An introduction to finite p-groups: regular p-groups and groups of maximal class

Gustavo A. Fernández-Alcober

Matematika Saila
Euskal Herriko Unibertsitatea
Bilbao (Spain)
E-mail: mtpfealg@lg.ehu.es

XVI Escola de Álgebra

Brasília, July 2000

Contents

Introduction

In the pages that follow, I present the notes of the course I gave in the XVI Escola de Álgebra, held in Brasília in July of 2000. The aim of this course is to introduce the reader to the beautiful theory of finite p-groups, with special emphasis on two important families: those of regular p-groups and of p-groups of maximal class. The course is addressed to postgraduate students and the only prerequisite assumed is some basic knowledge of Group Theory.

The wild behaviour of finite p-groups is well-known and it prevents any attempt at a general classification. In fact, only the p-groups of order at most p^6 have been completely classified for a general prime p (see [9]). This can be extended [23] to the groups of order less than or equal to 2^8 in the case $p = 2$. This situation has naturally led to restricting the study of p-groups to particular families. For this reason, after introducing the most basic properties of general finite p-groups in Lecture 1, I have decided to focus on the two families mentioned above as a way of getting the flavour of how one works with p-groups. The choice of these two specific families has been more than a matter of personal taste. On the one hand, we have nowadays quite complete theories for both regular p-groups and p-groups of maximal class. Even if these theories are not elementary at all, it is possible to develop them from scratch in a course of this length and level. On the other hand, these two types of groups have played an important role in the theory of finite p-groups, since the results obtained for them have suggested generalizations that have contributed to a better understanding of arbitrary p-groups. Thus the knowledge of the classical families of regular p-groups and p-groups of maximal class is a good starting point for any student interested in doing research in finite p-groups, before going into more recent achievements, such as the theory of powerful p-groups or the study of p-groups according to their coclass. There is a third reason to include these two families together in a course like this, which is that the development of the theory of p-groups of maximal class depends essentially at some critical points on properties of regular p-groups. This will be clear in Lecture 4.

Although the results presented in the course are well-known, the organization of the material reflects the particular viewpoint of the author and differs at some places from the exposition of this subject that is currently available in textbooks or research papers. Moreover, several proofs have been modified or rewritten. Among them, I would like to point out the proof of Theorem 3.2, which has been substantially shortened. Also, an emphasis has been laid on trying to substitute the use of an associated Lie ring for cumbersome group commutator calculations. All of this results, I believe, in a simplified account of these important theories. On the other hand, I have included at the end of every lecture a set of exercises intended for the reader to practise the new concepts that have been introduced. I strongly recommend trying to do these exercises.

I would like to take this opportunity to thank the organizers of the XVI Escola de Álgebra for inviting me to give this course and for their hospitality during my visit to Brasília. I would also like to express my thanks to my colleagues Andrei Jaikin-Zapirain and Leire Legarreta for reading parts of the manuscript and drawing some errors to my attention.

Bilbao
October 2000

Gustavo A. Fernández-Alcober

Lecture 1

Fundamental facts about p-groups and central series

1.1 Finite p-groups

Recall that a finite p-group is a group whose order is a power of p, where p is a prime. The key to the fundamentals of the theory of finite p-groups is the following fact, which will allow us to use inductive arguments in the proofs.

Theorem 1.1. *Let G be a finite p-group and N a non-trivial normal subgroup of G. Then $N \cap Z(G) \neq 1$. In particular, the centre of a non-trivial p-group is non-trivial.*

Proof. Since N is normal in G, G acts on N by conjugation. We have that $|\operatorname{Orb}_G(n)| = |G : C_G(n)|$ for any $n \in N$ and G is a p-group, hence the length of each orbit is a power of p. Furthermore, the orbits of length one correspond to the elements in N which commute with every element in G, that is, to $N \cap Z(G)$. Since N is the disjoint union of its orbits, it follows that

$$|N| = |N \cap Z(G)| + \sum_{i=1}^{r} |\operatorname{Orb}_G(n_i)|,$$

where $n_1, \ldots, n_r$ are representatives of the orbits of length greater than one. By reducing this last equality modulo p and taking into account that $|N| > 1$, we get that

$$|N \cap Z(G)| \equiv 0 \pmod p$$

and consequently $N \cap Z(G) \neq 1$. $\square$

Corollary 1.2. *Let G be a finite p-group. Then any normal subgroup of G of order p is central in G.*

The following consequence of Theorem 1.1 has also great importance in the theory of finite p-groups.

Theorem 1.3. *Let G be a finite p-group.*

(i) *If $H < G$ then $H < N_G(H)$. **(The normalizer condition.)***

(ii) *If M is a maximal subgroup of G then M is normal in G and $|G : M| = p$.*

Proof. (i) We argue by induction on $|G|$. The result is obvious when $|G| = p$, so we suppose that $|G| > p$. If $Z(G)$ is not contained in H then $H < HZ(G) \leq N_G(H)$ and we are done. So we may assume that $Z(G) \leq H$. Since $Z(G) \neq 1$, the induction hypothesis yields that $H/Z(G) < N_{G/Z(G)}(H/Z(G)) = N_G(H)/Z(G)$ and consequently $H < N_G(H)$.

(ii) If M is maximal in G, we obtain from (i) that $N_G(M) = G$, that is, $M \trianglelefteq G$. Then the factor group G/M is a p-group without non-trivial subgroups. It follows that G/M has order p and $|G : M| = p$. □

Our next result shows that the subgroups of a p-group are rather well situated.

Theorem 1.4. *Let G be a finite p-group of order p^m.*

(i) *If N is a normal subgroup of G of order p^k, then there is a series*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_k = N \leq \cdots \leq G_m = G \tag{1.1}$$

such that $G_i \trianglelefteq G$ and $|G_{i+1} : G_i| = p$ for all i. In particular, a p-group has normal subgroups of every possible order.

(ii) *If H is a subgroup of G of order p^k, then there is a series*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_k = H \leq \cdots \leq G_m = G \tag{1.2}$$

such that $G_i \trianglelefteq G_{i+1}$ and $|G_{i+1} : G_i| = p$ for all i. Thus every subgroup of a p-group is subnormal.

Proof. (i) We argue by induction on $|G|$. Suppose first that $N \neq 1$. Then Theorem 1.1 yields that $Z = N \cap Z(G) \neq 1$. Choose any subgroup G_1 in Z of order p. Then G_1 is normal in G and the result follows by applying the induction hypothesis to G/G_1 for the normal subgroup N/G_1. Finally, if $N = 1$ then we may take (1.1) to be any of the series obtained from the previous argument.

(ii) We use induction on $|G|$. If $H = G$ then we may use part (i) to obtain the series we seek. Otherwise H is contained in a maximal subgroup M of G and the induction hypothesis yields a series such as (1.2) whose last term is M. Since we know from Theorem 1.3 that $M \trianglelefteq G$, the proof is complete. □

For a finite group G, the intersection of its maximal subgroups is called the *Frattini subgroup* of G and is denoted by $\Phi(G)$. Since the image of a maximal subgroup under an automorphism of G is again a maximal subgroup, $\Phi(G)$ is a characteristic subgroup of G. One of the reasons why this subgroup plays an important role is the following result.

Theorem 1.5. *Let G be a finite group and $x_1, \ldots, x_n \in G$. Then we have that $G = \langle x_1, \ldots, x_n \rangle$ if and only if $G/\Phi(G) = \langle x_1\Phi(G), \ldots, x_n\Phi(G) \rangle$.*

Proof. Clearly, it suffices to prove the "if" part of the theorem. If $\langle x_1, \ldots, x_n \rangle$ does not equal G then it is contained in a maximal subgroup M of G. But then $\langle x_1\Phi(G), \ldots, x_n\Phi(G) \rangle$ is contained in $M/\Phi(G)$, which is a proper subgroup of $G/\Phi(G)$. Thus necessarily $G = \langle x_1, \ldots, x_n \rangle$. $\square$

When G is a finite p-group, the Frattini subgroup determines the minimal number of generators of G.

Theorem 1.6 (Burnside's Basis Theorem)**.** *Let G be a finite p-group. Then:*

(i) *$G/\Phi(G)$ is an elementary abelian p-group and consequently it may be viewed as a vector space over $\mathbb{F}_p$.*

(ii) *The set $\{x_1, \ldots, x_d\}$ is a minimal generating set of G if and only if $\{x_1\Phi(G), \ldots, x_d\Phi(G)\}$ is a basis of $G/\Phi(G)$.*

(iii) *The minimal number d of generators of the group G coincides with the dimension of $G/\Phi(G)$ as an $\mathbb{F}_p$-vector space. In other words, $|G : \Phi(G)| = p^d$.*

Proof. (i) We have to prove that $x\Phi(G)y\Phi(G) = y\Phi(G)x\Phi(G)$ and $(x\Phi(G))^p = \Phi(G)$ for all $x, y \in G$, that is, that $x^{-1}y^{-1}xy$, $x^p \in \Phi(G)$. By the definition of $\Phi(G)$, it suffices to see that $x^{-1}y^{-1}xy$, $x^p \in M$ for any maximal subgroup M of G. This is obvious since, according to Theorem 1.3, G/M is a group of order p.

(ii) From the previous theorem we have that $S = \{x_1, \ldots, x_d\}$ is a generating set of G if and only if $\overline{S} = \{x_1\Phi(G), \ldots, x_d\Phi(G)\}$ is a generating set of $G/\Phi(G)$. Hence S is a minimal generating set if and only if $\overline{S}$ is, which amounts to $\overline{S}$ being a basis of $G/\Phi(G)$.

(iii) This is immediate from (ii). $\square$

If G is a finite group, we will denote by $d(G)$ the minimal number of generators of G.

1.2 Commutators and commutator subgroups

The *commutator* of two elements x, y of a group G is defined by

$$[x,y] = x^{-1}y^{-1}xy = x^{-1}x^y,$$

so that x and y commute if and only if $[x,y]=1$. For commutators of length greater than 2, we keep the left-normed convention, so that

$$[x_1,x_2,x_3,\ldots,x_{n-1},x_n] = [[\ldots[[x_1,x_2],x_3],\ldots,x_{n-1}],x_n].$$

More generally, *higher commutators* in $x_1,\ldots,x_n$ are defined recursively as follows:

(i) Commutators in $x_1,\ldots,x_n$ are higher commutators.

(ii) Any commutator whose components are higher commutators is also a higher commutator.

The length of a higher commutator is the number of its components, that is, the length of the list of elements x_i that one gets after deleting brackets in the higher commutator. Thus

$$[[x,y],[y,z],x] \qquad \text{and} \qquad [x,[y,[y,z],x]]$$

are higher commutators of length 5 in x, y, z.

We define the commutator subgroup of two subgroups H and K of G by means of

$$[H,K] = \langle [h,k] \mid h\in H,\ k\in K\rangle,$$

and similarly for $[H_1,H_2,\ldots,H_n]$ and higher commutator subgroups. We collect the main properties of commutators and commutator subgroups in our next result.

Theorem 1.7. *Let G be a group, $x,y,z\in G$ and $H,K,L\le G$. Then:*

(i) $[y,x]=[x,y]^{-1}$.

(ii) $[x,y]^\sigma = [x^\sigma,y^\sigma]$ *for any homomorphism* $\sigma: G\to G^*$.

(iii) $[xy,z]=[x,z][x,z,y][y,z]$ *and* $[x,yz]=[x,z][x,y][x,y,z]$.

(iv) $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x=1$. *(Witt's Identity.)*

(v) $[H,K]=[K,H]$.

(vi) *K normalizes H if and only if $[H,K] \leq H$, and K centralizes H if and only if $[H,K] = 1$.*

(vii) *$[H,K]^\sigma = [H^\sigma, K^\sigma]$ for any homomorphism $\sigma : G \to G^*$. In particular, the commutator subgroup of two characteristic (normal) subgroups of G is again characteristic (normal).*

(viii) *If N is a normal subgroup of G then $[HN/N, KN/N] = [H,K]N/N$.*

(ix) *If HK is a subgroup of G and H normalizes L then $[HK,L] = [H,L][K,L]$.*

Proof. Parts (i) through (iv) are easily checked by expanding the commutators involved. As for (v), note that

$$\begin{aligned}[K,H] &= \langle [k,h] \mid k \in K,\, h \in H \rangle = \langle [h,k]^{-1} \mid k \in K,\, h \in H \rangle \\ &= \langle [h,k] \mid h \in H,\, k \in K \rangle = [H,K].\end{aligned}$$

Now (vi) is obvious and (vii) is a consequence of (ii). Also, (viii) is immediate from (vii) if we consider σ to be the natural epimorphism from G onto G/N.

So we are only left with proving (ix). It is clear that $[H,L][K,L] \leq [HK,L]$. For the reverse inclusion, let us first see that $[H,L][K,L]$ is a subgroup. Observe that, for any $k \in K$ and $l, l' \in L$,

$$[k,l]^{l'} = [k,l][k,l,l'] = [k,l']^{-1}[k,ll'] \in [K,L],$$

by part (iii). Hence L normalizes $[K,L]$. Since H normalizes L, $[H,L]$ also normalizes $[K,L]$ and, in particular, $[H,L][K,L]$ is a subgroup. Now that we know this, in order to prove that $[HK,L]$ is contained in this subgroup, it suffices to see that any generator $[hk,l]$ lies there. Since $[hk,l] = [h,l][h,l,k][k,l]$ and $[h,l,k] \in [H,L,K] \leq [L,K] = [K,L]$, the result follows. □

Theorem 1.8 (Three subgroup lemma)**.** *Let H, K and L be subgroups of G and N a normal subgroup of G. If $[H,K,L], [K,L,H] \leq N$ then $[L,H,K] \leq N$.*

Proof. We may work in the factor group G/N and thus assume that $N = 1$. Since $[H,K,L] = [K,L,H] = 1$, it follows from Witt's Identity that $[l,h^{-1},k] = 1$ for all $h \in H$, $k \in K$ and $l \in L$. By substituting h^{-1} for h we obtain that $[l,h,k] = 1$. Since $[L,H]$ is generated by the commutators $[l,h]$, it follows that $[L,H,K] = 1$. □

The *lower central series* of a group G is defined inductively by means of $\gamma_1(G) = G$ and $\gamma_{i+1}(G) = [\gamma_i(G), G]$. It follows from (vii) in Theorem 1.7 that $\gamma_i(G)$ is characteristic in G for all i. The following is one of the most important properties of this series.

Theorem 1.9. *For any group G, $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$.*

Proof. We argue by induction on i. The result for $i = 1$ is a consequence of the definition of the lower central series. When $i \geq 2$ the induction hypothesis yields that $[\gamma_{i-1}(G), \gamma_j(G), G] \leq [\gamma_{i+j-1}(G), G] = \gamma_{i+j}(G)$ and $[\gamma_j(G), G, \gamma_{i-1}(G)] = [\gamma_{j+1}(G), \gamma_{i-1}(G)] \leq \gamma_{i+j}(G)$. Then we deduce from the three subgroup lemma that $[\gamma_i(G), \gamma_j(G)] = [G, \gamma_{i-1}(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$. □

Corollary 1.10. *Let G be a group. Then any higher commutator of elements of G whose length is i lies in the subgroup $\gamma_i(G)$.*

Proof. This is clear from Theorem 1.9 and the definition of higher commutators, by induction on i. □

We will very frequently use the following consequence of (viii) in Theorem 1.7.

Theorem 1.11. *Let G be a group and let N be a normal subgroup of G. Then $\gamma_i(G/N) = \gamma_i(G)N/N$ for all $i \geq 1$.*

1.3 Nilpotent groups

A group G is called *nilpotent* if $\gamma_{c+1}(G) = 1$ for some c. The smallest such c is then called the *nilpotency class* of G. For instance, the nilpotent groups of class one are precisely the abelian groups. From the definition of the lower central series, it is clear that the higher the class of a nilpotent group is, the further the group is from being abelian.

Next we see that the property of being nilpotent may be characterized in terms of a different series of G, which is called the *upper central series* of G and is defined recursively by means of $Z_0(G) = 1$ and $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. Observe that $[H, G] \leq Z_i(G)$ if and only if $H \leq Z_{i+1}(G)$.

Lemma 1.12. *Let G be a nilpotent group of class c. Then $\gamma_{c+1-i}(G) \leq Z_i(G)$ for all $0 \leq i \leq c$.*

Proof. This follows by induction on i. If $i = 0$ then $\gamma_{c+1}(G) = 1 = Z_0(G)$ and the result holds. On the other hand,

$$[\gamma_{c+1-i}(G), G] = \gamma_{c+1-(i-1)}(G) \leq Z_{i-1}(G),$$

by the induction hypothesis, and consequently $\gamma_{c+1-i}(G) \leq Z_i(G)$. □

Theorem 1.13. *A group G is nilpotent of class c if and only if $Z_c(G) = G$ and $Z_{c-1}(G) \neq G$.*

Proof. First of all, observe that $Z_c(G) = G$ implies that $\gamma_2(G) = [Z_c(G), G] \leq Z_{c-1}(G)$, $\gamma_3(G) \leq [Z_{c-1}(G), G] \leq Z_{c-2}(G)$, and eventually $\gamma_{c+1}(G) \leq Z_0(G) = 1$. Thus G is nilpotent of class $\leq c$. On the other hand, according to the previous lemma, if G is nilpotent of class c then $\gamma_1(G)$ is contained in $Z_c(G)$ and therefore $Z_c(G) = G$. Now the result follows from these two remarks. $\square$

Thus the class of a nilpotent group is the length of both its upper and lower central series.

Corollary 1.14. *Any finite p-group is nilpotent.*

Proof. Let G be a finite p-group. Suppose that, for some index i, we have that $Z_i(G) \neq G$. Then $G/Z_i(G)$ is a non-trivial p-group and Theorem 1.1 yields that $Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$ is also non-trivial. Hence $Z_i(G) < Z_{i+1}(G)$. So, as far as it does not reach G, the upper central series is strictly increasing. Since G is finite, this means that this series must reach G some time and, according to Theorem 1.13, G is nilpotent. $\square$

If G has order p^m, the proof of the previous corollary shows in fact that G has nilpotency class $\leq m$. This can be sharpened a bit as follows.

Theorem 1.15. *Let G be a p-group of order $p^m \geq p^2$. Then:*

(i) *The nilpotency class of G is at most $m - 1$.*

(ii) *If G has nilpotency class c then $|G : Z_{c-1}(G)| \geq p^2$.*

(iii) $|G : G'| \geq p^2$.

Proof. Let c be the nilpotency class of G. We begin by proving (ii). Suppose by way of contradiction that $|G : Z_{c-1}(G)| = p$. If $c = 1$ this means that $|G| = p$, contrary to our assumption. Hence $c \geq 2$ and

$$\frac{G/Z_{c-2}(G)}{Z(G/Z_{c-2}(G))} = \frac{G/Z_{c-2}(G)}{Z_{c-1}(G)/Z_{c-2}(G)} \cong \frac{G}{Z_{c-1}(G)}$$

is a cyclic group. Consequently $G/Z_{c-2}(G)$ is abelian* and $Z_{c-1}(G) = G$, which is a contradiction. This proves (ii). Now (iii) is a consequence of Lemma 1.12, which assures that $G' \leq Z_{c-1}(G)$.

Finally, since the series

$$G = Z_c(G) > Z_{c-1}(G) > \cdots > Z(G) > Z_0(G) = 1$$

has c steps, it follows from (ii) that $p^m = |G| \geq p^{c+1}$. Hence $c \leq m - 1$ and (i) holds. $\square$

*Remember that a group G is abelian if $G/Z(G)$ is cyclic.

Corollary 1.16. *Let G be a p-group and let N be a normal subgroup of G of index $p^i \geq p^2$. Then $\gamma_i(G) \leq N$.*

Proof. The group G/N has order $p^i \geq p^2$. It follows from part (i) of Theorem 1.15 that G/N has class $\leq i-1$ and consequently $\gamma_i(G/N) = \overline{1}$. Since $\gamma_i(G/N) = \gamma_i(G)N/N$, this proves that $\gamma_i(G) \leq N$. □

Definition 1.17. We say that a p-group of order $p^m \geq p^2$ is a *p-group of maximal class* if it has nilpotency class $m - 1$.

