eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
ZTF-FCT
Zientzia eta Teknologia Fakultatea
Facultad de Ciencia y Tecnología

Finite p-groups

Final Degree Dissertation
Degree in Mathematics

Iker de las Heras Kerejeta

Supervisor:
Gustavo Adolfo Fernández Alcober

Leioa, June 24, 2015

Contents

Introduction

The objective of this dissertation is the study of a fundamental type of finite groups, the finite p-groups for a prime number p. In the redaction of it we have presupposed some familiarity with the basic theory of the group theory, as well as some basic results of the action of a group in a set and the theory of representation.

For the analysis of finite p-groups, it is essential the knowledge of some concepts. Thus, in the first chapter we firstly introduce the concept of *commutator of elements* as well as the *commutator of subgroups*, studying some of their properties, giving generators for a commutator of subgroups, and proving the so-called Three Subgroup Lemma, which will be used constantly throughout the dissertation. Making use of this, we also define and study the central series of a group with special emphasis in the lower and the upper central series. Finally, the nilpotent groups are analysed and we give some characterizations of them for general groups and two more characterizations for finite groups. All these notions are based on the notes [2] and they are presented in the first chapter in order to familiarise with them and, therefore, facilitate the understanding of the second and the third ones.

In the second chapter, based also on [2], some general results of finite p-groups are presented. First, we will prove that they are nilpotent, so that the finite p-groups satisfy the properties of nilpotent groups. We also define the *Frattini subgroup* of a group as the intersection of its maximal subgroups and we show that its elements are called *non-generators* since they can be removed from any system of generators of the group. Furthermore, we unite these two ideas, proving the Burnside Basis Theorem, which shows that a finite p-group can always be seen as a vector-space if we factor out its Frattini subgroup. The *Omega* and *Agemo* subgroups are defined in other to give a result which allows us to calculate the Frattini subgroup explicitly. Finally, we will analyse the orders of central factors of the lower and the upper central series, and we will define the p-groups of *maximal class*, showing that in this special kind of groups, the lower and the upper central series coincide and that they are as large as possible.

Finally in the last chapter, based on material from three research papers, we develop the theory of a really special kind of finite p-groups introduced in 1987: the *powerful p-groups*. This definition can be extended for subgroups to define the *powerfully embedded* subgroups, and thus, it is proved that if a finite p-group is powerful, then its Frattini subgroup, the subgroups of the lower central series, the subgroups of the derived series, etc. are powerfully embedded subgroups. These groups satisfy really interesting properties. Indeed, they have many properties in common with abelian groups. For instance, the minimum number of generators of a subgroup

of a powerful p-group is less than or equal to the minimum number of generators of the group for $p > 2$ ([4]), or the subgroup generated by all the elements of order less than or equal to a power of p, is exactly the set formed by these elements ([3]). To finalise the chapter, we delve deeper and, based on [8], we prove that although any finite p-group can not be seen as a subgroup of a powerful p-group, any p-group can be seen as a section of a powerful p-group.

In the Appendix, we expose some examples and exercises to a better understanding of all the concepts presented in these three chapters.

Chapter 1

Commutators and Nilpotent Groups

We begin this chapter with the definition of the *commutator*, which will be used again and again throughout the dissertation. We also will study the *central series* of a group and we will expose some examples to a better understanding of them. Finally, we will give the definition of *nilpotent groups* and some properties which will characterize them.

1.1 Commutators and commutator calculus

Definition 1.1. Let G be a group and $x, y \in G$. The *commutator* of x and y is the element

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

If we have n elements, the commutator is recurrently calculated:

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

We say that this is a commutator of length n.

Remark 1.2. For convenience, we also speak about commutators of length 1, by which we simply mean elements of the group G. This is very useful when we want to prove results by induction on the length of commutators.

We can also define the commutator between subsets of a group G.

Definition 1.3. If $X, Y \subseteq G$,

$$[X, Y] = \langle\, [x, y] \mid x \in X, y \in Y \rangle.$$

Similarly, we can define the commutator of n subsets as

$$[X_1, \ldots, X_n] = [[X_1, \ldots, X_{n-1}], X_n].$$

Remark 1.4. Again, it is interesting to define commutators of length 1 when working with *subgroups*. In this case, the commutator is the subgroup itself.

In order to work with the commutator, we should know the way in which it interacts with multiplication, inversion, conjugation, etc. In this section we will see different results which will let us make calculus with them.

Theorem 1.5. *Let G be a group and $x, y, z \in G$. The commutator between elements has the following properties:*

i) *x and y commute* $\Leftrightarrow [x, y] = 1$.

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

iii) $x^y = x[x, y]$ *and* $xy = yx[x, y]$.

iv) *If we have a group homomorphism $\sigma : G \to G^*$, then*

$$\sigma([x, y]) = [\sigma(x), \sigma(y)].$$

In particular, if the homomorphism is conjugation,

$$[x, y]^z = [x^z, y^z].$$

v)

$$[xy, z] = [x, z]^y[y, z]$$

and

$$[x, yz] = [x, z][x, y]^z.$$

vi) *For any $n \in \mathbb{N}$,*

$$[x^n, y] = [x, y]^{x^{n-1}}[x, y]^{x^{n-2}} \dots [x, y]^x[x, y]$$

and

$$[x, y^n] = [x, y][x, y]^y \dots [x, y]^{y^{n-2}}[x, y]^{y^{n-1}}.$$

vii) *Witt's identity:*

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

Proof. *i)* If $[x, y] = 1$, by definition,

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

and this holds if and only if $xy = yx$, that is, if x and y commute.

ii) Using the definition of the commutator,

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

and this is equal to $[y, x]$.

iii) It is a direct consequence of the definition of the commutator.

iv) Using the definition of homomorphism,

$$\begin{aligned}\sigma([x,y]) &= \sigma(x^{-1}y^{-1}xy) = \sigma(x^{-1})\sigma(y^{-1})\sigma(x)\sigma(y)\\ &= \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y) = [\sigma(x),\sigma(y)].\end{aligned}$$

v) On the one hand,

$$[xy,z] = (xy)^{-1}z^{-1}(xy)z = y^{-1}x^{-1}z^{-1}xyz.$$

On the other hand,

$$\begin{aligned}[x,z]^y[y,z] &= (x^{-1}z^{-1}xz)^y y^{-1}z^{-1}yz\\ &= y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz\\ &= y^{-1}x^{-1}z^{-1}xyz.\end{aligned}$$

Therefore, the identity is proved. The other one is proved analogously.

vi) Induction on n. For $n = 1$ it is obvious. For a general n, we have

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

and by hypothesis of induction, this is equal to

$$[x,y]^{x^{n-1}}[x,y]^{x^{n-2}}\dots[x,y]^x[x,y].$$

The proof of the other result is similar.

vii) We just have to expand the commutators:

$$\begin{aligned}&[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x\\ &\quad= y^{-1}[[x,y^{-1}],z]yz^{-1}[[y,z^{-1}],x]zx^{-1}[[z,x^{-1}],y]x\\ &\quad= y^{-1}[y^{-1},x]z^{-1}[x,y^{-1}]zyz^{-1}[z^{-1},y]x^{-1}\\ &\qquad\qquad [y,z^{-1}]xzx^{-1}[x^{-1},z]y^{-1}[z,x^{-1}]yx\\ &\quad= y^{-1}yx^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}zyz^{-1}zy^{-1}z^{-1}yx^{-1}y^{-1}zyz^{-1}\\ &\qquad\qquad xzx^{-1}xz^{-1}x^{-1}zy^{-1}z^{-1}xzx^{-1}yx = 1.\end{aligned}$$

□

Corollary 1.6. *Let G be a group and $x,y \in G$. If x commutes with $[x,y]$, then $[x^n,y] = [x,y]^n$ for all $n \in \mathbb{N}$. In the same way, if y commutes with $[x,y]$, then $[x,y^n] = [x,y]^n$.*

Proof. If x commutes with $[x,y]$, it follows that $[x,y]^{x^i} = [x,y]$ for any $i \geq 0$, and using the sixth part of the previous theorem,

$$[x^n,y] = [x,y]^{x^{n-1}}[x,y]^{x^{n-2}}\dots[x,y]^x[x,y] = [x,y]^n,$$

so we are done. □

Theorem 1.7. *Let G be a group and H and K subgroups of G. Then,*

i) H normalizes K if and only if $[H,K] \leq K$. Furthermore, H centralizes K if and only if $[H,K] = 1$.

ii) $[H,K] = [K,H]$.

iii) If $\sigma : G \to G^*$ is a homomorphism, then $\sigma([H,K]) = [\sigma(H), \sigma(K)]$.

Proof. i) By definition,

$$[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle = \langle (k^{-1})^h k \mid h \in H, k \in K \rangle,$$

and since H normalizes K, $(k^{-1})^h \in K$, so that

$$[H,K] \leq \langle k_1 k_2 \mid k_1, k_2 \in K \rangle = K.$$

The converse is also true because if $[H,K] \leq K$, the generators of $[H,K]$ are in K, i.e. $(k^{-1})^h k \in K$, so $k^h \in K$ for all $h \in H$.

Moreover, $[H,K] = 1$ implies that the generators of $[H,K]$ are in the trivial subgroup, so

$$(k^{-1})^h k = 1,$$

whence $k^h = k$ for all $k \in K, h \in H$, which proves that H centralizes K. In the same way, if H centralizes K, then $(k^{-1})^h k = 1$ for all $h \in H$ and $k \in K$, so $[H,K] = 1$.

ii) We have

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

iii) Using the property "the images of the generators of a group are generators of the image of the group",

$$\begin{aligned} \sigma([H,K]) &= \sigma(\langle [h,k] \mid h \in H, k \in K \rangle) \\ &= \langle \sigma([h,k]) \mid h \in H, k \in K \rangle \\ &= \langle [\sigma(h), \sigma(k)] \mid h \in H, k \in K \rangle \\ &= [\sigma(H), \sigma(K)]. \end{aligned}$$

□

Using this theorem, the following results are immediate.

Corollary 1.8. *Let G be a group. Then,*

i) $H \leq Z(G) \Leftrightarrow [H,G] = 1$.

ii) $N \trianglelefteq G \Leftrightarrow [N,G] \leq N$.

Corollary 1.9. *Let G be a group, N a normal subgroup of G and let us put $\overline{G} = G/N$. Then,*

$$\overline{[H,K]} = \left[\overline{H}, \overline{K}\right],$$

for every $H, K \leq G$.

Proof. It is enough to consider the homomorphism

$$\begin{array}{rccc} \sigma : & G & \longrightarrow & \overline{G} \\ & g & \longmapsto & \overline{g}. \end{array}$$

□

Corollary 1.10. *i) If H and K are characteristic subgroups in G, then $[H,K]$ is also characteristic, i.e., it is fixed under all automorphisms of G.*

ii) If $H, K \trianglelefteq G$, then $[H,K] \trianglelefteq G$.

Theorem 1.11. *Let G be a group and $H, K \leq G$. Then, both H and K normalize $[H,K]$. In other words, $[H,K] \trianglelefteq \langle H, K\rangle$.*

Proof. Let us see that H normalizes $[H,K]$. We have to check that $[h,k]^{h'} \in [H,K]$ for every $h, h' \in H$ and $k \in K$. Using the fifth property of Theorem 1.5,

$$[hh', k] = [h,k]^{h'}[h',k],$$

so that,

$$[h,k]^{h'} \in [H,K]$$

since $[hh', k], [h', k] \in [H,K]$. Likewise, by symmetry, K normalizes $[H,K]$, and the theorem follows. □

In general, if $n \geq 3$, $[X_1, \ldots, X_n]$ and $\langle\, [x_1, \ldots, x_n] \mid x_i \in X_i\rangle$ need not be equal, even in the case that $X_1, \ldots, X_n$ are subgroups of G. For example, if we consider the subgroups $H_i = \langle (i \;\; i+1)\rangle$ of Σ_n for $1 \leq i \leq n-1$ with $n \geq 3$, then

$$\langle [h_1, \ldots, h_{n-1}] \mid h_i \in H_i\rangle = \langle (1 \;\; n-1 \;\; n)\rangle$$

while $[H_1, \ldots, H_{n-1}] = A_n$, as we will see in Exercise 4 in the Appendix.

However, this problem disappears if we are working with normal subgroups. Moreover, the following theorem gives generators of the groups of the type $[N_1, \ldots, N_n]$ where $N_i \trianglelefteq G$ for all $i = 1, \ldots, n$ if we know generators of all the subgroups $N_1, \ldots, N_n$. This is really useful when working with this kind of groups. We will start with a lemma.

Lemma 1.12. *Let G be a group and H a subgroup of G. Then,*

$$C_G(H) \trianglelefteq N_G(H).$$

Proof. Let us take $x \in C_G(H^g)$. By Theorem 1.5, this happens if and only if $[h^g, x] = 1$ for all $h \in H$, and we observe that

$$[h^g, x] = 1, \forall h \in H \Leftrightarrow [h, x^{g^{-1}}]^g = 1, \forall h \in H \Leftrightarrow [h, x^{g^{-1}}] = 1, \forall h \in H.$$

Again, by Theorem 1.5, this happens if and only if $x^{g^{-1}} \in C_G(H)$, that is, $x \in C_G(H)^g$. Thus, we have proved that

$$C_G(H^g) = C_G(H)^g.$$

Now, taking $g \in N_G(H)$, we have

$$C_G(H^g) = C_G(H).$$

Thus, $C_G(H)^g = C_G(H)$ for all $g \in N_G(H)$, and we are done. □

Theorem 1.13. *Let G be a group, $N_1, \dots, N_k$ normal subgroups of G and $X_1, \dots, X_k$ subsets such that $N_i = \langle X_i \rangle$, for all $i = 1, \dots, k$. Then,*

$$[N_1, \dots, N_k] = \langle [x_1, \dots, x_k]^g \mid x_i \in X_i, g \in G \rangle.$$

In particular,

$$[N_1, \dots, N_k] = \langle [n_1, \dots, n_k] \mid n_i \in N_i \rangle.$$

Proof. Induction on k. For $k = 1$ it is obvious.

Let us prove the result for a general k, supposing that it is true for $k - 1$. We put

$$N = \langle [x_1, \dots, x_k]^g \mid x_i \in X_i, g \in G \rangle$$

to simplify the notation. By Corollary 1.10, $[N_1, \dots, N_k]$ is normal in G, so it is trivial that

$$N \subseteq [N_1, \dots, N_k],$$

so let us prove the other inclusion. Since N is obviously normal, we consider $\overline{G} = G/N$. Thus, if we take any $x_k \in X_k$, we have $[\overline{x}_1, \dots, \overline{x}_{k-1}, \overline{x}_k] = [[\overline{x}_1, \dots, \overline{x}_{k-1}], \overline{x}_k] = \overline{1}$, so $[\overline{x}_1, \dots, \overline{x}_{k-1}] \in C_{\overline{G}}(\overline{N}_k)$, since $\overline{N}_k = \langle \overline{X}_k \rangle$. In addition, $\overline{N}_k$ is normal in $\overline{G}$, and by the previous lemma, $C_{\overline{G}}(\overline{N}_k)$ is also normal in $\overline{G}$, so $[\overline{x}_1, \dots, \overline{x}_{k-1}]^{\overline{g}} \in C_{\overline{G}}(\overline{N}_k)$ and then

$$[[\overline{x}_1, \dots, \overline{x}_{k-1}]^{\overline{g}}, \overline{n}_k] = \overline{1}$$

for all $x_i \in X_i$, $g \in G$ and $n_k \in N_k$. By hypothesis of induction,

$$[N_1, \dots, N_{k-1}] = \langle [x_1, \dots, x_{k-1}]^g \mid x_i \in N_i, g \in G \rangle,$$

so $\overline{n_k}$ commutes with the generators of $[\overline{N}_1, \dots, \overline{N}_{k-1}]$ and

$$[\overline{N}_1, \dots, \overline{N}_{k-1}, \overline{N}_k] = \overline{1},$$

that is,

$$[N_1, \dots, N_k] \subseteq N,$$

as required.

In particular, by taking $X_i = N_i$ for all $i = 1, \dots, k$, we get the second result in the statement of the theorem. □

It is interesting to know the relation between $[HK, L]$ and $[H, L][K, L]$. The theorem below shows that if H normalizes L these two terms are equal, but to prove this, firstly, we need a lemma.

Lemma 1.14. *Let G be a group and $H, K \leq G$ such that H normalizes K. Then, $HK \leq G$.*

Proof. It is known that HK is a subgroup if and only if $HK = KH$. Since H normalizes K, we have $H^k = H$ for all $k \in K$, so

$$HK = \bigcup_{k\in K} Hk = \bigcup_{k\in K} kk^{-1}Hk = \bigcup_{k\in K} kH^k = \bigcup_{k\in K} kH = KH,$$

as we wanted. □

Theorem 1.15. *Let H, K and L be subgroups of a group G. If H normalizes L, then*

$$[HK, L] = [H, L][K, L] \text{ and } [L, HK] = [L, H][L, K].$$

Proof. By Theorem 1.7, it suffices to prove the first equality. Obviously, $[H, L]$ and $[K, L]$ are contained in $[HK, L]$, so

$$[H, L][K, L] \subseteq [HK, L].$$

To prove the other inclusion, first of all it is necessary to check that $[H, L][K, L]$ is a subgroup of G. Thus, if we see that the generators of $[HK, L]$ are in $[H, L][K, L]$ we will be done. So, is $[H, L][K, L]$ a subgroup?

Using the previous lemma, it is enough to see that $[H, L]$ normalizes $[K, L]$. By Theorem 1.11, L normalizes $[K, L]$, and since H normalizes L, by Theorem 1.7, we have $[H, L] \leq L$. Then, $[H, L]$ normalizes $[K, L]$ and $[H, L][K, L]$ is a subgroup.

Now we have to check that the generators of

$$[HK, L] = \langle [hk, l] \mid h \in H, k \in K, l \in L \rangle$$

are in $[H, L][K, L]$. Indeed,

$$[hk, l] = [h, l][h, l, k][k, l] = [h, l][[h, l], k][k, l],$$

and since H normalizes L,

$$[[h, l], k] \in [[H, L], K] \subseteq [L, K] = [K, L]$$

so the proof is complete. □

Corollary 1.16. *Let G be a group and $H, K, L \leq G$, such that HK is a subgroup of G. If one of the subgroups H or K normalizes L, then*

$$[HK, L] = [H, L][K, L].$$

Remark 1.17. In particular, if $N \trianglelefteq G$, we have

$$[HK, N] = [H, N][K, N] \text{ and } [N, HK] = [N, H][N, K].$$

Theorem 1.18 (P. Hall's Three Subgroup Lemma)**.** *Let G be a group and N a normal subgroup of G. If $[H, K, L] \leq N$ and $[K, L, H] \leq N$, then $[L, H, K] \leq N$.*

Proof. Let us take first $N = 1$. Thus, we have $[H, K, L] = 1$ and $[K, L, H] = 1$, so what we have to prove is that $[L, H, K] = 1$.

By Witt's identity, if we take $h \in H$, $k \in K$ and $l \in L$, then $[l, h^{-1}, k] = 1$. Since h can be an arbitrary element of the subgroup H we can replace h by h^{-1}, so $[l, h, k] = [[l, h], k] = 1$. In other words, every $k \in K$ commutes with all generators $[l, h]$ of $[L, H]$. It follows that $[L, H, K] = [[L, H], K] = 1$.

If $N \neq 1$, we take $\overline{G} = G/N$, and we have $\overline{[H, K, L]} = \overline{1}$ and $\overline{[K, L, H]} = \overline{1}$. Then, as we have just proved $\overline{[L, H, K]} = \overline{1}$, and this means that $[L, H, K] \leq N$. □

1.2 Lower central series

Definition 1.19. The *lower central series* of a group G is the descending series of subgroups denoted $\{\gamma_i(G)\}_{i \geq 1}$ and defined as

$$\begin{aligned}
&\gamma_1(G) = G \\
&\gamma_2(G) = [G, G] \\
&\gamma_3(G) = [\gamma_2(G), G] = [G, G, G] \\
&\quad \vdots \\
&\gamma_i(G) = [\gamma_{i-1}(G), G] = [G, \overset{i}{\ldots}, G] \\
&\quad \vdots
\end{aligned}$$

Definition 1.20. The subgroup $\gamma_2(G) = [G, G]$ is called *the derived subgroup* or *the commutator subgroup* of G, and it is denoted G'.

The derived subgroup is important because it is the smallest normal subgroup of G such that the quotient group of G by this subgroup is abelian. In other words, G/N is abelian if and only if N contains the derived subgroup. Indeed, if $\overline{G} = G/N$,

$$\overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x} \Leftrightarrow [\overline{x}, \overline{y}] = \overline{1} \Leftrightarrow [x, y] \in N,$$

for all $x, y \in G$.

