ACTA ARITHMETICA
LXI.4 (1992)

The Galois module of a twisted element in the p^m-th cyclotomic field

by

KURT GIRSTMAIR (Innsbruck)

1. Introduction and results. For a natural number n let $\xi_n \in \mathbb{C}$ denote the primitive nth root of unity: $\xi_n = e^{2\pi i/n}$. Then $\mathbb{Q}_n = \mathbb{Q}[\xi_n]$ is the nth cyclotomic field and $G_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ is its Galois group over $\mathbb{Q}$. The field $\mathbb{Q}_n$ is a module over the group ring $\mathbb{Q}[G_n]$ of G_n, and, by the normal basis theorem, it is isomorphic to $\mathbb{Q}[G_n]$ itself. In what follows let $n = p^m$, where p is a prime number and m a nonnegative integer. Let $q = p^e$, $e \geq 1$, be another power of p. For $x \in \mathbb{Q}_n$ we consider

$$x_{nq} = \xi_{nq} x \in \mathbb{Q}_{nq} .$$

We call x_{nq} the *twisted element* of x, because it arises from x by means of the rotation of the plane $\mathbb{C}$ through $2\pi/(nq)$. It is almost obvious that the Galois module $\mathbb{Q}[G_{nq}]x_{nq}$ is contained in $\mathbb{Q}[G_{nq}]\xi_{nq}$ (cf. proof of Theorem 1 below). Suppose that d is the number of divisors of $p-1$. Then $\mathbb{Q}[G_{nq}]\xi_{nq}$ is the direct sum of d simple $\mathbb{Q}[G_{nq}]$-submodules if $p \geq 3$, and it is the direct sum of two simple submodules for $p = 2$ and $nq \geq 4$. Hence $\mathbb{Q}[G_{nq}]\xi_{nq}$ has 2^d different submodules for $p \geq 3$, and four different submodules for $p = 2$, $nq \geq 4$. We consider the case $q \neq 2$ first. Here $\mathbb{Q}[G_{nq}]x_{nq}$ is always one of the two *trivial* submodules of $\mathbb{Q}[G_{nq}]\xi_{nq}$; indeed, we show

THEOREM 1. *Let p be a prime, $n = p^m$, $q = p^e$, $m \geq 0$, $e \geq 1$. In addition, if $p = 2$, let $e \geq 2$. For each element $x \in \mathbb{Q}_n$, $x \neq 0$,*

$$\mathbb{Q}[G_{nq}]x_{nq} = \mathbb{Q}[G_{nq}]\xi_{nq} .$$

For $q = 2$ the result is different: Let M_1, M_2 be the simple submodules of $\mathbb{Q}[G_{2n}]\xi_{2n}$, $n = 2^m \geq 4$. For $k = 1, 2$, let

$$V_k = \{x \in \mathbb{Q}_n \,;\, \mathbb{Q}[G_{2n}]x_{2n} = M_k\} \cup \{0\} .$$

THEOREM 2. *With the above notations, V_k is a $\mathbb{Q}$-subspace of $\mathbb{Q}_n$ of dimension* $\dim V_k = n/4$, $k = 1, 2$. *Moreover,*

$$\mathbb{Q}_n = V_1 \oplus V_2 .$$

2. Proofs. We adopt the above notations. Most of the representation theory of $\mathbb{Q}[G_n]$ we use in the sequel can be found in [1], Section 1, and in [4].

Consider the map

$$\mathbb{Z} \setminus p\mathbb{Z} \to G_n, \quad k \mapsto \sigma_k ,$$

where $\sigma_k(\xi_n) = \xi_n^k$. This map is surjective and multiplicative. It is used in order to identify the character group

$$X_n = \{\chi : G_n \to \mathbb{C}^\times ; \chi \text{ a group homomorphism}\}$$

of G_n with the group of Dirichlet characters modulo n. Indeed, put

$$\chi(k) = \begin{cases} \chi(\sigma_k) & \text{if } p \nmid k, \\ 0 & \text{otherwise.} \end{cases}$$

For an element $\alpha = \sum\{a_\sigma \sigma ; \sigma \in G_n\}$ in $\mathbb{Q}[G_n]$ let $\chi(\alpha) = \sum a_\sigma \chi(\sigma) \in \mathbb{C}$. Let $Y \subseteq X_n$ be a *conjugacy class* of characters, i.e., all characters χ, χ' in Y generate the same group $\langle\chi\rangle = \langle\chi'\rangle$. Then the group ring $\mathbb{Q}[G_n]$ splits into the simple submodules

$$\mathbb{Q}[G_n]_Y = \{\alpha \in \mathbb{Q}[G_n] ; \chi(\alpha) \neq 0 \text{ only if } \chi \in Y\} ,$$

of $\mathbb{Q}$-dimension $\dim \mathbb{Q}[G_n]_Y = |Y|$.

