ACTA ARITHMETICA
LI (1988)

Minkowski units in certain metacyclic fields

by

ROMAN MARSZAŁEK (Wrocław)

1. Let K be a normal extension of the rationals with metacyclic Galois group of order pm, where p is a prime and $m|p-1$. The main result of this paper (Theorem 2) yields certain necessary conditions for K to have a Minkowski unit; in case of prime m and small p they are also sufficient (Theorem 2 (iii)). The first of these conditions (conditon (b)) is a relation involving the class numbers of certain subfields of K, condition (c) requires the surjectivity of the norm from the units in K to those in the only normal proper subfield of K, and condition (d) requires the existence of a Minkowski unit in the above-mentioned subfield.

Our results are similar to those obtained by D. Duval ([2], Théorème 5.2) concerning real fields with Galois groups of the type (p, p). We shall also correct a mistake in the papers of N. Moser [5] and [6] (Lemme VI.5 and Lemme 4.4, respectively).

We shall use the following notation and definitions:

For any number field Λ we put:

U_Λ = the group of units in Λ,

V_Λ = the group of roots of unity in Λ,

E_Λ = the quotient group U_Λ/V_Λ.

If Λ is normal, then the above abelian groups have a natural structure of $\mathbf{Z}[\mathrm{Gal}(\Lambda/Q)]$-modules. For any group Γ acting on a set X, we define:

$X^\Gamma = \{x \in X\colon \gamma x = x, \gamma \in \Gamma\}$,

$\Gamma^\sim = \sum_{\gamma\in\Gamma} \gamma \in \mathbf{Z}[\Gamma]$,

$\langle\gamma\rangle$ = the subgroup of Γ generated by $\gamma \in \Gamma$.

We say that a normal extension Λ of the rationals with $\Gamma = \mathrm{Gal}(\Lambda/Q)$ has a *Minkowski unit* if E_Λ is a cyclic $\mathbf{Z}[\Gamma]$-module. In the case of real Λ this holds if and only if Λ has a conjugate system of fundamental units.

Let M_1, M_2 be $\mathbf{Z}[\Gamma]$-modules and let f be a 1-cocycle from

$Z^1(\Gamma, \mathrm{Hom}_Z(M_2, M_1))$. Recall that f is a map $\Gamma \to \mathrm{Hom}_Z(M_2, M_1)$ such that if we write $f(\gamma)(m) = f_\gamma(m)$, then for all $m \in M_2$ and $\gamma, \delta \in \Gamma$ we have

$$f_{\gamma\delta}(m) = \gamma f_\delta(m) + f_\gamma(\delta m).$$

On the Z-direct sum $M_1 \oplus M_2$ we can define the *action of* Γ by

$$\gamma(m_1, m_2) = (\gamma m_1 + f_\gamma(m_2), \gamma m_2)$$

for $\gamma \in \Gamma$ and $m_1 \in M_1$, $m_2 \in M_2$. The $Z[\Gamma]$-module M obtained in this way is denoted by $(M_1, M_2; f)$. If the choice of the cocycle f is obvious we write simply $M = (M_1, M_2)$. The $Z[\Gamma]$-module M is called an *extension* of M_1 by M_2.

2. Let G be a metacyclic group of order pm, where p is a prime and $m|p-1$. Thus

$$G = \{\sigma^i\tau^j \colon i = 0, \ldots, p-1; j = 0, \ldots, m-1\}$$

and $\tau\sigma = \sigma^r\tau$, where r is an mth primitive root of unity mod p.

Let K be a normal extension of the rationals with $\mathrm{Gal}(K/Q) = G$. We put:

$k = K^{\langle\sigma\rangle}$,

$L = K^{\langle\tau\rangle}$,

ζ is a pth primitive root of unity,

A is the ring of integers in $Q(\zeta)$,

$\mathscr{P} = A(1-\zeta)$,

ψ is the automorphism of $Q(\zeta)$ mapping ζ onto ζ^r,

$A_1 = A \cap Q(\zeta)^{\langle\psi\rangle}$,

$\mathscr{P}_1 = A_1 \cap \mathscr{P}$,

θ is an mth primitive root of unity.

