Note on a Paper of E Artin

By Genjiro FUJISAKI

Department of Mathematics, College of General Education, University of Tokyo, Komaba, Meguro-ku, Tokyo 153

(Received September 10, 1974)

1. Let $\mathfrak{o}$ be a Dedekind domain with quotient field F. Let K/F be a finite separable extension of nth degree and $\mathfrak{O}$ be the integral closure of $\mathfrak{o}$ in K, that is, the subring of K consisting of all integral elements over $\mathfrak{o}$. Then $\mathfrak{O}$ is a Dedekind domain with quotient field K and, as a module over $\mathfrak{o}$, $\mathfrak{O}$ is torsion-free and finitely generated of rank n.

Let $\tilde{\mathfrak{O}}$ be the complementary set of $\mathfrak{O}$ relative to $\mathfrak{o}$, that is, the set of elements $\alpha\in K$ such that $\mathrm{tr}_{K/F}(\alpha\omega)\in\mathfrak{o}$ for all $\omega\in\mathfrak{O}$, $\mathrm{tr}_{K/F}$ denoting the trace from K to F. Then $\tilde{\mathfrak{O}}$ is a non-zero fractional $\mathfrak{O}$-ideal in K, and the inverse ideal $\mathfrak{D}(\mathfrak{O}/\mathfrak{o})=\tilde{\mathfrak{O}}^{-1}$ is an integral ideal in $\mathfrak{O}$, called the *different* of $\mathfrak{O}$ over $\mathfrak{o}$ (or of K/F, fixing $\mathfrak{O}$ and $\mathfrak{o}$ once for all). The *discriminant* $\mathfrak{d}(\mathfrak{O}/\mathfrak{o})$ of $\mathfrak{O}$ over $\mathfrak{o}$ is then defined to be the norm $N_{K/F}(\mathfrak{D}(\mathfrak{O}/\mathfrak{o}))$ of the different $\mathfrak{D}(\mathfrak{O}/\mathfrak{o})$. $\mathfrak{d}(\mathfrak{O}/\mathfrak{o})$ is a non-zero integral ideal in $\mathfrak{o}$.

The following theorems are due to Artin [1].

THEOREM 1. *With notations and definitions explained as above, let $K=F(\theta)$ be a finite separable extension of* nth *degree, $\theta\in\mathfrak{O}$ denoting any generating element of K over F. Then there exists a non-zero fractional $\mathfrak{o}$-ideal $\mathfrak{a}$ in F satisfying the equation*

$$\mathfrak{d}(\mathfrak{O}/\mathfrak{o})=d(\theta)\mathfrak{a}^2,$$

$d(\theta)=d_{K/F}(\theta)$ denoting the discriminant of θ relative to K/F.

The ideal class of $\mathfrak{a}$ is uniquely defined by $\mathfrak{O}/\mathfrak{o}$ and is independent of choice of generating element θ.

THEOREM 2. *Using notations as in Theorem* 1, *the following two conditions are equivalent with each other.*

(1) *$\mathfrak{O}$ is a free $\mathfrak{o}$-module of rank n, that is, there exists a basis $\omega_1,\cdots,\omega_n$ of K over F such that*

$$\mathfrak{O}=\mathfrak{o}\omega_1+\cdots+\mathfrak{o}\omega_n.$$

(2) *The ideal $\mathfrak{a}$ is principal in F.*

If $\mathfrak{O}$ is, as an $\mathfrak{o}$-module, a direct sum of the form $\mathfrak{O}=\mathfrak{o}\omega_1+\cdots+\mathfrak{o}\omega_n$, we shall

say that $\{\omega_1, \cdots, \omega_n\}$ is a *minimal basis* of $\mathfrak{O}$ over $\mathfrak{o}$ (or K over F).

In this paper, we shall describe proof of these theorems in detail to some extent, and give some examples of Dedekind domains $\mathfrak{o}$ with quotient field F (number field) and extensions K/F, some of which do not have any minimal basis, some of which have minimal bases.