Proposition 1.21. *Every subgroup of the lower central series of a group G is characteristic.*

Proof. It is immediate by Corollary 1.10. □

Remark 1.22. Let G be a group and $N \trianglelefteq G$. If we put $\overline{G} = G/N$, then, by Corollary 1.9

$$\gamma_i(\overline{G}) = \overline{\gamma_i(G)},$$

in other words,

$$\gamma_i(G/N) = \gamma_i(G)N/N.$$

Theorem 1.23. *Let G be a group and X a subset such that $G = \langle X \rangle$. Then,*

$$\gamma_i(G) = \langle [x_1, \ldots, x_i]^g \mid x_j \in X, g \in G \rangle$$

for every $i \geq 2$. In particular,

$$\gamma_i(G) = \langle [g_1, \ldots, g_i] \mid g_j \in G \rangle.$$

Proof. It is enough to apply Theorem 1.13 and the definition of $\gamma_i(G)$. □

Corollary 1.24. *If $G = \langle X \rangle$, then*

$$\gamma_i(G) = \langle [x_1, \ldots, x_i], \gamma_{i+1}(G) \mid x_j \in X \rangle.$$

Proof. It is obvious that

$$\gamma_i(G) \supseteq \langle [x_1, \ldots, x_i], \gamma_{i+1}(G) \mid x_j \in X \rangle.$$

By the previous theorem, it suffices to see that the generators $[x_1, \ldots, x_i]^g$ of $\gamma_i(G)$ are in the subgroup on the right. Applying Theorem 1.5,

$$[x_1, \ldots, x_i]^g = [x_1, \ldots, x_i][[x_1, \ldots, x_i], g] = [x_1, \ldots, x_i][x_1, \ldots, x_i, g],$$

and $[x_1, \ldots, x_i, g] \in \gamma_{i+1}(G)$, so we are done. □

Lemma 1.25. *Let G be a group. Then,*

$$[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G),$$

for $i, j \geq 0$.

Proof. We will demonstrate it by induction on j. For $j = 1$, $\gamma_1(G) = G$, so

$$[\gamma_i(G), \gamma_1(G)] = [\gamma_i(G), G] = \gamma_{i+1}(G),$$

and it holds. If it is true for $j-1$, let us see that it is true for j. By hypothesis of induction, we have $[\gamma_{j-1}(G), \gamma_i(G), G] \leq [\gamma_{i+j-1}(G), G] = \gamma_{i+j}(G)$ and $[\gamma_i(G), G, \gamma_{j-1}(G)] = [\gamma_{i+1}(G), \gamma_{j-1}(G)] \leq \gamma_{i+j}(G)$, and using the Three Subgroup Lemma,

$$[G, \gamma_{j-1}(G), \gamma_i(G)] = [\gamma_{j-1}(G), G, \gamma_i(G)] = [\gamma_j(G), \gamma_i(G)] = [\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G).$$

□

Theorem 1.26. *Let G be a group and $X, Y \subseteq G$ such that $G/G' = \langle \overline{X} \rangle$ and $\gamma_{i-1}(G)/\gamma_i(G) = \langle \overline{Y} \rangle$. Then,*

$$\frac{\gamma_i(G)}{\gamma_{i+1}(G)} = \langle [\overline{x}, \overline{y}] \mid x \in X, y \in Y \rangle.$$

Proof. It suffices to see that $\gamma_i(G) = \langle [x,y], \gamma_{i+1}(G) \mid x \in X, y \in Y \rangle$. We put

$$N = \langle [x,y], \gamma_{i+1}(G) \mid x \in X, y \in Y \rangle$$

to simplify the notation, and since $[x,y] \in [X,Y] = [Y,X] \subseteq [\gamma_{i-1}(G), G] = \gamma_i(G)$, it is clear that

$$N \subseteq \gamma_i(G).$$

Let us see that N is normal in G. Taking the generators, we have $[x,y]^g = [x,y][x,y,g]$ for every $x \in X, y \in Y, g \in G$, and $[x,y,g] \in \gamma_{i+1}(G)$. Furthermore, $\gamma_{i+1}(G)$ is normal in G, so N is also normal.

By hypothesis, $G/G' = \langle \overline{X} \rangle$ and $\gamma_{i-1}(G)/\gamma_i(G) = \langle \overline{Y} \rangle$, that is, $G = \langle X, G' \rangle$ and $\gamma_{i-1}(G) = \langle Y, \gamma_i(G) \rangle$, and by Theorem 1.13,

$$\gamma_i(G) = [\gamma_{i-1}(G), G] = \langle [x,y]^g, [a,y]^g, [x,b]^g, [a,b]^g \mid x \in X, y \in Y, a \in G', b \in \gamma_i(G), g \in G \rangle.$$

Since N is normal, it suffices to check that $[x,y], [a,y], [x,b], [a,b] \in N$. It is obvious that $[x,y] \in N$, and furthermore, $[a,y] \in [G', \gamma_{i-1}(G)] \leq \gamma_{i+1}(G)$, $[x,b] \in [G, \gamma_i(G)] = \gamma_{i+1}(G)$ and $[a,b] \in [G', \gamma_i(G)] \leq \gamma_{i+2}(G) \leq \gamma_{i+1}(G)$, so $\gamma_i(G) \subseteq N$, and we have finished. □

Definition 1.27. We say that a group G has finite exponent if there exists a natural number e such that $g^e = 1$ for all $g \in G$. The minimum value of e is called the *exponent* of G and we denote it by $\exp G$.

Lemma 1.28. *Let G be a group. Then, the factor group $\gamma_i(G)/\gamma_{i+1}(G)$ is abelian for all $i \geq 1$.*

Proof. We have

$$\gamma_i(G)' = [\gamma_i(G), \gamma_i(G)] \leq [\gamma_i(G), G] = \gamma_{i+1}(G),$$

so the quotient is abelian. □

Theorem 1.29. *Let G be a group such that $\exp G/G' < \infty$. Then, $\exp \gamma_i(G)/\gamma_{i+1}(G) < \infty$ for all $i > 1$. Moreover,*

$$\exp \frac{\gamma_i(G)}{\gamma_{i+1}(G)} \mid \exp \frac{\gamma_{i-1}(G)}{\gamma_i(G)} \mid \ldots \mid \exp \frac{G}{G'}.$$

Proof. Induction on i. For $i = 1$, it is true by hypothesis. If it holds for the case $i-1$, let us see that it also holds for the case i. Let e be the exponent of $\gamma_{i-1}(G)/\gamma_i(G)$. If we see that $\overline{g}^e = \overline{1}$ for every $\overline{g} \in \gamma_i(G)/\gamma_{i+1}(G)$, it will follow that $\exp \gamma_i(G)/\gamma_{i+1}(G) \mid e$, and the proof will be complete. By the previous lemma, these quotient groups are all abelian, so it suffices to check it only for a system of generators.

By Theorem 1.26, $[\overline{x}, \overline{y}]$ where $x \in G$ and $y \in \gamma_{i-1}(G)$ are generators of $\gamma_i(G)/\gamma_{i+1}(G)$, and by Theorem 1.5,

$$[\overline{x}, \overline{y}^e] = [\overline{x}, \overline{y}][\overline{x}, \overline{y}]^{\overline{y}} \cdots [\overline{x}, \overline{y}]^{\overline{y}^{e-1}} = [\overline{x}, \overline{y}][\overline{x}, \overline{y}][\overline{x}, \overline{y}, \overline{y}] \cdots [\overline{x}, \overline{y}][\overline{x}, \overline{y}, \overline{y}^{e-1}] = [\overline{x}, \overline{y}]^e,$$

since the commutators of length 3 are in $\gamma_{i+1}(G)$. By hypothesis $\exp \gamma_{i-1}(G)/\gamma_i(G) = e$, so we have $y^e \in \gamma_i(G)$, that is, $[x, y^e] \in \gamma_{i+1}(G)$. Hence, $[\overline{x}, \overline{y}]^e = [\overline{x}, \overline{y}^e] = \overline{1}$, and $\exp \gamma_i(G)/\gamma_{i+1}(G) \mid e$. □

1.3 Central series

Definition 1.30. A *central series* of a group G is a descending sequence of normal subgroups

$$N_1 \geq N_2 \geq \ldots \geq N_r \geq N_{r+1}$$

such that $[N_i, G] \leq N_{i+1}$ for all $i = 1, \ldots, r$. We say that the series is of length r.

More generally, we say that an infinite series of subgroups of G is a central series if every finite piece of it is central.

Remark 1.31. i) Since $[N_i, G] \leq N_{i+1}$, and $N_{i+1} \leq N_i$, it follows that $N_i \trianglelefteq G$ for $i = 1, \ldots, r$ by Theorem 1.8. Note also that $[N_{r+1}, G] \leq [N_r, G] \leq N_{r+1}$, so also $N_{r+1} \trianglelefteq G$.

ii) The property $[N_i, G] \leq N_{i+1}$ is equivalent to $N_i/N_{i+1} \leq Z(G/N_{i+1})$. For this reason, we say that the successive quotients are central in G.

Example 1.32. 1 The lower central series is a particular case of a central series.

2 We can refine a central series introducing terms between two subgroups and it will continue being a central series.

3 If we take any $N \trianglelefteq G$, the following series is central:

$$N \geq [N, G] \geq [N, G, G] \geq \ldots.$$

If we take $N = G$, we obtain the lower central series.

4 By Remark 1.31, another way to construct a central series is taking a normal subgroup $N \trianglelefteq G$, which will be the last term of the series, and taking a subgroup M such that $M/N \leq Z(G/N)$. Then, we take a subgroup K such that $K/M \leq Z(G/M)$, and so on.

Using the idea of the last example and taking the trivial group as the last term of the series, we obtain a series which is dual to the lower central series, called the upper central series.

Definition 1.33. Let G be a group. The *upper central series* $\{Z_i(G)\}_{i \geq 0}$ of G is defined recurrently as follows:

$$\begin{aligned} Z_0(G) &= 1 \\ Z_1(G) &= Z(G) \\ &\vdots \\ Z_{i+1}(G)/Z_i(G) &= Z(G/Z_i(G)) \\ &\vdots \end{aligned}$$

for $i \geq 1$.

Remark 1.34. If $x \in Z_{i+1}(G)$, we know that x commutes with all elements of G modulo $Z_i(G)$, so $x \in Z_{i+1}(G)$ and $[x, G] \leq Z_i(G)$ are equivalent conditions.

In parallel to Theorem 1.29, there is also a property for the upper central series, which will be shown in the following theorem.

Theorem 1.35. *Let G be a group such that $\exp Z(G) < \infty$. Then, $\exp Z_{i+1}(G)/Z_i(G) < \infty$ for all $i > 0$. Moreover,*

$$\exp \frac{Z_{i+1}(G)}{Z_i(G)} \mid \exp \frac{Z_i(G)}{Z_{i-1}(G)} \mid \cdots \mid \exp \frac{Z_1(G)}{Z_0(G)} = \exp Z(G).$$

Proof. Induction on i. For $i = 0$ it holds by hypothesis. Let us prove it for a general i. Let $e = \exp Z_i(G)/Z_{i-1}(G)$. We have to check that if $xZ_i(G) \in Z_{i+1}(G)/Z_i(G)$, then $x^e Z_i(G) = Z_i(G)$, in other words, if $x \in Z_{i+1}(G)$, then $x^e \in Z_i(G)$. By Remark 1.34, the conditions $x^e \in Z_i(G)$ and $[x^e, G] \leq Z_{i-1}(G)$ are equivalent. Let us consider $\overline{G} = G/Z_{i-1}(G)$. We know that $[x, g] \in Z_i(G)$ for every $g \in G$, and this means that $[\overline{x}, \overline{g}] \in Z_i(G)/Z_{i-1}(G) = Z(\overline{G})$. Thus, by Corollary 1.6, since $[\overline{x}, \overline{g}]$ commutes with $\overline{x}$, we have

$$[\overline{x}^e, \overline{g}] = [\overline{x}, \overline{g}]^e,$$

and this is equal to $\overline{1}$ since $e = \exp Z_i(G)/Z_{i-1}(G)$. Therefore, $[x^e, g] \in Z_{i-1}(G)$ for every $g \in G$, as we wanted. □

We can generalize Lemma 1.25, which was focused on the lower central series, and give a result for central series in general.

Theorem 1.36. *Let G be a group, and $N_1 \trianglerighteq N_2 \trianglerighteq \ldots \trianglerighteq N_{r+1}$ a central series of G. Then, $[N_i, \gamma_j(G)] \leq N_{i+j}$, where if $i + j > r + 1$, $N_{i+j} = N_{r+1}$.*

Proof. The proof is practically the same as that of Lemma 1.25. □

Corollary 1.37. *Let G be a group. Then,*

$$[Z_i(G), \gamma_j(G)] \leq Z_{i-j}(G),$$

where $Z_{i-j}(G) = 1$ if $i - j < 0$.

In particular, $[Z_i(G), \gamma_i(G)] = 1$ for every $i \geq 1$.

1.4 Nilpotent groups

Theorem 1.38. *Let G be a group. Then, the following conditions are equivalent:*

i) G has a finite central series from 1 to G.

ii) The lower central series reaches 1.

iii) The upper central series reaches G.

Moreover, the length of the central series of i) is greater than or equal to the length of the lower central series or of the upper central series. As a consequence, both the upper and the lower central series have the same length.

Proof. It is obvious that *ii)* or *iii)* imply *i)*, so let us prove *i)* $\Rightarrow$ *ii)* and *i)* $\Rightarrow$ *iii)*.

Firstly, let us suppose that there exists a central series such that

$$G = N_1 \geq N_2 \geq \ldots \geq N_{r+1} = \{1\}.$$

Then, by definition of the central series,

$$\begin{aligned} \gamma_1(G) &= G = N_1, \\ \gamma_2(G) &= [\gamma_1(G), G] = [N_1, G] \leq N_2, \\ \gamma_3(G) &= [\gamma_2(G), G] \leq [N_2, G] \leq N_3, \end{aligned}$$

and in general,

$$\gamma_i(G) \leq N_i.$$

In particular, $\gamma_{r+1}(G) \leq N_{r+1} = \{1\}$, and it follows that *i)* implies *ii)*.

Analogously,

$$\begin{aligned} &N_{r+1} = 1 = Z_0(G), \\ &[N_r, G] \leq N_{r+1} = 1 \Rightarrow N_r \leq Z(G) = Z_1(G), \\ &[N_{r-1}, G] \leq N_r \leq Z_1(G) \Rightarrow N_{r-1} \leq Z_2(G), \end{aligned}$$

since $[N_{r-1}, G] \leq Z_1(G)$ implies $N_{r-1}/Z_1(G) \leq Z(G/Z_1(G))$. In general,

$$N_{r-i+1} \leq Z_i(G),$$

and in particular, $G = N_1 \leq Z_r(G)$.

Observe that the length of both the upper and the lower central series is at most r.

□

Definition 1.39. If a group G satisfies any of the conditions of the previous theorem, we say that G is *nilpotent*. The minimum length of a central series of G which goes from G to 1 is called the *nilpotency class* of G.

Remark 1.40. The nilpotency class of G is c if and only if $\gamma_{c+1}(G) = 1$ but $\gamma_c(G) \neq 1$. Equivalently, if and only if $Z_c(G) = G$ but $Z_{c-1}(G) \neq 1$.

Example 1.41. 1 In a trivial way, the nilpotency class of $\{1\}$ is 0.

2 If $G \neq \{1\}$, the nilpotency class of G is 1 if and only if G is abelian.

3 By Exercise 3 in the Appendix, the nilpotency class of $D_8 = \langle a, b \mid a^4 = b^2 = 1, a^b = a^{-1} \rangle$ is 2.

Remark 1.42. By Theorem 1.23, we know that $\gamma_i(G) = 1$ if and only if all the commutators of length i are trivial. Then, G has nilpotency class less than or equal to i if and only if all the commutators of length i are trivial. The same is true for commutators with a set of generators.

Thus, the nilpotency class of a group in some sense measures how far a group is from being abelian.

Remark 1.43. Let G be a group of class c and $G = N_1 \geq N_2 \geq \ldots \geq N_{c+1} = 1$ a central series of G of length c. In the proof of the previous theorem we have seen that $\gamma_i(G) \leq N_i$ and $N_{c+1-i} \leq Z_i(G)$, in other words, the ith term of the series from the top contains $\gamma_i(G)$ and the ith term from the bottom is contained in $Z_i(G)$.

As a particular case, we have

$$\gamma_{c+1-i}(G) \leq Z_i(G)$$

for all $i = 0, \ldots, c$. For instance,

$$G' \leq Z_{c-1}(G).$$

Proposition 1.44. *If a group G is nilpotent of class c, then all subgroups of G and all quotients of G are also nilpotent of class less than or equal to c.*

Proof. Let H be a subgroup of G and N a normal subgroup of G. Since G is nilpotent of class c, there exists a central series $G = N_1 \geq \ldots \geq N_c = 1$, and let us consider the series $H = N_1 \cap H \geq \ldots \geq N_c \cap H = 1$ and $G/N = N_1N/N \geq \ldots \geq N_cN/N = N/N$. It is easy to prove that they are central series of H and G/N respectively, so we are done. Otherwise, $\gamma_{c+1}(H) \leq \gamma_{c+1}(G) = 1$ and $\gamma_{c+1}(G/N) = \gamma_{c+1}(G)N/N = N/N = \overline{1}$ already implies that H and G/N are of class $\leq c$. □

Remark 1.45. By Exercise 6 in the Appendix it follows that the direct product of nilpotent groups is nilpotent, and its class is the maximum of the nilpotency classes of the factors.

Theorem 1.46. *Let G be a nilpotent group. Then,*

i) If $1 \neq N \trianglelefteq G$, then $N \cap Z(G) \neq 1$. In particular, if $G \neq 1$, then $Z(G) \neq 1$.

ii) If $1 \neq N \trianglelefteq G$, then $[N, G] < N$.

iii) Every subgroup H is subnormal in G, that is, there exist subgroups $H_0, \ldots, H_n$ of G such that

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G.$$

iv) If $H < G$, then $H < N_G(H)$.

v) Every maximal subgroup of G is normal in G, and therefore, it has prime index in G.

Proof. *i)* Let c be the nilpotency class of G. By definition of the nilpotency class, we can deduce that $[N, G, \overset{c}{\ldots}, G] \leq \gamma_{c+1}(G) = 1$, and we take the smallest t such that $[N, G, \overset{t}{\ldots}, G] = 1$. Thus, $[N, G, \overset{t-1}{\ldots}, G] \neq 1$. By Corollary 1.8, $[N, G, \overset{t-1}{\ldots}, G] \leq Z(G)$, and in addition, $[N, G, \overset{t-1}{\ldots}, G] \leq N$ since N is normal, so $[N, G, \overset{t-1}{\ldots}, G] \leq N \cap Z(G)$ and $[N, G, \overset{t-1}{\ldots}, G] \neq 1$.

ii) If we suppose that $[N, G] = N$, then $[N, G, \overset{i}{\ldots}, G] = N$ for all $i \geq 1$, but if G is nilpotent of class c, then $[N, G, \overset{c}{\ldots}, G] = 1$, which is absurd.

iii) We consider the series $H = H\gamma_{c+1}(G) \leq H\gamma_c(G) \leq \ldots \leq H\gamma_1(G) = G$. Observe that $[H\gamma_{i+1}(G), \gamma_i(G)] \leq [G, \gamma_i(G)] \leq \gamma_{i+1}(G) \leq H\gamma_{i+1}(G)$, so by Corollary 1.7, $\gamma_i(G)$ normalizes $H\gamma_{i+1}(G)$. Furthermore, $H \leq H\gamma_{i+1}(G) \leq N_G(H\gamma_{i+1}(G))$, so $H\gamma_i(G) \leq N_G(H\gamma_{i+1}(G))$. In other words, $H\gamma_{i+1}(G) \trianglelefteq H\gamma_i(G)$.

iv) By *iii*), we have $H = H_0 \trianglelefteq H_1 \ldots \trianglelefteq H_n = G$. We can suppose that all the inclusions are proper, and obviously $H_1 \leq N_G(H)$, so $H < N_G(H)$.

v) If $H \leq G$ is a maximal subgroup of G, then $H < G$, and by *iv*), $H < N_G(H) \leq G$, so since H is maximal, $N_G(H) = G$, that is, $H \trianglelefteq G$.

Furthermore, if we consider $\overline{G} = G/H$, since H is maximal, by correspondence, $\overline{G}$ has not proper subgroups, so it is cyclic of order p for a prime p. Thus, the index of H in G is p, as required. □

Example 1.47. 1 A nilpotent group need not have maximal subgroups. For example, $\mathbb{Q}$ is nilpotent since it is abelian, but it has not maximal subgroups.

2 There exist finite groups which satisfy *i*) but are not nilpotent. For example, in the group

$$SL_2(K) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K) \mid \det(A) = 1 \right\}$$

being K a field with $|K| > 3$, one can prove that every normal proper subgroup is contained in the centre, and if $|K|$ is odd, the centre is not trivial. However, $SL_2(K)$ is not nilpotent.

In the case of finite groups, we can say even more about their nilpotency. With the exception of the first condition of the previous theorem, all other conditions characterize the finite nilpotent groups. Moreover, after the following lemmas we will see two other characterizations of them.