On A and $Z[\theta]$ we can introduce a $Z[G]$-module structure in the following way. We let σ act on A as multiplication by ζ, and τ as the automorphism ψ. On $Z[\theta]$, σ acts trivially and τ acts as multiplication by θ. In this way all ideals of $Z[\theta]$ as well as those of A which are ψ-invariant acquire a $Z[G]$-module structure.

Consider the $Z[G]$-modules

$$\tilde{E}_K = \{x \in E_K \colon x^{1+\sigma+\ldots+\sigma^{p-1}} = 1\} \quad \text{and} \quad E_0 = \tilde{E}_K/E_K.$$

Thus E_K is a $Z[G]$-extension of $\tilde{E}_K$ by E_0. It was shown in [5] (Prop. III6) that

$$E_K \simeq \bigoplus_{j=0}^{m-1} \mathscr{P}^{e_j}\mathfrak{a}_j,$$

where $0 \leqslant e_j \leqslant m-1$ and the $\mathfrak{a}_j$ are ideals of A_1, the class of the ideal $\prod_{j=0}^{m-1} \mathfrak{a}_j$ being uniquely determined by E_K. Since σ acts trivially on E_0 one obtains

$$E_K \simeq \left(\bigoplus_{j=0}^{m-1} \mathscr{P}^{e_j}\mathfrak{a}_j, \mathfrak{b}\right), \tag{1}$$

where $\mathfrak{b}$ is a $Z[\langle\tau\rangle]$-module of Z-rank $m-1$.

If we put

$$a = (E_K \colon E_L E_{L^\sigma} \ldots E_{L^{\sigma^{m-1}}} E_k),$$

then by Théorème 7 of [3] we get the equality

$$h_K p^{(m-1)(m+2)/2} = a h_k h_L^m. \tag{2}$$

3. We now give a necessary condition for K to have a Minkowski unit in the general case:

THEOREM 1. *If a real metacyclic extension K of degree pm over Q has a Minkowski unit, then*

$$h_k h_L^m = p^t h_K \quad \textit{with } t \geqslant m-1.$$

Proof. Using the formula $\tau^j\sigma^i = \sigma^{ir^j}\tau^j$ and Corollaire to Proposition I3 of [7], we have

$$E_{\sigma^{jw}(L)} = E_K^{\langle\sigma^j\tau\rangle} = (E_K)^{\langle\sigma^j\tau\rangle} \quad \text{and} \quad E_k = (E_K)^{\langle\sigma\rangle}$$

where $w(r-1) \equiv 1 \pmod p$, $0 \leqslant j \leqslant m-1$. Since $E_K \simeq R = Z[G]/ZG^\sim$, by Proposition I3 of [7], we get

$$(E_K \colon E_L E_{\sigma^w(L)} \ldots E_{\sigma^{w(m-1)}(L)} E_k) = \left(R \colon \sum_{j=0}^{m-1} R^{\langle\sigma^j\tau\rangle} + R^{\langle\sigma\rangle}\right).$$

The index a, however, does not depend on the choice of a generator of $\langle\sigma\rangle$ according to (2), so one has

$$a = \left(R \colon \sum_{j=0}^{m-1} R^{\langle\sigma^j\tau\rangle} + R^{\langle\sigma\rangle}\right).$$

Using Proposition I4 of [7] we obtain

$$a = (R \colon R_1),$$

where $R_1 = \langle\sigma\rangle^\sim R + \sum_{j=0}^{m-1} \langle\sigma^j\tau\rangle^\sim R$.

Since for any subgroup H of G, $G^\sim Z[G]$ is an ideal of $H^\sim Z[G]$, we have a Z-isomorphism

$$Z[G]/T \simeq R/R_1,$$

where $T = \langle\sigma\rangle^{\sim} \boldsymbol{Z}[G]+\sum_{j=0}^{m-1} \langle\sigma^j\tau\rangle^{\sim} \boldsymbol{Z}[G]$.

