Can. J. Math., Vol. XXXII, No. 5, 1980, pp. 1229–1243

CAPITULATION IN CLASS FIELD EXTENSIONS OF TYPE (p, p)

S. M. CHANG AND R. FOOTE

1. Introduction. Let K be a number field, $K^{(1)}$ its Hilbert class field, that is, the maximal abelian unramified extension of K, let $K^{(2)}$ be the Hilbert class field of $K^{(1)}$, and let $G = \mathrm{Gal}(K^{(2)}/K)$ (alternatively, for p a prime the first and second p class fields enjoy properties analogous to those of the respective class fields discussed in this introduction; the particulars may be found surrounding Lemma 2). Since G/G' is the largest abelian quotient of G, $G/G' = \mathrm{Gal}(K^{(1)}/K)$ and so G' is the abelian group $\mathrm{Gal}(K^{(2)}/K^{(1)})$; moreover, class field theory provides (Artin) maps φ_K, $\varphi_{K^{(1)}}$ which are isomorphisms of the class groups C_K, $C_{K^{(1)}}$ onto G/G', G' respectively. In the remarkable paper [**1**] E. Artin computed the composition $V_{G'}$:

$$\begin{tikzcd} G \arrow[r, "\text{proj.}"] & G/G' \arrow[r, "\varphi_K^{-1}"] & C_K \arrow[r, "e"] & C_{K^{(1)}} \arrow[r, "\varphi_K(1)"] & G', \end{tikzcd}$$

where e is the homomorphism induced on the class groups by extending ideals of K to ideals of $K^{(1)}$, and he gave a formula for computing $V_{G'}$, the now familiar transfer (Verlagerung) homomorphism, in terms of the group G alone (see Lemma 1). In 1930 P. Furtwängler proved that $V_{G'}$ is the trivial homomorphism ([**4**]) and consequently $e : C_K \to C_{K^{(1)}}$ is the trivial map or, equivalently, every ideal of K when extended to $K^{(1)}$ becomes a principal ideal (capitulates) in $K^{(1)}$.

There may, however, be intermediate fields L, $K \subsetneq L \subsetneq K^{(1)}$, which enjoy this "principal ideal property": every ideal of K becomes principal when extended to L, and any characterization of these fields would be of interest. Artin's argument demonstrated more generally that the intermediate field L has the principal ideal property if and only if for the corresponding subgroup H of G, the transfer $V_H : G \to H/H'$ is the trivial homomorphism. Thus, for example, in the case when $K^{(1)}/K$ is a cyclic extension no proper subfield of $K^{(1)}$ containing K has the principal ideal property (see Theorem 1).

Already when $\mathrm{Gal}(K^{(1)}/K) \cong Z_p \times Z_p$, for some prime p, the situation becomes more complicated, and it is this configuration on which we focus. We are concerned chiefly with the quantitative problem: given $n \in \{0, 1, \ldots, p + 1\}$ is there a number field K as above with exactly n

Received November 21, 1978 and in revised form April 1, 1980.

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

of the intermediate fields $L_1, \ldots, L_{p+1}$ enjoying the principal ideal property (such K is said to have capitulation number n)?

For $p = 2$ the structure of G is highly restricted and group theory asserts that the only permissible values of n are 0, 1 and 3, each of which is realized by $K = \mathbf{Q}(\sqrt{-m})$, for certain $m \in \mathbf{Z}^+$ (Theorem 2).

For odd primes p and each $n \in \{0, 1, \ldots, p + 1\}$ we construct p-groups G with $G/G' \cong Z_p \times Z_p$ and with the property that if K is a number field and $\mathrm{Gal}(K^{(2)}/K) \cong G$, then K has capitulation number n (the difficult existence problem for K is not touched on). Although for odd p there are group theoretic examples for every $n \in \{0, \ldots, p + 1\}$, when $p = 3$ in addition much of the isomorphism structure of any example G can be determined for certain values of n, and so this case merits separate treatment in [**3**]. In contrast, when $p \geqq 5$ the family, $\mathscr{G}_n$, of p-groups whose corresponding number fields (if they exist) have class groups of type (p,p) and capitulation number n seems to be much more diverse in isomorphism type: specifically, motivated by the pioneering work of Scholz and Taussky [**10**] we show that group theory imposes little, if any, restriction on the number of intermediate fields, $L_1, \ldots, L_{p+1}$, which are of type (A) (see Theorem 4 and its prelude for details).

The paper concludes in a positive vein with a conjecture on the elements of $\mathscr{G}_n$ of minimal order and some field theoretic implications.

2. Preliminaries. For any finite group X and subgroup Y of X let $V_Y : X \rightarrow Y/Y'$ be the transfer homomorphism (see Lemma 1(i)). Let G be a p-group for p a prime and define

$$\mathscr{H}(G) = \{H | H \leqq G, |G : H| = p\},$$
$$\mathscr{H}_0(G) = \{H | H \in \mathscr{H}(G), \ker V_H = G\},$$
$$\mathscr{H}_x(G) = \{H | H \in \mathscr{H}(G), \ker V_H \neq G\}.$$

Recall that G is regular if and only if $\forall\, x, y \in G$, $(xy)^p = x^p y^p c^p$, for some $c \in \langle x, y \rangle'$.

We assume familiarity of elementary p-group theory; in particular, each $H \in \mathscr{H}(G)$ is normal in G, hence also $H' \lhd G$.

The homomorphisms V_H, for $H \in \mathscr{H}(G)$, admit the following facile formulae:

LEMMA 1. *Let X be a finite group, $Y \leqq X$, G a p-group, $H \in \mathscr{H}(G)$;*

(i) *for $x \in X$ let $\mathscr{O}_1, \ldots, \mathscr{O}_n$ be the orbits of x acting on the left cosets of Y by left multiplication; if $|\mathscr{O}_i| = m_i$ and $g_i Y \in \mathscr{O}_i$, $1 \leqq i \leqq n$, then*

$$V_Y(x) = \prod_{i=1}^{n} g_i^{-1} x^{m_i} g_i Y',$$

(ii) *for $x \in G - H$, $V_H(x) = x^p H'$,*

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

(iii) *if* $G = \langle x, H\rangle$, *for* $y \in H$,

$$V_H(y) = yy^xy^{x^2}\dots y^{x^{p-1}}\quad H' = x^p(x^{-1}y)^pH',$$

(iv) *if G is regular and G' is of exponent p*, $V_H(g) = g^pH'$, $\forall\, g \in G$.

