Can. J. Math., Vol. XXXI, No. 2, 1979, pp. 436–440

MULTIPLICATIVE GROUPS UNDER FIELD EXTENSION

WARREN MAY

Let K be a field and L an extension field. L. Fuchs [**2**, Problem 98] has suggested studying the change in multiplicative groups in going from K^* to L^*. We wish to indicate difficulties that arise in trying to relate the group theoretic structure of L^* to that of K^*, even when K^* has particularly simple structure and the extension is quadratic.

First let us note a trivial fact. If $[L : K] = n < \infty$ and K^* has a free direct factor A, then L^* has a free direct factor isomorphic to A. To see this, let ϕ be the composite $L^* \to K^* \to A$ of the norm map followed by the projection map. Then L^* has a free direct factor isomorphic to $\phi(L^*)$. But the image of the norm map contains $(K^*)^n$, hence $\phi(L^*) \cong A$. The simple structure that we shall consider for K^* is the direct product of a finite cyclic group and a free abelian group. Consequently, L^* will have a large free direct factor. However, we shall show that the complementary factor may be essentially as arbitrary as possible for a subgroup of the multiplicative group of a field. More precisely, we shall appeal to a construction in [**4**] to prove

THEOREM 1. *Let G be any abelian group whose torsion subgroup is locally cyclic with nontrivial 2-component. Then there exist a field K and a quadratic extension field L such that $K^* \cong \mathbf{Z}(2) \times A$ for some free abelian group A, while $L^* \cong G \times B$ for some free abelian group B.*

The proof of the theorem utilizes transcendentals, therefore one might wonder what can occur in the more constrained situation in which K is required to be an algebraic extension of the rational numbers $\mathbf{Q}$.

THEOREM 2. *Let G be any countable torsion-free abelian group. Then there exist a field K, algebraic over $\mathbf{Q}$, and a quadratic extension field L such that $K^* \cong \mathbf{Z}(2) \times A$ for some free abelian group A, while $L^* \cong \mathbf{Z}(4) \times G \times B$ for some free abelian group B.*

We conjecture that G need not be torsion-free, but we have been unable to prove a parallel to Theorem 1. First we shall give two propositions that will be needed for the proof of Theorem 2. Most of the field theory that we use can be found in [**3**].

PROPOSITION 1. *Let K be a finite extension field of $\mathbf{Q}$ and L a finite extension field of K. Then $L^*/K^* \cong A \times B$, where A is a free abelian group and B is finite.*

Received January 6, 1978.

Proof. Let D and E be the divisor groups of K and L, respectively, and regard D as embedded in E in the usual fashion (reflecting extension of ideals). Let $D' \subseteq D$ be the free subgroup generated by the prime divisors of K that have all extensions to L unramified. For each such prime, choose a prime of L lying above it. The remaining primes of L generate a complement of D' in E, thus E/D' is free. Since only finitely many primes of K ramify in L, D/D' is finitely generated, therefore E/D is the product of a free group and a finite group.

Let U and V denote the unit groups (units in the ring of algebraic integers) in K and L, respectively, and let D_0 and E_0 denote the subgroups of principal divisors in D and E, respectively. There are natural isomorphisms $K^*/U \cong D_0$ and $L^*/V \cong E_0$. Moreover, $K^* \cap V = U$, and the induced inclusion $(K^*/U) \subseteq (L^*/V)$ agrees with $D_0 \subseteq E_0$. The class group D/D_0 is known to be finite, thus what we have shown about E/D implies that E_0/D_0 is the product of a free group and a finite group. The same applies to the isomorphic group L^*/VK^*. But $(VK^*/K^*) \cong (V/U)$. One knows from the Dirichlet unit theorem that V is finitely generated. It follows that L^*/K^* is the product of a free group and a finite group, thus the proposition is proved.

If H is an abelian group, let $T(H)$ denote its torsion subgroup. We consider an aspect of $T(L^*/K^*)$ in

PROPOSITION 2. *Let K be a field, L an extension field, and p a prime different from the characteristic of K. Assume that $L = K(\alpha)$, where $\alpha^p \in K\backslash K^p$. If $p = 2$, further assume that $L \neq K(i)$ $(i^2 = -1)$. Then $T(L^*/K^*) = (\langle\alpha\rangle T(L^*)K^*)/K^*$.*

Proof. We observe that $[L : K] = p$. Consider $\beta \in L^*$ of prime-power order modulo K^*. First suppose that the order is q^r for some prime $q \neq p$, and let $\beta^{q^r} = \gamma \in K^*$. If N is the norm map from L to K, then $N(\beta)^{q^r} = \gamma^p$, hence $\gamma = \gamma_1^{q^r}$ for some $\gamma_1 \in K^*$. Thus $\beta = \gamma_1\zeta$ for some root of unity $\zeta \in L^*$. Thus $\beta K^* \in T(L^*)K^*$.