Now we need

LEMMA 1. *Let $H < G$ and let $G = \bigcup_{i=1}^{N} Hg_i$ be the decomposition of G into the union of disjoint right cosets. Then*

$$H^{\sim}\boldsymbol{Z}[G] = H^{\sim} \sum_{i=1}^{N} \boldsymbol{Z}g_i.$$

Proof. Since for every $y \in \boldsymbol{Z}[G]$

$$y = \sum_{h\in H} \sum_{i=1}^{N} a_{hg_i} hg_i,$$

one obtains

$$H^{\sim} y = \sum_{x\in H} \sum_{i=1}^{N} \sum_{w\in H} a_{hg_i} xhg_i = \sum_{x\in H} \sum_{i=1}^{N} \sum_{w\in H} a_{x^{-1}wg_i} wg_i$$

by substituting $w = xh$. Finally,

$$H^{\sim} y = \sum_{w\in H} w \sum_{i=1}^{N} \Big(\sum_{x\in H} a_{x^{-1}wg_i}\Big)g_i.$$

This lemma gives

$$T = \langle\sigma\rangle^{\sim} \boldsymbol{Z}[\langle\tau\rangle]+\sum_{j=0}^{m-1} \langle\sigma^j\tau\rangle^{\sim} \boldsymbol{Z}[\langle\sigma\rangle].$$

Now we shall use the formula

$$a = (Z[G]:T) \tag{3}$$

to estimate the index a. For convenience we shall assume that arithmetical operations on indices running from 0 to $p-1$ are performed mod p. If $x = \sum_{i=0}^{p-1} \sum_{j=0}^{m-1} \lambda_{ij}\tau^j\sigma^i \in \boldsymbol{Z}[G]$ is an element of T, then there exist rational integers a_{ij} and ω_j such that

$$x = \sum_{i=0}^{p-1} \sum_{j=0}^{m-1} \omega_j\tau^j\sigma^i+\sum_{s=0}^{m-1} \sum_{h=0}^{p-1} a_{hs}\Big(\sum_{j=0}^{m-1} (\sigma^s\tau)^j\Big)\sigma^h.$$

Applying the formula $\sigma^i\tau^j = \tau^j\sigma^{i\bar{r}^j}$ $(r\bar{r} \equiv 1 \pmod p)$, we have

$$(\sigma^s\tau)^j = \tau^j\sigma^{s\varphi_j}$$

where $\varphi_0 = 0$, $\varphi_j = \bar{r}+\bar{r}^2+\ldots+\bar{r}^j$ with $1 \leqslant j \leqslant m-1$. Thus

$$x = \sum_{s=0}^{m-1} \sum_{j=0}^{m-1} \sum_{h=0}^{p-1} a_{hs}\tau^j\sigma^{s\varphi_j+h}+\sum_{i=0}^{p-1} \sum_{j=0}^{m-1} \omega_j\tau^j\sigma^i = \sum_{i=0}^{p-1} \sum_{j=0}^{m-1} \Big(\omega_j+\sum_{s=0}^{m-1} a_{i-s\varphi_j,s}\Big)\tau^j\sigma^i$$

by substituting $i = s\varphi_j+h$ in the first term. It follows that

$$\lambda_{ij} = \omega_j+\sum_{s=0}^{m-1} a_{i-s\varphi_j,s}, \tag{4}$$

where $0 \leqslant i \leqslant p-1$, $0 \leqslant j \leqslant m-1$.

Let $\mu_{ij} = \lambda_{ij}-\lambda_{i0}$ and let, for $1 \leqslant d \leqslant m-2$ and $d+1 \leqslant j \leqslant m-1$, $x_{hj}^{(d)}$ be integer solutions of the following system of linear congruences:

$$\sum_{h=1}^{d} x_{hj}^{(d)}\varphi_h^{d-w}+\varphi_j^{d-w} \equiv 0 \pmod p, \tag{5}$$

where $0 \leqslant w \leqslant d-1$. The system (5) is always solvable because $0, \varphi_1, \ldots, \varphi_d$ are distinct mod p.

Now we shall show that

$$F_j^{(0)} = \sum_{i=0}^{p-1} \mu_{ij} \equiv 0 \pmod p \tag{6}$$

for $1 \leqslant j \leqslant m-1$ and

$$F_j^{(d)} = \sum_{i=0}^{p-1} i^d\Big(\mu_{ij}+\sum_{h=1}^{d} x_{hj}^{(d)}\mu_{ih}\Big) \equiv 0 \pmod p \tag{7}$$

for $1 \leqslant d \leqslant m-2$, $d+1 \leqslant j \leqslant m-1$. The congruences (6) follow immediately from (4). To prove (7), we use (4) to get

