Minkowski units in certain metacyclic fields

by

ROMAN MARZALEK (Wroclaw)

1. Let $K$ be a normal extension of the rationals with metacyclic Galois group of order $pm$, where $p$ is a prime and $mp - 1$. 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 (condition (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 $A$ we put:

$U_A = \text{the group of units in } A,$

$V_A = \text{the group of roots of unity in } A,$

$E_A = \text{the quotient group } U_A/V_A.$

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

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

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

$\langle \gamma \rangle = \text{the subgroup of } \Gamma \text{ generated by } \gamma \in \Gamma.$

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

Let $M_1, M_2$ be $Z[\Gamma]$-modules and let $f$ be a 1-cocycle from
where $0 \leq e_j \leq m-1$ and the $a_j$ are ideals of $A_1$, the class of the ideal $\prod_{j=0}^{m-1} a_j$ being uniquely determined by $E_K$. Since $\sigma$ acts trivially on $E_0$ one obtains

$$E_K \cong \left( \bigoplus_{j=0}^{m-1} \sigma^{e_j} a_j, b \right),$$

where $b$ is a $Z[\langle \sigma \rangle]$-module of $Z$-rank $m-1$.

If we put

$$a = (E_K; E_1, E_1, \ldots, E_{e_{m-1}}, E_0),$$

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

$$h_K p^{\langle e_m-1 \rangle / (m-1)} = a h_K n_r.$$  

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

$$h_K n_r = h_K n_r$$

with $t \geq m-1$.

**Proof.** Using the formula $\tau / \sigma = \sigma^{w(t)}$ and Corollaire to Proposition 13 of [7], we have

$$E_{w(t)} = E_K^{(w(t))} = (E_K)^{(w(t))}$$

and $E_k = (E_K)^{(w(t))}$

where $w(t) \equiv 1 \pmod{p}$, $0 \leq j \leq m-1$. Since $E_k \cong R = Z[G]/ZG^\times$, by Proposition 13 of [7], we get

$$(E_K; E_1, E_1, \ldots, E_{e_{m-1}}, E_0) = \left( R; \bigoplus_{j=0}^{m-1} R^{e_j} + R^{(w(t))} \right).$$

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

$$a = \left( R; \bigoplus_{j=0}^{m-1} R^{e_j} + R^{(w(t))} \right).$$

Using Proposition 14 of [7] we obtain

$$a = (R; R_1),$$

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

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

$$Z[G]/T \cong R / R_1,$$
where $T = \langle \sigma \rangle Z[G] + \sum_{j=0}^{m-1} \langle \sigma^j \tau \rangle Z[G]$. 

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

$$H^{-1}Z[G] = H^{-1} \bigcup_{i=1}^{N} Zg_i.$$ 

**Proof.** Since for every $y \in Z[G]$

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

one obtains

$$H^{-1}y = \sum_{h \in H} \sum_{i=1}^{N} a_{ih} x h g_i = \sum_{h \in H} \sum_{i=1}^{N} a_{ih^{-1}} x h g_i,$$

by substituting $w = x h$. Finally,

$$H^{-1}y = \sum_{i=1}^{N} w \sum_{i=1}^{N} \left( \sum_{s \in H} a_{i}^{-1} w h g_i \right) g_i.$$

This lemma gives

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

Now we shall use the formula

$$a = (Z[G]:T)$$

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

$$x = \sum_{i=0}^{p-1} \sum_{j=0}^{m-1} \lambda_{ij} \tau^i \sigma^j \in Z[G]$$
is an element of $T$, then there exist rational integers $\lambda_{ij}$ and $\omega_j$ such that

$$x = \sum_{i=0}^{p-1} \sum_{j=0}^{m-1} \lambda_{ij} \tau^i \sigma^j + \sum_{h=0}^{m-1} \sum_{s=0}^{m-1} a_{hs} \sigma^s \tau^h.$$

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

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

where $\sigma_0 = 0$, $\tau_j = 1 + \tau^2 + \ldots + \tau^{p^j}$ with $1 \leq j \leq m-1$. Thus

$$x = \sum_{i=0}^{p-1} \sum_{j=0}^{m-1} \lambda_{ij} \tau^i \sigma^j + \sum_{h=0}^{m-1} \sum_{s=0}^{m-1} a_{hs} \sigma^s \tau^h.$$

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

$$\lambda_{ij} = \omega_j + \sum_{s=0}^{m-1} a_{s \tau_j + h},$$

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

Let $\mu_{ij} = \lambda_{ij} - \lambda_{0j}$ and let, for $1 \leq d \leq m-2$ and $d+1 \leq j \leq m-1$, $x_{i,j}^d$ be integer solutions of the following system of linear congruences:

$$\sum_{h=1}^{d} x_{i,j}^d \varphi_i \psi_i^{d-w} \equiv 0 \pmod{p},$$

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

Now we shall show that

$$F_{i,j}^0 = \sum_{i=0}^{p-1} \mu_{ij} = 0 \pmod{p}$$

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

$$F_{i,j}^0 = \sum_{i=0}^{p-1} \mu_{ij} + \sum_{h=1}^{d} x_{i,j}^d \mu_{ih} = 0 \pmod{p}$$