Lemma 1.48 (Frattini's argument)**.** *Let G be a finite group and $N \trianglelefteq G$. If $P \in \mathrm{Syl}_p(N)$, then $G = NN_G(P)$.*

Proof. Let g be any element of G. Then, $P^g \leq N^g = N$, and $|P^g| = |P|$, so since $P \in \mathrm{Syl}_p(N)$, we have $P^g \in \mathrm{Syl}_p(N)$. All Sylow p-subgroups of a group are always conjugate in the group, whence P and P^g are conjugate in N, and this means that there exists $n \in N$ such that $P^g = P^n$. Hence, we have $P^{gn^{-1}} = P$, that is, $gn^{-1} \in N_G(P)$ and since $g = (gn^{-1})n \in N_G(P)N$, we conclude that $G \subseteq NN_G(P)$. The other inclusion is obvious, so $G = NN_G(P)$. □

Lemma 1.49. *Let G be a finite group and $P \in \mathrm{Syl}_p(G)$. If $N_G(P)$ is contained in H, then H is self-normalizing in G, that is, $H = N_G(H)$.*

Proof. On the one hand, we have $P \leq N_G(P) \leq H$, so $P \in \mathrm{Syl}_p(H)$, and on the other hand, $H \trianglelefteq N_G(H)$. Thus, by the Frattini argument,

$$N_G(H) = HN_{N_G(H)}(P) \leq HN_G(P) = H.$$

□

Theorem 1.50. *Let G be a finite group. Then, conditions ii), iii), iv) and v) of the previous theorem, as well as the following two conditions, are equivalent to G being nilpotent:*

vi) *Every Sylow subgroup of G is normal.*

vii) *G is the direct product of its Sylow subgroups.*

Proof. In the proof of the previous theorem we have seen

$$G \text{ nilpotent} \Rightarrow ii) \quad \text{and} \quad G \text{ nilpotent} \Rightarrow iii) \Rightarrow iv) \Rightarrow v).$$

Now, we will prove

$$ii) \Rightarrow G \text{ nilpotent} \quad \text{and} \quad v) \Rightarrow vi) \Rightarrow vii) \Rightarrow G \text{ nilpotent}.$$

Let us start. Assuming $ii)$, if $1 \neq N \trianglelefteq G$, then $[N, G] < N$. Thus, $G > [G, G] = \gamma_2(G) > \gamma_3(G) = [\gamma_2(G), G] > \ldots > \gamma_i(G) > \gamma_{i+1}(G) = [\gamma_i(G), G]$, and since G is finite, we must have $\gamma_{c+1}(G) = 1$ for some $c \in \mathbb{N}$, so G is nilpotent.

Let us prove $v) \Rightarrow vi)$. By contradiction, we assume that there exists $P \in \mathrm{Syl}_p(G)$ not normal in G. Then, $N_G(P) < G$, and we consider a maximal subgroup M in G containing $N_G(P)$. By hypothesis, M is normal in G, and using Lemma 1.49, $N_G(M) = M$. This means that $M \ntrianglelefteq G$, which is absurd, so we have proved that every Sylow subgroup of G is normal.

Now, we suppose that G satisfies $vi)$. Let $P_1, \ldots, P_t$ be the Sylow subgroups of G for different divisors of $|G|$. Since by hypothesis every $P_i \trianglelefteq G$ for $i = 1, \ldots, t$, it follows that every $P_{i_1} \ldots P_{i_k}$ is a subgroup of G for $k \geq 2$ and $k \leq t$. Thus,

$$|P_1 \ldots P_t| = \frac{|P_1 \ldots P_{t-1}||P_t|}{|P_1 \ldots P_{t-1} \cap P_t|},$$

and we can apply this formula several times to obtain

$$|P_1 \ldots P_t| = \frac{|P_1| \ldots |P_t|}{|I|},$$

where

$$I = |P_1 P_2 \ldots P_{t-1} \cap P_t||P_1 P_2 \ldots P_{t-2} \cap P_{t-1}| \ldots |P_1 \cap P_2|.$$

However, since $|P_i|$ and $|P_j|$ are coprime for all $i, j \in \{1, \ldots, t\}$ with $i \neq j$, we have $P_i \cap P_j = 1$, so $|P_i P_j| = |P_i||P_j|$. Then, $|P_i P_j|$ and $|P_k|$ are coprime for any $k \in \{1, \ldots, t\}$ with $k \neq i, j$ so again, $P_i P_j \cap P_k = 1$. Repeating the same procedure, it can be proved that for every $i \in \{1, \ldots, t\}$ it follows that $P_i \cap P_{i_1} \ldots P_{i_k} = 1$ with $k \geq 1$, $k \leq t - 1$ and $i \neq i_j$ for $j \in \{1, \ldots, k\}$, and in particular, $|I| = 1$. Therefore,

$$|P_1 \ldots P_t| = |P_1| \ldots |P_t| = |G|.$$

Thus, we have $G = P_1 \ldots P_t$ and also $P_i \cap P_1 \ldots P_{i-1} P_{i+1} \ldots P_t = 1$ and $P_i \trianglelefteq G$ for $i = 1, \ldots, t$, that is, $G = P_1 \times \cdots \times P_t$, as required.

All that remains is to see that $vii)$ implies that G is nilpotent. The finite p-groups (groups such that their orders are powers of a prime p), such as the Sylow subgroups of a group, are all nilpotent, as we will see in the next chapter in Corollary 2.5, and furthermore, as we have said in Remark 1.45, the direct product of nilpotent groups is nilpotent, so the proof is complete. □

Chapter 2

Finite p-groups

Finite p-groups are fundamental tools in understanding the structure of finite groups. In the 1870-1900 period, they saw such highlights as the Sylow theorems. Later, in the 1900-1940, the finite groups grew immensely, and the work of P. Hall revolutionized the study of p-groups and was the first major result in this area since Sylow.

In this chapter we will see the general properties of finite p-groups and we will introduce the concept of the Frattini subgroup. Finally, in the last section, we will analyse the orders of the central factors of the lower and the upper central series of finite p-groups.

2.1 Definition and properties

Definition 2.1. Let p be a prime number. A group is said to be a p-group if the order of every element of the group is a power of p.

Remark 2.2. By using the well-known theorems of Lagrange and Cauchy, a finite group is a p-group if and only if its order is a power of p.

Example 2.3. An example of an infinite p-group is the group

$$C_{p^\infty} = \{z \in \mathbb{C}^* \mid o(z) \text{ is a power of } p\} = \left\{e^{(2\pi i/p^n)k} \mid n \in \mathbb{N}, k = 0, 1, \ldots, p^n - 1\right\}$$

known as *Prüfer p-group*.

In the last proof of the previous chapter we have said that every finite p-group is nilpotent. This is a really important result, since it will provide us with many of the properties of the finite p-groups. Our first purpose will be to prove it.

Theorem 2.4. *Let G be a finite p-group and N a normal subgroup of G such that $N \neq 1$. Then, $N \cap Z(G) \neq 1$. In particular, if $G \neq 1$, then $Z(G) \neq 1$.*

Proof. If $N = Z(G)$ we are done, so let us suppose that $N \neq Z(G)$. Since N is normal, its order, which is a multiple of p, is equal to the sum of the sizes of the different conjugacy classes of its elements. Let g be an element of N such that $g \notin Z(G)$. Then, since G is finite,

$$1 \neq |\operatorname{Cl}_G(g)| = |G : C_G(g)| = \frac{|G|}{|C_G(g)|},$$

so p divides $|\mathrm{Cl}_G(g)|$, that is, p divides every size of a non-trivial conjugacy class of an element of N. Furthermore, since the conjugacy class of an element of the centre is trivial, the sum of the orders of the conjugacy classes of $N \cap Z(G)$ is exactly $|N \cap Z(G)|$, so $|N|$ (a multiple of p) is equal to the sum of the sizes of different classes which are multiples of p and $|N \cap Z(G)|$. As a consequence, $|N \cap Z(G)|$ is also a multiple of p, and since $|N \cap Z(G)| \geq 1$, the result follows. □

As said in the previous chapter, this is just a property of the nilpotent groups, not a characterization. However, it will be essential to prove the following corollary, which indeed says that the finite p-groups are nilpotent.

Corollary 2.5. *Every finite p-group is nilpotent.*

Proof. If G is trivial or abelian it is immediate, so let G be a non-trivial and non-abelian p-group, and let us construct the upper central series of G. By the previous theorem $Z(G) \neq 1$, so we write $Z_1(G) = Z(G)$ and we consider the quotient group $G/Z_1(G)$. Obviously, since G is non-abelian, $G/Z_1(G)$ is a non-trivial p-group, so again by the previous theorem, $Z(G/Z_1(G)) \neq Z_1(G)/Z_1(G)$, and we write $Z(G/Z_1(G)) = Z_2(G)/Z_1(G)$ with $Z_2(G) > Z_1(G)$. In general, using the same argument, it follows that if $Z_{i-1}(G) \neq G$, then $Z_i(G) > Z_{i-1}(G)$, and since G is finite, $Z_i(G)$ will reach a point where $Z_i(G) = G$. Then, G is nilpotent. □

Remark 2.6. An infinite p-group need not be nilpotent. For instance, let us consider the restricted direct product $\prod_{i \in I} G_i$ where I is an infinite set of indices and G_i is a finite p-group for every $i \in I$. If we analyse the jth subgroup of the lower central series, we get

$$\gamma_j(\prod_{i \in I} G_i) = \prod_{i \in I} \gamma_j(G_i),$$

and this is equal to 1 if and only if $\gamma_j(G_i) = 1$ for all $i \in I$, i.e., if the nilpotency classes of the p-groups $\{G_i\}_{i \in I}$ are bounded. So, we take p-groups G_i such that their nilpotency classes grow as the index i grows, and we have found our counterexample.

However, another problem arises: is it possible to get a p-group whose nilpotency class is as large as we want? The answer to this question is "yes".

To prove it, we define the following group for an arbitrary $n \in \mathbb{N}$:

$$P_n = \langle a, b \mid a^{p^n} = b^{p^{n-1}} = 1, a^b = a^{1+p} \rangle.$$

We can see in Exercise 9 in the Appendix that the nilpotency class of this group is n, so we have finished.

Turning to finite p-groups, since they are all nilpotent, we already know many of their properties, such as:

i) If M is a maximal subgroup of G, then M is normal in G and $|G : M| = p$, in other words, $G/M \cong C_p$.

ii) The minimal normal subgroups of G are the subgroups of order p which are contained in $Z(G)$.

We could also say that every subgroup of a p-group, by its nilpotency, is subnormal in the group. Nevertheless, there is a stronger theorem that generalizes it.

To motivate this result, we observe that every finite p-group has an element of order p. This statement could be proved by using Cauchy's Theorem and saying that since p is a prime number, every p-group G has an element of order p. However, this can be deduced in an easier way by using Lagrange's Theorem; let p^n be the order of G. We take $g \in G$, $g \neq 1$, and its order must be a power of p less than or equal to p^n, so we consider the group $\langle g \rangle$, which is cyclic, and we are done by taking an element of order p of $\langle g \rangle$.

Moreover, if $\langle g \rangle$ were normal in G, so would be all subgroups of $\langle g \rangle$ since they would be characteristic in $\langle g \rangle$, whence we could get normal subgroups of G for every order which divides the order of g. In fact, the following theorem shows that in a p-group G, there exist normal subgroups for every power of p dividing $|G|$.

Theorem 2.7. *Let G be a finite p-group of order p^n. Then:*

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

$$1 = G_0 \leq G_1 \leq \ldots \leq G_k = N \leq \ldots \leq G_n = G$$

such that $G_i \trianglelefteq G$ and $|G_{i+1} : G_i| = p$ (that is, $|G_i| = p^i$) for all $i = 0, \ldots, n-1$.

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

$$1 = G_0 \leq G_1 \leq \ldots \leq G_k = H \leq \ldots \leq G_n = G$$

such that $G_i \trianglelefteq G_{i+1}$ and $|G_{i+1} : G_i| = p$ (that is, $|G_i| = p^i$) for all $i = 0, \ldots, n-1$.

Proof. Let us prove the first part by induction on n. For $n = 0$, we have $|G| = 1$, so $G = 1$, and there is nothing to prove. Let us suppose that it is true for the case $n-1$ and let us see that it is also true for the case n. Let us consider two cases. If $N \neq 1$ with $N \trianglelefteq G$, by Theorem 2.4 we have $N \cap Z(G) \neq 1$, and we take G_1 of order p contained in $N \cap Z(G)$. Thus, we have $G_1 \trianglelefteq G$ and $G_1 \leq N$, and we consider the quotient group G/G_1. So, $N/G_1 \trianglelefteq G/G_1$ and since $|G/G_1| = p^{n-1}$, by hypothesis of induction, there exists a series

$$\overline{1} = \frac{G_1}{G_1} \leq \frac{G_2}{G_1} \leq \ldots \leq \frac{N}{G_1} \leq \ldots \leq \frac{G_n}{G_1} = \frac{G}{G_1}$$

with $G_i/G_1 \trianglelefteq G/G_1$ and $|G_{i+1}/G_1 : G_i/G_1| = p$ for all $i = 1, \ldots, n-1$. Thus, by the correspondence theorem, we obtain a series $1 = G_0 \leq G_1 \leq G_2 \leq \ldots \leq N \leq \ldots \leq G_n = G$ with $G_i \trianglelefteq G$ and $|G_{i+1} : G_i| = p$ for all $i = 0, \ldots, n-1$, and this is the series which we are looking for.

If $N = 1$, any of the series constructed in the previous case satisfies the conditions required.

To prove the second part of the theorem, we observe that since G is nilpotent, H is subnormal in G, so there exists a series

$$1 = H_0 \trianglelefteq H = H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_t = G.$$

However, we need a series such that the index of every two consecutive subgroups is p. We can get it by taking the quotient groups H_{i+1}/H_i, which are finite p-groups, and applying the previous part of the theorem to refine our series. □

Theorem 2.8. *Let G be a finite p-group of order p^n, and $G = G_1 \geq G_2 \geq \ldots \geq G_n \geq G_{n+1} = 1$ a series of normal subgroups of G with $|G_i : G_{i+1}| = p$ for all $i = 1, \ldots, n$. If we take an element of G from each difference, that is, $g_i \in G_i \setminus G_{i+1}$, then:*

i) $G = \left\{ g_1^{i_1} g_2^{i_2} \ldots g_n^{i_n} \mid 0 \leq i_j \leq p-1, \forall j \in \{1, \ldots, n\} \right\}$ *without repetitions.*

ii) If we know how the exponents g_i^p and the commutators $[g_i, g_j]$ (with $i > j$) are represented in the form given in i), then we can also express the product of any two elements $g_1^{i_1} \ldots g_n^{i_n}$ and $g_1^{j_1} \ldots g_n^{j_n}$ in the form $g_1^{k_1} \ldots g_n^{k_n}$.

We say that we have a power-commutator presentation *of G.*

Proof. We will prove *i)* by induction on n. For $n = 0$ it is obvious. For a general n, by induction we have

$$G_2 = \{ g_2^{i_2} \ldots g_n^{i_n} \mid 0 \leq i_j \leq p-1, \forall j \in \{2, \ldots, n\} \}.$$

Since G_2 is normal in G, $|G : G_2| = p$ and $g_1 \notin G_2$, it follows that $G = \langle g_1, G_2 \rangle = \langle g_1 \rangle G_2$, so $G/G_2 = \langle \overline{g_1} \rangle$. However, $G/G_2 \cong C_p$ since $|G : G_2| = p$, so every $\overline{g} \in G/G_2$ is of the form $\overline{g} = \overline{g_1}^{i_1}$ with $0 \leq i_1 \leq p-1$. Thus, every coclass of G_2 is of the form $g_1^{i_1} G_2$, so every element of G can be represented as $g_1^{i_1} x$ with $i_1 \in \{0, \ldots, p-1\}$ and $x \in G_2$. With this we conclude that

$$G = \left\{ g_1^{i_1} \ldots g_n^{i_n} \mid 0 \leq i_j \leq p-1, \forall j \in \{1, \ldots, n\} \right\},$$

and furthermore, there are not repetitions. Indeed, if it had any repetitions, the cardinality of $\left\{ g_1^{i_1} \ldots g_n^{i_n} \mid 0 \leq i_j \leq p-1, \forall j \in \{1, \ldots, n\} \right\}$ would be less than p^n, and it would not be equal to G since $|G| = p^n$.

To prove *ii)* we apply the induction again. Thus,

$$\begin{aligned}
(g_1^{i_1} \ldots g_n^{i_n})(g_1^{j_1} \ldots g_n^{j_n}) &= g_1^{i_1} \ldots g_n^{i_n - 1} g_n g_1 g_1^{j_1 - 1} \ldots g_n^{j_n} \\
&= g_1^{i_1} \ldots g_n^{i_n - 1} g_1 g_n [g_n, g_1] g_1^{j_1 - 1} \ldots g_n^{j_n} \\
&= g_1^{i_1} g_1 g_2 [g_2, g_1] g_2 [g_2, g_1] \ldots g_n [g_n, g_1] g_1^{j_1 - 1} \ldots g_n^{j_n},
\end{aligned}$$

and doing this with all g_1, we get an element of the form $g_1^{i_1 + j_1} x$, where x is a product of elements of G_2 and commutators $[g_i, g_1]$, for $n \geq i > 1$. However, since G_2 is normal in G, we deduce that every $[g_i, g_1]$ is in G_2, whence we know how to express $[g_i, g_1]$ in terms of $g_2, \ldots, g_n$, and if $i_1 + j_1 < p$ we have finished by induction. Otherwise, $i_1 + j_1 = k_1 + \lambda p$, with $0 \leq k_1 \leq p-1$, and $g_1^{i_1 + j_1} x = g_1^{k_1} (g_1^p)^\lambda x$, so since $g_1^p \in G_2$, again we can express g_1^p in terms of $g_2, \ldots, g_n$, and using the same argument we are done. □

2.2 The Frattini subgroup in finite p-groups

In this section we will introduce the concept of the Frattini subgroup, named after Giovanni Frattini, who defined it in a paper published in 1885, and we will see some result related with it when working with p-groups.

Definition 2.9. Let G be a group. The *Frattini subgroup* of G, denoted by $\Phi(G)$, is the intersection of all maximal subgroups of G. If G has not any maximal subgroups we can define the Frattini subgroup of G as $\Phi(G) = G$.

Remark 2.10. Since we will work only with finite groups, there will always exist maximal subgroups, except for the trivial group.

Proposition 2.11. *The Frattini subgroup of a group is characteristic.*

Proof. The image under the automorphisms of every maximal subgroup of a group is also maximal, so the result is immediate. □

Theorem 2.12. *Let G be a finite group and X a subset of G. Then, the following conditions are equivalent:*

i) $G = \langle X \rangle$.

ii) $G = \langle X, \Phi(G) \rangle$.

iii) $G/\Phi(G) = \langle \overline{X} \rangle$.

It is said that the elements of the Frattini subgroup are non-generators, because they can be removed from any system of generators.

Proof. *i)* $\Rightarrow$ *ii)* and *ii)* $\Leftrightarrow$ *iii)* are clear, so let us prove *ii)* $\Rightarrow$ *i)*. By contradiction, if $G \neq \langle X \rangle$, then, since G is finite, there exists a maximal subgroup M such that $\langle X \rangle \leq M$. Thus, we have $\langle X \rangle \leq M$ and $\Phi(G) \leq M$, so $\langle X, \Phi(G) \rangle \leq M$, but this is absurd because by hypothesis, $\langle X, \Phi(G) \rangle = G$. □

Corollary 2.13. *If $H \leq G$ and $G = H\Phi(G)$, then $H = G$.*

Theorem 2.14. *Let G be a group, N a normal subgroup of G and put $\overline{G} = G/N$. Then,*

i) $\overline{\Phi(G)} \leq \Phi\left(\overline{G}\right)$, *that is,* $\Phi(G)N/N \leq \Phi(G/N)$.

ii) If $N \leq \Phi(G)$, *then* $\overline{\Phi(G)} = \Phi\left(\overline{G}\right)$, *that is,* $\Phi(G/N) = \Phi(G)N/N = \Phi(G)/N$.

Proof. We will demonstrate *i)* and *ii)* simultaneously by simply observing the following:

$$\begin{aligned}
\Phi(G/N) &= \bigcap \{M/N \mid M/N \text{ maximal in } G/N\} \\
&= \bigcap \{M/N \mid M \text{ maximal in } G \text{ and } N \leq M\} \\
&= \left(\bigcap \{M \mid M \text{ maximal in } G \text{ and } N \leq M\}\right)/N \\
&\supseteq \left(\bigcap \{K \mid K \text{ maximal in } G\}\right) N/N = \Phi(G)N/N.
\end{aligned}$$

We will have the equality if $\bigcap \{M \mid M \text{ maximal in } G \text{ and } N \leq M\} = \Phi(G)N$. In particular, if $N \leq \Phi(G)$. □

There are a lot of results about the nilpotency of a finite group G related with its frattini subgroup $\Phi(G)$. In the same way that $\Phi(G)$ or its elements can be removed from a system of generators, nor does it affect on the nilpotency when the factor group $G/\Phi(G)$ is nilpotent and we consider the whole group G.

