Natural Science Report, Ochanomizu University, Vol. 27, No. 2, 1976 155
お茶の水女子大学 自然科学報告 第27巻 第2号

On the Isomorphisms of the Galois Groups of the Maximal Abelian Extensions of Imaginary Quadratic Fields

Midori Onabe

Department of Mathematics, Faculty of Science,
Ochanomizu University, Tokyo

(Received September 10, 1976)

Let Q be the rational number field. For any algebraic number field k of finite degree over Q, we shall denote by A_k the maximal abelian extension of k and by $Gal(A_k/k)$ the Galois group of A_k over k equipped with the Krull topology. The present paper exhibits some counter-examples to the following statement; for two algebraic number fields k and k' of finite degree over Q, an isomorphism $Gal(A_k/k)\cong Gal(A_{k'}/k')$ of the Galois groups of maximal abelian extensions A_k/k and $A_{k'}/k'$ implies an isomorphism $k\cong k'$. In other words we shall see that $Gal(A_k/k)$ does not determine the isomorphism class of an algebraic number field k. Furthermore, the counterexamples which we give will show that even if $Gal(A_k/k)$ and $Gal(A_{k'}/k')$ are isomorphic, the ideal class groups of k and k' are not necessarily isomorphic.

§ 1. Invariants of the character group of $Gal(A_k/k)$.

Let k be an algebraic number field of finite degree over Q and X the character group of $Gal(A_k/k)$ with discrete topology. The structure of $Gal(A_k/k)$ is determined by that of X by virtue of duality theorem. X is known to be a torsion group. We shall denote by X_l the l-component of X for any prime number l. Let $X_{l,\infty}$ be the largest divisible subgroup of X_l and $X'_{l,\infty}$ the subgroup of all divisible elements in X_l. Then $X_{l,\infty}$ is a direct summand of X_l. Since $X_{l,\infty}$ is of finite rank,[1] $X_{l,\infty}$ is isomorphic to the direct product of finite number of $Z(l,\infty)$, where $Z(l,\infty)$ is the group of roots of unity whose orders are powers of l. Thus X_l is isomorphic to the direct product of finite number of $Z(l,\infty)$ and $X_l/X_{l,\infty}$. We shall denote by $\dim X_l$ the number of $Z(l,\infty)$ in the above direct product. $X_l/X_{l,\infty}$ is a countable reduced l-group, so that the structure is determined by the Ulm invariants.[2] Let υ_ν $(\nu=1,2,\cdots)$ be

1) Let M be a torsion abelian l-group and L the subgroup of M which consists of all the elements x of M with $x^l=1$. Then L may be regarded as a vector space over the prime field of characteristic l, of which dimension we shall call *the rank of* M.

2) cf. [2].

the Ulm invariants attached to finite ordinal numbers and $\upsilon_{\infty,\nu}$ $(\nu=1, 2,\cdots)$ be the Ulm invariants attached to transfinite ordinal numbers $(\omega+\nu-1$ $(\nu=1, 2, \cdots))$. $\upsilon_{\infty,\nu}$ $(\nu=1, 2, \cdots)$ coincide with the Ulm invariants of $X'_{l,\infty}$ $/X_{l,\infty}$. Since $X'_{l,\infty}/X_{l,\infty}$ is of finite rank, $X'_{l,\infty}/X_{l,\infty}$ is a finite group[3]; $\upsilon_{\infty,\nu}$ is the number of cyclic factors of order l^ν in the direct decomposition of $X'_{l,\infty}/X_{l,\infty}$. Then the structure of X_l is determined by $\dim X_l$, υ_ν $(\nu=$ $1, 2, \cdots)$ and $\upsilon_{\infty,\nu}$ $(\nu=1, 2, \cdots)$. Following the terminology of Kubota, we shall call υ_ν and $\upsilon_{\infty,\nu}$ *the finite and the infinite Ulm invariants of* X_l respectively. *The structure of* X *is determined by the set of invariants* $\dim X_l$, υ_ν $(\nu=1, 2, \cdots)$ *and* $\upsilon_{\infty,\nu}$ $(\nu=1, 2, \cdots)$, *where* l *runs all prime numbers.*

§ 2. The result of Kubota.

