ON IRREDUCIBLE TAME REPRESENTATIONS OF THE ABSOLUTE GALOIS EXTENSION OF A LOCAL FIELD K AND SYMPLECTIC-TYPE EXTENSIONS OF K

BY

MOSHE JARDEN AND JÜRGEN RITTER

Introduction

The absolute tame Galois group $G(K)$ of a local p-adic number field K is well known: it is generated by two elements σ, τ subject to the relation $\sigma\tau\sigma^{-1} = \tau^q$, where q is the number of elements of the residue field of K. One is also familiar with the finite-dimensional complex representation theory of such metabelian profinite groups: possibly the best general information is that each irreducible representation ρ turns up as the induced representation of an abelian character of some maximal abelian normal subgroup H of $G = G(K)/\ker \rho$. The aim of our paper is to bring the two things together in an explicit way, and we succeed in doing this very nicely when restricting ourselves to the case of irreducible representations of small degree. To be precise, we only consider irreducible representations of a degree n that divide $q - 1$; equivalently we may say that ζ_n (which is a primitive *n-th* root of unity) belongs to K and that n is relatively prime to the residue characteristic of K. This second formulation somehow reminds of the assumption made in the so-called Kummer theory. And indeed, in a way similar to it, one can here establish a correspondence between certain tame Galois extensions N/K on one side and the irreducible representations of degree n of $G(K)$ on the other side. These N/K show up as the fixed fields of the kernels of our representations; their Galois groups are of an "n-symplectic" type, which means, firstly, that the centers are cyclic, and secondly, that the groups are non-abelian extensions herefrom by a group of type $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$; especially they are nilpotent groups. In Section II.2 of our paper we describe all tame normal extensions N/K having a Galois group G of this n-symplectic type. Now, if ρ is a faithful irreducible representation of G of degree n, then it is induced by an abelian character λ of a maximal abelian normal subgroup H, and we are interested in the intermediate fields within N/K that belong to H and to the kernel of λ. Obviously, even if ρ is fixed, there are several possibilities for H and λ. But we can show that, up to K-isomorphism, the fixed field of $\ker \lambda$ is fully determined by ρ and by the order of λ. We also derive a special choice

Received January 13, 1981.

of H and λ implying that G is metacyclic. All this is done in Chapter II. In the first chapter we put together some auxiliary results.

I. Vocabulary and Auxiliary Results

I.1. Symplectic modules. Our first section is concerned with free R-modules V of a finite rank m, where $R = \mathbf{Z}/n\mathbf{Z}$ and n is some integer greater than or equal to 2. We call V a *symplectic module* if it is equipped with a bilinear form $(\ ,\ ): V^2 \to R$ such that $(v, v) = 0$ for every $v \in V$.

A system $\{u_1, u_2, \ldots, u_k\}$ of elements of V is said to be *symplectic* if k is even, if $(u_{2i-1}, u_{2i}) = 1$ for $1 \leqslant i \leqslant k/2$, and if $(u_i, u_j) = 0$ for all other pairs. Obviously $\{u_1, u_2, \ldots, u_k\}$ is then linearly independent. If $k = m$, $\{u_1, \ldots, u_m\}$ is a free set of generators for V over R and we then speak of a *symplectic basis*. We should also like to recall here the following two common definitions:

(1) A submodule U of V is *isotropic* if $(u, u') = 0$ for all $u, u' \in U$.

(2) V is *non-degenerate* if to each $0 \neq v \in V$ one finds a $v' \in V$ with $(v, v') \neq 0$.

There is no problem in proving the following fact:

LEMMA I.1.1. *Let V be a non-degenerate symplectic module of rank m over $R = \mathbf{Z}/n\mathbf{Z}$.*

(a) *For every $u \in V$ there exists $v \in V$ such that the order of (u, v) in R coincides with the order of u in V.*

(b) *Every symplectic system $\{u_1, \ldots, u_k\}$ in V can be extended to a symplectic basis; in particular, V has a symplectic basis and m is even.*

(c) *$|U|^2 = |V|$ holds for every maximal isotropic submodule U.*

I.2. Sympletic-type groups.

LEMMA AND DEFINITION I.2.1. *Let G be a finite non-abelian group and let m, n be positive integers such that*

(a) *the center $Z = Z(G)$ is cyclic and*

(b) *the quotient group $V = G/Z$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^m$.*

We then call G a symplectic-type group with invariants m and n.
The following hold for G:

(1) *The commutator subgroup G' is contained in Z and has the order n. In particular, G is nilpotent.*

(2) *Every generator z of G' gives rise to a non-degenerate symplectic $\mathbf{Z}/n\mathbf{Z}$-structure on V via*

$$(*) \qquad [x, y] = z^{(\bar{x}, \bar{y})}, \quad x, y \in G;$$

here $\bar{x}$ is the image of x under the canonical map $G \to V$.

(3) *$n \geq 2$, m is even, and V has a symplectic basis over $\mathbf{Z}/n\mathbf{Z}$ with respect to* (*).

(4) *If A is a maximal abelian subgroup in G, then $Z \subset A$, $A \lhd G$, and $|A| = |Z| \cdot n^{m/2}$.*

Proof. The assumption that $V = G/Z$ is abelian implies that $G' \subset Z$. It follows that G' is cyclic and that $[ab, c] = [a, c][b, c]$. Hence $1 = [a^n, b] = [a, b]^n$, and so the order of G' divides n. On the other hand, choose an element $x \in G$ with ord $\bar{x} = n$. If l is a prime divisor of n, and if $l \neq n$, then $x^{n/l} \notin Z$ and therefore there exists a $y \in G$ such that $[x, y]^{n/l} = [x^{n/l}, y] \neq 1$. We may conclude that $|G'| = n$. For a generator z of G' now look at (*). The map $(\ ,\ ): V^2 \to \mathbf{Z}/n\mathbf{Z}$ defined in this way is bilinear, symplectic and non-degenerate. By Lemma I.1.1, B has a symplectic basis and m is even. Every maximal abelian subgroup A must contain Z and therefore also G'. It follows that A is normal and that $\bar{A} = A/Z$ is a maximal isotropic submodule of V, so apply Lemma I.1.1 (c). ∎

Remark. From the nilpotency of G one easily deduces that G is the direct product of a cyclic group Z_0 which is contained in Z and has order prime to n, and a symplectic-type group G_0 having the same invariants m, n as G and the additional property that each prime dividing $|G_0|$ also divides n.

