

UNIT GROUPS OF INFINITE ABELIAN EXTENSIONS

WARREN MAY

ABSTRACT. Let F be a finite extension field of the rational numbers, \mathcal{O} , and let K be an infinite abelian extension of F . Let S be a finite set of prime divisors of \mathcal{O} including the Archimedean one. An S -unit of K is a field element which is a local unit at all prime divisors of F which do not restrict on \mathcal{O} to a member of S . It is shown that the group of S -units of K is the direct product of the group of roots of unity of K with a free abelian group.

The question of determining the structure of the unit group in certain infinite extensions of \mathcal{O} arose in some work of the author [2] on group algebras. In that case, the field K is the maximal cyclotomic extension of F . The conclusion of the theorem that we prove has been obtained (for entirely different purposes) by DiBello [1] for a restricted class of abelian extensions, one not including the maximal cyclotomic ones. Since the result is somewhat unexpected, it seems worthwhile to give an exposition of it which is independent of the applications.

We first prove a simple lemma on groups. If G is an abelian group and H a subgroup, we define the *purification* of H in G , denoted $(H)_\infty$, to be the set of all $x \in G$ such that $x^n \in H$ for some positive integer, n . In other words, $(H)_\infty$ is the inverse image of the torsion subgroup of G/H under the natural map. Let p be a prime number. We define the p -*purification* of H in G , denoted $(H)_p$, to be the set of all $x \in G$ such that $x^{p^r} \in H$ for some positive integer, r . Then $(H)_p$ is the inverse image of the p -torsion subgroup of G/H under the natural map.

LEMMA. *Let G be a countably generated torsion free abelian group. Assume that for any finitely generated subgroup, H' , there exists a subgroup, H , containing H' , such that the purification of H in G is finitely generated. Then G is free.*

PROOF. Let g_1, g_2, \dots be generators for G . By induction we shall construct finitely generated subgroups, $\{W_i | 1 \leq i\}$, and subsets, $\{B_i | 1 \leq i\}$, of G such that for any positive integer, n , we have that g_1, \dots, g_n are in W_n , G/W_n is torsion free, B_n is a free basis for W_n , and $B_1 \subseteq B_2 \subseteq \dots \subseteq B_n$. If this can be done, then $G = \bigcup_i W_i$ implies that $\bigcup_i B_i$ is a free basis for G .

Received by the editors November 4, 1969.

AMS Subject Classifications. Primary 1065, 1066, 1250; Secondary 2080.

Key Words and Phrases. Infinite field extension, abelian field extension cyclotomic field extension, units.

To start the induction, let H'_1 be the subgroup generated by g_1 and choose $H_1 \supseteq H'_1$ such that $(H_1)_\infty$ is finitely generated. Put $W_1 = (H_1)_\infty$ and let B_1 be some free basis for W_1 . Now assume that W_{n-1} and B_{n-1} have been constructed. Let H'_n be the subgroup generated by W_{n-1} and the element g_n . Then we may select a subgroup $H_n \supseteq H'_n$ such that $(H_n)_\infty$ is finitely generated. Put $W_n = (H_n)_\infty$. Now W_n/W_{n-1} is finitely generated and torsion free, hence free. Therefore W_{n-1} is a direct summand of W_n and so we may choose a free basis, B_n , of W_n such that $B_{n-1} \subseteq B_n$. This completes the induction.

We now fix the set, S , of prime divisors of \mathfrak{Q} for the remainder of the paper. If L is an algebraic number field, then we shall denote the group of S -units of L by $U(L)$. Let $U(L)_t$ be the torsion subgroup of $U(L)$. We shall use $\bar{U}(L)$ to denote the quotient group, $U(L)/U(L)_t$. In case M is another algebraic number field such that $M \supseteq L$, then $U(M) \supseteq U(L)$ and $U(M)_t \cap U(L) = U(L)_t$, hence we may regard $\bar{U}(L)$ as naturally embedded in $\bar{U}(M)$.

THEOREM. *Let F be a finite extension field of \mathfrak{Q} and K an abelian extension field of F . Let $U(K)$ be the group of S -units of K . Then $U(K)$ is the direct product of the group of roots of unity of K with a free abelian group.*

PROOF. (1) It suffices to prove that $\bar{U}(K)$ is free. If K' is the field obtained by adjoining all roots of unity to K , then K' is an abelian extension of F and $\bar{U}(K') \supseteq \bar{U}(K)$. Therefore it is sufficient to prove the theorem for K' . Hence we may assume that K contains all the roots of unity. For n a positive integer, we will let ζ_n denote a primitive n th root of unity.

We may apply the lemma to $\bar{U}(K)$ since it is countably generated. So suppose that we are given a finitely generated subgroup of $\bar{U}(K)$. Then we may select a field F' such that $K \supseteq F' \supseteq F$, $\bar{U}(F')$ contains the given subgroup, and F' is of finite degree over \mathfrak{Q} .

To prove the theorem, we shall show that $(\bar{U}(F'))_\infty$ is finitely generated (where all purifications are understood to be in $\bar{U}(K)$). We may replace F' by F since K is an abelian extension of F' . Hence it suffices to show that $(\bar{U}(F))_\infty$ is finitely generated.

