ACTA ARITHMETICA
LXX.3 (1995)

On relative integral bases for unramified extensions

by

Kevin Hutchinson (Dublin)

0. Introduction. Since $\mathbb{Z}$ is a principal ideal domain, every finitely generated torsion-free $\mathbb{Z}$-module has a finite $\mathbb{Z}$-basis; in particular, any fractional ideal in a number field has an "integral basis". However, if K is an arbitrary number field the ring of integers, A, of K is a Dedekind domain but not necessarily a principal ideal domain. If L/K is a finite extension of number fields, then the fractional ideals of L are finitely generated and torsion-free (or, equivalently, finitely generated and projective) as A-modules, but not necessarily free. Beginning with some classical results of Artin and Chevalley (Propositions 1.1 and 1.2), we give some criteria for the existence or nonexistence of A-bases for ideals in L or for the ring of integers of L in the case where L/K is unramified (Theorem 1.10 and Corollary 2.3). In particular, we show how the existence of an integral basis is (under mild hypotheses) determined by purely group-theoretic properties of the Galois group of the normal closure of L/K. We prove the main results for arbitrary finite separable field extensions L/K. The arguments were suggested by reading [4].

1. Unramified extensions. We begin by recalling some of the basic facts about lattices (finitely generated torsion-free modules) over a Dedekind domain. If P is a lattice over the Dedekind domain A, then $P \cong I_1 \oplus \ldots \oplus I_n$ where $I_1, \ldots, I_n$ are ideals of A and furthermore $I_1 \oplus \ldots \oplus I_n \cong J_1 \oplus \ldots \oplus J_m$ if and only if $n = m$ and $I_1 \ldots I_n \cong J_1 \ldots J_m$. Note also that if I and J are fractional ideals of A, then $I \cong J$ if and only if $[I] = [J]$, where $[K]$ denotes the class of the ideal K in $Cl(A)$, the ideal classgroup of A. It follows that the module $P \cong I_1 \oplus \ldots \oplus I_n$ is determined up to isomorphism by its rank, n, and the class $[I_1 \ldots I_n] \in Cl(A)$, called the Steinitz class of P and denoted $c(P)$. For example, if $J \subseteq A$ is an ideal representing $c(P)$ then $P \cong A^{\oplus(n-1)} \oplus J$. In particular P has an A-basis (i.e., P is free as an A-module) if and only if $c(P) = 1$. (For details, see for example [1], [3] or [5].)

Suppose now that A is a Dedekind domain with field of fractions K and that L/K is a finite separable extension of fields of degree n. Let B be the integral closure of A in L. Then B is a Dedekind domain and any fractional ideal I of B is an A-lattice of rank n. We recall the following basic results on the Steinitz class of such a lattice:

PROPOSITION 1.1. *If I is any fractional ideal of B then*

$$c(I) = c(B)\mathrm{N}_{L/K}[I].$$

PROPOSITION 1.2. *If $\delta_{B/A}$ is the relative discriminant of B over A and if $d_{L/K}$ is the discriminant of any K-basis of L, then*

$$\delta_{B/A} = J^2(d_{L/K})$$

where J is a fractional ideal of A representing the ideal class $c(B)$.

(For proofs, see [3].)

Here are some simple corollaries:

COROLLARY 1.3. *There exists an ideal of B which has an A-basis if and only if*

$$c(B) \in \mathrm{N}_{L/K}(Cl(B)).$$

Proof. By 1.1, I is A-free $\Leftrightarrow$ $1 = c(I) = \mathrm{N}_{L/K}[I]c(B) \Leftrightarrow c(B) = \mathrm{N}_{L/K}[I^{-1}]$.

COROLLARY 1.4.

$$c(B)^2 \;=\; [\delta_{B/A}] = \mathrm{N}_{L/K}[D_{B/A}]$$

where $D_{B/A}$ is the different of B relative to A.

Proof. This is immediate from 1.2.

COROLLARY 1.5. *If n is odd, there exists an ideal of B which has an A-basis.*

More generally, if the torsion abelian group $Cl(A)/\mathrm{N}_{L/K}Cl(B)$ has no nontrivial 2-torsion there exists a fractional ideal of B with an A-basis.

Proof. Since $[c(B)\mathrm{N}_{L/K}Cl(B)]^2 = 1$ in $Cl(A)/\mathrm{N}_{L/K}Cl(B)$, by 1.4, the hypothesis implies that $c(B) \in \mathrm{N}_{L/K}Cl(B)$ and hence there exists an A-free fractional ideal of B.

