INTERNATIONAL COMPUTER SCIENCE INSTITUTE

1947 Center St. • Suite 600 • Berkeley, California 94704-1198 • (510) 643-9153 • FAX (510) 643-7684

Elementary Proofs of some Results on Representations of p-groups

M.A. Shokrollahi

TR-95-054

September 1995

Abstract

A result of Roquette [3] states that if D is an absolutely irreducible representation of a p-group G over the field of complex numbers, then D can be realized in $K(\chi(g) \mid g \in G)$, where χ is the character of D and $K = \mathbb{Q}$ or $K = \mathbb{Q}(i)$ according to whether $p \neq 2$ or $p = 2$. Based on Baum and Clausen's [1] algorithm for computing the irreducible representations of supersolvable groups, we give an elementary proof of a theorem which, among other well-known facts on representations of p-groups, implies Roquette's result.

1 Introduction and Preliminaries

A matrix representation D of a finite group G over a field L is said to be realizable over a subfield M of L if there exists an invertible matrix T such that $TD(g)T^{-1}$ has entries in M for all $g \in G$. Denoting by χ the character of D and by $M(\chi)$ the character field $M(\chi(g) \mid g \in G)$ of D over M, it is easily seen that any subfield L' of L containing M such that D is realizable over L' contains $M(\chi)$, see below. An arbitrary representation of an arbitrary group G may not be realizable over its character field. If G is a p-group, however, it was proved by Roquette [3] that any irreducible representation of G with character χ is realizable over $K(\chi)$ where $K = \mathbb{Q}$ if G has odd order and $K = \mathbb{Q}(i)$ otherwise. We obtain this result as a corollary to the main theorem of this paper, which also implies that $K(\chi)$ is always a cyclotomic field, thereby proving that nontrivial irreducible representations of $\mathbb{Q}G$ always have degree $p^a(p-1)$ for some a.

The proof of the main theorem is elementary in the sense that it only uses some basic knowledge about the representation theory of finite groups, as well as some simple results on cyclotomic fields. For the convenience of the reader all the results we need are gathered in the rest of this section.

1.1 Monomial Matrices

A regular matrix A is called monomial, if it has in each row and in each column exactly one nonzero entry. Hence, any monomial $m \times m$-matrix is of the form $P_\pi \mathrm{diag}\,(a_1, \ldots, a_m)$, where P_π is the permutation matrix corresponding to the permutation $\pi \in S_m$, and $\mathrm{diag}\,(a_1, \ldots, a_m)$ is the diagonal matrix with the nonzero diagonal entries $a_1, \ldots, a_m$. A monomial matrix is called e-monomial, if its nonzero entries are eth roots of unity. For instance, the $n \times n$-identity matrix I_n is 1-monomial. An $mn \times mn$-matrix A is called *block e-monomial* if there exists a permutation π of $\{0, \ldots, m-1\}$ and e-monomial matrices $A_0, \ldots, A_{m-1}$ such that $A = (P_\pi \otimes I_n)(\oplus_{i=0}^{m-1} A_i)$, where $\otimes$ denotes the Kronecker product. By abuse of notation, we will in the sequel abbreviate $P_\pi \otimes I_n$ simply by π, if m and n are clear from the context.

LEMMA 1. *Let m and n be integers, $A_0, \ldots, A_{m-1}, B_0, \ldots, B_{m-1}$, and $X_0, \ldots, X_{m-1}$ be e-monomial $n \times n$-matrices over a field L, $1 = c_0, c_2, \ldots, c_{m-1}$ be nonzero elements of L, π, τ, and σ be permutations of the set $\{0, \ldots, m-1\}$, and $A := \tau(\oplus A_i)$, $B := \pi(\oplus B_i)$, and $N := \sigma(\oplus c_i X_i)$.*

(1) *For $p \geq 1$ any solution x of $x^p B^p = C^p$ is a pe-th root of unity.*

(2) *Suppose that $NAN^{-1} = B$ and that τ is an m-cycle. Then all the c_i are eth roots of unity belonging to the field generated by the entries of the A_i, B_i, and X_i.*

PROOF. (1) is obvious, so we concentrate on (2). The condition $NAN^{-1} = B$ is equivalent to the matrix equation

$$\tau\left(\bigoplus_{k=0}^{p-1} c_{\tau k} X_{\tau k} A_k c_k^{-1} X_k^{-1}\right) = \sigma^{-1}\pi\sigma\left(\bigoplus_{k=0}^{p-1} B_{\sigma k}\right).$$

