Bull. Fac. Educ. Mie Univ. **55** (*Natur. Sci*): 45 – 54, 2004

Decomposition of $F^{\times}/F^{\times n}$ as a Galois Module

Naoya Sakaguchi and Harutaka Koseki

Department of Mathematics, Mie University, Tsu 514-8507, Japan

Abstract: A direct sum decomposition of the Galois module $F^{\times}/F^{\times n}$ is given for an arbitrary finite Galois extension F/F_0, $[F_0 : \mathbf{Q}] < \infty$, where each summand is indecomposable and of finite length. In the case where F/F_0 is a cyclic p-extension the summands of $F^{\times}/F^{\times p}$ are determined explcitly.

1. Preliminaries on FL-decompositions

In this paper we call a decomposition $M = \bigoplus_{i \in I} M_i$ of a left module M over a ring R as an FL-decomposition, if each summand M_i is indecomposable and of finite length. Here indecomposable module means a nonzero module which has no nontrivial direct summand. Any nonzero module of finite length has an FL-decomposition with finitely many summands. If a module M with an FL-decomposition $M = \bigoplus_{i \in I} A_i$ has another decomposition $M = \bigoplus_{j \in J} B_j$ into indecomposables, Krull-Remak-Schmidt Theorem assures that there exists a bijection $\varphi : I \to J$ such that $A_i \simeq B_{\varphi(i)}$ for all $i \in I$, *cf.* [4, Ch. 7].

For modules with FL-decompositions $M = \bigoplus_{i \in I} M_i$, $N = \bigoplus_{j \in J} N_j$, we say that M and N are almost same if there exists a bijection $\varphi : I - I_0 \to J - J_0$ outside some finite sets $I_0 \subset I$ and $J_0 \subset J$ such that $M_i \simeq N_{\varphi(i)}$ for all $i \in I - I_0$. We compare the FL-decomposability of modules M and N and discuss their almost sameness in the following cases:

Case A: M is a submodule of N where $Q := N/M$ is of finite length,

Case B: $N = M/L$ where L is a submodule of M of finite length.

Proposition 1.1. *In Case A, suppose that R is left Noetherian and M is FL-decomposable. Then N is FL-decomposable, and M and N are almost same.*

Proof. We may write $N = K + M$ with K a finitely generated submodule of N. Let $M = \bigoplus_{i \in I} M_i$ be an FL-decomposition of M. Since R is left Noeterian $K \cap M$ is finitely generated, hence included in $\bigoplus_{i \in I_0} M_i$ for a finite $I_0 \subset I$. Both $K \cap M$ and $K/K \cap M$, included in modules of finite length, are of finite length. Hence K is of finite length. Now we have

$$N = \left(K + \bigoplus_{i \in I_0} M_i \right) + \left(\bigoplus_{i \in I - I_0} M_i \right) = \left(K + \bigoplus_{i \in I_0} M_i \right) \oplus \left(\bigoplus_{i \in I - I_0} M_i \right)$$

where $K + \bigoplus_{i \in I_0} M_i$ is of finite length, hence a finite direct sum of indecomposable modules of finite length. $\square$

Proposition 1.2. *In Case B, suppose that M is FL-decomposable. Then N is FL-decomposable, and M and N are almost same.*

Proof. Let $M = \bigoplus_{i \in I} M_i$ be an FL-decomposition of M. We have $L \subset \bigoplus_{i \in I_0} M_i$ with a finite $I_0 \subset I$, which implies

$$N = M/L = \left(\left(\bigoplus_{i \in I_0} M_i \right) \Big/ L \right) \oplus \left(\bigoplus_{i \in I - I_0} M_i \right)$$

where $(\bigoplus_{i \in I_0} M_i)/L$ is of finite length. □

One can cinsider the reversed versions of the above propositions, in which one assumes the FL-decomposability of N instead of M. However Brune [2] shows that if R is an Artin algebra of infinite representation type, there exist an R-module N and its maximal submodule M such that N is FL-decomposable but M is not. An example of such R is the group algebra $R = \mathbf{F}_p[G]$ of a finite group G with non-cyclic Sylow p-subgroups, cf. [3, Sect. 64]. Hence the reversed version of Proposition 1.1 does not hold, and one can easily see from this that the reversed version of Proposition 1.2 also fails. But for our later purpose we discuss the reversed versions under some finiteness conditions on the FL-decomposition of N.

Let $N = \bigoplus_{j \in J} N_j$ be an FL-decomposition of N. In Case A, let $\pi : N \to Q$ be the projection and let $\pi_j : N_j \to Q$ be the restriction of π to N_j. We say that the family of morphisms π_j, $j \in J$, is reducible to a subfamily π_k, $k \in J_0 \subset J$, if for each $j \in J$ there exist $k \in J_0$ and $h \in \mathrm{Hom}_R(N_j, N_k)$ with $\pi_j = \pi_k h$. In Case B, let $\pi : M \to N$ be the projection and let $X_j := \pi^{-1}(N_j)$. It is an extension of N_j by L. We say that the family of extensions X_j, $j \in J$, is reducible to a subfamily X_k, $k \in J_0 \subset J$, if for each $j \in J$ there exist $k \in J_0$ and $\tilde{h} \in \mathrm{Hom}_R(X_j, X_k)$ such that the restriction of $\tilde{h}$ to L is the identity. We consider the following conditions on the FL-decomposition of N:

C_1: The family π_j, $j \in J$, is reducible to a finite subfamily,

C_2: The family X_j, $j \in J$, is reducible to a finite subfamily.