We will give an explicit example below of an extension of number fields L/K where no fractional ideal of L has a basis over the ring of integers of K (Example 1.14).

Recall that if no prime of A ramifies in B, then $\delta_{B/A} = A$.

COROLLARY 1.6. *If no prime of A ramifies in B and if $Cl(A)$ has no nontrivial 2-torsion, then B has an A-basis.*

Proof. Since $\delta_{B/A} = A$, we have $c(B)^2 = [\delta_{B/A}] = 1$ by 1.4 and hence $c(B) = 1$ by hypothesis.

If D is a Dedekind domain, let $U(D)$ denote the group of units of D. Thus we have:

COROLLARY 1.7. *Suppose that no prime of A ramifies in B and that $d_{L/K}$ is the discriminant of any K-basis of L. Then B has an A-basis if and only if $d_{L/K} = ua^2$ with $u \in U(A)$ and $a \in K^*$.*

Proof. By 1.2, $A = J^2(d_{L/K})$ where J represents $c(B)$. Thus, $(d_{L/K}) = J^{-2}$ and hence B is A-free $\Leftrightarrow$ J is a principal ideal $\Leftrightarrow$ $(d_{L/K})$ is the square of a principal ideal $\Leftrightarrow$ $d_{L/K} = ua^2$.

Suppose now that θ is a primitive element for L/K. Let E be the normal closure of L/K and let G be the Galois group of E/K, H the Galois group of E/L. Let $\{\sigma_1, \ldots, \sigma_n\}$ be a set of representatives for the elements of the coset space G/H. Let $d = d(\theta) = d_{L/K}(1, \theta, \ldots, \theta^{n-1}) = \prod_{i \neq j}(\sigma_i(\theta) - \sigma_j(\theta)) = \alpha(\theta)^2$ where $\alpha = \alpha(\theta) = \prod_{i<j}(\sigma_i(\theta) - \sigma_j(\theta))$. Finally, let C be the integral closure of A in E.

LEMMA 1.8. *If no prime of A ramifies in B and if either $U(C)^2 \cap K = U(A)^2$ or $[E : L]$ is odd and $U(B)^2 \cap K = U(A)^2$, then B has an A-basis if and only if $\alpha \in K$.*

Proof. If $\alpha \in K$ then $d = \alpha^2$ in K and hence B is A-free by 1.7 (without the added hypotheses on squares of units). Conversely, suppose that B is A-free. Then $\alpha^2 = d = ua^2 \Rightarrow (a^{-1}\alpha)^2 = u \Rightarrow u \in U(C)^2 \cap K \Rightarrow u \in U(A)^2 \Rightarrow \alpha^2 = (va)^2$ for some $v \in U(A) \Rightarrow \alpha = \pm va \in K$ if $U(C)^2 \cap K = U(A)^2$. If $[E : L]$ is odd then $\alpha \in L$ and thus in the argument just given, $a^{-1}\alpha \in L$ and hence $u \in U(B)^2 \cap K$.

Note. The condition on units $U(B)^2 \cap K = U(A)^2$ is not very restrictive. In the number field case, for instance, there are only finitely many quadratic extensions of the field K of the form $K(\sqrt{u})/K$ where u is a unit of K and the condition simply says that any such extension is not contained in L.

Recall that if σ is a permutation of the set $\{x_1, \ldots, x_n\}$, then σ is an even permutation if and only if

$$\sigma\Big(\prod_{i<j}(x_i - x_j)\Big) = \prod_{i<j}(x_i - x_j).$$

Thus $\alpha(\theta) \in K \Leftrightarrow \sigma(\alpha(\theta)) = \alpha(\theta)$ for all $\sigma \in G \Leftrightarrow \sigma$ acts as an even permutation on $\{\sigma_1(\theta), \ldots, \sigma_n(\theta)\}$ for all $\sigma \in G \Leftrightarrow$ each $\sigma \in G$ acts evenly on the G-set G/H since the map $G/H \to \{\sigma_1(\theta), \ldots, \sigma_n(\theta)\}, \sigma_i H \mapsto \sigma_i(\theta)$ is an isomorphism of G-sets.

We will say that the group G *acts evenly on* the G-set X if each element of G acts on X as an even permutation. Otherwise we will say that G *acts oddly on* X.