In addition to the above notations we shall use the following ones:

N; the absolute degree of k
l; a prime number
$\mathfrak{l}_1, \mathfrak{l}_2, \cdots$; all the prime factors of l in k
$\boldsymbol{e}_{l,\nu}$; the group of the units of k which are l^ν-powers in every $\mathfrak{l}_i$-completion $k_{\mathfrak{l}_i}$ of k
μ_l; the natural number which satisfies $l^{\mu_l}=(\boldsymbol{e}_{l,\nu} : \boldsymbol{e}_{l,\nu+1})$ for every sufficiently large ν
ζ_l; a primitive l-th root of unity
ν_l; the natural number such that the field $k(\zeta_l)$ contains a primitive l^{ν_l}-th root of unity but no primitive l^{ν_l+1}-th root of unity
b_ν; the number of direct factors of order l^ν in the direct decomposition of the ideal class group of k into indecomposable cyclic groups
$\mathfrak{w}_{\mathfrak{l}_i}$; the group of roots of unity in $k_{\mathfrak{l}_i}$
$k^\times$ and $k_{\mathfrak{l}_i}^\times$; the multiplicative group of k and $k_{\mathfrak{l}_i}$ respectively
$B^{(\nu)}$; the group of $\beta\in k$ such that the principal ideal (β) is the l^ν-th power of an ideal of k $(\nu=0, 1, 2, \cdots)$
$B_*^{(\nu)}$; the group of $\beta\in B^{(\nu)}$ such that β is in $\mathfrak{w}_{\mathfrak{l}_i}k_{\mathfrak{l}_i}^{\times l^\nu}$ for every i $(\nu=0, 1, 2, \cdots)$.

Then the theorem of Kubota ([1]) can be expressed as follows.

THEOREM.
(i) $\dim X_l=N-\mu_l$.
(ii) $\upsilon_\nu=\begin{cases} 0 & (\nu<\nu_l) \\ \infty & (\nu\geqq\nu_l). \end{cases}$

3) A reduced torsion abelian group of finite rank is a finite group. (cf. [2] 9. theorem 9).

(iii) *If $l\neq 2$ or $l=2$ and k is not strongly radical,*[4]

$$l^{\upsilon_\infty,\nu}=l^{\upsilon_\nu}\frac{(B^{(\nu-1)}:B_*^{(\nu-1)})(B^{(\nu+1)}:B_*^{(\nu+1)})}{(B^{(\nu)}:B_*^{(\nu)})^2} \qquad (\nu=1, 2, \cdots).$$

§ 3. Invariants $\dim X_l$ and υ_ν for imaginary quadratic fields.

From now on we shall consider imaginary quadratic fields $Q(\sqrt{-m})$, where m is a square-free integer >0.

As $\mu_l=0$ for any imaginary quadratic field, $\dim X_l=N-\mu_l=2$ for all prime l.

From the definition of ν_l we have the following.

$$\nu_2=2, \quad \nu_l=1 \ (l\neq 2) \quad \text{for} \quad Q(\sqrt{-1}),$$
$$\nu_l=1 \quad (\text{for all } l) \quad \text{for} \quad Q(\sqrt{-m}), \ m\neq 1.$$

We observe that the finite Ulm invariants υ_ν $(\nu=1, 2, \cdots)$ are the same for all $Q(\sqrt{-m})$, $m\neq 1$.

§ 4. Strongly radical fields.

Let $Q(2, \infty)$ be the field obtained by adjunction to Q of all 2^m-th roots of unity, where m runs natural numbers. An algebraic number field k of finite degree is said to be *a radical field* if the intersection $k\cap Q(2, \infty)$ is a real field. If k is a radical field, there exists a natural number $T\geqq 2$ such that $k\cap Q(2, \infty)=Q(\zeta_{2^T}+\zeta_{2^T}^{-1})$, where ζ_{2^T} is a primitive 2^T-th root of unity. Setting $\lambda_T=(\zeta_{2^{T+1}}+\zeta_{2^{T+1}}^{-1})^2$, we call λ_T *the radical number of* k. Now denoting by $\mathfrak{l}_1, \mathfrak{l}_2, \cdots$ all the prime factors of 2 and by $k_{\mathfrak{l}_i}$ the $\mathfrak{l}_i$-completion of k, we say that k is *strongly radical* if we have $\lambda_T=\lambda_i^2\zeta_i$, for every i, where λ_i is an element of $k_{\mathfrak{l}_i}$ and ζ_i is a root of unity in $k_{\mathfrak{l}_i}$.