Of course, any group of order p^2 and any non-abelian p-group of order p^3 have maximal class. We provide more examples of groups of maximal class in Exercise 1.7. The final part of this course will be devoted to the study of the p-groups of maximal class and we will be able to give rather precise information about their general structure.

1.4 The Lie ring associated to the lower central series

The difficulty in the study of groups comes mainly from the fact that the multiplication need not be commutative. Nevertheless, as part (iii) in Theorem 1.7 shows, commutation is close to being bilinear. Also, part (iv) in the same theorem resembles the Jacobi identity. This suggests a way of relating groups to Lie rings. We first recall the definition of a Lie ring.

Definition 1.18. Let L be a set endowed with two operations, written $+$ and $[\ ,\ ]$. We say that $(L, +, [\ ,\ ])$ is a *Lie ring* if the following conditions hold:

(i) $(L, +)$ is an abelian group.

(ii) $[\ ,\ ]$ is bilinear: $[x + y, z] = [x, z] + [y, z]$ and $[x, y + z] = [x, y] + [x, z]$ for all $x, y, z \in L$.

(iii) $[x, x] = 0$ for any $x \in L$.

(iv) The Jacobi identity holds: $[x, y, z] + [y, z, x] + [z, x, y] = 0$ for all $x, y, z \in L$. (The product of more than two elements is defined via the left-normed convention.)

Moreover, if L is a vector space over a field K and $[\lambda x, y] = \lambda[x, y] = [x, \lambda y]$ for all $\lambda \in K$, $x, y \in L$, we say that L is a *Lie K-algebra*.

We refer to $[\ ,\ ]$ as the *Lie product* or *Lie commutator* in L. Observe that, as a consequence of (ii) and (iii),

$$0 = [x + y, x + y] = [x, x] + [x, y] + [y, x] + [y, y] = [x, y] + [y, x]$$

and hence $[y, x] = -[x, y]$ for any $x, y \in L$.

Let us now explain how we may associate to any group G a Lie ring $L(G)$ by using the lower central series. Set $L_i = \gamma_i(G)/\gamma_{i+1}(G)$ for $i \geq 1$, which is an abelian group, since $\gamma_i(G)' \leq [\gamma_i(G), G] = \gamma_{i+1}(G)$. We use additive notation in this group, instead of the more natural multiplicative one. Thus $x\gamma_{i+1}(G) + y\gamma_{i+1}(G) = xy\gamma_{i+1}(G)$. Then we may define a product $[\ ,\ ]$ in the direct sum

$$L(G) = \bigoplus\nolimits_{i \geq 1} L_i$$

in the following way. Define first the product of two elements $x\gamma_{i+1}(G) \in L_i$, $y\gamma_{j+1}(G) \in L_j$ by means of

$$[x\gamma_{i+1}(G), y\gamma_{j+1}(G)] = [x, y]\gamma_{i+j+1}(G) \in L_{i+j}.$$

(Observe that $[x, y] \in \gamma_{i+j}(G)$ according to Theorem 1.9.) This definition does not depend on the choice of the representatives x and y of the cosets, since

$$\begin{aligned}[xt, yu] &\equiv [x, yu][x, yu, t][t, yu] \equiv [x, yu] \\ &\equiv [x, u][x, y][x, y, u] \equiv [x, y] \pmod{\gamma_{i+j+1}(G)}\end{aligned}$$

for any $t \in \gamma_{i+1}(G)$, $u \in \gamma_{j+1}(G)$. Then we extend the definition of $[\ ,\ ]$ to all of $L(G)$ by linearity.

We say that an element in $L(G)$ is *homogeneous* if it belongs to some L_i, that is, if it is of the form $x\gamma_{i+1}(G)$ with $x \in \gamma_i(G)$.

Theorem 1.19. *Let G be any group. Then $L(G)$ is a Lie ring.*

Proof. We have to prove conditions (ii), (iii) and (iv) in the definition of a Lie ring. Let us begin by (ii). Choose arbitrary homogeneous elements $x\gamma_{i+1}(G), y\gamma_{i+1}(G) \in L_i$ and $z\gamma_{j+1}(G) \in L_j$. Then

$$\begin{aligned}[x\gamma_{i+1}(G) + y\gamma_{i+1}(G), z\gamma_{j+1}(G)] &= [xy\gamma_{i+1}(G), z\gamma_{j+1}(G)] = [xy, z]\gamma_{i+j+1}(G) \\ &= [x, z][x, z, y][y, z]\gamma_{i+j+1}(G) \\ &= [x, z][y, z]\gamma_{i+j+1}(G) \\ &= [x, z]\gamma_{i+j+1}(G) + [y, z]\gamma_{i+j+1}(G), \\ &= [x\gamma_{i+1}(G), z\gamma_{j+1}(G)] + [y\gamma_{i+1}(G), z\gamma_{j+1}(G)]\end{aligned} \tag{1.3}$$

since $[x, z, y] \in [\gamma_i(G), \gamma_j(G), \gamma_i(G)] \leq \gamma_{i+j+1}(G)$. Analogously,

$$[z\gamma_{j+1}(G), x\gamma_{i+1}(G) + y\gamma_{i+1}(G)] = [z\gamma_{j+1}(G), x\gamma_{i+1}(G)] + [z\gamma_{j+1}(G), y\gamma_{i+1}(G)]. \tag{1.4}$$

Now for generic elements $a, b, c \in L(G)$, we can decompose them as the sum of their homogeneous components and the relations $[a+b, c] = [a, c] + [b, c]$ and $[c, a+b] = [c, a] + [c, b]$ follow immediately from (1.3), (1.4) and the definition of the Lie product in $L(G)$.

For the proof of (iii), we observe that

$$[x\gamma_{i+1}(G), x\gamma_{i+1}(G)] = [x, x]\gamma_{2i+1}(G) = \gamma_{2i+1}(G) = 0$$

and

$$\begin{aligned}[x\gamma_{i+1}(G), y\gamma_{j+1}(G)] &= [x, y]\gamma_{i+j+1}(G) = [y, x]^{-1}\gamma_{i+j+1}(G) = -[y, x]\gamma_{i+j+1}(G) \\ &= -[y\gamma_{j+1}(G), x\gamma_{i+1}(G)]\end{aligned}$$

for any $x \in \gamma_i(G)$, $y \in \gamma_j(G)$. Then we can decompose any $a \in L(G)$ as the sum of its homogeneous components, $a = \sum_{i \geq 1} a_i$, to get that

$$\begin{aligned}[a, a] &= \Big[\sum_{i\geq 1} a_i, \sum_{i\geq 1} a_i\Big] = \sum_{i,j\geq 1} [a_i, a_j] \\ &= \sum_{i<j} ([a_i, a_j] + [a_j, a_i]) + \sum_{i\geq 1} [a_i, a_i] = 0.\end{aligned}$$

In order to prove the Jacobi identity, it also suffices to consider homogeneous elements. Take $x\gamma_{i+1}(G) \in L_i$, $y\gamma_{j+1}(G) \in L_j$ and $z\gamma_{k+1}(G) \in L_k$. Witt's Identity yields that

$$\begin{aligned}1 &= [x, y^{-1}, z][x, y^{-1}, z, y][y, z^{-1}, x][y, z^{-1}, x, z][z, x^{-1}, y][z, x^{-1}, y, x] \\ &\equiv [x, y^{-1}, z][y, z^{-1}, x][z, x^{-1}, y] \pmod{\gamma_{i+j+k+1}(G)}.\end{aligned} \tag{1.5}$$

On the other hand, the bilinearity of the Lie product shows that

$$\begin{aligned}[x, y^{-1}]\gamma_{i+j+1}(G) &= [x\gamma_{i+1}(G), y^{-1}\gamma_{j+1}(G)] = [x\gamma_{i+1}(G), -y\gamma_{j+1}(G)] \\ &= -[x, y]\gamma_{i+j+1}(G)\end{aligned}$$

and consequently

$$\begin{aligned}[x, y^{-1}, z]\gamma_{i+j+k+1}(G) &= [[x, y^{-1}]\gamma_{i+j+1}(G), z\gamma_{k+1}(G)] \\ &= -[[x, y]\gamma_{i+j+1}(G), z\gamma_{k+1}(G)] = -[x, y, z]\gamma_{i+j+k+1}(G).\end{aligned}$$

Hence (1.5) yields that

$$\begin{aligned}0 &= [x, y, z]\gamma_{i+j+k+1}(G) + [y, z, x]\gamma_{i+j+k+1}(G) + [z, x, y]\gamma_{i+j+k+1}(G) \\ &= [x\gamma_{i+1}(G), y\gamma_{j+1}(G), z\gamma_{k+1}(G)] + [y\gamma_{j+1}(G), z\gamma_{k+1}(G), x\gamma_{i+1}(G)] \\ &\quad + [z\gamma_{k+1}(G), x\gamma_{i+1}(G), y\gamma_{j+1}(G)],\end{aligned}$$

which proves the Jacobi identity. $\square$

The Lie ring $L(G)$ is especially important when the group G is nilpotent: in that case $\gamma_{c+1}(G) = 1$ for some c and therefore

$$L(G) = L_1 \oplus L_2 \oplus \cdots \oplus L_c.$$

There are many applications of the ring $L(G)$ to problems related to nilpotent groups; E.I. Khukhro's book [10] and Chapter VIII of the book [8] by B. Huppert and N. Blackburn are good references. The advantage of passing from a group G to its associated Lie ring $L(G)$ comes from the fact that it is easier to work with the Lie product in $L(G)$ than with commutators in G. We give a couple of easy examples of this method in Exercises 1.10 and 1.11. The results there could also be obtained directly, but it is simpler to prove them by working in the associated Lie ring.

Exercises

1.1. Prove that any group of order p^2 is abelian.

1.2. Let G be a finite p-group of order $\geq p^2$.

(i) Prove that $|C_G(x)| \geq p^2$ for any $x \in G$.

(ii) Prove that $|C_G(x)| \geq |C_{G/N}(xN)|$ for any $x \in G$. (Hint: Write the order of the centralizer as the quotient of the order of the group by the size of the corresponding conjugacy class.*)

(iii) Deduce that the property of having an element x such that $|C_G(x)| = p^2$ is hereditary for factor groups of order $\geq p^2$.

1.3. Let G be a group and let X be an arbitrary generating set of G. Prove that

$$G' = \langle [x,y]^g \mid x,y \in X,\ g \in G \rangle.$$

(Hint: Call N the subgroup to the right of the equality above. Then N is normal in G and G/N is abelian.)

1.4. Let G be a group and H a subgroup of G such that $G' = H'$. Prove that $\gamma_i(G) = \gamma_i(H)$ for all $i \geq 2$. (Hint: Argue by induction on i. Observe that $\gamma_{i+1}(G) = [\gamma_{i-1}(H), H, G]$ and use the three subgroup lemma.)

1.5. Let G be a finite group. In this problem we prove that

$$\gamma_i(G) = \langle [x_1,\dots,x_i] \mid x_1,\dots,x_i \in G \rangle \tag{1.6}$$

for all $i \geq 1$.

---

* We are showing in fact that this property holds in any finite group.

(i) Prove that $N_i = \langle [x_1, \ldots, x_i] \mid x_1, \ldots, x_i \in G \rangle$ is a normal subgroup of G.

(ii) Suppose that (1.6) holds for i. Prove that $\gamma_i(G/N_{i+1})$ is central in G/N_{i+1} and deduce that $\gamma_{i+1}(G)$ is contained in N_{i+1}. Conclude that (1.6) holds also for $i+1$. Hence the result is always true.

1.6. Prove by induction on i that

$$Z_i(G) = \{g \in G \mid [g, x_1, \ldots, x_i] = 1 \text{ for all } x_1, \ldots, x_i \in G\}.$$

1.7. Prove that the following 2-groups have maximal class:

(i) The dihedral groups: $D_{2^m} = \langle a, b \mid a^{2^{m-1}} = b^2 = 1,\ a^b = a^{-1} \rangle, \quad m \geq 3.$

(ii) The semidihedral groups: $SD_{2^m} = \langle a, b \mid a^{2^{m-1}} = b^2 = 1,\ a^b = a^{-1+2^{m-2}} \rangle$, $m \geq 4$.

(iii) The generalized quaternion groups: $Q_{2^m} = \langle a, b \mid a^{2^{m-1}} = 1,\ a^{2^{m-2}} = b^2,\ a^b = a^{-1} \rangle, \quad m \geq 3.$

1.8. We say that a Lie ring L is *abelian* if $[x, y] = 0$ for any $x, y \in L$. If G is a group, prove that $L(G)$ is abelian if and only if $\gamma_2(G) = \gamma_3(G)$. Deduce that if G is nilpotent then $L(G)$ is abelian if and only if G is abelian.

1.9. Let G be any group and $L(G) = \oplus_{i \geq 1} L_i$ its associated Lie ring. Prove that $[L_i, L_1] = L_{i+1}$ for all $i \geq 1$. (If A and B are subgroups of a Lie ring L, $[A, B]$ is defined as the subgroup generated by all Lie products $[a, b]$ where $a \in A$ and $b \in B$.)

1.10. Let G be a group. If $G/G' = \langle x_1 G', \ldots, x_s G' \rangle$ and $\gamma_i(G)/\gamma_{i+1}(G) = \langle y_1 \gamma_{i+1}(G), \ldots, y_t \gamma_{i+1}(G) \rangle$ then

$$\gamma_{i+1}(G)/\gamma_{i+2}(G) = \langle [x_j, y_k] \gamma_{i+2}(G) \mid j = 1, \ldots, s,\ k = 1, \ldots, t \rangle.$$

(Hint: Work in $L(G)$ and use Exercise 1.9. Produce also a proof without considering $L(G)$.)

1.11. Let G be any group.

(i) Suppose that every element in the factor group $\gamma_i(G)/\gamma_{i+1}(G)$ has order a divisor of n. Prove that the same is true for all the quotients $\gamma_j(G)/\gamma_{j+1}(G)$ for $j \geq i$. (Hint: Working in the Lie ring $L(G)$, it suffices to see that $nL_j = 0$. By Exercise 1.9, L_j is generated by elements of the form $[a, b]$ where $a \in L_{j-1}$, $b \in L_1$. Use induction on j. How does the proof read if we do not use the associated Lie ring?)

(ii) If G is nilpotent and is generated by elements of p-power order, deduce from (i) that every element in G has p-power order. Does this property hold for soluble groups?

1.12. Let G be a nilpotent group generated by elements $x_1, \ldots, x_d$ of finite order. In this exercise we prove that G is then finite. (Observe that this is obvious if G is abelian.)

(i) Let n be the least common multiple of the orders of $x_1, \ldots, x_d$. Prove that any element of $\gamma_i(G)/\gamma_{i+1}(G)$ has order dividing n for any $i \geq 1$. (Recall the previous exercise.)

(ii) Deduce that all the quotients $\gamma_i(G)/\gamma_{i+1}(G)$ are finite. (Hint: According to Exercise 1.10, $\gamma_i(G)/\gamma_{i+1}(G)$ is a finitely generated abelian group.)

(iii) Use the nilpotency of G to deduce that G is finite.

(iv) What is the maximum possible order of a nilpotent group of class 3 generated by two elements of order p?

(v) Prove that the group

$$D_\infty = \langle x, y \mid y^2 = 1,\ x^y = x^{-1} \rangle$$

is an infinite soluble group generated by 2 elements of order 2.

Lecture 2

Basic properties of regular p-groups

2.1 The subgroups $\Omega_i(G)$ and $\mho_i(G)$

In this section we introduce two series of subgroups which are meaningful in the study of the power structure of a p-group. The subgroups of these series are defined as follows.

Definition 2.1. Let G be a finite p-group. For any $i \geq 0$ we define

$$\Omega_i(G) = \langle x \in G \mid x^{p^i} = 1 \rangle,$$

that is, the subgroup generated by the elements of G whose order is $\leq p^i$ and

$$\mho_i(G) = \langle x^{p^i} \mid x \in G \rangle.$$

(The symbol $\mho$ is read "agemo", that is, the letters of the word "omega" in reverse order, which reflects what happens with the symbols.)

It is clear that both $\Omega_i(G)$ and $\mho_i(G)$ are characteristic subgroups of G. On the other hand, according to Theorem 1.6, $G/\Phi(G)$ is an elementary abelian group and consequently $x^p \in \Phi(G)$ for any $x \in G$. Thus $\mho_1(G) \leq \Phi(G)$. Our next result clarifies the relation between $\Phi(G)$ and $\mho_1(G)$.

Theorem 2.2. *Let G be a finite p-group. Then:*

(i) $\Phi(G)$ *is the smallest subgroup N of G such that G/N is elementary abelian.*

(ii) $\Phi(G) = G'\mho_1(G)$.

Proof. (i) We already know from Theorem 1.6 that $G/\Phi(G)$ is elementary abelian. Suppose now that the quotient G/N is elementary abelian. Then G/N may be viewed as an $\mathbb{F}_p$-vector space and consequently the intersection of its maximal subgroups is trivial (for any non-zero vector v there is a maximal subspace not containing v). Since a maximal subgroup of G/N is of the form M/N with M maximal in G, it follows that the intersection of the maximal subgroups of G containing N equals N. This proves that $\Phi(G) \le N$.

(ii) A factor group G/N is elementary abelian if and only if $[x, y] \in N$ and $x^p \in N$ for any $x, y \in G$, that is, if and only if $G'\mho_1(G) \le N$. It follows from (i) that $\Phi(G) = G'\mho_1(G)$. ☐

Recall that the *exponent* of a group G, written $\exp G$, is the least common multiple of the orders of its elements. In the case of a p-group, this is simply the maximum order of the elements of G. If $\exp G = p^e$ then $x^{p^e} = 1$ for all $x \in G$, so that $\Omega_e(G) = G$. Thus we have an ascending series

$$1 = \Omega_0(G) \le \Omega_1(G) \le \cdots \le \Omega_{e-1}(G) \le \Omega_e(G) = G, \tag{2.1}$$

which we call the Ω-*series* of G. Similarly, $\mho_e(G) = 1$ and we have the following descending series,

$$G = \mho_0(G) \ge \mho_1(G) \ge \cdots \ge \mho_{e-1}(G) \ge \mho_e(G) = 1, \tag{2.2}$$

which is referred to as the $\mho$-*series* of G.

The $\mho$-series of a p-group is strictly decreasing, since

$$\mho_{i+1}(G) \le \mho_1(\mho_i(G)) \le \Phi(\mho_i(G)) < \mho_i(G)$$

as long as $\mho_i(G) \ne 1$. Thus the $\mho$-series of a p-group of exponent p^e has exactly e steps. Nevertheless the inclusions in the Ω-series need not be proper. Consider for instance the dihedral 2-group $D_{2^m} = \langle a, b \mid a^{2^{m-1}} = b^2 = 1,\ a^b = a^{-1} \rangle$ for $m \ge 3$. It may be generated by two elements of order 2, ab and b, whence $\Omega_1(D_{2^m}) = D_{2^m}$ and the Ω-series of D_{2^m} reduces to two terms, even if $\exp D_{2^m} = 2^{m-1}$.

When the p-group G is abelian, the subgroups $\Omega_i(G)$ and $\mho_i(G)$ are particularly well behaved.

Theorem 2.3. *Let G be a finite abelian p-group. For any $i \ge 0$ we have that:*

(i) $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.

(ii) $\mho_i(G) = \{x^{p^i} \mid x \in G\}$.