I.3. Induced faithful irreducible representations. In this section we are mainly concerned with complex irreducible representations of finite monomial groups G. These are groups every irreducible representation of which is induced from an abelian character of a subgroup. Examples are the meta-abelian and nilpotent groups, which show up in the next section (cf. Huppert [4, Chapter V, Section 18]). We collect some known facts from representation theory and refer for the proofs to [8, Sections 2 and 3] (the assumption made there, namely that G is a p-group, can be replaced by G being monomial without changing the corresponding arguments).

I.3.1 (A). If the irreducible representation $\rho = \mathrm{ind}_H^G \lambda$ is induced from an abelian character λ of a normal subgroup H of G, then

$$\mathrm{Ker}\ \rho = \bigcap_{x \in G} (\mathrm{Ker}\ \lambda)^x.$$

In particular, ρ is faithful if and only if the trivial group 1 is the only subgroup of Ker λ which is normal in G.

I.3.1 (B). Let G be a finite monomial group having a faithful irreducible representation ρ.

(a) If A is a maximal normal abelian subgroup of G that contains G', then $(G:A) = \dim \rho$ and ρ is induced from an abelian character of A.

(b) All the faithful irreducible representations of G have the same dimension.

I.3.1 (C). A necessary and sufficient condition for a finite nilpotent group G to possess a faithful irreducible representation is that $Z(G)$ is cyclic.

Combining Lemma I.2.1 and I.3.1 we have:

COROLLARY I.3.2. *A symplectic-type group G with invariants m, n has a faithful irreducible representation of dimension n.*

For the purpose of later applications we also state the following two lemmas.

LEMMA I.3.3. *Let $T \leq A \leq G$ be finite groups satisfying:*

(a) *The subgroup A is maximal normal abelian and G/A is abelian of order n.*
(b) *The subgroup T is normal in A and A/T is cyclic.*
(c) *The only normal subgroup of G which is contained in T is 1.*

If λ is an abelian character of A such that Ker $\lambda = T$, *then $\rho = \mathrm{ind}_A^G\lambda$ is a faithful irreducible representation of dimension n.*

Proof. We apply Mackey's criterium and show that if an element $x \in G$ satisfies $\lambda^x = \lambda$, then $x \in A$.

Indeed, if $t \in T$, then $\lambda(t^x) = \lambda(t)$, hence $t^x \in T$ and $x \in N_G(T)$. In particular, T is a normal subgroup of $A_1 = \langle A, x\rangle$. The factor group A_1/T is abelian. Namely A is Abelian and for every $a \in A$ we have $\lambda(a^x) = \lambda(a)$, hence $[a, x] \in T$. It follows that $A_1' \leq T$. But, as G/A is abelian, A_1 is normal in G and thus also $A_1' \lhd G$, so $A_1' = 1$. Using the maximality of A, we deduce that $A_1 = A$ and $x \in A$. ∎

LEMMA I.3.4. *Let $A \lhd G$ be finite groups and suppose that A has an abelian character λ such that $\rho = \mathrm{ind}_A^G\lambda$ is a faithful irreducible representation of G.*

(a) *The group A is maximal abelian.*
(b) *The index $(A\colon \mathrm{Ker}\ \lambda)$ is equal to the exponent of A.*
(c) *If h is a generator of A modulo* Ker λ, *then $A = \langle h\rangle \times \mathrm{Ker}\ \lambda$.*

Proof. (a) The group A is abelian, since A' is a normal subgroup of G which is contained in $T = \mathrm{Ker}\ \lambda$, and hence $A' = 1$.

If A_1 is an abelian subgroup that contains A and if $x \in A_1$, then $\tau^x = \tau$. By Mackey's criterion $x \in A$ and therefore $A_1 = A$.

(b) Let $e = (A:T)$ and let h be a generator of H modulo T. Then $\exp(A)$

$\geqslant$ ord $h \geqslant e$. On the other hand A^e is a normal subgroup of G which is contained in T hence $A^e = 1$. ■

II. Tame Field Extensions and Representation Theory

Let K be a finite extension of $\mathbf{Q}_p$. We consider a finite Galois extension N of K and suppose that $G = \mathcal{G}(N/K)$ is a symplectic-type group with invariants m, n, where n is prime to p. If M is the fixed field of $Z(G)$ in N, then $\mathcal{G}(M/K) \cong (\mathbf{Z}/n\mathbf{Z})^m$ and $m \geqslant 2$ is even. In particular, M contains a cyclic totally ramified extension L of K of degree n. It follows that a primitive *n-th* root, ζ_n, of unity belongs to K and moreover, that M is the maximal abelian extension of K of exponent n. Hence $m = 2$. By Lemma I.2.1, G' is a cyclic group and every generator z of G' defines a non-degenerate symplectic structure on $\mathcal{G}(M/K)$ by the formula

$$[x, y] = z^{(\bar{x},\bar{y})}, \quad x, y \in G.$$

We say that N/K is an *n-symplectic type extension.*

On the other hand the *n-th* norm residue symbol defines a non-degenerate bilinear form on $K^\times/K^{\times n}$. If $\zeta_{2n} \in K$, then every element of $K^\times/K^{\times n}$ is perpendicular to itself with respect to this form (cf. Serre [9, p. 217]) and therefore $K^\times/K^{\times n}$ becomes a non-degenerate symplectic module in the sense of Section I.1. The local reciprocity isomorphism $K^\times/K^{\times n} \cong \mathcal{G}(M/K)$ transfers the symplectic structure from $K^\times/K^{\times n}$ to $\mathcal{G}(M/K)$. The fact that the rank of $\mathcal{G}(M/K)$ is 2 implies that it is possible to choose the generator of G' such that the two symplectic structures on $\mathcal{G}(M/K)$ coincide.