Lemma 1.9. *Let G be a finite group and H a subgroup of odd order. Then G acts oddly on G/H if and only if the Sylow 2-subgroups of G are nontrivial and cyclic.*

Proof. Since every element of odd order in a permutation group is even, G acts oddly on a set X if and only if some element of G of 2-power order acts oddly. Suppose that $\sigma \in G, \sigma \neq 1$ has 2-power order and let C be the cyclic subgroup of G generated by σ. Let $\tau \in G$ and consider the orbit of $\tau H \in G/H$ under C. The stabilizer of C on τH is $C \cap \tau H \tau^{-1} = 1$ since $\tau H \tau^{-1}$ has odd order and C has 2-power order. Thus G/H decomposes into $[G : H]/|C|$ orbits each of length $|C|$. Thus, as a permutation, σ factors as a product of $[G : H]/|C|$ cycles, each of length $|C|$. But each cycle of length $|C|$ in turn factors as a product of $|C|-1$ transpositions and hence σ factors as a product of $\frac{[G:H]}{|C|}(|C|-1)$ transpositions. Since $|C|-1$ is odd, σ acts oddly $\Leftrightarrow [G : H]/|C|$ is odd $\Leftrightarrow$ C is a Sylow 2-subgroup of G.

Combining 1.8 and 1.9 we obtain:

Theorem 1.10. *Suppose that L/K is a finite separable extension of fields and that E is the normal closure of L/K. Suppose that A is a Dedekind domain with field of fractions K and that B and C are the integral closures of A in L and E respectively. If $[E : L]$ is odd and $U(B)^2 \cap K = U(A)^2$ and if no prime of A ramifies in B then B has an A-basis if and only if the Sylow 2-subgroup of G is not nontrivial and cyclic.*

This generalises the result (see [3]) that if L/K is Galois, unramified of odd degree, then B has an A-basis. However, here is an example of an unramified extension L/K of odd degree for which B is not free as an A-module.

Example 1.11. Let F be the splitting field of $f(X) = X^3 - X + 1$ over $\mathbb{Q}$. The discriminant of $f(X)$ is -23, so $\mathrm{Gal}(F/\mathbb{Q}) = S_3$, the symmetric group on three letters. Let $E = F(\sqrt{2})$ and $K = \mathbb{Q}(\sqrt{-46})$. E is the splitting field of $f(X)$ over $\mathbb{Q}(\sqrt{2})$ and hence E is unramified (at any finite prime) over $\mathbb{Q}(\sqrt{-23}, \sqrt{2})$ by the arguments of Uchida [6] (Theorem 1 and Corollary). $\mathbb{Q}(\sqrt{-23}, \sqrt{2})$ is in turn unramified over K and thus E/K is a Galois unramified extension with $\mathrm{Gal}(E/K) = S_3$. Let H be any subgroup of $\mathrm{Gal}(E/K)$ of order 2 and let $L = E^H$. Let A, B and C be the rings of integers of K, L and E respectively. Since $U(A) = \{\pm 1\}$ and $\sqrt{-1} \notin \mathbb{Q}(\sqrt{-23}, \sqrt{2})$ it follows that $U(C)^2 \cap K = U(A)^2$. Since S_3 acts oddly on S_3/H, $\alpha \notin K$ and thus B is not a free A-module by 1.8.

If $[E : L] = |H|$ is even, then 1.9 is easily seen to fail and there is no simple criterion for G to act oddly on G/H. However, in certain circumstances one can provide criteria. We will consider this below.

For the present we specialize to the case where L/K is an extension of number fields and A is the ring of integers of L. In this situation classfield theory allows us to control the norm map $\mathrm{N}_{L/K} : Cl(B) \to Cl(A)$:

LEMMA 1.12. *Let K_1 be the Hilbert classfield of K. Let $\varrho_K : Cl(A) \to \mathrm{Gal}(K_1/K)$ be the Artin isomorphism. Then ϱ_K induces an isomorphism $\mathrm{N}_{L/K}(Cl(B)) \to \mathrm{Gal}(K_1/K_1 \cap L)$.*

Proof. Let L_1 be the Hilbert classfield of L. Then $L_1 \supseteq K_1$ and if $\varrho_L : Cl(B) \to \mathrm{Gal}(L_1/L)$ is the Artin isomorphism for L and $\mathrm{res}_{L/K}$ is the restriction map $\mathrm{Gal}(L_1/L) \to \mathrm{Gal}(K_1/K)$, then $\varrho_K \mathrm{N}_{L/K} = \mathrm{res}_{L/K}\varrho_L$ and hence ϱ_K induces an isomorphism $\mathrm{N}_{L/K}(Cl(B)) \to \mathrm{res}_{L/K}(\mathrm{Gal}(L_1/L)) = \mathrm{Gal}(K_1/L \cap K_1)$.

