GALOIS MODULE STRUCTURE OF pTH-POWER CLASSES OF EXTENSIONS OF DEGREE p

BY

JÁN MINÁČ[*][†]

Department of Mathematics, Middlesex College
University of Western Ontario, London, Ontario N6A 5B7, Canada
e-mail: minac@uwo.ca

AND

JOHN SWALLOW

Department of Mathematics, Davidson College
Box 7046, Davidson, NC 28035, USA
e-mail: joswallow@davidson.edu

ABSTRACT

For fields F of characteristic not p containing a primitive pth root of unity, we determine the Galois module structure of the group of pth-power classes of K for all cyclic extensions K/F of degree p.

The foundation of the study of the maximal p-extensions of fields K containing a primitive pth root of unity is a group of the pth-power classes of the field: by Kummer theory this group describes elementary p-abelian quotients of a maximal p-extension. The size of the group controls the number of generators of the Galois group of the maximal p-extension. Furthermore, as K varies among the Galois extensions of the base field F, the Galois module structure of pth-power classes plays a fundamental role in the investigation of the Galois group of the maximal p-extension of F. In particular, in the nineteen-sixties Borevič and Faddeev closely studied the Galois module structure of the pth-power classes of K for

[*] Research supported in part by the Natural Sciences and Engineering Research Council of Canada and by the special Dean of Science Fund at the University of Western Ontario.

[†] Supported by the Mathematical Sciences Research Institute, Berkeley.

Received July 22, 2002

cyclic extensions K/F of degree p in the case when F is a local field, and in the seventies Miki used this structure in the service of Galois embedding problems (see [Bo], [Fad], and [Mi]).

From a cohomological point of view, the Galois module structure of pth-power classes is especially important. These Galois modules may be naturally identified with the first cohomology groups of maximal p-extensions with $\mathbb{F}_p$-coefficients. (See [S, Chapter 1].) It is moreover conjectured that the entire Galois cohomology ring of K with coefficients in $\mathbb{F}_p$ of degree at least one is generated by its first cohomology group. (See [V] for a proof in the case of $p = 2$ as well as comments on this conjecture which was initially considered by Beilinson, Bloch-Kato, Lichtenbaum, and Milnor.) As a result, for the investigation of the action of the Galois group $\mathrm{Gal}(K/F)$ on the Galois cohomology of K with coefficients in $\mathbb{F}_p$, it should be sufficient to understand the Galois module structure of the pth-power classes of K. Furthermore, this is necessary for the study of a Galois cohomology ring of F with coefficients in $\mathbb{F}_p$ using the Lyndon–Hochschild–Serre spectral sequence attached to a group extension of an absolute Galois group of K by $\mathrm{Gal}(K/F)$.

Hence the question of determining the Galois module structure of the pth-power classes of K is a fundamental question related to both the structure of the Galois cohomology of F and the structure of the maximal p-extensions of F.

It is surprising that one can determine this Galois module structure for all cyclic field extensions of degree p, when the base field contains a primitive pth root of unity, and that the proofs are elementary. Just as in the case of local fields, the structure depends upon only the norm subgroup, its intersection with the subgroup of pth roots of unity, and the multiplicative subgroup of the base field. When we first approached these results, the main tools employed were Waterhouse's elegant treatment of Galois closures of certain Kummer extensions, as well as a criterion for the realization of a nonabelian Galois group of order p^3 and exponent p as a Galois group over our base field. We were able, however, to simplify our proofs considerably. In particular, we require in this paper only Hilbert's Theorem 90, basic Kummer theory, and linear algebra over $\mathbb{F}_p[\mathrm{Gal}(K/F)]$.

Our results remain closely related to Galois embedding problems considered in [Ma], [Ma-Ng], and [Wat], and this relationship remains worthy of precise formulation. The embedding problems related to our work concern the realization of Galois groups H that may be obtained by the extension of an elementary abelian p-group by a cyclic group $G = \mathrm{Gal}(K/F)$ of order p. The solution of such a problem is a Galois extension L/F containing K/F such that $\mathrm{Gal}(L/F) \cong H$ and the Galois restriction from L to K induces the surjective homomorphism $H \longrightarrow G$. The connection with the G-module structure of pth-power classes of K lies in the fact that all possible solutions of these embedding problems may be obtained by adjoining pth roots of elements in a suitable G-submodule of pth-power classes of K. Using results obtained in this paper, one can in particular exhibit some interesting cases when a solution of one embedding problem implies an automatic solution of another embedding problem. A detailed exposition of the applications of the results of this paper to embedding problems will be a topic of subsequent work.

It is clear that one can generalize the main theorems to a larger family of field extensions K/F than we are considering here. Also, these results may be applied to calculations in Galois cohomology, and the study of Galois groups of maximal p-extensions of fields. We concentrate here, however, on the short exposition of a solution of a main significant problem.

1. Main theorems

Let F be a field of characteristic not p containing a primitive pth root of unity ξ_p. Let K be a cyclic extension $K = F(\sqrt[p]{a})$, $K^\times = K \setminus \{0\}$ and $J = K^\times/K^{\times p}$.

Denote $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ by G, where $\sigma \in \mathrm{Gal}(K/F)$ such that $\sqrt[p]{a}^{\sigma-1} = \xi_p$. For G-modules V, denote by V^G the fixed submodule of V.

Maps related to the norm will play an important role, and as a result we use N in several different ways. As an element of $\mathbb{F}_p[G]$ we let $N := 1 + \sigma + \cdots + \sigma^{p-1}$. We also view N as the resulting G-homomorphism $V \longrightarrow V$. Then we write $N(J)$ for the image of J, and $N(K^\times)$ for the image of $K^\times$.

The following two theorems classify all modules J using only information about the extension K/F encoded in the multiplicative subgroup of F.