The $c_{\tau^k 0}$ can be computed recursively, starting with $c_0 = 1$, by dividing by eth roots of unity. As τ is an m-cycle, this gives all the c_i, and the proof is complete. □

1.2 Representations and Algebraic Conjugacy

We recall some basic facts about representations of finite groups. Let G be a finite group, L be a field of characteristic zero, and Δ be a matrix representation of LG. Δ can be considered as a matrix representation of $L'G$ for any field extension L' of L in an obvious manner. We call Δ absolutely irreducible iff it is irreducible as a matrix representation of G over an algebraic closure of L. For a subfield M of L we define $\mathrm{def}_M(\Delta)$ as the smallest subfield of L containing M which contains all the entries of all $\Delta(g)$, $g \in G$. If χ denotes the character of Δ, then the *character field* $M(\chi)$ of Δ is defined as $M(\chi(g) \mid g \in G)$. Obviously, $M(\chi)$ is always contained in $\mathrm{def}_M(\Delta)$. If σ is a field and $X := (x_{ij}) \in L^{n \times n}$, we define $X^\sigma := (x_{ij}^\sigma)$, where x_{ij}^σ is the image of x_{ij} under σ. Analogously, Δ^σ is defined as Δ^σ by $\Delta^\sigma(g) := \Delta(g)^\sigma$ for all $g \in G$. Clearly, Δ^σ is a representation of LG which is (absolutely) irreducible iff Δ is. Furthermore, if $\Delta \sim \Phi$, then $\Delta^\sigma \sim \Phi^\sigma$, where $\sim$ denotes equivalence of representations over L.

From now on suppose that L is a splitting field of G of characteristic zero which is a cyclic galois extension of a subfield M. Let σ be a fixed generator of this group. For an irreducible representation Δ of LG we are interested in those subfields M' of L containing M such that Δ is *realizable* over M', i.e., such that there exists $\Delta' \sim \Delta$ with $\mathrm{def}_M(\Delta') = M'$. Any such M' contains $M(\chi)$, where χ denotes the character of Δ. Indeed, if τ is a generator of $\mathrm{Gal}(L/M')$, then $\Delta'^\tau = \Delta'$, hence $\chi(g)^\tau = \chi(g)$ for all $g \in G$, which implies that $M(\chi)^\tau = M(\chi)$.

Suppose now that F is an irreducible representation of MG, which is not necessarily absolutely irreducible, and consider F as a representation of LG. Let D be an irreducible constituent of F over L. As $F^\sigma = F$, D^{σ^i} is also an irreducible constituent of F for all i. Let χ denote the character of D, and let $m := [M(\chi) : M]$. Then $D, D^\sigma, \ldots, D^{\sigma^{m-1}}$ are pairwise inequivalent and hence, $\Delta := D \oplus D^\sigma \oplus \cdots \oplus D^{\sigma^{m-1}}$ is a constituent of F. If D is realizable over its character field $M(\chi)$, then Δ is realizable over M. Postponing the proof of this for a moment, we see that the following holds.

PROPOSITION 2. *The notation being as above, suppose that all the irreducible representations of LG are realizable over their character fields. If F is an irreducible representation of MG, then there exists an irreducible representation D of LG such that $F \sim \oplus_{i=0}^{m-1} D^{\sigma^i}$, where m is the degree of the character field of D over M.*

PROOF. By the discussions preceding the proposition it suffices to show the following: if L' is a field extension of degree m of M contained in L, τ is a generator of $\mathrm{Gal}(L'/M)$, and D is an irreducible representation of $L'G$, then $\Delta := \oplus_{i=0}^{m-1} D^{\sigma^i}$ is realizable over M. Let ω be a primitive element of the extension $L' \supseteq M$, and $C := \left((\omega^j)^{\tau^i}\right)_{i=0}^{m-1}$. C is invertible. Let d be the degree of D, and $T := C \otimes I_d$. Then it is easily checked that for all $g \in G$ the matrix $T^{-1}\Delta(g)T$ has coefficients in M. $\square$

Now let N be a normal subgroup of G of prime index such that L is also a splitting field of N, and let F and F' be representations of LN. The *intertwining space* $\mathrm{Int}\,(F, F')$ is the L-space defined as the set of all those matrices X over L such that $XF(\nu) = F'(\nu)X$ for all $\nu \in N$. This space contains an invertible matrix iff $F \sim F'$.