(iii) $|G : \Omega_i(G)| = |\mho_i(G)|$ *(and consequently also $|G : \mho_i(G)| = |\Omega_i(G)|$).*

Proof. The map $f : G \to G$ defined by $f(x) = x^{p^i}$ is a homomorphism, since G is abelian. The set $\{x \in G \mid x^{p^i} = 1\}$ is the kernel of f and is consequently a subgroup of G. Since $\Omega_i(G)$ is generated by this set, we deduce that (i) holds. Part (ii) follows similarly by observing that the image of f is a subgroup. Finally, by the first isomorphism theorem $|G : \operatorname{Ker} f| = |\operatorname{Im} f|$ and this proves (iii). $\square$

The first isomorphism theorem shows in fact that $G/\Omega_i(G) \cong \mho_i(G)$ in any abelian p-group. In Exercise 2.1 we will prove that $G/\mho_i(G) \cong \Omega_i(G)$ also holds.

None of the statements in the last theorem remains true for general finite p-groups. We have already mentioned that $\Omega_1(D_{2^m}) = D_{2^m}$, while not all elements of D_{2^m} have order 2. On the other hand, if $G = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1}\rangle$ then the set of squares of the elements of G is $\{1, a^2, b^2\}$, which is not a subgroup. Note also that part (iii) need not hold even if (i) and (ii) are true: we have that $|Q_8 : \Omega_1(Q_8)| = 4 \neq |\mho_1(Q_8)| = 2$. In Exercises 2.3 and 2.4 and in Section 3.2 of the next lecture we provide examples like these for any prime.

Let us end this section by indicating two general properties of the subgroups $\Omega_i(G)$ and $\mho_i(G)$.

Theorem 2.4. *Let G be a finite p-group.*

(i) *If $\exp G = p^e$ then $\mho_i(G) \le \Omega_{e-i}(G)$.*

(ii) *For any $N \trianglelefteq G$, $\mho_i(G/N) = \mho_i(G)N/N$.*

Proof. (i) It suffices to observe that any generator x^{p^i} of $\mho_i(G)$ has order $\le p^{e-i}$.

(ii) Use the bar notation in $\overline{G} = G/N$. Then

$$\mho_i(\overline{G}) = \langle \overline{x}^{p^i} \mid \overline{x} \in \overline{G}\rangle = \langle \overline{x^{p^i}} \mid x \in G\rangle = \overline{\mho_i(G)},$$

that is, $\mho_i(G/N) = \mho_i(G)N/N$. $\square$

2.2 Phillip Hall's compilation formula

The key to the proof of Theorem 2.3 is the fact that $x^n y^n = (xy)^n$ in any abelian group. Of course, this equality does not hold in general, but there is a remarkable formula of Phillip Hall that relates $x^n y^n$ to $(xy)^n$ in any group by using commutators in x and y. To begin with, let us consider the case $n = 2$. We have that

$$x^2y^2 = x(xy)y = x(yx[x,y])y = xyxy[x,y][x,y,y] = (xy)^2[x,y][x,y,y], \quad (2.3)$$

where we have used twice the identity $ab = ba[a,b]$. This simple fact is the key to any compilation formula: the effect of moving an element b one position to the left is the appearance of a commutator involving b. Note that (2.3) may be written as $x^2y^2 = (xy)^2c_2$, where $c_2 \in \langle x, y\rangle'$.

For $n = 3$, we observe that

$$\begin{aligned} x^3y^3 &= x(x^2y^2)y = x(xy)^2c_2y = x(xy)^2yc_2[c_2, y] \\ &= (xy)^3[(xy)^2, y]c_2[c_2, y]. \end{aligned} \tag{2.4}$$

By Theorem 1.7, we have that $[xy, y] = [x, y][x, y, y] = c_2$ and consequently

$$[(xy)^2, y] = c_2[c_2, xy]c_2 = c_2^2[c_2, xy][c_2, xy, c_2].$$

It follows from (2.4) that $x^3y^3 = (xy)^3c_2^3c_3$ for some element $c_3 \in \gamma_3(\langle x, y\rangle)$.

These calculations show the difficulty of handling the general case with an arbitrary value of n, at least with the same approach as with $n = 2$ and 3. Nevertheless we will be able to obtain an expression relating x^ny^n to $(xy)^n$ thanks to a very ingenious argument, which we take from Chapter 6 in [6] and which is based on the general rearrangement principle in Lemma 2.5 below.

Let $X = \{x_1, \dots, x_m\}$ be a finite sequence of elements in a group and let $p = x_1 \dots x_m$ be their product. (Just for this section p is not a prime!) Even if there may be repetitions among the elements x_i, we consider them to be distinguishable because of their different symbolic names.* We partition X into subsets $X_1, \dots, X_n$, and we want to reorder the elements in the product p so that the elements belonging to X_1 appear in the first place, then they are followed by the elements from X_2, and so on. This requires moving some elements to the left with changes of the form $ab = ba[a, b]$, which means that, apart from the elements $x_1, \dots, x_m$ themselves, in the expression for p there will appear commutators whose components are some of the x_i. For any subset S of $R = \{1, \dots, n\}$ with more than one element, denote by X_S the set of higher commutators whose components are exclusively drawn from the X_i with $i \in S$ and which have at least one component from each of these subsets. Then we have the following result.

Lemma 2.5. *Order the non-empty subsets of $R = \{1, \dots, n\}$ according to their size and, among the subsets of the same size, lexicographically. Then*

$$p = \prod_{\varnothing \neq S \subseteq R} q_S,$$

*For those with an acquaintance with the theory of free groups, it should be said that the natural setting for the result that follows is in fact the free group F freely generated by $x_1, \dots, x_m$. This makes clearer the argument in the text, since the elements in the product $p = x_1 \dots x_m$ are really different in that case. Then any rearrangement formula we derive for the product p can be transferred to products of elements in an arbitrary group, since the subgroup that these elements generate is a homomorphic image of F. This shows by the way that the formulas we obtain are universal, the same for all groups.

where the factors occur in the given ordering of the subsets of R and each q_S is a product of elements in X_S.

Proof. We begin by collecting to the left the elements in X_1. As observed above, this has the effect of producing commutators of the form $[a,b]$, where b belongs to X_1 and a does not. That is, $[a,b] \in X_{1i}$ for some $i \geq 2$. (We drop the brackets and the comma from the set $\{1,i\}$ for an easier notation.) Hence we may write $p = q_1 p'$, where q_1 is the product of the elements in X_1 and p' is a product of elements from the sets $X_2, \dots, X_n, X_{12}, \dots, X_{1n}$.

We continue by collecting to the left the elements in X_2 and next with the rest of the subsets X_S, according to the order established for the subsets S of R. Suppose that, at some stage, we have already moved left all the elements corresponding to the subsets X_T for the $T \subseteq R$ which are "smaller" than S. Then our next step is to collect the elements in X_S. For this purpose, we will have to carry out changes of the form $ab = ba[a,b]$, where $b \in X_S$ and $a \in X_T$ for some T "greater" than S. The new element appearing in the product p is the commutator $[a,b]$, which belongs to $X_{S\cup T}$. Since the subset $S \cup T$ is posterior to S in the ordering we have chosen for the subsets of R, we can ensure that:

(i) These changes do not alter the collection of elements we had obtained so far.

(ii) No new element of X_S arises when collecting to the left an element of X_S. Consequently the elements in X_S can be collected in a finite number of steps.

Since R has a finite number of subsets, this procedure eventually ends and we get the formula in the statement of the lemma. □

The proof of the lemma shows clearly that the elements $q_1, \dots, q_n$ in the above formula are the products of the elements in $X_1, \dots, X_n$, respectively, multiplied in the same order as they appear in the product $p = x_1 \dots x_m$. Nevertheless, it is impossible in practice to obtain general expressions for all of the q_S.

For any non-empty subset S of R, let p_S denote the product of the elements in the sets X_i, $i \in S$, in the same order as in $p = x_1 \dots x_m$. Equivalently, p_S is the result of substituting 1 in p for the elements in the sets X_i, $i \notin S$. Observe that, by Lemma 2.5,

$$p_S = \prod_{\varnothing \neq T \subseteq S} q_T, \tag{2.5}$$

since any higher commutator which has a component equal to 1 is itself equal to 1.

We may now proceed to prove the main result in this section.

Theorem 2.6 (Hall's Compilation Formula). *Let G be a group and $x, y \in G$. Then there exist elements $c_i = c_i(x,y) \in \gamma_i(\langle x,y\rangle)$ such that*

$$x^n y^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \dots c_n^{\binom{n}{n}}$$

for all $n \in \mathbb{N}$.

Proof. We compile the elements in the product $p = x^n y^n$ by choosing the set X_1 to consist of the first x and the first y appearing in p, X_2 of the second x and second y, and so on up to X_n. Set $R = \{1, \dots, n\}$. According to Lemma 2.5 we may write

$$x^n y^n = \prod_{\varnothing \neq S \subseteq R} q_S = (xy)^n \prod_{S \subseteq R,\ |S| \geq 2} q_S. \tag{2.6}$$

Let S be any subset of R with i elements. We have that $p_S = x^i y^i$ depends only on i and not on S. It follows from (2.5) and induction on i that the same is true for the q_S: all the q_S such that $|S| = i$ take a common value c_i. Furthermore, this value depends clearly only on i and not on n. Lemma 2.5 shows that c_i is a product of higher commutators in x, y of length at least i. It follows from Corollary 1.10 that $c_i \in \gamma_i(\langle x,y\rangle)$. Now R has $\binom{n}{i}$ subsets with i elements, hence each c_i appears this number of times in the expression (2.6). Since these occurrences of c_i are consecutive, we conclude that

$$x^n y^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \dots c_n^{\binom{n}{n}},$$

as desired. □

It follows from the comment in the footnote in page 18 that the formula in the previous theorem is universal and does not depend on the elements x, y, nor on the group G.

2.3 Definition and first properties of regular p-groups

Hall's compilation formula is specially meaningful when we use it with a prime exponent p, since the binomial coefficients $\binom{p}{i}$ are divisible by p for $1 \leq i \leq p-1$. Consequently, we may write $x^p y^p = (xy)^p z c_p$ for some element z which is a p-th power in $\langle x,y\rangle'$. This suggests the following definition.

Definition 2.7. Let G be a finite p-group. We say G is a *regular* p-group if $x^p y^p \equiv (xy)^p \pmod{\mho_1(\langle x,y\rangle')}$ for every $x, y \in G$. (Equivalently, if $c_p(x,y) \in \mho_1(\langle x,y\rangle')$ for every $x, y \in G$.)

The condition in the definition of a regular p-group is local, since it only involves the subgroup generated by x and y. Hence all subgroups and quotient groups of regular p-groups are again regular. Surprisingly, we will see in Exercise 2.7 that regularity is not maintained when taking direct products. The theory of regular p-groups is almost fully developed in P. Hall's fundamental paper on p-groups [5], where he introduces this concept. Other references for regular p-groups are Section 10 in Chapter III of Huppert's book [7] and Section 3 in Chapter 4 of Suzuki's second volume [26].

Of course, all abelian p-groups and all groups of exponent p are regular. If we want to produce further examples of regular p-groups, we run into the problem that the condition in their definition has to be checked for every pair of elements in the group, what may lead to cumbersome calculations. Our next result comes to our help and shows that, at least for odd p, the family of regular p-groups consists of many other groups than the ones mentioned above.

Theorem 2.8. *Let G be a finite p-group.*

(i) *If the class of G is less than p then G is regular. In particular, any p-group of order $\le p^p$ is regular.*

(ii) *If $\gamma_{p-1}(G)$ is cyclic then G is regular. Hence if $p > 2$ and G' is cyclic then G is regular.*

(iii) *A regular 2-group is abelian.*

Proof. (i) If G has class less than p then $\gamma_p(G) = 1$. Hence $\gamma_p(\langle x, y\rangle) = 1$ and $c_p(x, y) = 1$ for any $x, y \in G$, which proves the regularity of G.

(ii) Assume that $\gamma_{p-1}(G)$ is cyclic. If $p = 2$ then $G = \gamma_1(G)$ is cyclic and the result is obvious. Suppose now that $p > 2$. Choose any two elements $x, y \in G$ and put $H = \langle x, y\rangle$. Then $\gamma_{p-1}(H)$ is also cyclic. If $\gamma_{p-1}(H) \neq 1$ then $\gamma_p(H) < \gamma_{p-1}(H)$ and consequently

$$\gamma_p(H) \le \mho_1(\gamma_{p-1}(H)) \le \mho_1(H').$$

Hence $c_p(x, y) \in \mho_1(H')$ in this case. Otherwise $\gamma_{p-1}(H) = 1$ and $c_p(x, y) \in \gamma_p(H) = 1$. We conclude that G is a regular p-group.

(iii) Suppose G is a regular 2-group. Let $x, y \in G$ and write $H = \langle x, y\rangle$. We have from (2.3) that

$$x^2y^2 = (xy)^2[x, y][x, y, y] = (xy)^2[x, y]^y$$

and the regularity of G yields that $[x, y]^y \in \mho_1(H')$. Since $\mho_1(H')$ is normal in H, we also have that $[x, y] \in \mho_1(H')$. Then $H/\mho_1(H')$ is abelian and consequently

$$H' \le \mho_1(H') \le \Phi(H'),$$

by using Theorem 2.2. But this may only happen if $H' = 1$. Hence any two elements of G commute and G is abelian. $\square$

We will provide examples in Lecture 3 showing that a group of order p^{p+1} need not be regular.

In the rest of this section we prove the most basic properties of regular p-groups, which illustrate some similarities with abelian p-groups. In particular, Theorem 2.3 also holds for regular p-groups. These properties will be needed in Lecture 4 when we study the structure of the p-groups of maximal class.

Lemma 2.9. *Let G be a regular p-group and let $x, y \in G$. Then $x^p = y^p$ if and only if $(x^{-1}y)^p = 1$.*

Proof. We argue by induction on $|G|$. Set $H = \langle x, y \rangle$. Since G is regular, we may write $x^{-p}y^p = (x^{-1}y)^p z$ for some element $z \in \mho_1(H')$. Hence the equivalence claimed in the statement of the lemma will be proved if we show that $\mho_1(H') = 1$ whenever $x^p = y^p$ or $(x^{-1}y)^p = 1$. Of course, if H is abelian then there is nothing to prove, so we may assume that H is non-abelian.

Suppose first that $x^p = y^p$. Then y and x^p commute and consequently $x^p = (x^p)^y = (x^y)^p$. Since H is not cyclic, there is a maximal subgroup M of H containing x. But M is normal in H, so it also contains x^y. By applying the induction hypothesis to M, we deduce that $[x, y]^p = (x^{-1}x^y)^p = 1$. Now, we know from Exercise 1.3 that H' is generated by the elements of the form $[x, y]^h$ where $h \in H$, all of which have order dividing p. By the induction hypothesis, the lemma holds in H' and in particular the product of two elements of H' of order dividing p has again order dividing p. Hence $\mho_1(H') = 1$ in this case.

Assume now that $(x^{-1}y)^p = 1$. Conjugating by x^{-1} we obtain that also $(yx^{-1})^p = 1$. Then the implication already proved gives that $(xy^{-1}x^{-1}y)^p = 1$, that is, $[x^{-1}, y]^p = 1$. Since $H = \langle x^{-1}, y \rangle$, we conclude as above that $\mho_1(H') = 1$. $\square$

Theorem 2.10. *Let G be a regular p-group. Then:*

(i) *For any $x, y \in G$ and any $i \geq 0$, we have that $x^{p^i} = y^{p^i}$ if and only if $(x^{-1}y)^{p^i} = 1$.*

(ii) *For any $i \geq 0$, $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.*

(iii) *For any $i \geq 0$, $\mho_i(G) = \{x^{p^i} \mid x \in G\}$.*

(iv) *For any $i \geq 0$, $|G : \Omega_i(G)| = |\mho_i(G)|$ (and consequently also $|G : \mho_i(G)| = |\Omega_i(G)|$).*

Proof. First of all, observe that if (i) holds for a particular value of i, then the set $\{x \in G \mid x^{p^i} = 1\}$ is a subgroup and consequently it coincides with $\Omega_i(G)$. Hence (ii) follows from (i). Also, all the results are obvious for $i = 0$, so we may assume $i \geq 1$.

(i) By the previous lemma, we already know that this result holds when $i = 1$. Let us use induction on i. Then $x^{p^i} = y^{p^i}$ is equivalent to $(x^{-p}y^p)^{p^{i-1}} = 1$. Put $\overline{G} = G/\Omega_{i-1}(G)$. Since we are assuming that (i) holds for $i-1$, we also have that (ii) is valid for $i-1$ and $\Omega_{i-1}(G)$ consists exactly of the elements whose order divides p^{i-1}. Hence $x^{p^i} = y^{p^i}$ amounts to $\overline{x}^p = \overline{y}^p$. By using the result again for $i = 1$, this is equivalent to $(\overline{x}^{-1}\overline{y})^p = \overline{1}$, that is, to $(x^{-1}y)^p \in \Omega_{i-1}(G)$. Thus we conclude that $x^{p^i} = y^{p^i}$ if and only if $(x^{-1}y)^{p^i} = 1$, as desired.

(iii) We argue again by induction on i. Let us see that, given any $x, y \in G$, there exists $z \in G$ such that $x^p y^p = z^p$. This is clearly equivalent to (iii) for $i = 1$.

We use induction on $|G|$. Set $H = \langle x, y \rangle$ and $K = \langle xy, \Phi(H) \rangle$. If $K = H$ then H is cyclic and there is nothing to prove. So we may assume that $K < H$. Since G is regular, we have that $x^p y^p = (xy)^p c$ for some $c \in \mho_1(H') \leq \mho_1(K)$. Then $(xy)^p c$ is a product of two elements in $\mho_1(K)$ that, applying the induction hypothesis to K, can be written in the form z^p. Thus $x^p y^p = z^p$ and we are done.

For general i, observe that

$$\mho_1(\mho_{i-1}(G)) = \{x^p \mid x \in \mho_{i-1}(G)\} = \{x^{p^i} \mid x \in G\}$$

is a subgroup of G. Then necessarily $\mho_i(G) = \{x^{p^i} \mid x \in G\}$.

(iv) It follows from parts (i) and (ii) that $x^{p^i} = y^{p^i}$ if and only if $x^{-1}y \in \Omega_i(G)$, that is, if and only if $x\Omega_i(G) = y\Omega_i(G)$. Hence the map from $G/\Omega_i(G)$ to $\mho_i(G)$ given by $x\Omega_i(G) \mapsto x^{p^i}$ is well-defined and injective. But by part (iii) it is also surjective, hence a bijection. It follows that $|G : \Omega_i(G)| = |\mho_i(G)|$. □

It must be noted, however, that neither of the isomorphisms $G/\Omega_i(G) \cong \mho_i(G)$ and $G/\mho_i(G) \cong \Omega_i(G)$ need hold in a regular p-group. (See Exercise 2.6.)

Corollary 2.11. *If a regular p-group G is generated by elements of order $\leq p^e$ then* $\exp G \leq p^e$.

Proof. Let $G = \langle x_1, \ldots, x_d \rangle$, where each x_i has order $\leq p^e$. Then $x_1, \ldots, x_d \in \Omega_e(G)$ and consequently $G = \Omega_e(G)$. Since G is regular, it follows from part (ii) in Theorem 2.10 that every element in G has order $\leq p^e$ and $\exp G \leq p^e$. □

Corollary 2.12. *Let G be a regular p-group. Then the sequence of indices of the consecutive terms of the Ω- and $\mho$-series of G are the same, but in reverse order.*

Proof. Observe that

$$|\Omega_{i+1}(G) : \Omega_i(G)| = \frac{|G : \Omega_i(G)|}{|G : \Omega_{i+1}(G)|} = |\mho_i(G) : \mho_{i+1}(G)|,$$

by part (iv) in Theorem 2.10. □

2.4 Commutators and p-powers in regular p-groups

In this final section we show that there is a close relation between the commutator structure and the power structure in a regular p-group G. More precisely, we prove Theorem 2.14 below, which says that "agemos" (that is, p-powers) may be taken out of commutator subgroups of normal subgroups. In fact, we prove this result under the weaker condition that all proper (equivalently, maximal) subgroups of G are regular. This precision will be important in Section 3.1 of Lecture 3, where we provide a regularity criterion which is fundamental in the theory of p-groups of maximal class. The theorem relies on the following lemma.

