Seminaire Delange-Pisot-Poitou
(Theorie des Nombres)
1980-81

ON A QUESTION OF COLLIOT-THELENE

H. W. Lenstra, Jr.
University of Amsterdam

The contents of this note are taken from a letter that I wrote several years ago in response to the following question of J.-L. Colliot-Thélène: given a number field K, does there exists a finitely generated subgroup $W \subset K^*$ that is dense in $(K \otimes_{\mathbb{Q}} \mathbb{R})^*$? (Cf. J. reine angew. Math. 320 (1980), p. 171.) I answered this question affirmatively for the case that K is abelian over $\mathbb{Q}$. J.-L. Brylinski proved the same result independently using Baker's theorem. My own proof, reproduced below, is purely algebraic, and it works in fact for a slightly larger class of number fields. Subsequently M. Waldschmidt dealt with the case of an arbitrary number field, as an application of a new result in transcendence theory; see Invent. math. 63 (1981), pp. 99 and 110-111; his lecture in this volume (13 Oct. 1980), Cor. 4.3; and the lecture by J.-J. Sansuc (23 Feb. 1981), §4. The present note is published at the request of Waldschmidt.

Theorem. Let $K/\mathbb{Q}$ be finite abelian. Then there is a finitely generated subgroup $W \subset K^*$ which is dense in $(K \otimes_{\mathbb{Q}} \mathbb{R})^*$.

Lemma. Let G be a finite abelian group, M a free $\mathbb{R}[G]$-module of rank one, and E, F sub-$\mathbb{Z}[G]$-modules of M such that

(a) E is a lattice in M;

(b) $E \subset F$, and F/E contains a sub-$\mathbb{Z}[G]$-module isomorphic to $\mathbb{Z}[G]$.

Then F is dense in M.

Proof of the Lemma. Let $\hat{M}$ be the Pontryagin dual of M and $(\ ,\ ): M \times \hat{M} \to \mathbb{R}/\mathbb{Z}$ the inner product. Let G act on $\hat{M}$ by $(\sigma x, \sigma y) = (x,y)$ $(x \in M,\ y \in \hat{M},\ \sigma \in G)$, then $\hat{M}$ is also free of rank one over $\mathbb{R}[G]$. Put $E^{\perp} = \{y \in \hat{M}: \forall x \in E: (x,y) = 0\}$. This is a G-stable lattice in $\hat{M}$. From $E^{\perp} \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}[G]$ (as $\mathbb{R}[G]$-modules) and a known theorem (Bourbaki, Groupes et algèbres de Lie, Ch. V, annexe) we see that $E^{\perp} \otimes_{\mathbb{Z}} \mathbb{Q} \cong_{\mathbb{Q}[G]} \mathbb{Q}[G]$, so $E^{\perp}$ is $\mathbb{Z}[G]$-isomorphic to a left ideal of $\mathbb{Z}[G]$. Now let $F^{\perp} = \{y \in \hat{M}: \forall\ x \in F: (x,y) = 0\}$. This is the dual of $M/\bar{F}$, where $\bar{F}$ is the closure of F in M, so $F^{\perp} = 0$ implies $\bar{F} = M$, as required. Suppose that $F^{\perp} \neq 0$. Clearly, $F^{\perp}$ is a $\mathbb{Z}[G]$-submodule of $E^{\perp}$, so from the existence of an embedding $E^{\perp} \subset \mathbb{Z}[G]$ and the fact that G is abelian (only used here) we see that $rE^{\perp} \subset F^{\perp}$ for some non-zero element $r = \sum_{\sigma} m_{\sigma}\sigma \in \mathbb{Z}[G]$. Let $\bar{r} = \sum m_{\sigma}\sigma^{-1}$. Then for all $x \in F$, $y \in E^{\perp}$ we have $(\bar{r}x,y) = (x,ry) \in (x,F^{\perp}) = 0$. By duality, this means that $\bar{r}F \subset E$, contradicting assumption (b) of the lemma. This proves the lemma.

Remark. It is clear from the proof that the condition that G is abelian can be replaced by the condition that every left ideal of $\mathbb{Q}[G]$ is a two-sided; or, equivalently, that $\mathbb{Q}[G]$ is isomorphic, as a ring, to a product of division rings. We classify such groups at the end of this note. For groups G not satisfying this condition the lemma is wrong.