II.1. Tamely ramified extension. Look at our finite extension K of $\mathbf{Q}_p$ and fix a prime element π of K. Let N be a finite tamely ramified extension of K. Denote by f and e the residue degree and the ramification index of N/K, respectively; denote also $s = q^f - 1$ where q is the order of the residue field $\overline{K}$ of K. Then $U = K(\zeta_s)$ is the maximal unramified extension of K in N and there exists a unit u of U such that $N = U(\pi u)^{1/e}$ (cf. Lang [6, p. 52]). As every one-unit of N is an *e-th* power, the unit u can be taken as $u = \zeta_s^i$, where $0 \leqslant i \leqslant e$. Therefore

$$\begin{array}{l} N = U((\pi u)^{1/e}) \\ e \,\| \\ U = K(\zeta_s) \\ f \,\# \\ K \end{array}$$

where the symbol $=$ means totally ramified and $\#$ means unramified.

LEMMA II.1.1. *Continue with the above assumptions.*

(a) *The extension N/U is normal (hence cyclic) if and only if $e \mid q^f - 1$.*

(b) *The extension N/K is normal if and only if $e \mid q^f - 1$ and $e \mid i(q - 1)$.*

In this case $\mathcal{G}(N/K)$ *is generated by two elements* σ, τ *with the defining relations* $\sigma^f = \tau^i$, $\tau^e = 1$ *and* $\sigma\tau\sigma^{-1} = \tau^q$.

Moreover, $\mathrm{Res}_U\sigma$ *is the Frobenius automorphism of* U/K *and* $\langle\tau\rangle = \mathcal{G}(N/U)$.

(c) *The extension* M/K *is abelian if and only if* $e \mid (q - 1)$.

In this case the exponent of $\mathcal{G}(N/K)$ *is given by*

$$\exp \mathcal{G}(N/K) = \mathrm{lcm}\left(e, \frac{fe}{\gcd(i, e)}\right) \tag{1}$$

(d) *The extension* N/K *is cyclic if and only if* $e \mid q - 1$ *and* $\gcd(i, e, f) = 1$.

Proof. In order to see (b) and (c) we assume the extension N/U to be normal and prove first that N/K normal is equivalent to $e \mid i(q - 1)$. So suppose that N/K is normal. Let $\alpha = (\pi\zeta_s^i)^{1/e}$ and let σ be any extension of the Frobenius automorphism of U/K to N. Then $U(\alpha) = U(\sigma\alpha)$. Hence there exists an integer k which is prime to e, and an element $\gamma \in U$ such that $\alpha^e = (\sigma\alpha)^{ek}\gamma^e$ (cf. Birch [1, p. 90]). Thus

$$\pi\zeta_s^i = \pi^k\zeta_s^{iqk}\gamma^e. \tag{2}$$

Taking the U-values of both sides of (2), we find that $k \equiv 1 \bmod e$. Hence, by modifying γ by a power of π, we may take $k = 1$ and arrive at $\zeta_s^{i(q-1)} = \gamma^e$. Since ζ_s is a generator of the cyclic group of roots of unity in K having order prime to p, and since $e \mid s$, we get $e \mid i(q - 1)$. Reversing the arguments, one obtains the other direction of the implication.

The generators σ and τ of $\mathcal{G}(N/K)$ are given by

$$\sigma\zeta_s = \zeta_s^q, \quad \sigma(\pi\zeta_s^i)^{1/e} = \zeta_s^{i(q-1)/e}(\pi\zeta_s^i)^{1/e},$$

$$\tau\zeta_s = \zeta_s, \quad \tau(\pi\zeta_s^i)^{1/e} = \zeta_s^{s/e}\zeta_s^{i/e}$$

(cf. Hasse [2, Chapter 16] or Koch [5, Section 5]) and they obey the generating relations mentioned above. From them we also get the first part of (c). Moreover $\mathrm{ord}\ \mathrm{Res}_u\sigma = f$. Hence $f \mid \mathrm{ord}\ \sigma$, which together with $\sigma^f = \tau^i$ implies

$$\frac{\mathrm{ord}\ \sigma}{\gcd(\mathrm{ord}\ \sigma, f)} = \frac{\mathrm{ord}\ \tau}{\gcd(\mathrm{ord}\ \tau, i)}$$

Thus $\mathrm{ord}\ \sigma = ef \cdot \gcd(e, i)^{-1}$, and, if N/K is abelian, then

$$\exp \mathcal{G}(N/K) = \mathrm{lcm}(\mathrm{ord}\ \tau, \mathrm{ord}\ \sigma) = \mathrm{lcm}(e, ef \cdot \gcd(e, i)^{-1}).$$

For (d), first suppose that $e \mid q - 1$ and that $\gcd(i, e, f) = 1$. By (c) N/K is abelian.

Claim. There exist integers x, y, z such that $xe + yf + zi = 1$ and $\gcd(z, f) = 1$.

Indeed, let $d = \gcd(e, f)$. Then $\gcd(i, d) = 1$ and hence there exists a

z such that $zi \equiv 1 \bmod d$. The number z is relatively prime to d. Hence, by replacing z if necessary by a number of the form $z + kd$, we can assume that $\gcd(z, f) = 1$ (e.g., use Exercise 4 on p. 36 of LeVeque [7]). There exists now an x such that $xe \equiv 1 - zi \bmod f$, since $\gcd(e, f) \mid 1 - zi$. Hence there exists a y such that $xe = 1 - zi - yf$, and our claim is true.

It follows from the choice of z that

$$\operatorname{ord} \operatorname{Res}_U \sigma^z \tau^y = \operatorname{ord}(\operatorname{Res}_U \sigma)^z = \operatorname{ord} \operatorname{Res}_U \sigma = f.$$

Thus $f \mid \operatorname{ord} \sigma^z \tau^y$ and, as $(\sigma^z \tau^y)^f = \tau^{zi+yf} = \tau$, we have $\operatorname{ord} \sigma^z \tau^y = ef = [N:K]$.

