gf_g\ \text{ and }\ d_i\geqq 2\ \text{ if }\ d_i\neq 0\,.$$

Thus we may assume

$$d_1 = 3, \quad f_1 = 1 \quad \text{and} \quad d_i = 0 \quad (i \geqq 2)$$

and then we see $e_1=2$ and $e_i=1$ $(i \geqq 2)$ from Lemma 1.

Thus, in all cases, we have proved that the inertia group T is a group of order 2 generated by a transposition and so any prime divisor in $\boldsymbol{Q}(\sqrt{d(F)})$ of p is unramified in K. This means that (b) of Th. 1 and a part "(A) $\Rightarrow$ (B)" of Th. 2 hold. A part (a) of Th. 1 follows from Lemma 3. In fact, the Galois group of $K/\boldsymbol{Q}$, considered as a permutation group of degree n, is a primitive permutation group by Lemma 3. It is well known that, if a primitive permutation group contains a transposition, it is a symmetric group. (See also [**Y1**, p. 476].)

3.2. The proof of a part "(B) $\Rightarrow$ (A)" of Th. 2.

Let p be a prime divisor of $d(F)$. Then we may assume $e_1=2$, $f_1=1$ and $e_i=1$ $(i \geqq 2)$. If p is odd, we see $d_1=1$ and $d_i=0$ $(i \geqq 2)$ from (a) of Lemma 1. Then we have $p \| d(F)$. Thus if $d(F)$ is odd, $d(F)$ is a discriminant of a quadratic field. Suppose $p=2$. Then we see $d_1=2$ or 3 and $d_i=0$ $(i \geqq 2)$ from (b) of Lemma 1. If $d_1=3$ then $d(F)$ is a discriminant of a quadratic field. Suppose $d_1=2$. Since the inertia group of a prime divisor in K of 2 is a group of order 2 generated by a transposition by Lemma 2, it induces a nontrivial automorphism on $\boldsymbol{Q}(\sqrt{d(F)})$, because the subgroup of the Galois group of $K/\boldsymbol{Q}$ corresponding to $\boldsymbol{Q}(\sqrt{d(F)})$ consists of even permutations. This means that 2 is ramified in $\boldsymbol{Q}(\sqrt{d(F)})$ and so $d(F)/4 \equiv -1 \bmod 4$. Thus, also in this case, $d(F)$ is a discriminant of a quadratic field.

§ 4. Concluding remarks.

Let $\mathcal{F}_{ur,n}$ be the class of non-conjugate algebraic number fields of degree n which satisfy the conditions (a) and (b) in Th. 1, and let $\mathcal{F}_{qd,n}$ be the class of non-conjugate algebraic number fields of degree n with the discriminant equal to that of a quadratic number field. Theorem 1 shows

$$(*) \qquad \mathcal{F}_{ur,n} \supseteqq \mathcal{F}_{qd,n} .$$

All examples of algebraic number fields in $\mathcal{F}_{ur,n}$ which are obtained in [**F1**], [**O**], [**YY**] and [**U**] belongs to $\mathcal{F}_{qd,n}$. In fact, for such examples, the condition (B) of Th. 2 is satisfied. It is not so difficult to see that the equality hold in (*) if $n \leqq 5$ (see [**Y2**, Remark in p. 107] or Lemmas 4 and 5 below). If $n \geqq 6$, however, the equality does not hold as is seen in Example 1 below. (See also [**N**, Example 2].) It seems to be difficult to state the conditions that an algebraic number field belongs to the family $\mathcal{F}_{ur,n}$ in terms of its discriminant.

In Lemma 4 and 5 below, F is an algebraic number field of degree n and K be the Galois closure of F over $\boldsymbol{Q}$, and the Galois group of the extension $K/\boldsymbol{Q}$ is regarded as a permutation group of degree n (on the set of conjugates of F over $\boldsymbol{Q}$).

LEMMA 4. *The following condition* (C) *is equivalent to* (B) *in Theorem* 2.

(C) *The inertia group of every ramified prime of K is a group of order* 2 *generated by a transposition.*

In particular, if F satisfies (C), *then $F\in\mathfrak{F}_{qd,n}$, i.e., the discriminant $d(F)$ of F is equal to that of $\boldsymbol{Q}(\sqrt{d(F)})$.*

PROOF. This is immediate from Lemma 2.

Furthermore, we have clearly

LEMMA 5. *Assume that $d(F)$ is not square in $\boldsymbol{Q}$. Then the following two statements are equivalent:*

I. *The extension $K/\boldsymbol{Q}(\sqrt{d(F)})$ is unramified.*

II. *The inertia group of every ramified prime of K is a group of order* 2 *generated by an odd permutation.*

As applications of Lemmas 4 and 5, we will exhibit some examples of unramified extensions of quadratic fields which are obtained from fields in $\mathfrak{F}_{ur,n}-\mathfrak{F}_{qd,n}$ or not in $\mathfrak{F}_{ur,n}$.