$$\begin{aligned} F_j^{(d)} = {} & \Big[\omega_j-\omega_0+\sum_{h=1}^{d} x_{hj}^{(d)}(\omega_h-\omega_0)\Big] \sum_{i=0}^{p-1} i^d \\ & +\sum_{i=0}^{p-1} i^d \sum_{s=0}^{m-1} a_{i-s\varphi_j,s}-\sum_{i=0}^{p-1} i^d \sum_{s=0}^{m-1} a_{is} \\ & +\sum_{i=0}^{p-1} i^d \sum_{h=1}^{d} x_{hj}^{(d)} \sum_{s=0}^{m-1} a_{i-s\varphi_h,s}-\sum_{i=0}^{p-1} i^d \sum_{h=1}^{d} x_{hj}^{(d)} \sum_{s=0}^{m-1} a_{is}. \end{aligned}$$

Since $\sum_{i=0}^{p-1} i^d \equiv 0 \pmod p$ one obtains

$$\begin{aligned} F_j^{(d)} & \equiv \sum_{s=0}^{m-1} \sum_{i=0}^{p-1} \Big\{\sum_{h=1}^{d} x_{hj}^{(d)}[(i+s\varphi_h)^d-i^d]+[(i+s\varphi_j)^d-i^d]\Big\} a_{is} \\ & \equiv \sum_{s=0}^{m-1} \sum_{i=0}^{p-1} \sum_{w=0}^{d-1} \binom{d}{w} s^{d-w} i^d \Big[\varphi_j^{d-w}+\sum_{h=1}^{d} x_{hj}^{(d)}\varphi_h^{d-w}\Big] a_{is} \equiv 0 \pmod p \end{aligned}$$

by (5).

Thus the coordinates of x are zeros of the linear forms $F_j^{(d)}$ which turn out to be linearly independent mod p. To prove this suppose that there are integers $\alpha_j^{(d)}$ such that

$$F = \sum_{j=1}^{m-1} \alpha_j^{(0)} F_j^{(0)} + \sum_{d=1}^{m-2} \sum_{j=d+1}^{m-1} \alpha_j^{(d)} F_j^{(d)}$$

is a linear form with coefficients vanishing mod p.

Though $\alpha_j^{(d)}$ are defined only for $d+1 \leqslant j \leqslant m-1$ we extend their range by putting $\alpha_j^{(d)} = 0$ for $1 \leqslant j \leqslant d$. We also put $x_{hj}^{(d)} = 0$ for $d+1 \leqslant h \leqslant m-1$.

Using (6) and (7), we get

$$\begin{aligned} F &= \sum_{j=1}^{m-1} \sum_{i=0}^{p-1} \alpha_j^{(0)} \mu_{ij} + \sum_{d=1}^{m-2} \sum_{j=d+1}^{m-1} \sum_{i=0}^{p-1} i^d \alpha_j^{(d)} \mu_{ij} + \sum_{i=0}^{p-1} \sum_{d=1}^{m-2} \sum_{j=d+1}^{m-1} \sum_{h=1}^{d} i^d \alpha_j^{(d)} x_{hj}^{(d)} \mu_{ih} \\ &= \sum_{i=0}^{p-1} \sum_{j=1}^{m-1} \sum_{d=0}^{m-2} i^d \alpha_j^{(d)} \mu_{ij} + \sum_{i=0}^{p-1} \sum_{h=1}^{m-1} \sum_{d=1}^{m-2} \sum_{j=d+1}^{m-1} i^d \alpha_j^{(d)} \mu_{ih} \\ &= \sum_{i=0}^{p-1} \sum_{j=1}^{m-1} \Big[\alpha_j^{(0)} + \sum_{d=1}^{m-2} \Big(\alpha_j^{(d)} + \sum_{t=d+1}^{m-1} \alpha_t^{(d)} x_{jt}^{(d)}\Big) i^d\Big] \mu_{ij} \end{aligned}$$

by substituting in the last but one line j for h and t for j in the second term. Since the coefficients of F are all equal to $0 \pmod p$ it follows that for $d+1 \leqslant j \leqslant m-1$

$$\alpha_j^{(0)} + \sum_{d=1}^{m-2} \Big(\alpha_j^{(d)} + \sum_{t=d+1}^{m-1} \alpha_t^{(d)} x_{jt}^{(d)}\Big) i^d \equiv 0 \pmod p.$$

But by definition $x_{jt}^{(d)} = 0$ for $d+1 \leqslant j \leqslant m-1$, so

$$\sum_{d=1}^{m-2} \alpha_j^{(d)} i^d \equiv 0 \pmod p,$$

where $i = 0, \ldots, p-1$. Thus for $d+1 \leqslant j \leqslant m-1$ we obtain

$$\alpha_j^{(d)} \equiv 0 \pmod p,$$

which proves the linear independence mod p of the $m(m-1)/2$ linear forms $F_j^{(d)}$.