Proof. For (i) see [**6**, Theorem 7.3.3]. Part (ii) and the initial assertion of (iii) are translations of (i); the second equality of (iii) follows from (ii) by writing $y = xx^{-1}y$ and using the fact V_H is a homomorphism. To prove (iv), by (ii) we need only consider $y \in H$. Let $x \in G - H$ so (iii) gives $V_H(y) = x^p(x^{-1}y)^pH'$. By the regularity of G,

$$x^p(x^{-1}y)^p = x^px^{-p}y^pc^p,$$

for some $c \in G'$, and since G' is assumed to have exponent p,

$$x^p(x^{-1}y)^p = y^p,$$

as desired.

It is worth observing that the study of capitulation of ideal classes of K of p-power order in subfields of $K^{(1)}$ is equivalent to the study of capitulation in the corresponding subfields of $K_p{}^{(1)}$ where $K_p{}^{(i)}$ (the ith member of the Hilbert p class field tower) is defined inductively by $K_p{}^{(0)} = K$, $K_p{}^{(i)}$ is the maximal abelian unramified extension of $K_p{}^{(i-1)}$ of degree a power of p, $\forall\, i \geqq 1$; moreover, the same transfer correspondence applies:

LEMMA 2. *Let K be a number field, $G =$ $\mathrm{Gal}(K^{(2)}/K)$, $\mathfrak{U}$ an ideal class of K of p-power order, G' the element $\varphi_K(\mathfrak{U})$ of* $\mathrm{Gal}(K^{(1)}/K)$ *(φ_K the Artin map), L any field with $K \subseteq L \subseteq K^{(1)}$, $H =$ $\mathrm{Gal}(K^{(2)}/L)$, and let $-$ denote the natural projection $G \to G/O^p(G)$, where $O^p(G)$ is the group generated by all p'-elements of G (i.e. the smallest normal subgroup of G whose quotient is a p-group); then* $\mathrm{Gal}(K_p{}^{(1)}/K)$ *is a Sylow p-subgroup of* $\mathrm{Gal}(K^{(1)}/K)$, $\mathrm{Gal}(K_p{}^{(2)}/K) \cong \bar{G}$, *and $\mathfrak{U}$ becomes principal in $L \Leftrightarrow \mathfrak{U}$ becomes principal in $L \cap K_p{}^{(1)} \Leftrightarrow V_{\bar{H}}(a) = \overline{1H'}$.*

Proof. This follows immediately from the observation that for fields $E \subseteq F$, $\mathrm{Norm}_{F/E^\circ}e = d$, where d is multiplication by the degree of F/E. Alternatively, one may translate the field theory to corresponding statements about finite groups and verify the lemma by completely elementary group theoretic manipulations.

In light of Lemma 2, rather than assuming $\mathrm{Gal}(K^{(1)}/K)$ is a p-group with certain properties, we need merely hypothesize properties of the Sylow p-subgroup of $\mathrm{Gal}(K^{(1)}/K)$ and work with the p class field tower in place of the general class field tower.

We say a field L with $K \subseteq L \subseteq K_p{}^{(1)}$ has the *principal p-ideal property* if, and only if, every ideal class of K of p-power order becomes

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

principal in L. Define the *p-capitulation number* of K to be the number of fields L with $K \subsetneq L \subsetneq K_p^{(1)}$ such that L has the principal p-ideal property (so if $\mathrm{Gal}(K^{(1)}/K)$ has Sylow p-subgroups of type (p, p), this number equals $|\mathscr{H}_0(\mathrm{Gal}(K_p^{(2)}/K))|$).

THEOREM 1. *If for a number field K $\mathrm{Gal}(K_p^{(1)}/K)$ is cyclic and L is a field with $K \subseteq L \subseteq K_p^{(1)}$, L has the principal p-ideal property if and only if $L = K_p^{(1)}$.*

Proof. Let $G = \mathrm{Gal}(K_p^{(1)}/K)$ and $H = \mathrm{Gal}(K_p^{(1)}/L)$: since the p-group $\mathrm{Gal}(K_p^{(2)}/K)$ has commutator quotient group isomorphic to the cyclic group G, by Burnside's Basis Theorem [**6**, Corollary 5.1.2] $\mathrm{Gal}(K_p^{(2)}/K)$ is abelian, whence $K_p^{(2)} = K_p^{(1)}$ and $G = \mathrm{Gal}(K_p^{(2)}/K) = \langle x \rangle$. Moreover, by Lemma 2 every ideal class of K of p-power order becomes principal in L if and only if $V_H(x) = 1$. By Lemma 1(i),

$$V_H(x) = x^{|G:H|} = x^{|L:K|},$$

so the result follows.

THEOREM 2. *If K is a number field with $\mathrm{Gal}(K_2^{(1)}/K) \cong Z_2 \times Z_2$, then if $K_2^{(1)} \neq K_2^{(2)}$ there is at most one field L with $K \subsetneq L \subsetneq K_2^{(1)}$ which enjoys the principal 2-ideal property; if $K_2^{(1)} = K_2^{(2)}$, every intermediate field enjoys the principal 2-ideal property.*

Proof. This is a direct computation of transfers using the fact that 2-groups G with $G/G' \cong Z_2 \times Z_2$ are either dihedral, quasidihedral or generalized quaternion. See [**8**] for the details and for examples of imaginary quadratic number fields with 2-capitulation numbers 0, 1 and 3.

THEOREM 3. *For each $n \in \{0, 1, 2, 3, 4\}$ there is a 3-group G with $G/G' \cong Z_3 \times Z_3$, G' abelian such that if K is a number field with $\mathrm{Gal}(K_3^{(2)}/K) \cong G$, then K has 3-capitulation number n.*

Proof. See [**3**] for the proof and for further details concerning G.

3. p-capitulation numbers for $p \geqq 5$. In this section p is a prime $\geqq 5$ and for each $n \in \{0, 1, \dots, p + 1\}$,

$$\mathscr{G}_n = \{G | G \text{ is a } p\text{-group, } G/G' \cong Z_p \times Z_p,\ G' \text{ abelian and } |\mathscr{H}_0(G)| = n\}.$$

We give two separate constructions to show $\mathscr{G}_n \neq \emptyset$, for each such n. The first construction (Lemma 5) is technically simpler but the second (Lemma 7) has the advantage of yielding groups of smaller order when $n > \frac{1}{2}(p + 1)$ and allows greater flexibility in "placing" the kernels of the transfers V_H, $H \in \mathscr{H}_x(G)$.