Conversely, suppose that N/K is a cyclic extension, so there exist z, y such that $\operatorname{ord} \sigma^z \tau^y = ef$. Then

$$\operatorname{ord} \tau^{zi+yf} = \operatorname{ord}(\sigma^z \tau^y)^f = e.$$

As $e \mid q - 1$, $\gcd(zi + yf, e) = 1$, and consequently $\gcd(i, f, e) = 1$. ∎

We conclude this section by adding the following elementary divisibility properties.

LEMMA II.1.2. *Let $a \neq 1$ be an integer and let l be a prime such that $a \equiv 1 \bmod l$.*

(a) *If $l \nmid m$ then $v_l(a^m - 1) = v_l(a - 1)$.*
Here, for a natural number n, we take $v_l(n) = i$ if $l^i \mid n$ but $l^{i+1} \nmid n$.
(b) *Assuming $a \equiv 1 \bmod 4$ if $l = 2$, we have, for every $n \in \mathbf{N}$,*

$$v_l(a^n - 1) = v_l(a - 1) + v_l(n)$$

(c) *If $a \equiv 1 \bmod r$ and every prime divisor of n divides r, then $a^n \equiv 1 \bmod 4r$.*

Proof. *If $l \nmid m$, then $(a^m - 1)/(a - 1) = a^{m-1} + a^{m-2} + \cdots + 1 \equiv m \not\equiv 0 \bmod l$.* It follows from (a) and an easy induction argument that it suffices to only prove (b) for $n = 1$, and here it is a consequence of Newton's binomial formula (cf. [7, p. 50]). Assertion (c) can be proved by induction on the number of the (not necessarily distinct) prime divisors of n. ∎

II.2. The classification of symplectic-type extensions. In addition to the earlier notation we now introduce the abbreviation $N_{n,f,e,j}$ for the tame extension $U_f((\pi\zeta_s^{jn})^{1/e})$ of K; here f, e, j and $n \geq 2$ are integers, e and n both prime to p, $s = q^f - 1$, and $U_f = K(\zeta_s)$. Thus e is its ramification index and f its residue degree.

THEOREM A. *A finite tamely ramified extension N of K is of an n-symplectic type if and only if $N = N_{n,f,e,j}$ and the following conditions are*

satisfied:

(1) $n \mid q - 1$;
(2) $n \mid f$;
(3) $n \mid e$;
(4) $\dfrac{e}{n} \Big| q - 1$
(5) $\gcd\left(n, \dfrac{q-1}{e/n}\right) = 1$;
(6) $\gcd\left(j, \dfrac{e}{n}, \dfrac{f}{n}\right) = 1$.

Proof. Suppose first that N/K is an n-symplectic type Galois extension. By what we have said at the beginning of this chapter, N contains the maximal abelian extension $M = U_n(\pi_n)$ of K of exponent n, where $\pi_n = \pi^{1/n}$. Also $\zeta_n \in K$, and thus $n \mid q - 1$. Now $n = f(M/K)$ divides $f = f(N/K)$ and U_f is the maximal unramified extension of K in N. It follows from Section II.1 that $N = U_f((\pi\zeta_s^i)^{1/e})$, where $s = q^f - 1$.

We observe now that $K(\pi_n)$ and U_f are linearly disjoint over K. Hence $[U_f(\pi_n): U_f] = n$, which means that $e = nr$, where $r = [N: U_f(\pi_n)]$ divides the order of the center $Z = \mathcal{G}(N/M)$ of $G = \mathcal{G}(N/K)$.

The extension $N/K(\pi_n)$ is abelian, since its Galois group has the center Z as a subgroup with a cyclic factor $\mathcal{G}(M/K(\pi_n))$. The ramification degree of $N/K(\pi_n)$ is r, thus $r \mid q - 1$.

By Lemma I.2.1, $\mathcal{G}(N/K(\pi_n))$ is maximal abelian. Hence, if l is a prime divisor of n, then $N/K(\pi_{n/l})$ is a non-abelian extension with lr as its ramification index. It follows that $lr \nmid q - 1$, so $\gcd(n, (q-1)/r) = 1$.

From the fact that N/K is normal we deduce that $e \mid i(q - 1)$. Therefore $i = nj$ for some $j \in N$.

Finally we observe that the ramification index and the residue degree of the cyclic extension N/M are e/n and f/n, respectively. Writing N in the form $N = M(\zeta_s, (\pi_n\zeta_s^j)^{1/r})$, we deduce that $\gcd(j, e/n, f/n) = 1$.

Conversely, suppose that the positive integers n, f, e, j satisfy conditions (1)–(6). We prove that $N = N_{n,f,e,j}$ is a Galois extension of K of an n-symplectic type.

First note that if a prime l divides n, then it also divides $r = e/n$. Also, $q \equiv 1 \bmod r$. Hence $q^n \equiv 1 \bmod e$, by Lemma II.1.2, which implies that $e \mid q^f - 1$. In addition $e \mid n(q - 1)$, thus N/K is a Galois extension. Its Galois group G is non-abelian, since $e \nmid q - 1$. Condition (6) implies that N/M is a cyclic extension. We still have to prove that $\mathcal{G}(N/M) = Z(G)$: The group G has two generators with the defining relations

$$\sigma^f = \tau^{jn}, \qquad \tau^e = 1, \qquad \sigma\tau\sigma^{-1} = \tau^q. \tag{7}$$

Claim. $\mathcal{G}(N/M) = \langle \sigma^n, \tau^n \rangle$. Indeed, both σ^n and τ^n belong to $\mathcal{G}(N/M)$, since $\mathcal{G}(M/K)$ is an abelian extension of exponent n. Also, τ^n generates

$\mathcal{G}(N/U_f(\pi_n))$ and $Res_{U_f(\pi_n)}\sigma^n$ generates $\mathcal{G}(U_f(\pi_n)/M)$. Thus σ^n and τ^n generate $\mathcal{G}(N/M)$. Because of $q^n \equiv 1 \bmod e$ and (4), we now get $\sigma\tau^n\sigma^{-1} = \tau^{nq} = \tau^n$ and $\sigma^n\tau\sigma^{-n} = \tau^{q^n} = \tau$, and so both σ^n and τ^n, and therefore also $\mathcal{G}(N/M)$, are contained in $Z(G)$.