Lemma 2.13. *Let G be a p-group all of whose proper subgroups are regular and let $x, y \in G$. Then for any $i, j \geq 0$ we have that $[x^{p^i}, y^{p^j}] = 1$ if and only if $[x, y]^{p^{i+j}} = 1$.*

Proof. First of all, observe that

$$[x^{p^i}, y] = x^{-p^i}(x^{p^i})^y = x^{-p^i}(x^y)^{p^i}.$$

Now

$$\langle x, x^y \rangle = \langle x, [x, y] \rangle \leq \langle x, G' \rangle \leq \langle x, \Phi(G) \rangle,$$

and this last subgroup is proper in G by Theorem 1.5 (unless G is cyclic, in which case the result holds trivially). Hence $\langle x, x^y \rangle$ is a regular p-group and we may use part (i) in Theorem 2.10 to obtain that $[x^{p^i}, y] = 1$ if and only if $[x, y]^{p^i} = (x^{-1}x^y)^{p^i} = 1$. Since taking the inverse of a commutator interchanges its two components, the same result holds if the p-power appears in the second component of the commutator. Now the lemma follows easily:

$$[x^{p^i}, y^{p^j}] = 1 \Leftrightarrow [x^{p^i}, y]^{p^j} = 1 \Leftrightarrow [x^{p^{i+j}}, y] = 1 \Leftrightarrow [x, y]^{p^{i+j}} = 1.$$

□

Theorem 2.14. *Let G be a p-group all of whose proper subgroups are regular and let M, N be normal subgroups of G. Then*

$$[\mho_i(M), \mho_j(N)] = \mho_{i+j}([M, N])$$

for any $i, j \geq 0$.

Proof. Consider the factor group $\overline{G} = G/\mho_{i+j}([M,N])$. In order to prove the inclusion $\subseteq$, it suffices to see that the image of $[\mho_i(M), \mho_j(N)]$ in $\overline{G}$ reduces to the trivial subgroup. This amounts to saying that the generators of $\mho_i(M)$ and $\mho_j(N)$ commute modulo $\mho_{i+j}([M,N])$, in other words, that $[\overline{m}^{p^i}, \overline{n}^{p^j}] = \overline{1}$. But, according to Lemma 2.13, this is equivalent to $[\overline{m}, \overline{n}]^{p^{i+j}} = \overline{1}$, which is obviously true.

Let us see that the reverse inclusion also holds. Set $\overline{G} = G/[\mho_i(M), \mho_j(N)]$. In this quotient group we have that $[\overline{m}^{p^i}, \overline{n}^{p^j}] = \overline{1}$ for any $m \in M$, $n \in N$, so we deduce from Lemma 2.13 that $[\overline{m}, \overline{n}]^{p^{i+j}} = \overline{1}$. It follows that the commutator subgroup $[\overline{M}, \overline{N}]$ is generated by elements of order $\leq p^{i+j}$. Since $[M,N]$ is a proper subgroup of G, it is regular and then Corollary 2.11 proves that $\exp[\overline{M}, \overline{N}] \leq p^{i+j}$. Consequently $\mho_{i+j}([M,N]) \subseteq [\mho_i(M), \mho_j(N)]$, as desired. $\square$

Exercises

2.1. Let G be an abelian p-group. Prove that $G/\mho_i(G) \cong \Omega_i(G)$ for any $i \geq 0$. (Hint: Use the structure theorem for finite abelian groups.)

2.2. Hall's compilation formula is very useful as a theoretical tool, since it applies to any group. However, under some particular conditions on the group, there may be more interesting formulas that give an explicit expression for the elements $c_i(x,y)$ in that case. This exercise gives a formula of that type.

Let G be a group and let $x, y \in G$. Write $H = \langle x, y \rangle$ and assume that the subgroup $\langle y, H' \rangle$ is abelian.

(i) Prove that
$$(xy)^n = x^n y^{x^{n-1}} y^{x^{n-2}} \dots y^{x^2} y^x y$$
for any $n \in \mathbb{N}$. (Observe that this holds without any conditions.)

(ii) Deduce that
$$(xy)^n = x^n y^n [y, x^{n-1}][y, x^{n-2}] \dots [y, x^2][y, x].$$

(iii) Prove by induction on i that
$$[y, x^i] = [y, x]^i [y, x, x]^{\binom{i}{2}} [y, x, x, x]^{\binom{i}{3}} \dots [y, x, \overset{i}{\ldots}, x]^{\binom{i}{i}}.$$

(iv) Prove the following relation for binomial coefficients:
$$\sum_{i=k}^{n-1} \binom{i}{k} = \binom{n}{k+1}.$$

(Hint: Argue by induction on $n \geq k+1$ and recall the identity $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$.)

(v) Conclude that

$$(xy)^n = x^n y^n [y,x]^{\binom{n}{2}} [y,x,x]^{\binom{n}{3}} \dots [y,x,\overset{n-1}{\dots},x]^{\binom{n}{n}}. \tag{2.7}$$

(vi) Reread the proof of Hall's compilation formula and adapt it to give an alternative proof that (2.7) holds under the condition imposed that $\langle y, H' \rangle$ is abelian. (Hint: Choose the sets $X_1, \dots, X_n$ as in Theorem 2.6 in order to rearrange the product $x^n y^n$. Since $\langle y, H' \rangle$ is abelian, a careful analysis of the proof of Lemma 2.5 shows that the only commutators arising from the collecting process are of the form $[x, y, x, \dots, x]$. Moreover, all the components in such a commutator belong to different sets X_i. Hence $q_S = [x, y, x, \overset{i-2}{\dots}, x]$ for any subset S of $R = \{1, \dots, n\}$ with $i \geq 2$ elements. Deduce (2.7) from this.)

2.3. Let $G = H[N]$ be the semidirect product of $H = \langle b \rangle \cong C_{p^2}$ and $N = \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_{p-1} \rangle \cong C_{p^2} \times C_p \times \dots \times C_p$ with respect to the action given by

$$a_1^b = a_1 a_2, \ a_2^b = a_2 a_3, \ \dots \ , \ a_{p-1}^b = a_{p-1} a_1^{-p}.$$

(i) Prove that $G' = \langle a_2, \dots, a_{p-1}, a_1^{-p} \rangle$ and note that $\exp G' = p$. Calculate the rest of the terms of the lower central series and deduce that G has class p.

(ii) Let $x \in G$. Then x can be written in the form $x = uv$, with $u = b^i a_1^j$ and $v \in G'$. Show that $x^p = u^p$. (Hint: Use part (v) of Exercise 2.2.)

(iii) Prove that b^p and a_1^p are central elements in G. Deduce that the value of u^p only depends on the residue classes of i and j modulo p.

(iv) Prove that $(ba_1)^p = b^p$. Use this and (iii) to derive that the number of different powers x^p is greater than p and smaller than p^2. Hence the set $\{x^p \mid x \in G\}$ is not a subgroup of G.

2.4. Let G be the group with the same defining relations as the one in the previous exercise, but with $b^{p^2} = 1$ changed to $b^p = a_1^p$. This is a group of order p^{p+1}.

(i) Prove that $\mho_1(G) = \langle a_1^p \rangle$. Hence $\mho_1(G)$ coincides with the set of p-th powers of the elements of G. (Hint: The group $G/\langle a_1^p \rangle$ has order p^p and is generated by elements of order p.)

(ii) As in Exercise 2.3, $G' = \langle a_2, \dots, a_{p-1}, a_1^{-p} \rangle$ has exponent p. Then $\Omega_1(G) = G'$ and, as a consequence, $\Omega_1(G)$ is the set of the elements $x \in G$ such that $x^p = 1$. (Hint: Observe that $\Omega_1(G) = \langle \Omega_1(M) \mid M \text{ is maximal in } G \rangle$. Now the maximal subgroups of G are either $\langle a_1 \rangle G'$ or of the form $\langle ba_1^j \rangle G'$. Since $o(a_1) = p^2$ and, as in the previous exercise, $(ba_1^j)^p = b^p$, we derive that $|\mho_1(M)| \geq p$ for any maximal subgroup M of G. Deduce from the regularity of the maximal subgroups that $\Omega_1(M) = G'$ and conclude that $\Omega_1(G) = G'$.)

(iii) However, it follows from (i) and (ii) that $|G : \Omega_1(G)| \neq |\mho_1(G)|$.

2.5. Let G be a regular p-group and suppose that $G = H[N]$ is a semidirect product of two of its subgroups. Then $\Omega_i(G) = \Omega_i(H)\Omega_i(N)$ and $\mho_i(G) = \mho_i(H)\mho_i(N)$ for all $i \geq 0$. (Hint: The inclusion $\Omega_i(H)\Omega_i(N) \subseteq \Omega_i(G)$ is obvious. In order to obtain the equality, prove that $|\Omega_i(H)\Omega_i(N)| \geq |\Omega_i(G)|$ by relating the order of these subgroups with the indices of the “agemo” subgroups, taking into account that G is regular.)

2.6. Let p be an odd prime.

(i) Prove that the group $G = \langle a, b \mid a^{p^3} = b^{p^2} = 1,\ a^b = a^{1+p} \rangle$ is a regular p-group such that $G/\Omega_1(G) \not\cong \mho_1(G)$. (Hint: Use Exercise 2.5 to find the subgroups $\mho_1(G)$ and $\Omega_1(G)$.)

(ii) Prove that the group $G = \langle a, b, c \mid a^{p^2} = b^p = c^p = 1,\ [a,b] = [a,c] = 1,\ b^c = ba^p \rangle$ is a regular p-group such that $G/\mho_1(G) \not\cong \Omega_1(G)$.

(iii) Prove that the group $G = \langle a, b, c \mid a^{p^3} = b^p = c^{p^2} = 1,\ [a,b] = 1,\ a^c = a^{1+p},\ b^c = ba^p \rangle$ is a regular p-group such that $G/\mho_1(G) \not\cong \Omega_1(G)$ and $G/\Omega_1(G) \not\cong \mho_1(G)$.

It is not very difficult to prove that these groups are examples of minimum order with respect to the properties stated. (Try it!)

2.7. In this exercise we prove that the direct product of two regular p-groups need not be regular.

(i) Prove that the group $G = \langle a, b \mid a^{27} = b^9 = 1,\ a^b = a^4 \rangle$ is regular.

(ii) Let $G_1 = \langle a_1, b_1 \rangle$ and $G_2 = \langle a_2, b_2 \rangle$ be two copies of G, and consider the following two elements of $G_1 \times G_2$: $x = b_1a_2$, $y = a_1b_2$. Check that $x^3y^3 = (xy)^3a_1^9$. (Hint: Use Exercise 2.2 to prove that $b^3a^3 = (ba)^3a^9$ and $a^3b^3 = (ab)^3$ hold in G.)

(iii) Let $H = \langle x, y \rangle$. Prove that $a_1^9 \notin \mho_1(H')$ and conclude that $G_1 \times G_2$ is not regular. (Hint: Prove first that $[x, y] = a_1^{-3} a_2^3$ and then derive that $H' = \langle a_1^9, a_2^9, a_1^{-3} a_2^3 \rangle$. Consequently $\mho_1(H') = \langle a_1^{-9} a_2^9 \rangle$.)

Lecture 3

From regular p-groups to p-groups of maximal class

3.1 A condition implying regularity

In this section we prove that any p-group G such that $|G : \mho_1(G)| \le p^{p-1}$ is necessarily regular. This result will be crucial in Lecture 4 when we study the power structure of a p-group of maximal class of arbitrary order. We will prove this regularity criterion by induction on the order of G and we need the following lemma.

Lemma 3.1. *Let G be a p-group such that $|G : \mho_1(G)| \le p^{p-1}$. Then $|H : \mho_1(H)| \le p^{p-1}$ for any subgroup H of G.*

Proof. If $p = 2$ then $|G : \Phi(G)| \le |G : \mho_1(G)| \le 2$ and G is cyclic. Hence any subgroup H of G is also cyclic and $|H : \mho_1(H)| \le 2$. Let us now prove the result when $p > 2$. By Theorem 1.4, we may assume without loss of generality that H is maximal in G. Suppose, by way of contradiction, that $|H : \mho_1(H)| \ge p^p$. Again by Theorem 1.4, it is possible to choose a subgroup $N \trianglelefteq G$ such that $\mho_1(H) \le N \le H$ and $|H : N| = p^p$.

By factoring out N we may suppose that $|G| = p^{p+1}$ and $\exp H = p$. Then any proper subgroup of G has order $\le p^p$ and is consequently regular. It follows from Theorem 2.14 that $[\mho_1(G), G] = \mho_1(G') \le \mho_1(H) = 1$. On the other hand, since $|G : \mho_1(G)| \le p^{p-1}$ and $p > 2$, Corollary 1.16 yields that $\gamma_{p-1}(G) \le \mho_1(G)$ and we derive that $\gamma_p(G) = [\gamma_{p-1}(G), G] \le [\mho_1(G), G] = 1$.

Hence G has class less than p and it is a regular p-group. Then

$$|G : \mho_1(G)| = |\Omega_1(G)| \ge |\Omega_1(H)| = p^p,$$

which is a contradiction. $\square$

Theorem 3.2. *Let G be a p-group such that $|G : \mho_1(G)| \leq p^{p-1}$. Then G is regular.*

Proof. Again we may assume that $p > 2$. Let G be a counterexample of minimum order. According to the previous lemma, the condition $|G : \mho_1(G)| \leq p^{p-1}$ is hereditary for subgroups. Thus all proper subgroups of G are regular. It follows that we only need to check the regularity condition on elements x, y such that $G = \langle x, y\rangle$.

Since $|G : \mho_1(G)| \leq p^{p-1}$ and $p > 2$, we have that $\gamma_{p-1}(G) \leq \mho_1(G)$. By applying Theorem 2.14 we get that $\gamma_p(G) \leq [\mho_1(G), G] = \mho_1(G')$. In particular, the element $c_p(x, y)$ belongs to $\mho_1(G') = \mho_1(\langle x, y\rangle')$ and G is regular. □

3.2 Irregular p-groups of minimal order

We have already seen in Section 2.3 of Lecture 2 that any p-group of order $\leq p^p$ is regular. Next we see that there are irregular p-groups of order p^{p+1} for any prime p.

Let us see how the construction works. Let G be the subgroup of Σ_{p^2} generated by the following permutations:

$$\sigma_1 = (1\ 2\ \ldots\ p),\ \sigma_2 = (p+1\ p+2\ \ldots\ 2p),\ \ldots\ ,\\ \sigma_p = ((p-1)p+1\ (p-1)p+2\ \ldots\ p^2)$$

and

$$\tau = (1\ p+1\ \ldots\ (p-1)p+1)\,(2\ p+2\ \ldots\ (p-1)p+2)\ \ldots (p\ 2p\ \ldots\ p^2).$$

All these permutations have order p and

$$\sigma_1^\tau = \sigma_2,\ \sigma_2^\tau = \sigma_3,\ \ldots, \sigma_{p-1}^\tau = \sigma_p,\ \sigma_p^\tau = \sigma_1. \tag{3.1}$$

Hence τ normalizes the subgroup $\langle \sigma_1, \ldots, \sigma_p\rangle$ and G has order p^{p+1}. (This proves, by the way, that G is a Sylow p-subgroup of the symmetric group Σ_{p^2}. This group is also isomorphic to the wreath product of two cyclic groups of order p.) Since the element

$$\tau\sigma_1 = (1\ p+1\ \ldots\ (p-1)p+1\ 2\ p+2\ \ldots\ (p-1)p+2\ 3 \ldots\ ) \tag{3.2}$$

has order p^2, the set $\{x \in G \mid x^p = 1\}$ is not a subgroup and consequently G is irregular.*

*Another example of an irregular p-group of order p^{p+1} is the group in Exercise 2.4. However, the Sylow p-subgroups of Σ_{p^2} are the most quoted example.

Since p-groups of class $< p$ are regular, an irregular p-group of order p^{p+1} has necessarily class p. This proves the following remark, that shows a first connection between regular p-groups and groups of maximal class.

Remark 3.3. An irregular p-group of minimal order is a p-group of maximal class.

We will devote the rest of these notes to the study of p-groups of maximal class. As a result, we will obtain information on the power and commutator structure (though in no way a classification) of the irregular p-groups of minimal order.

We end this section with a refinement of Hall's compilation formula for a prime exponent. More precisely, we give an expression for the element $c_p(x, y)$. Curiously, in the course of the proof it will be fundamental to work in the Sylow p-subgroup of Σ_{p^2} that we have introduced above.

Theorem 3.4. *Let G be a group and $x, y \in G$. If p is a prime then the element $c_p = c_p(x, y)$ of Hall's compilation formula satisfies the congruence*

$$c_p \equiv [y, x, \overset{p-1}{\ldots}, x]^a \prod_i v_i^{a_i} \pmod{\gamma_{p+1}(\langle x, y\rangle)}, \tag{3.3}$$

where $a \equiv -1 \pmod p$, the a_i are integers and each v_i is a commutator of the form $[y, x, z_3, \ldots, z_p]$ such that $z_j \in \{x, y\}$ for all j and $z_j = y$ at least once.

Proof. Let $H = \langle x, y\rangle$. It follows from Exercise 1.10 that $\gamma_2(H)/\gamma_3(H)$ is generated by $[y, x]\gamma_3(H)$. By applying repeatedly this exercise, we obtain that $\gamma_p(H)/\gamma_{p+1}(H)$ is generated by the elements of the form $[y, x, z_3, \ldots, z_p]\gamma_{p+1}(H)$ with $z_j \in \{x, y\}$. This proves that c_p satisfies a congruence such as (3.3). We only need to check that $a \equiv -1 \pmod p$.

Let now G be the Sylow p-subgroup of Σ_{p^2} defined above. As we mentioned after the proof of Hall's compilation formula, the element $c_p(x, y)$ may be considered as a universal expression in x, y (a word in x, y), valid in any group. So we may analyse the value of a by studying the formula (3.3) in this particular group for any couple of elements. We choose $x = \tau$ and $y = \sigma_1$. According to (3.1), the subgroup $\langle\sigma_1, \ldots, \sigma_p\rangle$ is normal in G. Since this subgroup is also abelian, it follows that any commutator in which σ_1 appears at least twice must be trivial. Hence $v_i = 1$ for all i. On the other hand, G has order p^{p+1} and consequently $\gamma_{p+1}(G) = 1$. Thus (3.3) reads

$$c_p(\tau, \sigma_1) = [\sigma_1, \tau, \overset{p-1}{\ldots}, \tau]^a.$$

From (3.1) we get that

$$[\sigma_1, \tau] = \sigma_1^{-1}\sigma_2, \quad [\sigma_2, \tau] = \sigma_2^{-1}\sigma_3, \quad \ldots \quad , [\sigma_p, \tau] = \sigma_p^{-1}\sigma_1$$

and it follows easily that

$$c_p(\tau,\sigma_1) = (\sigma_1^{n_1}\dots\sigma_{p-1}^{n_{p-1}}\sigma_p)^a \tag{3.4}$$

for some integers n_i. But, on the other hand,

$$1 = \tau^p\sigma_1^p = (\tau\sigma_1)^p c_2^{\binom{p}{2}}\dots c_{p-1}^{\binom{p}{p-1}} c_p = (\tau\sigma_1)^p c_p,$$

and we derive from (3.2) that $1 = \sigma_1\dots\sigma_p c_p$, that is,

$$c_p(\tau,\sigma_1) = (\sigma_1\dots\sigma_p)^{-1}. \tag{3.5}$$

By comparing the exponents of σ_p in (3.4) and (3.5), it finally follows that $a \equiv -1 \pmod p$, as desired.* $\square$

The previous theorem will be essential in the study of the structure of the p-groups of maximal class of order $\geq p^{p+2}$, as we will see in Section 4.4 of Lecture 4.