Proposition 1.3. *In Case A, suppose that R is left Noetherian and N has an FL-decomposition $N = \bigoplus_{j \in J} N_j$ satisfying C_1. Then M is FL-decomposable, and M and N are almost same.*

Proof. By C_1 the family π_j, $j \in J$, is reducible to a finite subfamily π_k, $k \in J_0$. For each $j \in J$ we choose $k(j) \in J_0$ and $h_j \in \mathrm{Hom}_R(N_j, N_{k(j)})$ satisfying $\pi_j = \pi_{k(j)} h_j$. For $j \in J_0$ we put $k(j) = j$ and take the identity of N_j as h_j. Define an endomorphism e of N by

$$e(\Sigma_{j \in J} n_j) = \Sigma_{j \in J} h_j(n_j) \qquad (n_j \in N_j).$$

This is an idempotent of $\mathrm{End}_R(N)$, hence $N = \mathrm{im}(e) \oplus \ker(e)$. Hence $\ker(e)$, being isomorphic to $\bigoplus_{j \in J - J_0} N_j$, is FL-decomposable, and N and $\ker(e)$ are almost same. On the other hand we have $\pi = \pi e$, hence $\ker(e) \subset \ker(\pi) = M$, and $M/\ker(e) \subset N/\ker(e)$ is of finite length. Hence by Proposition 1.1 M is FL-decomposable, and $\ker(e)$ and M are almost same. □

Proposition 1.4. *In Case B, suppose that N has an FL-decomposition* $N = \bigoplus_{j \in J} N_j$ *satisfying* C_2. *Then M is FL-decomposable, and M and N are almost same.*

Proof. By C_2 the family X_j, $j \in J$, is reducible to a finite subfamily X_k, $k \in J_0$. For each $j \in J$ we choose $k(j) \in J_0$ and $\tilde{h}_j \in \mathrm{Hom}_R(X_j, X_{k(j)})$ such that the restriction of $\tilde{h}_j$ to L is the identity. For $j \in J_0$ we put $k(j) = j$ and take the identity of X_j as $\tilde{h}_j$. We then put

$$\tilde{e}(\Sigma_{j \in J} m_j) = \Sigma_{j \in J} \tilde{h}_j(m_j) \qquad (m_j \in X_j).$$

The well-definedness of $\tilde{e}$ is deduced from $\tilde{h}_j|L = id_L$. It is an idempotent of $\mathrm{End}_R(M)$, hence $M = \mathrm{im}(\tilde{e}) \oplus \ker(\tilde{e})$ where $\mathrm{im}(\tilde{e})$ is of finite length. Let $h_j \in \mathrm{Hom}_R(N_j, N_{k(j)})$ be the morphism induced from $\tilde{h}_j$ and define $e \in \mathrm{End}_R(N)$ in the same way as in the proof of Proposition 1.3. We then have $N = \mathrm{im}(e) \oplus \ker(e)$ where $\mathrm{im}(e)$ is of finite length. Now π induces an isomorphism from $\ker(\tilde{e})$ to $\ker(e)$. In fact, using $\pi\tilde{e} = e\pi$ and $\tilde{h}_j|L = id_L$ one verifies that π induces an epimorphism from $\ker(\tilde{e})$ to $\ker(e)$. On the other hand $L \subset \mathrm{im}(\tilde{e})$ implies $L \cap \ker(\tilde{e}) = 0$, hence it is a monomorphism. The assertion follows. □

2. Decomposition of $F^{\times}/F^{\times n}$

Throughout the following we denote by F_0 an algebraic number field, $[F_0 : \mathbf{Q}] < \infty$, by F a finite Galois extension of F_0, and by G the Galois group: $G = \mathrm{Gal}(F/F_0)$. Let $n > 1$ be an integer and let $\mathbf{Z}/(n)[G]$ be the group algebra of G over the finite ring $\mathbf{Z}/(n)$. In this section we discuss the $\mathbf{Z}/(n)[G]$-module structure of $F^{\times}/F^{\times n}$.

Let I_F, J_F, U_F, and C_F be, respectively, the ideal group of F, the group of principal ideals of F, the unit group of F, and the ideal class group of F. We have the following exact sequences of left $\mathbf{Z}/(n)[G]$-modules:

$$0 \to U_F/U_F^n \to F^{\times}/F^{\times n} \to J_F/J_F^n \to 0, \tag{1}$$

$$0 \to J_F/J_F \cap I_F^n \to I_F/I_F^n \to C_F/C_F^n \to 0, \tag{2}$$

$$0 \to J_F \cap I_F^n/J_F^n \to J_F/J_F^n \to J_F/J_F \cap I_F^n \to 0. \tag{3}$$

Note that U_F/U_F^n, C_F/C_F^n and $J_F \cap I_F^n/J_F^n$ are finite modules.