Next we observe that both extensions $N/K(\pi_n)$ and N/U_n are abelian, as $r \mid q - 1$ and $e \mid q^n - 1$. The maximal intermediate fields of $K(\pi_n)/K$ and U_n/K have the form $K(\pi_{n/l})$ and $U_{n/l}$, respectively, where l is a prime divisor of n. Condition (5) implies that $lr \nmid q - 1$. Also $e \nmid q^{n/l} - 1$. Indeed, by (5), if $e \mid q^{n/l} - 1$, then $n \left| \dfrac{q^{n/l} - 1}{q - 1} \right.$. If $l \neq 2$ or $l = 2$ and $q \equiv 1 \bmod 4$, we get a contradiction to Lemma II.1.2. Otherwise $l = 2$ and $v_2(q - 1) = 1$. But in this case also $v_2(n) = 1$, hence $n/2$ is odd and we have again reached a contradiction to Lemma II.1.2. It follows that $N/K(\pi_{n/l})$ and $N/U_{n/l}$ are not abelian extensions.

Combining the results of the last paragraph we have that $\mathcal{G}(N/K(\pi_n))$ and $\mathcal{G}(N/U_n)$ both are maximal abelian subgroups of G. Therefore

$$Z(G) \leqslant \mathcal{G}(N/K(\pi_n)) \cap \mathcal{G}(N/U_n) = \mathcal{G}(N/M),$$

as desired. ■

II.3. Irreducible tame representations. Denote by K_{tr} the maximal tamely ramified extension of K. Our intention is to study irreducible representations ρ of $\mathcal{G}(K_{tr}/K)$ of a "small" dimension n, where by "small" we mean that $n \mid q - 1$ or, equivalently, that $\zeta_n \in K$. It is well known that Ker ρ is an open subgroup of $\mathcal{G}(K_{tr}/K)$. The fixed field N of Ker ρ is therefore a finite normal tamely ramified extension of K, and ρ defines a faithful irreducible representation $\overline{\rho}$ of $\mathcal{G}(N/K)$.

THEOREM B. *Let N be a finite normal tamely ramified extension of K. Assume that every prime divisor of $e = e(N/K)$ divides $q - 1$. If $G = \mathcal{G}(N/K)$ has a faithful irreducible representation ρ of dimension n and $n \mid q - 1$ (and $4 \mid q - 1$ if n is even), then N/K is an n-symplectic type extension; in particular N/K is a nilpotent extension.*

Proof. We again write N in the form $N = U_f((\pi\zeta_s^i)^{1/e})$ and show that N has the form $N_{n,f,e,j}$ with n, f, e, j satisfying the conditions of Theorem A.

The subgroup $\mathcal{G}(N/U_f)$ is normal and cyclic, and $\mathcal{G}(U_f/K)$ is cyclic, so G is meta-cyclic and therefore monomial. Also $G' \leqslant \mathcal{G}(N/U_f)$ and thus, by I.3.1 (b), ρ is induced from an abelian character of a maximal abelian group A containing $\mathcal{G}(N/U_f)$; also $(G:A) = n$. In particular $n \mid f$ and the fixed field of A in N is U_n. This implies that $e \mid q^n - 1$ but $e \nmid q^{n/l} - 1$ for every prime divisor l of n. Thus for every prime divisor l of n there exists a prime l' such that

$$v_{l'}(e) > v_{l'}(q^{n/l} - 1).$$

However, if $l' \neq l$, then $v_{l'}(e) \leq v_{l'}(q^n - 1) = v_{l'}(q^{n/l} - 1)$, by II.1.2. Hence $l' = l$ and

$$v_l(e) \geq v_l(q^{n/l} - 1) + 1 \geq v_l(q - 1) + v_l(n).$$

On the other hand, again from II.1.2 we get

$$v_l(e) \leq v_l(q^n - 1) = v_l(q - 1) + v_l(n),$$

and so together, for every prime divisor l of n, $v_l(e) = v_l(q - 1) + v_l(n)$. In particular, n divides e; so let $r = e/n$. If $l \mid r$ but $l \nmid n$, then $l \mid q - 1$, by assumption, and

$$v_l(r) = v_l(e) \leq v_l(q^n - 1) = v_l(q - 1).$$

Therefore $r \mid q - 1$ and $\gcd(n, (q - 1)/r) = 1$. From N/K being normal we get $e \mid i(q - 1)$. Consequently $n \mid i$, and we write $j = i/n$. Now $\pi_n = (\pi)^{1/n} = \zeta_s^{-j}(\pi\zeta_s^i)^{r/e}$ belongs to N and $M = U_n(\pi_n)$ is contained in N. The group $G = \mathcal{G}(N/K)$ is generated by two elements σ, τ with the defining relations (7) of section II.2. As in the proof of Theorem A, one shows that $\mathcal{G}(N/M)$ is generated by σ^n and τ^n, and that both of them belong to $Z(G)$. Thus $\mathcal{G}(N/M)$ is a subgroup of $Z(G)$, which is cyclic, as G admits a faithful irreducible representation. It follows that N/M is a cyclic extension, which implies that $\gcd(j, r, f/n) = 1$. Thus, all the conditions of Theorem A are satisfied. ■

It should be mentioned that in the theorem one cannot give up either of the assumptions "$n \mid q - 1$", "$2 \mid n$ implies $4 \mid q - 1$", or "every prime divisor of e divides $q - 1$".

II.4. Induced structures. Consider a fixed extension $N = N_{n,f,e,j}$ of K of an n-symplectic type. In particular, the relations (1) to (6) of Theorem A are satisfied. They also imply:

(7) $l \mid e$ implies $l \mid q - 1$;
(8) $e \mid q^n - 1$;
(9) $e \mid q^f - 1$;
(10) $l \mid n$ implies $l \mid r$, and $v_l(r) = v_l(q - 1)$;
(11) $e \mid n(q - 1)$.