Theorem 2.15. *Let G be a finite group and N a normal subgroup of G. If $\Phi(G) \leq N$, then*

$$N/\Phi(G) \text{ nilpotent} \Rightarrow N \text{ nilpotent.}$$

Proof. Let us see that every Sylow subgroup of N is normal in N. If $P \in \mathrm{Syl}_p(N)$, then $P\Phi(G)/\Phi(G) \in \mathrm{Syl}_p(N/\Phi(G))$, and by hypothesis $N/\Phi(G)$ is nilpotent, so $P\Phi(G)/\Phi(G) \trianglelefteq N/\Phi(G)$. Thus, $P\Phi(G)/\Phi(G)$ is characteristic in $N/\Phi(G)$, and since $N \trianglelefteq G$, we have

$$P\Phi(G)/\Phi(G) \trianglelefteq G/\Phi(G).$$

It follows that $P\Phi(G) \trianglelefteq G$ and since $P \in \mathrm{Syl}_p(P\Phi(G))$ (note that $P \leq P\Phi(G) \leq N$), using the Frattini argument and Corollary 2.13 we get

$$G = N_G(P)P\Phi(G) = N_G(P)\Phi(G) = N_G(P),$$

that is, P is normal in G, and in particular P is normal in N. □

Corollary 2.16. *If G is a finite group, $\Phi(G)$ is nilpotent.*

Proof. It is a particular case taking $N = \Phi(G)$. □

Corollary 2.17. *If G is a finite group and $G/\Phi(G)$ is nilpotent, then G is nilpotent.*

Theorem 2.18. *Let G be a finite group. Then, G is nilpotent if and only if $G' \leq \Phi(G)$.*

Proof. Supposing that G is nilpotent, we have that every maximal subgroup M of G has prime index, whence G/M is abelian. Thus, G' is contained in every maximal subgroup M, and, of course, it is also in their intersection.

If we suppose that $G' \leq \Phi(G)$, then $G/\Phi(G)$ is abelian and therefore nilpotent. Using the last corollary, it follows that G is nilpotent. □

There is an important result in the theory of finite p-groups called *Burnside's basis theorem*, but to understand it, first, we need to know some definitions such as *elementary abelian p-group* or *minimal system of generators*.

Definition 2.19. A finite abelian p-group is said to be *elementary abelian* if every non-trivial element has order p, that is, $x^p = 1$ for all $x \in G$. This is equivalent to saying that $G \cong C_p \times \overset{m}{\cdots} \times C_p$, for some $m \in \mathbb{N}$.

Remark 2.20. Using additive notation, $g^p = 1$ means $pg = 0$. On the other hand, being G abelian, it is a $\mathbb{Z}$-module, and since $pg = 0$ for all $g \in G$, $p\mathbb{Z}$ acts trivially on G. Hence, we can see G as a $\mathbb{Z}/p\mathbb{Z}$-module, which is to say, as an $\mathbb{F}_p$-vector space.

Definition 2.21. Let G be a group. We say that a system of generators of G is *minimal* if any proper subset of it generates a proper subgroup of G. On the other hand, we write $d(G)$ for the minimum number of generators with which G can be generated.

The following example will make the meaning of this last definition clear.

Example 2.22. Let $G = \langle x \rangle \cong C_6$. Then $d(G) = 1$, but $\{x^2, x^3\}$ is a minimal system of generators of length 2.

Theorem 2.23 (Burnside's Basis Theorem)**.** *Let G be a finite p-group. Then:*

i) $G/\Phi(G)$ *is elementary abelian.*

ii) A subset $\{x_1, x_2, \ldots, x_d\}$ *is a minimal system of generators of* G *if and only if* $\{x_1\Phi(G), \ldots, x_d\Phi(G)\}$ *is a basis of* $G/\Phi(G)$*. As a result, all minimal systems of generators have the same size.*

iii) The minimum number $d(G)$ *of generators of* G *is the* $\mathbb{F}_p$*-dimension of* $G/\Phi(G)$*, that is,* $d(G) = \dim_{\mathbb{F}_p} G/\Phi(G)$.

Proof. i) Let $M_1, \ldots, M_k$ be the maximal subgroups of G, so that $\Phi(G) = M_1 \cap \ldots \cap M_k$. We define the following homomorphism:

$$\begin{array}{rcl} \phi : G & \longrightarrow & G/M_1 \times \cdots \times G/M_k \\ g & \longmapsto & (gM_1, \ldots, gM_k). \end{array}$$

It is easy to check that $(gM_1, \ldots, gM_k) = (M_1, \ldots, M_k)$ if and only if $g \in M_1 \cap \ldots \cap M_k$, so $\ker \phi = M_1 \cap \ldots \cap M_k = \Phi(G)$. Now, by the first isomorphism theorem,

$$\frac{G}{\Phi(G)} \cong \operatorname{Im} \phi$$

and since $\operatorname{Im} \phi$ is a subgroup of $G/M_1 \times \cdots \times G/M_k$, which is elementary abelian since all G/M_i are cyclic of order p, $\operatorname{Im} \phi$ is also elementary abelian and we have finished.

ii) By Theorem 2.12, $\{x_1, \ldots, x_d\}$ is a minimal system of generators of G if and only if $\{x_1\Phi(G), \ldots, x_d\Phi(G)\}$ is a minimal system of generators of $G/\Phi(G)$, that is, if and only if it is a basis of the $\mathbb{F}_p$-vector space $G/\Phi(G)$.

iii) This property is an immediate consequence of *ii)*. □

Definition 2.24. Let G be a finite p-group. For all $i \geq 0$, the *omega subgroup* $\Omega_i(G)$ is the subgroup generated by all the elements of G whose order divides p^i, that is,

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

In the same way, the *agemo subgroup* $\mathfrak{V}_i(G)$ is the subgroup generated by all powers x^{p^i} for $x \in G$, that is,

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

Nowadays, it is more common the notation G^{p^i} to refer to the agemo subgroup $\mathfrak{V}_i(G)$.

Theorem 2.25. *Let G be a finite p-group. Then:*

i) $\Phi(G)$ *is the smallest normal subgroup of* G *such that the quotient group is elementary abelian.*

ii) $\Phi(G) = G'G^p$.

Proof. i) By Burnside's Basis Theorem, $G/\Phi(G)$ is elementary abelian. Let N be another normal subgroup of G such that G/N is elementary abelian. Then, by Remark 2.20, G/N can be seen as an $\mathbb{F}_p$-vector space, and the maximal subgroups are precisely the maximal subspaces. It is known that in vector spaces, the intersection of all maximal subspaces is trivial, whence $\Phi(G/N) = \overline{1}$. By Theorem 2.14, $\Phi(G)N/N \leq \Phi(G/N) = \overline{1}$, so $\Phi(G) \leq N$.

ii) By definition, G/N is elementary abelian if and only if G/N is abelian and $\overline{x}^p = \overline{1}$ for all $x \in G$ (that is, $x^p \in N$ for all $x \in G$). This is equivalent to $G' \leq N$ and $G^p \leq N$, and this happens if and only if $G'G^p \leq N$. Thus, $G'G^p$ is the smallest normal subgroup of G such that the quotient group is elementary abelian. By the previous part, it follows that $\Phi(G) = G'G^p$. □

2.3 Orders of central factors

In the last section of the chapter we will analyse the index of two consecutive subgroups of the upper or the lower central series.

Theorem 2.26. *Let G be a p-group of order $p^n \geq p^2$ and nilpotency class c. Then:*

i) $|G : Z_{c-1}(G)| \geq p^2$.

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

iii) $c \leq n - 1$.

Proof. i) By contradiction, let us suppose that $|G : Z_{c-1}(G)| = p$. If $c = 1$, we have $|G| = p$, which is false by hypothesis. If $c \geq 2$, we consider the quotient group $G/Z_{c-2}(G)$, and using the definition of upper central series and the third isomorphism theorem,

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

which is of order p, so cyclic. In general, if H is a group and $H/Z(H)$ is cyclic, then H is abelian. Therefore, $G/Z_{c-2}(G)$ is abelian and $Z_{c-1}(G) = G$, which is absurd.

ii) By Remark 1.43 in Chapter 1, $\gamma_2(G) \leq Z_{c-1}(G)$, and since $|G : Z_{c-1}(G)| \geq p^2$, it follows that $|G : G'| \geq p^2$.

iii) The index of every two consecutive subgroups of a central series of G is greater than or equal to p, and by the previous results, both the upper and the lower central series have two consecutive subgroups whose index is p^2. Then, since

$$p^n = |G| = \prod_{i=1}^{c} |\gamma_i(G) : \gamma_{i+1}(G)|,$$

we deduce $c \leq n - 1$. □

Let us see what would happen if $c = n - 1$. By the formula used in the proof of *iii*) of the previous theorem, it can be deduced that $|G : G'| = p^2$ and $|\gamma_i(G) : \gamma_{i+1}(G)| = p$ for every $i = 2, \dots, c$. Analogously, using the formula

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

we deduce that $|G : Z_{c-1}(G)| = p^2$ and $|Z_{i+1}(G) : Z_i(G)| = p$ for every $i = 0, \dots, c-2$. Furthermore, since $\gamma_i(G) \leq Z_{c-i+1}(G)$ for every i, we finally conclude that $\gamma_i(G) = Z_{c-i+1}(G)$. The property that $c = n - 1$ is really interesting, so let us give a definition to the groups that satisfy it.

Definition 2.27. We say that a finite p-group of order $p^n \geq p^2$ is of *maximal class* if its nilpotency class is $n - 1$.

Example 2.28. 1 Every group of order p^2 is a p-group of maximal class.

2 Every non-abelian group of order p^3 is a p-group of maximal class.

3 If $p = 2$, we can deduce from Exercise 7 in the Appendix that D_{2^n}, Q_{2^n} with $n \geq 3$ and SD_{2^n} with $n \geq 4$ are 2-groups of maximal class. Further, by Exercise 8, we can construct, for any prime p and any $n \geq 2$, a p-group of maximal class of order p^n.

As we have seen in the previous theorem, we always have a lower bound for the first index of the lower central series, or the last one of the upper central series. The theorem after the following lemma shows that if we have a group N, we can obtain a better lower bound for all orders of the consecutive central factors (except for possibly the last one) of N if N is included in a subgroup of the lower central series of another group G, with $N \trianglelefteq G$. So, let us see first the mentioned lemma, which will be used to prove the theorem.

Lemma 2.29. *Let M and N be normal subgroups of a group G. Then,*

$$[N, \gamma_i(M)] \leq [N, M, \overset{i}{\dots}, M]$$

for all $i \geq 1$.

Proof. Let us prove it by induction on i. For $i = 1$ is trivial. Let us suppose that the result is true for $i-1$ and let us see it for i. Since N and M are normal in G, $[N, M, \overset{i}{\dots}, M]$ is also normal in G, and by hypothesis of induction, $[N, \gamma_{i-1}(M), M] \leq [N, M, \overset{i}{\dots}, M]$ and $[M, N, \gamma_{i-1}(M)] = [N, M, \gamma_{i-1}(M)] \leq [N, M, \overset{i}{\dots}, M]$, so using the Three Subgroup Lemma,

$$[\gamma_i(M), N] = [\gamma_{i-1}(M), M, N] \leq [N, M, \overset{i}{\dots}, M].$$

□

Theorem 2.30. *Let G be a finite p-group and $N \trianglelefteq G$. If $N \leq \gamma_i(G)$ and $\gamma_{j+1}(N) \neq 1$, then $|\gamma_j(N) : \gamma_{j+1}(N)| \geq p^i$ (that is, the consecutive indices of the lower central series of N are all greater than or equal to p^i, except for possibly the last term of the series).*

Proof. Using that $N \leq \gamma_i(G)$ and the previous lemma, we have

$$\gamma_{j+1}(N) = [\gamma_j(N), N] \leq [\gamma_j(N), \gamma_i(G)] \leq [\gamma_j(N), G, \overset{i}{\ldots}, G].$$

Furthermore, since $\gamma_j(N)$ is characteristic in N and $N \trianglelefteq G$, then $\gamma_j(N) \trianglelefteq G$. Thus, if $\gamma_{j+1}(N) \neq 1$, using that G is nilpotent, we have

$$\gamma_j(N) > [\gamma_j(N), G] > [\gamma_j(N), G, G] > \ldots > [\gamma_j(N), G, \overset{i}{\ldots}, G] \geq \gamma_{j+1}(N),$$

and the result follows since the index of two consecutive subgroups of the series is at least p. □

Chapter 3

Powerful p-groups

The theory of powerful p-groups was created by A. Lubotzky and A. Mann in 1987, although it was also anticipated in an earlier work of M. Lazard in 1965. The exposition in this chapter follows [6] and includes some theorems from [4], [3] and [8]. The proofs, however, are here inflated to a more verbose form and, in addition, we also prove the cases of $p = 2$.

3.1 Definition and properties

Definition 3.1. Let G be a finite p-group. If p is an odd prime, G is said to be *powerful* if $[G, G] \leq G^p$. If $p = 2$, we say that G is powerful if $[G, G] \leq G^4$.

Remark 3.2. If the definition were not different for $p = 2$, then every 2-group G would be powerful. Indeed, if we consider the factor group G/G^2, every element of G/G^2 has order at most two, so for every $\overline{a}, \overline{b} \in G/G^2$, we have

$$\overline{a}\overline{b} = (\overline{a}\overline{b})^{-1} = \overline{b}^{-1}\overline{a}^{-1} = \overline{b}\overline{a}.$$

Hence, G/G^2 is abelian, and $[G, G] \leq G^2$.

Example 3.3. Obviously, abelian p-groups are powerful. On the other hand, if $\exp G = p$ and G is powerful, it follows that $[G, G] \leq G^p = 1$, so that G is abelian.

We can define in a relative way the property of being powerful for a subgroup, as we do in the following definition.

Definition 3.4. A subgroup N of a finite p-group G is said to be *powerfully embedded* in G for an odd prime p if $[N, G] \leq N^p$. If $p = 2$, then N is powerfully embedded if $[N, G] \leq N^4$.

Remark 3.5. i) Note that by Corollary 1.8, a powerfully embedded subgroup N is always normal in G, and of course, N is powerful itself.

ii) Unlike in the case of the whole group G, if N is a subgroup of G, it could happen that $[N, G] \not\leq N^2$. For example, let $G = \langle x \rangle \ltimes \langle a, b, c \rangle$, such that $\langle a, b, c \rangle \cong C_2 \times C_2 \times C_2$, and

the action of $\langle x \rangle$ on $\langle a, b, c \rangle$ is given by

$$\begin{array}{rccc} \varphi: & \langle x \rangle & \longrightarrow & \text{Aut } \langle a, b, c \rangle \\ & x & \longrightarrow & \alpha \end{array}$$

such that

$$\begin{array}{rccc} \alpha: & \langle a, b, c \rangle & \longrightarrow & \langle a, b, c \rangle \\ & a & \longrightarrow & ab \\ & b & \longrightarrow & bc \\ & c & \longrightarrow & c. \end{array}$$

Since $\langle a, b, c \rangle$ is elementary abelian, it is a vector-space, and it is easy to see that α is an automorphism of order 4 since its matrix is

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

and $A^4 = I_3$, $A^2 \neq I_3$. We note that $[a, x] = b$, $[b, x] = c$ and $[c, x] = 1$, so G' lies in $\langle a, b, c \rangle$ and then $(G')^2 = 1$. Furthermore, since $[a, x] = b \in G'$, we have $[b, x] = c \in \gamma_3(G)$, so $\gamma_3(G) = [G', G] \neq 1$. Therefore, $[G', G] \not\leq (G')^2$.

By Theorem 1.5, if φ is a homomorphism, then, for an odd prime p, we have $\varphi(N)^p = \varphi(N^p) \geq \varphi([N, G]) = [\varphi(N), \varphi(G)]$, so the image of a powerfully embedded subgroup is powerfully embedded in the image of G, and the same is true for the case of $p = 2$. In particular, if N is powerfully embedded in G, its image will be powerfully embedded in any factor group.

If M and N are powerfully embedded subgroups of G, the subgroups $[M, N]$, M^p and MN are also powerfully embedded, but it is not that simple to prove; we will first need two lemmas.

Lemma 3.6. *Let G be a finite p-group and N a normal subgroup of G. Then:*

i) If $[N, G] \leq [N, G]^p [N, G, G]$, then $[N, G] = 1$.

ii) If $[N, G] \leq K[N, G]^p [N, G, G]$, where $K \trianglelefteq G$, then $[N, G] \leq K$.

Proof. i) By contradiction, we assume that $[N, G] \neq 1$. Thus, since G is nilpotent, $[N, G, G] < [N, G]$, and by Theorem 2.7, if we consider the group $G/[N, G, G]$, it can be easily deduced that there exists a subgroup L such that $[N, G, G] \leq L \leq [N, G]$ and $|[N, G] : L| = p$. Then, $[N, G]^p \leq L$, and it follows that $[N, G, G] \leq L$ and $[N, G]^p \leq L$, so

$$[N, G] \leq [N, G]^p [N, G, G] \leq L,$$

which is a contradiction. Then, $[N, G] = 1$.

ii) It suffices to consider the group $\overline{G} = G/K$. Thus, we have $\left[\overline{N}, \overline{G}\right] \leq \left[\overline{N}, \overline{G}\right]^p \left[\overline{N}, \overline{G}, \overline{G}\right]$, and by *i*), we have $\left[\overline{N}, \overline{G}\right] = \overline{1}$, in other words, $[N, G] \leq K$. □

This latter lemma is really useful when we want to prove that a subgroup N is powerfully embedded in a group G, since it will suffice to prove that $[N,G] \leq N^p[N,G,G]$ for $p > 2$ or $[N,G] \leq N^4[N,G]^2[N,G,G]$ for $p = 2$.

Furthermore, it allows us to assume that $N^p = 1$, $[N,G,G] = 1$ or both $N^p[N,G,G] = 1$ for $p > 2$, or, if $p = 2$, $N^4 = 1$, $[N,G]^2 = 1$, $[N,G,G] = 1$ or that any possible combination of them is trivial. Indeed, otherwise we could consider the respective factor group and then, after proving that in this factor group $\overline{N}$ is powerfully embedded in $\overline{G}$, by the lemma we would be done.

Lemma 3.7. *Let N and M be normal subgroups of a p-group G such that $[N,M,G,G] = 1$. Then:*

i) If p is an odd prime, then $[N^p, M] = [N,M]^p$.

ii) If $p = 2$ and $[N,M,G]^2 = 1$, then $[N^4, M] = [N,M]^4$.

iii) If $p = 2$ and $[N,M,G] = 1$, then $[N^2, M] = [N,M]^2$.

Proof. We take first $p \neq 2$. We note that since $[N,M,G,G] = 1$, the subgroup $[N,M]$ is abelian. Indeed, by Lemma 2.29,

$$[[N,M],[N,M]] \leq [[N,M],[G,G]] \leq [[N,M],G,G] = 1.$$

Thus, by Exercise 1,

$$[n^p, m] = [n,m]^p [n,m,n]^{p(p-1)/2} \in [N,M]^p,$$

and in addition, n and $[n,m,n]$ commute since $[N,M,G,G] = 1$, so by Corollary 1.6,

$$[n,m]^p = [n^p, m][n,m,n^p]^{-(p-1)/2} \in [N^p, M].$$

Thus, we get

$$[N^p, M] = \langle [n^p, m]^g \mid n \in N, m \in M, g \in G \rangle \leq [N,M]^p$$

and, since $[N,M]$ is abelian and generated by all commutators $[n,m]$ with $n \in N$, $m \in M$,

$$[N,M]^p = \langle [n,m]^p \mid n \in N, m \in M \rangle \leq [N^p, M],$$

whence $[N^p, M] = [N,M]^p$.

Let us prove *ii*). Because of the same reason, we get $[n^4, m] = [n,m]^4 [n,m,n]^6$, and since $[n,m,n]^6 = ([n,m,n]^2)^3 \in [N,M,G]^2 = 1$, it follows that $[n^4, m] = [n,m]^4$. Again, since $[N,M]$ is abelian, we conclude that

$$\begin{aligned} [N^4, M] &= \langle [n^4, m]^g \mid g \in G, n \in N, m \in M \rangle \\ &= \langle ([n,m]^4)^g \mid g \in G, n \in N, m \in M \rangle \\ &= \langle [n,m]^4 \mid n \in N, m \in M \rangle^G = [N,M]^4. \end{aligned}$$

Finally, the proof of *iii*) is trivial following the same argumentation. □

Remark 3.8. In the case of $p = 2$ it is not true that $[N^2, M] = [N, M]^2$ under the condition $[N, M, G, G] = 1$, even if we also assume as in *ii)* of the previous lemma that $[N, M, G]^2 = 1$. For instance, going back to the second example of Remark 3.5, we take $G = \langle x \rangle \ltimes \langle a, b, c \rangle$ in the same way and let us calculate $\gamma_4(G)$. By Theorem 1.23,

$$G' = \langle [a, x], [b, x], [c, x] \rangle^G = \langle b, c \rangle^G,$$

and since $b^x = bc$ and $c^x = c$, the subgroup $\langle b, c \rangle$ is normal in G, so $G' = \langle b, c \rangle$. Now,

$$\gamma_3(G) = [G', G] = \langle [b, x], [c, x] \rangle^G = \langle c \rangle^G = \langle c \rangle,$$

since $c^x = c$, and so $\gamma_3(G)^2 = 1$. Also,

$$\gamma_4(G) = \langle [c, x] \rangle^G = 1,$$

whence we are in the conditions of the lemma, with $N = M = G$. Since $(G')^2 = 1$, if we prove that $[G^2, G] \neq 1$, we will have proved that $[G^2, G] \neq [G, G]^2$. By contradiction, $[G^2, G] = 1$ implies $G^2 \leq Z(G)$, but this is not true since $a^{x^2} = (a^x)^x = (ab)^x = abbc = ac$, and so, $x^2 \notin Z(G)$.