Among the $\mathbf{Z}/(n)[G]$-modules in the above exact sequences, the structure of I_F/I_F^n is well-known. Let $P(F)$ be the set of all prime ideals of F, and let $P(F)/G$ be a set of representatives for all G-orbits in $P(F)$. For $L \in P(F)/G$, let G_L be its decomposition group. The uniqueness of the prime factorization in I_F implies

$$I_F/I_F^n \simeq \bigoplus_{L \in P(F)/G} \mathbf{Z}/(n)[G/G_L].$$

Here, for a subgroup H of G, $\mathbf{Z}/(n)[G/H]$ denotes the induced module $\mathrm{Ind}_H^G \mathbf{1}$. Namely it is the Abelian group defined by

$$\mathbf{Z}/(n)[G/H] = \{\lambda \in \mathbf{Z}/(n)[G] : \lambda\tau = \lambda \text{ for all } \tau \in H\}$$

with the $\mathbf{Z}/(n)[G]$-module structure induced by the left translation by G. Let

$C(G)/G$ be a set of representatives for all conjugacy classes of the cyclic subgroups (including the trivial group) of G, and let $P_r(F)/G$ denote a finite set of representatives for all $L \in P(F)$ ramified in F/F_0. By Hilbert's ramification theory and Chebotarev density theorem, we may rewrite the above expression for I_F/I_F^n as

$$I_F/I_F^n \simeq \bigoplus_{H \in C(G)/G} \mathbf{Z}/(n)[G/H]^{\oplus\infty} \oplus \bigoplus_{L \in P_r(F)/G} \mathbf{Z}/(n)[G/G_L],$$

where "$A^{\oplus\infty}$" denotes the direct sum of countably infinite copies of A. Since each summand in the right-hand-side is of finite length, I_F/I_F is FL-decomposable. It is clear that the FL-decomposition has only a finite number of isomorphism classes of summands.

We now apply the results of Sect. 1. Since $\mathbf{Z}/(n)[G]$ is a finite ring we see that an FL-decomposition $N = \bigoplus_{j \in J} N_j$ of a left $\mathbf{Z}/(n)[G]$-module N satisfies the conditions C_1 and C_2 if there are only finitely many isomorphism classes among the summands. Thus we may apply Proposition 1.3 to the exact sequence (2), then Proposition 1.4 to (3) and (1). Hence $\mathbf{Z}/(n)[G]$-modules

$$I_F/I_F^n, \qquad J_F/J_F \cap I_F^n, \qquad J_F/J_F^n, \qquad F^\times/F^{\times n}$$

are FL-decomposable, and they are almost same. Let $L_n(G)$ be a set of representatives for all isomorphism classes of indecomposable summands of $\mathbf{Z}/(n)[G/H]$, H running through cyclic subgroups of G. We have

Theorem 2.1. *The $\mathbf{Z}/(n)[G]$-module $F^\times/F^{\times n}$ is decomposed as*

$$F^\times/F^{\times n} \simeq \bigoplus_{V \in L_n(G)} V^{\oplus\infty} \oplus \bigoplus_{W \in S_n(F/F_0)} W,$$

where $S_n(F/F_0)$ is a finite set of indecomposable $\mathbf{Z}/(n)[G]$-modules with multiplicity, possibly empty, whose members are of finite length and isomorphic to no member of $L_n(G)$.

Remark. Suppose that $n = p$ is a prime and does not divide the order of G. Then every $\mathbf{F}_p[G]$-module is completely reducible by Maschke's theorem, and any irreducible $\mathbf{F}_p[G]$-module is a summand of $\mathbf{F}_p[G]$. Thus in this case $S_p(F/F_0)$ is empty and $L_p(G)$ is a set of representatives for all isomorphism classes of irreducible $\mathbf{F}_p[G]$-modules.

Let F^{ab} be the maximal abelian extension of F and put

$$\mathrm{Gal}(F^{ab}/F)/\mathrm{Gal}(F^{ab}/F)^n = \mathrm{Gal}(F^{ab}/F^{(n)}).$$

Then $F^{(n)}/F_0$ is Galois, hence G acts on $\mathrm{Gal}(F^{(n)}/F)$ by $\gamma\theta = \tilde{\gamma}\theta\tilde{\gamma}^{-1}$, $\gamma \in G$, $\theta \in \mathrm{Gal}(F^{(n)}/F)$, where $\tilde{\gamma}$ is a lift of γ to $\mathrm{Gal}(F^{(n)}/F_0)$. We regard $\mathrm{Gal}(F^{(n)}/F)$ as a left $\mathbf{Z}/(n)[G]$-module in this way. Now let ζ_n be a fixed primitive n-th root of unity and suppose $\zeta_n \in F$. We then have the Kummer pairing

$$\mathrm{Gal}(F^{(n)}/F) \times F^\times/F^{\times n} \to \mu_n = \langle \zeta_n \rangle, \qquad (\theta, \alpha) \mapsto \langle \theta, \alpha \rangle = (\theta - 1)(\alpha^{1/n}).$$

Let $\chi_n : G \to \mathbf{Z}/(n)^\times$ be the cyclotomic character ($\gamma\zeta_n = \zeta_n^{\chi(\gamma)}$ for $\gamma \in G$). The action of G on $\mathrm{Gal}(F^{(n)}/F)$ is related to that on $F^\times/F^{\times n}$ by

$$\langle \gamma\theta, \alpha\rangle = \gamma\langle \theta, \gamma^{-1}\alpha\rangle = \langle \theta, \chi_n(\gamma)\gamma^{-1}\alpha\rangle, \qquad \gamma \in G,$$

cf. [5, Chap. 6]. For a $\mathbf{Z}/(n)[G]$-module A we denote by A^* its contragredient:

$$A^* = \mathrm{Hom}_{\mathbf{Z}/(n)}(A, \mathbf{Z}/(n)), \qquad (\gamma f)(a) = f(\gamma^{-1}a) \quad (a \in A, f \in A^*, \gamma \in G).$$

Theorem 2.1, together with the above formula, implies

$$\begin{aligned}\mathrm{Gal}(F^{(n)}/F) &= \chi_n \otimes (F^\times/F^{\times n})^* \\ &\simeq \prod_{V \in L_n(G)} (\chi_n \otimes V^*)^\infty \times \prod_{W \in S_n(F/F_0)} \chi_n \otimes W^*\end{aligned}$$

where "A^∞" denotes the direct product of countably infinite copies of A. Since $\mathbf{Z}/(n)[G/H]^*$ is isomorphic to $\mathbf{Z}/(n)[G/H]$ for any subgroup H of G we get the following

Theorem 2.2. *If $\zeta_n \in F$, the $\mathbf{Z}/(n)[G]$-module $\mathrm{Gal}(F^{(n)}/F)$ is decomposed as*

$$\mathrm{Gal}(F^{(n)}/F) \simeq \prod_{V \in L_n(G)} (\chi_n \otimes V)^\infty \times \prod_{W \in S_n(F/F_0)} \chi_n \otimes W^*,$$

where $S_n(F/F_0)$ is same as that in Theorem 2.1.

