Advanced Studies in Pure Mathematics 17, 1989
Algebraic Number Theory — in honor of K. Iwasawa
pp. 83–87

A Note on Norm-Coherent Units in Certain Z_p-Extensions

Ehud de Shalit

Dedicated to K. Iwasawa, on the occasion of his seventieth birthday

Let K be a number field and L a finite abelian extension of K. One of the major open problems in number theory is to construct a large group of units in L, using transcendental functions associated with K. This has only been accomplished when K is Q or imaginary quadratic, two cases that are distinguished by the absence of units in the base other than roots of unity. Indeed, if we seek a procedure suitable for a wide variety of K, it should rather *not* produce units already in the base field. We therefore introduce the group E_L^0 of units in L whose norm to K is 1, and ask for an explicit group C_L of finite index in E_L^0. In the two mentioned cases C_L is the group of circular or elliptic units, and $[E_L^0: C_L]$ is equal to the class number $h(L)$ (in the elliptic case) or $h(L^+)$ (wnen $K=Q$ and L^+ is the real subfield of L), times a well understood "fudge factor" (see [3] and [8]).

Another feature of both circular and elliptic units is that they appear in norm-coherent sequences in Z_p extensions. This is significant for two reasons. First, we can base a proof of the fact that they are units on their norm-compatibility. Secondly, for *any* norm coherent sequence of units, R. Coleman associates in [2] a certain "generating power series" with coefficients in the completion of K. If the sequence happens to come from (C_{L_n}) $((L_n)$ is the Z_p-tower), this power series is the Taylor expansion of the global function giving the special units. Thus the Coleman power series is an infinitesimal object, midway between the individual unit and the global, transcendental, generating function.

In this note we study units in certain Z_p extensions obtained from torsion points on abelian varieties with complex multiplication. We prove that there are "many" norm coherent sequences of units. In view of the remarks made above, this may be seen as (weak) evidence for the existence of "abelian units".

I would like to thank R. Coleman for suggesting the problem to me.

Received November 19, 1986.

Similar ideas were used by him (unpublished) and by Iwasawa [5] and Gold [4] in the cyclotomic theory.

1.

All number fields are considered as subfields of $\boldsymbol{C}$. Fix a CM field F, $[F:\boldsymbol{Q}]=2g$, and a CM type $\Phi\subset\mathrm{Emb}(F,\boldsymbol{C})$. Let K be a number field and X a g-dimensional abelian variety with complex multiplications by $\mathcal{O}_F$ and type Φ. Both X and $\mathrm{End}(X)$ are assumed to be defined over K. In such a case K contains a CM field F^*, the reflex of (F,Φ) ([7] § 8.5, Proposition 30). Let Φ^* be the reflex CM type, and $\Phi^*_K=\{\sigma\in\mathrm{Emb}(K,\boldsymbol{C})|\sigma|F^*\in\Phi^*\}$. If for any set of embeddings S, we let $\tilde{S}$ be the automorphisms of $\bar{\boldsymbol{Q}}$ extending elements of S, then $\sigma\in\tilde{\Phi}^*_K\Leftrightarrow\sigma^{-1}\in\tilde{\Phi}$.

Let p be a prime that splits completely in both F and K, above which X has good reduction. Let P be a prime of F dividing p,

$$X[P^n]=\{u\in X(\bar{\boldsymbol{Q}})\,|\,\alpha(u)=0\quad\forall\,\alpha\in P^n\},$$

the set of P^n division points in X, and

$$L_n=K(X[P^n]),$$

the field that they generate.

Proposition 1. (i) $\mathrm{Gal}(L_n/K)$ *is cyclic of order* $(p-1)p^{n-1}$.

(ii) *Let* $\mathfrak{p}$ *be a prime of* K *dividing* p. *If* $P\,|\det\Phi^*_K(\mathfrak{p})$, *then* $\mathfrak{p}$ *is totally ramified in* L_∞, *and otherwise it is unramified there. Precisely half the primes* $\mathfrak{p}$ *are ramified in* L_∞.

(iii) *Every prime not above* p *is unramified in* L_∞/L_1.