Now all imaginary quadratic fields $Q(\sqrt{-m})$ except $Q(\sqrt{-1})$ and $Q(\sqrt{-2})$ are radical fields with $Q(\sqrt{-m})\cap Q(2, \infty)=Q$. Therefore the radical number is 2.

PROPOSITION 1. *$Q(\sqrt{-m})$ $(m\neq 1, 2)$ is strongly radical if and only if $m\equiv 1 \pmod 8$ (m : odd), or if $m/2\equiv \pm 1 \pmod 8$ (m : even).*

PROOF. If $Q(\sqrt{-m})$ $(m\neq 1, 2)$ is strongly radical, we have $2=\lambda_i^2\zeta_i$, where $\lambda_i, \zeta_i\in Q(\sqrt{-m})_{\mathfrak{l}_i}$ and ζ_i is a root of unity, for every prime factor $\mathfrak{l}_i$ of 2. A necessary and sufficient condition for the statement to hold is that $Q(\sqrt{-m})_{\mathfrak{l}_i}$ contains at least one of the three numbers $\sqrt{-1}$, $\sqrt{2}$, $\sqrt{-2}$, for every $\mathfrak{l}_i$; namely Q_2 contains at least one of the three numbers $\sqrt{m}$, $\sqrt{-2m}$, $\sqrt{2m}$, that is $m\equiv 1 \pmod 8$ when m is odd or $m/2\equiv \pm 1 \pmod 8$ when m is even.

4) See § 4 for the definition of a strongly radical field.

From this proposition, $Q(\sqrt{-m})$ $(m\neq 1, 2)$ with the class number 1 or 2 are not strongly radical. Furthermore the following proposition holds.

PROPOSITION 2. *$Q(\sqrt{-m})$ with the class number odd is not strongly radical.*

PROOF. This follows from Proposition 1 and the next two lemmas.

LEMMA 1. *Let h be the class number of $Q(\sqrt{-m})$ and r the number of prime factors of m. Then 2^{r-1} divides h.*

LEMMA 2. *Let p be a prime number such that $p\equiv 1 \pmod 4$ and h the class number of $Q(\sqrt{-p})$. Then h is even.*

These two lemmas immediately follow from the genus theorem: the number of genus in the narrow sense of a quadratic field is 2^{t-1}, where t is the number of prime factors of the discriminant of the field. (cf. [3] appendix (1)).

§ 5. Infinite Ulm invariants $\upsilon_{\infty,\nu}$.

For all imaginary quadratic fields with the class number 1, $B^{(\nu)}=B_*^{(\nu)}$ for all l and ν, by the definition of $B^{(\nu)}$ and $B_*^{(\nu)}$. Then $l^{\upsilon_{\infty,\nu}}=l^{b_\nu}=l^0$. This leads to $\upsilon_{\infty,\nu}=0$ for all l and ν.

Now we discuss imaginary quadratic fields $k=Q(\sqrt{-m})$ with the class number prime, say, q. Let $\mathfrak{a}$ be a non-principal ideal of k. There exists $\alpha\in k$ such that $\mathfrak{a}^q=(\alpha)$, where (α) is the principal ideal generated by α.

(i) In case $l=q$.

$$B^{(\nu)}=\{\beta\in k^\times ;\ (\beta) \text{ is } q^\nu\text{-th power of an ideal of } k\}.$$

If $\beta\in B^{(\nu)}$, $\nu\neq 0$, (β) is the form $(\gamma)^{q^\nu}$ or $\mathfrak{a}^{q^\nu}(\gamma)^{q^\nu}$ or $\cdots$ or $\mathfrak{a}^{(q-1)q^\nu}(\gamma)^{q^\nu}$, where $\gamma\in k^\times$, namely $(\gamma)^{q^\nu}$ or $(\alpha)^{q^{\nu-1}}(\gamma)^{q^\nu}$ or $\cdots$ or $(\alpha)^{(q-1)q^{\nu-1}}(\gamma)^{q^\nu}$. Since the units of $k=Q(\sqrt{-m})$ $(m\neq 1, 3)$ are ± 1, we have

$$B^{(\nu)}=\{\pm\gamma^q,\ \pm\alpha^{q^{\nu-1}}\gamma^{q^\nu},\ \cdots,\ \pm\alpha^{(q-1)q^{\nu-1}}\gamma^{q^\nu};\ \gamma\in k^\times\} \qquad (\nu\neq 0),$$

$$B_*^{(\nu)}=\{\beta\in B^{(\nu)};\ \beta\in\mathfrak{w}_\mathfrak{l}k_\mathfrak{l}^{\times q^\nu}, \text{ for every prime factor } \mathfrak{l} \text{ of } \mathfrak{q}\}.$$

Now we consider two types, type A and type B_q, for $k=Q(\sqrt{-m})$.

type A: There exists a prime factor $\mathfrak{l}$ of q such that $\alpha\notin\mathfrak{w}_\mathfrak{l}k_\mathfrak{l}^{\times q}$.