THEOREM 1: *Suppose $p > 2$. As an $\mathbb{F}_p[G]$-module, J decomposes as*

$$J = X \oplus Y \oplus Z$$

where

(1) *X is an indecomposable $\mathbb{F}_p[G]$-submodule, of dimension 1 if $\xi_p \in N(K^\times)$ and of dimension 2 if $\xi_p \notin N(K^\times)$;*

(2) *Y is a free $\mathbb{F}_p[G]$-submodule with $Y^G = N(J)$; and*

(3) *Z is a trivial $\mathbb{F}_p[G]$-module.*

Moreover, the rank of any maximal free $\mathbb{F}_p[G]$-submodule of J is equal to the rank of $N(J)$ as an $\mathbb{F}_p$-module.

THEOREM 2: *Suppose $p = 2$. As an $\mathbb{F}_2[G]$-module, J decomposes as*

$$J = X \oplus Y \oplus Z$$

where

(1) *X is of dimension 1 if $-1 \in N(K^\times)$ and is $\{0\}$ otherwise;*
(2) *Y is a free $\mathbb{F}_2[G]$-submodule with $Y^G = N(J)$; and*
(3) *Z is a trivial $\mathbb{F}_2[G]$-module.*

Moreover, the rank of any maximal free $\mathbb{F}_2[G]$-submodule of J is equal to the rank of $N(J)$ as an $\mathbb{F}_2$-module.

The results in Theorem 1 and Theorem 2 imply that each $\mathbb{F}_p[G]$-module J can be written as a sum of cyclic $\mathbb{F}_p[G]$-modules. Because each cyclic $\mathbb{F}_p[G]$-module is an indecomposable module, and each ring of the $\mathbb{F}_p[G]$-endomorphisms of such a module is a local ring, we can conclude that our decompositions are unique. This follows from the Krull–Schmidt–Remak–Azumaya theorem. (See [Fac, page 24].)

In the next theorem, which is a supplement to both Theorems 1 and 2, we determine the multiplicity of each cyclic $\mathbb{F}_p[G]$-module in a decomposition of an $\mathbb{F}_p[G]$-module J using the arithmetic invariants associated with a field extension K/F. We provide a direct proof of this theorem, and in particular we do not use the Krull–Schmidt–Remak–Azumaya theorem quoted above. We use the same notation as above, and we also set $\Upsilon(K) = 1$ or 0 depending upon whether $\xi_p \in N(K^\times)$ or $\xi_p \notin N(K^\times)$. For each set A we denote by $|A|$ the cardinal number of A. Observe that each nonzero cyclic $\mathbb{F}_p[G]$-module M is characterized by its $\dim_{\mathbb{F}_p} M \in \{1, 2, \ldots, p\}$.

THEOREM 3: *Let $J \cong \bigoplus_{i=1}^{p}(\bigoplus_{j\in\mathfrak{K}_i} M_{i,j})$ be a decomposition of J into $\mathbb{F}_p[G]$-cyclic modules $M_{i,j}$, where $\dim_{\mathbb{F}_p} M_{i,j} = i$ and $\mathfrak{K}_i$ are index sets for each $i \in \{1, 2, \ldots, p\}$.*

Then we have

(1) *$|\mathfrak{K}_1| + 1 = 2\Upsilon(K) + \dim_{\mathbb{F}_p}(F^\times/N(K^\times))$;*
(2) *If $p > 2$ then $|\mathfrak{K}_2| = 1 - \Upsilon(K)$;*
(i) *If $3 \le i \le (p-1)$ then $\mathfrak{K}_i = \emptyset$; and*
(p) *$|\mathfrak{K}_p| = \dim_{\mathbb{F}_p} N(J)$.*

The proofs of Theorems 1, 2 and 3 are presented in Section 3.

As a consequence of these theorems and their proofs, we have the following results on extremal cases. A short proof of each is given in the last section of this paper.

Recall that if $p > 2$ then $a \in F \setminus F^p$ is *p-rigid* if, whenever the cyclic algebra $(\frac{a,b}{F,\xi_p})$ is of trivial class in $\mathrm{Br}(F)$, then $[b] \in \langle [a] \rangle$ in $F^\times/F^{\times p}$. For a discussion of p-rigidity and G-invariant modules J, see [War]. For the basic properties of cyclic algebras and Brauer groups, see [P, Chapters 14 and 15]. In Corollary 1, part (1) below, we consider the trivial module $J = (0)$ to be a free $\mathbb{F}_p[G]$-module.

COROLLARY 1:

(1) *J is a free $\mathbb{F}_p[G]$-module precisely when $p = 2$, $-1 \notin N(K^\times)$, and $F^\times = N(K^\times) \cup -N(K^\times)$.*

(2) *If $p > 2$ then J contains no free direct summand precisely when a is p-rigid. If $p = 2$ then J contains no free direct summand precisely when $N(K^\times)/F^{\times 2} \subset \langle [a] \rangle \subset F^\times/F^{\times 2}$. (In this case it follows that $\sqrt{-1} \in K^\times$.)*

(3) *If $p > 2$ then J is G-invariant precisely when a is p-rigid and $\xi_{p^2} \in K^\times$. If $p = 2$ then J is G-invariant precisely when J contains no free summand.*

It is worth pointing out that in the corollary above, we can replace "free direct summand of J" by "free submodule of J", as it is well known that each free submodule of an $\mathbb{F}_p[G]$-module is in fact its summand. (See [C, Theorem 11.2].)

Observe that if J is an $\mathbb{F}_p[G]$-module as above, and φ: $H \longrightarrow G$ is any isomorphism, we can consider J to be an $\mathbb{F}_p[H]$-module and the isomorphism type of this module is independent of the choice of φ. In particular, if we have two $\mathbb{F}_p[G_i]$-modules J_i, $i = 1, 2$ with $G \cong G_i$, $i = 1, 2$, we may consider both modules J_i as modules over the same group ring $\mathbb{F}_p[G]$. We shall apply this remark to the following situation.