3.3 Normal subgroups of a p-group of maximal class

We begin in this section the systematic study of the p-groups of maximal class. The main reference in the theory of p-groups of maximal class is N. Blackburn's paper [1]. All the results about p-groups of maximal class that we present in this and the next lecture are already present in Blackburn's work, even if the organization of the material and some of the proofs are different. It must be noted that A. Wiman [28] had previously published a paper on p-groups of maximal class, and that he introduced some of the ideas that Blackburn developed later on, but some of the conclusions that Wiman reached were unfortunately erroneous. A more modern reference for the theory of p-groups of maximal class is Section 14 of Chapter III in Huppert's book [7]. Also, we want to acknowledge the influence of the work of R.T. Shepherd [25] on some aspects of our exposition of this subject.

The first result tells us that these groups have a very simple lattice of normal subgroups.

Theorem 3.5. *Let G be a p-group of maximal class of order p^m. Then:*

(i) *We have that $|G : G'| = p^2$ and $|\gamma_i(G) : \gamma_{i+1}(G)| = p$ for $2 \leq i \leq m-1$. Hence $|G : \gamma_i(G)| = p^i$ for $2 \leq i \leq m$.*

*It is possible to use Exercise 2.2 to avoid some calculations in the final part of the proof of this theorem. More precisely, instead of obtaining the value of $[\sigma_1,\tau,\overset{p-1}{\dots},\tau]$, it is enough to compare the two relations between $\tau^p\sigma_1^p$ and $(\tau\sigma_1)^p$ that provide Hall's compilation formula and part (v) of Exercise 2.2. We recommend the reader to try to complete the details.

(ii) *Unless G is cyclic of order p^2, we have that $\Phi(G) = G'$ and $d(G) = 2$.*

(iii) *The only normal subgroups of G are the $\gamma_i(G)$ and the maximal subgroups of G. More precisely, if N is a normal subgroup of G of index $p^i \geq p^2$ then $N = \gamma_i(G)$.*

(iv) *If N is a normal subgroup of G of index $\geq p^2$ then G/N has also maximal class.*

(v) *$Z_i(G) = \gamma_{m-i}(G)$ for $0 \leq i \leq m-1$.*

Proof. (i) We have that

$$p^m = |G| = |G : G'| \prod_{i=2}^{m-1} |\gamma_i(G) : \gamma_{i+1}(G)|.$$

Now it suffices to observe that $|G : G'| \geq p^2$, by Theorem 1.15, and that $|\gamma_i(G) : \gamma_{i+1}(G)| \geq p$ for $2 \leq i \leq m-1$.

(ii) We know that $G' \leq \Phi(G)$, so part (i) yields that $|G : \Phi(G)| \leq p^2$. If $|G : \Phi(G)| = p$ then $G/\Phi(G)$ is cyclic and so G is also cyclic, of course of order p^2. Otherwise $|G : \Phi(G)| = p^2$ and, by Burnside's Basis Theorem, $d(G) = 2$.

(iii) Let N be any normal subgroup of G and write $|G : N| = p^i$ with $0 \leq i \leq m$. If $i = 0$ or 1 then $N = \gamma_1(G)$ or N is maximal in G. Otherwise $i \geq 2$ and $\gamma_i(G) \leq N$ by Corollary 1.16. Since $|G : \gamma_i(G)| = p^i$, we conclude that $N = \gamma_i(G)$.

(iv) This is immediate from (iii) and (i), since the class of $G/\gamma_i(G)$ is $i-1$ whenever $2 \leq i \leq m$.

(v) By Theorem 1.15, we have that $|G : Z_{m-2}(G)| \geq p^2$. Since $|Z_{i+1}(G) : Z_i(G)| \geq p$ for $0 \leq i \leq m-3$ and

$$p^m = |G| = |G : Z_{m-2}(G)| \prod_{i=0}^{m-3} |Z_{i+1}(G) : Z_i(G)|,$$

all the inequalities above must in fact be equalities. It follows that $|G : Z_i(G)| = p^{m-i}$ for $0 \leq i \leq m-2$ and, by part (iii), $Z_i(G) = \gamma_{m-i}(G)$. □

3.4 Degree of commutativity of a p-group of maximal class and the associated Lie algebra

A group of order p^2 is always abelian (recall Exercise 1.1) and therefore isomorphic to either C_{p^2} or $C_p \times C_p$. The groups of order p^3 are also well-known. There are only two isomorphism classes of non-abelian groups, which correspond to D_8 and Q_8 for $p = 2$ and to the groups

$$M_{p^3} = \langle a, b \mid a^{p^2} = b^p = 1,\ a^b = a^{1+p} \rangle$$

and

$$E_{p^3} = \langle a, b, c \mid a^p = b^p = c^p = 1,\ a^c = ab,\ [a,b] = [b,c] = 1 \rangle$$

for odd p. Thus there is no loss of generality if we only deal henceforth with p-groups of maximal class of order $\geq p^4$. In this case we may introduce the characteristic maximal subgroup of the following definition, which plays a fundamental role in the development of the general theory of p-groups of maximal class. In the sequel, when G is a p-group of maximal class we will write $G_i = \gamma_i(G)$ for $i \geq 2$ and $G_0 = G$.

Definition 3.6. Let G be a p-group of maximal class of order p^m. We define $G_1 = C_G(G_2/G_4)$ (the action of G on G_2/G_4 being induced by conjugation). In other words, G_1 is composed of the elements $x \in G$ such that $[x, G_2] \leq G_4$.

If N is a normal subgroup of G such that $|G/N| \geq p^4$, it is clear from the definition that $(G/N)_1 = G_1/N$.

Theorem 3.7. *Let G be a p-group of maximal class. Then G_1 is a characteristic maximal subgroup of G.*

Proof. Let $f \in \operatorname{Aut} G$. Since G_2 and G_4 are characteristic subgroups of G, we have that

$$[f(x), G_2] = [f(x), f(G_2)] = f([x, G_2]) \leq f(G_4) = G_4.$$

This proves that G_1 is characteristic in G.

On the other hand, since G_1 is the kernel of the action of G on G_2/G_4, the factor group G/G_1 embeds in $\operatorname{Aut}(G_2/G_4)$. But $|G_2 : G_4| = p^2$, so $G_2/G_4 \cong C_{p^2}$ or $C_p \times C_p$. In the first case, $|\operatorname{Aut}(G_2/G_4)| = p(p-1)$, while in the second $|\operatorname{Aut}(G_2/G_4)| = |GL_2(p)| = (p^2-1)(p^2-p)$. In any case, the highest power of p dividing $|\operatorname{Aut}(G_2/G_4)|$ is p, so we deduce that $|G : G_1| \leq p$. If $G_1 = G$ then $G_3 = [G, G_2] = [G_1, G_2] \leq G_4$. This is only possible if $G_3 = 1$, what contradicts that $|G| \geq p^4$. $\square$

It follows that, with the notation introduced above, $|G_i : G_{i+1}| = p$ for $0 \leq i \leq m-1$ and $G_i = 1$ for $i \geq m$.

The invariant we introduce in our next definition may be considered as the key to the analysis of the structure of p-groups of maximal class. It measures to what extent the terms of the series $\{G_i\}_{i \geq 1}$ commute with each other.

Definition 3.8. Let G be a p-group of maximal class. We define the *degree of commutativity* of G, which we denote by $l(G)$ or simply by l, by means of

$$l(G) = \max\{k \leq m-2 \mid [G_i, G_j] \leq G_{i+j+k} \text{ for all } i, j \geq 1\}.$$

It is clear that $l(G) = m-2$ if and only if G_1 is abelian. In fact, $l(G) = m-2$ holds if and only if G has an abelian maximal subgroup: if M is maximal in G and abelian then $G_2 = G' \leq M$ and $[M, G_2] = 1 \leq G_4$, whence $M = G_1$. This is the case of the 2-groups D_{2^m}, SD_{2^m} and Q_{2^m} introduced in Exercise 1.7 and of the Sylow p-subgroups of Σ_{p^2}. The p-groups of maximal class with an abelian maximal subgroup were completely classified by A. Wiman in [27] and the number of them is $2 + (m-2, p-1)$. Hence we may assume, whenever it is convenient, that $l(G) < m-2$.

On the other hand, since the factor group G_i/G_{i+1} is cyclic, we have that $[G_i, G_i] = [G_i, G_{i+1}]^*$ for all i. In particular $[G_1, G_1] = [G_1, G_2]$ and consequently the equality $l(G) = m-3$ never holds. Also, if $|G| = p^4$ then $[G_1, G_1] = [G_1, G_2] \leq G_4 = 1$, hence G_1 is abelian and $l(G) = 2$.

We know that the terms of the lower central series of any group G satisfy the condition $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$ for all i, j. Therefore $l(G) \geq 0$ for any group of maximal class.

Definition 3.9. A p-group of maximal class is called *exceptional* if $l(G) = 0$.

We will see that this name is appropriate for this type of groups: they can only exist under restrictive conditions on the order of the group.

The following result is straightforward.

Theorem 3.10. *Let G be a p-group of maximal class of order p^m and let N be a normal subgroup of G of order $p^t \leq p^{m-4}$. (Therefore $|G/N| = p^{m-t} \geq p^4$ and it makes sense to speak about the degree of commutativity of G/N.) Then either $l(G/N) = m-t-2$ or $l(G/N) \geq l(G)$.*

We have already indicated that the Lie ring $L(G)$ associated to a nilpotent group G can be a very useful tool for studying the commutator structure of the group. However, if G is a p-group of maximal class of order p^m, most of the information about commutation in G is lost when passing to $L(G)$. For instance, if $l(G) \geq 1$ then

$$G_1/\gamma_2(G) \oplus (\oplus_{i \geq 2} L_i)$$

is an abelian maximal ideal of $L(G)$, while G only has an abelian maximal subgroup when $l(G) = m-2$. Hence, the standard Lie ring associated to the lower

*If G is any group and N is a normal subgroup of G such that G/N is cyclic, then $G' = [G, N]$. It suffices to observe that $G/[G, N]$ is abelian.

central series has no interest for the study of the group G in that case. Clearly, the loss of information is due to the fact that, for $i, j \geq 2$, the commutator of an element of $\gamma_i(G)$ with an element of $\gamma_j(G)$ lies in a subgroup of the lower central series posterior to its "natural destination", which is $\gamma_{i+j}(G)$: in fact, at least in $\gamma_{i+j+l}(G)$, where $l = l(G)$. This suggests a modification in the definition of the associated Lie ring, by allowing the degree of commutativity to play a role in the Lie commutators. More precisely, we may consider the abelian group $\mathcal{L}(G) = \oplus_{i\geq 0}\,\mathcal{L}_i$, where $\mathcal{L}_i = G_i/G_{i+1}$ and define on it a product [,] by giving the following commutators between homogeneous elements: if $x \in G_i$ and $y \in G_j$ then

$$[xG_{i+1}, yG_{j+1}] = \begin{cases} [x,y]G_{i+j+2}, & \text{if } i = 0 \text{ or } j = 0; \\ [x,y]G_{i+j+l+1}, & \text{if } i, j \geq 1. \end{cases}$$

It can be checked, in the same way as for $L(G)$, that $\mathcal{L}(G)$ is a Lie ring. In fact, since $pa = 0$ for any $a \in \mathcal{L}(G)$, it is a Lie algebra over $\mathbb{F}_p$ of dimension m. It is clear that $\mathcal{L}(G)^k = \sum_{i\geq k}\mathcal{L}_i$ for any $k \geq 2$ and therefore $\mathcal{L}(G)$ is nilpotent of class $m-1$, in other words, a Lie algebra of maximal class.*

Definition 3.11. We say that $\mathcal{L}(G)$ is the *Lie algebra associated* to the p-group of maximal class G.

3.5 Uniform elements

Let G be a p-group of maximal class of order p^m. In the same way as we have defined in the previous section the subgroup $G_1 = C_G(G_2/G_4)$, we may consider more generally the so-called *two-step centralizers* $C_G(G_i/G_{i+2})$ for $1 \leq i \leq m-2$. As happened with G_1, all these subgroups are characteristic and maximal in G. Since $[G_1, G_1] = [G_1, G_2] \leq G_4$, we have that $C_G(G_1/G_3) = G_1$ and, consequently, it is enough to consider the two-step centralizers for $2 \leq i \leq m-2$.

Definition 3.12. Let G be a p-group of maximal class of order p^m. We say that $s \in G$ is a *uniform element* if $s \notin \cup_{i=2}^{m-2}\, C_G(G_i/G_{i+2})$.

The first question that arises is whether any p-group of maximal class has uniform elements, that is, whether it is true or not that $G \neq \cup_{i=2}^{m-2}\, C_G(G_i/G_{i+2})$. It turns out that this property always holds, as was shown by Blackburn, but this will not be completely established until Section 4.4 in Lecture 4. However, we can make some considerations at this moment.

*A Lie ring L is said to be nilpotent if $L^k = 0$ for some k. If L is a nilpotent Lie algebra of dimension $m \geq 2$ over a field K, then $\dim L/L^2 \geq 2$ and consequently the nilpotency class of L is at most $m-1$.

First of all, observe that, by the Correspondence Theorem, G may be written as the union of certain maximal subgroups of G if and only if the union of the corresponding subgroups in $G/\Phi(G)$ is also the whole group. But the group $G/\Phi(G) \cong C_p \times C_p$ has exactly $p+1$ maximal subgroups and they are all necessary if we want to decompose $G/\Phi(G)$ as a union of maximal subgroups. This proves that G has a uniform element if and only if the number of different two-step centralizers $C_G(G_i/G_{i+2})$ is at most p.

On the other hand, it is possible to derive the existence of uniform elements from properties about the degree of commutativity of G. For example, if $l(G) \geq 1$ then $[G_1, G_i] \leq G_{i+2}$ for all $i \geq 1$ and all the two-step centralizers coincide with G_1, what proves that uniform elements exist under that assumption. Actually, it suffices to suppose that $l(G/Z(G)) \geq 1$. In that case, since $Z(G) = G_{m-1}$ by Theorem 3.5, it easily follows that $[G_1, G_i] \leq G_{i+2}$ for $1 \leq i \leq m-3$ and there are at most two different two-step centralizers, G_1 and $C_G(G_{m-2})$.

In fact, Blackburn showed the existence of uniform elements simultaneously with some properties about the degree of commutativity. More precisely, he proved the following theorem.

Theorem 3.13 (Blackburn's Theorem). *Let G be a p-group of maximal class of order p^m. Then the following statements hold:*

(i) *If $l(G) = 0$ then $p \geq 5$, m is even and $6 \leq m \leq p+1$.*

(ii) *$l(G/Z(G)) \geq 1$.*

(iii) *G has uniform elements.*

The proof of this theorem has been split into several sections in the next lecture and it requires showing first some structural properties of the p-groups of maximal class, which are also interesting for themselves.

Parts (i) and (ii) in Blackburn's Theorem justify the term "exceptional groups" that is used for the groups with degree of commutativity zero. On the other hand, it is shown in Exercise 3.6 that, for any $p \geq 5$ and $6 \leq m \leq p+1$, m even, there exist p-groups of maximal class of order p^m satisfying $l(G) = 0$.

Note that the condition in part (ii) of Blackburn's Theorem only makes sense if $|G| \geq p^5$. With the purpose of not increasing unnecessarily the length of the statements of the theorems, we will always omit from them this kind of obvious conditions.

We may ask: why is so important the existence of uniform elements in the p-groups of maximal class? This will be clear in the light of our next theorem and also in Section 4.1 in the following lecture where, assuming that there exist uniform elements, we develop a set of tools which are fundamental for any study of the p-groups of maximal class. First we need a lemma.

Lemma 3.14. *Let G be a p-group of maximal class of order p^m and suppose that G has a uniform element s. If $1 \le i \le m-2$ and $x \in G_i - G_{i+1}$, then $[s,x] \in G_{i+1} - G_{i+2}$.*

Proof. Since $x \in G_i$, it is obvious that $[s,x] \in G_{i+1}$ and we only have to prove that $[s,x] \notin G_{i+2}$. Suppose on the contrary that $[s,x] \in G_{i+2}$. If we write $\overline{G} = G/G_{i+2}$, this means that $\overline{s}$ and $\overline{x}$ commute in $\overline{G}$. We also have that $[s, G_{i+1}] \le G_{i+2}$ or, what is the same, that $\overline{s}$ centralizes $\overline{G}_{i+1}$. Since $G_i = \langle x, G_{i+1}\rangle$ (recall that $|G_i : G_{i+1}| = p$), it follows that $\overline{s}$ centralizes $\overline{G}_i$. Then $[s, G_i] \le G_{i+2}$ and $s \in C_G(G_i/G_{i+2})$, what contradicts that s is a uniform element. □

Theorem 3.15. *Let G be a p-group of maximal class of order p^m and suppose that G has a uniform element s. Then the following properties hold:*

(i) *$C_G(s) = \langle s\rangle Z(G)$.*

(ii) *$s^p \in Z(G)$ and consequently $o(s) \le p^2$ and $|C_G(s)| = p^2$.*

(iii) *The conjugates of s are exactly the elements in the coset sG_2.*

(iv) *For $0 \le t \le m-4$, the subgroup $H = \langle s, G_{t+1}\rangle$ is a p-group of maximal class of order p^{m-t} and such that $H_i = G_{i+t}$ for every $i \ge 1$. Hence, either $l(H) = m-t-2$ or $l(H) \ge l(G)+t$.*

Proof. (i) Let g be any element of G. Since $G = \langle s\rangle G_1$, we may write $g = s^i x$, where $i \in \mathbb{Z}$ and $x \in G_1$. Then $g \in C_G(s)$ if and only if $[s,x] = 1$. But, according to the previous lemma, if $x \in G_i - G_{i+1}$ with $1 \le i \le m-2$ then $[s,x] \in G_{i+1} - G_{i+2}$ and, in particular, $[s,x] \ne 1$. It follows that $x \in G_{m-1} = Z(G)$. Hence $C_G(s) = \langle s\rangle Z(G)$.

(ii) In the proof of (i) we have actually seen that $C_{G_1}(s) = Z(G)$. Since $s^p \in G_1$ commutes with s, it follows that $s^p \in Z(G)$.

(iii) The size of the conjugacy class of s in G is $|G : C_G(s)| = p^{m-2} = |sG_2|$. Since any conjugate of s, say $s^g = s[s,g]$, belongs to sG_2, we deduce that the elements in the coset sG_2 are precisely the conjugates of s.

(iv) There is nothing to prove if $t = 0$, so let us assume that $t \ge 1$. It is clear from part (ii) that $|H| = p|G_{t+1}| = p^{m-t}$. By applying repeatedly Lemma 3.14, for any $x \in G_{t+1} - G_{t+2}$ we have that

$$[x, s, \overset{i-1}{\ldots}, s] \in G_{i+t} - G_{i+t+1} \quad \text{for } 2 \le i \le m-t-1. \tag{3.6}$$

In particular, for $i = m-t-1$ it follows that $1 \neq [x, s, \overset{m-t-2}{\ldots}, s] \in \gamma_{m-t-1}(H)$ and H has maximal class. In order to prove that $H_i = G_{i+t}$, we suppose first that $i \geq 2$. From (3.6) we have that H_i has an element in the difference $G_{i+t} - G_{i+t+1}$. By using this property not only with H_i, but also with any H_j contained in H_i, we derive that H_i has elements in all the differences $G_k - G_{k+1}$ for $i + t \leq k \leq m-1$. Consequently $G_{i+t} \leq H_i$ and, since both subgroups have the same order, the equality follows. On the other hand, $[G_{t+1}, H_2] = [G_{t+1}, G_{t+2}] \leq G_{2t+3} \leq G_{t+4} = H_4$ and we obtain that $H_1 = G_{t+1}$. Finally, if $l = l(G)$ then $[H_i, H_j] = [G_{i+t}, G_{j+t}] \leq G_{i+j+l+2t} = H_{i+j+l+t}$ for any $i, j \geq 1$ and therefore either $l(H) = m-t-2$ or $l(H) \geq l(G) + t$. □

Of course, once Blackburn's Theorem is proved, there will be no need to assume the existence of s in the statement of the previous theorem.

Exercises

3.1. Let G be a (not necessarily finite) group of exponent p. Let x, y be elements of G and define $H = \langle x, y \rangle$.

