Comm. in Alg. **21(5)** (1993), 1603-1609.

ON REDUCTION OF p-GROUPS

Leila Schneps

U.R.A. 741 du CNRS, Laboratoire de Mathématiques
Faculté des Sciences de Besançon
25030 Besançon Cedex

ABSTRACT

We define the notion of irreducibility of a p-group and show how any p-group G can be reduced to an irreducible group H. We show that G is realizable as the Galois group of a regular extension of $\mathbb{Q}(T)$ if H is. Finally, we give some sufficient conditions on the number of generators of a p-group and the structure of its Frattini subgroup for it to be reducible to the trivial group.

*

§1. Reduction of p-groups

Let p be a fixed prime, and let G be a p-group of order p^n. We recall several equivalent definitions of the Frattini subgroup $\Phi(G)$ of G:

(i) $\Phi(G)$ is the intersection of all the maximal subgroups of G,

(ii) $\Phi(G)$ is the subgroup of G generated by all p-th powers of elements in G together with the commutator subgroup of G,

(iii) $\Phi(G)$ is the set of *non-generators* of G, i.e. $\Phi(G)$ consists of elements $x \in G$ having the following property: if H is a subgroup of G such that G is generated by x and H, then $G = H$.

The Frattini subgroup is a normal subgroup of G. Suppose $|\Phi(G)| = p^m$. By definition (ii), $G/\Phi(G)$ is an elementary abelian p-group of rank $n - m$. We define $g = n - m$: g is the cardinal of any minimal set of generators for G.

Definition: A p-group G is *irreducible* if all of its abelian normal subgroups lie inside $\Phi(G)$.

We define the notion of "reducibility" in the opposite way: G is *reducible* if it has a (not necessarily proper) abelian normal subgroup A not lying in $\Phi(G)$.

The basic idea of this article is to study the number of generators and the structure of the Frattini subgroup of a p-group in order to obtain information about its reducibility and in particular, the possibility of reducing it down to the trivial group. We are basically concerned with considering p-groups as semi-direct and partial semi-direct products with abelian kernel. In some cases we may use the notation $G = A \rtimes H$ even when H (resp. A) is the trivial group: then $G = A$ (resp. H).

We recall that a group G is a *partial semi-direct product* of A and H_1 if $G = AH_1$ where A is a normal subgroup of G and H_1 is a proper subgroup (cf. [G]). Such a group is always a quotient of the usual semi-direct product $A \rtimes H_1$ where the action of H_1 on A is the one given by conjugation in G. For any semi-direct product $A \rtimes H$, we can define exactly which quotients give partial semi-direct products AH_1: they can be constructed as follows. For each element $h \in H_1$, let ψ_h be the corresponding automorphism of A. Let M be a subgroup of H_1 and suppose that M' is a subgroup of A which is isomorphic to M: let $\phi : M \to M'$ be the isomorphism and for $m \in M \subset K$ write $m' = \phi(m) \in M' \subset A$. Suppose in addition that for each $m \in M$, ψ_m is the automorphism of A given by conjugation by m', and for each $h \in H_1$, $\psi_{h^{-1}mh}$ is the automorphism of A given by conjugation by $h^{-1}m'h$. Let D be the subgroup of $A \rtimes H_1$ given by $\{m'm^{-1} \mid m \in M\}$. Then D is a normal subgroup of $A \rtimes H_1$ and $(A \rtimes H_1)/D$ is a partial semi-direct product AH_1 such that $A \cap H_1 \simeq M$.

We note that a partial semi-direct product AH_1 is actually a semi-direct product $A \rtimes H_1$ if and only if $A \cap H_1 = 1$, and that a quotient of $A \rtimes H_1$ which is a partial semi-direct product AH_1 is particular in that it contains subgroups isomorphic to A and H_1, for by the definition of D we have $D \cap A = 1$ and $D \cap H_1 = 1$.

Definition: Let H be an irreducible p-group. The *class* $\mathcal{C}_H$ is the smallest set of p-groups (for a fixed prime p) defined by the following rules:

(i) H is in $\mathcal{C}_H$

(ii) $\mathcal{C}_H$ is closed under partial semi-direct products of the form AH_1 where A is an abelian group and H_1 is in $\mathcal{C}_H$.

Lemma 1: *(i) Every element G of a class $\mathcal{C}_H$ contains H as a subgroup.*

(ii) H is the unique irreducible member of $\mathcal{C}_H$.

Proof: (i) This is obvious for an element of $\mathcal{C}_H$ is formed by a finite sequence of partial semi-direct products with abelian kernel, beginning with H, and every step thus contains H as a subgroup.