Now suppose that β has order p^r modulo K^*, and let $\beta^{p^r} = \gamma \in K^*$. First we consider the case where $\gamma = \gamma_1^p$ for some $\gamma_1 \in K^*$. Let ζ denote a primitive pth root of unity. Then $\beta^{p^{r-1}} = \gamma_1\zeta^m$ for some m. We must have $p \nmid m$, for otherwise the order of β modulo K^* would be less than p^r. For the same reason, we must have $\zeta \notin K$. Therefore $L \supseteq K(\zeta) \supseteq K$, with $[K(\zeta) : K] > 1$. But $[K(\zeta) : K]$ divides $p - 1$ and $[L : K] = p$. This contradiction implies that no such β can exist. Thus we may assume that $\gamma \in K^p$. Except possibly when $p = 2$, $r > 1$ and $i \notin K$, we have $[K(\beta) : K] = p^r$ (see [**3**, Chapter VIII, Section 9]), and hence $r = 1$. Let us deal with the exceptional case first. Thus, we are momentarily assuming that $p = 2$, $i \notin K$ and $[K(\beta) : K] < 2^r$. Under these circumstances, it is known that $\gamma = -4\delta^4$ for some $\delta \in K$. From $\beta^{2^r} = -4\delta^4$, we see that $i \in L$ and hence $L = K(i)$. But this case is excluded in the hypothesis of the proposition. Therefore we may return to the situation where $\beta^p = \gamma$ and $[K(\beta) : K] = p$. Then we have $K(\beta) = L = K(\alpha)$. Let K' be generated over K by a primitive pth root of unity. Since $[K' : K]$ divides $p - 1$, it follows that $L \cap K' = K$, hence $[LK' : K'] = p$. Thus LK' is a cyclic extension of K' of degree p, and we may apply Kummer theory. Since $LK' = K'(\alpha) = K'(\beta)$, we have $\beta = \alpha^m\gamma$, where $\gamma \in K'$ and $p \nmid m$. But $\gamma = \beta\alpha^{-m} \in L$ also, hence $\gamma \in K$. Thus $\beta K^* \in \langle \alpha \rangle K^*$. We have therefore shown the proposition.

We remark that the excluded case is more intricate. For example, if $K = \mathbf{Q}$ and $\alpha = i$, then $1 + i \in T(L^*/K^*)$, but $1 + i \notin (\langle \alpha \rangle T(L^*)K^*)/K^*$.

Proof of theorem 1. We shall take L to be the field constructed in the proof of Theorem 3 in [**4**]. Referring to that proof, we observe that G is a subgroup of L^*, $L = \mathbf{Q}(G)$, L^*/G is a free abelian group, and there exists a torsion-free basis for G consisting of elements that are algebraically independent over $\mathbf{Q}(T(G))$ (called K in [**4**]). Let H be a finitely generated subgroup of G. Decompose H as $H = \langle \zeta \rangle \times \langle h_1 \rangle \times \ldots \times \langle h_n \rangle$, where ζ is a root of unity and $h_1, \ldots, h_n$ are torsion-free elements of G. We claim that $h_1, \ldots, h_n$ are algebraically independent over $\mathbf{Q}(\zeta)$. By the remark on the torsion-free basis for G, there exist elements $g_1, \ldots, g_m \in G$ that are algebraically independent over $\mathbf{Q}(\zeta)$, and a positive integer k such that $\langle h_1^k, \ldots, h_n^k \rangle \subseteq \langle g_1, \ldots, g_m \rangle$. But any basis for $\langle g_1, \ldots, g_m \rangle$ is clearly algebraically independent, hence it follows from the stacked basis theorem that $\langle h_1^k, \ldots, h_n^k \rangle$ has a basis that is algebraically independent. Therefore $h_1, \ldots, h_n$ are algebraically independent over $\mathbf{Q}(\zeta)$. It follows that the automorphism of $\mathbf{Q}(\zeta)$ sending ζ to ζ^{-1} can be extended to a unique automorphism σ_H of $\mathbf{Q}(H)$ such that $\sigma_H(h) = h^{-1}$ for every $h \in H$. If $H_1 \subseteq H_2$ are two finitely generated subgroups of G, then σ_{H_1} is the restriction of σ_{H_2} to $\mathbf{Q}(H_1)$. Put $\sigma = \bigcup \sigma_H$, where the union is taken over all finitely generated subgroups H of G. Then σ is an automorphism of L such that $\sigma(g) = g^{-1}$ for every $g \in G$. Let K be the fixed field of σ. Then $[L : K] = 2$ since σ has order two. Moreover, $K^* \cap G = \langle -1 \rangle$, hence $K^*/\langle -1 \rangle$ is isomorphic to a subgroup of the free abelian group L^*/G. Thus $K^* \cong \mathbf{Z}(2) \times A$ for some free abelian group A, and $L^* \cong G \times B$ for some free abelian group B.