Since by Théorème 10 of [3] the index a is a power of p, (3) implies now

$$a = p^w,$$

where $w \geqslant m(m-1)/2$. This together with (2) establishes Theorem 1.

4. Now we shall prove three lemmas.

Lemma 2. *Let M_0, M_1, N be $\boldsymbol{Z}[G]$-modules and*

$$f, f' \in Z^1(G, \mathrm{Hom}_{\boldsymbol{Z}}(M_1, N)), \quad f_0 \in Z^1(G, \mathrm{Hom}_{\boldsymbol{Z}}(M_0, N)).$$

If $\mathrm{Hom}_{\boldsymbol{Z}[G]}(N, M_1) = 0$ and the extensions $(M_1, N; f)$, $(M_1, N; f')$ are $\boldsymbol{Z}[G]$-isomorphic, then there exists a $\boldsymbol{Z}[G]$-isomorphism

$$(M_0 \oplus M_1 \oplus M_1, N; f_0, f, f') \simeq (M_0 \oplus M_1, N; f_0 \nu, f) \oplus M_1,$$

where ν is a suitable automorphism of N.

Proof. Since $\mathrm{Hom}_{\boldsymbol{Z}[G]}(N, M_1) = 0$, we can use Corollary (34.5) of [1]. Thus there exist $\lambda \in \mathrm{Aut}(M_1)$, $\nu \in \mathrm{Aut}(N)$ and $c \in \mathrm{Hom}_{\boldsymbol{Z}}(N, M_1)$ such that

$$\lambda f'_g(m) = f_g(\nu m) + gc(m) - c(gm), \qquad g \in G,$$

and thus we can define a $\boldsymbol{Z}[G]$-isomorphism

$$\Psi\colon (M_0 \oplus M_1 \oplus M_1, N; f_0, f, f') \to (M_0 \oplus M_1, N; f_0 \nu, f) \oplus M_1$$

by putting

$$(m_0, m_1, m'_1, n) \xrightarrow{\Psi} (m_0, 2m_1 - \lambda m'_1 - c(n), \nu n, m_1 - \lambda m'_1 - c(n)).$$

From now on we confine ourselves to the case where $m = q$ is a prime.

Lemma 3. *If γ is a $\boldsymbol{Z}[G]$-generator for the $\boldsymbol{Z}[G]$-module $\boldsymbol{Z}[\theta]$, then*

$$\mathrm{An}(\gamma) = \boldsymbol{Z}[G](1-\sigma) + \boldsymbol{Z}[G]\langle\tau\rangle^{\sim},$$

where $\mathrm{An}(\gamma)$ denotes the annihilator ideal of γ.

Proof. If α, β are $\boldsymbol{Z}[G]$-generators of $\boldsymbol{Z}[\theta]$, then they are units in the ring $\boldsymbol{Z}[\theta]$, so there is a $\boldsymbol{Z}[G]$-isomorphism φ of $\boldsymbol{Z}[\theta]$ such that $\varphi(\alpha) = \beta$. Since $\mathrm{An}(\varphi(\alpha)) = \mathrm{An}(\alpha)$ we may assume $\gamma = 1$. Let

$$x = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{ij} \sigma^i \tau^j \in \boldsymbol{Z}[G]$$

be an element of $\mathrm{An}(1)$. Then

$$x \cdot 1 = \sum_{j=0}^{q-1} \sum_{i=0}^{p-1} a_{ij} \theta^j = \sum_{j=0}^{q-2} \sum_{i=0}^{p-1} (a_{ij} - a_{i,q-1}) \theta^j = 0,$$

so

$$\sum_{i=0}^{p-1} a_{ij} = \sum_{i=0}^{p-1} a_{i,q-1}$$

for $j = 0, \ldots, q-1$. Therefore we have

$$\begin{aligned} x &= \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{i0} \sigma^i \tau^j + \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} (a_{ij} - a_{i0}) \sigma^i \tau^j \\ &= \Big(\sum_{i=0}^{p-1} a_{i0} \sigma^i\Big) \sum_{j=0}^{q-1} \tau^j + \sum_{j=0}^{q-1} \sum_{i=0}^{p-1} (a_{ij} - a_{i0})(\sigma^i \tau^j - \tau^j) \\ &\in \boldsymbol{Z}[G]\langle\tau\rangle^{\sim} + \boldsymbol{Z}[G](1-\sigma). \end{aligned}$$