2. In the theory of modules over a Dedekind domain $\mathfrak{o}$, the following theorems are fundamental.

THEOREM A. *For a module M over $\mathfrak{o}$, the following conditions are equivalent.*
(1) *M is torsion-free and finitely generated.*
(2) *M is projective and finitely generated.*
(3) *M is isomorphic to a direct sum $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_k$ of fractional $\mathfrak{o}$-ideals.*

THEOREM B. *Two direct sums $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ and $\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ of non-zero fractional ideals are isomorphic as $\mathfrak{o}$-modules if and only if $r=s$ and ideal class of $\mathfrak{a}_1 \cdots \mathfrak{a}_r$ is equal to that of $\mathfrak{b}_1 \cdots \mathfrak{b}_s$.*

Now, as in section 1°, let F be the quotient field of a Dedekind domain $\mathfrak{o}$, and let $K=F(\theta)$ be a finite separable extension of nth degree. Denoting by $\mathfrak{O}$ the integral closure of $\mathfrak{o}$ in K, we may suppose $\theta \in \mathfrak{O}$.

It is well-known that every non-zero fractional $\mathfrak{O}$-ideal $\mathfrak{A}$ is, as a module over $\mathfrak{o}$, torsion-free and finitely generated of rank n. Therefore, by Theorem A, there exist a basis $\gamma_1, \cdots, \gamma_n$ of K/F and non-zero fractional $\mathfrak{o}$-ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ such that

$$\mathfrak{A} = \mathfrak{a}_1\gamma_1 + \cdots + \mathfrak{a}_n\gamma_n.$$

It is noted that, by Theorem B, choosing a suitable basis $\gamma_1, \cdots, \gamma_n$ and a suitable ideal $\mathfrak{a}$, we may suppose $\mathfrak{a}_1 = \cdots = \mathfrak{a}_{n-1} = \mathfrak{o}$, $\mathfrak{a}_n = \mathfrak{a}$.

Denoting by $(\gamma_i^{(j)})$ the conjugates of γ_i over F, it is easy to see that an ideal $\mathfrak{a}_1^2 \cdots \mathfrak{a}_n^2 (\det(\gamma_i^{(j)}))^2$, which shall be denoted by $d(\mathfrak{A})$, is uniquely determined by $\mathfrak{A}$, and is independent of choice of $\gamma_1, \cdots, \gamma_n$ and $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$. $d(\mathfrak{A})$ is a non-zero fractional $\mathfrak{o}$-ideal in F.

The following theorem is also due to Artin [1].

THEOREM 3. *The notations being the same as above, let $\mathfrak{A}$ be a non-zero fractional $\mathfrak{O}$-ideal in K. Then we have*

$$d(\mathfrak{A}) = (\mathrm{N}_{K/F}(\mathfrak{A}))^2 d(\mathfrak{O}).$$

Now, let $A \in GL(n, F)$ be a transformation matrix between two bases $1, \theta, \cdots, \theta^{n-1}$ and $\gamma_1, \cdots, \gamma_n$, i.e., a non-singular matrix with coefficients in F such that

$$(\gamma_1, \cdots, \gamma_n) = (1, \theta, \cdots, \theta^{n-1})A.$$

Then an easy calculation shows that

$$\det(\gamma_i^{(j)})^2=d(\theta)(\det A)^2,$$

whence we have

$$d(\mathfrak{A})d(\theta)^{-1}=(\mathfrak{a}_1\cdots\mathfrak{a}_n(\det A))^2.$$

Now, let $\mathfrak{A}=\mathfrak{O}$. As noted before, we may choose, by Theorem B, $\mathfrak{a}_1=\cdots=\mathfrak{a}_{n-1}=\mathfrak{o}$ and $\mathfrak{a}_n=\mathfrak{a}$ for some ideal $\mathfrak{a}$ so that

$$\mathfrak{O}=\mathfrak{o}\gamma_1+\cdots+\mathfrak{o}\gamma_{n-1}+\mathfrak{a}\gamma_n,$$

whence the equation

$$d(\mathfrak{O})d(\theta)^{-1}=(\mathfrak{a}(\det A))^2$$

follows. This shows, as is easily seen, that $\mathfrak{O}$ has a minimal basis over $\mathfrak{o}$ if and only if an ideal $d(\mathfrak{O})d(\theta)^{-1}$ is a square of some principal ideal in F. Therefore, in order to prove Theorems 1 and 2, it is sufficient to show that $d(\mathfrak{O})$ actually coincides with $\mathfrak{d}(\mathfrak{O}/\mathfrak{o})$. It seems to me that Artin did not write his proof of this fact in his paper [1], only for saving lines. So we shall give an elementary proof of a theorem, due to Artin [1].