In the sequel, we denote by $F \uparrow G$ the induction of F to G along the set $(1, g, \ldots, g^{p-1})$ of representatives. If F is an absolutely irreducible representation of N, then so is the

representation F^g defined by $F^g(\nu) := F(g\nu g^{-1})$. Obviously, $(F \uparrow G)^\sigma = F^\sigma \uparrow G$, and $(F^g)^\sigma = (F^\sigma)^g$.

There is an intimate connection between the set of irreducible representations of G and that of N to which we refer in the sequel as Clifford Theory. The main results we need are summarized in the following.

THEOREM 3. *Notation being as above, suppose that F is an irreducible representation of LN. Then we have the following:*

(1) *If $F^g \sim F$, then F has p inequivalent irreducible extensions $D_0^{(F)}, \ldots, D_{p-1}^{(F)}$ to irreducible representations of LG.*

(2) *If $F \not\sim F^g$, then $\Delta_F := F \uparrow G$ is an irreducible representation of LG, and $\Delta_F \downarrow N = \oplus_{i=0}^{p-1} F^{g^i}$.*

(3) *The set formed by all $D_i^{(F)}$ and all Δ_F, where F ranges over a set of pairwise inequivalent irreducible matrix representations of LN, is a set of pairwise inequivalent irreducible matrix representations of LG.*

A simple proof of this theorem can be found, e.g., in the book by Clausen and Baum [2].

1.3 Hilbert's Theorem 90

Let L be a cyclic field extension of M and let the corresponding Galois group be generated by σ, say. If $[L\colon M] = m$ and $S \in \mathrm{GL}(m, L)$, then we define the relative *norm* of S *with respect to* σ by $\mathrm{N}_\sigma(S) := S^{\sigma^{m-1}} \cdots S^\sigma S$. If $m = 1$, then this is the norm of field elements in the usual sense, and is in particular independent of σ; for this reason we also write $\mathrm{N}_{L/M}$ for N_σ if $m = 1$. Note however that if $m > 1$, then the norm of S does not even need to belong to $M^{n\times n}$. The following theorem, due to Speiser [5], is a generalization of Hilbert's Theorem 90.

THEOREM 4. *Assume that L/M has a cyclic Galois group generated by σ and let $S \in \mathrm{GL}(n, L)$. There exists $T \in \mathrm{GL}(n, L)$ such that $S = T^{-1}T^\sigma$ if and only if $\mathrm{N}_\sigma(S) = I_n$.*

An easy alternative proof of this theorem can be found in Serre's book [4].

1.4 Cyclotomic Fields

For an integer n let L_n denote the *cyclotomic field* generated over $\mathbb{Q}$ by a primitive nth root of unity. For instance, $L_2 = \mathbb{Q}$, and $L_4 = \mathbb{Q}(i)$. We denote by $\mu(L_n)$ the set of roots of unity contained in L_n. Hence, $\mu(L_n)$ is the group of $(2n)$th roots of unity if n is odd, and it is the group of nth roots of unity of n is even. In the following we set $K := \mathbb{Q}$ if $p \neq 2$ and $K := L_4 = \mathbb{Q}(i)$ if $p = 2$. For $1 \leq d \leq n$ let $\ell_{p^d} := [L_{p^d}\colon K]$.

It is well-known that $(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathrm{Gal}(L_{p^n}/\mathbb{Q})$ canonically, the isomorphism being $c \mapsto (\sigma_c\colon \zeta \mapsto \zeta^c)$, where ζ is a primitive p^nth root of unity. Consequently, L_{p^n} is a cyclic extension of K of degree ℓ_{p^n}. We let γ denote an element of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ such that the Galois group $\mathrm{Gal}(L_{p^n}/K)$ is generated by σ_γ. Identifying γ with an integer, we see that for any $d \leq n$ the highest power of p dividing $\gamma^{\ell_{p^d}} - 1$ is p^d. (Otherwise, σ_γ would generate a proper subgroup of $\mathrm{Gal}(L_{p^n}/K)$.)