We have in this case

$$B_*^{(\nu)}=\{\pm\gamma^q ;\ \gamma\in k^\times\}.$$

Since $\{1, \alpha^{q^{\nu-1}}, \cdots, \alpha^{(q-1)q^{\nu-1}}\}$ is a complete set of representatives of the cosets of $B^{(\nu)}$ modulo $B_*^{(\nu)}$, we have

$$(B^{(\nu)} : B_*^{(\nu)}) = q \qquad (\nu \neq 0).$$

Therefore

$$q^{v_{\infty,\nu}} = q^{b_\nu} \frac{(B^{(\nu-1)} : B_*^{(\nu-1)})(B^{(\nu+1)} : B_*^{(\nu+1)})}{(B^{(\nu)} : B_*^{(\nu)})^2} = q^{b_\nu} = q^0 = 1 \qquad (\nu = 2, 3, \cdots)$$

$$q^{v_{\infty,1}} = q^{b_1} \frac{(B^{(0)} : B_*^{(0)})(B^{(2)} : B_*^{(2)})}{(B^{(1)} : B_*^{(1)})^2} = q \frac{1 \cdot q}{q^2} = 1.$$

So we have

$$v_{\infty,\nu} = 0 \qquad (\nu = 1, 2, \cdots).$$

type B: $\alpha \in \mathfrak{w}_\mathfrak{l} k_\mathfrak{l}^{\times q}$ *for all prime factors* $\mathfrak{l}$ *of* q.

Since $B_*^{(\nu)} = B^{(\nu)}$, we have $(B^{(\nu)} : B_*^{(\nu)}) = 1$. Therefore $q^{v_{\infty,\nu}} = q^{b_\nu}$; $v_{\infty,\nu} = b_\nu$. So we have

$$v_{\infty,\nu} = \begin{cases} 1 & (\nu = 1) \\ 0 & (\nu = 2, 3, \cdots). \end{cases}$$

(ii) In case $l \neq q$.

$$\begin{aligned} B^{(\nu)} &= \{\beta \in k^\times ; (\beta) \text{ is the } l^\nu\text{-th power of an ideal of } k\} \\ &= \{\beta \in k^\times ; (\beta) \text{ is the form } (\gamma)^{l^\nu} \text{ or } \mathfrak{a}^{l^\nu}(\gamma)^{l^\nu} \text{ or} \\ &\qquad \cdots \text{ or } \mathfrak{a}^{(q-1)l^\nu}(\gamma)^{l^\nu}, \text{ where } \gamma \in k^\times\}. \end{aligned}$$

Since $\mathfrak{a}^{sl^\nu}$ $(s = 1, 2, \cdots, q-1)$ cannot be a principal ideal in k, we have

$$\begin{aligned} B^{(\nu)} &= \{\beta \in k^\times ; (\beta) = (\gamma)^{l^\nu}, \ \gamma \in k^\times\} \\ &= \{\pm \gamma^{l^\nu} ; \gamma \in k^\times\} \\ &= B_*^{(\nu)}. \end{aligned}$$

Then $(B^{(\nu)} : B_*^{(\nu)}) = 1$. Therefore $l^{v_{\infty,\nu}} = l^{b_\nu} = l^0$. Then we have

$$v_{\infty,\nu} = 0 \qquad (\nu = 1, 2, \cdots).$$

Thus we obtained the following theorem.