Suppose $p > 2$ and $K_1 = F_1(\sqrt[p]{a})$ and $K_2 = F_2(\sqrt[p]{a})$ are two cyclic extensions of degree p. We also set $T_i = K_i^\times/K_i^{\times p}, G_i = \mathrm{Gal}(K_i/F_i)$ for $i = 1, 2$, and using any isomorphisms φ_i: $G \longrightarrow G_i$ as above we consider both modules T_1 and T_2 as modules over $\mathbb{F}_p[G]$. (We write here T_i instead of J_i so that we avoid possible confusion with our notation for the socle series employed later in this paper.)

Using this notation we shall formalize our classification of $\mathbb{F}_p[G]$-modules J by means of arithmetic invariants associated with the multiplicative group $F^\times$ as follows.

COROLLARY 2: *The $\mathbb{F}_p[G]$-modules T_1 and T_2 are isomorphic if and only if the following three conditions are valid:*

(1) $\xi_p \in N(K_1^\times) \Leftrightarrow \xi_p \in N(K_2^\times)$.

(2) $\dim_{\mathbb{F}_p} N(K_1^\times)/F_1^{\times p} = \dim_{\mathbb{F}_p} N(K_2^\times)/F_2^{\times p}$.

(3) $\dim_{\mathbb{F}_p} F_1^\times/N(K_1^\times) = \dim_{\mathbb{F}_p} F_2^\times/N(K_2^\times)$.

For $p = 2$ we obtain a similar Corollary 3. We use the same notation as in the case of $p > 2$ above. Moreover, we set $\Upsilon(K_i) = 1$ or 0 depending upon whether $-1 \in N(K_i^\times)$ or $-1 \notin N(K_i^\times)$, for both $i = 1, 2$.

COROLLARY 3: *The $\mathbb{F}_2[G]$-modules T_1 and T_2 are isomorphic if and only if the following two conditions are valid:*

(1) $2\Upsilon(K_1) + \dim_{\mathbb{F}_2} F_1^\times/N(K_1^\times) = 2\Upsilon(K_2) + \dim_{\mathbb{F}_2} F_2^\times/N(K_2^\times)$.

(2) $\Upsilon(K_2) + \dim_{\mathbb{F}_2} N(K_1^\times)/F_1^{\times 2} = \Upsilon(K_1) + \dim_{\mathbb{F}_2} N(K_2^\times)/F_2^{\times 2}$.

2. Cyclic modules and fixed elements of J

This section contains a few basic facts used in our proofs of Theorems 1 and 2. For any subset $\{x, y, \ldots\}$ of V we denote by $\langle x, y, \ldots \rangle$ the $\mathbb{F}_p$-submodule of V spanned by $\{x, y, \ldots\}$.

We freely use basic Kummer theory (see [A-T, Chapter 6, Section 2]), and, depending upon the context, we use additive and multiplicative notation for our $\mathbb{F}_p[G]$-modules occurring as submodules of $K^\times/K^{\times p}$.

Let $A = \bigoplus_{j=0}^{p-1} \mathbb{F}_p \tau^j$ be a free $\mathbb{F}_p[G]$-module on one generator 1, where σ acts by multiplication by τ. For $i = 1, \ldots, p-1$, let A_i denote the cyclic $\mathbb{F}_p[G]$-submodule

$$A_i = \langle (\tau - 1)^i, (\tau - 1)^{i+1}, \ldots, (\tau - 1)^{p-1} \rangle, \text{ and set also } A_p = \{0\}.$$

The dimension of A/A_i is i, and the $\mathbb{F}_p[G]$-modules A/A_i exhaust the isomorphism classes of indecomposable $\mathbb{F}_p[G]$-modules. When describing an indecomposable $\mathbb{F}_p[G]$-module, we will use length synonymously with dimension. The only proper $\mathbb{F}_p[G]$-submodules of A/A_i are cyclic and they are the images of A/A_i under $(\sigma - 1)^j$ for $j = 1, \ldots, i-1$.

The socle series of J will be important for the determination of indecomposable submodules of J. The socle series of J is defined by $J_1 = J^G$ and $(J_i/J_{i-1}) = (J/J_{i-1})^G$ for $i > 1$. We have that $J_i = \ker(\sigma - 1)^i$, when $(\sigma - 1)^i$ is considered as an endomorphism of J.

Indecomposable submodules of J may therefore be obtained as follows. We write the elements of J as $[\gamma], \gamma \in K^\times$. For $[\gamma] \in J_i \setminus J_{i-1}$ let $\gamma_j = \gamma^{(\sigma-1)^j}$ for $j = 0, 1, \ldots, i-1$. Then the $\mathbb{F}_p$-submodule $M_\gamma := \langle [\gamma], [\gamma_1], \ldots, [\gamma_{i-1}] \rangle$ of J is a cyclic $\mathbb{F}_p[G]$-submodule of dimension i isomorphic to A/A_i.

In the proof of Theorem 1 in the next section, we shall construct submodules X, Y and Z of J such that X is a cyclic submodule of J of length 1 or 2, Z is a trivial submodule of J, and Y is a free $\mathbb{F}_p[G]$-submodule of J. An important part of the proof will be to show that X, Y and Z generate J as an $\mathbb{F}_p[G]$-module. In order to do this we need to construct a module Y which is sufficiently large. The following lemma will be used to show that we have enough free cyclic submodules of J to construct our sufficiently large free $\mathbb{F}_p[G]$-submodule Y of J.

LEMMA 1: *Suppose $p > 2$ and let l denote the length of M_γ.*

(a) *If $3 \le l \le p$, then there exists an element $[\alpha] \in J$ such that $\langle N([\alpha])\rangle = M_\gamma^G$.*

(b) *If $l = 2$ and γ cannot be written as $\gamma = a^{r/p}\gamma_1$ for some $r \in \mathbb{Z}$ and $[\gamma_1] \in J_1$, then there exists an integer $t \in \mathbb{Z}$ and $[\alpha] \in J$ such that $\langle N([\alpha])\rangle = (M_{a^{t/p}\gamma})^G$.*

Proof: Let $3 \le l \le i \le p$. We show by induction on i that there exists an element $\alpha_i \in K^\times$ such that $\langle [\alpha_i]^{(\sigma-1)^{i-1}}\rangle = M_\gamma^G$. Then we may set $\alpha := \alpha_p$ and the proof of the first part of our lemma will be complete. If $i = l$ we set $\alpha_l = \gamma$. Assume now that $l \le i < p$ and that our statement is true for i.