In each of the constructions G' will be elementary abelian, that is, an F_pG/G'-module. In order to describe these representations we introduce

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

the following notation: let F be the field of p elements, $A \cong Z_p \times Z_p$ (written multiplicatively), $A_1, \ldots, A_{p+1}$ the subgroups of A of order p with $A_1 = \langle \sigma \rangle$, $A_2 = \langle \tau \rangle$, $A_{i+2} = \langle \sigma^i \tau \rangle$ and let I be the ideal of FA generated by $\{\alpha - 1 | \alpha \in A\}$ (the augmentation ideal); for any left FA-module V, $\forall\, \alpha \in A$, $v \in V$,

$$[v, \alpha] = \alpha(v) - v = (\alpha - 1)v,$$

and $\forall\, B \leqq A$, $W \subseteq V$,

$$[W, B] = \mathrm{Span}_F\{[w, \beta] | w \in W, \beta \in B\},$$
$$C_W(B) = \{w | w \in W \text{ and } \beta(w) = w, \forall\, \beta \in B\}.$$

The first lemma ensures that once FA-modules V have been constructed with certain properties, a suitable extension of V by A can always be realized.

LEMMA 3. *If V is a cyclic FA-module with generator u and $(\sigma - 1)^{p-1}V = 0 = (\tau - 1)^{p-1}V$, then there is a p-group G with $G/G' \cong A$, $G' = V$, $G = \langle s, t\rangle$, $[s, t] = u$ and s, t acting by conjugation on V induce the transformations σ, τ respectively; moreover, if $I^{p-1}V = 0$, z_1, z_2 any elements of $C_V(A)$ and s_1, t_1 any two generators of G, such a group exists with the additional properties $s_1{}^p = z_1$, $t_1{}^p = z_2$.*

Proof. Theorem III.22 of [**12**] may be used to produce G.

Alternatively, G may be constructed by letting $\langle \hat{s}\rangle$, $\langle \hat{t}\rangle$ be cyclic groups of order p^2 and first forming the semi-direct product $G_0 = V\langle \hat{s}\rangle$ where $\hat{s}$ induces σ on V. Since $(\sigma - 1)^p = \sigma^p - \mathbf{1}$ annihilates V by hypothesis, $\hat{s}^p$ is the identity on V. Moreover,

$$(\hat{s}u)^p = \hat{s}^p u \sigma(u) \ldots \sigma^{p-1}(u) = \hat{s}^p$$

by virtue of

$$1 + \sigma + \ldots + \sigma^{p-1} = (\sigma - 1)^{p-1} = 0.$$

Thus since $\hat{s}$ acts (by conjugation) on a basis $v_1, \ldots, v_n$ of V with the same matrix as $\hat{s}u$ acting on the basis $\tau(v_1), \ldots, \tau(v_n)$, the map $T: G_0 \rightarrow G_0$ defined by $T(\hat{s}) = \hat{s}u$ and $T(v) = \tau(v)$, $\forall\, v \in V$ extends to an automorphism of G_0 which fixes $\hat{s}^p$. Now form the semi-direct product $G_1 = G_0\langle \hat{t}\rangle$ with $\hat{t}$ inducing T on G_0: since

$$T^p(\hat{s}) = \hat{s}u\tau(u) \ldots \tau^{p-1}(u) \quad \text{and} \quad (\tau - 1)^{p-1} = 0,$$

T is an automorphism of G_0 of order p, that is, $\hat{t}^p$ centralizes G_0.

To complete the argument, since $[\hat{s}, \hat{t}] = u$ and since for $\sigma^i\tau^j \in A$, $v \in V$,

$$(\sigma^i\tau^j - 1)v = [v, \hat{s}^i\hat{t}^j],$$

$I^{k-1}V$ is the kth term of the lower central series of G_1. If $I^{p-1} = 0$, G_1 has

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

class $\leqq p$ and $I^{p-2}V \leqq Z = C_V(A)$. Thus G_1/Z has class $\leqq p-1$ whence by [7, Corollary 12.3.1] is a regular p-group. Let $\hat{s}_1, \hat{t}_1$ be any generators of G_1 and write $\hat{s}_1 = \hat{s}^i\hat{t}^j$, $\hat{t} = \hat{s}^k\hat{t}^l$. By the regularity of G_1/Z,

$$\begin{aligned} \hat{s}_1^{\,p} &\equiv \hat{s}^{ip}\hat{t}^{jp} (\mathrm{mod}\ Z),\\ \hat{t}_1^{\,p} &\equiv \hat{s}^{kp}\hat{t}^{lp} (\mathrm{mod}\ Z), \end{aligned}$$

so because $\langle \hat{s}^p, \hat{t}^p, Z\rangle$ is elementary abelian and $\langle \hat{s}^p, \hat{t}^p\rangle \cap Z = 1$,

$$\langle \hat{s}_1^{\,p}, \hat{t}_1^{\,p}\rangle \cong Z_p \times Z_p \quad\text{and}\quad \langle \hat{s}_1^{\,p}, \hat{t}_1^{\,p}\rangle \cap Z = 1.$$

Finally, since $\langle \hat{s}_1^{\,p}, \hat{t}_1^{\,p}\rangle \leqq \langle Z, \hat{s}^p, \hat{t}^p\rangle = Z(G_1)$ we may quotient G_1 by the central subgroup $\langle \hat{s}_1^{\,p}z_1^{-1}, \hat{t}_1^{\,p}z_2^{-1}\rangle$ (which will not collapse V) to obtain the desired G.

LEMMA 4. *For each $n \in \{1, 2, \ldots, p-1\}$ there is a cyclic FA-module V of dimension $\frac{1}{2}(n+1)n$ with the properties:*

(i) $I^nV = 0$,

(ii) $\dim_F C_V(A) = n$,

(iii) $\dim_F[V, A_i] \cap C_V(A) = n-1$, $1 \leqq i \leqq p+1$, *and*

(iv) *for any distinct* $i_1, \ldots, i_n \in \{1, 2, \ldots, p+1\}$, $\bigcap_{j=1}^{n} [V, A_{i_j}] = 0$

Proof. Let V be a vector space over F of dimension $\frac{1}{2}n(n+1)$ with basis $\{u_{ij} | i = 1, \ldots, n, j = 1, \ldots, i\}$ and define an action of A on V by

$$\begin{aligned} \sigma(u_{ij}) &= u_{ij} + u_{ij+1}, & 1 \leqq i \leqq n, 1 \leqq j \leqq i-1,\\ \tau(u_{ij}) &= u_{ij} + u_{i-1j}, & 2 \leqq i \leqq n, 1 \leqq j \leqq i-1,\\ \sigma(u_{ii}) &= \tau(u_{ii}) = u_{ii}, & 1 \leqq i \leqq n. \end{aligned}$$

First of all, clearly σ, τ commute in their action on V; furthermore,

$$(\sigma - 1)^{j-i}(\tau - 1)^{n-i}u_{n1} = u_{ij}$$

whence $(\sigma - 1)^nV = 0 = (\tau - 1)^nV$, so as $n \leqq p-1$ σ, τ induce automorphisms of order p on V and, moreover, V is visibly a cyclic FA-module with generator u_{n1}.