Let p be a prime number. We shall prove that: if $\zeta_p \in F$, then $(\bar{U}(F))_p$ is finitely generated; and if $\zeta_p \notin F$, then $(\bar{U}(F))_p = \bar{U}(F)$. The standard unit theorem implies that $\bar{U}(F)$ is finitely generated, and since $\zeta_p \in F$ for only finitely many p , the theorem will follow immediately.

(2) We shall use $\bar{}$ to indicate the natural image of S -units in $\bar{U}(K)$. Suppose that $\alpha^m = \beta$ for some $\alpha \in \bar{U}(K)$, $\beta \in \bar{U}(F)$, and positive integer

m . Since K contains all roots of unity, we may choose $v \in U(K)$ and $u \in U(F)$ such that $\bar{v} = \alpha$, $\bar{u} = \beta$ and $v^m = u$. Suppose that m is the order of \bar{v} modulo $\bar{U}(F)$. Then $X^m - u$ must be irreducible over F . To see this, assume the contrary. Then for some integer, j , satisfying $1 \leq j < m$, and for some root of unity, ζ , we have $v^j \zeta \in F$. If η is a j th root of ζ , then $(v\eta)^j \in F$ implies that $\bar{v}^j = (\bar{v}\bar{\eta})^j \in \bar{U}(F)$, contradicting the assumption on m .

Let p be a prime and let r be the positive integer satisfying $\zeta_{p^r} \notin F$ and $\zeta_{p^{r-1}} \in F$. We claim that p^{r-1} is an exponent for the p -torsion subgroup of $\bar{U}(K)/\bar{U}(F)$. Suppose not. Then there exists an element $v \in U(K)$ satisfying $v^{p^r} = u \in U(F)$ and such that \bar{v} has order p^r modulo $\bar{U}(F)$. Now $X^{p^r} - u$ is the minimal polynomial of v over F and moreover $F(v)$ is normal over F since K is an abelian extension of F . Hence $X^{p^r} - u$ splits in $F(v)$ and so $\zeta_{p^r} \in F(v)$. Then $F(\zeta_{p^r}) \neq F$ implies that $X^{p^r} - u$ is reducible over $F(\zeta_{p^r})$ and therefore we can write $u = u_2^p$ for some $u_2 \in F(\zeta_{p^r})$. For some j , we then have $v^{p^{r-1}} = u_2 \zeta_{p^r}^j$. Hence $F(\zeta_{p^r}) \supseteq F(v^{p^{r-1}})$. Consider the case $r = 1$. Then $[F(\zeta_p) : F]$ is a divisor of $p - 1$ while also $[F(v) : F] = p$. This contradiction establishes our claim in this case. Now suppose $r \geq 2$. Then $[F(\zeta_{p^r}) : F] = [F(v^{p^{r-1}}) : F] = p$, hence $F(\zeta_{p^r}) = F(v^{p^{r-1}})$. Since $\zeta_p \in F$ and our extension is abelian, we may apply Kummer theory to deduce that $v^{p^{r-1}} = u_3 \zeta_{p^r}$ for some $u_3 \in F$. But in fact $u_3 \in U(F)$ and we then have $\bar{v}^{p^{r-1}} \in \bar{U}(F)$, contrary to hypothesis. Hence our claim is demonstrated.

(3) Suppose that $\zeta_p \notin F$. Then the result above implies that the p -torsion subgroup of $\bar{U}(K)/\bar{U}(F)$ is trivial and so $(\bar{U}(F))_p = \bar{U}(F)$ in this case. Now suppose that $\zeta_p \in F$. Let r be as above and put $q = p^{r-1}$. Let A be the set of all $v \in U(K)$ such that $v^q \in U(F)$ and put $E = F(A)$. Then $\bar{U}(E) \supseteq (\bar{U}(F))_p$ and the proof will be finished if we can show that $\bar{U}(E)$ is finitely generated. This will be true if $[E : F] < \infty$. Since $\zeta_q \in F$, we may apply Kummer theory and hence the problem reduces to showing that $(F^{*q}A^q : F^{*q})$ is finite. Now

$$(F^{*q}A^q / F^{*q}) \subseteq (F^{*q}U(F) / F^{*q})$$

and moreover $(F^{*q}U(F) / F^{*q})$ is isomorphic to $U(F)/U(F)^q$ since $U(F) \cap F^{*q} = U(F)^q$. But $U(F)$ is finitely generated and so $U(F)/U(F)^q$ is finite. This completes the proof of the theorem.

The theorem fails for arbitrary normal extensions, in fact, even for solvable ones as the following example shows. Let F be any finite extension of \mathbb{Q} which possesses a unit of infinite order, say u . Put $E = F(\{\zeta_p\})$ where p runs through all primes. For every p , choose v_p such that $v_p^2 = u$ and put $K = E(\{v_p\})$. Then K is normal over F and is solvable since each step in the tower $F \subseteq E \subseteq K$ is clearly abelian.

However $\overline{U}(K)$ is not free since \bar{u} is a nonidentity element which has a p th root for every prime p .

REFERENCES

1. L. V. DiBello, *Dedekind fields and some related classes of infinite algebraic number fields*, Thesis, University of Rochester, Rochester, N. Y., 1969.
2. W. May, *Group algebras over finitely generated rings*, J. Algebra (to appear).

UNIVERSITY OF ROCHESTER, ROCHESTER, NEW YORK 14627