THEOREM 4. *With notations and definitions we have explained above,* $d(\mathfrak{O})$ *is the discriminant* $\mathfrak{d}(\mathfrak{O}/\mathfrak{o})$ *of* $\mathfrak{O}$ *over* $\mathfrak{o}$.

Proof. We may choose a suitable fractional ideal $\mathfrak{a}$ and a basis $\omega_1,\cdots,\omega_n$ of K over F, such that

$$\mathfrak{O}=\mathfrak{a}\omega_1+\mathfrak{o}\omega_2+\cdots+\mathfrak{o}\omega_n.$$

Then

$$d(\mathfrak{O})=\mathfrak{a}^2(\det(\omega_i^{(j)}))^2,$$

where $(\omega_i^{(j)})$ denotes the conjugates of ω_i relative to F, as before.

Let $\tilde{\omega}_1,\cdots,\tilde{\omega}_n$ be the complementary basis to the basis $\omega_1,\cdots,\omega_n$, that is, $\{\tilde{\omega}_1,\cdots,\tilde{\omega}_n\}$ is a basis of K/F such that $\mathrm{tr}_{K/F}(\omega_i\tilde{\omega}_j)=\delta_{ij}$ $(1\leq i,j\leq n)$. Since the inverse $\mathfrak{D}^{-1}$ of the different $\mathfrak{D}=\mathfrak{D}(\mathfrak{O}/\mathfrak{o})$ is a complementary set of $\mathfrak{O}$ relative to $\mathfrak{o}$, it can be calculated (cf. [2]) that

$$\mathfrak{D}^{-1}=\mathfrak{a}^{-1}\tilde{\omega}_1+\mathfrak{o}\tilde{\omega}_2+\cdots+\mathfrak{o}\tilde{\omega}_n,$$

whece, by definition,

$$d(\mathfrak{D}^{-1})=\mathfrak{a}^{-2}(\det(\tilde{\omega}_i^{(j)}))^2.$$

Now, Theorem 3 shows that

$$d(\mathfrak{D}^{-1})=\mathrm{N}_{K/F}(\quad^{-1})^2d(\mathfrak{O})=\mathfrak{d}(\mathfrak{O}/\mathfrak{o})^{-2}d(\mathfrak{O}).$$

Therefore, we have the equation

$$\mathfrak{a}^{-2}(\det(\tilde{\omega}_i^{(j)})^2)=\mathfrak{d}(\mathfrak{O}/\mathfrak{o})^{-2}\mathfrak{a}^2(\det(\omega_i^{(j)})^2).$$

But, as we can easily calculate

$$\det(\tilde{\omega}_i^{(j)})^2=\det(\omega_i^{(j)})^{-2},$$

it follows that

$$\mathfrak{d}(\mathfrak{O}/\mathfrak{o})^2=(\mathfrak{a}^2\det(\omega_i^{(j)})^2)^2=d(\mathfrak{O})^2,$$

whence we have

$$\mathfrak{d}(\mathfrak{O}/\mathfrak{o})=d(\mathfrak{O}).$$

3. We shall give *some examples of Dedekind domains* $\mathfrak{o}$ *with quotient fields* F *(quadratic number fields) and quadratic extensions* K/F*, which do not have any minimal basis of* K *over* F.

As usual, let $\boldsymbol{Z}$ be the ring of rational integers and let $\boldsymbol{Q}$ be the rational number field. Before describing examples, we shall state the following theorem, which will be needed to calculate examples.