Notice for any $\alpha \in A$, the coefficient of u_{rs} in the expansion of $(\alpha - 1)u_{ij}$ with respect to the given basis is zero unless $r \leqq i$, $s \geqq j$ and at least one of these inequalities is strict. This easily means (i) holds.

Now let $Z = \mathrm{Span}_F\{u_{11}, \ldots, u_{nn}\}$ so certainly $Z \subseteq C_V(A)$; and, conversely, $v \in C_V(A)$ implies the coefficient of u_{ij} in v is zero unless $i = j$, whereupon $Z = C_V(A)$ so (ii) is established.

To prove (iii) and (iv) let $u_i = u_{ii}$, $1 \leqq i \leqq n$, and $W = \mathrm{Span}_F\{u_{i+1i} | 1 \leqq i \leqq n-1\}$. Since $\bigcap_{j=1}^{n} [V, A_{ij}]$ is an FA-submodule of V, it will be zero if and only if its intersection with $C_V(A) = Z$ is zero. For each $\alpha \in A$, only the terms $(\alpha - 1)u_{i+1i}$ contribute to $(\alpha - 1)V \cap Z$, whence

$$(\alpha - 1)V \cap Z = (\alpha - 1)W \cap Z = (\alpha - 1)W.$$

Recall $A_1 = \langle \sigma\rangle$, $A_{i+2} = \langle \sigma^i\tau\rangle$, $0 \leqq i \leqq p-1$, so set $Z_i = [W, A_i]$.

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

Thus

$$\begin{aligned} Z_1 &= \operatorname{Span}_F\{u_2, u_3, \ldots, u_n\} \quad \text{and} \\ Z_i &= \operatorname{Span}_F\{u_j + (i-2)u_{j+1} | 1 \leqq j \leqq n-1\}, \quad 2 \leqq i \leqq p+1. \end{aligned}$$

Thus each Z_i is codimension 1 in Z, which, incidentally, verifies (iii). The one dimensional spaces Z/Z_1, Z/Z_i have bases $u_1 + Z_1$, $u_n + Z_i$, $2 \leqq i \leqq p+1$, respectively and since for $i \geqq 2$, $u_j \equiv (2-i)u_{j+1} \pmod{Z_i}$, $u_j \equiv (2-i)^{n-j}u_n \pmod{Z_i}$. Define $\varphi : Z \rightarrow \prod_{i=1}^{p+1} (Z/Z_i)$ by

$$\varphi(v) = (\pi_1(v), \ldots, \pi_{p+1}(v)),$$

$\pi_i : Z \rightarrow Z/Z_i$ being the natural projection. With respect to the u_i basis of Z and the above described basis of each Z/Z_i the matrix of φ is the $(p+1) \times n$ array

$$E = \begin{pmatrix} 1 & 0 & \_ & \_ & \_ & \_ & \_ & 0 & 0 \\ 0 & 0 & \_ & \_ & \_ & \_ & \_ & 0 & 1 \\ & & & (2-j)^{n-i} & & & & & \end{pmatrix}_{\substack{i=3,\ \ldots,\ n \\ j=1,\ \ldots,\ p+1}}$$

Any n distinct rows of E are linearly independent because the square matrix formed by n such rows consists of possibly one or both of the first two rows of E together with a Vandermonde matrix, whence it will have non-zero determinant. This means for any distinct $i_1, \ldots, i_n \in \{1, 2, \ldots, p+1\}$ the map

$$Z \rightarrow (Z/Z_{i_1}) \times \ldots \times (Z/Z_{i_n})$$

given by

$$v \mapsto (\pi_{i_1}(v), \ldots, \pi_{i_n}(v))$$

is non-singular. Thus the kernel of this map, which is $\bigcap_{j=1}^{n} Z_{i_j}$, is zero, as desired for (iv).

LEMMA 5. *For each* $m \in \{0, 1, \ldots, p-3, p+1\}$, $\mathscr{G}_m \neq \emptyset$.

Proof. Consider first when $m \neq 0, p+1$, set $n = m+1$ and let V be the FA-module described by Lemma 4. By (ii), (iii) and (iv), $\bigcap_{i=2}^{n} [V, A_i] \cap C_V(A)$ is one dimensional with basis, say, z. Let G be the group supplied by Lemma 3 such that $s^p = z$, $t^p = 1$. Again, I^kV is the $(k+1)^{\text{st}}$ member of the lower central series of G, so Lemma 4(i) asserts G has class $\leqq n+1 \leqq p-1$, whence G is a regular p-group by [**7**, Corollary 12.3.1]. Since G' is elementary abelian, $\mho_1(G) = \langle x^p | x \in G\rangle = \langle z\rangle$, so by Lemma 1(iv) for $H \in \mathscr{H}(G)$, $V_H = 1$ if and only if $z \in H'$. Since G' is abelian, if $H = \langle G', s^it^j\rangle$, then

$$H' = [G', s^it^j] = (\sigma^i\tau^j - 1)V.$$

By Lemma 4(iv) and the choice of z, $z \in H'$ if and only if $H = \langle G', s^it\rangle$, $0 \leqq i \leqq n-2$, which shows that $G \in \mathscr{G}_{n-1} = \mathscr{G}_m$.

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

For the remaining values let G be a non-abelian group of order p^3 and let G be of exponent p, if $m = p + 1$ and not of exponent p, if $m = 0$. Thus G is again regular and $\mho_1(G) = 1, Z(G)$ respectively. Since each maximal subgroup of G is abelian, by Lemma 1(iv) $G \in \mathscr{G}_m$ in each case.

In fact, with slightly more effort the case $m = p - 2$ could also be dealt with in Lemma 5 (even though G may not be regular); however, since this value will be treated in more detail shortly, it does not seem worthwhile to do so.