Proof of theorem 2. We shall carry out the construction of L within the complex numbers. By Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many p such that $p \equiv 1 \pmod{12}$. Since such primes satisfy $p \equiv 1 \pmod 4$, there is a factorization $p = (a + bi)(a - bi)$, where $a \pm bi$ are nonassociate primes in the Gaussian integers. Note that $(a + bi) \cdot (a - bi)^{-1}$ lies on the unit circle, and that these elements for various p are independent free generators. Select a basis for G, and let the subgroup generated by it be G_0. Since G_0 is of countable rank, we may assume that G_0 is generated by a subset of the elements given above. Since the circle group is divisible, we may in fact assume that G is realized as a subgroup of the unit circle. Choose a chain of subgroups $G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots$ such that $(G_{n+1} : G_n) = p_n$ for some

https://doi.org/10.4153/CJM-1979-047-5 Published online by Cambridge University Press

prime p_n $(n \geqq 0)$, and such that $\bigcup_n G_n = G$. For each $n \geqq 0$, select α_n such that $G_{n+1} = \langle G_n, \alpha_n \rangle$. Then $\alpha_n \notin G_n$, $\alpha_n^{p_n} \in G_n$. We define $L_0 = \mathbf{Q}(i)$, $L_n = L_0(G_n)$ for $n \geqq 1$, and $L = L_0(G)$. Observe that $L_{n+1} = L_n(\alpha_n)$ and $\bigcup_n L_n = L$.

Let C be the maximal cyclotomic extension of $\mathbf{Q}$. We shall prove by induction on n that there exist free groups $B_0, B_1, \ldots$ such that $L_n^* = \langle i \rangle \times G_n \times \prod_{j \leqq n} B_j$, and such that $[L_n \cap C : L_0]$ is a power of 2. The elements $(a + bi) \cdot (a - bi)^{-1}$ used earlier to give a basis for G_0 are part of a free basis for $L_0^*/\langle i \rangle$, as can be seen from unique factorization in the Gaussian integers. In fact, it is easy to see that there exists a free group B_0 such that $L_0^* = \langle i \rangle \times G_0 \times B_0$, and such that all odd primes $p \not\equiv 1 \pmod{12}$ form part of a set of free generators for B_0. Clearly, $L_0 \cap C = L_0$. Thus we have shown the initial step of the induction.