Theorem 3.9. *Let G be a finite p-group and N and M powerfully embedded subgroups of G. Then:*

i) *$[N, M]$ is powerfully embedded in G.*

ii) *N^p is powerfully embedded in G.*

iii) *NM is powerfully embedded in G.*

Proof. i) By Lemma 3.6, we may assume that $[N, M, G, G] = 1$, and if $p = 2$, also that $[N, M, G]^2 = 1$. Note that since N and M are normal in G, so is $[G, N, M][M, G, N]$. Obviously, $[G, N, M] \leq [G, N, M][M, G, N]$ and $[M, G, N] \leq [G, N, M][M, G, N]$, so by the Three Subgroup Lemma,

$$[N, M, G] \leq [G, N, M][M, G, N].$$

By definition of powerfully embedded subgroups, if $p > 2$, then

$$[G, N, M][M, G, N] = [[N, G], M][N, [M, G]] \leq [N^p, M][N, M^p],$$

and by Lemma 3.7, $[N^p, M][N, M^p] = [N, M]^p$. Then, $[[N, M], G] \leq [N, M]^p$, and $[N, M]$ is powerfully embedded in G. If $p = 2$, then

$$[G, N, M][M, G, N] = [[N, G], M][N, [M, G]] \leq [N^4, M][N, M^4],$$

and again by Lemma 3.7, $[N^4, M][N, M^4] = [N, M]^4$, that is $[[N, M], G] \leq [N, M]^4$.

ii) We begin with $p > 2$. Again, we may assume that $[N^p, G, G] = 1$. Since $[N, G] \leq N^p$ by hypothesis, it follows that $[N, G, G, G] \leq [N^p, G, G] = 1$. Then, by Lemma 3.7, $[N^p, G] = [N, G]^p$, and again, by hypothesis, $[N, G]^p \leq (N^p)^p$. Therefore, $[N^p, G] \leq (N^p)^p$, as we wanted.

If $p = 2$, we will assume that $[N^2, G, G] = [N^2, G]^2 = 1$ and in the same way we deduce that $[N, G, G, G] = 1$. Furthermore, $[N, G, G]^2 \leq [N^4, G]^2 \leq [N^2, G]^2 = 1$, so now we can apply Lemma 3.7, and making the same computations as in the case of $p > 2$, we get $[N^2, G] \leq (N^4)^2$. Let us prove that $(N^4)^2 \leq (N^2)^4$. By Corollary 1.37, $[Z_2(G), \gamma_2(G)] = 1$, and by Exercise 2, $N^2 \leq Z_2(G)$. So, $[n^4, g] = [n^2 n^2, g] = [n^2, g]^{n^2}[n^2, g] = [n^2, g]^2 = 1$, for all $n \in \mathbb{N}$ and $g \in G$, whence $N^4 \leq Z(G)$. Then, $(N^4)^2 = N^8 \leq (N^2)^4$, and we are done.

iii) Let $p > 2$. By Remark 1.17 and the hypothesis, $[NM, G] = [N, G][M, G] \leq N^p M^p$. Besides, $N^p M^p \leq (NM)^p$ since the generators of the group

$$N^p M^p = \langle n^p \mid n \in N \rangle \langle m^p \mid m \in M \rangle = \langle n^p, m^p \mid n \in N, m \in M \rangle$$

are in the group

$$(NM)^p = \langle (nm)^p \mid nm \in NM \rangle.$$

Indeed, $n^p = (n1)^p$ and $m^p = (1m)^p$, so the proof is complete. For $p = 2$ the procedure is the same. □

By Theorem 3.9, we can easily deduce that if G is powerful, then $[G, G]$ and G^p are powerfully embedded subgroups in G. Now, we are interested in knowing if $\Phi(G)$, $G^{(k)}$ and $\gamma_k(G)$ for all $k \in \mathbb{N}$ are powerfully embedded subgroups. However, this can be also deduced from Theorem 3.9 since $\Phi(G) = G'G^p$, and using induction on k for $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$ and $\gamma_k(G) = [\gamma_{k-1}(G), G]$.

One of the most important things about powerful p-groups is that they have many properties similar to abelian groups, like those exposed in the following two theorems. However, we need three more lemmas to prove them.

Lemma 3.10. *Let G be a group and N a normal subgroup of G. If G/N is cyclic, then $[G, G] = [G, N]$.*

Proof. We consider the quotient group $\overline{G} = G/[G, N]$ and we note that $\overline{N} \leq Z(\overline{G})$. Furthermore, G/N is cyclic, and by the third isomorphism theorem, $\overline{G}/\overline{N} \cong G/N$. Thus, since $\overline{N}$ is in the center of $\overline{G}$, and since $\overline{G}/\overline{N}$ is cyclic, it follows that $\overline{G} = G/[G, N]$ is abelian. Therefore, $[G, G] \leq [G, N]$, and since the other inclusion is trivial, we conclude that $[G, G] = [G, N]$. □

Lemma 3.11. *Let N be a powerfully embedded subgroup of a p-group G. Then, for any $h \in G$, the subgroup $H = \langle h \rangle N$ is a powerful p-group and:*

i) If p is odd, then $[H, H] \leq N^p$.

ii) If $p = 2$, then $[H, H] \leq N^4$.

Proof. Let us prove the result for an odd prime p. Since N is powerfully embedded in G, in particular it is normal in G, and of course, it is also normal in H. By the previous lemma, since H/N is obviously cyclic, it follows that $[H, H] = [N, H]$. Then, since N is powerfully embedded in G,

$$[H, H] = [N, H] \leq [N, G] \leq N^p \leq H^p,$$

that is, H is a powerful p-group and $[H, H] \leq N^p$. For $p = 2$ the proof is exactly the same. □

Lemma 3.12. *Let G be a finite p-group of class 2. If $p > 2$, then $G^p = \{g^p \mid g \in G\}$.*

Proof. Let a and b be two arbitrary elements of G. Since G is nilpotent of class 2, we have $[a,b] \in G' \leq Z(G)$, so $\langle a, [a,b]\rangle'$ is abelian, and by Exercise 1 in the Appendix, we know that

$$(ab)^p = a^p b^p [b,a]^{\binom{p}{2}} [b,a,a]^{\binom{p}{3}} \dots [b,a,\overset{p-1}{\dots},a]^{\binom{p}{p}} = a^p b^p [b,a]^{p(p-1)/2},$$

that is, $a^p b^p = (ab)^p [a,b]^{p(p-1)/2}$. Furthermore, since $[G', G] = \gamma_3(G) = 1$, it follows by Corollary 1.8 that G' is in the center, so $a^p b^p = (ab)^p [a,b]^{p(p-1)/2} = (ab[a,b]^{(p-1)/2})^p$ (recall that $p > 2$). Thus, every product of pth powers is a pth power as well, and since by definition every element of G^p is a product of pth powers, we are done. □

Theorem 3.13. *Let G be a powerful p-group. Then, the subgroup G^p coincides with the subset $\{g^p \mid g \in G\}$.*

Proof. Let us take first $p > 2$, and let us prove the result by induction on $|G|$. If $G = 1$, the result holds. If $|G| \geq p$, then we consider the factor group $\overline{G} = G/(G^p)^p$. Since G is powerful and by Theorem 3.9 G^p is powerfully embedded in G, we have $\gamma_3(G) = [G,G,G] \leq [G^p, G] \leq (G^p)^p$, so $\gamma_3\left(\overline{G}\right) = \overline{1}$, or which is the same, $\overline{G}$ is nilpotent of class at most 2. Thus, we apply Lemma 3.12 and we have that $\overline{G}^p = \{\overline{g}^p \mid \overline{g} \in \overline{G}\}$. If we take $a \in G^p$, then, $\overline{a} \in \overline{G}^p = \{\overline{g}^p \mid \overline{g} \in \overline{G}\}$, that is, there exists $b \in G$ such that $a \in b^p (G^p)^p$. We consider the subgroup $H = \langle b \rangle G^p$, and by Lemma 3.11, it follows that H is powerful. Besides, $a \in H^p$ since $a \in b^p (G^p)^p$, and we consider two cases: if $H \neq G$, then $a \in \{h^p \mid h \in H\}$ by hypothesis of induction. Suppose now that $H = G$. By Theorem 2.25, $\Phi(G) = G' G^p$, so $G^p \leq \Phi(G)$. Thus, by Corollary 2.13, $G = \langle b \rangle G^p = \langle b \rangle$, and the theorem obviously holds for cyclic groups.

If $p = 2$, then $[G,G] \leq G^4 \leq (G^2)^2$, so the quotient group $\overline{G} = G/(G^2)^2$ is abelian and $\overline{G}^2 = \{\overline{g}^2 \mid \overline{g} \in \overline{G}\}$. We continue as in the previous case and the proof is complete. □

The following theorem generalizes the previous one.

Theorem 3.14. *If G is a powerful p-group, then:*

i) For every $k \in \mathbb{N}$, the subgroup G^{p^k} coincides with the subset $\{g^{p^k} \mid g \in G\}$. In particular, $(G^{p^i})^{p^j} = G^{p^{i+j}}$ for all $i, j \in \mathbb{N}$.

ii) G^{p^k} is powerfully embedded in G for all $k \in \mathbb{N}$.

iii) The subgroups G^{p^i} with $i \in \mathbb{N}$ form a central series of G, and if p^e is the exponent of G, then the nilpotency class of G is less than or equal to e.

Proof. We will prove *i)* and *ii)* simultaneously by induction on k. For $k = 1$, the previous theorem implies *i)* while Theorem 3.9 implies *ii)*. For $k > 1$, we suppose that $G^{p^{k-1}} = \{g^{p^{k-1}} \mid g \in G\}$ and that $G^{p^{k-1}}$ is powerfully embedded. Then,

$$G^{p^k} = \langle g^{p^k} \mid g \in G \rangle = \langle (g^{p^{k-1}})^p \mid g \in G \rangle = \langle x^p \mid x \in G^{p^{k-1}} \rangle,$$

and by the previous theorem, since $G^{p^{k-1}}$ is in particular powerful,

$$(G^{p^{k-1}})^p = \{x^p \mid x \in G^{p^{k-1}}\} = \{g^{p^k} \mid g \in G\}.$$

Thus, $G^{p^k} = \{g^{p^k} \mid g \in G\}$, and, moreover, $G^{p^k} = (G^{p^{k-1}})^p$ is powerfully embedded by Theorem 3.9.

To prove *iii)*, it follows by *ii)* that $[G^{p^i}, G] \leq (G^{p^i})^p$, and by *i)*, we have $(G^{p^i})^p = G^{p^{i+1}}$, that is, $[G^{p^i}, G] \leq G^{p^{i+1}}$, so we are done by the definition of central series. □

To finalize the section, we show that the result of Lemma 3.7 can be generalized and improved when working with powerful p-groups.

Lemma 3.15 (Interchanging lemma)**.** *If N and M are powerfully embedded subgroups in a finite p-group G, then $[N^{p^i}, M^{p^j}] = [N, M]^{p^{i+j}}$ for all $i, j \in \mathbb{N}$.*

Proof. Let us begin with $p > 2$. Firstly we will prove that $[N^p, M] = [N, M]^p$. If we take $[N, M, G, G] = 1$, then, by Lemma 3.7 the result holds. Otherwise, we consider the subgroup $\overline{G} = G/[N, M]^{p^2}$. We note that by Theorem 3.14,

$$[N, M, G, G] \leq [[N, M]^p, G] \leq ([N, M]^p)^p = [N, M]^{p^2},$$

so $\left[\overline{N}, \overline{M}, \overline{G}, \overline{G}\right] = \overline{1}$, and we deduce that

$$[N^p, M][N, M]^{p^2} = [N, M]^p[N, M]^{p^2} = [N, M]^p.$$

However, by Theorem 2.25, since $[N, M]^p$ is in particular powerful, $\Phi([N, M]^p) = [N, M]^{p^2}$, and by Theorem 2.13 we conclude that $[N^p, M] = [N, M]^p$.

If $p = 2$, then we also have $[N, M, G] \leq [N, M]^4$, so we can use the same argumentation.

Now, using Theorem 3.14, we have

$$[N^{p^i}, M^{p^j}] = [(N^{p^{i-1}})^p, M^{p^j}] = [N^{p^{i-1}}, M^{p^j}]^p,$$

and using again Theorem 3.14 several times, with a simple argument of induction on $i + j$ the lemma follows. □

3.2 Generators of powerful p-groups

In this section we will see what we can say about the generators of the subgroups of a powerful p-group, knowing the generators of this latter.

Theorem 3.16. *Let G be a powerful p-group and $g_1, \ldots, g_k \in G$ such that $G = \langle g_1, \ldots, g_k \rangle$. Then, $G^p = \langle g_1^p, \ldots, g_k^p \rangle$.*

Proof. We take $p > 2$ and we first assume that $G^{p^2} = 1$. By Theorem 3.14,

$$\gamma_3(G) = [G, G, G] \leq [G^p, G] \leq (G^p)^p = G^{p^2} = 1,$$

so G is nilpotent of class at most 2 and $[G,G]^p \leq (G^p)^p = G^{p^2} = 1$. As we have done in the proof of Lemma 3.12, $(xy)^p = x^p y^p [y,x]^{p(p-1)/2}$, but in this case we can say that since $[x,y]^{p(p-1)/2} = ([x,y]^{(p-1)/2})^p \in [G,G]^p$ (recall that $p > 2$), it follows that $(xy)^p = x^p y^p$, for all $x, y \in G$. The subgroup G^p is generated by the pth powers of products of the elements g_i for $i = 1, \ldots, k$, for which

$$(g_{i_1} \ldots g_{i_{s-1}} g_{i_s})^p = (g_{i_1} \ldots g_{i_{s-1}})^p g_{i_s}^p = \ldots = g_{i_1}^p \ldots g_{i_{s-1}}^p g_{i_s}^p.$$

Hence, G^p is generated by the elements g_i^p for all $i = 1, \ldots, k$.

If $G^{p^2} \neq 1$, then we consider the group $\overline{G} = G/G^{p^2}$. Thus, $\overline{G}^{p^2} = \overline{1}$ and by the previous case we have $\overline{G}^p = \langle \overline{g_1}^p, \ldots, \overline{g_k}^p \rangle$. By Theorem 2.12, $G^{p^2} = (G^p)^p \leq \Phi(G^p)$, so $G^p = \langle g_1^p, \ldots, g_k^p, G^{p^2} \rangle = \langle g_1^p, \ldots, g_k^p \rangle$, as required.

If $p = 2$, then, $G' \leq G^4$, so G/G^4 is abelian and the result holds following the same procedure. □

Now we are interested in the minimal number of generators. Although $H \leq G$, it could happen that $d(H) \not\leq d(G)$. The most significant example of this possible situation is the following: any finite group G of order n, by Cayley's Theorem, can be embedded in Σ_n, but while $d(\Sigma_n) = 2$ (since $\{(1\ 2), (1\ \ldots\ n)\}$ is a system of generators), $d(G)$ need not be less than or equal to 2.

Even in the case that G is a p-group, $H \leq G$ does not imply $d(H) \leq d(G)$. For example, let us define $A = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle \cong C_p \times \cdots \times C_p$ and the following automorphism of A:

$$\begin{array}{rccc} \alpha: & A & \longrightarrow & A \\ & a_i & \longrightarrow & a_i a_{i+1} \end{array}$$

for $i \geq 1$ with $a_i = 1$ if $i > n$. Then,

$$\alpha^k(a_i) = \alpha^{k-1}(a_i a_{i+1}) = \alpha^{k-2}(a_i a_{i+1}^2 a_{i+2}) = \ldots = a_i a_{i+1}^{\binom{k}{1}} a_{i+2}^{\binom{k}{2}} \ldots a_{i+k}^{\binom{k}{k}},$$

and if $p^m \geq n$, then

$$\alpha^{p^m}(a_i) = a_i a_{i+1}^{\binom{p^m}{1}} a_{i+2}^{\binom{p^m}{2}} \ldots a_{i+p^m}^{\binom{p^m}{p^m}}.$$

However, since $p \mid \binom{p^m}{j}$ for every $1 \leq j \leq p^m - 1$, all powers of a_j are divisible by p, so that $a_j^{\binom{p^m}{j}} = 1$. Furthermore, since $p^m \geq n$, we have $i + p^m \geq 1 + p^m \geq n + 1$, so $a_{i+p^m} = 1$. Therefore, $\alpha^{p^m}(a_i) = a_i$ for every a_i whence $o(\alpha)$ divides p^m, or which is the same, $o(\alpha)$ is a power of p.

Now, we define $G = \langle x \rangle \ltimes A$ such that $a_i^x = \alpha(a_i)$. Then, since $[a_i, x] = a_i^{-1} a_i^x = a_{i+1}$ for every i, we can obtain every element of G with x and a_1, that is, $G = \langle a_1, x \rangle$ and $d(G) = 2$. However, $d(A) = n$, as we wanted.

Nevertheless, the following theorem shows that if G is a powerful p-group, then every subgroup of G can be generated by no more generators than G.

For the proof of the theorem we need a lemma.

Lemma 3.17. *Let G be a p-group and $H \leq G$. If a subset of H is contained in a minimal system of generators of G, then it can be extended to a system of generators of H.*

Proof. Let $S = \{h_1, \dots, h_r\}$ be a subset of H contained in a minimal system of generators of G: $\{h_1, \dots, h_r, g_1, \dots, g_t\}$. Then, working in $G/\Phi(G)$, we know that

$$\{h_1\Phi(G), \dots, h_r\Phi(G), g_1\Phi(G), \dots, g_t\Phi(G)\}$$

is a basis, and then, $\{h_1\Phi(G), \dots, h_r\Phi(G)\}$ is linearly independent.

By Theorem 2.25, $\Phi(H) = H'H^p$, and since $H'H^p \leq G'G^p$, it follows that $\Phi(H) \leq H \cap \Phi(G)$. Then, by the second and the third isomorphism theorems,

$$\frac{H\Phi(G)}{\Phi(G)} \cong \frac{H}{H \cap \Phi(G)} \cong \frac{H/\Phi(H)}{(H \cap \Phi(G))/\Phi(H)}$$

is a quotient subgroup of $H/\Phi(H)$. By contradiction, let us suppose that the system $\{h_1\Phi(H), \dots, h_r\Phi(H)\}$ is not linearly independent in $H/\Phi(H)$. Then, by the isomorphism defined above, $\{h_1\Phi(G), \dots, h_r\Phi(G)\}$ would not be linearly independent in $H\Phi(G)/\Phi(G) \leq G/\Phi(G)$, which is absurd. Hence, it is linearly independent and it can be extended to a basis of $H/\Phi(H)$:

$$\{h_1\Phi(H), \dots, h_r\Phi(H), h_{r+1}\Phi(H), \dots, h_s\Phi(H)\}.$$

Thus, by Theorem 2.23, $\{h_1, \dots, h_r, h_{r+1}, \dots, h_s\}$ is a minimal system of generators of H and the proof is complete. □

Theorem 3.18. *Let G be a powerful p-group and H a subgroup of G. Then, $d(H) \leq d(G)$.*

Proof. We will prove the result by induction on the order of G, so we may assume that $|G| > 1$ and we put $d = d(G)$. Since G is powerful, by Theorem 2.25, $\Phi(G) = G^p$, so we consider the factor group $\overline{G} = G/G^p$, of which, by Theorem 2.23, we know that it is an $\mathbb{F}_p$-vector space. We take the subspace $\overline{H} = HG^p/G^p$ and a basis of it $\{\overline{h_1}, \dots, \overline{h_r}\}$, and we extend this basis to a basis of $\overline{G}$, $\{\overline{h_1}, \dots, \overline{h_r}, \overline{g_1}, \dots, \overline{g_u}\}$. Then, again by Theorem 2.23, we have that $\{h_1, \dots, h_r, g_1, \dots, g_u\}$ is a minimal system of generators of G and, in particular, $d = r + u$.