Set $c = N(\alpha_i)$. Since $[\alpha_i]^{(\sigma-1)^{p-1}} = [c]$ and $i < p$ we see that $[c] = [1] \in J$. Because $c \in F^\times \cap K^{\times p}$ from Kummer theory, we conclude that $c = a^s f^p$ for some $f \in F^\times$ and $s \in \mathbb{Z}$. Then $N(\alpha_i/fa^{s/p}) = 1$. By Hilbert's Theorem 90 there exists an element $\omega \in K^\times$ such that $\omega^{\sigma-1} = \alpha_i/fa^{s/p}$. Then $\omega^{(\sigma-1)^2} = \alpha_i^{(\sigma-1)}/\xi_p^s$. Therefore $\langle \omega^{(\sigma-1)^i}\rangle = M_\gamma^G$ and we can set $\alpha_{i+1} := \omega$.

Now we shall prove the second part of our lemma. Assume $l = 2 = i$. Proceeding in the same way as above, we see that for $\alpha_2 = \gamma$ we have $N(\alpha_2) = c = a^s f^p$ for some $f \in F^\times$ and $s \in \mathbb{Z}$.

As before we see that there exists an element $\omega \in K^\times$ such that $\omega^{\sigma-1} = \alpha_2/fa^{s/p}$. Then $\omega^{(\sigma-1)^2} = (\alpha_2 a^{-s/p})^{(\sigma-1)} = (\gamma a^{-s/p})^{(\sigma-1)}$. Observe that $\gamma a^{-s/p} \notin J_1$ by our hypothesis, and therefore the length of $M_{\gamma a^{-s/p}}$ is again 2. Hence we can set $\alpha_3 := \omega$. We can then continue by induction on i as above, concluding that there exists an element $\alpha := \alpha_p$ such that $\langle N([\alpha])\rangle = (M_{\gamma a^{-s/p}})^G$ as required. ∎

Remark 1: In the case of $\xi_p \in N(K^\times)$ we do not need the adjusting factor $a^{t/p}$ in part (b) of Lemma 1. Also in this case no restriction on γ is necessary and γ can be any element of $K^\times$ such that the length of M_γ is 2.

Indeed let $\beta \in K^\times$ such that $N(\beta) = \xi_p$. As before we have $\omega^{(\sigma-1)} = \alpha_2/fa^{s/p}$ for some $\omega \in K^\times$ and $s \in \mathbb{Z}$. Then set $\theta = (\beta^{(\sigma-1)^{p-3}})^s\,\omega$. Then $\theta^{(\sigma-1)^2} = \alpha_2^{(\sigma-1)}$. Hence we may set $\alpha_3 := \theta$. We may then continue by induction on i to conclude that there exists an element $\alpha := \alpha_p$ such that $\langle N([\alpha])\rangle = M_\gamma^G$.

In the next lemma we determine J_1 in terms of arithmetic invariants of K/F encoded in the multiplicative group of F. We write $\epsilon(F^\times)$ for the subgroup $F^\times K^{\times p}/K^{\times p}$ of J.

LEMMA 2:

(a) *If* $\xi_p \notin N(K^\times)$ *then* $J_1 = \epsilon(F^\times)$.

(b) *If* $\xi_p \in N(K^\times)$ *then* $J_1 \cong \epsilon(F^\times) \oplus \langle\delta\rangle$ *where* $\delta \in K^\times, \sigma(\delta)/\delta = \lambda^p$ *and* $N(\lambda) = \xi_p$.

Proof: Suppose that $\theta \in K^\times$ such that $[\theta] \in J_1$. Then $\sigma(\theta)/\theta = \lambda^p$ for some $\lambda \in K^\times$, and hence $N(\lambda)^p = 1$. Hence we see that $N(\lambda) = \xi_p^c$ for some $c \in \mathbb{Z}$. Now consider the case $\xi_p \notin N(K^\times)$. Then $N(\lambda) = 1$, because otherwise ξ_p would be a norm of a suitable power of λ. Therefore from Hilbert's Theorem 90 we see that $\sigma(\theta)/\theta = \sigma(k^p)/k^p$ for some $k \in K^\times$. We conclude that $\theta/k^p \in F^\times$ and hence $[\theta] = [f]$ for some $f \in F^\times$. Therefore if $\xi_p \notin N(K^\times)$ then $J_1 = \epsilon(F^\times)$ as required.

Now assume that $\xi_p \in N(K^\times)$. Then $\xi_p = N(\lambda)$ for some $\lambda \in K^\times$ and by Hilbert's Theorem 90 there exists an element $\delta \in K^\times$ such that $\sigma(\delta)/\delta = \lambda^p$. Then the $\mathbb{F}_p[G]$-submodule of J generated by δ and $\epsilon(F^\times)$ is isomorphic with $\epsilon(F^\times) \oplus \langle\delta\rangle$. Now for each $[\theta] \in J_1, \sigma(\theta)/\theta = \nu^p, N(\nu) = \xi_p^c, c \in \mathbb{Z}$, and therefore we have $[\theta] \in \epsilon(F^\times)[\delta]^c$. Hence $J_1 \cong \epsilon(F^\times) \oplus \langle\delta\rangle$ as required. ∎

Remark 2: It is worthwhile to observe that we have the following short exact sequence:

$$0 \longrightarrow \langle[a]\rangle \xrightarrow{i} F^\times/F^{\times p} \xrightarrow{\epsilon} J_1 \xrightarrow{N} \langle[a]\rangle,$$

where $\langle[a]\rangle$ is the subgroup of $F^\times/F^{\times p}$ generated by $[a] \in F^\times/F^{\times p}$, i is the inclusion map, ϵ is the natural homomorphism induced by the inclusion map $F^\times \longrightarrow K^\times$ and N is the map induced by the norm map $N\colon K^\times \longrightarrow F^\times$. Moreover, the map $N\colon J_1 \longrightarrow \langle[a]\rangle$ is surjective if and only if $\xi_p \in N(K^\times)$.