Proof. Let $[K:\boldsymbol{Q}]=2d$. The notation $\det\Phi$ means the product over all $\sigma\in\Phi$. Clearly $(P,\det\Phi^*_K(\mathfrak{p}))=1$ if and only if $(P,\sigma(\mathfrak{p}))=1$ for all $\sigma\in\Phi^*_K$ (in some Galois extension containing both K and F), if and only if $(\det\Phi(P),\mathfrak{p})=1$, and this happens for d of the $2d$ primes $\mathfrak{p}$ dividing p. Let $R=\mathcal{O}_{K,\mathfrak{p}}$, and consider the p-divisible group $X(P)=(X[P^n])_{n\geq 0}$ over R (X has good reduction at $\mathfrak{p}$ by assumption). Let ψ be the grossencharacter attached to X/K by the theory of complex multiplication. Then $\psi(\mathfrak{p})$ is an endomorphism of X which lifts the absolute Frobenius of the reduction of $X \bmod \mathfrak{p}$. In F, $(\psi(\mathfrak{p}))=\det\Phi^*_K(\mathfrak{p})$. If $(P,\det\Phi^*_K(\mathfrak{p}))=1$, then $X(P)$ is étale over R, and L_∞ is unramified at $\mathfrak{p}$. On the other hand, if $P\,|\det\Phi^*_K(\mathfrak{p})$, then $X(P)$ is connected, and the corre sponding formal group $\hat{X}(P)$ is a Lubin-Tate group of height 1 over R. It follows that the inertia and the decomposition groups of $\mathfrak{p}$ in $\mathrm{Gal}(L_\infty/K)$ coincide, and their representation in $\mathrm{Aut}(X(P))=\mathcal{O}^\times_{F,P}\cong\boldsymbol{Z}^\times_p$ is onto $\boldsymbol{Z}^\times_p$. Since the full Galois group is also faithfully represented in $\boldsymbol{Z}_p^\times$, $\mathfrak{p}$ does not decompose in L_∞, and is therefore totally ramified. This proves (i) and (ii). Part (iii) follows from the well-known fact that only primes dividing p may ramify in a $\boldsymbol{Z}_p$ extension. Incidentally it shows that X has good reduction everywhere over L_1.

2.

Let E_n be the group of units in L_n,

$$E_n^0=\{u\in E_n \mid N_{n,0}(u)=1\},$$
$$E_n'=\bigcap{}_{m\geq n} N_{m,n}E_m, \qquad (N_{m,n}=N_{L_m/L_n}).$$

Choose any of the primes $\mathfrak{p}$ that ramify in L_∞/K. Let Φ_n be the localization of L_n at the unique prime above $\mathfrak{p}$. Since $\Phi_0\cong\boldsymbol{Q}_p$ and Φ_n is the n^{th} layer in the division tower of a Lubin Tate group, the only unit in Φ_0 that is a universal norm from Φ_∞ is 1. A fortiori, no unit of K other than 1 is a universal norm from L_∞, and $E_n'\subset E_n^0$. Clearly $rank\, E_n^0=rank\, E_n-(d-1)$. Our aim is to show that $rank\, E_n'=rank\, E_n^0$. In other words $[E_n: E_n'E_0]<\infty$.

Theorem 2. *Assume that Leopoldt's conjecture holds in K. Let h_n be the p-part of the class number of L_n. Then*

(i) $[E_n^0: E_n'] \mid h_n$,

(ii) *Every $e_n\in E_n'$ appears in a norm-coherent sequence $(e_m)\in \varprojlim E_m$.*

3.

Proof. Let A_n be the p-part of the class group Cl_n of L_n. Let $m\geq n\geq 1$, and $\mathfrak{g}=\mathrm{Gal}\,(L_m/L_n)$, a cyclic group of order p^{m-n}. Consider the two exact sequences

$$(1) \qquad 1\longrightarrow E_m\longrightarrow L_m^\times\longrightarrow P_m\longrightarrow 1$$

$$(2) \qquad 1\longrightarrow P_m\longrightarrow I_m\longrightarrow Cl_m\longrightarrow 1,$$

where I_m is the group of fractional ideals, and P_m the subgroup of principal ones. As in [5] it is easy to get from (1) and (2) a long exact sequence in Galois cohomology (we abbreviate $H^i(-)=H^i(\mathfrak{g}, -)$):

$$(3) \qquad 0\longrightarrow H^1(E_m)\longrightarrow (I_m^{\mathfrak{g}}/P_n)(p)\longrightarrow A_m^{\mathfrak{g}}$$
$$\longrightarrow \mathrm{Ker}\,(H^2(E_m)\longrightarrow H^2(L_m^\times))\longrightarrow 0.$$

