Canad. Math. Bull. Vol. 26 (3), 1983

THE FIELD GENERATED BY THE DISCRIMINANT OF THE CLASS INVARIANTS OF AN IMAGINARY QUADRATIC FIELD

BY

D. S. DUMMIT*, R. GOLD, AND H. KISILEVSKY†

ABSTRACT. This note determines the quadratic field generated by the square root of the discriminant of the modular equation satisfied by the special value $j(\alpha)$ of the modular function j for α an integer in an imaginary quadratic field.

Let k be an imaginary quadratic field. Then it is known [1] that the Hilbert class field H of k is generated over k by adjoining to k any one of the algebraic integers $j(\mathfrak{A}_1), \ldots, j(\mathfrak{A}_h)$, where $\mathfrak{A}_1, \ldots, \mathfrak{A}_h$ are ideals of k representing the h classes of the class group C_k of k and j is the modular function. Here $j(\mathfrak{A}) = j(\tau)$, where $\mathfrak{A}$ has an ordered $\mathbb{Z}$-basis 1, τ with $\tau \in k, \operatorname{Im}(\tau) > 0$.

The minimal polynomial of the algebraic integer $j(\tau)$ has rational integer coefficients, is of degree h, and has a rational integral discriminant. This discriminant can be written as D^2 where

$$D = \prod_{r<s} [j(\mathfrak{A}_r) - j(\mathfrak{A}_s)].$$

In this paper we determine the field $\mathbb{Q}(D)$ generated over the field of rational numbers $\mathbb{Q}$ by D and obtain in particular the sign of D^2 [c.f. 2]. As is shown in [1], page V-12, formula (7) and the preceding remark,

$$j(\bar{\mathfrak{A}}) = j(-\bar{\tau}) = \overline{j(\tau)} = \overline{j(\mathfrak{A})}.$$

Hence,

$$\bar{D} = \prod_{r<s} [j(\bar{\mathfrak{A}}_r) - j(\bar{\mathfrak{A}}_s)],$$

and since the class of $\bar{\mathfrak{A}}$ in C_k is the inverse of the class of $\mathfrak{A}$ in C_k, $\bar{D} = D$ or $-D$ depending on the sign of the permutation representation of inversion on C_k. If n denotes the number of generators of the Sylow-2-subgroup of C_k, then

Received by the editors September 11, 1981 and, in revised form, October 5, 1982.
AMS classification number: 10D25.
* This research was supported in part by a NSF Grant.
† This research was supported in part by a NSERC Grant.

C_k has precisely 2^n classes fixed by inversion (i.e. classes of order 2) and so the number of transpositions in the cycle decompositon of inversion is $\frac{1}{2}(h-2^n)$. Hence

$$\bar{D}=(-1)^{(h-2^n)/2}D.$$

This is already sufficient to determine the sign of D^2, since $D^2 \in \mathbb{Q}$, so D^2 is positive if and only if $D \in \mathbb{R}$, i.e. $\bar{D}=D$. Since 2^n divides h, it follows that

$$D^2>0 \text{ if and only if either (a) } h \equiv 1, 2 \bmod 4 \text{ or (b) } n>1$$

(so $D^2<0$ if and only if (a) $h \equiv 3 \bmod 4$ or (*b*) $h \equiv 0 \bmod 4$ and $n=1$).

In the same way, we may determine when D is fixed by the automorphisms of Gal(H/k), the Galois group of H over k. These automorphisms may be identified by the Artin isomorphism with $\sigma_{\mathfrak{A}}$, where $\mathfrak{A}$ is an ideal of $k, \sigma_{\mathfrak{A}}$ depending only on the class of $\mathfrak{A}$ in C_k and having action $\sigma_{\mathfrak{A}}(j(\mathfrak{B}))=j(\mathfrak{A}^{-1}\mathfrak{B})$ for every ideal $\mathfrak{B}$.