LEMMA 5. *With the above notation the following hold:*

(1) *If M is a subfield of L_{p^n} of index p, then $M = L_{p^{n-1}}$.*

(2) *Let $n \geq m$ and suppose that $L_{p^m} \supseteq K$. Then $\mathrm{N}_{L_{p^n}/L_{p^m}}(\mu(L_{p^n})) = \mu(L_{p^m})$.*

(3) *Let $L := L_{p^n}$, $M := L_{p^m}$ for some $m \leq n$ such that $M \supseteq K$, d be an integer ≥ 1, $S \in L^{d\times d}$ be p^n-monomial, and σ be a generator of $\mathrm{Gal}(L_{p^n}/L_{p^m})$. If $\mathrm{N}_\sigma(S) = cI_d$ for some $c \in L$, then there exist some $a \in \mu(L)$ and some $T \in \mathrm{GL}(d, L)$ such that $T^{-1}T^\sigma = aS$.*

PROOF. Part (1) is obvious.

(2) Let $L := L_{p^n}$ and $M := L_{p^m}$. Then $\lambda := [M\colon K] = \ell_{p^m}$. Hence M is the fixed field of σ_γ^λ and $\eta := \mathrm{N}_{L/M}(\zeta) = \zeta^s$, where $s = (\gamma^{\lambda p^{n-m}} - 1)/(\gamma^\lambda - 1) = (\gamma^{\ell_{p^n}} - 1)/(\gamma^{\ell_{p^m}} - 1)$ and ζ is a primitive p^nth root of unity. As the highest p-power dividing s is p^{n-m}, η is a primitive p^mth root of unity. This yields the assertion for $p = 2$. For $p \neq 2$ we still have to show that $\mathrm{N}_{L/M}(-1) = -1$. But this is clear, since $\mathrm{N}_{L/M}(-1) = (-1)^{[L:M]} = -1$.

(3) The product of two p^n-monomial matrices is again p^n-monomial, hence c is a p^nth root of unity. Since $\mathrm{N}_\sigma(S)^\sigma = S\mathrm{N}_\sigma(S)S^{-1}$, we see that $c \in M$, hence $c \in \mu(M)$. By Pat (2) of this lemma there exists $a \in \mu(L)$ such that $\mathrm{N}_{L/M}(a) = c^{-1}$. Hence, $\mathrm{N}_\sigma(aS) = I_d$, and Hilbert's Theorem 90 implies the existence of T. □

2 The Main Theorem

During this section we assume that G is a group of order p^n, where p is a prime and $n \geq 1$, that $\mathcal{T} := (G = G_n > G_{n-1} > \cdots > G_0 = \{1\})$ is a chief series of G with factors $G_i/G_{i-1} =: \langle g_i G_{i-1}\rangle$, and that $\mathcal{T}_i := (G_i > G_{i-1} > \cdots > G_0)$ for $0 \leq i \leq n$. We work with a fixed generator σ of $\mathrm{Gal}(L_{p^n}/K)$.

THEOREM 6. *With the above notation there exists for all $1 \leq i \leq n$ a set $\mathcal{F}_i$ of pairwise inequivalent absolutely irreducible matrix representations of $L_{p^n}G_i$ with the following properties:*

(1) *All $F \in \mathcal{F}_i$ are p^i-monomial and their degree is a power of p. Moreover, $\mathrm{def}_K(F)$ is a cyclotomic field for all $F \in \mathcal{F}_i$ which equals $\mathbb{Q}$ if and only if F is the trivial representation.*

(2) *For $i < j \leq n$ let $\pi_j \in Sym\mathcal{F}_i$ be the permutation satisfying $F^{g_j} \sim \pi_j F$. Then for all $F \in \mathcal{F}$ the space $\mathrm{Int}\,(F^{g_j}, \pi_j F)$ is generated by a p^i-monomial matrix X_{jF} satisfying $\mathrm{def}_K(X_{jF}) \subseteq \mathrm{def}_K(F)$.*

(3) *Let $\delta_i \in Sym\mathcal{F}_i$ be the permutation defined by $F^\sigma \sim \delta_i F$. Then $\mathrm{Int}\,(F^\sigma, \delta_i F)$ is generated by a p^i-monomial matrix M_F.*

(4) *For $F \in \mathcal{F}_i$ with character χ the degree $[\mathrm{def}_K(F)\colon K(\chi)]$ divides the degree of F, hence is a p-power.*

(5) *For $F \in \mathcal{F}$ with character χ the field $K(\chi)$ is a cyclotomic field. In case $p \neq 2$ this field is equal to $\mathbb{Q}$ if and only if F is the trivial representation.*

This theorem implies the following well-known results.