The group $G = \mathcal{G}(N/K)$ admits, by Corollary I.3.2, a faithful irreducible representation. In this section we consider intermediate fields $K \subseteq L \subseteq F \subseteq N$ and call the pair (L, F) an *induced structure for* N/K of *dimension* n if the subgroups $T = \mathcal{G}(N/F)$ and $A = \mathcal{G}(N/L)$ satisfy the conditions of Lemma I.3.3. In field theoretic terms this means:

(a) The extension L/K is abelian of order n; the extension N/L is abelian; and if $K \subseteq L_0 \subseteq L$, then N/L_0 is not abelian.
(b) The extension F/L is cyclic.
(c) The Galois hull of F/K is N.

By that lemma the group A has an abelian character λ with Ker $\lambda = T$ such that the induced representation to G is faithful and irreducible of dimension n.

Our aim is to give a description of all the induced structures (L, F) for N/K. Meanwhile, we start with the following clear result.

LEMMA II.4.1. *Every extension of K of degree n is abelian and is contained in N. There are $\sigma(n)$ (the sum of the divisors of N) of them and they are explicitly given as*

$$L_{d,k} = U_d(\pi_{d,k}) \text{ for } d \mid n \text{ and } k = 0, \ldots, n/d$$

where $\pi_{d,k} = (\pi\zeta_{q^d-1}^k)^{d/n}$ is a prime element of $L_{d,k}$.

LEMMA II.4.2. *The subgroups $\mathcal{G}(N/L_{d,k})$ of G are maximal abelian, and for each of them there exists a field F such that $(L_{d,k}, F)$ is an induced structure of dimension n for N/K.*

Proof. The ramification index of $N/L_{d,k}$ is

$$e(N/L_{d,k}) = e(N/K) \cdot e(L_{d,k}/K)^{-1} = dr,$$

and $q^d \equiv 1 \bmod dr$, as $q \equiv 1 \bmod r$. Hence $A = \mathcal{G}(N/L_{d,k})$ is an abelian normal subgroup of G of index n.

We know that G admits a faithful irreducible representation of dimension n. Also $G' \leq \mathcal{G}(N/M) \leq \mathcal{G}(N/L_{d,k})$. Hence by I.3.1 (B), A is a maximal abelian subgroup, ρ is induced from an abelian character λ of A. Denote by F the fixed field of Ker λ in N. Then $(L_{d,k}, F)$ is an induced structure of dimension n for N/K. ■

THEOREM C. *Let (L, F) be an induced structure of dimension n for N/K. Then N/F is an unramified extension and $[N:F]$ divides n. Precisely, if $L = L_{d,k}$, then*

$$[N:F] = \gcd\left(jd - \frac{kd}{n} \cdot \frac{q^f - 1}{q^d - 1}, dr, \frac{f}{d}\right).$$

Proof. Let $E = U_s \cap F$ be the maximal unramified extension of K which is contained in F. Then F is linearly disjoint from U_s over E. The extension U_s/K is normal, N/U_s is cyclic and $U_s \subseteq U_sF \subseteq N$. So U_sF is a normal extension of K. It follows that $U_sF = N$ and N/F is an unramified extension.

In order to prove the degree formula we write N in the form

$$N = L_{d,k}(\zeta_s, (\pi_{d,k}\zeta_s^c)^{1/dr}) \quad \text{with} \quad c = jd - \frac{kd}{n} \cdot \frac{q^f - 1}{q^d - 1}.$$

By (3) and Lemmas II.1.1 and II.4.2, $\mathcal{G}(N/L_{d,k})$ is abelian and has the

exponent

$$\operatorname{lcm}\left(dr, \frac{fr}{\gcd(c, dr)}\right).$$

Using the abbreviation $b = \gcd(c, dr)$, Lemma I.3.4, and the rules

$$\operatorname{lcm}(x, y) = \frac{xy}{\gcd(x, y)}, \qquad z \cdot \gcd(x, y) = \gcd(zx, zy),$$

we now deduce that

$$[N:F] = \frac{fr}{\operatorname{lcm}\left(dr, \frac{fr}{b}\right)} = \gcd\left(b, \frac{f}{d}\right) = \gcd\left(c, dr, \frac{f}{d}\right).$$

Finally, we prove that $[N:F] | n$, namely that every prime l satisfies the inequality

$$\min\left\{v_l(c), v_l(dr), v_l\left(\frac{f}{d}\right)\right\} \leq v_l(n).$$

This is clear if $v_l(dr) \leq v_l(n)$ or $v_l\left(\frac{f}{d}\right) \leq v_l(n)$. We can therefore suppose that

$$v_l(d) + v_l(r) > v_l(n) \quad \text{and} \quad v_l(f) > v_l(n) + v_l(d)$$

But then $v_l(r) > v_l(n/d) \geq 0$ and $v_l(f/n) > v_l(d) \geq 0$, and so, by (4) and (6), $v_l(q - 1) > 0$ and $v_l(j) = 0$. Thus

$$v_l\left(\frac{kd}{n} \cdot \frac{q^f - 1}{q^d - 1}\right) \geq v_l(d) - v_l(n) + v_l(f/d) > v_l(jd) \quad \text{and}$$

$$v_l(c) = v_l(jd) \leq v_l(n). \quad \blacksquare$$

LEMMA II.4.4. *Let $K \subseteq F$, $F' \subseteq N$ be two intermediate fields such that N/F and N/F' are unramified extensions of the same degree m, where m divides n. Suppose that $4 \mid q - 1$ if n is even. Then $F \cong_K F'$.*

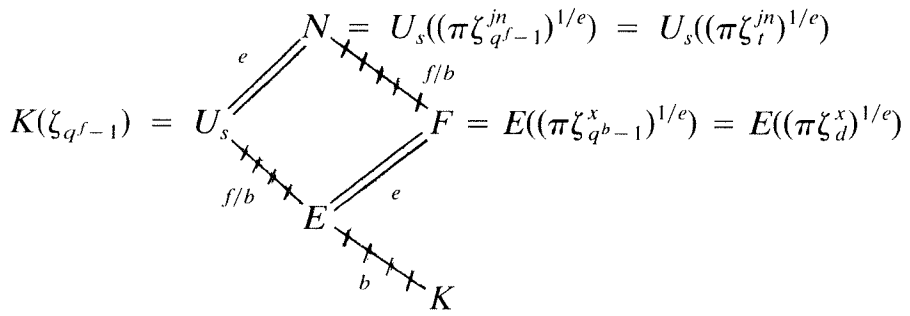
Proof. Suppose first that $[N:K]$ is divisible only by primes that divide n, so that in particular the n, e and f all have the same prime factors.