The fact that $[N(\theta)] \in \langle[a]\rangle$ for each $[\theta] \in J_1$ follows from the fact that $N(\theta) \in F^\times \cap K^{\times p}$. The exactness at $F^\times/F^{\times p}$ follows from Kummer theory. The exactness at J_1 can be seen as follows.

Suppose that $[\theta] \in J_1$. Then $\sqrt[p]{N(\theta)} \in K^\times$ and $[N(\theta)] = [1] \in F^\times/F^{\times p}$ if and only if $\sigma(\sqrt[p]{N(\theta)})/\sqrt[p]{N(\theta)} = 1$. Set $\sigma(\theta)/\theta = \lambda^p, \lambda \in K^\times$. Then the condition $\sigma(\sqrt[p]{N(\theta)})/\sqrt[p]{N(\theta)} = 1$ translates as $N(\lambda) = 1$. Using Hilbert's Theorem 90 as in the proof of Lemma 2, part (a) above, we see that $N(\lambda) = 1$ if and only if $[\theta] \in \epsilon(F^\times)$.

Finally, if $\xi_p \notin N(K^\times)$ we know that $\epsilon\colon F^\times/F^{\times p} \longrightarrow J_1$ is surjective and hence $N\colon J_1 \longrightarrow \langle[a]\rangle$ is trivial. If $\xi_p \in N(K^\times)$, then $\epsilon\colon F^\times/F^{\times p} \longrightarrow J_1$ is not surjective and therefore N must be surjective.

3. Proofs

Proof of Theorem 1: In the first part of this proof we shall construct some submodules X, Y and Z of J, and we shall show that they generate a submodule of J isomorphic to $X \oplus Y \oplus Z$. In the second part of this proof we shall show that X, Y and Z generate the full module J.

We first construct X. If $\xi_p \in N(K^\times)$, then by Remark 2 at the end of Section 2 we see that there exists an element $\delta \in K^\times$ such that $N(\delta) = a$ and $[\delta] \in J_1$. Then we set $X = \langle[\delta]\rangle$.

If $\xi_p \notin N(K^\times)$, then let $\delta = \sqrt[p]{a}$ and $X = \langle[\delta], [\xi_p]\rangle \subset J_2$. If $[\xi_p] = [1]$, then a root of unity ξ_{p^2} of order p^2 lies in $K^\times$ and we can pick ξ_{p^2} such that $\xi_p = N(\xi_{p^2})$, contrary to hypothesis. Because $[\sqrt[p]{a}]^{\sigma-1} = [\xi_p]$, X is isomorphic to A/A_2.

We proceed to construct Y. Let $\mathcal{I}$ be an $\mathbb{F}_p$-basis for $N(J)$. For each $[x] \in \mathcal{I}$ we construct a free $\mathbb{F}_p[G]$-module $M(x)$, as follows. Choose a representative $x \in F^\times$ for $[x]$, such that $x \in N(K^\times)$. Choose $\gamma \in K^\times$ such that $x = N(\gamma)$. Finally set $M(x) = M_\gamma$.

We claim that the $M(x)$, $[x] \in \mathcal{I}$, are independent. First we show by induction on the number of modules that a finite set of modules $M(x)$ is independent. The base case is trivial. Now suppose that $W = M(x') \cap \sum_{[x'] \neq [x]} M(x) \neq \{0\}$. Then W contains the 1-dimensional submodule $V = M(x') \cap J_1$. If $M(x') = M_\omega$, then $V = \langle[N(\omega)]\rangle = \langle[x']\rangle$. Since $[x'] \in W$, $[x']$ is a finite sum $\sum_{[x'] \neq [x]}[m(x)]$ where $[m(x)] \in M(x)$. By induction the modules $M(x)$ appearing in the sum are independent. Then since $[x']$ is in J_1, each $[m(x)] \in J_1$ as well. But then each $[m(x)] \in \langle[x]\rangle$, hence $[m(x)] \in N(J)$. Since $[x']$ and the finite number of elements $[x]$ considered above are distinct elements of an $\mathbb{F}_p$-base for $N(J)$, they are independent, and we have a contradiction.

Now if $W = M(x') \cap \sum_{[x'] \neq [x]} M(x) \neq \{0\}$ where the sum is infinite, the same argument holds, since $[x'] \in V = W \cap J_1$ is a finite sum of elements $[m(x)]$. Hence the $M(x)$, $[x] \in \mathcal{I}$, are independent.

Let $Y = \bigoplus_{\mathcal{I}} M(x)$. Then Y is a free $\mathbb{F}_p[G]$-module with a generating set in one-to-one correspondence with a generating set for $N(J)$ as an $\mathbb{F}_p$-module. Moreover, $Y^G = \bigoplus M(x)^G = \bigoplus\langle[x]\rangle = N(J)$.

Let Z be any complement in $\epsilon(F^\times)$ of the $\mathbb{F}_p$-submodule of J generated by $N(J)$ and $X \cap \epsilon(F^\times)$. Clearly Z is a trivial $\mathbb{F}_p[G]$-module.

We claim that X, Y, and Z are independent $\mathbb{F}_p[G]$-submodules of J. If $W = Y \cap Z \neq \{0\}$, then W is a submodule of $\epsilon(F^\times)$. Let $[x] \in W$. Then $[x]$ lies in $Y \cap J_1 = N(J)$, as well as in Z. But Z is a complement of $\epsilon(F^\times)$ of a submodule containing $N(J)$, a contradiction. Therefore the $\mathbb{F}_p[G]$-submodule of J generated by Y and Z is isomorphic with $Y \oplus Z$.