COROLLARY 7. (ROQUETTE [3]) *An absolutely irreducible representation of G with character χ is always realizable over $K(\chi)$.*

PROOF. Since $M := K(\chi)$ is a cyclotomic field contained in $L := L_{p^n}$ by Theorem 6(5), the Galois group of L over M is cyclic and generated by an element τ, say. F and F^τ have the same character, hence they are equivalent. Switching to an equivalent representation, we see by Theorem 6(3) that $\mathrm{Int}\,(F, F^\tau)$ is generated by a p^n-monomial matrix S, say. As $\mathrm{N}_\tau(S) \in \mathrm{Int}\,(F, F)$, we obtain $\mathrm{N}_\tau(S) = cI_f$ for some $c \in L$, where f is the degree of F. Replacing S by an appropriate multiple if necessary, we conclude from Lemma 5(3) that there exists $T \in \mathrm{GL}(f, L)$ such that $S = (T^\tau)^{-1}T$. Hence $TFT^{-1} = T^\tau F^\tau (T^\tau)^{-1}$, which shows that F is realizable over $K(\chi)$. □

COROLLARY 8. *Any nontrivial irreducible representation of a p-group over $\mathbb{Q}$ has degree $p^a(p-1)$ for some $a \in \mathbb{N}$.*

PROOF. For $p = 2$ the assertion is obvious by part (1) of the above theorem. So assume that $p \neq 2$. Let Δ be a nontrivial irreducible representation of $\mathbb{Q}G$ and view Δ as a representation of L_nG. By Proposition 2 there exists an irreducible representation D of L_nG such that $\Delta \sim \oplus_{i=1}^m D^{\sigma^i}$, where $m = [\mathbb{Q}(\chi)\colon \mathbb{Q}]$, χ being the character of D, and σ is a generator of the Galois group of $\mathbb{Q}(\chi)$ over $\mathbb{Q}$. In particular, the degree of Δ is m times that of D. As $\mathbb{Q}(\chi)$ is a cyclotomic field unequal to $\mathbb{Q}$ by Theorem 6(5), we obtain $m = p^b(p-1)$ for some b and the assertion follows by Theorem 6(1). □

The rest of this section is devoted to the proof of the above theorem. Note first that part (5) of the theorem is a consequence of parts (1) and (4) by Lemma 5(1). So we are left with the proof of parts (1)–(4). For this we use induction on i. The case $i = 0$ being trivial, let us discuss the induction step $i - 1 \to i$. Let $F \in \mathcal{F}_{i-1}$. There exist two possibilities for the conjugate representation F^{g_i}: either $F^{g_i} \sim F$ or $F^{g_i} \not\sim F$.

Suppose that $F^{g_i} \sim F$. By Clifford Theory (Theorem 3) F has p inequivalent absolutely irreducible extensions $D_0^{(F)}, \ldots, D_{p-1}^{(F)}$. Let D be such an extension and $X := D(g_i)$. Then $X \in \mathrm{Int}\,(F^{g_i}, F)$ and $X^p = F(g_i^p)$. Hence there exist p solutions $c_0, \ldots, c_{p-1}$ of the matrix equation $c^p X_{iF}^p = F(g_i^p)$ and $D_k^{(F)}$ is given by $D_k^{(F)} \downarrow G_{i-1} = F$ and $D_k^{(F)}(g_i) = c_k X_{iF}$ for $0 \leq k < p$. By Lemma 1(1) and the induction hypothesis the c_k are p^ith roots of unity. Hence these irreducible representations are p^i-monomial, and their field of definition is a cyclotomic field contained in L_{p^i}. For $p \neq 2$ this field is equal to $\mathbb{Q}$ iff $\mathrm{def}_K(F)$ equals $\mathbb{Q}$ and $c_k \in \mathbb{Q}$. By the induction hypothesis this means that F is the trivial representation of G_{i-1} and $c_k = 1$, which in turn implies that $D_k^{(F)}$ is the trivial representation of G_i.