According to Theorem 3.16, $G^p = \langle h_1^p, \dots, h_r^p, g_1^p, \dots, g_u^p\rangle$, and we can say without loss of generality that $\{h_1^p, \dots, h_s^p, g_1^p, \dots, g_v^p\}$ is a minimal system of generators of G^p with $s \leq r$ and $v \leq u$. By the previous lemma, the subset $\{h_1^p, \dots, h_s^p\}$ can be extended to a minimal system of generators of $H \cap G^p$: $\{h_1^p, \dots, h_s^p, h_1', \dots, h_t'\}$. Now, by Theorem 3.9, G^p is powerful and $|G^p| < |G|$, so by hypothesis of induction, $s + t = d(H \cap G^p) \leq d(G^p) = s + v$, that is, $t \leq v \leq u$.

In summary, we have that $HG^p/G^p = \langle \overline{h_1}, \dots, \overline{h_r}\rangle$, whence, by the second isomorphism theorem, $H/(H \cap G^p) = \langle \overline{h_1}, \dots, \overline{h_r}\rangle$. On the other hand, we have proved that $H \cap G^p = \langle h_1^p, \dots, h_s^p, h_1', \dots, h_t'\rangle$, with $t \leq u$. Therefore, $H = \langle h_1, \dots, h_r, h_1', \dots, h_t'\rangle$ and $d(H) \leq r + t \leq r + u = d$, as required. □

3.3 Omega subgroups of powerful p-groups

As we have seen, if G is a powerful p-group, the subgroup G^p coincides with the set of all the pth powers of elements of G. The logical question in this situation would be whether the subgroups $\Omega_i(G)$ coincide with the set of all the elements whose orders divide p^i. The next theorem gives

an affirmative answer to this question for the primes $p > 2$. If $p = 2$, the result changes slightly and it is not as good as the previous one.

However we will need several result before we can prove this theorem: Kummer's Theorem and P. Hall's formula. Kummer's Theorem asserts that given integers $n \geq m \geq 0$ and a prime number p, the maximum integer k such that p^k divides the binomial coefficient $\binom{n}{m}$ is equal to the number of carries when m is added to $n - m$ in base p. The proof of this theorem can be found in [7] or, if a more modern reference was desired, in Theorem 13.6 of [1]. Nevertheless, we only will need a particular case of this result in which n is a power of p, and its proof is much simpler than the one of the general case.

Lemma 3.19. *Let $n \geq 1$ be an integer and p a prime number. If v expresses the p-adic valuation of a number, then $v\left(\binom{p^n}{k}\right) = n - v(k)$, for $1 \leq k \leq p^n$.*

Proof. If $k = p^n$ the result is clear since $v(p^n) = n$. If $1 \leq k < p^n$, we have $v(p^n - k) = v(k)$. Indeed, if p^r for some $r < n$ divides $p^n - k$, then p^r divides k, and analogously, if p^r divides k, then $r < n$ and p^r divides $p^n - k$. So, taking valuation in the equality

$$k!\binom{p^n}{k} = p^n(p^n - 1)\dots(p^n - (k-1)),$$

since $v(st) = v(s) + v(t)$ for any $s, t \in \mathbb{Z}$, we get

$$\begin{aligned} v(1) + v(2) + \ldots + v(k) + v\left(\binom{p^n}{k}\right) &= v(p^n) + v(p^n - 1) + \ldots + v(p^n - (k-1)) \\ &= v(p^n) + v(1) + \ldots + v(k-1), \end{aligned}$$

and the result follows. □

The other result we need is P. Hall's formula, which relates $x^m y^m$ and $(xy)^m$:

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

where $c_i \in \gamma_i(H)$ with $H = \langle x, y \rangle$. This formula was proved by P. Hall in [5], but its proof is not given here since it is too long. The reader can find a more modern proof of it in Theorem 3.5 of [9]. In our case, if m is a power of p, then

$$x^{p^j} y^{p^j} = (xy)^{p^j} c_2^{\binom{p^j}{2}} c_3^{\binom{p^j}{3}} \dots c_{p^j}^{\binom{p^j}{p^j}},$$

where $c_i \in \gamma_i(H)$ with $H = \langle x, y \rangle$, and we can say by the previous lemma that if $p^k \mid i$ but $p^{k+1} \nmid i$, then $c_i^{\binom{p^j}{i}} \in \gamma_i(H)^{p^j}$, and consequently,

$$(xy)^{p^j} \equiv x^{p^j} y^{p^j} \pmod{\gamma_2(H)^{p^j} \gamma_p(H)^{p^{j-1}} \dots \gamma_{p^j}(H)}.$$

Theorem 3.20. *Let G be a powerful p-group for an odd prime p. Then, for every $i \geq 0$:*

i) *If $x, y \in G$ and $o(y) \leq p^i$, then $o([x,y]) \leq p^i$.*

ii) *If $x, y \in G$ are such that $o(x) \leq p^{i+1}$ and $o(y) \leq p^i$, then $o([x^{p^j}, y^{p^k}]) \leq p^{i-j-k}$ for all $j, k \geq 0$. If $i-j-k < 0$, then p^{i-j-k} is interpreted as 1.*

iii) *$\exp \Omega_i(G) \leq p^i$ (that is, $\Omega_i(G) = \{g \in G \mid o(g) \leq p^i\}$).*

Proof. We apply induction on the order of G globally to all assertions of the theorem. Thus, since the results are clear for $G = 1$, we assume that *i)*, *ii)* and *iii)* hold for $|G| = p^{n-1}$ and we prove it for $|G| = p^n$.

i) Since the order of y is less than or equal to p^i, so is the order of $(y^{-1})^x$. Thus, we set $T = \langle y, G' \rangle$ and the commutator $[x,y] = (y^{-1})^x y$ is a product of two elements of order less than or equal to p^i in T, whence $[x,y] \in \Omega_i(T)$. By Lemma 3.11, T is powerful. In addition, T is a proper subgroup of G since, otherwise, if $T = G$, then $G = \langle y, G' \rangle = \langle y, \Phi(G) \rangle = \langle y \rangle$ and the result trivially holds. Then, by induction, we apply *iii)* on T and we conclude that since $[x,y] \in \Omega_i(T)$, the order of $[x,y]$ is $\leq p^i$, as required.

ii) In this case, we apply reverse induction on i. We write $\exp G = p^e$, and firstly, we prove the result for $i \geq e$. Since G is powerful, by the Interchanging Lemma, $[G^{p^j}, G^{p^k}] = (G')^{p^{j+k}} \leq G^{p^{j+k}}$, so $[x^{p^j}, y^{p^k}] = g^{p^{j+k}}$ for some $g \in G$, and $o([x^{p^j}, y^{p^k}]) = o(g^{p^{j+k}}) \leq p^{e-j-k} \leq p^{i-j-k}$. Suppose now that $i < e$, and we consider the subgroup $T = \langle x^{-1}, x^{y^{p^k}} \rangle = \langle x^{-1}, x^{-1} x^{y^{p^k}} \rangle = \langle x, [x, y^{p^k}] \rangle$. By P. Hall's formula, since $[x^{p^j}, y^{p^k}] = (x^{-1})^{p^j} (x^{y^{p^k}})^{p^j}$ and $x^{-1} x^{y^{p^k}} = [x, y^{p^k}]$, we get

$$[x^{p^j}, y^{p^k}] \equiv [x, y^{p^k}]^{p^j} \pmod{\gamma_2(T)^{p^j} \gamma_p(T)^{p^{j-1}} \dots \gamma_{p^j}(T)}.$$

By *i)*, we have $o([x, y^{p^k}]) \leq o(y^{p^k}) \leq p^{i-k}$, so it follows that $[x, y^{p^k}]^{p^j} \in \Omega_{i-j-k}(T)$. Note that, arguing as in the last paragraph, the induction on the group order yields that $\exp \Omega_n(T) \leq p^n$ for all n. Then, if we prove that all the subgroups of the congruence lie in $\Omega_{i-j-k}(T)$, then, since their product also lies in $\Omega_{i-j-k}(T)$, we can conclude that the order of $[x^{p^j}, y^{p^k}]$ is at most p^{i-j-k}, as desired.

First, by Theorem 1.23, we have $\gamma_2(T) = \langle [x, [x, y^{p^k}]] \rangle^T$. By *i)*, the order of $[x, [x, y^{p^k}]]$ is at most p^{i-k}, so $\langle [x, [x, y^{p^k}]] \rangle \leq \Omega_{i-k}(T)$. Besides, $\Omega_{i-k}(T)$ is normal in T, so that

$$\gamma_2(T) = \langle [x, [x, y^{p^k}]] \rangle^T \leq \Omega_{i-k}(T)^T = \Omega_{i-k}(T).$$

Then, we get $\gamma_2(T)^{p^j} \leq \Omega_{i-k}(T)^{p^j} \leq \Omega_{i-j-k}(T)$. Let us now prove, by induction on r, that $\gamma_{r+2}(T) \leq \Omega_{i-k-r}(T)$ for all $r \geq 0$. We have just seen this for $r = 0$. In the general case, it suffices to show, by the definition of the lower central series, that if $a \in \gamma_{r+1}(T)$ and $b \in T$, then $o([a,b]) \leq p^{i-k-r}$. Since by hypothesis of induction $\gamma_{r+1}(T) \leq \Omega_{i-k-r+1}(T)$, we know that $o(a) \leq p^{i-k-r+1}$. On the other hand, since

$$[T,T] = \langle [x, y^{p^k}, x] \rangle^T \leq [G, G^{p^k}, G]^T = [G^{p^k}, G, G]$$

we have $a \in \gamma_{r+1}(T) \leq [G^{p^k}, G, \overset{r+1}{\dots}, G]$, and by Theorem 3.14,

$$[G^{p^k}, G, \overset{r+1}{\dots}, G] \leq [G^{p^{k+1}}, G, \overset{r}{\dots}, G] \leq \dots \leq G^{p^{k+r+1}}.$$

Thus, $a = g^{p^{k+r+1}}$ for some $g \in G$, and then, $o(g) \leq p^{i+2}$. But $b \in T$ has order less than or equal to p^{i+1}, so the reverse induction on i we are applying yields that $o([a,b]) = o([g^{p^{k+r+1}}, b]) \leq p^{i-k-r}$.

Now, if $r \geq 1$, we have $\gamma_{p^r}(T) \leq \gamma_{r+2}(T)$, and consequently $\gamma_{p^r}(T)^{p^{j-r}} \leq \Omega_{i-j-k}(T)$, and we are done.

iii) Let x, y and z be elements of G of order p. Then, since G is powerful, $[x,y] = g^p$ for some $g \in G$. Furthermore, by i), the order of g^p is at most p, so the order of g is at most p^2. Then, by ii), the order of $[x,y,z] = [g^p, z]$ is 1, that is, $[x,y,z] = 1$. Hence, since x, y and z are three arbitrary generators of $\Omega_1(G)$, the nilpotency class of $\Omega_1(G)$ is at most 2. As in the proof of Lemma 3.12, we have

$$(xy)^p = x^p y^p [y,x]^{\binom{p}{2}}.$$

Since $x^p = y^p = [x,y]^p = 1$, it follows that $(xy)^p = 1$. Therefore, $\exp \Omega_1(G) \leq p$. For the general case, we consider the quotient group $\overline{G} = G/\Omega_1(G)$ and by the induction on the order of the group, we get $\exp \Omega_{i-1}\left(\overline{G}\right) \leq p^{i-1}$. Thus, if we take an element $g \in \Omega_i(G)$, since the generators of $\Omega_i(G)$ are the elements of G whose orders are at most p^i, we know that $g = x_1 \dots x_r$ with $x_s^{p^i} = 1$ for every $s = 1, \dots, r$. Since $x_s^{p^i} = (x_s^{p^{i-1}})^p = 1$, it follows that $x_s^{p^{i-1}} \in \Omega_1(G)$, that is, $\overline{x_s}^{p^{i-1}} = \overline{1}$. Then, every $\overline{x_s}$ is in $\Omega_{i-1}(\overline{G})$, whence $\overline{g} \in \Omega_{i-1}(\overline{G})$. Therefore, $\overline{g}^{p^{i-1}} = \overline{1}$, that is, $g^{p^{i-1}} \in \Omega_1(G)$, and since $\exp \Omega_1(G) \leq p$, we conclude that $g^{p^i} = (g^{p^{i-1}})^p = 1$, so $\exp \Omega_i(G) \leq p^i$. □

For the case of $p = 2$, as said, the result changes slightly: if G is a powerful 2-group, then $\exp \Omega_i(G) \leq 2^{i+1}$. For instance, we take $A = \langle a \rangle \times \langle b \rangle \cong C_2 \times C_8$ and we consider $G = \langle x \rangle \ltimes A$ with $o(x) = 2$, $a^x = ab^4$ and $b^x = b$. Obviously, $x, a \in \Omega_1(G)$, but

$$(xa)^2 = xaxa = x^2 a^x a = ab^4 a = a^2 b^4 = b^4 \neq 1,$$

and $xa \in \Omega_1(G)$.

3.4 Finite p-groups as sections of powerful p-groups

The next thing we want to check is whether any p-group can be seen as a subgroup of a powerful p-group. Unfortunately, this is not true. For example, for $p > 2$, we consider the symmetric group Σ_{p^2}. We define $\tau_i = (ip+1\ ip+2\ \dots\ (i+1)p)$, for $i = 0, \dots, p-1$ and we set $Q = \langle \tau_0, \dots, \tau_{p-1} \rangle$. Thus, since τ_i and τ_j are disjoint for $i \neq j$, we have $Q \cong C_p \times \overset{p}{\dots} \times C_p$ and $|Q| = p^p$. Now, we also define

$$\sigma = \Big(1\ p+1\ 2p+1\ \dots\ (p-1)p+1\Big)\Big(2\ p+2\ 2p+2\ \dots (p-1)p+2\Big)\dots\Big(p\ 2p\ 3p\ \dots\ p^p\Big),$$

and we put $P = Q\langle\sigma\rangle$. Firstly, we have to check if P is a subgroup of Σ_{p^2}, but it is immediate using Lemma 1.14 since $\sigma \in N_{\Sigma_{p^2}}(Q)$. Indeed, $\tau_i^\sigma = \tau_{i+1}$ if $i < p-1$ and $\tau_{p-1}^\sigma = \tau_1$. We observe that $Q \cap \langle\sigma\rangle = 1$, so

$$|P| = \frac{|Q||\langle\sigma\rangle|}{|Q \cap \langle\sigma\rangle|} = \frac{p^p p}{1} = p^{p+1},$$

that is, P is a p-group. Every generator defined for P is of order p, so $P \leq \Omega_1(P)$, and then $P = \Omega_1(P)$.

Now, $|\Sigma_{p^2}| = p^2! = 1 \cdot 2 \dots p \dots 2p \dots (p-1)p \dots p^2$, so the p-adic valuation of $|\Sigma_{p^2}|$ is $p+1$, whence P is a Sylow p-subgroup of Σ_{p^2}. If we take the cycle $\rho = (1\ 2\ \dots\ p^2)$, its order, which is p^2, is a power of p, so ρ is in a Sylow p-subgroup. Then, there exists $g \in G$ such that $\rho^g \in P$, and the order of ρ^g remains p^2. Then, $\exp \Omega_1(P) = \exp P \geq p^2$. If P were a subgroup of a powerful p-group G, then $\exp \Omega_1(G) \geq \exp \Omega_1(P) \geq p^2$, and by the previous theorem, this is a contradiction.

The same occurs when $p = 2$. If we consider the dihedral group D_{2^n} with $n \geq 4$, then

$$D_{2^n} = \langle a, b \mid a^{2^{n-1}} = b^2 = 1, a^b = a^{-1} \rangle = \langle ba, b \rangle,$$

and since both ba and b are of order 2, because of the same reason as the previous example, $\Omega_1(D_{2^n}) = D_{2^n}$, but $\exp D_{2^n} = 2^{n-1} \geq 2^3$ since $n \geq 4$.

Nevertheless, even though not every p-group can be seen as a subgroup of a powerful p-group, every p-group can be seen as a section of a powerful p-group. To prove this, we need to develop a little bit the theory of $GL_n(K)$, the group of all the n-by-n invertible matrices over the field K.

Throughout the rest of the chapter, we will denote by E_{ij} the matrix of zeros with 1 in the position (i, j). Note that $E_{ij}E_{kl} = \delta_{jk}E_{il}$ where $\delta_{jk} = 1$ if $j = k$ and $\delta_{jk} = 0$ if $j \neq k$. The following definition will be essential when working in $GL_n(K)$.

Definition 3.21. Let K be a field. We say that a matrix of $GL_n(K)$ is a *transvection* if it is of the form

$$t_{ij}(\alpha) = I_n + \alpha E_{ij},$$

where $\alpha \in K$.

This type of matrices are really important and useful in the theory of matrices, so let us see some basic properties of them.

Theorem 3.22. *Let K be a field and $\alpha, \beta \in K$. Then,*

i) $t_{ij}(\alpha)t_{ij}(\beta) = t_{ij}(\alpha + \beta)$.

ii) $t_{ij}(\alpha)^n = t_{ij}(n\alpha)$ *for every* $n \in \mathbb{Z}$. *In particular,* $t_{ij}(\alpha)^{-1} = t_{ij}(-\alpha)$.

iii) If $j \neq k$ *or* $i \neq l$

$$[t_{ij}(\alpha), t_{kl}(\beta)] = I_n,$$

if $j = k$

$$[t_{ij}(\alpha), t_{kl}(\beta)] = t_{il}(\alpha\beta)$$

and if $i = l$

$$[t_{ij}(\alpha), t_{kl}(\beta)] = t_{jk}(-\alpha\beta).$$

Proof. i) It is immediate computing the product.

ii) It is immediate by i).

iii) If $j \neq k$ or $i \neq l$, the result is trivially true since $E_{ij}E_{kl} = E_{kl}E_{ij} = 0$.
If $j = k$, then

$$\begin{aligned}
&[I_n+\alpha E_{ij}, I_n + \beta E_{jl}] \\
&\quad = (I_n - \alpha E_{ij})\,(I_n - \beta E_{jl})\,(I_n + \alpha E_{ij})\,(I_n + \beta E_{jl}) \\
&\quad = (I_n - \alpha E_{ij} - \beta E_{jl} + \alpha\beta E_{il})(I_n + \alpha E_{ij} + \beta E_{jl} + \alpha\beta E_{il}) \\
&\quad = I_n + \alpha E_{ij} + \beta E_{jl} + \alpha\beta E_{il} - \alpha E_{ij} - \alpha\beta E_{il} - \beta E_{jl} + \alpha\beta E_{il} \\
&\quad = I_n + \alpha\beta E_{il},
\end{aligned}$$

and the result holds. If $i = l$, the commutator is calculated in the same way. □

We will work with the group under multiplication of all the n-by-n unitriangular matrices over the field K, which is denoted by $UT_n(K)$. Thus, let us see a result related with it.

Theorem 3.23. *The group $UT_n(\mathbb{F}_p)$ is a Sylow p-subgroup of $GL_n(\mathbb{F}_p)$.*

Proof. The order of $GL_n(\mathbb{F}_p)$ is the number of different n-by-n invertible matrices, which is

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)\dots(p^n - p^{n-1}),$$

so its Sylow p-subgroups have order $pp^2p^3\dots p^{n-1} = p^{(n-1)n/2}$.

On the other hand, the order of $UT_n(\mathbb{F}_p)$ is the number of the unitriangular matrices. Since we can freely choose in $\mathbb{F}_p$ any entry above the main diagonal and the number of such entries is $1 + 2 + \dots + n - 1 = n(n-1)/2$, then,

$$|UT_n(\mathbb{F}_p)| = p^{n(n-1)/2},$$

and therefore, the theorem follows. □

Remark 3.24. It is known by representation theory that every group is isomorphic to a subgroup of $GL_n(K)$ for some $n \in \mathbb{N}$ and for any field K. Thus, the previous theorem shows that if P is an arbitrary p-group, then, for some $g \in GL_n(\mathbb{F}_p)$, the group P^g (which is isomorphic to P) is isomorphic to a subgroup of $UT_n(\mathbb{F}_p)$, let us call it Q. In other words,

$$P \cong P^g \cong Q \leq UT_n(\mathbb{F}_p)$$

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

Finally, let us check that the set of matrices defined in the following lemma is a group, since the proof of the following theorem is based on it.