EXAMPLE 1. Let $f(t)=t^6+t^4-3t^3+t^2+3t+3$, $F=\boldsymbol{Q}(\theta)$, where θ is a root of $f(t)=0$, and K be the splitting field over $\boldsymbol{Q}$ of $f(t)$. Then we have $d(f)=d(F)=-2^3\cdot 3^3\cdot 37\cdot 7577$ and

$$f(t)\equiv(t+1)^2(t^4+t+1) \mod 2$$

$$f(t)\equiv t^2(t+1)^2(t-1)^2 \mod 3\,.$$

Other prime divisors 37 and 7577 of $d(F)$ satisfy the condition in (B) of Th. 2. (Note the remark after Th. 2 in the introduction.) Thus we see from Lemmas 2 and 4 that the condition II of Lemma 5 is satisfied, and so $K/\boldsymbol{Q}(\sqrt{d(f)})$ is unramified. It is easy to see that the Galois group of $K/\boldsymbol{Q}$ is Σ_6. Thus we have $F\in\mathfrak{F}_{ur,n}-\mathfrak{F}_{qd,n}$.

EXAMPLE 2. Let $f(t)=t^6-t^5-t^4+t+1$, F and K be as above. Then we have $d(f)=d(F)=-11691=-3^3\cdot 433$, and $f(t)\equiv(t^3+t^2+2t+1)^2 \mod 3$. Thus, as in Example 1, we see that $K/\boldsymbol{Q}(\sqrt{-3\cdot 433})$ is unramified. We note that the Galois group of $K/\boldsymbol{Q}$ is a group of order 72 which is isomorphic to the wreath product of Σ_3 by Z_2 (cf. [S] for the method of computations of Galois groups), and so $K/\boldsymbol{Q}(\sqrt{-3\cdot 433})$ is an unramified extension with the Galois group isomorphic to a Frobenius group of order 36.

EXAMPLE 3. Let $f(t)=t^7-t^6-t^5+t^4-t^3-t^2+2t+1$, and F and K be as above. Then $d(f)=d(F)=-357911=-71^3$ and $f(t)\equiv(t+15)(t+22)^2(t+47)^2(t+65)^2 \bmod 71$. Therefore, by Lemma 5, $K/\boldsymbol{Q}(\sqrt{-71})$ is unramified. The Galois group of $K/\boldsymbol{Q}$ is isomorphic to a dihedral group of order 14 (cf. [**YK**]), and so $K/\boldsymbol{Q}(\sqrt{-71})$ is an unramified extension with a cyclic group of order 7 as the Galois group. This shows that K is the absolute class field of $\boldsymbol{Q}(\sqrt{-71})$, since the class number of $\boldsymbol{Q}(\sqrt{-71})$ is 7.

Finally, we note that, in Yamamura [**Y2**], very interesting observations are done on the "density" of $\mathcal{F}_{ur,n}$ and $\mathcal{F}_{qd,n}$.

References

[F1] G. Fujisaki, On an example of an unramified Galois extension, (in Japanese), Sûgaku, **9** (1957), 97-99,

[F2] G. Fujisaki, Introduction to Algebraic Number Theory, (in Japanese), Shoukabou, 1975.

[K] K. Komatsu, Square-free discriminants and affect-free equations, Tokyo J. Math., **14** (1991), 57-60.

[M] E. Maus, Computation of integral bases in certain S_n extensions of $\boldsymbol{Q}$, J. Symbolic Comput., **4** (1987), 99-102.

[N] J. Nakagawa, On the Galois group of a number field with square free discriminant, Comment. Math. Univ. St. Paul., **37** (1988), 95-98.

[O] H. Osada, The Galois groups of the polynomials X^n+aX^l+b, J. Number Theory, **25** (1987), 230-238.

[S] R.P. Stauduhar, The determination of Galois groups, Math. Comp., **27** (1973), 981-996.

[U] K. Uchida, Unramified extensions of quadratic number fields, I, Tôhoku Math. J., **7** (1970), 138-140.

[W] B.L. van der Waerden, Die Zerlegengs-und Trägheitsgruppe als Permutationsgruppen, Math. Ann., **111** (1935), 731-733.

[YK] K. Yamazaki, The computation of Galois groups, (in Japanese), Report of Symposium at Osaka Univ., (ed. T. Kondo), 1981, pp. 9-57.

[YY] Y. Yamamoto, On ramified Galois extensions of quadratic number fields, Osaka J. Math., **7** (1970), 57-76.

[Y1] K. Yamamura, On unramified Galois extensions of real quadratic number fields, Osaka J. Math., **23** (1986), 471-478.

[Y2] K. Yamamura, Some analogue of Hilbert's irreducibility theorem and the distribution of algebraic number fields, J. Fac. Sci. Univ. Tokyo, **38** (1991), 99-135.

Takeshi KONDO
Department of Mathematics
Tokyo Woman's Christian University
Zenpukuji, Suginami-ku, Tokyo, 167
Japan