THEOREM C. *Let* d_1 *and* d_2 *be the discriminants of different quadratic fields* $\boldsymbol{Q}(\sqrt{m_1})$ *and* $\boldsymbol{Q}(\sqrt{m_2})$*, respectively. Let* d_3 *be the discriminant of quadratic field* $\boldsymbol{Q}(\sqrt{m_1m_2})$*. Then the absolute discriminant* D_K *of bicyclic biquadratic field* $K=\boldsymbol{Q}(\sqrt{m_1},\sqrt{m_2})$ *is equal to* $D_K=d_1d_2d_3$.

Now, let m (≥ 5) be any square-free integer such that $m\equiv 1 \pmod 4$. Let $F=\boldsymbol{Q}(\sqrt{-m})$ and $K=\boldsymbol{Q}(\sqrt{2},\sqrt{-m})$, which is a quadratic extension of F. The ring $\mathfrak{o}=\mathfrak{o}_F$ of integers in F is a Dedekind domain and the ring $\mathfrak{O}=\mathfrak{o}_K$ of integers in K is the integral closure of $\mathfrak{o}$ in K. We shall prove

PROPOSITION 1. K/F *(i.e.,* $\mathfrak{o}_K/\mathfrak{o}_F$*) has no minimal basis.*

Proof. The absolute discriminant of $K=\boldsymbol{Q}(\sqrt{2},\sqrt{-m})$ is, by Theorem C, $D_K=2^3\cdot(-2^2m)\cdot(-2^3m)=2^8m^2$. Therefore, the relative discriminant $\mathfrak{d}(K/F)=\mathfrak{d}(\mathfrak{o}_K/\mathfrak{o}_F)$ can be calculated by the well known formula

$$D_K=d_F^2\,\mathrm{N}_{K/F}(\mathfrak{d}(K/F)),$$

d_F denoting the discriminant $-4m$ of F, so that we have $\mathfrak{d}(K/F)=(2\mathfrak{o}_F)^2$.

Now, since $K=F(\sqrt{2})$, we may take $\theta=\sqrt{2}$ and we can calculate $d(\theta)=d_{K/F}(\theta)=2^3$. Hence, an ideal $\mathfrak{d}(K/F)d(\theta)^{-1}$ is $(2\mathfrak{o}_F)^{-1}$, which shall be proved not to be a square of any principal ideal in F.

LEMMA 1. *The ideal* $2\mathfrak{o}_F$ *is not a square of any principal ideal in* F.

Proof. We can prove Lemma 1 by using the theory about ambiguous ideal classes in quadratic fields (cf. proof of Lemma 2), but we shall show here a quite elementary proof of this lemma.

The rational prime 2 is ramified in F, so that $2\mathfrak{o}_F=\mathfrak{p}_2^2$, $\mathfrak{p}_2=2\boldsymbol{Z}+(1+\sqrt{-m})\boldsymbol{Z}$ being a prime ideal in F. To prove lemma, it suffices to show that $\mathfrak{p}_2$ is not principal. Suppose $\mathfrak{p}_2$ is principal, then there exist $\alpha,\beta\in\boldsymbol{Z}$ such that $\mathfrak{p}_2=(\alpha+\beta\sqrt{-m})\mathfrak{o}_F$. Since the prime ideal $\mathfrak{p}_2$ contains 2 and $1+\sqrt{-m}$, there are $x,y,z,u\in\boldsymbol{Z}$, $(x,y)\neq(0,0)$, $(z,u)\neq(0,0)$, such that

$$2=(\alpha+\beta\sqrt{-m})(x+y\sqrt{-m}),$$

$$1+\sqrt{-m}=(\alpha+\beta\sqrt{-m})(z+u\sqrt{-m}),$$

whence we have

$$2=\alpha x-\beta ym,\ 1=\alpha z-\beta um,$$

$$0=\alpha y+\beta x,\quad 1=\alpha u+\beta z.$$

We eliminate α and obtain $2y=-\beta\cdot(y^2m+x^2)$. Taking note of the fact $m\geq 5$ and $(x,y)\neq(0,0)$, we compare the absolute values of both sides and we have $\beta=0$. Hence $\mathfrak{p}_2=\alpha\mathfrak{o}_F$ with $\alpha, z\in\boldsymbol{Z}, \alpha z=1$, which means $\mathfrak{p}_2=\mathfrak{o}_F$, contradiction!