Now assume that $L_n^* = \langle i \rangle \times G_n \times \prod_{j \leqq n} B_j$ and that $[L_n \cap C : L_0]$ is a power of 2. We shall write $\alpha = \alpha_n$, $p = p_n$ and $\alpha^p = \beta$. Since G is torsion-free, β has p-height 0 in G_n, thus $\beta \notin L_n^p$. Therefore, $[L_{n+1} : L_n] = p$. We claim that $[L_{n+1} \cap C : L_0]$ is a power of 2, and that $T(L_{n+1}^*) = \langle i \rangle$. Suppose that $[L_{n+1} \cap C : L_n \cap C] = m > 1$. This is a normal extension (since contained in C), consequently $L_n(L_{n+1} \cap C) \supseteq L_n$ is a normal extension of degree m. Since the extension is contained in L_{n+1}, we conclude that $m = p$, and that L_{n+1} is a normal extension of L_n. The polynomial $X^p - \beta$ splits in L_{n+1}, hence L_{n+1} contains a primitive pth root of unity. This root of unity must therefore lie in L_n because its degree over L_n divides $p - 1$. From the decomposition of L_n^*, we conclude that $p = 2$. Thus we have shown that $[L_{n+1} \cap C : L_0]$ is a power of 2. To show the statement $T(L_{n+1}^*) = \langle i \rangle$, first suppose that $\zeta \in T(L_{n+1}^*)$ is a primitive qth root of unity for q an odd prime. Then $\mathbf{Q}(\zeta) \subseteq L_{n+1} \cap C$. By what we have just shown above, this implies that $q - 1$ is a power of 2; therefore $q \not\equiv 1 \pmod{12}$. Moreover, $\sqrt{q} \in \mathbf{Q}(i, \zeta)$ (see [**3**, Chap. VIII, Section 3]), thus $\sqrt{q} \in L_{n+1}$. By the way B_0 was chosen, q has height 0 in B_0, hence height 0 in L_n^*. Therefore $[L_n(\sqrt{q}) : L_n] = 2$. Consequently, $p = 2$ and $L_n(\sqrt{q}) = L_{n+1} = L_n(\alpha)$. By Kummer theory, we may conclude that $\sqrt{q} = \alpha\gamma$ for some $\gamma \in L_n^*$. Hence $q = \beta\gamma^2$, where $\beta \in G_n$. But this is impossible since q has height 0 in L_n^*/G_n. Therefore, $T(L_{n+1}^*)$ has trivial q-component for odd primes q. Now suppose that a primitive 8th root of unity $\zeta_8 \in T(L_{n+1}^*)$. Since $\zeta_8 \notin L_n$, we must have $p = 2$ and $L_{n+1} = L_n(\zeta_8)$. Again by Kummer theory, we have $\zeta_8 = \alpha\gamma$, hence $1 = \beta^4\gamma^8$. Since G is torsion-free and the 2-height of β in G_n is 0, it follows that the 2-height of β^4 in G_n is 2. Thus the 2-height of β^4 in L_n^* is 2. But the 2-height of γ^8 in L_n^* is at least 3. This contradiction implies that $\zeta_8 \notin T(L_{n+1}^*)$. Thus $T(L_{n+1}^*) = \langle i \rangle$, and we have demonstrated our claim.

We are now ready to prove the remaining part of the induction step. Proposition 2 together with what we have just shown imply that $T(L_{n+1}^*/L_n^*) = G_{n+1}L_n^*/L_n^*$, thus Proposition 1 implies that $L_{n+1}^*/G_{n+1}L_n^*$ is free. Therefore, we can write $L_{n+1}^* = (G_{n+1}L_n^*) \times B_{n+1}$ for some free group B_{n+1}. Consider $G_{n+1}L_n^*$. Since G_{n+1} is torsion-free and G_{n+1}/G_n is torsion, it follows that $G_{n+1} \cap$

$(\langle i\rangle \times \prod_{j\leqq n}B_j) = 1$. Thus $G_{n+1}L_n^* = \langle i\rangle \times G_{n+1} \times \prod_{j\leqq n}B_j$. Therefore $L_{n+1}^* = \langle i\rangle \times G_{n+1} \times \prod_{j\leqq n+1}B_j$, and the induction is finished.

If we define $B = \oplus_{j<\omega}B_j$, then B is free, and it is clear that $L^* = \langle i\rangle \times G \times B$. As in the proof of Theorem 1, L is closed under complex conjugation since G is contained in the unit circle, and since $L = L_0(G)$. Define $K = L \cap \mathbf{R}$, hence $[L:K] = 2$. Since $K^* \cap G = 1$, it follows that the projection $\langle i\rangle \times G \times B \to \langle i\rangle \times B$ is injective on K^*. Thus $K^* \cong \mathbf{Z}(2) \times A$ for some free group A. The proof of the theorem is complete.

References

1. P. M. Cohn, *Eine bemerkung über die multiplikative gruppe eines körpers*, Arch. Math. *13* (1962), 344–348.

2. L. Fuchs, *Infinite abelian groups, Vol. II* (Academic Press, New York, 1973).

3. S. Lang, *Algebra* (Addison-Wesley, Reading, Mass., 1965).

4. W. May, *Multiplicative groups of fields*, Proc. London Math. Soc. *24* (1972), 295–306.

5. E. Schenkman, *On the multiplicative group of a field*, Arch. Math. *15* (1964), 282–285.

University of Arizona,
Tucson, Arizona