COROLLARY 1.13. *Suppose that L/K is unramified and that L contains the maximal abelian unramified 2-extension of K. Then there exists an ideal of B with an A-basis if and only if B has an A-basis.*

Proof. L/K unramified $\Rightarrow c(B)^2 = 1$ and since L contains the maximal abelian unramified 2-extension of K, $\mathrm{N}_{L/K}(Cl(B))$ has odd order by 1.12. Thus $c(B) = 1 \Leftrightarrow c(B) \in \mathrm{N}_{L/K}(Cl(B))$.

EXAMPLE 1.14. Let $K = \mathbb{Q}(\sqrt{-14})$, $F = K(\sqrt{2})$, $L = K(\sqrt{2\sqrt{2}-1})$. Then L is the Hilbert classfield of K (see, for example, Cox [2]). Clearly $\mathrm{Gal}(L/K) \cong Cl(A)$ is cyclic of order 4 and $\mathrm{Gal}(F/K)$ is cyclic of order 2. Let B be the ring of integers of L and let C be the ring of integers of F. Note that $U(A) = \{\pm 1\}$ and that $\sqrt{-1} \notin L$ (for otherwise we would have $\sqrt{-1} \in F = \mathbb{Q}(\sqrt{-14}, \sqrt{2})$ which is clearly false). It follows that $U(B)^2 \cap K = U(C)^2 \cap K = U(A)^2 = 1$. Thus neither B nor C has an A-basis by 1.9. No ideal of B is A-free by 1.13.

However $\mathrm{N}_{F/K}(Cl(C))$ is the unique subgroup of order 2 in $Cl(A)$ by 1.12 and thus, since $c(C)^2 = 1$ (because F/K is unramified), $c(C) \in \mathrm{N}_{F/K}(Cl(C))$ and so there exist ideals of C which are A-free.

2. "Odd" group actions. In this section we prove a few results on oddness of transitive group actions where the stabilizer has even order. In the case where the stabilizer has a normal complement, a criterion for oddness can be given:

THEOREM 2.1. *Suppose that G is a finite group with subgroup H. Suppose that H has a normal complement N. Let S be a Sylow 2-subgroup of H and suppose the elements $\sigma_1, \ldots, \sigma_r$, of orders $2^{m_1}, \ldots, 2^{m_r}$, generate S. Then G acts oddly on G/H if and only if either the Sylow 2-subgroups of N are* *nontrivial and cyclic or*

$$\sum_{k=0}^{m_i-1} 2^{m_i-k-1}|C_N(\sigma_i^{2^k})| \not\equiv (2^{m_i}-1)|N| \bmod 2^{m_i+1}$$

for some $i \in \{1,\ldots,r\}$ *where* $C_N(\tau) = \{\mu \in N \mid \mu\tau = \tau\mu\}$ *for* $\tau \in G$.

Proof. Since $G = HN$ and since a product of two even permutations is even, G acts oddly on G/H if and only if either H or N acts oddly on G/H. Now, the bijection of sets $N \leftrightarrow G/H$ induces an isomorphism of N-sets if N acts on N by left multiplication and a bijection of H-sets if H acts on N by conjugation. Thus N acts oddly on G/H if and only if the Sylow 2-subgroup of N is nontrivial and cyclic by Lemma 1.9 (with $G = N$ and $H = 1$). Clearly H acts oddly on N by conjugation if and only if S does. S acts oddly on N if and only if some σ_i does. It remains to show that σ_i acts as an odd permutation if and only if

$$\sum_{k=0}^{m_i-1} 2^{m_i-k-1}|C_N(\sigma_i^{2^k})| \not\equiv (2^{m_i}-1)|N| \bmod 2^{m_i+1}.$$

Fix i and let $\sigma = \sigma_i$, $m = m_i$. Let $r_k = |C_N(\sigma^{2^k})|$. Consider the action of σ on N by conjugation. N decomposes as a union of orbits of length 2^k, $k \le m$. If $\tau \in N$, then the orbit of τ has length 2^k if and only if σ^{2^k} fixes τ but $\sigma^{2^{k-1}}$ does not; i.e., if and only if $\tau \in C_N(\sigma^{2^k}) - C_N(\sigma^{2^{k-1}})$. Thus the number of orbits of length 2^k is

$$s_k = \frac{1}{2^k}(r_k - r_{k-1}).$$

Thus the permutation σ factors as a product of the form

$$\prod_{k=1}^{m}\Big(\prod_{j=1}^{s_k}\sigma_{kj}\Big)$$

where σ_{kj} is a 2^k-cycle. Hence σ_{kj} in turn factors as a product of $2^k - 1$ transpositions and hence σ factors as a product of t transpositions where