Next fix $\chi \in X_n$. According to [3], [1] there is a map $y(\chi|-) : \mathbb{Q}_n \to \mathbb{C}$ with the following properties:

(i) $y(\chi|-)$ is χ-*linear*, i.e., for all $\alpha \in \mathbb{Q}[G_n]$ and all $x \in \mathbb{Q}_n$, $y(\chi|\alpha x) = \chi(\alpha) y(\chi|x)$.

(ii) Let Y be the conjugacy class of χ. Then

$$\mathbb{Q}_{n,Y} = \{x \in \mathbb{Q}_n ; y(\chi'|x) \neq 0 \text{ only if } \chi' \in Y\}$$

is the uniquely determined $\mathbb{Q}[G_n]$-submodule of $\mathbb{Q}_n$ that is isomorphic to $\mathbb{Q}[G_n]_Y$.

The map $y(\chi|-)$ is uniquely determined by χ up to factors in $\mathbb{C}^\times$; this means that the maps $c \cdot y(\chi|-)$, $c \in \mathbb{C}^\times$, are the only ones having properties (i), (ii), too.

Consider the numbers $y(\chi|\xi_n) \in \mathbb{C}$, $\chi \in X_n$. Then $y(\chi|\xi_n) \neq 0$ iff χ is a primitive character modulo n (cf. [4]). Hence

$$\mathbb{Q}[G_n]\xi_n = \bigoplus \mathbb{Q}_{n,Y} ,$$

where Y runs through the conjugacy classes of primitive characters modulo n. We obtain

Lemma 1. *Let n be as above, and let $x \in \mathbb{Q}_n$. Then*

(1) $\mathbb{Q}[G_n]x \subseteq \mathbb{Q}[G_n]\xi_n$ *iff* $y(\chi|x) = 0$ *for all imprimitive characters* $\chi \bmod n$;

(2) $\mathbb{Q}[G_n]x = \mathbb{Q}[G_n]\xi_n$ *iff* $\{\chi\in X_n\,;\, y(\chi|x) \neq 0\} = \{\chi\in X_n\,;\, \chi$ *primitive*$\}$.

For the proof of Theorem 1 we need two additional lemmas.

LEMMA 2. *Let p be a prime, $n = p^m$, $q = p^e$, $m \geq 0$, $e \geq 1$. For $p = 2$ let $e \geq 2$.*

(1) *For each $k \in \{1, \ldots, n\}$ there is a uniquely determined number $j \in \{1, \ldots, n\}$ such that $1 + qk \equiv (1 + q)^j \bmod nq$.*

(2) *The map $\{1, \ldots, n\} \to \{1, \ldots, n\} : k \mapsto j$ is bijective.*

(3) *Let k, $k' \in \{1, \ldots, n\}$ and let j, j' be their images under the above map. Let $0 \leq l \leq m$. Then $k \equiv k' \bmod p^l$ iff $j \equiv j' \bmod p^l$. Furthermore, $k \equiv 0 \bmod p^l$ iff $j \equiv 0 \bmod p^l$.*

The proof of Lemma 2 consists, essentially, in the observation that the subgroups $\{\overline{1 + qk}\,;\, k = 1, \ldots, n\}$ and $\langle\,\overline{1 + q}\,\rangle$ of $(\mathbb{Z}/nq\mathbb{Z})^\times$ coincide and have order n (cf. [2], p. 72 ff.). Note, however, that the map $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : \overline{k} \mapsto \overline{j}$ is *not* a group homomorphism in general.

LEMMA 3. *Let p be a prime, $m \geq 2$, and $n = p^m$. Let $\beta = \sum\{b_j\sigma_j\,;\, j \in \{1, \ldots, n\}, p\nmid j\} \in \mathbb{Q}[G_n]$ be such that $\beta\xi_n = 0$. Then $b_j = b_{j'}$ for all j, j' with $j \equiv j' \bmod n/p$.*

Proof. Put $M = \{\alpha \in \mathbb{Q}[G_n]\,;\, \alpha\xi_n = 0\}$. According to Lemma 1, the element $\beta = \sum b_j\sigma_j$ is in M iff $\chi(\beta) = 0$ for each primitive character $\chi \bmod n$. From this we conclude that

$$\dim M = |\{\chi \in X_n\,;\, \chi \text{ is imprimitive}\}| = \varphi(n/p)\,,$$

where φ is Euler's function. Observe now that $Z^p - \xi_n^p = Z^p - \xi_{n/p}$ is the minimal polynomial of ξ_n over $\mathbb{Q}_{n/p}$. This means that the trace

$$T(\xi_n^j) = \sum\{\sigma_{j'}\xi_n\,;\, j' \equiv j \bmod n/p\}$$

vanishes for each j, $j \in \{1, \ldots, n\}$, $p\nmid j$. Hence the elements

$$\alpha_j = \sum\{\sigma_{j'}\,;\, j' \in \{1, \ldots, n\},\ j' \equiv j \bmod n/p\}\,,$$