We now provide another construction which focuses on the subgroups in $\mathscr{H}_x$ rather than those in $\mathscr{H}_0$ (by constructing G with $|\mathscr{H}_x(G)| = m$):

LEMMA 6. *For each $m \in \{1, 2, \ldots, p - 2\}$ there exists a cyclic FA-module V of dimension $\frac{1}{2}m(m + 3)$ with the properties:*

(i) $I^{m+1}V = 0$,

(ii) $\dim_F C_V(A) = m$,

(iii) $\dim_F[V, A_i] \cap C_V(A) = m - 1, \quad 1 \leqq i \leqq m$,

(iv) $\bigcap_{i=1}^{m} [V, A_i] = 0$, *and*

(v) $C_V(A) \subseteq [V, A_i], \quad m + 1 \leqq i \leqq p + 1$.

Proof. Let U be a vector space of dimension $\frac{1}{2}m(m - 1)$ over F with basis $\{u_{ij} | i = 1, 2, \ldots, m - 1, j = 1, 2, \ldots, i\}$; for each $i \in \{1, 2, \ldots, m\}$ let Y_i be a 2 dimensional vector space over F with basis $\{y_i, z_i\}$ and let $Y = Y_1 \oplus Y_2 \oplus \ldots \oplus Y_m$. Now put $V = U \oplus Y$, and set

$$Z = \text{Span}_F\{z_1, \ldots, z_m\}.$$

Define an action of A on V by

$\sigma(u_{ij}) = u_{ij} + u_{ij+1}, \quad 1 \leqq i \leqq m - 1, 1 \leqq j \leqq i - 1,$
$\sigma(y_1) = y_1,$
$\sigma(y_i) = y_i + z_i, \quad 2 \leqq i \leqq m,$
$\sigma(z_i) = z_i, \quad 1 \leqq i \leqq m,$
$\tau(u_{ij}) = u_{ij} + u_{i-1j}, \quad 2 \leqq i \leqq m - 1, 1 \leqq j \leqq i - 1,$
$\tau(y_i) = y_i - (i - 2)z_i, \quad 1 \leqq i \leqq m,$
$\tau(z_i) = z_i, \quad 1 \leqq i \leqq m,$

and for $1 \leqq i \leqq m - 1$,

$$\sigma(u_{ii}) = u_{ii} + \sum_{j=1}^{m} (a_{ij}y_j + c_{ij}z_j),$$

$$\tau(u_{ii}) = u_{ii} + \sum_{j=1}^{m} (b_{ij}y_j + d_{ij}z_j),$$

where $a_{ij}, b_{ij}, c_{ij}, d_{ij}$ are elements of F to be specified.

Notice first that for each $i \in \{1, \ldots, m\}$, Y_i is an FA-module on which the elements of A_i induce the identity transformation and the elements of $A - A_i$ are not the identity. Thus if $j \neq i$, $[Y_i, A_j]$ is one

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

dimensional, hence is the unique one dimensional FA-submodule of Y_i : $Y_i \cap Z$. Moreover, as in the proof of Lemma 4, $I^{m-1}(V/Y) = Y/Y$ and clearly $I^2Y = 0$, whence $I^{m+1}V = 0$, which is (i). Specifically, $(\sigma - 1)^{m+1}V = 0 = (\tau - 1)^{m+1}V$, so because $m + 1 < p$, σ and τ induce transformations of order p on V.

Clearly, $\sigma\tau(u_{ij}) = \tau\sigma(u_{ij})$, $1 \leqq j \leqq i - 2$, $1 \leqq i \leqq m - 1$, and $\sigma\tau(y) = \tau\sigma(y)$, $\forall\, y \in Y$. One computes that for $i \geqq 2$, $\sigma\tau(u_{i\,i-1}) = \tau\sigma(u_{i\,i-1})$ if and only if

$$\text{(6.1)} \quad a_{i-1\,j} = b_{ij} \quad \text{and} \quad c_{i-1\,j} = d_{ij}, \quad 2 \leqq i \leqq m - 1,\ 1 \leqq j \leqq m.$$

Similarly, for $i \geqq 1$, $\sigma\tau(u_{ii}) = \tau\sigma(u_{ii})$ if and only if

$$\text{(6.2)} \quad a_{i1} = 0 \quad \text{and} \quad b_{ij} = (2 - j)a_{ij}, \quad 1 \leqq i \leqq m - 1,\ 2 \leqq j \leqq m.$$

One sees that (6.1) together with (6.2) is equivalent to

$$\text{(6.3)} \quad \begin{aligned} &\text{(i) } a_{m-1\,1} = 0,\\ &\text{(ii) } a_{i-1\,j} = b_{ij} \quad \text{and} \quad c_{i-1\,j} = d_{ij}, \quad 2 \leqq i \leqq m - 1,\ 1 \leqq j \leqq m,\\ &\text{(iii) } a_{m-k\,j} = (2 - j)^{k-1}a_{m-1\,j}, \quad 1 \leqq j \leqq m,\ 2 \leqq k \leqq m - 1. \end{aligned}$$

Thus the specified action makes V into an FA-module if and only if (6.3) holds.

Continuing to work with indeterminate coefficients we find conditions under which assertion (iii) of the lemma is satisfied. For this, the following formula which the reader may verify by induction on k will be useful:

$$\text{(6.4)} \quad \sigma^k(u_{ii}) = u_{ii} + k\sum_{j=1}^{m} (a_{ij}y_j + c_{ij}z_j) + \tfrac{1}{2}k(k - 1)\sum_{j=2}^{m} a_{ij}z_j, \quad 1 \leqq i \leqq m - 1.$$

Thus (6.4) yields $\forall\, k \geqq 0$,

$$\text{(6.5)} \quad \sigma^k\tau(u_{ii}) = u_{ii} + \sum_{j=1}^{m} \{(ka_{ij} + b_{ij})y_j + (kc_{ij} + d_{ij})z_j\} + \sum_{j=2}^{m} \{\tfrac{1}{2}(k - 1)ka_{ij} + kb_{ij}\}z_j, \quad 1 \leqq i \leqq m - 1.$$

As in Lemma 4, since $\bigcap_{j=1}^{m} [V, A_j]$ is an FA-submodule of V, it will be zero if and only if its intersection with $C_V(A)$ is zero. We will eventually decide that $C_V(A) = Z$ so assume this equality holds for the moment. To have (iii) it will then certainly be necessary that $Z \not\subseteq [V, A_j]$, $1 \leqq j \leqq m$. In fact, we have already shown

$$[Y, A_j] = (Y_1 \cap Z) \oplus \ldots \oplus (Y_{j-1} \cap Z) \oplus (Y_{j+1} \cap Z) \oplus \ldots \oplus (Y_m \cap Z),$$

which is codimension one in Z, $1 \leqq j \leqq m$, so assuming $C_V(A) = Z$ if we could demonstrate $[V, A_j] \not\supseteq Z$, (iii) would be proven (observe that if