(ii) Suppose G is an irreducible group belonging to $\mathcal{C}_H$. Then G is formed by a finite sequence of partial semi-direct products starting with H. We may suppose that such a sequence has no trivial steps, i.e. partial semi-direct products $G = AK$ such that $A \subset \Phi(G)$, i.e. $G = AK = K$. In particular any group G in $\mathcal{C}_H$ except for H can be written as a non-trivial semi-direct product AH_1 for some H_1 in $\mathcal{C}_H$. But if G is irreducible, then since A is an abelian normal subgroup of G, we must have $A \subset \Phi(G)$, so $G = AH_1 = H_1$ and the semi-direct product is trivial. This is a contradiction unless $G = H$.

Definition: A *reduction procedure* for a p-group $G = H_0$ is a sequence of non-trivial abelian subgroups $A_1, \ldots, A_k$ and a sequence of subgroups $H_1 \supset \cdots \supset H_k$ such that H_k is irreducible and for $1 \leq i \leq k$, A_i is normal in H_{i-1} and H_{i-1} is a partial semi-direct product $A_i H_i$.

Definition: An irreducible group which can be reached by a reduction procedure on a p-group G is called a *reduced group* for G.

It is a consequence of Lemma 1 that a p-group G can never belong to a class $\mathcal{C}_H$ where $|H| > |G|$, so G belongs at most to a finite number of classes $\mathcal{C}_H$. By the definition of a reduction procedure, G belongs to the class $\mathcal{C}_H$ if and only if H is a reduced group for G: a reduction procedure is just the inverse of the process used to build up groups in the class $\mathcal{C}_H$.

We now give a condition on the possibility of a p-group G having the trivial group as reduced group.

Lemma 2: *If G has an irreducible quotient K, and G belongs to the class $\mathcal{C}_H$, then H has a quotient isomorphic to K.*

Proof: If G is itself irreducible, then it is clear. Suppose that G is reducible and $A_1, \ldots, A_k$ and $H_1, \ldots, H_k$ form a reduction procedure for G. Then G is a quotient of $A_1 \rtimes H_1$, so $A_1 \rtimes H_1$ has an irreducible quotient isomorphic to K, say $K \simeq (A_1 \rtimes H_1)/N$. But

$A_1/(A_1 \cap N)$ is an abelian normal subgroup of K, so it is contained in $\Phi(K)$, so in fact $K \simeq H_1/(H_1 \cap N)$, so K is a quotient of H_1. But H_1 is a quotient of $A_2 \rtimes H_2$, so by the same reasoning, K is a quotient of H_2, and in fact of H_i for every i. In particular K is a quotient of $H_k = H$.

Corollary: *If G has an irreducible quotient then G does not belong to the class $\mathcal{C}_1$.*

Remark 3: All abelian p-groups have trivial reduced groups. Also, all 2-groups of order ≤ 32 have trivial reduced groups: this can be proved by direct calculation. There are exactly 10 irreducible groups of order 64, all having abelian Frattini subgroups of order 16. In general, all p-groups of order less than or equal to p^4 have trivial reduced groups, but there exist irreducible groups of order p^5 for all $p \neq 2$ (cf. [D]).

Examples of irreducible groups

(1) For $p = 2$, we give three irreducible 2-groups of orders 64 and 128 all having abelian Frattini subgroups (of orders 16 or 32). Let $G = H \rtimes C_8$ where $H \simeq D_4 \times C_2$. Let H be generated by elements a, b and c with $a^2 = b^2 = c^2 = 1$, $(ab)^2 = -1$, $(a, b) = -1$, $(a, c) = 1$, $(b, c) = 1$. Let the C_8 factor be generated by an element d with $d^8 = 1$, which acts on H via the relations $(d, a) = abc$, $(d, b) = -ab$ and $(d, c) = 1$. Then $|G| = 128$ and G is irreducible. The Frattini subgroup of G is abelian of order 32 (in fact, a minimal set of generators for G has only 2 elements).

Let G_1 be the quotient of G by the subgroup $\{1, cd^4\}$. Then $|G_1| = 64$ and G_1 is irreducible, with abelian Frattini subgroup of order 16. Another irreducible group G_2 of order 64 is obtained by taking the quotient of G by the subgroup $\{1, -cd^4\}$.

(2) We give an example of an irreducible group of order p^5 for $p \neq 2$, due to Ralf Dentzer (cf. [D]). Let G be generated by a, b, c and d such that $a^{p^2} = b^p = c^p = d^p = 1$, $(a, b) = d$, $(c, a^{-1}) = a^p bd$, $(c, b^{-1}) = a^p$ and $(a, d) = (b, d) = (c, d) = 1$. Then $|G| = p^5$ and G is irreducible.