It follows that $\sigma_{\mathfrak{A}}(D)=\varepsilon_{\mathfrak{A}}D$, where $\varepsilon_{\mathfrak{A}}$ is the sign of the permutation of C_k given by multiplication by the class of $\mathfrak{A}$. The determination of $\varepsilon_{\mathfrak{A}}$ is a group-theoretic problem on the regular representation for finite groups:

Let G be a finite group and $g \in G$ be an element of order m. For any $x \in G$, the orbit of x under multiplication by g is $(x, gx, \ldots, g^{m-1}x)$ and there are $|G|/m$ disjoint cycles ($|G|=$ the order of G), so the sign of the permutation of multiplication by g on G is $(-1)^{(m-1)|G|/m}=(-1)^{|G|-|G|/m}$. Therefore, the sign of this permutation is -1 if and only if G has even order and the cyclic subgroup generated by g has odd index in G (so any Sylow-2-subgroup would be cyclic).

As a result, there is an automorphism $\sigma_{\mathfrak{A}}$ such that $\sigma_{\mathfrak{A}}(D)=-D$ if and only if C_k has a non-trivial cyclic Sylow-2-subgroup, i.e. $n=1$. In other words, D is invariant under the Galois group of H over k if and only if $n \neq 1$.

We now determine the field $\mathbb{Q}(D)$. Since D^2 is rational, $\mathbb{Q}(D)$ is at most a quadratic extension of $\mathbb{Q}$.

PROPOSITION. *With notation as above,*

$$\mathbb{Q}(D)=\begin{cases} \text{(i) } \mathbb{Q}, \textit{ if } h \equiv 1 \pmod 4 \textit{ or } n \geq 2 \\ \text{(ii) } k, \textit{ if } h \equiv 3 \pmod 4 \\ \text{(iii) } \textit{the unique real quadratic subfield of } H, \\ \qquad \textit{if } h \equiv 2 \bmod 4 \\ \text{(iv) } \textit{the unique imaginary quadratic subfield of} \\ \qquad H \textit{ not equal to } k, \textit{ if } n=1 \textit{ and } 4 \\ \qquad \textit{divides } h. \end{cases}$$

Proof. Suppose first that $n=0$ so that h is odd. Then D is fixed by all automorphisms of Gal(H/k) so that $\mathbb{Q}(D)$ is either $\mathbb{Q}$ or k according as D^2 is positive or negative, i.e. $h \equiv 1 \bmod 4$ or $h \equiv 3 \bmod 4$, respectively. This gives (ii) and the first statement of (i).

https://doi.org/10.4153/CMB-1983-045-4 Published online by Cambridge University Press

If $n=1$, D is not invariant under $\mathrm{Gal}(H/k)$, hence $\mathbb{Q}(D)$ is not contained in k. When $n=1$, H contains precisely three quadratic subfields: k, a second imaginary quadratic field, and a unique real quadratic field. Therefore, $\mathbb{Q}(D)$ is again determined by the sign of D^2. This gives (iii) and (iv).

Finally, if $n \geq 2$, D is invariant under $\mathrm{Gal}(H/k)$ and under complex conjugation, so that $\mathbb{Q}(D)=\mathbb{Q}$, and this completes the proof.

References

1. K. Iwasawa, "Class Fields", in *Seminar on Complex Multiplication*, A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, and J. P. Serre, Lecture Notes in Math., vol. **21** (1966), Springer-Verlag.
2. J. McKay, Dihedral Group D_7 as Galois Group over Q, Abstracts of A.M.S. (1980) 80-T-A215.

Mathematics Department
Princeton University
Current Address: University of Minnesota
Minneapolis, MN 55455

Mathematics Department
Ohio State University
Columbus, Ohio 43210

Mathematics Department
Concordia University
Montreal, Quebec H3G 1M8

https://doi.org/10.4153/CMB-1983-045-4 Published online by Cambridge University Press