$C_V(A) = Z$, since $Z = [Y, A_j]$, for $m < j \leqq p + 1$, (v) will be valid also). In fact, we find conditions under which $[V, A_j] \cap Y_j = 0$, for then $[V, A_j] \cap Z$ will equal $[Y, A_j] \cap Z$ from which the above direct sum decomposition will yield (iv) as well. Since only the terms $[u_{ii}, A_j]$ contribute to $[V, A_j] \cap Y$, the latter equality will be valid provided

$$[u_{ii}, A_j] \subseteq \bigoplus_{\substack{k=1\\ k \neq j}}^{m} Y_k,$$

and a direct computation using (6.5) shows this will indeed be true if

(6.6) (i) $a_{i1} = 0$,

(ii) $c_{i1} = 0$,

(iii) $(j - 2)a_{ij} + b_{ij} = 0$, and

(iv) $\frac{1}{2}(j - 2)(j - 3)a_{ij} = (j - 2)b_{ij} + (j - 2)c_{ij} + d_{ij} = 0$,

$1 \leqq i \leqq m - 1, 2 \leqq j \leqq m.$

Substituting (6.6) (iii) in (6.6) (iv) gives

(6.7) $-\frac{1}{2}(j - 1)(j - 2)a_{ij} + (j - 2)c_{ij} + d_{ij} = 0,$

$1 \leqq i \leqq m - 1, 2 \leqq j \leqq m.$

Thus in order that (6.6) and (6.3) hold simultaneously we may express a_{ij} in terms of a_{m-1j}, d_{ij} in terms of c_{i-1j} and solve (6.7) recursively to obtain the following formula which may be proved directly by induction on k:

(6.8) $c_{m-kj} = \frac{1}{2}(-1)^k(k - 1)(j - 1)(j - 2)^{k-1}a_{m-1j}$

$+ (-1)^k(j - 2)^{k-1}c_{m-1j}, 2 \leqq k \leqq m - 1, 2 \leqq j \leqq m.$

Conversely, (6.8) captures the relation between the c_{ij}'s so we obtain in summary:

(6.9) V is an FA-module of dimension $\frac{1}{2}m(m + 3)$ and assuming $C_V(A) = Z$, assertions (i)–(v) of the lemma will hold whenever $a_{ij}, b_{ij}, c_{ij}, d_{ij}$ are elements of F subject to:

(i) $a_{m-11} = 0$,

(ii) $c_{m-11} = 0$,

(iii) $a_{m-kj} = (2 - j)^{k-1}a_{m-1j}, \quad 1 \leqq j \leqq m, 2 \leqq k \leqq m - 1,$

(iv) $b_{ij} = a_{i-1j}, \quad 2 \leqq i \leqq m - 1, 1 \leqq j \leqq m,$

(v) $c_{m-kj} = \frac{1}{2}(-1)^k(j - 1)(j - 2)^{k-1}a_{m-1j}$

$+ (-1)^k(j - 2)^{k-1}c_{m-1j}, \quad 1 \leqq j \leqq m, 2 \leqq k \leqq m - 1,$

$d_{ij} = c_{i-1j}, \quad 2 \leqq i \leqq m - 1, 1 \leqq j \leqq m.$

Thus once the free parameters $a_{m-1j}, c_{m-1j}, 2 \leqq j \leqq m$ and d_{1j}, b_{1j} are specified, (6.9) determines the remaining coefficients.

To ensure that V is also a cyclic FA-module (with generator $u = u_{m-11}$)

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

first observe that as in Lemma 4 every u_{ij} is an FA multiple of u, viz.

$$u_{ij} = (\tau - 1)^{m-1-i}(\sigma - 1)^{j-1}u;$$

furthermore, z_i is an FA multiple of y_i, $1 \leqq i \leqq m$. Thus V will be cyclic provided each y_i is an FA multiple of u. For this to happen it suffices that if $W = \mathrm{Span}_F\{u_{11}, \ldots, u_{m-1m-1}\}$, then $(\sigma - 1)W + (\tau - 1)W$ contains a coset representative of each coset of Z in Y: because then for each $i \in \{1, 2, \ldots, m\}$ $\exists$ $t_i \in Z$ such that $y_i + t_i = \lambda_i u$, for some $\lambda_i \in FA$; then since $\tau - 1$ and $\sigma - 1$ are zero on Z, $z_1 = (\tau - 1)\lambda_1 u$, $z_i = (\sigma - 1)\lambda_i u$, $2 \leqq i \leqq m$, so every element of Z is an FA multiple of u, whence the differences $y_i = \lambda_i u - t_i$ are also. Consider the transformation $(\sigma - 1) : W \rightarrow Y/Z$ by $w \mapsto \sigma(w) - w + Z$. With respect to the bases $\{u_{ii}\}$, $\{y_i + Z\}$, this map has matrix ${}^t(a_{ij})$. Assuming (6.9)(i)–(vi) are in effect,

$$ {}^t(a_{ij}) = \left(\begin{array}{cccc|c} 0 & 0 & - - - - - - - - - - & 0 & 0 \\ 0 & 0 & - - - - - - - - - - & 0 & a_{m-12} \\ \hline & & & & a_{m-13} \\ & & & & \cdot \\ & & E & & \cdot \\ & & & & \cdot \\ & & & & a_{m-1m} \end{array}\right) $$

where $E = (e_{ij})$ is the square matrix of degree $m - 2$,

$$e_{ij} = (-j)^{m-i-1}a_{m-1j+2}.$$

Thus

$$E = \mathrm{diag}(a_{m-1,3}, \ldots, a_{m-1m}). (f_{ij}),$$

where $f_{ij} = (-j)^{m-i-1}$. If we denote by ${}^t(a_{ij})'$ the $(m - 1) \times (m - 1)$ matrix obtained from ${}^t(a_{ij})$ by deleting its first row, then

$$\det {}^t(a_{ij})' = \prod_{k=2}^{m} a_{m-1k} \cdot \det (f_{ij}).$$

Since (f_{ij}) is Vandermonde, ${}^t(a_{ij})$ has rank $m - 1$ if and only if $a_{m-12}, \ldots, a_{m-1m}$ are all non-zero. Now notice that the image of W under $\sigma - 1$ is contained in the $m - 1$ dimensional space spanned by $y_2 + Z, \ldots, y_m + Z$ and further, if $b_{11} \neq 0$, $\tau(u_{11}) - u_{11} + Z$ is not in this space. This proves

(6.10) V is a cyclic FA-module if conditions (6.9)(i)–(vi) hold and $b_{11}, a_{m-12}, \ldots, a_{m-1m}$ are all non-zero elements of F.