Since the opposite inclusion is obvious, Lemma 3 is proved.

LEMMA 4. *If $e \geqslant 1$ and $\mathfrak{a}$ is an ideal of A_1 then the $\boldsymbol{Z}[G]$-module $\boldsymbol{Z}[\theta] \oplus \mathscr{P}^e\mathfrak{a}$ is not cyclic.*

Proof. Assume to the contrary that $\boldsymbol{Z}[\theta] \oplus \mathscr{P}^e\mathfrak{a}$ is cyclic with a generator $(\gamma, (1-\zeta)^e u)$. Then, by Lemme 1(i) of [8], γ is a generator of $\boldsymbol{Z}[\theta]$ and $(1-\zeta)^e u$ is a generator of $\mathscr{P}^e\mathfrak{a}$.

If we put $\delta = \sum_{j=0}^{q-1} \psi^j[(1-\zeta)^e u]$, then $\delta \in A_1$, and $\delta \in \mathscr{P}\mathfrak{a}$ since $e \geqslant 1$. It follows that $\delta \in \mathscr{P}_1\mathfrak{a}$; but $\mathscr{P}_1$ totally ramifies in $Q(\zeta)$ and so $\delta \in \mathscr{P}^q\mathfrak{a}$. Now applying the identity

$$\boldsymbol{Z}[G]x = \sum_{j=0}^{q-1} A\psi^j(x),$$

$x \in \mathscr{P}^e\mathfrak{a}$, we obtain

$$\boldsymbol{Z}[G]\langle\tau\rangle^{\sim}(1-\zeta)^e u = \boldsymbol{Z}[G]\cdot\delta = A\delta \subset \mathscr{P}^q\mathfrak{a} \subset \mathscr{P}^{e+1}\mathfrak{a}$$

and

$$\boldsymbol{Z}[G](1-\sigma)(1-\zeta)^e u = \boldsymbol{Z}[G](1-\zeta)^{e+1}u \subset \mathscr{P}^{e+1}\mathfrak{a}$$

because $1 \leqslant e \leqslant q-1$. By Lemma 3

$$\mathrm{An}(\gamma)(1-\zeta)^e u \subset \mathscr{P}^{e+1}\mathfrak{a}.$$

Lemme 1(ii) of [8] now implies that $(\gamma, (1-\zeta)^e u)$ cannot be a generator for $\boldsymbol{Z}[\theta] \oplus \mathscr{P}^e\mathfrak{a}$, contrary to our assumption. This completes the proof of Lemma 4.

Two $\boldsymbol{Z}[G]$-modules M and M' are said to be *in the same genus* if for every prime l, the $\boldsymbol{Z}_l[G]$-modules $\boldsymbol{Z}_{(l)} \otimes M$ and $\boldsymbol{Z}_{(l)} \otimes M'$ are $\boldsymbol{Z}_{(l)}[G]$-isomorphic, where $\boldsymbol{Z}_{(l)}$ is the localization of $\boldsymbol{Z}$ at l.

Now we are able to prove

THEOREM 2. *Let K be a real metacyclic extension of degree pq over Q, where p, q are odd primes for which $q | p-1$, $q^2 \nmid p-1$. Then:*

(i) *If K has a Minkowski unit, then there exists an ideal $\mathfrak{a} \lhd A_1$ and*