$j \in \{1, \ldots, n/p\}$, $p\nmid j$, are in M. It is obvious that the α_j are $\mathbb{Q}$-linearly independent. So, for dimensional reasons, they form a $\mathbb{Q}$-basis of M. When the element $\beta \in M$ is expressed in terms of this basis, the assertion follows. ∎

Proof of Theorem 1. Let n, q be as in Theorem 1. Let

$$x = \sum_{k=1}^{n} a_k\xi_n^k \in \mathbb{Q}_n\,.$$

Then $x_{nq} = \sum\{a_k\xi_{nq}^{1+qk}\,;\, k = 1, \ldots, n\}$ is a linear combination of primitive nqth roots of unity. Therefore $x_{nq} \in \mathbb{Q}[G_{nq}]\xi_{nq}$ and $\mathbb{Q}[G_{nq}]x_{nq} \subseteq \mathbb{Q}[G_{nq}]\xi_{nq}$.

Next suppose that χ is primitive mod nq. Since $y(\chi|-)$ is determined up to factors in $\mathbb{C}^\times$ only, we may assume that $y(\chi|\xi_{nq}) = 1$. Suppose that $y(\chi|x_{nq}) = 0$. We show that $x = 0$, which proves the theorem, by Lemma 1. We use induction with respect to the exponent m. Let $m = 0$, i.e., $n = 1$ and $x \in \mathbb{Q}$. Then $0 = y(\chi|x_q) = y(\chi|x\xi_q) = x \cdot y(\chi|x\xi_q) = x$.

Now let $m > 0$, which means $p \mid n$, and let $n' = n/p$. The induction hypothesis is as follows: Let $q' = p^{e'}$, $e' \geq 1$ ($e' \geq 2$ for $p = 2$), $x' \in \mathbb{Q}_{n'}$, and χ' a primitive character mod $n'q'$; if $y(\chi'|x'_{n'q'}) = 0$ then $x' = 0$.

Take x as above. Then

$$y(\chi|x_{nq}) = \sum_{k=1}^{n} a_k \chi(1 + qk) = 0\,.$$

For each $j \in \{1, \ldots, n\}$ we put $b_j = a_k$, where k is the uniquely determined number in $\{1, \ldots, n\}$ with $(1 + q)^j \equiv 1 + qk \bmod nq$ (Lemma 2). Observe that $\eta = \chi(1 + q)$ is a primitive nth root of unity (use [2], p. 212, and Lemma 2). Now

$$y(\chi|x_{nq}) = \sum_{j=1}^{n} b_j \eta^j = 0\,.$$

Consider the case $n = p$ first. Because $1 + Z + \ldots + Z^{n-1}$ is the minimal polynomial of η over $\mathbb{Q}$, all the coefficients b_j are equal. Therefore $a_1 = \ldots = a_n$ and $x = 0$. Suppose now that $n = p^m$, $m \geq 2$. Put

$$x' = \sum \{a_k \xi_n^k\,;\, k \in \{1, \ldots, n\},\ p \mid k\}$$

and $x'' = x - x'$. The "trace argument" in the proof of Lemma 3 shows that $T(\eta^j) = 0$, for all $j \in \{1, \ldots, n\}$, $p \nmid j$ (T is the trace of $\mathbb{Q}_n$ over $\mathbb{Q}_{n'}$). Therefore $y(\chi|x''_{nq}) = 0$, which implies that $y(\chi|x'_{nq}) = y(\chi|x_{nq}) - y(\chi|x''_{nq}) = 0$. However, x'_{nq} is the same as $x'_{n'q'}$, with $n' = n/p$, $q' = qp$. The induction hypothesis yields $x' = 0$. Let

$$\beta = \sum \{b_j \sigma_j\,;\, j \in \{1, \ldots, n\},\ p \nmid j\} \in \mathbb{Q}[G_n]\,.$$