Proof of the Theorem. First assume that K is imaginary. There is a surjective G-homomorphism $(G = \mathrm{Gal}(K/\mathbb{Q}))$

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\psi} (K \otimes_{\mathbb{Q}} \mathbb{R})^{*}$$

derived from the isomorphism $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}^{\frac{1}{2}[K:\mathbb{Q}]}$ (as $\mathbb{R}$-algebras) and the exponential map $\mathbb{C} \to \mathbb{C}^{*}$. We apply the lemma to

$$M = K \otimes_{\mathbb{Q}} \mathbb{R},$$

$$E = \{x \in M: \exists\, n \in \mathbb{Z}: \psi(x) = 2^{n} \cdot (\text{a unit in } K^{*})\},$$

$$F = E \cdot \{x \in M: \psi(x) \in K^{*}, \text{ and every prime ideal occurring in } (\psi(x)) \text{ lies over } p\}$$

where p is a fixed odd prime splitting completely in $K/\mathbb{Q}$. The conditions of the lemma are easy consequences of the Dirichlet unit theorem and the finiteness of the class number. Also, F is finitely generated. By the lemma, F is dense in M so $\psi[F]$ is a finitely generated subgroup of K^* which is dense in $(K \otimes_{\mathbb{Q}} \mathbb{R})^*$, as required.

Next let K be real. This case can be dealt with by a similar argument, the main difference being that ψ is not onto but has a cokernel $\cong (\mathbb{Z}/2\mathbb{Z})^{[K:\mathbb{Q}]}$; this group is finite, and the result follows easily.

Alternatively, the case of real K can be dealt with by reducing it to the imaginary case: if $W \subset K(i)^*$ is dense in $(K(i) \otimes_{\mathbb{Q}} R)^*$, then $N_{K(i)/K}[W] \subset K^*$ is dense in a subgroup of finite index in $(K \otimes_{\mathbb{Q}} \mathbb{R})^*$.

Generally, this argument proves: if an algebraic number field K has a finitely generated subgroup $W \subset K^*$ which is dense in $(K \otimes_{\mathbb{Q}} \mathbb{R})^*$, then the same statement is true for every subfield of K.

Conversely, the case of imaginary K can be reduced to the case of real K, by an argument which yields in fact the following more general result:

Observation. Let K be a totally imaginary quadratic extension of a totally real number field K^+, and suppose that there exists a finitely generated subgroup $W^+ \subset (K^+)^*$ which is dense in $(K^+ \otimes_{\mathbb{Q}} \mathbb{R})^*$. Then there exists a finitely generated subgroup $W \subset K^*$ which is dense in $(K \otimes_{\mathbb{Q}} \mathbb{R})^*$.

The proof depends on the following reformulation.

Reformulation. Let $K/\mathbb{Q}$ be finite. Equivalent are:

(a) some finitely generated subgroup $W \subset K^*$ is dense in $(K \otimes_{\mathbb{Q}} \mathbb{R})^*$;

(b) every continuous character $\chi: (K \otimes_{\mathbb{Q}} \mathbb{R})^* \to \mathbb{C}^*$ mapping K^* to the roots of unity has finite order;

(c) every Hecke character of K which, as a function on ideals, assumes only roots of unity as its values, is of finite order.

Here (b) $\Leftrightarrow$ (c) is straightforward; (a) $\Rightarrow$ (b): if $\chi[K^*] \subset$ {roots of unity} then $\chi|W$ is of finite order, so also $\chi|\bar{W} = (K \otimes_{\mathbb{Q}} \mathbb{R})^*$; (b) $\Rightarrow$ (a), finally, is an exercise in topological algebra which is left to the reader; it relies on the classification of closed subgroups of finite dimensional real vector spaces.

A character $\chi: (K \otimes_{\mathbb{Q}} \mathbb{R})^* \to \mathbb{C}^*$ can uniquely be written as

$$\chi(x) = \prod_{\sigma} (\sigma x/|\sigma x|)^{n_\sigma} \cdot |\sigma x|^{c_\sigma} \qquad n_\sigma \in \mathbb{Z}, \quad c_\sigma \in \mathbb{C}$$

for $x \in (K \otimes_{\mathbb{Q}} \mathbb{R})^*$, where σ ranges over a set of orbit representatives of the set of $\mathbb{R}$-algebra homomorphisms $K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C}$ under the action of complex conjugation. If K is totally imaginary quadratic over K^+, with K^+ totally real, then the set of σ's for K can be identified with the set of σ's for K^+.