As a consequence of assuming $a_{m-12}, \ldots, a_{m-1m}$ are non-zero, $\sigma(u_{ii}) \neq u_{ii}$, $1 \leqq i \leqq m - 1$, so no element of $C_V(\sigma)$ may have a non-zero term in

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

u_{ij}, $\forall i, j$ — in particular, $C_V(A) \subseteq Y$, whence $C_V(A) = C_Y(A) = Z$, as hypothesized in (6.9).

Since (6.9) and (6.10) may certainly be satisfied simultaneously, the lemma is proven.

As before, we now use Lemma 3 to form the extension VA. The arguments concerning the position of the kernels could be simplified were we to ignore the case $n = 3$ in which the p-group we construct has class p and may therefore be irregular.

LEMMA 7. *For each* $n \in \{3, 4, \ldots, p\}$, $\mathscr{G}_n \neq \emptyset$; *moreover, given* $n_0 \in \{0, 1, \ldots, p + 1 - n\}$ $\exists$ $G \in \mathscr{G}_n$ *such that*

$$|\{H | H \in \mathscr{H}(G) \text{ and } \ker V_H = H\}| = n_0.$$

Proof. Set $m = p + 1 - n$ and let V be a cyclic FA-module with generator u satisfying the conclusions of Lemma 6. Let $Z = C_V(A)$ and for $1 \leqq i \leqq m$, let

$$Z_i = \bigcap_{\substack{j=1\\ j\neq i}} [V, A_j] \cap Z;$$

by (ii), (iii) and (iv) Z_i is a one dimensional space with basis, say, z_i. Define

$$\begin{aligned} (7.1)\quad \zeta &= \epsilon z_1 + z_2 + z_3 + \ldots + z_m, \\ \xi &= z_1 - z_3 - 2z_4 - \ldots - (n_0 - 2)z_{n_0} + \delta z_2, \end{aligned}$$

where

$$\epsilon = \begin{cases} 0, & \text{if } n_0 > 0, \\ 1, & \text{if } n_0 = 0, \end{cases} \qquad \delta = \begin{cases} 0, & \text{if } n_0 > 1, \\ 1, & \text{if } n_0 \leqq 1. \end{cases}$$

Let G be the group provided by Lemma 3 (written multiplicatively) with the additional property (using Lemma 6(i))

$$(7.2)\quad (s^{p-2}t)^p = \xi\zeta^{-2}, \quad (s^{p-1}t)^p = \xi\zeta^{-1}.$$

Now set $a_1 = s$, $a_i = s^{i-2}t$, $2 \leqq i \leqq p + 1$ and put $H_i = \langle a_i, G' \rangle = \langle a_i, V \rangle$, so $H \in \mathscr{H}(G)$ and $H_i' = [G, a_i]$.

We now compute V_{H_i}, $1 \leqq i \leqq p + 1$: if $i > m$, we may pick a_j, a_k with i, j, k distinct; then by Lemma 1(ii)

$$V_{H_i}(a_j) \equiv a_j^p (\text{mod } H_i') \quad \text{and} \quad V_{H_i}(a_k) \equiv a_k^p (\text{mod } H_i').$$

But since a_j^p, $a_k^p \in Z$ (one way to see this is by noting G/Z has class $\leqq p - 1$, whence is regular, and a_p^p, $a_{p+1}^p \in Z$) and by Lemma 6(v) $Z \leqq H_i'$, we have $G = \langle a_j, a_k \rangle \leqq \ker V_{H_i}$, as desired. Now for $i \leqq m$ observe that since $m \leqq p - 2$, a_p, $a_{p+1} \notin H_i$, so by Lemma 1(ii)

$$V_{H_i}(a_p) \equiv a_p^p (\text{mod } H_i') \quad \text{and} \quad V_{H_i}(a_{p+1}) \equiv a_{p+1}^p (\text{mod } H_i').$$

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

By definition of a_p, a_{p+1}

$$(7.3) \quad a_1 \equiv a_{p+1}a_p^{-1} (\text{mod } G'),$$
$$a_j \equiv a_{p+1}{}^j a_p{}^{1-j} (\text{mod } G'), \quad 2 \leqq j \leqq p + 1.$$

Computing V_{H_i} by using (7.3) and the fact that V_{H_i} is a homomorphism whose kernel contains G' gives:

$$(7.4) \quad V_{H_i}(a_1) \equiv \zeta (\text{mod } H_i'),$$
$$V_{H_i}(a_j) \equiv \zeta^{j-2}\xi (\text{mod } H_i'), \quad 2 \leqq j \leqq p + 1.$$

Recall that

$$H_i' \cap Z = Z_1 \times \ldots \times Z_{i-1} \times Z_{i+1} \times \ldots \times Z_m,$$

so by (7.1) $\zeta \not\equiv 1 (\text{mod } H_i')$ unless $i = 1$ and $n_0 > 0$, in which case

$$V_{H_i}(a_2) \equiv \xi \not\equiv 1 (\text{mod } H_i').$$

Thus for $1 \leqq i \leqq m$, V_{H_i} is not the trivial homomorphism.

We demonstrate ker $V_{H_i} = H_i$, $1 \leqq i \leqq n_0$: for this it suffices to show

$$V_{H_i}(a_i) \equiv 1 (\text{mod } H_i').$$

If $i = 1$, (7.1) and (7.4) ensure this. If $2 \leqq i \leqq n_0$,

$$V_{H_i}(a_i) \equiv (z_2{}^{i-2}z_3{}^{i-2} \ldots z_m{}^{i-2})(z_1{}^{+1}z_3{}^{-1} \ldots z_{n_0}{}^{-(n_0-2)}) (\text{mod } H_i'),$$
$$\equiv 1 (\text{mod } H_i'),$$

as desired.