Now suppose $W = X \cap (Y \oplus Z) \neq \{0\}$. Considering $W \cap J_1$ as above, we find that X is of dimension 2, $\xi_p \notin N(K^\times)$, and $W = \langle[\xi_p]\rangle$. If $[\xi_p] \in N(J)$ then $\xi_p a^c \in N(K^\times)$ for some $c \in \mathbb{Z}$. However, since $N(\sqrt[p]{a}) = a$, we have $\xi_p \in N(K^\times)$, a contradiction. Therefore $W \cap Y = \{0\}$ and $[\xi_p] = y + z$, $y \in Y$, $z \in Z$, with $z \neq 0$. Hence $y \in J_1 \cap Y = N(J)$, and $z = [\xi_p] - y$ is the relation in $\epsilon(F^\times)$. But Z is a complement in $\epsilon(F^\times)$ of the submodule generated by $N(J)$ and $(X \cap \epsilon(F^\times)) = \langle[\xi_p]\rangle$, a contradiction.

Let $\tilde{J}$ be the $\mathbb{F}_p[G]$-submodule of J generated by $X \cup Y \cup Z$. As we have shown above, $\tilde{J} \cong X \oplus Y \oplus Z$. We show that $J = \tilde{J}$ by induction on the socle series of J.

First we show $J_1 \subset \tilde{J}$. From our construction of modules X, Y and Z we see that $\epsilon(F^\times) \subset \tilde{J}$. Therefore from Lemma 2(a) in Section 2 we see that if $\xi_p \notin N(K^\times)$ then $J_1 \subset \tilde{J}$. If $\xi_p \in N(K^\times)$ then, from the definition of X and Lemma 2(b), we see that again $J_1 \subset \tilde{J}$.

For the inductive step, assume $J_i \subset \tilde{J}, 1 \leq i < p$, and let $[\gamma] \in J_{i+1} \setminus J_i$.

Let $\langle[b]\rangle = M_\gamma^G$. From our Lemma 1(a) in Section 2 we see that if $i \geq 2$ then $[b] \in N(J)$. If $i = 1$ and $\xi_p \in N(K^\times)$ we see from Remark 1 in Section 2 that again $[b] \in N(J)$. If $\xi_p \notin N(K^\times)$ then $[\sqrt[p]{a}] \in X$, and therefore it is sufficient to show that $[a^{t/p}\gamma] \in \tilde{J}$ for some $t \in \mathbb{Z}$. Therefore in this case if $\gamma = a^{r/p}\gamma_1$, where $r \in \mathbb{Z}$ and $[\gamma_1] \in J_1$, we see that $[\gamma] \in \tilde{J}$ and if γ cannot be written in this form, we replace γ by a suitable $a^{t/p}\gamma$, and we use Lemma 1(b) to conclude that $(M_{a^{t/p}\gamma})^G \subset N(J)$. Thus using Lemma 1 we have reduced our investigation to the case when $[b] \in N(J)$.

We may write $[b] = \sum_{\mathcal{I}} c_x[x]$ with $c_x \in \mathbb{F}_p$ and almost all $c_x = 0$. Now for each $[x]$, $M(x) = M_\omega$ for some $\omega \in K^\times$ with $N([\omega]) = [x]$. For each $[x]$, set $\gamma(x) = \omega^{(\sigma-1)^{p-i-1}}$, so that $[\gamma(x)] \in J_{i+1}$ and $[\gamma(x)]^{(\sigma-1)^i} = [x]$. Now let $[\Gamma] = \sum_{\mathcal{I}} c_x[\gamma(x)]$. The application of $(\sigma-1)^i$ to $[\Gamma]$ results in $\sum_{\mathcal{I}} c_x[x] = [b]$. Hence $[\gamma/\Gamma]$ lies in the kernel of $(\sigma-1)^i$, and $[\gamma/\Gamma] \in J_i \subset \tilde{J}$ by induction. Since $[\Gamma] \in \tilde{J}$, $[\gamma] \in \tilde{J}$. ∎

The proof of Theorem 2 below follows the previous proof with some modifications. Since in the case of $p = 2$ the length of the socle series of J is at most 2, the proof is simpler. Moreover, we make use of the well-known fact on elements of identical norm in quadratic extensions:

If $K = F(\sqrt{a}), a \in F^\times \setminus F^{\times 2}, \gamma_1, \gamma_2 \in K^\times$ and $N(\gamma_1) = N(\gamma_2)$ then $[\gamma_1] \in \epsilon(F^\times)[\gamma_2]$. Indeed by Hilbert's Theorem 90 we have $[\gamma_1] = [N(k)][\gamma_2]$ for some $k \in K^\times$. (See [L, page 202].)

Proof of Theorem 2: If $-1 \in N(K^\times)$, then we set $X = \langle[\delta]\rangle \subset J_1$ with δ such that $\delta^{\sigma-1} = \beta^2$ and $N(\beta) = -1$ (observe that then $[N(\delta)] = [a] \in F^\times/F^{\times 2}$). If $-1 \notin N(K^\times)$ then we set $X = \{0\}$.

Choose $\mathcal{I}$ to be an $\mathbb{F}_2$-basis of $N(J)$. For each $[x] \in \mathcal{I}$ choose a representative $x \in F^\times$ of $[x]$ and $\omega \in K^\times$ such that $x = N(\omega)$. Then set $M(x) = M_\omega$ and let Y be the submodule of J generated by all $M(x), x \in \mathcal{I}$. The same argument as in the proof of Theorem 1 shows that Y is a free $\mathbb{F}_2[G]$-submodule of J, and that $Y \cong \bigoplus M(x)$. Finally, let Z be any complement in $\epsilon(F^\times)$ of the $\mathbb{F}_2$-module $N(J)$. As before we check that X, Y and Z are independent, Z is a trivial $\mathbb{F}_2[G]$-module, and we let $\tilde{J} \cong X \oplus Y \oplus Z$ be the $\mathbb{F}_2[G]$-submodule of J generated by X, Y and Z.