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

$$F_{i,j}^0 = [\omega_d - \omega_0 + \sum_{h=1}^{d} x_{i,j}^d (\omega_d - \omega_0)] + \sum_{h=0}^{p-1} \sum_{s=0}^{m-1} a_{hs} \sum_{i=0}^{p-1} \sum_{j=0}^{d-1} x_{i,j}^d \sum_{s=0}^{m-1} a_{hs}.$$

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

$$F_{i,j}^0 = \sum_{i=0}^{p-1} \sum_{h=0}^{m-1} \sum_{s=0}^{m-1} x_{i,h}^d [\varphi_d \psi_i^{d-w} + \sum_{h=1}^{d} x_{i,h}^d \varphi_i^{d-w}] a_{hs} \equiv 0 \pmod{p}$$

by (5).
Thus the coordinates of $x$ are zeros of the linear forms $F^{(i)}$ which turn out to be linearly independent mod $p$. To prove this suppose that there are integers $a^{(i)}_j$ such that

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

is a linear form with coefficients vanishing mod $p$.

Though $a^{(i)}_j$ are defined only for $d+1 \leq j \leq m-1$ we extend their range by putting $a^{(i)}_j = 0$ for $1 \leq j \leq d$. We also put $a^{(i)}_j = 0$ for $d+1 \leq h \leq m-1$. Using (6) and (7), we get

$$ F = \sum_{j=1}^{m-1} a^{(0)}_j \mu_j + \sum_{d=1}^{m-2} \sum_{j=d+1}^{m-1} \sum_{i=0}^{p-1} j^{(d)} a^{(i)}_j \mu_j + \sum_{d=1}^{m-2} \sum_{j=d+1}^{m-1} \sum_{i=0}^{p-1} j^{(d)} a^{(d)}_j \mu_{j+d+1} $$

by substituting in the last but one line $\mu_j$ for $\alpha$ in the second term. Since the coefficients of $F$ are all equal to $0$ (mod $p$) it follows that for $d+1 \leq j \leq m-1$

$$ a^{(i)}_j \mu_j + \sum_{d=1}^{m-2} \sum_{j=d+1}^{m-1} \sum_{i=0}^{p-1} j^{(d)} a^{(i)}_j \mu_{j+d+1} \equiv 0 \pmod{p}.$$

But by definition $a^{(i)}_j = 0$ for $d+1 \leq j \leq m-1$, so

$$ \sum_{d=1}^{m-2} \sum_{j=d+1}^{m-1} \sum_{i=0}^{p-1} j^{(d)} a^{(i)}_j \mu_{j+d+1} \equiv 0 \pmod{p},$$

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

$$ a^{(i)}_j \equiv 0 \pmod{p},$$

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

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

$$ a = p^w,$$

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

4. Now we shall prove three lemmas.

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

$$ f, f^* \in Z_1(G, Hom_Z(M_1, N)), \quad f_0 \in Z_1(G, Hom_Z(M_0, N)).$$

If $Hom_{gr}(N, M_1) = 0$ and the extensions $(M_1, N, f), (M_1, N, f^*)$ are $Z[G]$-isomorphic, then there exists a $Z[G]$-isomorphism

$$ (M_0 \oplus M_1 \oplus M_1, N; f_0, f, f^*) \cong (M_0 \oplus M_1, N, f_0, f, f^*),$$

where $\varphi$ is a suitable automorphism of $N$.

**Proof.** Since $Hom_{gr}(N, M_1) = 0$, we can use Corollary (34.5) of [1]. Thus there exist $\lambda \in Aut(M_1), \nu \in Aut(N)$ and $c \in Hom_Z(N, M_1)$ such that

$$ \lambda f_0'(m) = f_0'(vm) + gc(m) - c(gm), \quad g \in G,$$

and thus we can define a $Z[G]$-isomorphism

$$ \Psi : (M_0 \oplus M_1 \oplus M_1, N, f_0, f, f^*) \to (M_0 \oplus M_1, N, f_0, f, f^*)$$

by putting

$$ (m_0, m_1, m_2) \mapsto (m_0, 2m_1 - \lambda m_1 - c(n), m_2 - \lambda m_1 - c(n)).$$

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

**Lemma 3.** If $\gamma$ is a $Z[G]$-generator for the $Z[G]$-module $Z[G]$ then

$$ An(\gamma) = Z[G] \langle 1 - s \rangle + Z[G] \langle \langle \gamma \rangle^+ \rangle,$$

where $An(\gamma)$ denotes the annihilator ideal of $\gamma$.

**Proof.** If $a, b$ are $Z[G]$-generators of $Z[G]$, then they are units in the ring $Z[G]$, so there is a $Z[G]$-isomorphism $\phi$ of $Z[G]$ such that $\phi(a) = b$. Since $An(\phi(a)) = An(b)$ we may assume $\gamma = 1$. Let

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

be an element of $An(1)$. Then

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

so

$$ \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{ij} = x = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{ij} \sigma^j \tau^j \in Z[G] \langle \langle \gamma \rangle^+ \rangle + Z[G] \langle 1 - s \rangle.$$

Since the opposite inclusion is obvious, Lemma 3 is proved.
LEMMA 4. If \( e \geq 1 \) and \( a \) is an ideal of \( A_1 \), then the \( \mathbb{Z}[G] \)-module \( \mathbb{Z}[\theta] \oplus \mathfrak{P}^e a \) is not cyclic.