3. Cyclic p-extensions

In the following p denotes a prime, $F_0/\mathbf{Q}$ a finite extension and F/F_0 a cyclic extension of degree p^e, $e \geq 1$. We determine explicitly the decomposition of $F^\times/F^{\times p}$ under the action of the Galois group $G = \mathrm{Gal}(F/F_0)$.

In this section we fix notation and summarize necessary facts about the extension F/F_0. We use the following notation:

σ: a fixed generator of the Galois group G,

F_i: the fixed field of the subgroup $\langle \sigma^{p^i}\rangle$, $0 \leq i \leq e$, in particular $F = F_e$,

$N^*_{F_j/F_i} := 1 + \sigma^{p^i} + \sigma^{2p^i} + \cdots + \sigma^{(p^{j-i}-1)p^i} \in \mathbf{Z}[G]$, $0 \leq i \leq j \leq e$.

As for the last one, we regard $N^*_{F_j/F_i}$ as an operator acting on $F^\times$. Its restriction to $F_j^\times$ coincides with the usual norm N_{F_j/F_i}. The operator acting on $F^\times/F^{\times p}$ induced by $N^*_{F_j/F_i}$ will be denoted by the same symbol.

Since F/F_0 is a p-extension the primitive p-th root of unity belongs to F if and only if it belongs to F_0. In the case $\zeta_p \in F_0$ the following propositions are known, *cf.* [1, Ch. 10]:

Proposition 3.1. *Suppose that $\zeta_p \in F_0$ and that there exists a cyclic extension E/F_0 of degree p^{e+1} with $F \subset E$. Then $\zeta_p \in N_{F/F_0}(F^\times)$, and one may write $E = F(s^{1/p})$ with $s \in F^\times$ satisfying*

$(\sigma - 1)s \in F^{\times p}$,

$N_{F/F_0}(t) = \zeta_p$ *for any solution* $t \in F^{\times}$ *of* $(\sigma - 1)s = t^p$.

Proposition 3.2. *Suppose that* $\zeta_p \in N_{F/F_0}(F^{\times})$. *Then there exists a unique class in* $F^{\times}/F_0^{\times}F^{\times p}$ *whose representative* $s \in F^{\times}$ *satisfies the two conditions in Proposition* 3.1. *For such s,* $E = F(s^{1/p})$ *is a cyclic extension of* F_0 *of degree* p^{e+1}.

For $s \in F^{\times}$ satisfying the above conditions we define the element S of the $\mathbf{F}_p[G]$-module $F^{\times}/F^{\times p}$ by $S := sF^{\times p}$. Then S satisfies

$$S \in \ker(\sigma - 1 : F^{\times}/F^{\times p} \to F^{\times}/F^{\times p}), \qquad S \notin F_{e-1}^{\times}F^{\times p}/F^{\times p}.$$

That S is contained in the kernel is clear. If $S \in F_{e-1}^{\times}F^{\times p}/F^{\times p}$ we may choose s in $F_{e-1}^{\times}$, hence $F(s^{1/p})/F_{e-1}$ contains independent intermediate fields F and $F_{e-1}(s^{1/p})$, both have degree p over F_{e-1}. Hence a contradiction.

For $k = 0, \dots, e-1$ we may consider the condition $\zeta_p \in N_{F/F_k}(F^{\times})$. If $k < j$ we have $N_{F/F_k} = N_{F/F_j}N_{F_j/F_k}^{*}$, hence $\zeta_p \in N_{F/F_k}(F^{\times})$ implies $\zeta_p \in N_{F/F_j}(F^{\times})$. If F_0 contains $\zeta_{p^{e-k+1}}$, a primitive p^{e-k+1}-th root of unity, the condition $\zeta_p \in N_{F/F_k}(F^{\times})$ is always satisfied. In the case where $\zeta_{p^{e-k+1}} \notin F_0$ and $\zeta_{p^{e-k}} \in F_0$, there exists a cyclic extension F/F_0 of degree p^e such that

$$\zeta_p \notin N_{F/F_k}(F^{\times}), \qquad \zeta_p \in N_{F/F_{k+1}}(F^{\times}).$$

In fact, we may choose a prime l of F_0 which is not a divisor of 2 and does not split completely in $F_0(\zeta_{p^{e-k+1}})$. Then the local field $F_{0,l}$ does not contain $\zeta_{p^{e-k+1}}$, hence $F_{0,l}^{\times}$ is decomposed as $\langle \zeta_{p^{e-k}} \rangle \times N$ with an open subgroup N. Let E be the cyclic extension of $F_{0,l}$ of degree p^{e-k} with $N_{E/F_{0,l}}(E^{\times}) = N$. By Grunwald-Wang theorem we can find a cyclic extension F/F_0 of degree p^e such that $F_L = E$ for a prime L of F lying above l, *cf.* [1, Ch. 10]. If $\mathscr{L}$ is a prime of F_k lying above l we have $F_{k,\mathscr{L}} = F_{0,l}$, hence $\zeta_p \notin N_{F/F_k}(F^{\times})$. On the other hand we have $\zeta_p \in N_{F/F_{k+1}}(F^{\times})$ automatically.