Finally, it remains to see that for $n_0 < i \leqq m$, ker $V_{H_i} \neq H_i$: if $i = 1$, we must have $n_0 = 0$ whence

$$V_{H_i}(a_1) = \zeta \equiv z_1{}^{\epsilon} \equiv z_1 (\text{mod } H_1');$$

if $i = 2$, we must have $n_0 \leqq 1$, whence

$$V_{H_2}(a_2) \equiv \xi \equiv z_2{}^{\delta} \equiv z_2 (\text{mod } H_2');$$

if $i \geqq 3$, since z_i appears to the zero power in ξ,

$$V_{H_i}(a_i) \equiv \zeta^{i-2} \equiv z_i{}^{i-2} (\text{mod } H_i').$$

This completes the proof of the lemma.

Before summarizing the field theoretic consequences of Lemmas 5 and 7 we repeat a definition from [**11**]: if K is a number field, $\mathfrak{U}$ a subgroup of order p (p any prime) in the ideal class group of K, H the subgroup of Gal$(K^{(1)}/K)$ given by $\mathfrak{U}$ under the Artin map φ_K, and L the fixed field of H, say $\mathfrak{U}$ (and H) are of type (A) if every ideal in $\mathfrak{U}$ becomes principal in L. In light of Lemma 2 this may be interpreted as follows: let $G =$ Gal$(K_p{}^{(2)}/K)$ and let $H_0 =$ Gal$(K_p{}^{(2)}/L)$; then H (or H_0) is of type (A)

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

if and only if the kernel of the transfer $G \to H_0/H_0'$ contains H_0. In this terminology Lemma 5 and Lemma 7 immediately yield

THEOREM 4. *If p is a prime $\geqq 5$, then for each $n \in \{0, 1, \ldots, p+1\}$ there is a p-group G with $G/G' \cong Z_p \times Z_p$, G' abelian such that if K is a number field with* $\mathrm{Gal}(K_p^{(2)}/K) \cong G$, *then K has p-capitulation number n; moreover, if $n \geqq 3$, for any $n_0 \in \{0, 1, \ldots, p+1-n\}$ such G exists with the additional property that if* $\mathrm{Gal}(K_p^{(2)}/K) \cong G$, *then of the $p+1-n$ intermediate fields L_i, $K \subsetneqq L_i \subsetneqq K_p^{(1)}$, which do not have the principal p-ideal property, exactly n_0 are of type (A).*

4. A conjecture and some implications.

Let p be a prime $\geqq 5$, $n \in \{0, 1, \ldots, p+1\}$, $\mathscr{K}_n = \{K | K$ is a number field with $\mathrm{Gal}(K_p^{(2)}/K) \in \mathscr{G}_n\}$. Although there are infinitely many fields with $\mathrm{Gal}(K_p^{(1)}/K)$ of type (p, p) (see [**5**]), little is understood of the individual $\mathscr{K}_n$, and, in particular, how n affects $[K_p^{(2)} : K]$. The insight accrued from the proofs in Section 3 and from an examination of the p-groups of small order motivate us to conjecture

(C1) for $n \in \{0, 1, \ldots, p+1\}$ and $K \in \mathscr{K}_n$,

$$[K_p^{(2)} : K_p^{(1)}] \geqq \min\{\tfrac{1}{2}(n+1)(n+2), \tfrac{1}{2}(p+1-n)(p+4-n)\}.$$

The advantage of having such a result in hand would be that the size of $[K_p^{(2)} : K_p^{(1)}]$ could be forced to be "large" if its p-capitulation number were "close to $(p+1)/2$"; moreover, access to the p-capitulation number of K can be achieved by a knowledge of the degree p extensions of K without going to the degree p^2 extension $K_p^{(1)}$.

A similar statement to (C1) which, instead of $|\mathrm{Gal}(K_p^{(2)}/K_p^{(1)})|$ asserts a lower bound for the rank of $\mathrm{Gal}(K_p^{(2)}/K_p^{(1)})$ could also be formulated but the value is more uncertain; the conjectured value for $[K_p^{(2)} : K_p^{(1)}]$ may be too large. If some lower bound, d_n, for this rank could be established, one could, for example, apply a Golod–Shafarevich type theorem to $K_p^{(1)}$ [**2**, Chapter IX, Theorem 3], to show if $K \in \mathscr{K}_n$ and $[K : \mathbf{Q}] < ((d_n - 2)/2p)^2$, then K has an infinite p class field tower (whose first stage has degree only p^2). A similar idea has been successfully exploited in [**9**].

Finally, if one were able, by other techniques, to decide $\mathscr{K}_n = \emptyset$, for some $n \in \{0, 1, \ldots, p+1\}$, this would force the existence of a counterexample to the conjecture that every p group is isomorphic to

$$\mathrm{Gal}(L_p^{(m)}/L),$$

for some $m \geqq 0$ and some number field L.

REFERENCES

1. E. Artin, *Ideal Klassen in Oberkörpern und allgemeines Reziprozitatsgesetz*, Abh. Math. Sem. Univ. Hamburg 7 (1930), 46–51.

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press

2. J. Cassels and A. Fröhlich, *Algebraic number theory*, Chapter IX (Academic Press, London, 1967).

3. S. M. Chang, *Capitulation problems in algebraic numberfields*, Ph.D. thesis, University of Toronto (1977).

4. P. Furtwängler, *Beweis der Hauptidealsatzes fur Klassenkörper algebraischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg *7* (1930), 14–36.

5. F. Gerth, *Number fields with prescribed l-class groups*, Proc. Amer. Math. Soc. *49* (1975), 284–288.

6. D. Gorenstein, *Finite groups* (Harper and Row, New York, 1968).

7. M. Hall, *The theory of groups* (Macmillan, New York, 1959).

8. H. Kisilevsky, *Number fields with class number congruent to* 4 mod 8 *and Hilbert's Theorem* 94, J. Number Theory *3* (1976), 271–279.

9. N. Matsumara, *On the class field tower of an imaginary quadratic number field*, Mem. Fac. Sci. Kyushu Univ. *31* (1977), 165–171.

10. A. Scholz and O. Taussky, *Die Hauptideale der Kubischen Klassenkörper imaginärquadratischer Zahlkörper*, J. Reine Angew, Math. *171* (1934), 19–41.

11. O. Taussky, *A remark concerning Hilbert's Theorem* 94, J. Reine Angew. Math. *239/240* (1970), 435–438.

12. H. Zassenhaus, *The theory of groups* (Chelsea, New York, 1949).

University of Toronto,
Toronto, Ontario;
University of Minnesota,
Minneapolis, Minnesota

https://doi.org/10.4153/CJM-1980-091-9 Published online by Cambridge University Press