Theorem 3.25. *Let p be a prime, and let G be the set of n-by-n unitriangular matrices over the ring*

$$\mathbb{Z}\left[\frac{1}{p}\right] = \left\{\frac{a}{p^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}\right\}$$

of the form $A = (a_{ij})$*, such that* $a_{ij} \in \frac{1}{p^{j-i-1}}\mathbb{Z}$*, for* $i < j$*. Then,* G *is a group, and*

$$G = \left\langle t_{ij}\left(\frac{1}{p^{j-i-1}}\right) \mid i < j \right\rangle.$$

Proof. Obviously, the operation is associative and the identity element is the identity matrix. It is routine to check that G is closed under multiplication, so we have to prove that every element of G has an inverse in G. However, if we first prove that every $A \in G$ is a product of transvections of the form $t_{ij}(\frac{1}{p^{j-i-1}})$, we will be done since, by Theorem 3.22, it can be easily deduced that the inverse of the transvections are in G. Thus, if we write $a_{ij} = \frac{\alpha_{ij}}{p^{j-i-1}}$, let us prove that

$$A = \prod_{i<j} t_{ij}\left(\frac{1}{p^{j-i-1}}\right)^{\alpha_{ij}}$$

where the order of the factors in this product corresponds with the following sorting of the indices such that $i < j$:

$$\{(n-1,n),(n-2,n),(n-2,n-1),\ldots,(2,n),\ldots,(2,3),(1,n),\ldots,(1,2)\}.$$

Indeed, if we write $t_{ij}(\frac{1}{p^{j-i-1}})^{\alpha_{ij}} = t_{ij}(\frac{\alpha_{ij}}{p^{j-i-1}})$ in the form $I_n + a_{ij}E_{ij}$, we have

$$\prod_{i<j}(I_n + a_{ij}E_{ij}) = I_n + \sum_{i<j} a_{ij}E_{ij} + \sum{}',$$

where $\sum'$ is a sum of the products in which there appear at least two matrices of the form E_{ij}. Because of the way in which we have sorted the indices, if we have $E_{ij}E_{kl}$, necessarily $j > k$, and $E_{ij}E_{kl} = 0$. Therefore,

$$\prod_{i<j} t_{ij}\left(\frac{1}{p^{j-i-1}}\right)^{\alpha_{ij}} = I_n + \sum_{i<j} a_{ij}E_{ij} = A,$$

and the proof is complete. □

Now, we are ready to expose the following theorem.

Theorem 3.26. *Each finite p-group* P *is isomorphic to a section of a powerful p-group* G*. In other words, there exist* $H \leq G$ *and* $K \trianglelefteq H$ *such that* $H/K \cong P$*.*

Proof. Let p be an odd prime, and let G be the group defined in the previous lemma. First, we want to show that $G' \leq G^p$. By Theorem 1.23,

$$G' = \left\langle \left[t_{ij}\left(\frac{1}{p^{i-j-1}}\right), t_{kl}\left(\frac{1}{p^{k-l-1}}\right)\right] \mid i < j, k < l \right\rangle^G,$$

and by Theorem 3.22, the value of these commutators is: if $j = k$

$$\left[t_{ij}\left(\frac{1}{p^{i-j-1}}\right), t_{jl}\left(\frac{1}{p^{j-l-1}}\right)\right] = t_{il}\left(\frac{1}{p^{i-l-2}}\right)$$

with $i < l-1$, and if $i = l$,

$$\left[t_{ij}\left(\frac{1}{p^{i-j-1}}\right), t_{ki}\left(\frac{1}{p^{k-i-1}}\right)\right] = t_{kj}\left(\frac{1}{p^{k-j-2}}\right)$$

with $k < j-1$. Otherwise, the commutators vanish. Therefore,

$$G' = \left\langle t_{ij}\left(\frac{1}{p^{i-j-2}}\right) \mid i < j-1 \right\rangle^G.$$

Let us prove that the subgroup $\left\langle t_{ij}(\frac{1}{p^{i-j-2}}) \mid i < j-1 \right\rangle$ is normal in G. In order to do this, we take the generators of G and their inverses (recall that G is not finite), and the generators of our subgroup and we observe that $[t_{ij}(\frac{1}{p^{i-j-2}}), t_{kl}(\pm\frac{1}{p^{k-l-1}})]$ is equal to I_n if $j \neq k$ or $i \neq l$, equal to $t_{il}(\pm\frac{1}{p^{i-l-3}})$ if $j = k$ or equal to $t_{kj}(\mp\frac{1}{p^{k-j-3}})$ if $i = l$. In any case, it lies in our subgroup, so it is normal, whence

$$G' = \left\langle t_{ij}\left(\frac{1}{p^{i-j-2}}\right) \mid i < j-1 \right\rangle,$$

or which is the same,

$$G' = \left\{ \begin{pmatrix} 1 & 0 & & & * \\ & 1 & 0 & & \\ & & 1 & 0 & \\ & & & \ddots & 0 \\ 0 & & & & 1 \end{pmatrix} \mid a_{ij} \in \frac{1}{p^{i-j-2}}\mathbb{Z}, \text{ for } j > i+1 \right\}.$$

We notice that $t_{ij}(\frac{1}{p^{i-j-2}}) = t_{ij}(\frac{1}{p^{i-j-1}})^p \in G^p$, so every generator given for G' is a pth power of a generator of G. Then, $G' \leq G^p$.

Observe that following a similar procedure several times with $\gamma_i(G)$ for $i \geq 2$, it follows that G is a nilpotent group of class $n-1$.

We consider now $\overline{G} = G/G^{p^n}$. Obviously, $\overline{G}$ is finitely generated and it is nilpotent since so is G. In addition, for any $\overline{g} \in \overline{G}$, it follows that $\overline{g}^{p^n} = \overline{1}$, so $\exp \overline{G} \leq p^n$, and of course, $\exp \overline{G}/\overline{G}' \leq p^n$. Thus, by Exercise 5 in the Appendix, $\overline{G}$ is finite, and since, as said, $\overline{g}^{p^n} = \overline{1}$ for every $\overline{g} \in \overline{G}$, it is a finite p-group. Moreover, since $\overline{G'} \leq \overline{G}^p$, the group $\overline{G}$ is a powerful p-group.

Let

$$K = \langle t_{ij}(1) \mid i < j \rangle = \left\{ \begin{pmatrix} 1 & & & & * \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \mid a_{ij} \in \mathbb{Z}, \text{ for } i < j \right\}$$

and let

$$L = \langle t_{ij}(p) \mid i < j \rangle = \left\{ \begin{pmatrix} 1 & & & & * \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \mid a_{ij} \in p\mathbb{Z}, \text{ for } i < j \right\}.$$

Obviously, K and L are subgroups of G. Besides, $L \triangleleft K$ since all $[t_{ij}(1), t_{kl}(p)]$ lie in L, so we consider the factor group K/L. This group is isomorphic to $UT_n(\mathbb{F}_p)$, the group of all upper triangular matrices in $GL_n(\mathbb{F}_p)$. Indeed, the kernel of the homomorphism which reduces every element of a matrix modulo p is L, and the isomorphism follows by the first isomorphism theorem. Then, by Theorem 3.23, the subgroup K/L is a Sylow p-subgroup of $GL_n(\mathbb{F}_p)$.

Let us show that $G^{p^n} \leq L$. We take $A = (a_{ij}) \in G$, and we write $B = A - I_n$. Then,

$$A^{p^n} = (I_n + B)^{p^n} = I_n + p^n B + \binom{p^n}{2} B^2 + \cdots + B^{p^n}.$$

Since $b_{ij} \in \frac{1}{p^{j-i-1}}\mathbb{Z}$ for $j > i$, and $b_{ij} = 0$ otherwise, it follows that in B^r, with $r < n$, the (i,j)th entry is 0 if $j \leq i + r$. Moreover, if b_{rij} is the (i,j)th entry of B^r, then $b_{rij} \in \frac{1}{p^{j-i-r}}\mathbb{Z} \subseteq \frac{1}{p^{n-r-1}}\mathbb{Z}$ since $j - i \leq r \leq n - 1$. If $r \geq n$, the terms from B^r on vanish (in particular, since $p^n > n$, we have $B^{p^n} = 0$). If p^k is the maximal power of p to divide r, by Lemma 3.19, $\binom{p^n}{r}$ is divisible by $p^{n-k} > p^{n-r}$, and thus $\binom{p^n}{r}B^r$ has all its entries integers divisible by p. Then, $A^{p^n} \in L$, and therefore, $G^{p^n} \leq L$. Now, by the third isomorphism theorem, we have

$$\frac{K/G^{p^n}}{L/G^{p^n}} \cong K/L,$$

so K/L is a section of the powerful group $\overline{G}$. Let P be an arbitrary p-group. The characterization of K/L as a Sylow p-subgroup of $GL_n(\mathbb{F}_p)$ noted above and Remark 3.24 show that P can be seen as a subgroup of K/L. Let us call this subgroup Q/L with $L \leq Q \leq K$, that is, $P \cong Q/L$. Then,

$$\frac{Q/G^{p^n}}{L/G^{p^n}} \cong Q/L \cong P,$$

and the proof is complete for $p > 2$.

If $p = 2$, we change our notation to insist that the (i,j)th entry of an element of G lies in $\frac{1}{2^{j-i-2}}\mathbb{Z}$, i.e., we replace the group G by G^2. Then, a similar argument applies.

□

Appendix A

Exercises

Exercise 1. Let G be a group, $x, y \in G$ and $H = \langle x, y \rangle$.

i) If H' is abelian, prove that

$$[y, x^i] = [y, x]^i [y, x, x]^{\binom{i}{2}} [y, x, x, x]^{\binom{i}{3}} \dots [y, x, \overset{i}{\dots}, x]^{\binom{i}{i}},$$

for $i \geq 1$. Obtain a similar expression for $[y^i, x]$.

ii) If $\langle y, H' \rangle$ is abelian, deduce that

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

for $n \geq 2$.

Solution. i) Let us prove the result by induction on i. For $i = 1$ it is clear, so let us suppose that it holds for $i - 1$ and let us prove it for i. By Theorem 1.5 it is known that

$$[y, x^i] = [y, x][y, x]^x \dots [y, x]^{x^{i-1}},$$

and since $[y, x]^z = [y, x][y, x, z]$ for any $z \in G$,

$$[y, x^i] = [y, x][y, x][y, x, x] \dots [y, x][y, x, x^{i-1}].$$

Now we note that $[y, x] \in H'$ and $[y, x, x^j] = [[y, x], x^j] \in H'$ for all $j = 1, \dots, i$, so they commute since H' is abelian, and we get

$$[y, x^i] = [y, x]^i [y, x, x] \dots [y, x, x^{i-1}].$$

By hypothesis of induction,

$$[y, x, x^j] = [[y, x], x^j] = [[y, x], x]^j [[y, x], x, x]^{\binom{j}{2}} \dots [[y, x], x, \overset{j}{\dots}, x]^{\binom{j}{j}},$$

for all $j = 1, \dots, i - 1$. In addition, all these commutators are in H', so replacing in the formula,

$$[y, x^i] = [y, x]^i [y, x, x]^{1+2+\dots+(i-1)} [y, x, x, x]^{\binom{2}{2}+\binom{3}{2}+\dots+\binom{i-1}{2}} \dots [y, x, x, \overset{i-1}{\dots}, x]^{\binom{i-1}{i-1}}.$$

Now, applying the well known combinatorial relation

$$\sum_{i=k}^{n-1} \binom{i}{k} = \binom{n}{k+1},$$

we finally obtain

$$[y, x^i] = [y, x]^i [y, x, x]^{\binom{i}{2}} [y, x, x, x]^{\binom{i}{3}} \dots [y, x, \overset{i}{\dots}, x]^{\binom{i}{i}}.$$

Making the same computation we can get

$$[y^i, x] = [y, x]^i [y, x, y]^{\binom{i}{2}} [y, x, y, y]^{\binom{i}{3}} \dots [y, x, y, \overset{i-1}{\dots}, y]^{\binom{i}{i}}$$

ii) We will use induction on n. For $n = 2$ it suffices to see that

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

and since y and $[y, x]$ commute, $(xy)^2 = x^2 y^2 [y, x]$. For a general n, we observe that $(xy)^n = xy(xy)^{n-1}$, and we apply the hypothesis of induction:

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

Using that $\langle y, H' \rangle$ is abelian,

$$\begin{aligned}(xy)^n &= xyx^{n-1}y^{n-1}[y, x]^{\binom{n-1}{2}} [y, x, x]^{\binom{n-1}{3}} \dots [y, x, \overset{n-2}{\dots}, x]^{\binom{n-1}{n-1}} \\ &= x^n y[y, x^{n-1}]y^{n-1}[y, x]^{\binom{n-1}{2}} [y, x, x]^{\binom{n-1}{3}} \dots [y, x, \overset{n-2}{\dots}, x]^{\binom{n-1}{n-1}} \\ &= x^n y^n [y, x^{n-1}][y, x]^{\binom{n-1}{2}} [y, x, x]^{\binom{n-1}{3}} \dots [y, x, \overset{n-2}{\dots}, x]^{\binom{n-1}{n-1}},\end{aligned}$$

and by part i) and using the formula $\binom{n}{j} = \binom{n-1}{j} + \binom{n-1}{j-1}$, we finally get

$$\begin{aligned}(xy)^n &= x^n y^n [y, x]^{\binom{n-1}{2}+\binom{n-1}{1}} [y, x, x]^{\binom{n-1}{3}+\binom{n-1}{2}} \dots [y, x, \overset{n-2}{\dots}, x]^{\binom{n-1}{n-1}+\binom{n-1}{n-2}} [y, x, \overset{n-1}{\dots}, x]^{\binom{n-1}{n-1}} \\ &= x^n y^n [y, x]^{\binom{n}{2}} [y, x, x]^{\binom{n}{3}} \dots [y, x, \overset{n-1}{\dots}, x]^{\binom{n}{n}}.\end{aligned}$$

□

Exercise 2. Let G be a group and X a subset of G such that $G = \langle X \rangle$.

i) Prove by induction on $i \geq 1$ that

$$Z_i(G) = \{g \in G \mid [g, x_1, \dots, x_i] = 1, \forall x_1, \dots, x_i \in X\}.$$

In particular,

$$Z_i(G) = \{g \in G \mid [g, x_1, \dots, x_i] = 1, \forall x_1, \dots, x_i \in G\}.$$

(In this way, the elements of the ith center are characterized by a property which is a clear generalization of the condition to be in the center.)

ii) Deduce that $Z_i(G/Z_j(G)) = Z_{i+j}(G)/Z_j(G)$ for all $i, j \geq 0$.

Solution. i) For $i = 1$, it is clear by the definition of the center. For a general i, we consider the quotient group $\overline{G} = G/Z_{i-1}(G)$, and by definition of the ith center, since $\overline{G} = \langle \overline{X} \rangle$, we have

$$g \in Z_i(G) \Leftrightarrow [\overline{g}, \overline{x}] = \overline{1}, \forall \overline{x} \in \overline{X} \Leftrightarrow [g, x] \in Z_{i-1}(G), \forall x \in X.$$

By hypothesis of induction, this latter happens if and only if $[g, x, x_1, \ldots, x_{i-1}] = 1$ for all $x, x_1, \ldots, x_{n-1} \in X$, as we wanted.

ii) By i), it follows that

$$\begin{aligned} Z_i(G/Z_j(G)) &= \{\overline{g} \mid [\overline{g}, \overline{x}_1, \ldots, \overline{x}_i] = \overline{1}, \forall x_1, \ldots, x_i \in G\} \\ &= \{\overline{g} \mid [g, x_1, \ldots, x_i] \in Z_j(G), \forall x_1, \ldots, x_i \in G\} \\ &= \{\overline{g} \mid [[g, x_1, \ldots, x_i], x_{i+1}, \ldots, x_{i+j}] = 1, \forall x_1, \ldots, x_{i+j} \in G\} \\ &= \{\overline{g} \mid g \in Z_{i+j}(G)\} \\ &= \frac{Z_{i+j}(G)}{Z_j(G)}. \end{aligned}$$

□

Exercise 3. Calculate the lower and upper central series of the following groups:

i) Σ_n, for $n \geq 3$.

ii) $D_{2n} = \langle a, b \mid a^n = b^2 = 1, a^b = a^{-1} \rangle$, for $n \geq 3$.

iii) $D_\infty = \langle a, b \mid b^2 = 1, a^b = a^{-1} \rangle$.

Solution. i) Let us start with the lower central series. Since $A_n = \langle \tau \in \Sigma_n \mid \tau \text{ is a 3-cycle} \rangle$, $|\Sigma_n : A_n| = 2$ and $(1\ 2) \notin A_n$, it follows that

$$\Sigma_n = \langle (1\ 2), \tau \mid \tau \in A_n \text{ is a 3-cycle} \rangle.$$

Thus, by Theorem 1.23,

$$\Sigma_n' = [\Sigma_n, \Sigma_n] = \langle [(1,2), \tau]^s [\sigma, \rho]^r \mid \tau, \sigma, \rho \text{ are 3-cycles and } s, r \in \Sigma_n \rangle.$$

However, if we denote $\tau = (i\ j\ k)$, then

$$[(1\ 2), \tau] = (\tau^{-1})^{(1\ 2)} \tau = (i\ k\ j)^{(1\ 2)} (i\ j\ k),$$

and making any possible combination with the values of i, j and k, we obtain that $[(1\ 2), \tau]$ is also a 3-cycle or 1. Hence, conjugating with s we can get any 3-cycle we want, and

$$\Sigma_n' = \langle \tau, [\sigma, \rho] \mid \tau, \sigma, \rho \text{ are 3-cycles} \rangle,$$

that is, $\Sigma_n' \leq A_n$. On the other hand, since $|\Sigma_n / A_n| = 2$, the quotient group is abelian so $A_n \leq \Sigma_n'$. Therefore, $\Sigma_n' = A_n$.

Now we consider two cases. If $n = 3$ or $n \geq 5$, A_n is a simple group, or which is the same, it has not normal subgroups except 1 and A_n, so $\gamma_3(\Sigma_n) = 1$ or $\gamma_3(\Sigma_n) = A_n$. Nevertheless, $\gamma_3(\Sigma_n) = 1$ implies $\Sigma_n' = A_n \leq Z(\Sigma_n)$, which is absurd since Σ_n has trivial center for $n \geq 3$, whence $\gamma_i(\Sigma_n) = A_n$ for every $i \geq 3$.

If $n = 4$, it is known that A_4 has exactly one proper non-trivial normal subgroup:

$$V = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

However, $(1\ 2\ 3) \in A_4$ and $[(1\ 2\ 3), (1\ 2)] \in \gamma_3(\Sigma_4)$, but

$$[(1\ 2\ 3), (1\ 2)] = (1\ 2\ 3) \notin V,$$

so by the same argument used in the previous case, $\gamma_3(\Sigma_4) = A_4$, and then $\gamma_i(\Sigma_4) = A_4$ for all $i \geq 3$.

This proves that Σ_n is not a nilpotent group for $n \geq 3$. To calculate the upper central series it is enough to notice that $Z(\Sigma_n) = 1$, so $Z_i(\Sigma_n) = 1$ for every $n \geq 3$.

ii) Let us prove by induction on i that $\gamma_i(D_{2n}) = \langle a^{2^{i-1}} \rangle$.

For $i = 2$, as we have done in i), $D_{2n}' = \langle [a,b]^g \mid g \in D_{2n} \rangle$, but

$$[a,b] = a^{-1}b^{-1}ab = a^{-1}a^b = a^{-1}a^{-1} = a^{-2},$$

so $D_{2n}' = \langle (a^{-2})^g \mid g \in D_{2n} \rangle$. Besides, since $\left(a^{-2}\right)^b = a^2$, the subgroup $\langle a^{-2} \rangle$ is normal in D_{2n}, so $D_{2n}' = \langle a^{-2} \rangle = \langle a^2 \rangle$. For a general i, by Theorem 1.13, since $\langle a^{2^{i-1}} \rangle$ is also normal in D_{2n},

$$\gamma_i(D_{2n}) = [\gamma_{i-1}(D_{2n}), D_{2n}] = [\langle a^{2^{i-2}} \rangle, \langle a, b \rangle] = \langle [a^{2^{i-2}}, b]^g \mid g \in D_{2n} \rangle = \langle a^{2^{i-1}} \rangle,$$

and we are done.

For the upper central series, first we compute the center of D_{2n}. Since $D_{2n} = \langle a \rangle \ltimes \langle b \rangle$, a general element of D_{2n} can be written as $a^i b^j$ with $i \in \{0, 1, \ldots, n-1\}$, $j \in \{0, 1\}$. Thus, $a^i b^j a = a a^i b^j$ if and only if $a^{b^j} = a$, that is, if $j = 0$, and $a^i b^j b = b a^i b^j$ if and only if $(a^b)^i = a^i$, that is, if $a^i = a^{-i}$. Then, we consider two cases. If n is odd, $Z(D_{2n}) = 1$, and then, $Z_i(D_{2n}) = 1$ for all $i \geq 1$. If n is even, $Z(D_{2n}) = \langle a^{n/2} \rangle$.

Now, by definition, $Z_2(D_{2n})/Z(D_{2n}) = Z(D_{2n}/Z(D_{2n}))$, and we observe that

$$\frac{D_{2n}}{Z(D_{2n})} \cong D_{2(n/2)}.$$

This isomorphism is easy to prove considering the isomorphism

$$\begin{array}{rccc} \varphi : & \overline{D_{2n}} & \longrightarrow & D_{2(n/2)} \\ & \overline{a} & \longmapsto & a' \\ & \overline{b} & \longmapsto & b', \end{array}$$

being $D_{2(n/2)} = \langle a', b' \mid (a')^{n/2} = (b')^2 = 1, (a')^{b'} = (a')^{-1} \rangle$. Again, we consider two cases. If $n/2$ is odd, $Z(D_{2(n/2)}) = 1$, and then $Z_2(D_{2n}) = Z(D_{2n})$. If $n/2$ is even, $Z(\overline{D_{2n}}) = \langle \overline{a}^{n/4} \rangle$, whence $Z_2(D_{2n}) = \langle a^{n/4}, a^{n/2} \rangle = \langle a^{n/4} \rangle$.

