59. Z_p-independent Systems of Units

By Claude LEVESQUE

Département de mathématiques et de statistique, Université Laval, Canada

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1992)

Abstract: Some systems of units known to be independent over $\boldsymbol{Z}$ are shown to be independent over some rings of p-adic integers.

§1. Introduction. Let p be a prime and let $\boldsymbol{Z}_p$ denote the ring of p-adic integers. In this note we plan to exhibit for a fixed prime p some $\boldsymbol{Z}_p$-independent systems of units. The motivation of this study is Leopoldt's conjecture for a finite algebraic extension K of $\boldsymbol{Q}$, which states that for every prime p the $\boldsymbol{Z}_p$-rank of the group E_K of units (modulo torsion) of K is equal to the $\boldsymbol{Z}$-rank of E_K; see [8] for the definitions and the details. Thanks to J. Ax and A. Brumer [1], Leopoldt's conjecture is known to hold true if K is abelian over $\boldsymbol{Q}$ or if K is in an abelian extension of some imaginary quadratic field.

Though transcendence methods are rather natural and quite powerful to deal with Leopoldt's conjecture (see [7]), a few mathematicians developed interesting algebraic methods to study this problem. For instance J. Buchmann and J. Sands [2, 3, 6] gave appealing algebraic characterizations of the conjecture. Moreover they explicitly exhibited two infinite parameterized families of fifth degree fields, whose Galois closure has Galois group isomorphic to the symetric group S_5 and whose unit group rank is two (resp. three), for which Leopoldt's conjecture is true for a fixed prime $p(\neq 5)$. The criterion that J. Buchmann and J. Sands used in [3] gives, for a fixed prime p, a necessary and a sufficient condition for a set of units to be independent over $\boldsymbol{Z}_p$. In the following section we will quote this criterion and, given a fixed prime p, we will use it to exhibit some parameterized families of pure fields of degree n for which a $\boldsymbol{Z}$-independent system of $\tau(n)-1$ units will be shown to be $\boldsymbol{Z}_p$-independent. Here $\tau(n)$ denotes the number of positive divisors of n, so $\tau(n)-1$ is a large number if n is divisible by many different primes.

§2. Systems of units. Let us consider the pure field $K=\boldsymbol{Q}(\omega)$ of degree n over $\boldsymbol{Q}$ where

$$\omega:=\sqrt[n]{D^n \pm 1}>1 \text{ with } D \in \boldsymbol{N},$$

and let us define ε_t by

$$\varepsilon_t:=\omega^t-D^t.$$

Then (under more general hypotheses) it was proved by F. Halter-Koch and H. -J. Stender [5] (cf. [4]) that

$$S:=\{\varepsilon_t: t \in \boldsymbol{N},\ t \mid n,\ t \neq n\}$$

is a $\boldsymbol{Z}$-independent system of $\tau(n)-1$ units of K. We want to prove the following result.

Theorem 2.1. *Let p be a fixed odd prime divisor of D such that $(p, n) = 1$. Then S is a $\boldsymbol{Z}_p$-independent system of units.*

Let us consider a set $\tilde{S}$ of r units of a field K which generates a group of finite index in the group generated by a fixed $\boldsymbol{Z}$-independent set S_0 of r units, and such that all the units of $\tilde{S}$ are congruent to 1 modulo (p^k) for some fixed integer $k \geq 1$; here (p^k) is the ideal of the ring O_K of integers of K generated by p^k. Consider $\langle \tilde{S} \rangle$, the group of units generated by $\tilde{S}$, and as in [3] define ϕ_k the homomorphism of the multiplicative group $\langle \tilde{S} \rangle$ into the additive group O_K/pO_K by

$$\phi_k(1 + p^k\alpha) = \alpha + pO_K.$$

Let us state a result which is contained in Corollary 2.4 of [3].

Proposition 2.2. *A set $\tilde{S}$ of r units congruent to 1 modulo (p^k) is $\boldsymbol{Z}_p$-independent if the image of $\langle \tilde{S} \rangle$ by ϕ_k in O_K/pO_K has dimension r as a vector space over $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$.*