THEOREM 1. *Let* $k = Q(\sqrt{-m})$ *be an imaginary quadratic field with the class number* q *(a prime),* $\mathfrak{a}$ *a non-principal ideal and* α *an element of* $k^\times$ *such that* $\mathfrak{a}^q = (\alpha)$. *Then* k *is said to belong to type A if there exists an ideal* $\mathfrak{l}$ *which is a prime factor of* q, *such that* $\alpha \in \mathfrak{w}_\mathfrak{l} k_\mathfrak{l}^{\times q}$. *Otherwise,* k *is said to belong to type* B_q. *Then the infinite Ulm invariants are*

$$v_{\infty,\nu} = 0 \quad (\textit{for all } l \textit{ and } \nu) \qquad \textit{if } k \textit{ belongs to type A.}$$

$$\begin{cases} v_{\infty,\nu} = \begin{cases} 1 & (l = q, \ \nu = 1) \\ 0 & (l = q, \ \nu = 2, 3, \cdots) \end{cases} \\ v_{\infty,\nu} = 0 \quad (l \neq q, \ \nu = 1, 2, \cdots) \end{cases} \qquad \textit{if } k \textit{ belongs to type } B_q.$$

As to $Q(\sqrt{-m})$ $(m \neq 1)$ with the class number 1, we shall agree that these fields belong to type A. Then putting together the results of § 3 and the theorem and taking into account the above agreement, we obtain the following.

THEOREM 2. *$Gal(A_k/k)$ and $Gal(A_{k'}/k')$ are isomorphic, if and only if k and k' belong to the same type.*

For example, $k=Q(\sqrt{-2})$, $k'=Q(\sqrt{-5})$.

type A	type B_2	type B_3	type B_5	type B_7	class number
$Q(\sqrt{-2})$, $Q(\sqrt{-3})$, $Q(\sqrt{-7})$, $Q(\sqrt{-11})$, $Q(\sqrt{-19})$, $Q(\sqrt{-43})$, $Q(\sqrt{-67})$, $Q(\sqrt{-163})$					1
$Q(\sqrt{-5})$, $Q(\sqrt{-6})$, $Q(\sqrt{-10})$, $Q(\sqrt{-13})$, $Q(\sqrt{-15})$, $Q(\sqrt{-22})$, $Q(\sqrt{-37})$, $Q(\sqrt{-58})$,	$Q(\sqrt{-35})$, $Q(\sqrt{-51})$, $Q(\sqrt{-91})$, $Q(\sqrt{-115})$, $Q(\sqrt{-123})$, $Q(\sqrt{-187})$, $Q(\sqrt{-235})$, $Q(\sqrt{-267})$, $Q(\sqrt{-403})$ $Q(\sqrt{-427})$				2
$Q(\sqrt{-23})$, $Q(\sqrt{-31})$, $Q(\sqrt{-59})$, $Q(\sqrt{-83})$, $Q(\sqrt{-139})$, $Q(\sqrt{-211})$, $Q(\sqrt{-283})$, $Q(\sqrt{-307})$, $Q(\sqrt{-379})$, $Q(\sqrt{-499})$		$Q(\sqrt{-107})$, $Q(\sqrt{-331})$			3
$Q(\sqrt{-47})$, $Q(\sqrt{-79})$, $Q(\sqrt{-103})$, $Q(\sqrt{-127})$, $Q(\sqrt{-131})$, $Q(\sqrt{-179})$, $Q(\sqrt{-227})$			$Q(\sqrt{-347})$, $Q(\sqrt{-443})$		5
$Q(\sqrt{-71})$, $Q(\sqrt{-151})$, $Q(\sqrt{-223})$, $Q(\sqrt{-251})$, $Q(\sqrt{-463})$, $Q(\sqrt{-467})$, $Q(\sqrt{-487})$					7

Now we classify in the table below the imaginary quadratic fields $Q(\sqrt{-m})$ $(m<500)$ with the class number 1, 2, 3, 5 and 7 according to their types. $Q(\sqrt{-1})$ belongs to an exceptional type (cf. § 3).

We can read in the table that *even if* $Gal(A_k/k)$ *and* $Gal(A_{k'}/k')$ *are isomorphic, the ideal class groups of* k *and* k' *are not necessarily isomorphic.* For example the Galois groups $Gal(A_k/k)$ are isomorphic for $k=Q(\sqrt{-2})$, $Q(\sqrt{-5})$, $Q(\sqrt{-23})$, $Q(\sqrt{-47})$ and $Q(\sqrt{-71})$, but the ideal class groups of them are not isomorphic.

References

[1] T. Kubota, Galois group of the maximal abelian extension over an algebraic number field, Nagoya Math. J. 12, 1957. pp. 177-189.

[2] I. Kaplansky, Infinite abelian groups, Univ. of Michigan Publ. in Math., No. 2, 1954.

[3] T. Takagi, Algebraic number theory, Iwanami, 1948.