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

If we put \( \delta = \sum_{j=0}^{s-1} A_j (1 - \zeta^e u) \), then \( \delta \in A_1 \), and \( \delta \in \mathfrak{P}^e a \) since \( e \geq 1 \). It follows that \( \delta \in \mathfrak{P}^e a \); but \( \mathfrak{P}^e a \) totally ramifies in \( Q(\zeta) \) and so \( \delta \in \mathfrak{P}^e a \). Now applying the identity

\[
\mathbb{Z}[G] x = \sum_{j=0}^{s-1} A_j \psi^j(x),
\]

\( x \in \mathfrak{P}^e a \), we obtain

\[
\mathbb{Z}[G](1 - \zeta^e u) = \mathbb{Z}[\theta] \cdot \delta = A \delta \subset \mathfrak{P}^e a \subset \mathfrak{P}^{e+1} a
\]

and

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

because \( 1 \leq e \leq q - 1 \). By Lemma 3

\[
\text{An}(\gamma)(1 - \zeta^e u) \subset \mathfrak{P}^{e+1} a.
\]

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

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

Now we are able to prove

THEOREM 2. Let \( K \) be a real metacyclic extension of degree \( pq \) over \( \mathbb{Q} \), where \( p, q \) are odd primes for which \( q | p - 1 \), \( q^2 \not| p - 1 \). Then:

(i) If \( K \) has a Minkowski unit, then there exists an ideal \( a \subset A_1 \) and

\[
\mathcal{E}_K \simeq \left( \bigoplus_{j=0}^{q-1} \mathfrak{P}^j, \mathbb{Z}[\theta] \right) \oplus \mathbb{Z}[\zeta] a,
\]

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

(b) \( h_k h_{\mathfrak{P}}^j = p^{t-1} \),

(c) \( N_{K/A}(\mathcal{E}_K) = \mathcal{E}_K \),

(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 \( \mathbb{Z}[\theta]/\mathbb{Z}[\theta] \).

(iii) If the class number of the field \( Q(\zeta^e) \) is \( 1 \), then (b), (c) and (d) are necessary and sufficient for \( K \) to have a Minkowski unit.

Proof. According to (1)

\[
\mathcal{E}_K \simeq \left( \bigoplus_{j=0}^{q-1} \mathfrak{P}^j a_j, \mathbb{Z}[\theta] \right) \oplus \bigoplus_{j=s+1}^{q-1} \mathfrak{P}^j a_j,
\]

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

\[
\mathcal{E}_K \simeq \left( \bigoplus_{j=0}^{q-1} \mathfrak{P}^j a_j, \mathbb{Z}[\theta] \right) \oplus \bigoplus_{j=s+1}^{q-1} \mathfrak{P}^j a_j.
\]

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

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

\[
\mathbb{Z}[G]/\mathbb{Z}^\gamma \simeq \left( \bigoplus_{j=0}^{q-1} \mathfrak{P}^j, \mathbb{Z}[\theta] \right) \oplus \mathbb{Z}[\zeta] a',
\]

where we may assume \( (a_j, pq) = 1 \). Suppose that \( E_K \) and \( \mathbb{Z}[G]/\mathbb{Z}^\gamma \) are in the same genus. In particular, for \( l \in \{ p, q \} \), \( \mathbb{Z}_l \otimes E_K \) is \( \mathbb{Z}_l[G] \)-cyclic and if we assume (i), we have

\[
\mathbb{Z}_l \otimes E_K \simeq \left( \bigoplus_{j=0}^{q-1} \mathfrak{P}^j, \mathbb{Z}_l[\theta] \right),
\]

where \( \mathfrak{p}_j = \mathbb{Z}_l[\zeta](1 - \zeta) \). Since the above module is \( \mathbb{Z}_l[G] \)-cyclic, since \( (\mathfrak{P}^j, \mathbb{Z}[\theta]) \) is non-trivial if and only if \( (\mathfrak{P}^j, \mathbb{Z}[\theta]) \) is so for \( l \in \{ p, q \} \) (see 21.5) in [1]), and since all lemmas and propositions used in the proof of (i) (a) are also valid for \( \mathbb{Z}_l[G] \)-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

$$E_k \cong \bigoplus_{j=0}^{q-1} b_j \oplus \mathbb{Z}^{q-1},$$

where $0 \leq e \leq q-1$ and $(e, pq) = 1$. 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 $Z[G]/ZG^*$ 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

$$E_k \cong \bigoplus_{j=0}^{q-1} b_j \oplus \mathbb{Z}^{q-1}.$$

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

Remark 1. Condition (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 $Z[G]/ZG^*$ 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 $q \leq 19$.

References