Assume now that $[\gamma] \in J_1$. Then $N(\gamma) \in F^\times \cap K^{\times 2} = F^{\times 2} \cup aF^{\times 2}$. If $N(\gamma) \in F^{\times 2}$ then $[\gamma] \in \epsilon(F^\times) \subset \tilde{J}$. If $N(\gamma) \in aF^{\times 2}$ then $[\gamma] \in [\delta]\epsilon(F^\times) \subset \tilde{J}$. Thus $J_1 \subset \tilde{J}$. Now suppose that $[\gamma] \in J\backslash J_1$. Let $\lambda = \gamma^{\sigma-1}$ and, since $\sigma-1 = \sigma+1$ in $\mathbb{F}_2[G]$, we see that $[\lambda] = [N(\gamma)] \neq [1]$. Hence for a suitable $\Gamma \in Y$ we have $[\gamma/\Gamma] \subset J_1$. Therefore $\tilde{J} = J$ as required. ▮

Proof of Theorem 3: We shall first show that if $3 \leq i \leq p-1$ then $\mathfrak{K}_i = \emptyset$. Suppose that this is not true and that there exists $M_{i,k} = M, 3 \leq i \leq (p-1), k \in \mathfrak{K}_i$, appearing as a summand in our decomposition of J.

Let m be a generator of M. Using the decomposition $J = X \oplus Y \oplus Z$ described in Theorem 1, we can write $m = u + v$, where $u \in Y$ and $v \in X \oplus Z$. Using the fact that $v \in J_2$ and $3 \leq i$ we see that we can find an element $n \in M \setminus \{0\}$ and $y \in Y \setminus Y \cap J_{p-1}$ such that $n = (\sigma-1)^k y$ for a suitable $k \in \mathbb{N}$.

Now write $y = \sum_{s=1}^t m_s$ where $m_s \in M_{a,j}, 1 \leq a \leq p$ and $j \in \mathfrak{K}_a$. Of course we assume that we choose at most one element from each $M_{a,j}$. Then from the equality $n = \sum_{s=1}^t (\sigma-1)^k m_s$ we see that we may assume that $n = (\sigma-1)^k m_1$ and $(\sigma-1)^k m_s = 0$ for $s \in \{2, \ldots, t\}$. Further, from our equalities $y = \sum_{s=1}^t m_s, (\sigma-1)^k m_s = 0$ for $s \in \{2, \ldots, t\}$ and $y \in J_p \setminus J_{p-1}$ we see that $m_1 \in J_p \setminus J_{p-1}$. But this implies that M is a free summand of J — a contradiction. Hence if $3 \leq i \leq p-1$ then $\mathfrak{K}_i = \emptyset$ as we claimed.

Now we consider the case of $i = p$. Since $N(J) = \bigoplus_{j \in \mathfrak{K}_p} N(M_{p,j})$ and each $N(M_{p,j})$ is a 1-dimensional $\mathbb{F}_p$-module, we see that $|\mathfrak{K}_p| = \dim_{\mathbb{F}_p} N(J)$.

Let us now consider the case of $i = 2$ and $p > 2$. We have

$$|\mathfrak{K}_2| = \dim_{\mathbb{F}_p}(((\sigma-1)J)^G/N(J)).$$

Therefore we see that $|\mathfrak{K}_2|$ is an invariant of J which does not depend upon any particular choice of the decomposition of J into a sum of cyclic submodules of

J. Therefore in order to determine $|\mathfrak{K}_2|$ we may use our decomposition $J = X \oplus Y \oplus Z$, where X, Y and Z are each thought of as a sum of their cyclic submodules. Thus in the case of $p > 2$, from Theorem 1 we conclude that $|\mathfrak{K}_2| = 1 - \Upsilon(K)$.

Finally, observe that if $p > 2$ then $|\mathfrak{K}_1| + |\mathfrak{K}_2| = \dim_{\mathbb{F}_p} J_1/N(J)$, and if $p = 2$ then $|\mathfrak{K}_1| = \dim_{\mathbb{F}_2} J_1/N(J)$. Applying Lemma 2 and observing that if $p > 2$ then $a \in N(K^\times)$ and if $p = 2$ then $a \in N(K^\times)$ if and only if $-1 \in N(K^\times)$, we obtain

$$1 + |\mathfrak{K}_1| = \dim_{\mathbb{F}_p}(F^\times/N(K^\times)) + 2\Upsilon(K). \quad \blacksquare$$

Proof of Corollary 1:

(1) From Theorem 3 we see that if $p > 2$ then J is a free $\mathbb{F}_p[G]$-module if and only if $\mathfrak{K}_1 = \emptyset = \mathfrak{K}_2$, and if $p = 2$ then J is a free $\mathbb{F}_p[G]$-module if and only if $|\mathfrak{K}_1| = \emptyset$. Therefore, if J is a free $\mathbb{F}_p[G]$-module, $p = 2$ and $-1 \notin N(K^\times)$. Moreover, assuming $p = 2, -1 \notin N(K^\times)$ we see that $\mathfrak{K}_1 = \emptyset$ if and only if $F^\times = N(K^\times) \cup -N(K^\times)$.

(2) J contains no free direct summand precisely when $N(J)$ is trivial. If $p > 2$ then $N(J)$ is trivial precisely when a is p-rigid. Suppose now that $p = 2$. Then we see that $N(J)$ is trivial if and only if $N(K^\times)/F^{\times 2} \subset \langle [a] \rangle \subset F^\times/F^{\times 2}$. Since $[-a] \in N(J)$ we see that in this case $\sqrt{-1} \in K^\times$.

(3) Suppose first that $p > 2$. If J is G-invariant then J contains no free direct summand. Hence a is p-rigid. If a is p-rigid then $N(J)$ is trivial, and J is G-invariant if additionally $\xi_p \in N(K^\times)$. By the definition of p-rigidity, $[\xi_p] \in \langle [a] \rangle$ in $F^\times/F^{\times p}$, which is equivalent with $\xi_{p^2} \in K^\times$. Now if $p = 2$ then J is G-invariant precisely when J contains no free direct summand. $\blacksquare$

Proof of Corollary 2: Suppose first that our three conditions mentioned in this corollary are valid. Then we see that if we use Theorem 1 and its proof, we can write $T_i = K_i^\times/K_i^{\times p}$ and $T_i = X_i \oplus Y_i \oplus Z_i, i = 1, 2$, where modules X_i, Y_i and Z_i are described in Theorem 1 and its proof.