4 Decomposition of $F^{\times}/F^{\times p}$ for cyclic p-extensions

We maintain the assumptions and notation of Sect. 3. The structure of the group algebra $\mathbf{F}_p[G]$, $G = \langle \sigma \rangle \simeq \mathbf{Z}/(p^e)$, is described as

$$\mathbf{F}_p[G] \simeq \mathbf{F}_p[x]/(x^{p^e} - 1) \simeq \mathbf{F}_p[t]/(t^{p^e}), \qquad \sigma - 1 \leftrightarrow t.$$

Then it is easy to see that there are exactly p^e isomorphism classes of indecomposable $\mathbf{F}_p[G]$-modules represented by

$$V(d) := \mathbf{F}_p[G]/((\sigma - 1)^d), \qquad d = 1, 2, \dots, p^e,$$

cf. [3, Sect. 64]. The set $L_p(G)$, which we defined in Sect. 2, is given by

$$L_p(G) = \{V(p^i) : i = 0, \dots, e\}$$

because $\mathbf{F}_p[G/\langle \sigma^{p^i} \rangle]$ is isomorphic to $V(p^i)$. Hence by Theorem 2.1 we may write

$$F^{\times}/F^{\times p} = \bigoplus_{i=0}^{e} V(p^i)^{\oplus \infty} \oplus \bigoplus_{d} V(d)^{\oplus m(d)}$$

where each d is not a power of p and $1 < d < p^e$. The Galois module structure of $F^{\times}/F^{\times p}$ is determined by the multiplicities $m(d)$. In the following $\ker(\sigma - 1)$, $\operatorname{im}(\sigma - 1)^d$ etc. denote $\ker(\sigma - 1 : F^{\times}/F^{\times p} \to F^{\times}/F^{\times p})$, $\operatorname{im}((\sigma - 1)^d : F^{\times}/F^{\times p} \to F^{\times}/F^{\times p})$ etc. Then one can easily verify the following multiplicity formula:

$$m(d) = \dim_{\mathbf{F}_p}[\ker(\sigma - 1) \cap \operatorname{im}(\sigma - 1)^{d-1}/\ker(\sigma - 1) \cap \operatorname{im}(\sigma - 1)^d].$$

We simplify the right-hand-side of the above formula. Note that for $d = p^i - 1$, $(\sigma - 1)^d$ coincides with $N^*_{F_i/F_0}$ as an operator on $F^{\times}/F^{\times p}$.

Lemma 4.1. (i) *If* $\zeta_p \notin N_{F/F_0}(F^{\times})$ *one has* $\ker(\sigma - 1) = F_0^{\times} F^{\times p}/F^{\times p}$.

(ii) *If* $\zeta_p \in N_{F/F_0}(F^{\times})$ *one has* $\ker(\sigma - 1) = \langle S \rangle \times (F_0^{\times} F^{\times p}/F^{\times p})$ *where* $S = sF^{\times p}$ *is the nonzero element of* $F^{\times}/F^{\times p}$ *defined in Sect.* 3.

Proof. Let $\alpha = aF^{\times p}$, $a \in F^{\times}$, be an arbitrary element of $F^{\times}/F^{\times p}$. Then

$$\alpha \in \ker(\sigma - 1) \Leftrightarrow (\sigma - 1)(a) = b^p \qquad (\exists b \in F^{\times})$$

and the element b must satisfy $N_{F/F_0}(b)^p = 1$. If $\zeta_p \notin N_{F/F_0}(F^{\times})$ we have $N_{F/F_0}(b) = 1$, namely $b \in (\sigma - 1)(F^{\times})$. Thus $\ker(\sigma - 1) \subset F_0^{\times} F^{\times p}/F^{\times}$ and the converse inclusion is obvious. Hence we get (1). Next, suppose $\zeta_p \in N_{F/F_0}(F^{\times})$. Then S is an element of $\ker(\sigma - 1)$ and any $t \in F^{\times}$ with $t^p = (\sigma - 1)(s)$ satisfies $N_{F/F_0}(t) = \zeta_p$, *cf.* Sect. 3. If the above element b satisfies $N_{F/F_0}(b) = \zeta_p^r$ then $b \in t^r(\sigma - 1)(F^{\times})$ and $(\sigma - 1)(a) \in (\sigma - 1)(s^r F^{\times p})$. Hence $\ker(\sigma - 1) \subset \langle S \rangle (F_0^{\times} F^{\times p}/F^{\times p})$ and the converse inclusion is obvious. By definition of S the product of $\langle S \rangle$ and $F_0^{\times} F^{\times p}/F^{\times p}$ is direct. Thus we get (2). □

Lemma 4.2. *One has* $\ker(\sigma - 1) \cap \operatorname{im}(\sigma - 1) \subset F_0^{\times} F^{\times p}/F^{\times p}$.