(3) (Universal p-groups). For any p-group G, we define the descending central p-sequence for G by $G \supset G_1 \supset G_2 \supset \cdots$, where each $G_{i+1} = G_i^p(G, G_i)$ (here (G, G_i) denotes the set of commutators of elements of G with elements of G_i, and $G_0 = G$). Note that $G_1 = \Phi(G)$. Clearly if G is finite then the sequence is finite: in this case we say m is the *length* of G if m is the smallest integer such that $G_m = 1$.

For $n \geq 1$, let F_n be the free group on n generators and let $F_n \supset F_{n,1} \supset F_{n,2} \supset \cdots$ be its descending central p-sequence. Define the *universal group of length m on n generators* by $F(m, n) = F_n/F_{n,m}$. This group is a finite p-group of length m on n generators and has the property that every p-group on n generators of length m is a quotient of it.

It is known (cf. [D]) that $F(2, n)$ belongs to $\mathcal{C}_1$ for all $n \geq 1$, so these groups are

always reducible. Consider the group $F(3,2)$ for $p = 2$. It is an irreducible 2-group of order 1024, with abelian Frattini subgroup of order 256. This shows in particular that every 2-group on 2 generators of length at most 3 (such as the groups in example (1)) has an abelian Frattini subgroup.

§2. On p-groups with small Frattini subgroups

We begin by giving a criterion for reducibility of a p-group.

Lemma 4: *Let $|G| = p^n$, and let m be the unique integer such that $(m^2 - m)/2 < n \leq (m^2 + m)/2$. Then there exists a normal abelian subgroup A in G such that $|A| \geq p^m$. In particular, if G is irreducible, then $|\Phi(G)| \geq p^m$.*

Proof: This is equivalent to the following theorem (Huppert [H, III, Satz 7.3]): if $|G| = p^n$, then any maximal abelian subgroup A of G has order p^a with $2n \leq a(a+1)$.

Lemma 5: *If $|\Phi(G)| = p^m$ and $|G| > p^{(m^2+m)/2}$, then G is reducible.*

Proof: By Lemma 4, there exists an abelian normal subgroup A in G of order at least p^{m+1}, since $2n > m^2 + m = m(m+1)$.

Lemma 6: *If G is irreducible with $|\Phi(G)| = p^m$, and $p^{(m^2-m)/2} < |G| \leq p^{(m^2+m)/2}$, then $\Phi(G)$ is abelian.*

Proof: By Lemma 4, G contains an abelian normal subgroup A of order at least p^m. If G is irreducible, then A is in $\Phi(G)$ so it is equal to $\Phi(G)$.

A consequence of Lemmas 4 to 6 is that an irreducible p-group cannot have order greater than $p^{(m^2+m)/2}$ if p^m is the order of its Frattini. We saw in Lemma 1 that every group G in a class $\mathcal{C}_H$ contains H as a subgroup, and therefore, since G is a p-group, we must have $\Phi(H) \subset \Phi(G)$. In particular, if a p-group G has a Frattini subgroup of order p^m, we have a bound on the order of its reduced groups. We state this in the following Lemma.

Lemma 7: *Let G be a p-group and let p^m be the order of its Frattini subgroup. Then a reduced group H of G must satisfy $|H| \leq p^{(m^2+m)/2}$.*

From now on we introduce the following notation to distinguish the cases $p = 2$ and $p \neq 2$: set $\epsilon = 0$ if $p = 2$ and $\epsilon = 1$ if $p \neq 2$.

Theorem 8: *Let $\mathcal{G}_{n,m}$ be a the set of p-groups of order p^n whose Frattini subgroups are*

of order p^m (so $0 \leq m \leq n$). Then

(i) If $n \leq 5 - \epsilon$, then all groups in $\mathcal{G}_{m,n}$ are in $\mathcal{C}_1$.

(ii) If $0 \leq m \leq 3 - \epsilon$ or $n - 1 \leq m \leq n$, then again, all groups in $\mathcal{G}_{n,m}$ are in $\mathcal{C}_1$.

(iii) If $m = 4 - \epsilon$ and $G \in \mathcal{G}_{m,n}$ has a non-abelian Frattini subgroup, then G is in $\mathcal{C}_1$.

(iv) If $4 - \epsilon \leq m \leq n - 2$ then there exist groups in $\mathcal{G}_{n,m}$ which are not in $\mathcal{C}_1$.

Proof: (i) was mentioned in Remark 3 (cf. [D]).

(ii) Obviously if $m = n$ then $G = 1$, and if $m = 0$ then G is elementary abelian. If $m = n - 1$ then G has only one generator so it is cyclic. Let $1 \leq m \leq 3 - \epsilon$ and let H be a reduced group for G. If $m = 1$ or $m = 2$ then by Lemma 4, $|H| \leq p^3$ so by Remark 3, $H = 1$ and G is in $\mathcal{C}_1$. If $p = 2$ and $m = 3$ then $|H| \leq 2^6$. By Remark 3, if $H \neq 1$ then H has order 64 and an abelian Frattini subgroup of order 16. But $H \subset G$ so $\Phi(H) \subset \Phi(G)$, and $|\Phi(G)| = 2^3$, so this is impossible and we must have $H = 1$.