Here $M(p)$ is the p-primary part of M. Since $\mathfrak{g}$ is cyclic we obtain the exact sequence

$$(4)\quad 0 \longrightarrow H^1(E_m) \longrightarrow (I_m^{\mathfrak{g}}/P_n)(p) \longrightarrow A_m^{\mathfrak{g}} \longrightarrow E_n \cap N_{m,n} L_m^{\times}/N_{m,n}E_m \longrightarrow 0.$$

From Herbrand's quotient ([6], ch. IX)

$$(5)\qquad Q(E_m) = \frac{|H^2(E_m)|}{|H^1(E_m)|} = \frac{1}{p^{m-n}},$$

and from (4), we derive the formula

$$(6)\qquad |A_m^{\mathfrak{g}}| = p^{(d-1)(m-n)} \cdot |A_n| \cdot [E_n : E_n \cap N_{m,n} L_m^{\times}]^{-1}.$$

We have used the fact, that in view of Proposition 1,

$$|(I_m^{\mathfrak{g}}/P_n)(p)| = [I_m^{\mathfrak{g}} : I_n] \cdot |A_n| = p^{d(m-n)} \cdot |A_n|.$$

Note also that (4) implies

$$(7)\qquad [E_n \cap N_{m,n} L_m^{\times} : N_{m,n} E_m] \,\big|\, |A_m^{\mathfrak{g}}|.$$

4.

Assume now that *Leopoldt's conjecture* holds in K.

Lemma 3. *There exists an integer ν, independent of n, such that for all $n \geq \nu$*

$$E_0^{(p-1)p^{n-1}} \subset N_{n,0} E_n \subset E_0^{p^{n-\nu}}.$$

Proof. The inclusion on the left is obvious, since $E_n \supset E_0$. To prove the one on the right fix an embedding of $\bar{\boldsymbol{Q}}$ in $\bar{\boldsymbol{Q}}_p$ and let $\sigma_1, \cdots, \sigma_d$ be the embeddings of K in $\bar{\boldsymbol{Q}}$ for which the corresponding induced primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_d$ are totally ramified. Let $\varepsilon_1, \cdots, \varepsilon_{d-1}$ be a fundamental system of units in $E_0 = \mathcal{O}_K^{\times}$ and put $\varepsilon_d = 1 + p$. Then Leopoldt's conjecture asserts that

$$(8)\qquad \det(\log_p \sigma_i(\varepsilon_j))_{1 \leq i, j \leq d} \neq 0$$

where $\log_p$ is the p-adic logarithm. If we let $U = \prod_{1 \leq i \leq d} \mathcal{O}_{K,\mathfrak{p}_i}^{\times}$, $\bar{E}_0 =$ the closure of E_0 in U, and $\langle \bar{E}_0 \rangle =$ its pro-p part, (8) implies that the $\boldsymbol{Z}_p$-rank of $\langle \bar{E}_0 \rangle$ is $d-1$. Now at each $\mathfrak{p}_i$ the localization of the extension L_n/K is totally ramified of degree $(p-1)p^{n-1}$ so the local norms of units fall into $1 + p^n \boldsymbol{Z}_p$ (identifying $K_{\mathfrak{p}_i}$ with $\boldsymbol{Q}_p$). Thus $N_{n,0} E_n \subseteq U^{p^{n-1}}$. If a ν as in the statement of the lemma does not exist, we can choose a sequence $\{e_i\}$, $e_i \in E_0$, $e_i \notin E_0^p$, $e_i \to 1$ in U, contradicting Leopoldt's conjecture.

Remark. K is totally imaginary, and for any complex conjugation ρ

of $\bar{Q}$, $\mathrm{Emb}(K, \bar{Q})=\{\sigma_i\}\cup\{\rho\circ\sigma_i\}$, so we could write Leopoldt's conjecture in the form (8). However, unless K is CM, the validity of (8) is not known to be independent of $\{\sigma_1, \cdots, \sigma_d\}$, so it should really be called "Leopoldt's conjecture for K, p, and $\{\sigma_1, \cdots, \sigma_d\}$". It is known, of course, for abelian K, as a result of the work of Baker and Brumer [1].

5.