Proof. By Lemma 4.1 we may assume $\zeta_p \in N_{F/F_0}(F^{\times})$ and our task is to show that $S \notin \operatorname{im}(\sigma - 1)$. Suppose $S \in \operatorname{im}(\sigma - 1)$ and write $S = (\sigma - 1)(R)$, $R \in F^{\times}/F^{\times p}$. First we treat the case $e = 1$. If $p = 2$, $\sigma - 1$ coincides with N_{F/F_0} on $F^{\times}/F^{\times p}$ and we get $S \in F_0^{\times} F^{\times p}/F^{\times p}$, a contradiction. So assume $p \neq 2$. We then have $R \in \ker(\sigma - 1)^2 \subset \ker(\sigma - 1)^{p-1}$. Writing $R = aF^{\times p}$, $a \in F^{\times}$, we get $N_{F/F_0}(a) \in F_0^{\times} \cap F^{\times p}$. Kummer theory then implies $a \in \langle q \rangle (\sigma - 1)(F^{\times}) F_0^{\times}$, with $q \in F^{\times}$ such that $(\sigma - 1)(q) = \zeta_p$. Hence we may write $(\sigma - 1)(a) = \zeta_p^r (\sigma - 1)^2(b)$, $b \in F^{\times}$. This argument for a applies to b and we get $(\sigma - 1)(a) = \zeta_p^r (\sigma - 1)^3(c)$, $c \in F^{\times}$. Proceeding this way we get $(\sigma - 1)(a) \in \langle \zeta_p \rangle (\sigma - 1)^{p-1}(F^{\times})$. Since $\zeta_p \in N_{F/F_0}(F^{\times})$ we get $S \in \operatorname{im}(\sigma - 1)^{p-1} = \operatorname{im} N_{F/F_0}$, hence $S \in F_0^{\times} F^{\times p}/F^{\times p}$, a contradiction. In the case $e > 1$ we use $\ker(\sigma - 1)^2 \subset \ker(\sigma - 1)^p = \ker(\sigma^p - 1)$. Replacing F_0 by F_1 in Lemma 4.1 we see that $\ker(\sigma^p - 1) = \langle S \rangle \times (F_1^{\times} F^{\times p}/F^{\times p})$, so we may write $R = S^r Q$, $Q \in F_1^{\times} F^{\times p}/F^{\times p}$. We then have, modulo $F_1^{\times} F^{\times p}/F^{\times p}$,

$$\begin{aligned} S &\equiv (\sigma - 1)(S^r Q) \equiv r(\sigma - 1)(S) \equiv r^2(\sigma - 1)^2(S) \\ &\equiv \cdots \equiv r^{p^e - 1}(\sigma - 1)^{p^e - 1}(S) \equiv r^{p^e - 1} N_{F/F_0}(S). \end{aligned}$$

Hence $S \in F_1^{\times} F^{\times p}/F^{\times p}$, a contradiction, because $S \notin F_{e-1}^{\times} F^{\times p}/F^{\times p}$ and $e > 1$. □

By Lemma 4.2 our multiplicity formula is simplified to

$$m(d) = \dim_{\mathbf{F}_p}[(F_0^\times F^{\times p}/F^{\times p}) \cap \mathrm{im}(\sigma-1)^{d-1}/(F_0^\times F^{\times p}/F^{\times p}) \cap \mathrm{im}(\sigma-1)^d]. \qquad (4)$$

Lemma 4.3. (i) $F_0^\times \cap N^*_{F_j/F_i}(F^\times) = N_{F_j/F_0}(F_j^\times)F_0^{\times p^{j-i}}$ *for* $0 \le i \le j \le e$.
(ii) $(F_0^\times \cap N^*_{F_j/F_i}(F^\times))F^{\times p} = N_{F_j/F_0}(F_j^\times)F^{\times p}$ *for* $0 \le i < j \le e$.

Proof. Let $a = N^*_{F_j/F_i}(b)$, $b \in F^\times$, be an element of $F_0^\times \cap N^*_{F_j/F_i}(F^\times)$. We have

$$\begin{aligned}(\sigma-1)a = 1 &\Rightarrow N_{F/F_i}((\sigma-1)(b)) = N_{F/F_j}((\sigma-1)(a)) = 1\\ &\Rightarrow (\sigma-1)(b) \in (\sigma^{p^i}-1)(F^\times) = (\sigma-1)N^*_{F_i/F_0}(F^\times)\\ &\Rightarrow b \in N^*_{F_i/F_0}(F^\times)F_0^\times\\ &\Rightarrow a \in N^*_{F_j/F_0}(c)F_0^{\times p^{j-i}} \qquad (\exists c \in F^\times).\end{aligned}$$

Here we have $(\sigma^{p^j}-1)c = (\sigma-1)N^*_{F_j/F_0}(c) = 1$, hence $c \in F_j^\times$. Thus the left-hand-side of (i) is included in the right-hand-side, and the converse inclusion is obvious. Statement (ii) is clear from (i). □

Now we can describe the explicit decomposition of $F^\times/F^{\times p}$. If $p = 2$ we assume $e \ge 2$, because the set $S_p(F/F_0)$ in Theorem 2.1 is clearly empty in the case $p = 2$, $e = 1$.