Let $E = U_s \cap F$. The F/E is a totally ramified extension and therefore it is linearly disjoint from U_s/E. Also U_sF is the maximal unramified extension of F in N. It follows that $U_sF = N$ and $[F:E] = e$ and $[U_s:E] = [N:F] = [N:F']$. Thus F' is a totally ramified extension of E of degree e as well.

Let $b = [E:K]$. Then there exist x, x' *and* a c such that

$$F = E(\pi\zeta_{q^b-1}^x)^{1/e} \quad \text{and} \quad F' = E(\zeta_e^c \cdot (\pi\zeta_{q^b-1}^{x'})^{1/e})$$

Of course F' is isomorphic over E to $E((\pi\zeta_{q^b-1}^{x'})^{1/e})$ and we can therefore assume that $c = 0$. We decompose now $q^b - 1$ in the form $q^b - 1 = dd'$, where d' is relatively prime to e and d is divisible only by primes that divide e. Then $\zeta_{q^b-1} = \zeta_d\zeta_{d'}$ and $\zeta_{d'}$ is an e-*th* power, hence $F = E((\pi\zeta_d^x)^{1/e})$ and $F' = E((\pi\zeta_d^{x'})^{1/e})$. Similarly we write $q^f - 1 = tt'$, where t' is relatively prime to e and get $N = U(\pi\zeta_t^{jn})^{1/e}$. Note that $b \mid f$ implies $q^b - 1 \mid q^f - 1$ and hence $s \mid t$.



The relation $U_sF = N$ implies

$$U_s((\pi\zeta_t^{jn})^{1/e}) = U_s((\pi\zeta_d^x)^{1/e}) = U_s((\pi\zeta_t^{xt/d})^{1/e}).$$

Consequently there exists a $\gamma \in U_s$ such that $\zeta_t^{jn} = \zeta_t^{xt/d}\gamma^e$. This γ satisfies $\gamma^{et} = 1$, so $\gamma = \zeta_t^u$, as et is divisible only by primes which divide e. It follows that $jn \equiv xt/d + eu \bmod t$. However, $e \mid t$, by (9) and by the definition of t. Hence

(a) $$xt/d \equiv jn \bmod e.$$

Consider now a prime l that divides either d or t. Then $l \mid e$ and therefore $l \mid q - 1$. Thus

(b) $$v_l(t) = v_l(q^f - 1) = v_l(q - 1) + v_l(f)$$

(c) $$v_l(d) = v_l(q^b - 1) = v_l(q - 1) + v_l(b)$$

and therefore

(d) $$v_l(t/d) = v_l(f/b) = v_l[N:F] \leqslant v_l(n) \leqslant v_l(e)$$

(Note that we have used here the assumption "$n \mid q - 1$ if $2 \mid n$".) In particular t/d divides both n and e. It follows from (a) that there exists a z such that

(e) $$x = jn \cdot \frac{d}{t} + \frac{zed}{t}.$$

The number of integers x modulo d of the form (e) is t/e. This is the number of elements in the set

$$Y = \left\{ \zeta_d^y \;\middle|\; y\frac{t}{d} \equiv jn \bmod e \right\}.$$

The elements ζ_d^x and $\zeta_d^{x'}$ obviously belong to Y. Note that the relation

$e \mid n(q-1)$ implies that if $\zeta_d^y \in Y$, then $\zeta_d^{yq} \in Y$. It follows that in order to prove that

$$\text{(f)} \qquad Y = \left\{ \zeta_d^{xq^a} \;\middle|\; a = 0, 1, 2, \ldots, \frac{t}{e} - 1 \right\}$$

it suffices to prove that all the elements on the right hand side of (f) are distinct. This means that we have to show that

$$\text{(g)} \qquad \zeta_d^{xq^m} = \zeta_d^x$$

implies $(t/e) \mid m$.

Indeed, let l be a prime factor of t/e. In particular $l \mid n$ and therefore we have, by (b), (10) and (3) that $v_l(r) > 0$ and that

$$\text{(h)} \qquad \begin{aligned} v_l(t/e) &= v_l(q-1) + v_l(f) - v_l(e) \\ &= v_l(r) + v_l(f) - v_l(e) = v_l(f/n). \end{aligned}$$

Hence $v_l(f/n) > 0$. It follows that $v_l(j) = 0$, by (6), and from this,

$$v_l\left(jn\frac{d}{t}\right) < v_l\left(ze\frac{d}{t}\right).$$

So, by (e) and (d),

$$v_l(x) = v_l(n) + v_l\left(\frac{d}{t}\right) = v_l(n) + v_l(b) - v_l(f).$$

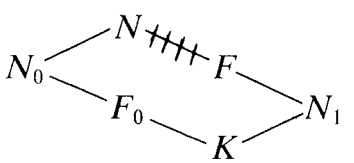
On the other hand, by (g), $d \mid x(q^m - 1)$. Hence

$$\begin{aligned} v_l(m) \geqslant v_l(d) - v_l(x) - v_l(q-1) &= v_l(b) - v_l(x) \\ &= v_l(f) - v_l(n) = v_l(t/e), \end{aligned}$$

by (c) and (h).

Thus t/e divides m and (f) is proved. We have therefore shown that there exists an integer a such that $\zeta_d^{x'}$ is equal to $\zeta_d^{xq^a}$ and thus is conjugate to ζ^x over K through the a-th power of the Frobenius automorphism of E/K. It follows that F' is isomorphic to F over K.

