PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 56, April 1976

RELATIVE INTEGRAL BASES

LAWRENCE C. WASHINGTON

ABSTRACT. We give necessary and sufficient conditions for certain quadratic extensions of imaginary quadratic fields to have relative integral bases.

Two recent papers ([2], [4]) have given examples of quadratic extensions of imaginary quadratic number fields for which there exists no relative integral basis. In this note, by using a theorem of Artin, we prove the following theorem, which contains these examples as a special case (namely, when $|a|$ is prime).

THEOREM. *Let $F = \mathbf{Q}(\sqrt{-D})$ be an imaginary quadratic field with discriminant $-D$. Let $a \equiv 1 \pmod 4$ be a square-free integer with $D \nmid a$, and let $E = \mathbf{Q}(\sqrt{-D}, \sqrt{a})$. Then E/F has a relative integral basis $\Leftrightarrow (a, D) = 1$.*

PROOF. Let $g = (a, D)$, so g is odd and square-free. The quadratic subfields of $E/\mathbf{Q}$ have discriminants a, $-D$, and $-aD/g^2$. Therefore, up to sign, these are the conductors of the nontrivial Dirichlet characters for $E/\mathbf{Q}$. By the conductor-discriminant formula, $D_{E/\mathbf{Q}}$ = discriminant of $E/\mathbf{Q} = (a^2D^2/g^2)$, regarded as an ideal of $\mathbf{Z}$. Letting $D_{E/F}$ = relative discriminant for E/F, we have

$$D^2 N_{F/\mathbf{Q}}(D_{E/F}) = D_{E/\mathbf{Q}} = (a^2D^2/g^2).$$

Therefore, $N_{F/\mathbf{Q}}(D_{E/F}) = (a^2/g^2)$. If σ restricted to F generates $\mathrm{Gal}(F/\mathbf{Q})$, then $\sigma(D_{E/F}) = D_{\sigma E/\sigma F} = D_{E/F}$. Consequently, $D_{E/F}^2 = N_{F/Q}(D_{E/F}) = (a/g)^2$, so $D_{E/F} = (a/g)$.

The polynomial $X^2 - a$ generates E/F, and the discriminant Δ of this polynomial is $4a$. Therefore, $\Delta^{-1} D_{E/F} = (g)/4g^2$.

We now need the following theorem of Artin ([1]): Let E/F be a finite extension, $D_{E/F}$ the relative discriminant, and Δ the discriminant of a polynomial defining E/F. Then E/F has a relative integral basis if and only if there is a principal ideal (z) of F such that $(z)^2 = \Delta^{-1} D_{E/F}$.

Consequently, our problem is reduced to determining when there exists $z \in F$ such that $(z)^2 = (g)$.

If $g = 1$, let $z = 1$. We find that E/F has a relative integral basis. In fact

Received by the editors April 14, 1975.
AMS (MOS) subject classifications (1970). Primary 12A99; Secondary 12A25, 13B20.
Key words and phrases. Relative integral bases, quadratic fields.

the basis for $Q(\sqrt{a})/Q$ is also a basis for E/F (see Lang [3, p. 68]).

If $g \neq 1$ we have two cases:

(i) $-D \not\equiv 1 \pmod 4$. In this case $z = x + y\sqrt{-D}$, with $x, y \in \mathbf{Z}$. Taking norms, we obtain $g^2 = N(z^2) = (x^2 + Dy^2)^2$, hence $g = x^2 + Dy^2$. Since $D \nmid a$, $g < D$. Therefore, $y = 0$. But g is square-free, so $g \neq x^2$. Therefore, z does not exist.

(ii) $-D \equiv 1 \pmod 4$. In this case we obtain $g = x^2 + xy + (1 + D)y^2/4$, with $x, y \in \mathbf{Z}$. Since g is square-free, $y \neq 0$. Therefore, $g \geqslant Dy^2/4 > gy^2/4$, so $y = \pm 1$; we also find that $4g \geqslant D > g$. Since D is a multiple of g and D is odd, $D = 3g$. Consequently, $g = x^2 \pm x + (1 + 3g)/4$, which implies $g = (2x \pm 1)^2$, contradiction. Therefore, z does not exist. Q.E.D.

In the cases considered by MacKenzie, Scheuneman, and Fujisaki, $|a|$ is a prime which divides D, so E/F is unramified; in fact, E is contained in the genus field of F. One may ask more generally whether or not E/F has a relative integral basis, where E is any subfield of the genus field of F. It turns out that the above case is an exception and that usually a basis exists.

THEOREM. *Let $F = \mathbf{Q}(\sqrt{d})$ be a quadratic number field with discriminant d, let $\{p_1, \ldots, p_n\}$ be a proper subset of the set of odd primes dividing d, and let $E = F(\sqrt{\pm p_1}, \ldots, \sqrt{\pm p_n})$, where $\pm p_i \equiv 1 \pmod 4$. If $n \geqslant 2$ then E/F has a relative integral basis.*

PROOF. Since E/F is unramified (outside ∞), $D_{E/F} = (1)$. To find Δ, consider the vector space basis for E/F consisting of all subproducts of $\prod_{i=1}^{n} \sqrt{\pm p_i}$. In the determinant expression for $\Delta^{1/2}$, each column is obtained by fixing a subproduct and multiplying by a column with entries ± 1, corresponding to the action of the Galois group of E/F on the subproduct. We factor out these subproducts from each column and are left with a $2^n \times 2^n$ matrix consisting of entries ± 1. Since $\sqrt{\pm p_i}$ appears in 2^{n-1} subproducts, we find that $\Delta^{1/2} = (\prod_{i=1}^{n} (\pm p_i)^{2^{n-2}}) \cdot m$, where m is a rational integer. Therefore, $\Delta^{-1} D_{E/F} = (\Delta^{-1})$ is the square of a principal ideal of F, so a relative integral basis exists for E/F. Q.E.D.

REFERENCES

1. E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, Colloq. Internat. du Centre National Recherche Scientifique, no. 24, CNRS, Paris, 1950, pp. 19–20; *Collected papers of Emil Artin*, Addison-Wesley, Reading, Mass., 1965, pp. 229–231. MR **13**, 113.

2. G. Fujisaki, *Some examples of number fields without relative integral bases*, J. Fac. Sci. Univ. Tokyo Sect. IA **21** (1974), 92–95.

3. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970. MR **44** #181.

4. R. E. MacKenzie and J. Scheuneman, *A number field without a relative integral basis*, Amer. Math. Monthly **78** (1971), 882–883. MR **44** #5292.

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, STANFORD, CALIFORNIA 94305