(i) Show that the Lie ring $L(H)$ associated to the lower central series of H is an algebra over $\mathbb{F}_p$.

(ii) Consider the elements $u = xG', v = yG' \in L_1$ and prove that there exist integers a_i such that

$$-[v, u, \overset{p-1}{\ldots}, u] + \sum_i a_i w_i = 0, \tag{3.7}$$

where the w_i are Lie commutators of the form $[v, u, z_3, \ldots, z_p]$ with $z_j \in \{u, v\}$ and at least once $z_j = v$. (Hint: Hall's compilation formula for $x^p y^p$ yields that $c_p(x, y) = 1$. Use then Theorem 3.4.)

(iii) For any $\lambda \in \mathbb{F}_p^*$, substitute λu for u in (3.7) and then sum all these expressions to derive that

$$[v, u, \overset{p-1}{\ldots}, u] = 0.$$

(Hint: For $1 \leq r < p-1$, the sum $S = \sum_{\lambda \in \mathbb{F}_p^*} \lambda^r$ equals zero, since $\alpha^r S = S$ for any $\alpha \in \mathbb{F}_p^*$ and, in particular, for a generator of $\mathbb{F}_p^*$.)

(iv) Deduce that $[y, x, \overset{p-1}{\ldots}, x] \in \gamma_{p+1}(H)$. This is known as *Zassenhaus' identity*. In particular, a group of exponent p and class p satisfies the identity $[y, x, \overset{p-1}{\ldots}, x] = 1$.

3.2. Let G be a regular p-group of class p such that $\exp G' = p$. Check that, with minor modifications, the argument in Exercise 3.1 shows that G satisfies the identity $[y, x, \overset{p-1}{\ldots}, x] = 1$. (Hint: The point is that $c_p(x, y) = 1$.)

3.3. Let G be a 2-group of maximal class. In this exercise we prove that G has a cyclic maximal subgroup by induction on the order of G.

(i) Observe that the result is straightforward if $|G| = 4$ or 8. (When $|G| = 8$ you may just use the classification of the groups of order 8 or otherwise recall that any group of exponent 2 is abelian.)

(ii) Suppose now that $|G| = 2^m \geq 2^4$. By induction there exists a maximal subgroup M of G such that $M/Z(G) = \langle \overline{a} \rangle$ is cyclic. Then for any $g \in G$ we can write $a^g = a^i z$, where $i \in \mathbb{Z}$ and $z \in Z(G)$. Deduce that $\langle a^2 \rangle \trianglelefteq G$ and consequently that $Z(G) \leq \langle a^2 \rangle$. Thus $M = \langle a \rangle$ is cyclic, as desired.

3.4. The aim of this exercise is to construct for any prime p and any $m \geq 3$ a p-group of maximal class of order p^m with an abelian maximal subgroup.

(i) Let H be the abelian group defined by generators $\{s_i \mid i \geq 1\}$ subject to the relations

$$s_i^p s_{i+1}^{\binom{p}{2}} \cdots s_{i+p-1}^{\binom{p}{p}} = 1, \text{ for } 1 \leq i \leq m-1; \quad s_i = 1, \text{ for } i \geq m.$$

Prove by induction on m that $|H| = p^{m-1}$.

(ii) Prove that the map s defined by $s_i \mapsto s_i s_{i+1}$ extends to an automorphism of order p of H, and that the semidirect product $G = \langle s \rangle [H]$ is a p-group of maximal class. Which is this group in the particular case $p = 2$?

3.5. Let G be a p-group of maximal class of order p^m. Show that the Lie rings $L(G)$ and $\mathcal{L}(G)$ are isomorphic if and only if $l(G) = 0$ or $m - 2$.

3.6. Let $p \geq 5$ be a prime and suppose that $6 \leq 2r \leq p + 1$. In this exercise we construct an exceptional p-group of maximal class of order p^{2r}.

(i) Let $A = \langle a_1, \ldots, a_r \rangle$ be an elementary abelian group of order p^r. Prove that the group B formed by the automorphisms of A that act trivially on $\langle a_r \rangle$ and on $A/\langle a_r \rangle$ is elementary abelian of order p^{r-1}. (Hint: Represent the automorphisms by matrices.)

(ii) Define automorphisms $b_1, \ldots, b_{r-1} \in B$ by means of

$$a_i^{b_j} = \begin{cases} a_i a_r^{(-1)^{r+i-1}\binom{r-j-1}{i-1}}, & \text{if } 1 \leq i \leq r-j; \\ a_i, & \text{if } i > r-j. \end{cases}$$

Prove that these automorphisms form a basis of B. (Hint: Observe that the corresponding matrices are linearly independent.)

(iii) Let us consider the semidirect product $H = B[A]$. Prove that the map s defined by

$$a_i^s = a_i a_{i+1}^{-1} \ (1 \le i \le r-2), \quad a_{r-1}^s = a_{r-1}, \quad a_r^s = a_r,$$
$$b_i^s = b_i b_{i+1}^{-1} \ (1 \le i \le r-2), \quad b_{r-1}^s = b_{r-1} a_1^{-1},$$

extends to an automorphism of H of order p.

(iv) Prove that the semidirect product $G = \langle s \rangle [H]$ is an exceptional p-group of maximal class of order p^{2r}.

Lecture 4

The proof of Blackburn's Theorem

4.1 Chains and the associated function α

If s is a uniform element of a p-group of maximal class G and $s_1 \in G_1 - G_2$, it follows from Lemma 3.14 that $[s_1, s] \in G_2 - G_3$, $[s_1, s, s] \in G_3 - G_4$ and continuing this way we obtain elements in every difference $G_i - G_{i+1}$. This suggests the following definition.

Definition 4.1. Let G be a p-group of maximal class, $s \in G$ a uniform element and $s_1 \in G_1 - G_2$. If we define recursively $s_i = [s_{i-1}, s]$ for every $i \geq 2$, we say that the sequence of elements $\{s, s_1, s_2, \ldots\}$ is a *chain* in G.

Of course, the existence of chains in G is equivalent to the existence of uniform elements. On the other hand, if $\{s, s_1, s_2, \ldots\}$ is a chain in G and $\overline{G}$ is a quotient of G of order $\geq p^4$, then $\{\overline{s}, \overline{s}_1, \overline{s}_2, \ldots\}$ is a chain in $\overline{G}$: it suffices to check that $\overline{s}$ is a uniform element of $\overline{G}$.

Sometimes it will be convenient to represent the uniform element by s_0, so that the chain is simply denoted by $\{s_i\}$. Then $s_i \in G_i - G_{i+1}$ for all $0 \leq i \leq m-1$ and $s_i = 1$ for $i \geq m$. Let $l = l(G)$. For any couple of indices $i, j \geq 1$ such that $i + j + l \leq m - 1$, we may write

$$[s_i, s_j] \equiv s_{i+j+l}^{\alpha(i,j)} \pmod{G_{i+j+l+1}} \tag{4.1}$$

for some integer $\alpha(i,j)$ which is uniquely determined modulo p and, consequently, can be considered as an element of $\mathbb{F}_p$. This way, we obtain a function

$$\begin{array}{rccl} \alpha : & \{(i,j) \in \mathbb{N}^2 \mid i + j \leq m - l - 1\} & \longrightarrow & \mathbb{F}_p \\ & (i,j) & \longmapsto & \alpha(i,j). \end{array}$$

Observe that we need to impose the condition $l(G) < m - 2$ if we want the domain of this function to be non-empty. Since $G_i = \langle s_i, G_{i+1} \rangle$, $G_j = \langle s_j, G_{j+1} \rangle$ and $[G_i, G_{j+1}], [G_{i+1}, G_j] \leq G_{i+j+l+1}$, it is clear from the congruence (4.1) that $\alpha(i,j) = 0$ if and only if $[G_i, G_j] \leq G_{i+j+l+1}$. Then the definition of the degree of commutativity assures that the function α is not zero.

This function α we have just introduced associated to the chain $\{s_i\}$ turns out to be a fundamental tool in the study of the p-groups of maximal class. It satisfies a number of properties that reflect the commutator and power relations among the elements s_i. The quickest way to obtain most of these properties is by working in the associated Lie algebra $\mathcal{L}(G)$. More precisely, if $\{s_i\}$ is a chain in G, we may consider the elements $e_i = s_i G_{i+1}$ in $\mathcal{L}(G)$. It is clear that $(e_0, e_1, \ldots, e_{m-1})$ is a basis of $\mathcal{L}(G)$ and that $e_i = 0$ for $i \geq m$. Then the congruence (4.1) and the definition of the Lie product in $\mathcal{L}(G)$ yield that

$$[e_i, e_j] = \alpha(i,j) e_{i+j+l}, \quad \text{for } i, j \geq 1,\ i + j \leq m - l - 1,$$

so that the values $\alpha(i,j)$ determine the structural constants of the Lie algebra $\mathcal{L}(G)$ with respect to the basis $(e_0, \ldots, e_{m-1})$, since the rest of the products among the elements e_i either are of the form $[e_i, e_0] = e_{i+1}$ or equal zero.

On the one hand, the Lie product in $\mathcal{L}(G)$ is alternating, so $\alpha(i,i) = 0$ and $\alpha(i,j) = -\alpha(j,i)$ whenever these values are defined. On the other hand, if $i, j \geq 1$ then the Jacobi identity applied to the elements e_0, e_i and e_j yields that

$$\begin{aligned} 0 &= [e_0, e_i, e_j] + [e_i, e_j, e_0] + [e_j, e_0, e_i] = [-e_{i+1}, e_j] + [\alpha(i,j) e_{i+j+l}, e_0] + [e_{j+1}, e_i] \\ &= -\alpha(i+1, j) e_{i+j+l+1} + \alpha(i,j) e_{i+j+l+1} + \alpha(j+1, i) e_{i+j+l+1}, \end{aligned}$$

and consequently

$$\alpha(i,j) = \alpha(i+1, j) + \alpha(i, j+1), \quad \text{for } i + j \leq m - l - 2. \tag{4.2}$$

Similarly, from the Jacobi identity for e_i, e_j and e_k $(i, j, k \geq 1)$ we obtain that

$$\alpha(i,j)\alpha(i+j+l, k) + \alpha(j,k)\alpha(j+k+l, i) + \alpha(k,i)\alpha(k+i+l, j) = 0,$$
$$\text{for } i + j + k \leq m - 2l - 1.$$

Observe also that (4.2) gives that $\alpha(i, i+1) = \alpha(i+1, i+1) + \alpha(i, i+2) = \alpha(i, i+2)$ whenever these values are defined.

There is one more property that the function α fulfills: it is periodic in its two components, with period $p - 1$. This is a consequence of the power structure of G and we must postpone its proof until Section 4.4. Nevertheless, we include this property in the statement of the following theorem, in order to collect in it the main properties of the function α.

Theorem 4.2. *Let G be a p-group of maximal class of order p^m and degree of commutativity $l < m-2$. Suppose that G has a chain and let α be the function associated to this chain. Then the following properties hold:*

P1. $\alpha \neq 0$.

P2. $\alpha(i,i) = 0$ *for* $2i \leq m-l-1$.

P3. $\alpha(i,j) = -\alpha(j,i)$ *for* $i+j \leq m-l-1$.

P4. $\alpha(i,j) = \alpha(i+1,j) + \alpha(i,j+1)$ *for* $i+j \leq m-l-2$.

P5. $\alpha(i,i+2) = \alpha(i,i+1)$ *for* $2i \leq m-l-3$.

P6. *If we write* $\mathcal{J}(i,j,k) = \alpha(i,j)\alpha(i+j+l,k) + \alpha(j,k)\alpha(j+k+l,i) + \alpha(k,i)$ $\alpha(k+i+l,j)$, *then* $\mathcal{J}(i,j,k) = 0$ *for* $i+j+k \leq m-2l-1$.

P7. $\alpha(i,j) = \alpha(i+p-1,j) = \alpha(i,j+p-1)$ *for* $i+j \leq m-l-p$.

Note that all the restrictions that apply to i, j and k in the above properties have the only purpose of assuring that all the values of the function α involved are actually defined. On the other hand, it is clear from P2 and P3 that, in order to determine the function α, it is enough to know the values $\alpha(i,j)$ with $i < j$ (or, alternatively, with $i > j$). Next we refine property P1.

Theorem 4.3. *Let G be a p-group of maximal class of order p^m and degree of commutativity $l < m-2$. Suppose that G has a chain and let α be the function associated to this chain. Then there exists some $j \in \{1,\dots,m-l-2\}$ such that $\alpha(1,j) \neq 0$. In other words, there exists some j such that $[G_1,G_j] = G_{j+l+1} \neq 1$.*

Proof. Suppose that $\alpha(1,j) = 0$ for all j. If we write property P4 in the form $\alpha(i,j) = \alpha(i-1,j) - \alpha(i-1,j+1)$, it readily follows by induction on i that $\alpha(i,j) = 0$ for all possible i and j, which is impossible according to P1. $\square$

Remark 4.4. In fact, once we have proved the periodicity claimed in property P7, we may even assert that there is some $j \in \{2,\dots,p-1\}$ such that $\alpha(1,j) \neq 0$. (Take into account that $\alpha(1,1) = 0$ by property P2.)

The key to the proof of the previous theorem has been the recurrence relation provided by property P4. This relation may also be used in order to obtain any value $\alpha(i,j)$ from the particular values of the form $\alpha(r,r+1)$, as we see in the following theorem, due to Shepherd [25]. The proof of this theorem is easier to write if we extend the definition of the binomial coefficients $\binom{n}{k}$ to all $n, k \in \mathbb{Z}$ as follows:

$$\binom{n}{k} = \begin{cases} \dfrac{n(n-1)\dots(n-k+1)}{k!}, & \text{if } k \geq 1; \\ 1, & \text{if } k = 0; \\ 0, & \text{if } k < 0. \end{cases}$$

These generalized binomial coefficients still satisfy the property $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$. On the other hand, it is clear that $\binom{n}{k} = 0$ for $0 \leq n < k$ and that $\binom{n}{k} = \binom{n}{n-k}$ for $n \geq 0$.

Theorem 4.5. *Let G be a p-group of maximal class of order p^m and degree of commutativity $l < m-2$. Suppose that G has a chain and let α be the function associated to this chain. If we write $x_r = \alpha(r, r+1)$ then*

$$\alpha(i,j) = \sum_{r=i}^{[(i+j-1)/2]} (-1)^{r-i} \binom{j-r-1}{r-i} x_r, \quad \textit{for } i < j. \tag{4.3}$$

Proof. By using generalized binomial coefficients, we may write (4.3) in the form

$$\alpha(i,j) = \sum_{r=i}^{j-1} (-1)^{r-i} \binom{j-r-1}{r-i} x_r.$$

(This way, it is possible that some of the x_r are not really defined because $2r+1 > m-l-1$, but this is irrelevant, since the corresponding coefficients are zero.) We prove the theorem by induction on $j-i$. When $j-i = 1$ or 2 the result is immediate. In the general case, we have that

$$\begin{aligned} \alpha(i,j) &= \alpha(i,j-1) - \alpha(i+1,j-1) \\ &= \sum_{r=i}^{j-2} (-1)^{r-i} \binom{j-r-2}{r-i} x_r - \sum_{r=i+1}^{j-2} (-1)^{r-i-1} \binom{j-r-2}{r-i-1} x_r \\ &= \sum_{r=i}^{j-2} (-1)^{r-i} \binom{j-r-2}{r-i} x_r + \sum_{r=i}^{j-2} (-1)^{r-i} \binom{j-r-2}{r-i-1} x_r \\ &= \sum_{r=i}^{j-2} (-1)^{r-i} \binom{j-r-1}{r-i} x_r = \sum_{r=i}^{j-1} (-1)^{r-i} \binom{j-r-1}{r-i} x_r, \end{aligned}$$

as desired. $\square$

We want to remark that, as soon as we prove the existence of uniform elements, we will be able to remove the hypothesis that G has a chain from the previous theorems.

4.2 Proof of Blackburn's Theorem for $|G| \le p^{p+2}$

The goal of this section is to prove the following theorem, which is just Blackburn's Theorem for the p-groups of maximal class of order less than or equal to p^{p+2}.

Theorem 4.6. *Let G be a p-group of maximal class of order $p^m \le p^{p+2}$. Then:*

(i) *G has uniform elements.*

(ii) *If $l(G) = 0$ then $p \ge 5$, m is even and $6 \le m \le p+1$.*

(iii) *$l(G/Z(G)) \ge 1$.*

Proof. (i) The number of different two-step centralizers $C_G(G_i/G_{i+2})$ is at most $m-3 \le p-1$. Hence G cannot be the union of these centralizers and there exist uniform elements.

(ii) First of all, recall that $l(G) = 2$ when $|G| = p^4$. Next we prove that if m is odd then $l(G) \ge 1$, by induction on m. Note that, according to part (i), it is possible to choose a chain in G and consequently we may work with the associated function α.

Suppose that $m = 5$. If $l(G) = 0$ then the condition $[G_1, G_2] \le G_4$ yields that $\alpha(1,2) = 0$. By property P5, we also have $\alpha(1,3) = 0$. But these values of α contradict Theorem 4.3 and hence $l(G) \ge 1$ in this case. This proves in particular that, under the assumption that $|G| \le p^{p+2}$, $l(G) = 0$ can only happen for $p \ge 5$.

Suppose now that $m = 2n+1 > 5$ and $l(G) = 0$. By the induction hypothesis, we have that $l(G/G_{m-2}) \ge 1$. This means that $[G_i, G_j] \le G_{i+j+1}$ for $i+j \le m-3$ and consequently

$$\alpha(i,j) = 0 \quad \text{for } i+j \le m-3. \tag{4.4}$$

On the other hand, property P6 yields that $\mathcal{J}(1,2,m-4) = 0$, that is, that

$$\alpha(1,2)\alpha(3,m-4) + \alpha(2,m-4)\alpha(m-2,1) + \alpha(m-4,1)\alpha(m-3,2) = 0,$$

and we deduce from (4.4) that $\alpha(1,m-2)\alpha(2,m-4) = 0$. By using Theorem 4.5 and taking into account (4.4), we obtain that $\alpha(1,m-2) = (-1)^{n-2}(n-1)x_{n-1}$ and $\alpha(2,m-4) = (-1)^{n-3}x_{n-1}$. Hence $(n-1)x_{n-1}^2 = 0$. Now the condition $m \le p+2$ assures that $n-1 \ne 0$ in $\mathbb{F}_p$, so we necessarily have that $x_{n-1} = 0$. But then $x_r = 0$ for all r and, again by Theorem 4.5, we reach the final contradiction that $\alpha = 0$.

What we have proved allows us to conclude that if $l(G) = 0$ then $p \ge 5$, m is even and $6 \le m \le p+1$.

(iii) Since $|G/Z(G)| = p^{m-1}$, if m is even then part (ii) yields that $l(G/Z(G)) \geq 1$. Suppose otherwise that m is odd. Then $l(G) \geq 1$ and, since we know from Theorem 3.10 that either $l(G/Z(G)) = m-3$ or $l(G/Z(G)) \geq l(G)$, we have that $l(G/Z(G)) \geq 1$ also in this case. $\square$

4.3 Power structure

We begin to examine the power structure of a p-group of maximal class when its order is $\leq p^{p+1}$.

Theorem 4.7. *Let G be a p-group of maximal class of order less than or equal to p^{p+1}. Then* $\exp G/Z(G) = \exp G_2 = p$.

Proof. We know that G has $p+1$ maximal subgroups. Since the number of different two-step centralizers $C_G(G_i/G_{i+2})$ is at most $m-3$ and $m \leq p+1$, there are at least two maximal subgroups M and N of G which are not of that kind. Consequently we may choose uniform elements $s \in M$ and $t \in N$. Since $|G : \Phi(G)| = p^2$, s and t generate G modulo $\Phi(G)$ and, by Theorem 1.5, $G = \langle s, t \rangle$. On the other hand, we obtain from Theorem 3.15 that $s^p, t^p \in Z(G)$. Thus $G/Z(G)$ can be generated by two elements of order p. Since $|G/Z(G)| \leq p^p$, this quotient is regular and it follows from Corollary 2.11 that $\exp G/Z(G) = p$.