(a) $E_K \simeq (\bigoplus_{\substack{j=0 \\ j \neq 1}}^{q-1} \mathscr{P}^j, \boldsymbol{Z}[\theta]) \oplus \boldsymbol{Z}[\zeta]\mathfrak{a}$,

where all extensions $(\mathscr{P}^j, \boldsymbol{Z}[\theta])$ are non-trivial,

(b) $\dfrac{h_k h_L^q}{h_K} = p^{q-1}$,

(c) $N_{K/k}(E_K) = E_k$,

(d) *the field k has a Minkowski unit.*

(ii) *Conditions* (b), (c) *of* (i) *are necessary and sufficient for E_K to be in the same genus as $\boldsymbol{Z}[G]/\boldsymbol{Z}G^{\sim}$.*

(iii) *If the class number of the field $Q(\zeta)^{\langle\psi\rangle}$ is 1, then* (b), (c) *and* (d) *are necessary and suffcient for K to have a Minkowski unit.*

Proof. According to (1)

$$E_K \simeq (\bigoplus_{j=0}^{s} \mathscr{P}^{e_j}\mathfrak{a}_j, \mathfrak{b}) \oplus \bigoplus_{j=s+1}^{q-1} \mathscr{P}^{e_j}\mathfrak{a}_j,$$

where the extensions $(\mathscr{P}^{e_j}\mathfrak{a}_j, \mathfrak{b})$ are non-trivial. The $\boldsymbol{Z}[\langle\tau\rangle]$-module $\mathfrak{b}$ is an ideal of $\boldsymbol{Z}[\theta]$ and by Lemme 2(i) of [8] it must be cyclic; hence, by Proposition 4 of [8] it is isomorphic to $\boldsymbol{Z}[\theta]$. Since, by Proposition 6 of [4], there is exactly one non-trivial extension $(\mathscr{P}^{e_j}, \boldsymbol{Z}[\theta])$ $(e_j \neq 1)$, we may apply Lemma 2 to deduce that the e_j's are distinct for $0 \leqslant j \leqslant s$. Furthermore, Proposition 6 of [8] and the assumption of the cyclicity of E_K yields that, for $s+1 \leqslant j \leqslant q-1$, the e_j's are also distinct. Since there is no non-trivial extension of $\mathscr{P}$ by $\boldsymbol{Z}[\theta]$ (see (3) in [4]), we obtain

$$E_K \simeq (\bigoplus_{\substack{j=0 \\ e_j \neq e_i \\ e_j \neq 1}}^{s} \mathscr{P}^{e_j}\mathfrak{a}_j, \boldsymbol{Z}[\theta]) \oplus \bigoplus_{\substack{j=s+1 \\ e_j \neq e_i}}^{q-1} \mathscr{P}^{e_j}\mathfrak{a}_j.$$

Using Lemma 4 and Lemme 3 of [8] we get $s = q-2$ and $e_{q-1} = 0$. Thus finally we obtain (i) (a) because E_K is determined up to isomorphism by the ideal class of the ideal $\prod_{j=0}^{q-1} \mathfrak{a}_j = \mathfrak{a}$. Now, (b) is a consequence of (a), of Proposition 2.4 in [6] and of (2), and (c) results from Corollaire of [7].

Since $\boldsymbol{Z}[G]/\boldsymbol{Z}G^{\sim}$ is cyclic and has $\boldsymbol{Z}$-rank $pq-1$, we can write, by the same reasons as for E_K,

$$\boldsymbol{Z}[G]/\boldsymbol{Z}G^{\sim} \simeq (\bigoplus_{\substack{j=0 \\ j \neq 1}}^{q-1} \mathscr{P}^j, \boldsymbol{Z}[\theta]) \oplus \boldsymbol{Z}[\zeta]\mathfrak{a}',$$

where we may assume $(\mathfrak{a}'_j, pq) = 1$. Suppose that E_K and $\boldsymbol{Z}[G]/\boldsymbol{Z}G^{\sim}$ are in the same genus. In particular, for $l \in \{p, q\}$, $\boldsymbol{Z}_{(l)} \oplus E_K$ is $\boldsymbol{Z}_{(l)}[G]$-cyclic and if we assume (1), we have

$$\boldsymbol{Z}_{(l)} \otimes E_K \simeq (\bigoplus_{j=0}^{q-1} \tilde{\mathscr{P}}_l^{e_j}, \boldsymbol{Z}_{(l)}[\theta]),$$

where $\tilde{\mathscr{P}}_l = \boldsymbol{Z}_{(l)}[\zeta](1-\zeta)$. Since the above module is $\boldsymbol{Z}_{(l)}[G]$-cyclic, since $(\mathscr{P}^e, \boldsymbol{Z}[\theta])$ is non-trivial if and only if $(\tilde{\mathscr{P}}_l^e, \boldsymbol{Z}_{(l)}[\theta])$ is so for $l \in \{p, q\}$ (see (25.15) in [1]), and since all lemmas and propositions used in the proof of (i) (a) are also valid for $\boldsymbol{Z}_{(l)}[G]$-modules, we can proceed as above to obtain (i) (a). Owing to Proposition 2.3 and 2.4 of [6], this gives (b) and (c).