We are now in a position to conclude the proof of Theorem 2. Lemma 3 implies that the indices

$$[N_{n,0}E_n : E_0^{(p-1)p^{n-1}}]$$

are bounded independently of n. Since for $m\geq n$

$$[N_{n,0}E_n : E_0^{(p-1)p^{n-1}}]=[N_{n,0}E_n^{p^{m-n}} : E_0^{(p-1)p^{m-1}}]\,|\,[N_{m,0}E_m : E_0^{(p-1)p^{m-1}}],$$

they are increasing, hence fixed for large n. Thus

$$[N_{n,0}E_n : N_{m,0}E_m]=p^{(d-1)(m-n)} \tag{9}$$

for $m\geq n\gg 0$.

Consider the groups E_n^0. For $m\geq n\gg 0$

$$\begin{aligned}[E_n^0 : N_{m,n}E_m^0]&=\frac{[E_n : N_{m,n}E_m]}{[N_{n,0}E_n : N_{m,0}E_m]} \qquad \text{(snake lemma)}\\ &=\frac{[E_n : E_n\cap N_{m,n}L_m^\times][E_n\cap N_{m,n}L_m^\times : N_{m,n}E_m]}{p^{(m-n)(d-1)}}\\ &=|A_n|\cdot|A_m^{\mathfrak{g}}|^{-1}\cdot[E_n\cap N_{m,n}L_m^\times : N_{m,n}E_m]\,\big|\,|A_n|,\end{aligned}$$

(use (9), (6) and (7)). This proves part (i), and (ii) is an easy consequence of it.

6.

The following lemma is part of the folklore, but since we did not find it in the literature, and since it fits into the spirit of this note, we bring it up here.

Lemma 4. *Let $e_n\in L_n^\times$ $(n\geq 1)$ and assume that $(\forall m\geq n)$ $N_{m,n}e_m=e_n$. Then e_n is an S-unit, where $S=\{\mathfrak{p}_1, \cdots, \mathfrak{p}_d\}$ is the set of primes that ramify in L_∞/L_1.*

Proof. Let ψ be the grossencharacter of L_1 (not K this time!) associated by the theory of complex multiplication to X/L_1. Since X has good reduction everywhere over L_1, ψ is unramified. Let $\mathfrak{q}$ be a prime of L_1 which is unramified in L_∞. Then the decomposition group of $\mathfrak{q}$ in L_∞/L_1 maps, under the representation of $\mathrm{Gal}(L_\infty/L_1)$ in $\boldsymbol{Z}_p^\times = \mathrm{Aut}(X(P))$, to the *open* subgroup generated by $\psi(\mathfrak{q})$. It follows that $\mathfrak{q}$ is finitely decomposed in L_∞. Let n_0 be such that every prime above $\mathfrak{q}$ is inert in L_∞/L_{n_0}. As $e_n = N_{m,n}e_m$ for $m \geq n \geq n_0$, the $\mathfrak{q}$-adic valuations of e_n are divisible by arbitrarily high powers of p. Hence, e_n is a unit above $\mathfrak{q}$ for $n \geq n_0$, therefore also for all $n \geq 1$.

Lemma 4 remains valid even without the assumption that p splits completely in K or F. The proof, which is a modified version of the one given above, is left to the reader (L_n is defined as in § 1).

References

[1] A. Brumer, On the units of algebraic number fields, Mathematika, **14** (1967), 121–124.

[2] R. Coleman, Division values in local fields, Invent. Math., **53** (1979), 91–116.

[3] R. Gillard-G. Robert, Groupes d'unites elliptiques, Bull. Soc. Math. France, **107** (1979), 305–317.

[4] R. Gold, Rational Coates-Wiles series, Illinois J. Math., **28** (1984), 379–382.

[5] K. Iwasawa, On cohomology groups of units for $\boldsymbol{Z}_p$ extensions, Amer. J. Math., **105** (1983), 189–200.

[6] S. Lang, Algebraic Number Theory, Addison-Wesley (1970).

[7] G. Shimura, Y. Taniyama, Complex multiplication of abelian varieties, Publ. Math. Soc. Japan, **6** (1961).

[8] W. Sinnot, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math., **62** (1980), 181–234.

Current address:
Institute of Mathematics
and Computer Science
The Hebrew University of Jerusalem
Givat Ram, 91904 Jerusalem