Theorem 4.4. *When* $G \simeq \mathbf{Z}/(p^e)$ *the* $\mathbf{F}_p[G]$*-module* $F^\times/F^{\times p}$ *is decomposed as follows:*

(i) *Suppose* $\zeta_p \notin F_0$ *or* $\zeta_p \in N_{F/F_0}(F^\times)$ *or* $p = 2$ *and* $-1 \in N_{F/F_1}(F^\times)$. *Then*

$$F^\times/F^{\times p} \simeq \bigoplus_{i=0}^{e} V(p^i)^{\oplus\infty}.$$

(ii) *Suppose* $\zeta_p \in F_0$ *and* $\zeta_p \notin N_{F/F_0}(F^\times)$ *and, if* $p = 2$, *suppose* $-1 \notin N_{F/F_1}(F^\times)$. *Let* k, $0 \le k < e$, *be the integer such that* $\zeta_p \notin N_{F/F_k}(F^\times)$ *and* $\zeta_p \in N_{F/F_{k+1}}(F^\times)$. *Then*

$$F^\times/F^{\times p} \simeq \bigoplus_{i=0}^{e} V(p^i)^{\oplus\infty} \oplus V(p^k+1).$$

Proof. We determine the multiplicities $m(p^i+1), \dots, m(p^{i+1}-1)$, $0 \le i < e$, by using the multiplicity formula (4). Here we assume $i > 0$ if $p = 2$. We hence investigate the descending chain

$$(F_0^\times F^{\times p}/F^{\times p}) \cap \mathrm{im}(\sigma-1)^{p^i} \supset \cdots \supset (F_0^\times F^{\times p}/F^{\times p}) \cap \mathrm{im}(\sigma-1)^{p^{i+1}-1}. \qquad (5)$$

Let $\alpha = aF^{\times p}$, $a \in F_0^\times$, be an arbitrary element of $F_0^\times F^{\times p}/F^{\times p}$. Then

$$\begin{aligned}\alpha \in \mathrm{im}(\sigma-1)^{p^i} = \mathrm{im}(\sigma^{p^i}-1) &\Leftrightarrow a \in (\sigma^{p^i}-1)(F^\times)F^{\times p}\\ &\Leftrightarrow N_{F/F_i}(a) = a^{p^{e-i}} \in N_{F/F_i}(F^\times)^p\\ &\Leftrightarrow N_{F/F_{i+1}}(a) = a^{p^{e-i-1}} \in \zeta_p^r N_{F/F_i}(F^\times) \qquad (\exists r).\end{aligned}$$

Note that in the case $\zeta_p \notin F_0^\times$ we have $r = 0$, because $\zeta_p \notin F_i^\times$. Hence in all cases the last condition is equivalent to

$$\zeta_p^{-r} N_{F/F_{i+1}}(a) \in F_0^\times \cap N_{F/F_i}(F^\times) \qquad (\exists r),$$

but Lemma 4.3(i) implies $F_0^\times \cap N_{F/F_i}(F^\times) = N_{F/F_0}(F^\times) F_0^{\times p^{e-i}}$. Hence $\alpha = aF^{\times p}$ belongs to $\mathrm{im}(\sigma-1)^{p^i}$ if and only if $a \in F_0^\times$ satisfies

$$\zeta_p^{-r} N_{F/F_{i+1}}(a) \in N_{F/F_{i+1}}(N^*_{F_{i+1}/F_0}(F^\times) F_0^{\times p}) \qquad (\exists r). \tag{6}$$

We now pass to case-by-case arguments.

Case A: $\zeta_p \notin N_{F/F_{i+1}}(F^\times)$ (including the case $\zeta_p \notin F_0$). In this case we have $r = 0$ hence the condition (6) is rewritten as

$$a \in (\sigma^{p^{i+1}} - 1)(F^\times) N^*_{F_{i+1}/F_0}(F^\times) F_0^{\times p} = N^*_{F_{i+1}/F_0}(F^\times) F_0^{\times p}$$

which implies $\alpha \in \mathrm{Im}(\sigma-1)^{p^{i+1}-1}$. Thus all modules in the chain (5) are equal in this case.

Case B: $\zeta_p \in N_{F/F_{i+1}}(F^\times)$. In this case ζ_p belongs to $F_0^\times$ and Lemma 4.3(i) implies $F_0^\times \cap N_{F/F_{i+1}}(F^\times) = N_{F/F_0}(F^\times) F_0^{\times p^{e-i-1}} = N_{F/F_{i+1}}(N^*_{F_{i+1}/F_0}(F^\times) F_0^\times)$. We may, therefore, take $t_{i+1} \in N^*_{F_{i+1}/F_0}(F^\times) F_0^\times$ with $N_{F/F_{i+1}}(t_{i+1}) = \zeta_p$. Then (6) is rewritten as

$$a \in t_{i+1}^r N^*_{F_{i+1}/F_0}(F^\times) F_0^{\times p} \qquad (\exists r).$$

Choosing an element u_{i+1} of $F_0^\times \cap t_{i+1} N^*_{F_{i+1}/F_0}(F^\times)$ we have

$$(F_0^\times F^{\times p}/F^{\times p}) \cap \mathrm{im}(\sigma-1)^{p^i} = \langle u_{i+1} F^{\times p} \rangle ((F_0^\times F^{\times p}/F^{\times p}) \cap \mathrm{im}(\sigma-1)^{p^{i+1}-1}).$$

Case B.1: $\zeta_p \in N_{F/F_i}(F^\times)$. In this case there exists an element t_i of $N^*_{F_i/F_0}(F^\times) F_0^\times$ with $N_{F/F_i}(t_i) = \zeta_p$, and we may put $t_{i+1} = N^*_{F_{i+1}/F_i}(t_i)$. Then

$$\begin{aligned} u_{i+1} F^{\times p} &\in (F_0^\times \cap N^*_{F_{i+1}/F_i}(F^\times) N^*_{F_{i+1}/F_0}(F^\times)) F^{\times p}/F^{\times p} \\ &= (F_0^\times \cap N^*_{F_{i+1}/F_i}(F^\times)) F^{\times p}/F^{\times p} \\ &= N_{F_{i+1}/F_0}(F_{i+1}^\times) F^{\times p}/F^{\times p} \qquad \text{(by Lemma 4.3(ii))}. \end{aligned}$$

Thus all modules in the chain (5) are equal in this case.