In the general case we can use the remark at the end of section I.2 and represent N as $N = N_0N_1$, where N_1/K is a cyclic extension of degree prime to n, and N_0/K is an n-symplectic type extension such that all the prime factors of $[N_0:K]$ divide n. In particular N_0 and N_1 are linearly disjoint over K. The assumption $[N:F] \mid n$ implies that $N_1 \subseteq F$. Also, N/F is an unramified extension and for $F_0 = N_0 \cap F$ we have $\gcd([N_0:F_0], [F:F_0]) = 1$. Thus N_0/F_0 is an unramified extension and $[N_0:F_0] = [N:F]$.



Similarly we obtain for $F_0' = N_0 \cap F'$ that $F' = F_0'N_1$ and that N_0/F_0' is an unramified extension whose degree is equal to $[N:F']$, hence also to $[N_0:F_0]$.

By the first part of the proof there exists a K-isomorphism $\phi_0:F_0 \to F_0'$. Any extension of ϕ_0 to an automorphism ϕ of N/K leaves N_1 invariant and hence maps F onto F'. ■

Combining Theorem C and Lemma II.4.4 we have:

THEOREM D. *If (L, F) and (L', F') are two induced structures of dimension n for N/K such that $[N:F] = [N:F']$, and assuming that $4 \mid q - 1$ if n is even, then $F \cong_K F'$.*

Also here, the extra assumption made in the theorem cannot be removed.

Having proved a uniqueness theorem for the induced structures of a given co-degree, we proceed now to prove an existence theorem for them.

THEOREM E. *Provided $4 \mid q - 1$ if n is even, there exists for every divisor m of n an induced structure (L, F) of dimension n for L/K such that $[N:F] = m$.*

Proof. Because of Theorem B, for every divisor d of n and for every integer $k \geqslant 0$ there is an induced structure $(L_{d,k}, F)$ of dimension n for N/K. From Theorem C we have

$$[N:F] = \gcd\left(jd - \frac{kd}{n} \cdot \frac{q^f - 1}{q^d - 1}, dr, \frac{f}{d}\right)$$

It therefore suffices to find a pair (d, k) such that $d \mid n$ and such that the right hand side of (22) is equal to m; this is merely a technical matter.

II.5. Splitting of the Galois group. We retain the notation and the assumption of the previous sections and draw some consequences about the structure of the group G and about its representations.

THEOREM F. *Assume again that $4 \mid q - 1$ if n is even. Then $N = SL$, where L is a cyclic totally ramified extension of degree n over K, N/L is a cyclic extension, $\mathcal{G}(L/K)$ operates faithfully on $\mathcal{G}(N/L)$ through conjugation and $S \cap L = K$. In particular, $G = \mathcal{G}(N/L) \cdot \mathcal{G}(N/S)$ is a semi-direct product.*

Proof. Apply Theorem E with $m = 1$, $k = 0$, and $d = \prod_l l^{v_l(f)}$, where l runs through all prime divisors of $\gcd(j, r, f)$. Because of (10), $L = L_{d,k}$

is a cyclic totally ramified extension of K of degree n, the extension N/L is cyclic, and $A = \mathcal{G}(N/L)$ is a maximal abelian subgroup (by Lemma II.4.2), which implies that $\mathcal{G}(L/K)$ operates faithfully on $\mathcal{G}(N/L)$ through conjugation.

We have still to show that the group G splits over A. Indeed, G is a niltpotent group (by Lemma I.2.1), and therefore it decomposes into the direct product of its l-Sylow subgroup. We can therefore assume, without loss of generality that G is an l-group.

If $l \neq 2$, then the splitting of G follows from Satz 5 of Gaschütz [3]. If $l = 2$, then the splitting follows from [8, Hilfsatz 5.1] unless G is a generalized quaternion group. In order to complete the proof we have therefore to show that the last case cannot happen.

Indeed, assume that G is a generalized quaternion group of order 2^{m+1}. Then it is generated by two elements x, y with the defining relations

$$x^{2^m} = 1, \quad x^{2^{m-1}} = y^2, \quad x^y = x^{-1}$$

(cf. Huppert [4, p. 91]). The center of G is generated by y^2 and is of order 2 and $G/Z(G)$ contains an element of order 2^{m-1}, namely $xZ(G)$. On the other hand, $G/Z(G)$ is a 2-elementary group, since G is of a 2-symplectic type. Hence $m = 2$ and $|G| = 8$. Now we use the assumption that $4 \mid q - 1$ and conclude by (10) of section II.4, that $n = 2$ and $4 \mid r$, hence 16 divides $nrf = |G|$, a contradiction. ■

Finally we add, without a proof, the following information about the irreducible representations of G.

THEOREM G. *Assume that $|G|$ is divisible only by primes that divide n.*

(a) *Every irreducible representation of G of dimension n is faithful.*

(b) *The group G has $(e/n^2) \cdot \phi(f)$ irreducible representations of dimension n, where ϕ is the Euler function.*

(c) *If z is a generator of $Z(G)$ and χ is a character of an irreducible representation ρ of G of dimension n, then χ vanishes on $G - Z(G)$ and $\chi(z) = n\xi$, where ξ is a primitive n^2ef-th root of unity.*

REFERENCES

1. B. J. BIRCH, "Cyclotomic fields and Kummer extensions" in *Algebraic number theory*, edited by Cassels and Fröhlich, Academic Press, London, 1967.
2. H. HASSE, *Number theory*, Springer, Berlin, 1980.
3. W. GASCHÜTZ, *Zur Erweiterungstheorie der endlichen Gruppen*, Crelle J., vol. 190 (1952), pp. 93–107.
4. B. HUPPERT, *Endliche Gruppen I*, Springer, Berlin, 1967.
5. H. KOCH, *Classification of the primitive projective representations of the Galois group of local fields*, Invent. Math., vol. 40 (1977), pp. 195–216.
6. S. LANG, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1968.

7. W. J. LeVeque, *Topics in number theory I,* Addison-Wesley, Reading, Mass., 1958.
8. J. Ritter, *Ein Induktionssatz fur rationale Charaktere von nilpotenten Gruppen,* Crelle J., vol. 254 (1972), pp. 133–151.
9. J.-P. Serre, *Corps locaux,* Hermann, Paris, 1968.

Tel Aviv University
Tel Aviv, Israel
Universität Augsburg
Augsburg, West Germany