We shall give *another example of series of quadratic fields F and quadratic extensions K/F, which has no minimal basis.*

Let p be a prime number such that $p\equiv 5 \pmod 8$, and let $F=\boldsymbol{Q}(\sqrt{2p}), K=\boldsymbol{Q}(\sqrt{2}, \sqrt{p})=F(\sqrt{2})$. Since the absolute discriminant D_K of K is equal to $D_K=8\cdot p\cdot 8p=(8p)^2$, the relative discriminant $\mathfrak{d}(K/F)$ of K/F can be calculated as in the above example, so that $\mathfrak{d}(K/F)=\mathfrak{o}_F$. We may put $\theta=\sqrt{2}$, then $d(\theta)=8$, whence $\mathfrak{d}(K/F)d(\theta)^{-1}=(2^{-1}\mathfrak{o}_F)^2$. The rational prime 2 is ramified in F, so that $2\mathfrak{o}_F=\mathfrak{p}_2^2$, where $\mathfrak{p}_2$ is the prime divisor of 2 in F. Therefore, we have $\mathfrak{d}(K/F)d(\theta)^{-1}=((2^{-1}\mathfrak{o}_F)\mathfrak{p}_2^{-1})^2$. Hence, if $\mathfrak{p}_2$ is not principal in F, then K/F does not have any minimal basis.

LEMMA 2. *$\mathfrak{p}_2$ is not principal in F.*

*Proof.** Since the absolute norm of fundamental unit of $F=\boldsymbol{Q}(\sqrt{2p})$, $p\equiv 5 \pmod 8$, is -1, every ideal class in the usual sense coincides with ideal class in the narrow sense. Hence, every ambiguous ideal class contains an ambiguous ideal.

The number of ambiguous ideal classes of $F=\boldsymbol{Q}(\sqrt{2p})$ is 2 and denoting by $\mathfrak{p}_p$ the prime divisor of p, ambiguous ideals (1), $\mathfrak{p}_2, \mathfrak{p}_p, \mathfrak{p}_2\mathfrak{p}_p=(\sqrt{2p})$ are, two by two, divided into the same ambiguous ideal classes ([4], Theorem 6.2). Hence $\mathfrak{p}_2$ and $\mathfrak{p}_p$ are in the same ambiguous ideal class, different from principal class. This means $\mathfrak{p}_2$ is not principal.

By the same way, it can be easily checked that $K=\boldsymbol{Q}(\sqrt{2}, \sqrt{p})$ (p prime, such that $p\equiv 5 \pmod 8$) *has* a minimal basis over $\boldsymbol{Q}(\sqrt{p})$ and $\boldsymbol{Q}(\sqrt{2})$, respectively.

Other examples: $K=\boldsymbol{Q}(\sqrt{2}, \sqrt{m})$, where $m\equiv 3 \pmod 4$ is any positive square-free integer, has a minimal basis over $\boldsymbol{Q}(\sqrt{2m})$, and $K=\boldsymbol{Q}(\sqrt{2}, \sqrt{p})$, p denoting prime such that $p\equiv 3 \pmod 4$, has a minimal basis over $\boldsymbol{Q}(\sqrt{p})$, since the prime divisor of 2 in $\boldsymbol{Q}(\sqrt{p})$ ($p\equiv 3 \pmod 4$) is principal.

* Proof is due to S. N. Kuroda.

References

[1] Artin, E., Questions de base minimale dans la théorie des nombres algébriques, *The Collected papers of E. Artin*, Addison-Wesley, pp. 229-231.
[2] Artin, E., *Theory of Algebraic Numbers*, Göttingen, 1956/57.
[3] Fujisaki, G., Some examples of number fields without relative integral bases, *J. Fac. Sci. Univ. of Tokyo*, **21**, 93-95 (1974).
[4] Takagi, T., *Lectures on Elementary Theory of Numbers* (in Japanese), Kyoritsu, Tokyo.