Case B.2: $\zeta_p \in N_{F/F_{i+1}}(F^\times)$, $\zeta_p \notin N_{F/F_i}(F^\times)$. We may put $t_{i+1} = (\sigma^{p^i} - 1)(h)$, $h \in F^\times$, because $N_{F/F_i}(t_{i+1}) = N_{F_{i+1}/F_i}(\zeta_p) = 1$. Set

$$c := N_{F/F_{i+1}}(h), \qquad s_i := c^p, \qquad S_i := s_i F_i^{\times p}.$$

Then s_i and S_i are exactly "s" and "S" if we replace the extension F/F_0 by F_i/F_0. In fact we have $(\sigma^{p^i} - 1)(c) = \zeta_p$ by definition, which implies $(\sigma-1)(c) \in F_i$, $N_{F_i/F_0}((\sigma-1)(c)) = \zeta_p$, $s_i \in F_i$. We now prove $u_{i+1} F^{\times p} \notin \mathrm{im}(\sigma-1)^{p^i+1}$. Suppose $u_{i+1} F^{\times p} \in \mathrm{im}(\sigma-1)^{p^i+1}$. Then we have $t_{i+1} F^{\times p} \in \mathrm{im}(\sigma-1)^{p^i+1}$ by definition. Since $\mathrm{im}(\sigma-1)^{p^i+1} = \mathrm{im}(\sigma^{p^i} - 1)(\sigma-1)$ we may write

$$t_{i+1} = (\sigma^{p^i} - 1)(h) = (\sigma^{p^i} - 1)(\sigma-1)(g) v^p, \qquad g, v \in F^\times.$$

We then have $N_{F/F_i}(v)^p = 1$ and the assumption $\zeta_p \notin N_{F/F_i}(F^\times)$ implies $N_{F/F_i}(v) = 1$. Hence we may write $h = (\sigma-1)(g) w^p f$ with $g, w \in F^\times$, $f \in F_i^\times$. If $p \neq 2$ we have

$s_i = N_{F/F_i}(h) \in (\sigma - 1)(F_i^\times)F_i^{\times p}$. If $p = 2$ we have $s_i = -N_{F/F_i}(h)$ but $-1 \in (\sigma - 1) \cdot (F_i^\times)$ (we have assumed $i > 0$ if $p = 2$). Hence in all cases we have $s_i \in (\sigma - 1) \cdot (F_i^\times)F_i^{\times p}$, namely

$$S_i \in \ker(\sigma - 1 : F_i^\times/F_i^{\times p} \to F_i^\times/F_i^{\times p}) \cap \operatorname{im}(\sigma - 1 : F_i^\times/F_i^{\times p} \to F_i^\times/F_i^{\times p}).$$

This is clearly a contradiction if $i = 0$. Replacing F by F_i in Lemma 4.2 we see that this is a contradiction also in the case $i > 0$. Hence we have

$$(F_0^\times F^{\times p}/F^{\times p}) \cap \operatorname{im}(\sigma - 1)^{p^i} = \langle u_{i+1}F^{\times p}\rangle \times ((F_0^\times F^{\times p}/F^{\times p}) \cap \operatorname{im}(\sigma - 1)^{p^{i+1}-1}),$$

$$u_{i+1}F^{\times p} \notin (F_0^\times F^{\times p}/F^{\times p}) \cap \operatorname{im}(\sigma - 1)^{p^i+1},$$

$$(F_0^\times F^{\times p}/F^{\times p}) \cap \operatorname{im}(\sigma - 1)^{p^i+1} = (F_0^\times F^{\times p}/F^{\times p}) \cap \operatorname{im}(\sigma - 1)^{p^{i+1}-1}.$$

Theorem is now clear from the above results. □

In Sect. 2 we have dicussed the $\mathbf{Z}/(n)[G]$-module $\operatorname{Gal}(F^{(n)}/F)$. The above theorem implies

Theorem 4.5. *When $G \simeq \mathbf{Z}/(p^e)$ and $\zeta_p \in F_0$, the $\mathbf{F}_p[G]$-module $\operatorname{Gal}(F^{(p)}/F)$ is decomposed as follows:*

(i) *Suppose $\zeta_p \in N_{F/F_0}(F^\times)$ or $p = 2$ and $-1 \in N_{F/F_1}(F^\times)$. Then*

$$\operatorname{Gal}(F^{(p)}/F) \simeq \prod_{i=0}^{e} V(p^i)^\infty.$$

(ii) *Suppose $\zeta_p \notin N_{F/F_0}(F^\times)$ and, if $p = 2$, suppose $-1 \notin N_{F/F_1}(F^\times)$. Let k be as in Theorem 4.4(ii). Then*

$$\operatorname{Gal}(F^{(p)}/F) \simeq \prod_{i=0}^{e} V(p^i)^\infty \times V(p^k + 1).$$

References

[1] E. Artin and J. Tate, Class Field Theory, Benjamin, New York, 1967.

[2] H. Brune, On finite representation type and a theorem of Kulikov, *in* Representation Theory II, pp. 170–176, Lecture Notes in Mathematics, Vol. 832, Springer Verlag, Berlin/Heidelberg/New York, 1980.

[3] C. W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience, New York, 1962.

[4] F. Kasch, Modules and Rings, Academic Press, London, 1982.

[5] S. Lang, Cyclotomic Fields I and II, Springer Verlag, Berlin/Heidelberg/New York, 1990.