Then $\beta\eta = y(\chi|x''_{nq}) = 0$. By Lemma 3, the coefficients of β fulfill: $b_j = b_{j'}$ for all $j, j' \in \{1, \ldots, n\}$, $p \nmid j, j'$, $j \equiv j' \bmod n'$. Then $a_k = a_{k'}$ for all $k, k' \in \{1, \ldots, n\}$, $p \nmid k, k'$, $k \equiv k' \bmod n'$. We obtain

$$x'' = \sum_{\substack{k=1 \\ p \nmid k}}^{n'} a_k \sum_{\substack{k'=1 \\ k' \equiv k \bmod n'}}^{n} \xi_n^{k'} = \sum_{\substack{k=1 \\ p \nmid k}}^{n'} a_k T(\xi_n^k)\,.$$

But the traces in the last sum vanish, whence $x'' = 0$ and $x = x' + x'' = 0$ follows. ∎

Proof of Theorem 2. Let $n = 2^m$, $m \geq 2$. There are exactly two conjugacy classes of primitive characters mod $2n$, viz. the set of even and the set of odd primitive characters (cf. [2], p. 212). Choose an arbitrary odd character χ_1 and an arbitrary even character χ_2, both of them primitive. Then

$$M_1 = \{z \in \mathbb{Q}[G_{2n}]\xi_{2n} \; ; \; y(\chi_1|z) = 0\} = \mathbb{Q}[G_{2n}](\xi_{2n} + \xi_{2n}^{-1}),$$
$$M_2 = \{z \in \mathbb{Q}[G_{2n}]\xi_{2n} \; ; \; y(\chi_2|z) = 0\} = \mathbb{Q}[G_{2n}](\xi_{2n} - \xi_{2n}^{-1}),$$

are the simple submodules of $\mathbb{Q}[G_{2n}]\xi_{2n}$. For each $\sigma \in G_{2n}$, $\chi_k(\sigma)$ is an $(n/2)$th root of unity, $k = 1, 2$, which shows that the $\mathbb{Q}$-linear map

$$g_k : \mathbb{Q}_n \to \mathbb{Q}_{n/2}, \qquad x \mapsto g_k(x) = y(\chi_k|\xi_{2n}x),$$

is well defined. Let V_k denote the kernel of g_k, $k = 1, 2$. Then

$$V_k = \{x \in \mathbb{Q}_n \; ; \; \xi_{2n}x \in M_k\} = \{x \in \mathbb{Q}_n \; ; \; \mathbb{Q}[G_{2n}]x_{2n} = M_k\} \cup \{0\},$$

since M_k is simple. Moreover,

$$\dim V_k = \varphi(n) - \dim g_k(\mathbb{Q}_n) \ge \varphi(n) - \varphi(n/2) = n/4, \qquad k = 1, 2.$$

But $V_1 \cap V_2 = \{0\}$, so $\dim(V_1 \oplus V_2) \ge n/2 = \dim \mathbb{Q}_n$. Thus $V_1 \oplus V_2 = \mathbb{Q}_n$ and $\dim V_k = n/4$, $k = 1, 2$. ■

EXAMPLE. Let $n = 2^m$ and $m \ge 2$ be as above. Consider the elements

$$x^+ = 1 + \xi_n^{-1}, \qquad x^- = 1 - \xi_n^{-1}$$

in $\mathbb{Q}_n$. Then $\xi_{2n}x^+ = \xi_{2n} + \xi_{2n}^{-1}$, $\mathbb{Q}[G_{2n}]x_{2n}^+ = M_1$, $\xi_{2n}x^- = \xi_{2n} - \xi_{2n}^{-1}$, $\mathbb{Q}[G_{2n}]x_{2n}^- = M_2$. Furthermore, $\mathbb{Q}[G_n]x^+ = \mathbb{Q}[G_n]x^- = \mathbb{Q} \oplus \mathbb{Q}[G_n]\xi_n$. Hence V_1 and V_2 cannot be $\mathbb{Q}[G_n]$-modules. Indeed, if they were, $\mathbb{Q} \oplus \mathbb{Q}[G_n]\xi_n \subseteq V_1 \cap V_2$ would follow, which is impossible.

Remark. Clearly the results of this note do not depend on the particular choice $\xi_n = e^{2\pi i/n}$ of a primitive nth root of unity. This choice was just made for reasons of convenience, e.g., for the sake of the simple relation $\xi_{nq}^q = \xi_n$.

References

[1] K. Girstmair, *Character coordinates and annihilators of cyclotomic numbers*, Manuscripta Math. 59 (1987), 375–389.

[2] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer, Berlin 1950.

[3] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. 201 (1959), 119–149.

[4] G. Lettl, *The ring of integers of an abelian number field*, ibid. 404 (1990), 162–170.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT INNSBRUCK
TECHNIKERSTR. 25/7
A-6020 INNSBRUCK, ÖSTERREICH

Received on 8.10.1991 (2181)