Now suppose that $F^{g_i} \not\sim F$. By Clifford Theory $F \uparrow G_i$ is irreducible and $(F \uparrow G_i) \downarrow G_{i-1} = \oplus_{k=0}^{p-1} F^{g_i^k}$. Let $\tau_i \in \mathrm{Sym}\,\mathcal{F}_{i-1}$ be such that $F^{g_i} \sim \tau_i F$ for $F \in \mathcal{F}_i$. As $F^{g_i^k} \sim \tau_i^k F$, we obtain $X_k := X_{i\tau_i^{k-1}F} \cdots X_{iF} \in \mathrm{Int}\,(F^{g_i^k}, \tau_i^k F)$. We set $X := \oplus_k X_k$ and define the representation $D := D_F$ by $D(a) := X(F \uparrow G_i)(a)X^{-1}$ for all $a \in G_i$. Note that

$$(D \downarrow G_{i-1})(b) = X(F \uparrow G_i \downarrow G_{i-1})(b)X^{-1} = \bigoplus_{k=0}^{p-1} (\tau_i^k F)(b) \tag{1}$$

for $b \in G_{i-1}$. Obviously, D is p^i-monomial (even p^{i-1}-monomial) as X and F are such, and its degree is p times that of F. Hence the induction hypothesis implies that D has p-power degree. Moreover, the p^i-monomiality of D implies that its field of definition is a cyclotomic field. If it is equal to $\mathbb{Q}$, then the field of definition of F is also equal to $\mathbb{Q}$, which means that F is the trivial representation by the induction hypothesis. But this is a contradiction, since $F^{g_i} \not\sim F$ by assumption.

We define $\mathcal{F}_i$ as the set formed by all $D_k^{(F)}$ for those $F \in \mathcal{F}_{i-1}$ such that $F^{g_i} \sim F$ and all D_F for those $F \in \mathcal{F}_{i-1}$ such that $F^{g_i} \not\sim F$. By Theorem 3 $\mathcal{F}_i$ is a set of pairwise inequivalent irreducible matrix representations of G_i. This settles part (1) of the theorem.

For $i < j \leq n$ let $\pi_j \in \operatorname{Sym} \mathcal{F}_i$ be such that $D^{g_j} \sim \pi_j D$ and $\tau_j \in \operatorname{Sym} \mathcal{F}_{i-1}$ be such that $F^{g_j} \sim \tau_j F$. If $D = D_k^{(F)}$ for some $F \in \mathcal{F}_{i-1}$ and some k, then $\pi_j D$ must be an extension of $\tau_j F$ and we can put $X_{jD} := X_{jF}$. Note that by the induction hypothesis X_{jD} is p^{i-1}-monomial and $\operatorname{def}_K(X_{jD}) \subseteq \operatorname{def}_K(F) \subseteq \operatorname{def}_K(D)$.

Suppose now that $D = D_F$ for some $F \in \mathcal{F}_{i-1}$. Then $\pi_j D$ is the unique $\Delta \in \mathcal{F}_i$ such that $\Delta \downarrow G_{i-1}$ contains $\tau_j F$. By (1) we have $\pi_j D = \oplus_{k=0}^{p-1} \tau_j^k \Phi$ for some $\Phi \in \mathcal{F}_{i-1}$. There is some permutation ρ of $\{0, \ldots, p-1\}$ such that $\tau_j F_k = \Phi_{\rho k}$. By Schur's Lemma there exist nonzero $c_0, \ldots, c_{p-1}$ such that

$$X_{jD} = \rho \cdot \left(\bigoplus_{k=0}^{p-1} c_k X_k \right) \in \operatorname{Int}(D^{g_j}, \tau_j D),$$

where $X_k := X_{jF_k}$. We may suppose that $c_0 = 1$. Since

$$X_{jD} D^{g_j}(g_i) X_{jD}^{-1} = (\tau_j D)(g_i),$$

Lemma 1(2) implies that the c_i are p^ith roots of unity and hence X_{jD} is p^i-monomial. (Note that $(\tau_j D)(g_i) = (0, \ldots, p-1)$ times a suitable matrix.) It remains to prove that $\operatorname{def}_K(X_{jD}) \subseteq \operatorname{def}_K(D)$. To this end, notice that $\operatorname{def}_K(F) = \operatorname{def}_K(F^{g_i^j})$ for all $0 \leq j < p$, hence the induction hypothesis implies that $\operatorname{def}_K(F) = \operatorname{def}_K(\tau_j F)$, which yields $\operatorname{def}_K(X_{jF}) \subseteq \operatorname{def}_K(F)$. We infer that