(iii) Suppose $m = 4 - \epsilon$ and let H be a reduced group for G. Then $|H| \leq (m^2 + m)/2$ and $\Phi(H) \subset \Phi(G)$. If $|\Phi(H)| \leq p^{3-\epsilon}$ then $H = 1$ and G is in $\mathcal{C}_1$. If $|\Phi(H)| = p^{4-\epsilon}$ then $\Phi(H) = \Phi(G)$. But then $\Phi(H)$ is abelian by Lemma 6, which contradicts the assumption on $\Phi(G)$.

(iv) Whenever $n \geq 6 - \epsilon$ we construct a p-group G of order p^n with exactly $n - 4 + \epsilon$ generators not belonging to $\mathcal{C}_1$. By Remark 3, when $p \neq 2$ there exist irreducible groups H of order p^5 whose Frattini subgroups must have order exactly p^3, for the Frattini cannot be smaller by Lemma 5, and if it were of order p^4 then G would have only one generator and would be cyclic. Also by Remark 3, there exist irreducible groups H of order 2^6 whose Frattini subgroups are of order 16. We take G to be a direct product $A \times H$ where H is irreducible of order p^5 (resp. 2^6) and A is elementary abelian of order p^{n-5} (resp. 2^{n-6}). Then G has $n-3$ generators if $p \neq 2$ and $n-4$ if $p = 2$. But $G/A \simeq H$ so by the corollary to Lemma 2, G cannot be in $\mathcal{C}_1$.

We remark that the condition $|\Phi(G)| \leq p^{3-\epsilon}$ implies in particular that G can contain elements of order at most $p^{4-\epsilon}$.

§3. p-groups as Galois groups over $\mathbb{Q}(T)$

A regular extension of $\mathbb{Q}(T)$ is an extension of $\mathbb{Q}(T)$ containing no algebraic extension of $\mathbb{Q}$ larger than $\mathbb{Q}$ itself. We say that a finite group G has the property Gal_T if it is realizable as the Galois group of a regular extension of $\mathbb{Q}(T)$.

The following theorem (see [M, Kap. IV, §3, Satz 2]) gives a condition for a semi-direct product with abelian kernel to have the property Gal_T.

Theorem 9: *Let $G = A \rtimes H_1$ be a semi-direct product with abelian kernel. Then G is realizable as the Galois group of a regular extension of $\mathbb{Q}(T)$ if and only if H_1 is.*

We obtain the following result on p-groups:

Theorem 10: *A p-group G has the property Gal_T if a reduced group H of G does. In particular, if G is in $\mathcal{C}_1$ then G has the property Gal_T.*

Proof: If G has a reduction procedure leading to H then there is a finite sequence of partial semi-direct products $H_{i+1} = A_i H_i$ with A_i abelian, $H = H_1$ and $G = H_k$ for some k. But if H_i has the property Gal_T, then every partial semi-direct product with abelian kernel $A_i H_i$ does, for $A_i H_i$ is a quotient of $A_i \rtimes H_i$ which has Gal_T by Theorem 9, and if a group has Gal_T then so do all of its quotients.

The following theorem is a corollary to Theorems 8 and 10 (recall that $\epsilon = 0$ if $p = 2$ and $\epsilon = 1$ if $p \neq 2$).

Theorem 11: *Let G be a p-group of order p^n and let g be the number of its generators, so $|\Phi(G)| = p^{n-g}$. Then G has the property Gal_T under either of the following conditions:*

(i) $g = 1$ or $n - 3 + \epsilon \leq g \leq n$,

(ii) $g = n - 4 + \epsilon$ and $\Phi(G)$ is not abelian.

ACKNOWLEDGMENTS

I would like to thank Ralf Dentzer for suggesting that all p-groups of a given order having "enough" generators ought to fall into a certain class of p-groups known to be Galois groups. I also thank the ETH Zürich for its hospitality and financial support during the preparation of this article.

REFERENCES

[D] R. Dentzer. On split embedding problems with abelian kernel, to appear.

[G] D. Gorenstein. Finite Groups. Harper & Row, New York- Evanston-London 1968.

[H] B. Huppert. Endliche Gruppen I. Springer-Verlag, Berlin- Heidelberg-New York 1967.

[M] B.H. Matzat. Konstruktive Galoistheorie. *LNM* Vol. **1284**, Berlin: Springer 1987.