In particular, we have that $\mho_1(G_1) \leq \mho_1(G) \leq Z(G)$. Since G_1 has order $\leq p^p$ and is consequently regular, we derive that $|G_1 : \Omega_1(G_1)| = |\mho_1(G_1)| \leq p$. It follows that $|G : \Omega_1(G_1)| = |G : G_1||G_1 : \Omega_1(G_1)| \leq p^2$ and, since $\Omega_1(G_1) \trianglelefteq G$, Theorem 3.5 proves that $G_2 \leq \Omega_1(G_1)$. Again by the regularity of G_1, we conclude that $\exp G_2 = p$. $\square$

In our next theorem we specify the power structure of the p-groups of maximal class of order $\geq p^{p+2}$. As will be clear in the proof of the theorem, this structure is completely determined from the information about the groups of order p^{p+2}, a case that is dealt with in the following lemma. We recall that, according to Theorem 4.6, if G is a p-group of maximal class and $|G| = p^{p+2}$, then it is possible to consider a chain in G.

Lemma 4.8. *Let G be a p-group of maximal class of order p^{p+2} and let $\{s_i\}$ be a chain in G. Then the following statements hold:*

(i) $s_1^p \equiv s_p^{-1} \pmod{G_{p+1}}$.

(ii) $\mho_1(G_1) = G_p$.

Proof. (i) By Hall's formula we have that $s_0^p s_1^p \equiv (s_0s_1)^p c_p \pmod{\mho_1(G_2)}$. If we apply Theorem 4.7 to the group G/G_{p+1}, it follows that $\exp G_2/G_{p+1} = p$ and consequently $\mho_1(G_2) \leq G_{p+1}$. So the previous congruence also holds modulo G_{p+1}. On the other hand, s_0 is a uniform element and Theorem 3.15 yields that $s_0^p \in Z(G) = G_{p+1}$. Furthermore, we know from Theorem 4.6 that $l(G) \geq 1$ and therefore any element in $G - G_1$ is uniform. In particular, s_0s_1 is a uniform element and also $(s_0s_1)^p \in G_{p+1}$. Thus we get the congruence $s_1^p \equiv c_p \pmod{G_{p+1}}$ and (i) will be proved if we see that $c_p \equiv s_p^{-1} \pmod{G_{p+1}}$. At this point Theorem 3.4 is fundamental: it says in this case that

$$c_p \equiv s_p^{-1} \prod_i v_i^{a_i} \pmod{G_{p+1}},$$

where each v_i is a commutator of the form $[s_1, s_0, z_3, \ldots, z_p]$ with $z_j \in \{s_0, s_1\}$ and at least one z_j equal to s_1. Since $l(G) \geq 1$, it follows that $v_i \in G_{p+1}$ for all i and consequently $c_p \equiv s_p^{-1} \pmod{G_{p+1}}$.

(ii) Part (i) proves that $s_1^p \notin G_{p+1}$ and, in particular, $\mho_1(G_1) \not\leq G_{p+1}$. On the other hand, by applying Theorem 4.7 to G/G_{p+1} we obtain that $\exp G/G_p = p$ and therefore $\mho_1(G_1) \leq G_p$. Since $\mho_1(G_1)$ is a normal subgroup of G, we conclude that $\mho_1(G_1) = G_p$. □

Theorem 4.9. *Let G be a p-group of maximal class of order $p^m \geq p^{p+2}$. Then the following statements hold:*

(i) *G_1 is regular.*

(ii) *$\mho_1(G_i) = G_{i+p-1}$ for all $i \geq 1$.*

(iii) *If $1 \leq i \leq m-p$ and $x \in G_i - G_{i+1}$ then $x^p \in G_{i+p-1} - G_{i+p}$.*

Proof. (i) If we apply the previous lemma to the quotient G/G_{p+2}, we get that $\mho_1(G_1/G_{p+2}) = G_p/G_{p+2}$ and therefore $\mho_1(G_1)G_{p+2} = G_p$. Since $\mho_1(G_1)$ is normal in G, it follows that $\mho_1(G_1) = G_p$ and $|G_1 : \mho_1(G_1)| = p^{p-1}$. Then Theorem 3.2 proves that G_1 is a regular p-group.

(ii) Since G_1 is regular, we have that $|\Omega_1(G_1)| = |G_1 : \mho_1(G_1)| = p^{p-1}$. But $\Omega_1(G_1)$ is normal in G, so necessarily $\Omega_1(G_1) = G_{m-p+1}$. Also, this group has exponent p, again by the regularity of G_1. This proves in particular that $\mho_1(G_i) = G_{i+p-1}$ for $i \geq m-p+1$. Now if $i \leq m-p+1$ then $\Omega_1(G_1) \leq G_i$ and consequently $\Omega_1(G_i) = \Omega_1(G_1)$. Since G_i is also regular, $|G_i : \mho_1(G_i)| = |\Omega_1(G_i)| = p^{p-1}$ and we conclude that $\mho_1(G_i) = G_{i+p-1}$.

(iii) Let $x \in G_i - G_{i+1}$. We know from part (ii) that $x^p \in G_{i+p-1}$. Suppose by way of contradiction that $x^p \in G_{i+p}$. Since $\mho_1(G_{i+1}) = G_{i+p}$, we have that

$G_i/G_{i+p} = \langle \overline{x}, \overline{G}_{i+1} \rangle$ is a regular group generated by elements of order p. It follows from Corollary 2.11 that $\exp G_i/G_{i+p} = p$ and therefore $\mho_1(G_i) \le G_{i+p}$. This is a contradiction with (ii). $\square$

4.4 Proof of Blackburn's Theorem for $|G| \ge p^{p+2}$

Thanks to the knowledge of the power structure of the p-groups of maximal class of order $\ge p^{p+2}$, we can now proceed to the proof of Blackburn's Theorem in this case, which is stated as follows.

Theorem 4.10. *Let G be a p-group of maximal class of order greater than or equal to p^{p+2}. Then:*

(i) *G has uniform elements.*

(ii) *$l(G) \ge 1$.*

Proof. (i) We are going to prove by induction on $i \ge 1$ that $[G_1, G_i] \le G_{i+2}$. Then all the two-step centralizers $C_G(G_i/G_{i+2})$ coincide with G_1 and G has uniform elements.

By Theorem 4.6, we have that $l(G/G_{p+2}) \ge 1$ and consequently $[G_1, G_i] \le G_{i+2}$ for $1 \le i \le p$. On the other hand, if $i > p$ then

$$[G_1, G_i] = [G_1, \mho_1(G_{i-p+1})] = \mho_1([G_1, G_{i-p+1}]) \le \mho_1(G_{i-p+3}) = G_{i+2}, \quad (4.5)$$

where we have used the induction hypothesis and Theorems 4.9 and 2.14.

(ii) Let us suppose that $l(G) = 0$. By part (i) we may consider a chain in G and its associated function α. As seen in the proof of (i), we have $[G_1, G_j] \le G_{j+2}$ for every j and this means that $\alpha(1, j) = 0$ for all possible j. This is a contradiction with Theorem 4.3. $\square$

We have developed the theory of p-groups of maximal class in a way that the proof of Blackburn's Theorem for $|G| \ge p^{p+2}$ relies on determining the power structure of these groups, what in turn depended on Blackburn's Theorem for the case that $|G| \le p^{p+2}$. It is possible, however, to provide a proof of both Theorem 4.10 and the power structure of the p-groups of maximal class of order $\ge p^{p+2}$ without studying first the groups of order $\le p^{p+2}$, as is shown by A. Mann in his paper [19]. Nevertheless, if we aim at presenting a completely developed theory of the p-groups of maximal class, as is our case, the quickest way of obtaining Theorem 4.10 is the one chosen in these notes.

Now we are in a position so as to prove property P7 of the associated function α. The key to it is that the powers s_i^p, which according to Theorem 4.9 belong to $G_{i+p-1} - G_{i+p}$, may be determined modulo G_{i+p}.

Theorem 4.11. *Let G be a p-group of maximal class of order greater than or equal to p^{p+2}. Consider a chain $\{s_i\}$ in G and let α be its associated function. Then:*

(i) $s_i^p \equiv s_{i+p-1}^{-1} \pmod{G_{i+p}}$ *for all* $i \geq 1$.

(ii) $\alpha(i,j) = \alpha(i+p-1,j) = \alpha(i,j+p-1)$ *for* $i+j \leq m-l-p$.

Proof. (i) Let $\overline{G} = G/G_{p+2}$. Then $\{\overline{s}_i\}$ is a chain in $\overline{G}$ and, by Lemma 4.8, we have that $\overline{s}_1^p \equiv \overline{s}_p^{-1} \pmod{\overline{G}_{p+1}}$. It follows that $s_1^p \equiv s_p^{-1} \pmod{G_{p+1}}$ and the case $i=1$ is already proved.

Suppose now that $i \geq 2$. According to Theorem 3.15, s_0 and $s_0 s_i$ are conjugate in G: there exists $g \in G$ such that $s_0 s_i = s_0^g$. Then

$$(s_0 s_i)^p = (s_0^g)^p = (s_0^p)^g = s_0^p,$$

since $s_0^p \in Z(G)$. It follows from Hall's compilation formula that $s_i^p \equiv c_p \pmod{\mho_1(H')}$, where $H = \langle s_0, s_i \rangle$. Since $H' \leq G_{i+1}$ and $\mho_1(G_{i+1}) = G_{i+p}$ by Theorem 4.9, we derive that $s_i^p \equiv c_p \pmod{G_{i+p}}$. We may now argue as in the proof of part (i) of Lemma 4.8 to obtain that $c_p \equiv s_{i+p-1}^{-1} \pmod{G_{i+p}}$. This proves that the result holds.

(ii) Let us express the commutador $[s_i^p, s_j]$ in two different ways. On the one hand,

$$[s_i^p, s_j] = s_i^{-p} s_j^{-1} s_i^p s_j = s_i^{-p} (s_i^{s_j})^p.$$

We deduce from the regularity of G_1 that $[s_i^p, s_j] \equiv [s_i, s_j]^p \pmod{\mho_1(H')}$, where $H = \langle s_i^{-1}, s_i^{s_j} \rangle$. Since $H = \langle s_i, [s_i, s_j] \rangle$ and these two generators commute modulo $G_{i+j+l+1}$, it follows that $H' \leq G_{i+j+l+1}$ and, consequently,

$$[s_i^p, s_j] \equiv [s_i, s_j]^p \pmod{G_{i+j+l+p}}.$$

By the definition of $\alpha(i,j)$ we have that $[s_i, s_j] \equiv s_{i+j+l}^{\alpha(i,j)} \pmod{G_{i+j+l+1}}$ and, using again that G_1 is regular, $[s_i, s_j]^p \equiv s_{i+j+l}^{p\alpha(i,j)} \pmod{G_{i+j+l+p}}$. We conclude from part (i) that

$$[s_i^p, s_j] \equiv s_{i+j+l+p-1}^{-\alpha(i,j)} \pmod{G_{i+j+l+p}}.$$

On the other hand, $s_i^p \equiv s_{i+p-1}^{-1} \pmod{G_{i+p}}$ and therefore

$$[s_i^p, s_j] \equiv [s_{i+p-1}^{-1}, s_j] \equiv [s_{i+p-1}, s_j]^{-1} \equiv s_{i+j+l+p-1}^{-\alpha(i+p-1,j)} \pmod{G_{i+j+l+p}}.$$

(All the congruences above are easy to justify. Try to do it.)

If we now compare the two expressions we have obtained for $[s_i^p, s_j]$, it follows that $\alpha(i+p-1,j) = \alpha(i,j)$. Finally, taking into account property P3, $\alpha(i,j+p-1) = -\alpha(j+p-1,i) = -\alpha(j,i) = \alpha(i,j)$. $\square$

Exercises

4.1. Let G be a p-group of maximal class of order p^{p+1}.

(i) Prove that G is irregular and, as a consequence, that all p-groups of maximal class of order $\geq p^{p+1}$ are irregular. (Hint: Let s be a uniform element of G and $s_1 \in G_1 - G_2$. Then $[s_1, s, \overset{p-1}{\ldots}, s] \neq 1$. This means that G does not fulfill one of the conditions in Exercise 3.2.)

(ii) Deduce that $|\mho_1(G)| = p$ and $\exp G = p^2$. Is it true that $\mho_1(G_i) = G_{i+p-1}$ for all $i \geq 1$? (Hint for the question: See what happens with a Sylow p-subgroup of Σ_{p^2}.)

4.2. Prove that a Sylow p-subgroup of Σ_{p^2} cannot be a quotient of a p-group of maximal class of order $> p^{p+1}$. (Hint: Suppose that G has maximal class and order $> p^{p+1}$, and that $H = G/N$ is isomorphic to a Sylow p-subgroup of Σ_{p^2}. What is then the power structure of H_1?)

4.3. Prove that a p-group G has maximal class if and only if G has an element with centralizer of order p^2. (Hint: In order to prove the "if" part, argue by induction on the order of G and take into account Exercise 1.2.)

4.4. Let G be a p-group of maximal class of order p^m.

(i) Prove that G has at most two different two-step centralizers: G_1 and $C_G(G_{m-2})$. Moreover, $G_1 \neq C_G(G_{m-2})$ if and only if $l(G) = 0$.

(ii) Show that any maximal subgroup H of G different from G_1 and $C_G(G_{m-2})$ is again a p-group of maximal class and that $H_i = G_{i+1}$ for all $i \geq 1$.

4.5. Let G be a finite p-group. In this exercise we show that the condition that $G/\gamma_{p+1}(G)$ is a group of maximal class suffices to assure that G is also a group of maximal class. For this purpose, we suppose that for some $k \geq p+1$ the quotient $G/\gamma_k(G)$ has maximal class and prove that $G/\gamma_{k+1}(G)$ has also maximal class.

(i) By factoring out $\gamma_{k+1}(G)$ we may assume that $\gamma_{k+1}(G) = 1$ and $\gamma_k(G) \neq 1$. Prove that $\gamma_k(G)$ has order $\leq p^2$ and exponent p. (Hint: Use Exercises 1.10 and 1.11.)

(ii) Suppose that $p > 2$. Then we may take a chain $\{\overline{s}_i\}$ in $G/\gamma_k(G)$. Prove that, for any subgroup N of G such that $|\gamma_k(G) : N| = p$, G/N is a group of maximal class such that $l(G/N) \geq 1$ and deduce that $[s_{k-1}, s_1] = 1$. Conclude that $|\gamma_k(G)| = p$ and hence that G has maximal class.

(iii) Suppose now that $p = 2$. Take again a subgroup N such that $|\gamma_k(G) : N| = 2$. Prove that $\gamma_k(G) = \mho_1(\gamma_{k-1}(G))N$ for any such N. (Hint: We know either from Exercise 3.3 or from Theorem 4.9 that $\gamma_{k-1}(G/N)$ is cyclic. What subgroup is then $\mho_1(\gamma_{k-1}(G/N))$?) Deduce that $\gamma_k(G) = \mho_1(\gamma_{k-1}(G))$. Then $\gamma_k(G)$ has order 2 and G has maximal class.

4.6. Deduce from the previous exercise that any 2-group such that $|G : G'| = 4$ is a group of maximal class. Is any 2-generated 2-group a group of maximal class? For odd p, does the condition $|G : G'| = p^2$ ensure that G has maximal class?

4.7. Let G be a p-group of maximal class of order $\geq p^{p+2}$. If N is an abelian normal subgroup of G of order p^t and $t = k(p-1) + r$ with $0 \leq r < p-1$, prove that

$$N \cong C_{p^{k+1}} \times \overset{r}{\cdots} \times C_{p^{k+1}} \times C_{p^k} \times \overset{p-r-1}{\cdots} \times C_{p^k}.$$

Lecture 5

The commutator structure of a p-group of maximal class

5.1 The classification of the 2-groups of maximal class

In the proof of Blackburn's Theorem in the previous lecture, it was essential the fact that the p-groups of maximal class have a very regular power structure. In this last lecture we are going to study the commutator structure of G, more precisely the behaviour of the commutator subgroups $[G_i, G_j]$ for $i, j \geq 1$. Naturally, this will be done through the analysis of the degree of commutativity $l(G)$ of the group. The main result, that we establish in Section 5.2, will be that $l(G)$ tends to infinity together with the order of the group. This fact will have surprising consequences about the structure of G. Furthermore, when the prime p equals 2 or 3 it is even possible to give a complete classification of the groups in question. In this first section we present the classification of the 2-groups of maximal class. Recall from Exercise 3.3 that G has a cyclic maximal subgroup in that case (by the way, this may also be seen as a consequence of Theorem 4.9 on the power structure of p-groups of maximal class, check it). We also know from Exercise 1.7 that the groups D_{2^m}, SD_{2^m} and Q_{2^m} have maximal class.

Theorem 5.1. *Let G be a 2-group of maximal class. Then G is isomorphic to one of the groups D_{2^m}, SD_{2^m} or Q_{2^m}.*

Proof. Let $M = \langle a \rangle$ be a cyclic maximal subgroup of G. Since $G_2 \leq M$, we necessarily have that $G_2 = \langle a^2 \rangle$ and consequently $G_i = \langle a^{2^{i-1}} \rangle$ for any $i \geq 2$. It is clear that M coincides with all the two-step centralizers $C_G(G_i/G_{i+2})$ and consequently any $b \in G - M$ is a uniform element of G. (This shows that we do not need Blackburn's Theorem to assure the existence of uniform elements in this case.) Then $G = \langle a, b \rangle$.

According to Theorem 3.15, we have that $b^2 \in Z(G) = \langle a^{2^{m-2}} \rangle$, so $b^2 = 1$ or $a^{2^{m-2}}$. On the other hand, Lemma 3.14 yields that $[a, b] \in \langle a^2 \rangle - \langle a^4 \rangle$. Hence $[a, b] = a^{2i}$ for some odd i, $1 \leq i < 2^{m-2}$. Then

$$1 = [a, b^2] = [a, b]^2 [a, b, b] = a^{4i}[a^{2i}, b] = a^{4i}[a, b]^{2i} = a^{4i}a^{4i^2} = a^{4i(i+1)}$$

and consequently $2^{m-1} \mid 4i(i+1)$. Since i is odd, we deduce that $2^{m-3} \mid i+1$. The condition $i < 2^{m-2}$ only leaves two possibilities: either $i = -1 + 2^{m-3}$ or $i = -1 + 2^{m-2}$. Then $a^b = a[a, b] = a^{1+2i}$ coincides either with $a^{-1+2^{m-2}}$ or with a^{-1}.

Let us now combine the possible cases that have arisen. If $b^2 = 1$ and $a^b = a^{-1+2^{m-2}}$ then $G \cong SD_{2^m}$, while for $a^b = a^{-1}$ we get that $G \cong D_{2^m}$. Assume now that $b^2 = a^{2^{m-2}}$. If $a^b = a^{-1}$ then $G \cong Q_{2^m}$. Let us finally see that in the case $a^b = a^{-1+2^{m-2}}$ the group G is isomorphic to SD_{2^m}. To this end, it suffices to observe that

$$(ba)^2 = b^2 a^b a = b^2 a^{-1+2^{m-2}} a = 1$$

and that $a^{ba} = a^{-1+2^{m-2}}$. □

5.2 Bounds for the degree of commutativity and their consequences

The 3-groups of maximal class were classified by Blackburn in his paper [1]. The key to the classification is the following result about the degree of commutativity.