To prove the observation, assume that $\chi(x)$ is a root of unity for all $x \in K^*$. We wish to prove that χ is of finite order. Assuming the result for K^+, we know that $\chi|(K^+ \otimes_{\mathbb{Q}} \mathbb{R})^*$ has finite order; since $\sigma x/|\sigma x| = \pm 1$ for all $x \in (K^+ \otimes_{\mathbb{Q}} \mathbb{R})^*$ and all σ, this implies that all c_σ are 0. Now all roots of unity $\chi(x) = \prod_\sigma (\sigma x/|\sigma x|)^{n_\sigma}$, for $x \in K^*$, have squares belonging to the normal closure of K over $\mathbb{Q}$, and therefore have bounded order. This proves the observation.

<u>Theorem</u>. Let G be a finite group. Then every left ideal of $\mathbb{Q}[G]$ is two-sided $\Leftrightarrow$ G is abelian or $G \cong A \oplus C_2^t \oplus Q$ with Q the quaternion group of order 8; C_2 cyclic of order 2; $t \in \mathbb{Z}_{>0}$; and A abelian of odd exponent e, such that the order of $2 \bmod e$ (multiplicatively) is odd.

<u>Proof</u>. If $H \subset G$ is a subgroup, then the left ideal generated by $\sum_{\sigma \in H} \sigma$ is two-sided if and only if H is normal in G. All subgroups $H \subset G$ are normal iff G is abelian or $G \cong A \oplus C_2^t \oplus Q$ with Q, C_2, t as above and A abelian of odd order (Huppert, Endliche Gruppen I, Ch. III, Satz 7.12). For abelian groups the theorem is clear. So let $G \cong B \oplus Q$, B abelian. Then $\mathbb{Q}[G] = \mathbb{Q}[B] \otimes_{\mathbb{Q}} \mathbb{Q}[Q]$, where $\mathbb{Q}[B]$ is a product of cyclotomic fields $\mathbb{Q}(\zeta_f)$, f dividing $\exp(B)$, each repeated a number of times, and $\mathbb{Q}[Q] \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H}_{\mathbb{Q}}$, $\mathbb{H}_{\mathbb{Q}} = ((-1,-1)/\mathbb{Q})$. So $\mathbb{Q}[G]$ is a direct product of fields $\mathbb{Q}(\zeta_f)$ and algebras $((-1,-1)/\mathbb{Q}(\zeta_f))$, $f|\exp(B)$, and each ideal of $\mathbb{Q}[G]$ is two-sided if and only if none of the rings $((-1,-1)/\mathbb{Q}(\zeta_f))$ is a 2×2-matrix

ring, for $f \mid \exp(B)$. If $f \leq 2$ this condition is of course satisfied. For $f > 2$, the field $\mathbb{Q}(\zeta_f)$ is totally complex, so $((-1,-1)/\mathbb{Q}(\zeta_f))$ is a 2×2-matrix ring iff $((-1,-1)/\mathbb{Q}(\zeta_f)_{\mathfrak{p}})$ is a 2×2-matrix ring for every prime $\mathfrak{p}$ lying over 2. The invariant of $((-1,-1)/\mathbb{Q}(\zeta_f)_{\mathfrak{p}})$ in the Brauer group $Br(\mathbb{Q}(\zeta_f)_{\mathfrak{p}}) \cong \mathbb{Q}/\mathbb{Z}$ equals $[\mathbb{Q}(\zeta_f)_{\mathfrak{p}} : \mathbb{Q}_2] \cdot (1/2) \bmod \mathbb{Z}$, and we conclude: $((-1,-1)/\mathbb{Q}(\zeta_f))$ is a 2×2-matrix ring for some $f \mid \exp(B)$ iff $[\mathbb{Q}_2(\zeta_{\exp(B)}) : \mathbb{Q}_2]$ is even. The theorem now follows easily. (Acknowledgements to R. W. van der Waall for the reference to Huppert.)