To prove Theorem 2.1, we want to use the criterion of the last proposition. First note that

$$\begin{aligned}\varepsilon_t^{n/t} &= (\omega^t - D^t)^{n/t} \\ &= \pm 1 + D^n + \sum_{j=1}^{n/t} \binom{n/t}{j} \omega^{n-tj}(-D^t)^j \\ &= \pm 1 + \binom{n}{t}(-D)^t\omega^{n-t} + D^{t+1}\alpha_t\end{aligned}$$

for some algebraic integer $\alpha_t \in O_K$. Letting $c = 1$(resp. 2) if $\omega^n = D^n + 1$ (resp. $D^n - 1$), we deduce

$$\varepsilon_t^{cn/t} = 1 - (-1)^{c+t}c\binom{n}{t} D^t\omega^{n-t} + D^{t+1}\beta_t$$

for some algebraic integer $\beta_t \in O_K$. Therefore we conclude that for all positive divisors t of n, $t \neq n$, we have

$$\eta_t := \varepsilon_t^{c\frac{n}{t}D^{n-t}} = 1 - (-1)^{c+t}c\binom{n}{t} D^n\omega^{n-t} + D^{n+1}\gamma_t$$

for some algebraic integer $\gamma_t \in O_K$.

Let us assume that s is an integer such that $p^s \parallel D$ (i.e., $p^s \mid D$ and $p^{s+1} \nmid D$). So we can count on the system

$$\tilde{S} := \{\eta_t : t \in \boldsymbol{N},\ t \mid n, t \neq n\}$$

of $\tau(n) - 1$ units which are all congruent to 1 modulo $p^{ns}O_K$. Taking $k = ns$ in Proposition 2.2, we have for all divisors t of n,

$$\phi_{ns}(\eta_t) = (-1)^{c+t+1}c\binom{n}{t}\left(\frac{D}{p^s}\right)^n \omega^{n-t} + pO_K.$$

Now the hypotheses that p^s is the exact power of p dividing D and that $(p, n) = 1$ imply that the coefficient of ω^{n-t} is coprime to p. In order to conclude that $\tilde{S}$ is $\boldsymbol{Z}_p$-independent, we only have to show by Proposition 2.2 that the image of the set $\{\omega^{n-t} : t \in \boldsymbol{N},\ t \mid n,\ t \neq n\}$ is a set of independent images under ϕ_{ns} in the $\boldsymbol{F}_p$-vector space O_K/pO_K. Denote by d_f the discriminant of the minimal polynomial f of ω, so $d_f = n^n m^{n-1}$ with $m = D^n \pm 1$. Then we have the conclusion since the powers $\omega^j (j = 0,1,\ldots,n-1)$ form a basis for an order of O_K of index dividing d_f and since $(d_f, p) = 1$.

In summary, an application of Proposition 2.2 gives that $\tilde{S}$ is $\boldsymbol{Z}_p$-independent. Since $\langle \tilde{S} \rangle$ is of finite index in $\langle S \rangle$ we conclude (as in Chapter II of [3]) that S is also $\boldsymbol{Z}_p$-independent.

§3. Concluding remarks. Of course if $p_i^{m_i} \| D$ for some prime integers $p_i (i = 1, \ldots, l)$, we have that S is a $\boldsymbol{Z}_{p_i}$-independent system of units for $i = 1, \ldots, l$, but this says nothing about the infinitude of the primes q such that S is $\boldsymbol{Z}_q$-independent. Finally note that the above proof works for $p = 2$ under the assumptions that $(2, n) = 1$ and that a sufficiently high power of 2 divides D (since the contribution of 2 in cn/t has to be taken into account): the integer k of Proposition 2.2 has to be adjusted accordingly.

Acknowledgements. The author is grateful to Dr. Jonathan Sands for stimulating conversations. The first draught of this paper was written during a sabbatical stay at Florida Atlantic University and benefitted from the financial support of NSERC (Canada) and FCAR (Québec).

References

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

[2] Buchmann, J. and Sands, J.: An algorithm for testing Leopoldt's conjecture. J. Number Theory, **27**, 92–105 (1987).

[3] ——: Leopoldt's conjecture in parameterized families. Proc. of the AMS, **104**, no. 1, 43–48 (1988).

[4] Frei, G. and Levesque, C.: On an independent system of units in the field $K = \boldsymbol{Q}(\sqrt[n]{D^n + d})$ where $d \mid D^n$. Abh. Math. Univ. Hamburg, **51**, 160–163 (1980).

[5] Halter-Koch, F. and Stender, H.-J.: Unabhängige Einheinten für die Körper $K = \boldsymbol{Q}(\sqrt[n]{D^n + d})$ mit $d \mid D^n$. ibid., **42**, 33–40 (1974).

[6] Sands, J.: Kummer's and Iwasawa's version of Leopoldt's conjecture. Canad. Math. Bul., **31**, 338–346 (1988).

[7] Waldschmidt, M.: Transcendance et exponentielles en plusieurs variables. Invent. Math., **63**, 97–127 (1981).

[8] Washington, L.: Introduction to Cyclotomic Fields. Graduate Texts in Math., Springer-Verlag (1982).