Now suppose that (b) and (c) hold. Then Proposition 2.3 of [6] and (c) give

$$E_K \simeq \Big(\bigoplus_{\substack{j=0\\ j\neq 1}}^{q-1} \mathcal{P}^j, \mathfrak{b}\Big) \oplus \mathcal{P}^e \mathfrak{a},$$

where $0 \leqslant e \leqslant q-1$ and $(\mathfrak{a}, pq) = 1$. Using Proposition 2.4 of [6] and (b) together with (2) one has $e = 0$. This proves (ii) because it suffices to localize at the primes dividing G to show that E_K and $Z[G]/ZG^{\sim}$ are in the same genus.

To prove (iii) we need only show that conditions (b), (c) and (d) are sufficient. The condition for p in (iii) shows that (a) and (b) imply

$$(8)\qquad E_K \simeq \Big(\bigoplus_{\substack{j=0\\ j\neq 1}}^{q-1} \mathcal{P}^j, \mathfrak{b}\Big) \oplus Z[\zeta].$$

According to the proof of Proposition 2.3 of [6], $N_{K/k}(E_K)$ and $p\mathfrak{b}$ are $Z[G]$-isomorphic, so conditions (c) and (d) imply that $\mathfrak{b}$ is $Z[G]$-cyclic, i.e., $\mathfrak{b} \simeq Z[\theta]$. Since there is exactly one, up to isomorphism, $Z[G]$-cyclic module of Z-rank $pq-1$, namely $Z[G]/ZG^{\sim}$, and this module is isomorphic to that in (8) with $\mathfrak{b}$ replaced by $Z[\theta]$, we conclude that E_K is $Z[G]$-cyclic. Thus we have shown Theorem 2.

Remark 1. Condition (i) (a) of Theorem 2 corrects a mistake in Lemme VI.5 of [5] and in Lemme 4.4 of [6]. The proofs of these lemmas base on the fact that every element of $Z[G]/ZG^{\sim}$ has a representative whose sum of its coefficients is zero, which is not true.

Remark 2. In (iii) of Theorem 2 condition (d) can be dropped if we assume that $q \leqslant 19$.

References

[1] C. W. Curtis and I. Reiner, *Methods of representation theory*, Wiley-Interscience, New York 1981.

[2] D. Duval, *Sur la structure galoisienne du groupe des unités d'un corps abélien réel de type* (p, p), J. Number Theory 13 (1981), 228–245.

[3] F. Halter-Koch and N. Moser, *Sur le nombre de classes de certaines extensions métacycliques sur Q ou sur un corps quadratique imaginaire*, J. Math. Japan 30 (1978), 237–248.

[4] Lena Chang Pu, *Integral representation of non abelian groups of order pq*, Michigan Math. J. 12 (1965), 231–246.

[5] N. Moser, *Constraintes galoisiennes sur le groupe des unités de certaines extensions de Q — applications arithmétiques*, Thése, Grenoble, 1978.

[6] — *Sur les unités d'une extension galoisienne non abélienne de degré pq du corps des rationnels, p et q nombres premiers impairs*, Ann. Inst. Fourier (Grenoble) 291 (1979), 137–158.

[7] — *Unités et nombre de classes d'une extension Galoisienne diédrale de Q*, Abh. Math. Sem. Univer. Hamburg 48 (1979), 54–75.

[8] N. Moser, *Théorème de densité de Tchebotareff et monogénéité de modules sur l'algèbre d'un groupe métacyclique*, Acta Arith. 42 (1983), 303–323.

INSTITUTE OF MATHEMATICS
WROCŁAW UNIVERSITY
Plac Grunwaldzki 2/4
50-384 Wrocław, Poland

Received on 4.3.1987
and in revised form on 22.6.1987 (1713)