$$\operatorname{def}_K(D) = \operatorname{def}_K(F). \tag{2}$$

The same argument yields $\operatorname{def}_K(X_k) \subseteq \operatorname{def}_K(F)$, hence Lemma 1(2) gives $\operatorname{def}_K(X_{jD}) \subseteq \operatorname{def}_K(F) = \operatorname{def}_K(D)$. This settles part (2) of the theorem.

The proof of the third part is quite similar to that of the second. Namely, if $D = D_k^{(F)}$ for some $F \in \mathcal{F}_{i-1}$, then one can set $M_D := M_F$. If $D = D_F$, then $\delta_i D \downarrow G_{i-1} = \oplus \tau_i^k \Phi$, for some $\Phi \in \mathcal{F}_{i-1}$. Putting $F_k := \tau_i^k F$ and $\Phi_k := \tau_i^k \Phi$, we see exactly as above that there exist p^{i-1}th roots of unity $c_0, \ldots, c_{p-1}$ such that $M_D = \rho \left(\oplus_{k=0}^{p-1} c_k X_k \right)$, where $X_k \in \operatorname{Int}(F_k^\rho, \Phi_{\rho k})$, and ρ is the permutation of $\{0, \ldots, p-1\}$ satisfying $\delta_{i-1} F_k = \Phi_{\rho k}$.

Let us now proceed with the proof of (4). Suppose that $D = D_k^{(F)}$ for some $F \in \mathcal{F}_{i-1}$ and some k. Clearly, F and D are of the same degree. Let χ denote the character of D, and ψ denote that of F. Let $\ell := [\operatorname{def}_K(D) \colon \operatorname{def}_K(F)]$, $q := [K(\chi) \colon K(\psi)]$, $m := [\operatorname{def}_K(F) \colon K(\psi)]$, and $n := [K(\psi) \colon K]$. Clearly, ℓ is the smallest positive integer such that $D^{(\sigma^{mn})^\ell} = D$. As $F^{\sigma^{mn}} = F$ and $\operatorname{Int}(D^{\sigma^{qnm}}, D) \subseteq \operatorname{Int}(F^{\sigma^{qnm}}, F) = \operatorname{Int}(F, F)$, we see that $D^{\sigma^{qmn}} = D$

and hence ℓ divides q. By the induction hypothesis m divides the degree of F. Hence $[\mathrm{def}_K(D)\colon K(\chi)] = m\ell/q$ divides the degree of F as it divides m.

If $D = D_F$ and χ denotes as above the character of D, then $K(\chi) \subseteq K(\psi)$. Let β denote a generator of $\mathrm{Gal}(K(\psi)/K(\chi))$. If $F^\beta \sim F$, then β is the identity and hence $K(\psi) = K(\chi)$. If $F^\beta \not\sim F$, then there exists a nonzero j such that $F^\beta \sim F^{g_i^j}$, as $D^\beta \sim D$. Hence $F^{\beta^p} \sim F^{g_i^p} \sim F$, and β^p is the identity which shows that $[K(\psi)\colon K(\chi)] = p$. Since $\mathrm{def}_K(D) = \mathrm{def}_K(F)$ by (2), we deduce from the induction hypothesis that $[\mathrm{def}_K(D)\colon K(\chi)]$ divides $p \deg F = \deg D$, and the proof of Theorem 6 is complete.

References

[1] U. Baum and M. Clausen: Computing irreducible representations of supersolvable groups. *Math. Comp.*, **63**, 351–359, (1994).

[2] M. Clausen and U. Baum: *Fast Fourier Transforms.* B.I. Wissenschaftsverlag, Mannheim, 1993.

[3] P. Roquette: Realisierung von Darstellungen endlicher nilpotenter Gruppen. *Arch. Math.*, **9**, 241–250, (1958).

[4] J.P. Serre: *Local Fields.* Springer Verlag, New York, 1979.

[5] A. Speiser: Zahlentheoretische Sätze aus der Gruppentheorie. *Math. Zeit.*, **5**, 1–6, (1919).