From condition (1) of our corollary we see that $X_1 \cong X_2$, from condition (2) we see that $Y_1 \cong Y_2$, and finally with condition (3) together with our choice of Z_i as an $\mathbb{F}_p$-complement of the $\mathbb{F}_p$-submodule of T_i generated by $X_i \cap \epsilon(F_i^\times)$ and $N(T_i)$ in $\epsilon(F_i^\times)$ we see that $Z_1 \cong Z_2$. Hence if conditions (1), (2) and (3) are valid, then $T_1 \cong T_2$.

Now assume that $T_1 = X_1 \oplus Y_1 + Z_1$ where submodules X_1, Y_1, Z_1 of T_1 are constructed as in the proof of Theorem 1 and ψ is an $\mathbb{F}_p[G]$-isomorphism $T_1 \longrightarrow T_2$. Set $X_2 = \psi(X_1), Y_2 = \psi(Y_1)$ and $Z_2 = \psi(Z_1)$. Then

$$T_2 = X_2 \oplus Y_2 \oplus Z_2.$$

We also see that $N(T_2) = N(Y_2) \cong N(Y_1) = N(T_1)$. Therefore we have $\dim_{\mathbb{F}_p} N(K_1^\times)/F_1^{\times p} = \dim_{\mathbb{F}_p} N(K_2^\times)/F_2^{\times p}$.

We shall now assume that X_1, Y_1 and Z_1 are decomposed into their cyclic summands, and we shall apply Theorem 3.

We obtain $\xi_p \in N(K_1^\times) \Leftrightarrow \mathfrak{K}_2 = \emptyset \Leftrightarrow \xi_p \in N(K_2^\times)$. Finally, from Theorem 3 we see that $\dim_{\mathbb{F}_p}(F_1^\times/N(K_1^\times)) = \dim_{\mathbb{F}_p}(F_2^\times/N(K_2^\times))$ as required. ∎

Finally we shall prove Corollary 3. Observe that this proof is a straightforward corollary of Theorem 3. We write $\mathfrak{K}_{2,1}$ for the index set $\mathfrak{K}_2$ used in Theorem 3 when applied to the field extension K_1/F_1. Similarly we extend this notation for other index sets under consideration.

Proof of Corollary 3: From Theorem 3 we see that $T_1 \cong T_2$ if and only if $|\mathfrak{K}_{1,1}| = |\mathfrak{K}_{1,2}|$ and $|\mathfrak{K}_{2,1}| = |\mathfrak{K}_{2,2}|$. Rewriting these equalities we obtain $T_1 \cong T_2$ if and only if we have the following two equalities:

(1) $2\Upsilon(K_1) + \dim_{\mathbb{F}_2} F_1^\times/N(K_1^\times) = 2\Upsilon(K_2) + \dim_{\mathbb{F}_2} F_2^\times/N(K_2^\times)$,

(2) $\Upsilon(K_2) + \dim_{\mathbb{F}_2} N(K_1^\times)/F_1^{\times 2} = \Upsilon(K_1) + \dim_{\mathbb{F}_2} N(K_2^\times)/F_2^{\times 2}$. ∎

ACKNOWLEDGEMENT: We gratefully acknowledge the support of the Mathematical Sciences Research Institute in Berkeley, California, where during the fall of 1999 the authors met, for our subsequent discussions led to the results in this paper. The first author is also very appreciative of the stimulating discussions with Adrian Wadsworth, and both authors thank the referee for encouragement and for a helpful suggestion concerning the exposition.

References

[A-T] E. Artin and J. Tate, *Class Field Theory*, Second printing, Addison-Wesley, Redwood City, CA, 1974.

[Bo] Z. I. Borevič, *The multiplicative group of cyclic p-extensions of a local field*, Trudy Matematicheskogo Institut imeni V. A. Steklova **80** (1965), 16–29.

[C] J. F. Carlson, *Modules and Group Algebras*, Notes by R. Suter, Lectures in Mathematics, ETH Zürich, Birkhäuser Verlag, Basel, 1996.

[Fac] A. Facchini, *Module Theory (Endomorphism Rings and Direct Sum Decompositions in Some Classes of Modules)*, Progress in Mathematics **167**, Birkhäuser Verlag, Basel, 1998.

[Fad] D. K. Faddeev, *On the structure of the reduced multiplicative group of a cyclic extension of a local field*, Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya **24** (1960), 145–152.

[L] T.-Y. Lam, *The Algebraic Theory of Quadratic Forms*, Second Printing, Benjamin Cummings, Massachusetts, 1980.

[Ma] R. Massy, *Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p*, Journal of Algebra **109** (1987), 508–535.

[Ma-Ng] R. Massy and T. Nguyen-Quang-Do, *Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3: étude locale-globale*, Journal für die reine und angewandte Mathematik **291** (1977), 149–161.

[Mi] H. Miki, *On the imbedding problem of local fields*, Journal of the Faculty of Science of the University of Tokyo, Section IA. Mathematics **23** (1976), 369–381.

[P] R. J. Pierce, *Associative Algebras*, Graduate Texts in Mathematics **88**, Springer-Verlag, Berlin, 1982.

[S] J.-P. Serre, *Galois Cohomology*, Springer-Verlag, Berlin, 1997. English translation of the original edition, *Cohomologie Galoisienne*.

[V] V. Voevodsky, *On 2-torsion in motivic cohomology*, http://www.math.uiuc.edu/K-theory/0502/index.html, 2001.

[War] R. Ware, *Galois groups of maximal p-extensions*, Transactions of the American Mathematical Society **333** (1992), 721–728.

[Wat] W. C. Waterhouse, *The normal closures of certain Kummer extensions*, Canadian Mathematical Bulletin **37** (1994), 133–139.