$$\begin{aligned}
t &= \sum_{k=1}^{m}(2^k-1)s_k = \sum_{k=1}^{m}(2^k-1)\frac{1}{2^k}(r_k - r_{k-1})\\
&= \frac{1}{2^m}\sum_{k=1}^{m}(2^m - 2^{m-k})(r_k - r_{k-1})\\
&= \frac{1}{2^m}\Big\{2^m(r_m - r_0) - \sum_{k=1}^{m} 2^{m-k}(r_k - r_{k-1})\Big\}\\
&= \frac{1}{2^m}\{(2^m-1)r_m - 2^{m-1}r_0 - 2^{m-2}r_1 - \ldots - r_{m-1}\}.
\end{aligned}$$

Thus σ acts oddly $\Leftrightarrow$ $t \not\equiv 0 \bmod 2$ $\Leftrightarrow$ $2^m t \not\equiv 0 \bmod 2^{m+1}$ $\Leftrightarrow$

$$\sum_{k=0}^{m-1} 2^{m-k-1} r_k \not\equiv (2^m - 1) r_m \bmod 2^{m+1}$$

proving the result since $r_m = |C_N(\sigma^{2^m})| = |C_N(1)| = |N|$.

COROLLARY 2.2. *Suppose G is a Frobenius group with kernel N and complement H. If $|H|$ is odd, then G acts evenly on G/H. If $|H|$ is even, then G acts oddly on G/H if and only if the Sylow 2-subgroups of H are cyclic of order 2^m and 2^{m+1} does not divide $|N| - 1$.*

Proof. Since it can easily be shown that the Sylow 2-subgroups of N cannot be nontrivial cyclic, it follows that if H has odd order then G acts evenly on G/H by 1.8. Suppose, on the other hand, that H has even order. If $\sigma \in H - \{1\}$ then $C_N(\sigma) = 1$. Suppose $\sigma \in H$ of order 2^m. Then $|C_N(\sigma^{2^k})| = 1$ for $k \le m-1$. Thus, by the proof of Theorem 2.1, σ acts oddly on $G/H \Leftrightarrow$

$$2^m - 1 \not\equiv (2^m - 1)|N| \bmod 2^{m+1}$$

$\Leftrightarrow$ 2^{m+1} does not divide $|N| - 1$. However, if σ does not generate a Sylow 2-subgroup of H then the order of such a group is 2^k with $k \ge m+1$ and hence σ acts evenly since 2^k divides $|N| - 1$ (because $|H|$ does). This proves the result.

A special case of 2.2 is the case where G is dihedral of order $2m$ with m odd and H is a subgroup of order 2. Then G acts oddly on G/H if and only if $m \not\equiv 1 \bmod 4$.

COROLLARY 2.3. *Suppose E/K is a Galois extension of fields with* $\mathrm{Gal}(E/K) = G$ *a Frobenius group with complement H. Let L be the fixed field of H. Suppose that A is a Dedekind domain with field of fractions K and that B and C are the integral closures of A in L and E respectively. Suppose that no prime of A ramifies in B and that $U(C)^2 \cap K = U(A)^2$. Then B has an A-basis if and only if one of the following holds*: (i) *$|H|$ is odd or* (ii) *the Sylow 2-subgroup of H is not cyclic or* (iii) *the Sylow 2-subgroup of H is cyclic of order 2^m and 2^{m+1} divides $[L : K] - 1$.*

Proof. This follows at once from 2.2 and 1.8.

Of course we could have stated a more general result using Theorem 2.1 rather than 2.2.

References

[1] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, CNRS XXIV (Colloq. Int., Paris, 1949), 19–20.

[2] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, 1989.
[3] A. Fröhlich, *Ideals in an extension field as modules over the algebraic integers in a finite number field*, Math. Z. 74 (1960), 29–38.
[4] L. McCulloh, *Frobenius groups and integral bases*, J. Reine Angew. Math. 248 (1971), 123–126.
[5] E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern I, II*, Math. Ann. 71 (1911), 328–353; 72 (1911), 297–345.
[6] K. Uchida, *Unramified extensions of quadratic number fields I*, Tôhoku Math. J. 22 (1970), 138–141.

DEPARTMENT OF MATHEMATICS
UNIVERSITY COLLEGE DUBLIN
BELFIELD, DUBLIN 4, IRELAND
E-mail: KHUTCH@IRLEARN.UCD.IE

Received on 6.7.1994 (2634)