Theorem 5.2. *Let G be a 3-group of maximal class of order 3^m. Then $l(G) \geq m-4$. Consequently G_1 has class ≤ 2, G_2 is abelian and G has derived length 2 (i.e., G is metabelian).*

Proof. Suppose $l(G) \leq m - 5$ and consider a function α associated to a chain in G. The condition on the degree of commutativity assures that the value $\alpha(1, 3)$ is defined and, by property P7, $\alpha(1, 3) = \alpha(1, 1) = 0$. It follows from property P5 that also $\alpha(1, 2) = 0$. These values are a contradiction with Remark 4.4. Hence $l(G) \geq m - 4$. Consequently $[G_1, G_1, G_1] \leq [G_3, G_1] \leq G_{l+4} = 1$ and $[G_2, G_2] \leq G_{l+4} = 1$. □

The best bound that can be obtained for $p = 5$ is much worse than the one for $p = 3$ and, as a result, the classification problem is much more difficult in this case. As a matter of fact, the 5-groups of maximal class have not been classified yet, even if the computational evidence suggests quite a regular pattern of isomorphism classes (see [22]). In spite of this, the bound we give below has interesting consequences.

Theorem 5.3. *Let G be a 5-group of maximal class of order 5^m. Then $l(G) \geq (m-6)/2$.*

Proof. Let us first make some preliminary remarks. Consider a function α associated to a chain in G. We are going to use freely the properties P1-P7 of α stated in Theorem 4.2. Put $x = \alpha(1,2)$ and let us express some values of α in terms of x. We have that $\alpha(1,3) = x$. On the other hand, by Theorem 4.5, $0 = \alpha(1,5) = \alpha(1,2) - 2\alpha(2,3)$ and therefore $\alpha(2,3) = 3x$. Finally, from the relation $\alpha(1,3) = \alpha(1,4) + \alpha(2,3)$ we obtain that $\alpha(1,4) = 3x$. Since we know from Remark 4.4 that $\alpha(1,j) \neq 0$ for some $j \in \{2,3,4\}$, it follows that $x \neq 0$.

Supose now that $2l(G) \leq m-7$. Then property P6 assures that $\mathcal{J}(1,2,3) = 0$, which is written as

$$\alpha(1,2)\alpha(3+l,3) + \alpha(2,3)\alpha(5+l,1) + \alpha(3,1)\alpha(4+l,2) = 0.$$

We derive from the above calculations that

$$2\alpha(1,5+l) + \alpha(2,4+l) - \alpha(3,3+l) = 0. \tag{5.1}$$

If we use property P4 in the form $\alpha(i,j) = \alpha(i-1,j) - \alpha(i-1,j+1)$, we obtain that

$$\alpha(2,4+l) = \alpha(1,4+l) - \alpha(1,5+l)$$

and

$$\alpha(3,3+l) = \alpha(1,3+l) - 2\alpha(1,4+l) + \alpha(1,5+l).$$

Substituting these values into (5.1), it follows that

$$\alpha(1,3+l) = 3\alpha(1,4+l).$$

Now we may use the periodicity of property P7 to transform this equality so that it relates in the same way two (cyclically) consecutive elements of the set $\{\alpha(1,1), \alpha(1,2), \alpha(1,3), \alpha(1,4)\}$. But this is impossible, since that set is precisely $\{0, x, x, 3x\}$ and $x \neq 0$. So necessarily $2l(G) \geq m-6$, as desired. $\square$

This bound for the degree of commutativity is sharp, since in [12, Theorem 3.8′] C.R. Leedham-Green and S. McKay have constructed, for each even integer $m \geq 6$, a 5-group of maximal class of order 5^m such that $2l(G) = m-6$.

Corollary 5.4. *Let G be a 5-group of maximal class. Then:*

(i) *The class of G_1 is at most 3, and G_2 has class at most 2.*

(ii) *The derived length of G is at most* 3.

Proof. (i) We have that

$$\gamma_4(G_1) = [G_1, G_1, G_1, G_1] = [G_1, G_2, G_1, G_1] \leq [G_4, G_1, G_1] \leq G_{2l+6} \leq G_m = 1,$$

by Theorem 5.3, and on the other hand,

$$\gamma_3(G_2) = [G_2, G_2, G_2] \leq G_{2l+6} = 1.$$

(ii) Since G' is nilpotent of class ≤ 2, its derived length is also ≤ 2. Hence the derived length of G is at most 3. □

Our next objective is to prove that there is a bound valid for any prime similar to the one given in Theorem 5.3 when $p = 5$. This general bound was obtained independently by R.T. Shepherd [25] and C.R. Leedham-Green and S. McKay [12]. The proof of Theorem 5.3 seems difficult to generalize to an arbitrary prime. In this text we follow the idea of Leedham-Green and McKay, that consists in extending the function α to all of $\mathbb{Z} \times \mathbb{Z}$ in a way that it keeps all its properties.

Theorem 5.5. *Let G be a p-group of maximal class of order p^m. Then $l(G) \geq (m - 3p + 6)/2$.*

Proof. Clearly, the bounds we know for the small primes allow us to assume that $p \geq 7$. Suppose that $2l(G) \leq m - 3p + 5$. Since the degree of commutativity is ≥ 0, this yields in particular that $m \geq 3p - 5 \geq p + 9$. Consider a function α associated to a chain in G. Then we extend α to a function $\gamma : \mathbb{Z} \times \mathbb{Z} \to \mathbb{F}_p$ by defining $\gamma(i, j) = \alpha(i_0, j_0)$, where $i_0, j_0 \in \{1, \dots, p-1\}$ are chosen to be congruent to i and j modulo $p - 1$. Note that this makes sense, since

$$m - l - 1 \geq m - \frac{m - 3p + 5}{2} - 1 = \frac{m + 3p - 7}{2} \geq \frac{4p + 2}{2} = 2p + 1$$

and consequently $\alpha(i_0, j_0)$ has an assigned value. Observe that, due to the period $p - 1$ of α, we have that $\gamma(i, j) = \alpha(i, j)$ for any pair (i, j) in the domain of α. Thus γ is an extension of α.

It is straightforward to check that properties P1-P5 and P7 also hold for the extended function γ. On the other hand, in order to prove that γ also fulfills P6, we have to see that $\mathcal{J}(i, j, k) = 0$ for all $i, j, k \in \mathbb{Z}$ (where $\mathcal{J}(i, j, k)$ is defined using γ). Since γ satisfies P7, we have that $\mathcal{J}(i, j, k) = \mathcal{J}(i_0, j_0, k_0)$. If any two of the values i_0, j_0 or k_0 are equal, it is immediate that $\mathcal{J}(i_0, j_0, k_0) = 0$. So we may assume that they are all different. It follows that $i_0 + j_0 + k_0 \leq (p - 3) + (p - 2) + (p - 1) = 3p - 6 \leq m - 2l - 1$ and then all the pairs to which

γ applies in $\mathcal{J}(i_0, j_0, k_0)$ are in the domain of α. Hence we can substitute α for γ throughout and $\mathcal{J}(i_0, j_0, k_0) = 0$ is simply a consequence of P6 for α.

Let us apply P6 to the triple $(i, i+1, 1-l)$ for an arbitrary $i \in \mathbb{Z}$. As $\gamma(i+1, i+1) = 0$ and $\gamma(i, i+2) = \gamma(i, i+1)$, it follows that

$$\gamma(i, i+1)\{\gamma(1-l, 2i+l+1) - \gamma(1-l, i+1)\} = 0. \tag{5.2}$$

Since γ has the same properties as α, the formula in Theorem 4.5 also applies to γ and any $\gamma(i,j)$ may be expressed in terms of the values $x_r = \gamma(r, r+1)$. In particular, that formula provides that

$$\begin{aligned}\gamma(1-l, 2i+l+1) &= \sum_{r=1-l}^{i} (-1)^{r+l-1} \binom{2i+l-r}{r+l-1} x_r \\ &= x_{1-l} - \cdots + (-1)^{i+l-1}(i+l)x_i\end{aligned}$$

and, similarly,

$$\gamma(1-l, i+1) = x_{1-l} + \sum{}',$$

where Σ' denotes some linear combination of the values x_r with $2 - l \le r \le (i-l+1)/2$. Now if we choose $i \ge 2-l$ then $(i-l+1)/2 < i$ and therefore it follows from (5.2) that

$$x_i \left\{ \sum{}'' + (-1)^{i+l-1}(i+l)x_i \right\} = 0, \tag{5.3}$$

where Σ'' is a linear combination of $x_{2-l}, \dots, x_{i-1}$.

Let us prove by induction on i that $x_i = 0$ for $i = 2-l, 3-l, \dots, p-1-l$. If $i = 2-l$ then (5.3) reduces to $-2x_{2-l}^2 = 0$, whence $x_{2-l} = 0$. If $2-l < i \le p-1-l$, the induction hypothesis yields that $x_{2-l} = \cdots = x_{i-1} = 0$ and consequently we have that $\Sigma'' = 0$ in (5.3). Hence $(-1)^{i+l-1}(i+l)x_i^2 = 0$ and, since $i + l \not\equiv 0 \pmod{p}$, it follows that $x_i = 0$. On the other hand, $x_{1-l} = \gamma(1-l, 2-l) = \gamma(p-l, 2-l) = -\gamma(2-l, p-l)$. But according to Theorem 4.5, this last value is a linear combination of $x_{2-l}, \dots, x_{p-1-l}$ and this proves that also $x_{1-l} = 0$.

Since γ has period $p-1$, it follows that $x_r = 0$ for all $r \in \mathbb{Z}$ and again by Theorem 4.5 and by properties P2 and P3, we conclude that $\gamma(i,j) = 0$ for any $i, j \in \mathbb{Z}$. This implies that $\alpha = 0$, which is a contradiction. $\square$

As in the case $p = 5$, the bound in the previous theorem has direct consequences about the structure of G.

Corollary 5.6. *Let G be a p-group of maximal class, where $p > 2$. Then:*

(i) *The class of G_1 is bounded by a function of p alone.*

(ii) *The class of* G_{p-2} *is* ≤ 2.

(iii) *The derived length of* G *is* $\leq \log_2(3p-3)$.

Proof. (i) We have that $G_1' = [G_1, G_2] \leq G_{l+3}$ and, in general, $\gamma_{i+1}(G_1) \leq G_{i(l+1)+2}$. By Theorem 5.2, we may assume that $p > 3$, so that $3p - 8 \geq 2$ and then Theorem 5.5 yields that

$$(3p-8)(l+1) + 2 \geq 2l + 3p - 6 \geq m.$$

Therefore $\gamma_{3p-7}(G_1) = 1$ and the class of G_1 is $\leq 3p - 8$.

(ii) Just observe that $\gamma_3(G_{p-2}) = [G_{p-2}, G_{p-2}, G_{p-2}] \leq G_{2l+3p-6} \leq G_m = 1$.

(iii) We have that $G'' = [G_2, G_3] \leq G_{l+5}$, $G''' \leq G'_{l+5} = [G_{l+5}, G_{l+6}] \leq G_{3l+11}$ and, in general, $G^{(i)} \leq G_t$, where $t = 3 \cdot 2^{i-1} + l(2^{i-1} - 1) - 1$. If the derived length of G is d then $G^{(d-1)} \neq 1$ and consequently

$$3 \cdot 2^{d-2} + l(2^{d-2} - 1) - 1 < m. \tag{5.4}$$

If $l(G) = 0$ then Blackburn's Theorem says that $|G| \leq p^{p+1}$. Hence $3 \cdot 2^{d-2} \leq p + 1$ and $d \leq \log_2 \frac{4}{3}(p+1) \leq \log_2(3p-3)$. (Recall that $p > 2$.)

Suppose now that $l(G) \geq 1$. Since $m \leq 2l + 3p - 6$ by Theorem 5.5, we get from (5.4) that

$$(l+3)2^{d-2} < 3l + 3p - 5.$$

It follows that

$$2^{d-2} < \frac{3l + 3p - 5}{l+3} = 3 + \frac{3p - 14}{l+3} \leq 3 + \frac{3p-14}{4} = \frac{3p-2}{4}$$

and consequently $2^d \leq 3p - 3$. This proves the result. □

There is a counter-intuitive aspect in the previous corollary: it asserts that, in a p-group whose class is as large as possible, there are however large subgroups whose class keeps small regardless of the order of the group. In particular, it follows from (ii) that any p-group of maximal class G can be surprisingly constructed from a group of class ≤ 2 by putting on top a group whose order only depends on p, and not on the order of G. On the other hand, note that the bound for the class of the maximal subgroup G_1 that we have found in the proof of (i) is far from being sharp: the best bound is $(p+1)/2$, as proved by R.T. Shepherd in [25].

We want to end this section with a remark about the sharpness of the bound for $l(G)$ obtained in Theorem 5.5. When $p = 5$ we already know the best possible bound, so we only need to worry when $p \geq 7$. In that case, it has been proved by the author [4] that the bound $l(G) \geq (m - 2p + 5)/2$ holds. This cannot be refined further, since Leedham-Green and McKay have constructed groups of arbitrarily large order with this degree of commutativity in [13, Theorem 6.8].

5.3 Suggestions for further study

It has been the aim of the author that these notes about the theories of regular p-groups and p-groups of maximal class both lay the foundations for and arouse the interest in embarking on a deeper study of finite p-group theory. In the hope that the objective has been achieved with some of the readers, I would like to end with some hints as to what direction to follow from this point onwards.

One possibility is to continue studying either of the families of p-groups described. In what respects regular p-groups, there is an important topic that we have left out in these notes, which is the existence of bases: a basis is a set $\{x_1, \ldots, x_d\}$ such that any $x \in G$ may be expressed uniquely in the form $x = x_1^{n_1} \ldots x_d^{n_d}$, with $0 \leq n_i < o(x_i)$ for each i. The proof that regular p-groups have bases can be found in Hall's original paper [5]; consult also [21] for a simplification in Hall's proof. I also recommend the series of papers by A. Mann [16, 17, 20]. In the first two, he investigates the minimal irregular groups, that is, p-groups all of whose proper sections are regular. The last one is devoted to normal subgroups N which are regularly embedded in a p-group G: this means that for all $x \in G$, $y \in N$, $x^p y^p = (xy)^p z$ for some $z \in \mho_1(\langle x, y\rangle')$. On the other hand, in [18] Mann studies the p-groups G such that G, as well as all sections of G, satisfy one of the properties (ii), (iii) or (iv) in Theorem 2.10.

As for p-groups of maximal class, the papers by C.R. Leedham-Green and S. McKay on the subject [12, 13, 14] provide an elegant way of constructing all the p-groups of maximal class in which the subgroup G_1 has class ≤ 2. They also study the classification problem and the automorphisms for a particular type of these groups in [15].

Another possibility I would like to comment on is to take up the theory of powerful p-groups and the study of p-groups according to their coclass. These two topics are particularly interesting because there has been very active research on them in the last two decades. On the one hand, powerful p-groups, which are defined by the condition that $G' \leq \mho_1(G)$ if $p > 2$, constitute a class of p-groups with a tame behaviour with respect to p-powers. So in this respect they resemble regular groups and, even if their theories are not directly related, they have some similar properties. For instance, powerful p-groups also have an interchanging property for commutators of agemo subgroups, although it does not apply to all normal subgroups. It is possible now to have access to the main properties of powerful p-groups without browsing research papers: the books [2] and [10], by J.D. Dixon et al. and E.I. Khukhro respectively, include a chapter on the subject. In the same way as regular p-groups serve for the development of the theory of p-groups of maximal class, there have been found several applications of powerful

p-groups. I would like to point out their use in the study of p-groups with a fixed coclass. The coclass of a p-group of order p^m and nilpotency class c is defined to be $m - c$. Thus the p-groups of maximal class are precisely the p-groups of coclass one. An appropriate use of powerful p-groups has permitted to generalize to arbitrary coclass some of the results we have proved for p-groups of maximal class. This has been a long term project, with many group-theorists involved, that finds its culmination in Leedham-Green's and Shalev's papers [11] and [24]. The most important result in these papers is that any p-group of coclass r has a normal subgroup of class ≤ 2 whose index is bounded by a function of p and r.

A final suggestion for further study is to dive into the theory of pro-p groups. These are inverse limits of finite p-groups and are also topological groups, with the topology inherited from the product topology. Although Shalev's proofs do not rely on them, these groups have played a very important role in the study of p-groups according to their coclass. Even if this is not the only application of pro-p groups to finite p-groups, the theory of pro-p groups also deserves attention for its own sake and research on the subject is very lively nowadays. The above-mentioned book [2] by Dixon et al. is a good way of getting started in this theory. On the other hand, the new book [3] by M.P.F. du Sautoy, D. Segal and A. Shalev includes the latest issues of research on this topic.

Bibliography

[1] N. BLACKBURN, On a special class of p-groups, *Acta Math.* **100** (1958), 45-92.

[2] J.D. DIXON, M.P.F. DU SAUTOY, A. MANN, D. SEGAL "Analytic pro-p groups", second enlarged edition, Cambridge Studies in Advanced Mathematics **61**, Cambridge University Press, Cambridge, 1999.

[3] M.P.F. DU SAUTOY, D. SEGAL, A. SHALEV, "New horizons in pro-p groups", Progress in Mathematics, Birkhäuser, Boston, 2000.

[4] G.A. FERNÁNDEZ ALCOBER, The exact lower bound for the degree of commutativity of a p-group of maximal class, *J. Algebra* **174** (1995), 523-530.

[5] P. HALL, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.* **36** (1933), 29-95.

[6] P. HALL, "Nilpotent groups", Queen Mary College Math. Notes, London, 1969.

[7] B. HUPPERT, "Endliche Gruppen, I", Springer, Berlin, 1967.

[8] B. HUPPERT, N. BLACKBURN, "Finite groups, II", Springer, Berlin, 1982.

[9] R. JAMES, The groups of order p^6 (p an odd prime), *Math. Comput.* **34** (1980), 613-637.

[10] E.I. KHUKHRO, "p-Automorphisms of finite p-groups", Cambridge University Press, Cambridge, 1997.

[11] C.R. LEEDHAM-GREEN, The structure of finite p-groups, *J. London Math. Soc. (2)* **50** (1994), 49-67.

[12] C.R. LEEDHAM-GREEN, S. MCKAY, On p-groups of maximal class, I, *Quart. J. Math. Oxford (2)* **27** (1976), 297-311.

[13] C.R. Leedham-Green, S. McKay, On p-groups of maximal class, II, *Quart. J. Math. Oxford (2)* **29** (1978), 175-186.

[14] C.R. Leedham-Green, S. McKay, On p-groups of maximal class, III, *Quart. J. Math. Oxford (2)* **29** (1978), 281-299.

[15] C.R. Leedham-Green, S. McKay, On the classification of p-groups of maximal class, *Quart. J. Math. Oxford (2)* **35** (1984), 293-304.

[16] A. Mann, Regular p-groups, *Israel J. Math.* **10** (1971), 471-477.

[17] A. Mann, Regular p-groups, II, *Israel J. Math.* **14** (1973), 294-303.

[18] A. Mann, The power structure of p-groups, I, *J. Algebra* **42** (1976), 121-135.

[19] A. Mann, Regular p-groups and groups of maximal class, *J. Algebra* **42** (1976), 136-141.

[20] A. Mann, Regular p-groups, III, *J. Algebra* **70** (1981), 89-101.

[21] Ming-Yao Xu, P. Hall's basis theorem for regular p-groups and its application to some classification problems, *Comm. Algebra* **19** (1991), 1271-1280.

[22] M.F. Newman, Groups of prime-power order, *Groups – Canberra 1989*, Lecture Notes in Mathematics (Springer, Berlin) **1456** (1990), 49-62.

[23] E.A. O'Brien, The groups of order 256, *J. Algebra* **143** (1991), 219-235.

[24] A. Shalev, The structure of finite p-groups: effective proof of the coclass conjectures, *Invent. Math.* **115** (1994), 315-345.

[25] R.T. Shepherd, "p-Groups of maximal class", Ph. D. thesis, University of Chicago, 1970.

[26] M. Suzuki, "Group Theory, II", Springer, Berlin, 1986.

[27] A. Wiman, Über mit Diedergruppen verwandte p-Gruppen, *Arkiv för Matematik, Astronomi och Fysik* **33A** (1946), 1-12.

[28] A. Wiman, Über p-Gruppen von maximaler Klasse, *Acta Math.* **88** (1952), 317-346.