In general, if $n = 2^r m$ with $m \nmid 2$, then $Z_i(D_{2n}) = \langle a^{n/2^i} \rangle$ for $i = 1, \dots, r$, and $Z_i(D_{2n}) = Z_r(D_{2n})$ for $i \geq r$.

We have proved that the dihedral group D_{2n} is nilpotent if and only if $2n$ is a power of 2, that is, if it is of the form D_{2^n} with $n \geq 3$. In this case, its nilpotency class will be $n-1$.

iii) The lower central series of D_∞ is calculated in the same way as the one of D_{2n}, while the upper central series is trivial since $Z(D_\infty) = 1$. Therefore, D_∞ is not nilpotent. □

Exercise 4. Let n be a natural number such that $n \geq 3$, and let us consider the subgroups $H_i = \langle (i\ i+1) \rangle$ of Σ_n for $1 \leq i \leq n-1$. Prove that

$$\langle [h_1, \dots, h_{n-1}] \mid h_i \in H_i \rangle = \langle (1\ n-1\ n) \rangle$$

while $[H_1, \dots, H_{n-1}] = A_n$.

Solution. We want to calculate $\langle [h_1, \dots, h_{n-1}] \mid h_i \in H_i \rangle$. We may assume that $h_i \neq 1$ for all $i = 1, \dots, n-1$ because if $h_i = 1$ for some i, then the whole commutator would be trivial and we could remove it from the subset of the generators. Thus, $h_i = (i\ i+1)$ for all $i = 1, \dots, n-1$, and let us prove by induction on n that $[h_1, \dots, h_{n-1}] = (1\ n-1\ n)$. For $n = 3$ it is immediate. Indeed,

$$[(1\ 2), (2\ 3)] = (2\ 1)(3\ 2)(1\ 2)(2\ 3) = (1\ 2\ 3).$$

We assume that the result is true for $n-1$ and let us prove that it also holds for n. We know that $[h_1, \dots, h_{n-1}] = [[h_1, \dots, h_{n-2}], h_{n-1}]$, and by hypothesis of induction we have $[h_1, \dots, h_{n-2}] = (1\ n-2\ n-1)$, so

$$\begin{aligned} [h_1, \dots, h_{n-1}] &= [[h_1, \dots, h_{n-2}], h_{n-1}] \\ &= [(1\ n-2\ n-1), (n-1\ n)] \\ &= (1\ n-1\ n-2)(n\ n-1)(1\ n-2\ n-1)(n-1\ n) \\ &= (1\ n-1\ n) \end{aligned}$$

and the result follows.

Now we want to check that $[H_1, \dots, H_{n-1}] = A_n$. We will prove it also by induction on n. For $n = 3$, we have to see that $[H_1, H_2] = A_3$. Since $[(1\ 2), (2\ 3)] = (1\ 2\ 3)$, it follows that $(1\ 2\ 3) \in [H_1, H_2]$, so $A_3 \leq [H_1, H_2]$. Besides, by Exercise 3, $[H_1, H_2] \leq [\Sigma_3, \Sigma_3] = A_3$, so $[H_1, H_2] = A_3$.

For a general n, we have by hypothesis of induction $[H_1, \dots, H_{n-1}, H_n] = [A_n, H_n]$. Again, we have $[A_n, H_n] \leq [\Sigma_{n+1}, \Sigma_{n+1}] = A_{n+1}$, so if we prove that a general 3-cycle $(i\ j\ k)$ of Σ_{n+1} is in $[H_1, \dots, H_n]$ we will be done. We take the element $[(i\ j\ n), (n\ n+1)] = (i\ n\ n+1) \in [A_n, H_n]$, and then,

$$(i\ n\ n+1)(j\ n\ n+1)^{-1} = (i\ j\ n+1) \in [A_n, H_n],$$

with $1 \leq i, j \leq n$, $i \neq j$. In other words, every 3-cycle which contains $n+1$ is in $[A_n, H_n]$. Then,

$$(i\ j\ n+1)(k\ i\ n+1) = (i\ j\ k) \in [A_n, H_n],$$

with $1 \leq i, j, k \leq n$ and different i, j and k. Thus, we have proved that every 3-cycle is in $[A_n, H_n]$, and then, $[A_n, H_n] = A_{n+1}$, so the proof is complete.

□

Exercise 5. Let G be a finitely generated nilpotent group such that $\exp G/G' < \infty$.

i) Prove that G is finite.

ii) Give an example showing that the previous result is not generally true if G is not nilpotent.

Solution. i) Since $\exp G/G' < \infty$, we have by Theorem 1.29 that $\exp \gamma_i(G)/\gamma_{i+1}(G) < \infty$ for all $i \geq 1$, and since G is finitely generated, G/G' is also finitely generated, whence by Theorem 1.26, $\gamma_i(G)/\gamma_{i+1}(G)$ is finitely generated. By Remark 1.28, these factor groups are all abelian, so it follows that $\gamma_i(G)/\gamma_{i+1}(G)$ is finite for all $i \geq 1$. Now, if the nilpotency class of G is c, then $\gamma_i(G) = 1$ for $i \geq c+1$, or which is the same, there is a finite number of non-trivial central factors. Consequently, G is finite.

ii) As we have seen in Exercise 3, $D_\infty = \langle a, b \mid b^2 = 1, a^b = a^{-1} \rangle$ is not nilpotent, and $\exp D_\infty/D'_\infty = \exp\langle a, b\rangle/\langle a^2\rangle = 2$. However, this group is not finite since neither is the order of a. □

Exercise 6. Let G, H and N be groups such that $G = H \times N$.

i) Prove that $\gamma_i(G) = \gamma_i(H) \times \gamma_i(N)$ and that $Z_i(G) = Z_i(H) \times Z_i(N)$ for every $i \geq 0$.

ii) Deduce that G is nilpotent of class c if and only if H and N are nilpotent and the maximum of the nilpotency classes of H and N is c.

Solution. i) Let us start with the lower central series. It suffices to see that

$$\begin{aligned}
\gamma_i(G) &= \langle [g_1, \ldots, g_i] \mid g_1, \ldots, g_i \in G \rangle \\
&= \langle [(h_1, n_1), \ldots, (h_i, n_i)] \mid (h_1, n_1), \ldots, (h_i, n_i) \in H \times N \rangle \\
&= \langle ([h_1, \ldots, h_i], [n_1, \ldots, n_i]) \mid h_1, \ldots, h_i \in H, n_1, \ldots, n_i \in N \rangle \\
&= \langle (h, n) \mid h \in \gamma_i(H), n \in \gamma_i(N) \rangle \\
&= \gamma_i(H) \times \gamma_i(N).
\end{aligned}$$

For the upper central series, by Exercise 2, we have

$$\begin{aligned}
Z_i(G) &= \{g \in G \mid [g, x_1, \ldots, x_i] = 1, \forall x_1, \ldots, x_i \in G\} \\
&= \{(h, n) \in H \times N \mid [(h, n), (h_1, n_1), \ldots, (h_i, n_i)] = 1, \\
&\qquad\qquad \forall h_1, \ldots, h_i \in H, \forall n_1, \ldots, n_i \in N\} \\
&= \{(h, n) \in H \times N \mid ([h, h_1, \ldots, h_i], [n, n_1, \ldots, n_i]) = (1, 1), \\
&\qquad\qquad \forall h_1, \ldots, h_i \in H, \forall n_1, \ldots, n_i \in N\} \\
&= \{(h, n) \in H \times N \mid h \in Z_i(H), n \in Z_i(N)\} \\
&= Z_i(H) \times Z_i(N).
\end{aligned}$$

ii) If G is nilpotent of class c, then $\gamma_c(G) \neq 1$, so by i), we have $\gamma_c(H) \times \gamma_c(N) \neq 1$, that is, one of them is not trivial. Furthermore, $\gamma_{c+1}(G) = 1$, so both $\gamma_{c+1}(H)$ and $\gamma_{c+1}(N)$ are trivial. Then, the maximum of the nilpotency classes of H and N is c and, in particular, they are nilpotent.

The other implication is proved in the same way. □

Exercise 7. Prove that the following finite p-groups are of maximal class.

i) $D_{2^n} = \langle a, b \mid a^{2^{n-1}} = b^2 = 1, a^b = a^{-1} \rangle$, for $n \geq 3$.

ii) $SD_{2^n} = \langle a, b \mid a^{2^{n-1}} = b^2 = 1, a^b = a^{-1+2^{n-2}} \rangle$, for $n \geq 4$.

iii) $Q_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, a^b = a^{-1} \rangle$, for $n \geq 3$.

Solution. i) It is immediate by Exercise 3.

ii) We will calculate the lower central series. The procedure will be the same as the one used in Exercise 3. Thus, we compute the commutator $[a, b] = a^{-1}a^b = a^{-2+2^{n-1}}$, and in addition, $\langle a^{-2+2^{n-1}} \rangle$ is normal in SD_{2^n} because of the same result as in the previous cases, so by Theorem 1.23, we have

$$SD'_{2^n} = \langle [a, b]^g \mid g \in SD_{2^n} \rangle = \langle a^{-2+2^{n-2}} \rangle.$$

Again using an argument of induction, if we suppose that $\gamma_{i-1}(SD_{2^n}) = \langle a^{\left(-2+2^{n-2}\right)^{i-2}} \rangle$, we get

$$\begin{aligned} \gamma_i(SD_{2^n}) &= [\gamma_{i-1}(SD_{2^n}), SD_{2^n}] \\ &= \left[\left\langle a^{\left(-2+2^{n-2}\right)^{i-2}} \right\rangle, \langle a, b \rangle \right] \\ &= \left\langle \left[a^{\left(-2+2^{n-2}\right)^{i-2}}, b \right]^g \mid g \in SD_{2^n} \right\rangle, \end{aligned}$$

and making computations, we get

$$\left[a^{\left(-2+2^{n-2}\right)^{i-2}}, b \right] = a^{\left(-2+2^{n-2}\right)^{i-1}}.$$

Since $\left\langle a^{\left(-2+2^{n-2}\right)^{i-1}} \right\rangle$ is normal in SD_{2^n}, we conclude that $\gamma_i(SD_{2^n}) = \left\langle a^{\left(-2+2^{n-2}\right)^{i-1}} \right\rangle$.

But, when is $a^{\left(-2+2^{n-2}\right)^{i-1}}$ equal to 1? This will happen when

$$\left(-2 + 2^{n-2}\right)^{i-1} \equiv 0 \pmod{2^{n-1}},$$

that is, when $\left(2(-1 + 2^{n-3})\right)^{i-1} \equiv 0 \pmod{2^{n-1}}$, and since $-1 + 2^{n-3}$ is not even for $n \geq 4$, the congruence holds if and only if $i \geq n$. Therefore, SD_{2^n} is nilpotent of class $n - 1$.

iii) Again, we prove that the lower central series is $\gamma_i(Q_{2^n}) = \langle a^{2^{i-1}} \rangle$ by induction on i. For $i = 2$, since $[a, b] = a^{-1}a^b = a^{-2}$, and $\langle a^{-2} \rangle = \langle a^2 \rangle$ is normal in Q_{2^n}, we have, as in the previous cases, $Q'_{2^n} = \langle a^2 \rangle$. For a general i, since

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

the result follows. Thus, the nilpotency class of Q_{2^n} is $n - 1$ and it is a 2-group of maximal class. □

Exercise 8. In this problem we will construct, for any prime p and any $n \geq 2$, a p-group of maximal class of order p^n. We take a homocyclic group $A = \langle a_1 \rangle \times \cdots \times \langle a_{p-1} \rangle \cong C_{p^r} \times \cdots \times C_{p^r}$, where $r \geq 1$ is arbitrary. (A group is said to be *homocyclic* if it is the direct product of cyclic groups of equal order.)

i) Prove that the assignments

$$a_1 \to a_1a_2,\ a_2 \to a_2a_3,\ \dots\ ,\ a_{p-2} \to a_{p-2}a_{p-1},\ a_{p-1} \to a_{p-1}\left(a_1^p a_2^{\binom{p}{2}} \dots a_{p-1}^{\binom{p}{p-1}}\right)^{-1}$$

define an automorphism σ of A.

Let us construct now the semidirect product $G = \langle\sigma\rangle \ltimes A$. We define the elements a_i for $i \geq p$ via the relation $a_{i+1} = [a_i, \sigma] = a_i^{-1}a_i^{\sigma}$. Observe that the equality $a_{i+1} = [a_i, \sigma]$ is also true for $i \geq 1$.

ii) Prove by induction on $i \geq p$ that

$$a_i = \left(a_{i-p+1}^p a_{i-p+2}^{\binom{p}{2}} \dots a_{i-1}^{\binom{p}{p-1}}\right)^{-1}.$$

iii) If $i > k(p-1)$, prove that $a_i \in A^{p^k}$. Deduce that

$$a_{k(p-1)} \equiv {a_{p-1}}^{(-p)^k} \pmod{A^{p^k}}.$$

iv) By *iii)*, $a_{r(p-1)} \neq 1$. Deduce that $\gamma_{r(p-1)}(G) \neq 1$.

v) Prove that $[a_i, \sigma^p] = 1$ for all i. Therefore, σ is an automorphism of order p and $|G| = p^{r(p-1)+1}$. Conclude that G is a p-group of maximal class.

vi) Deduce that there exist p-groups of maximal class for any order p^n.

Solution. i) First, we prove that σ is a homomorphism. We notice that

$$A = \langle a_1, \dots, a_{p-1} \mid a_1^{p^r} = \dots = a_{p-1}^{p^r} = 1 \text{ and } [a_i, a_j] = 1 \text{ for all } 1 \leq i, j \leq p-1\rangle,$$

and we only have to check that the images of the generators of A satisfy the relations of the presentation of A. However, this is trivial since the images of the generators of A are in A, which is abelian, and $\exp A = p^r$.

Let us prove that σ is surjective. It is known that the images of the generators of A are generators of $\sigma(A)$, that is,

$$\sigma(A) = \left\langle a_1a_2, \dots, a_{p-2}a_{p-1}, a_{p-1}\left(a_1^p a_2^{\binom{p}{2}} \dots a_{p-1}^{\binom{p}{p-1}}\right)^{-1}\right\rangle.$$

The group A is abelian, so by Theorem 2.25, $\Phi(A) = A^p$. Then, since $\left(a_1^p a_2^{\binom{p}{2}} \dots a_{p-1}^{\binom{p}{p-1}}\right)^{-1} \in A^p$ and by Theorem 2.12,

$$\sigma(A) = \langle a_1a_2, \dots, a_{p-2}a_{p-1}, a_{p-1}\rangle = \langle a_1a_2, \dots, a_{p-2}, a_{p-1}\rangle = \dots = \langle a_1, \dots, a_{p-2}, a_{p-1}\rangle,$$

so it follows that σ is surjective. In addition, A is finite, so σ is bijective, as required.

ii) For $i = p$ the result is clear. For the case of $i+1$, by the way in which we have defined a_{i+1}, we have $a_{i+1} = a_i^{-1}a_i^\sigma$, and by hypothesis of induction,

$$a_{i+1} = a_i^{-1}a_i^\sigma = a_i^{-1}\left(\left(a_{i-p+1}^p a_{i-p+2}^{\binom{p}{2}} \dots a_{i-1}^{\binom{p}{p-1}}\right)^{-1}\right)^\sigma.$$

Now, since σ is a homomorphism and $a_i^\sigma = a_i a_{i+1}$,

$$\begin{aligned} a_{i+1} &= a_i^{-1}\left(\left(a_{i-p+1}^p a_{i-p+2}^{\binom{p}{2}} \dots a_{i-1}^{\binom{p}{p-1}}\right)^{-1}\right)^\sigma \\ &= a_i^{-1}\left(\left(a_{i-p+1}^\sigma\right)^p \left(a_{i-p+2}^\sigma\right)^{\binom{p}{2}} \dots \left(a_{i-1}^\sigma\right)^{\binom{p}{p-1}}\right)^{-1} \\ &= a_i^{-1}\left(\left(a_{i-p+1}a_{i-p+2}\right)^p \left(a_{i-p+2}a_{i-p+3}\right)^{\binom{p}{2}} \dots \left(a_{i-1}a_i\right)^{\binom{p}{p-1}}\right)^{-1}. \end{aligned}$$

Finally, using that A is abelian and the hypothesis of induction,

$$\begin{aligned} a_{i+1} &= a_i^{-1}\left(\left(a_{i-p+1}a_{i-p+2}\right)^p \left(a_{i-p+2}a_{i-p+3}\right)^{\binom{p}{2}} \dots \left(a_{i-1}a_i\right)^{\binom{p}{p-1}}\right)^{-1} \\ &= a_i^{-1}\left(a_{i-p+1}^p a_{i-p+2}^{\binom{p}{2}} \dots a_{i-1}^{\binom{p}{p-1}}\right)^{-1}\left(a_{i-p+2}^p a_{i-p+3}^{\binom{p}{2}} \dots a_i^{\binom{p}{p-1}}\right)^{-1} \\ &= a_i^{-1}a_i\left(a_{i-p+2}^p a_{i-p+3}^{\binom{p}{2}} \dots a_i^{\binom{p}{p-1}}\right)^{-1} \\ &= \left(a_{i-p+2}^p a_{i-p+3}^{\binom{p}{2}} \dots a_i^{\binom{p}{p-1}}\right)^{-1}. \end{aligned}$$

iii) We will prove the result by induction on k. For $k = 1$, by *ii)* we have

$$a_i = \left(a_{i-p+1}^p a_{i-p+2}^{\binom{p}{2}} \dots a_{i-1}^{\binom{p}{p-1}}\right)^{-1},$$

and of course, $a_i \in A^p$. Let us prove the result for a general k. Again, by *ii)*,

$$a_i = \left(a_{i-p+1}^p a_{i-p+2}^{\binom{p}{2}} \dots a_{i-1}^{\binom{p}{p-1}}\right)^{-1},$$

and we observe that $i > k(p-1)$ implies $i - p + 1 > k(p-1) - p + 1 = (k-1)(p-1)$. So, by hypothesis of induction, $a_{i-p+j} \in A^{p^{k-1}}$ for every $j = 1, \dots, p-1$. Since A is abelian, it follows that $a_{i-p+j}^{\binom{p}{j}} \in A^{p^k}$, and then, $a_i \in A^{p^k}$, as required.

On the other hand, we have to prove that

$$a_{k(p-1)} \equiv {a_{p-1}}^{(-p)^{k-1}} \pmod{A^{p^k}}.$$

For $k=1$, the result trivially follows, so let us prove the result for a general k. We observe that

$$a_{k(p-1)} = \left(a^p_{(k-1)(p-1)} a^{\binom{p}{2}}_{(k-1)(p-1)+1} \dots a^{\binom{p}{p-1}}_{k(p-1)-1} \right)^{-1},$$

and by hypothesis of induction,

$$a_{(k-1)(p-1)} \equiv a_{p-1}^{(-p)^{k-2}} \pmod{A^{p^{k-1}}}.$$

Now, A is abelian, so

$$a^p_{(k-1)(p-1)} \equiv a_{p-1}^{(-p)^{k-1}} \pmod{A^{p^k}},$$

and since $a^{\binom{p}{j+1}}_{(k-1)(p-1)+j} \in A^{p^k}$ with $j=1,\dots,p-2$, we are done.

iv) By the previous part, since $A^{p^r}=1$, we have $a_{r(p-1)} = a_{p-1}^{(-p)^{r-1}}$, and since the order of a_{p-1} is p^r, then $a_{p-1}^{(-p)^{r-1}} \neq 1$. Now, we observe that $[a_1, \sigma, \overset{r(p-1)-1}{\dots}, \sigma] = [a_2, \sigma, \overset{r(p-1)-2}{\dots}, \sigma] = \dots = a_{r(p-1)} \neq 1$. Obviously $[a_1, \sigma, \overset{r(p-1)-1}{\dots}, \sigma] \in \gamma_{r(p-1)}(G)$, so that $\gamma_{r(p-1)}(G) \neq 1$.

v) We note that since $G/A = \langle \overline{\sigma} \rangle$ is abelian, $G' \leq A$, and since A is abelian, so is G'. Thus, by Exercise 1, we have

$$[a_i, \sigma^p] = [a_i, \sigma]^p [a_i, \sigma, \sigma]^{\binom{p}{2}} \dots [a_i, \sigma, \overset{p}{\dots}, \sigma]^{\binom{p}{p}} = a^p_{i+1} a^{\binom{p}{2}}_{i+2} \dots a^{\binom{p}{p}}_{i+p},$$

and by *ii*),

$$[a_i, \sigma^p] = a^p_{i+1} a^{\binom{p}{2}}_{i+2} \dots a^{\binom{p}{p}}_{i+p} = a^{-1}_{i+p} a_{i+p} = 1.$$

Hence, $[a_i, \sigma^p] = a_i^{-1} a_i^{\sigma^p} = 1$ for every $i \geq 1$, or which is the same, $a_i^{\sigma^p} = a_i$ for every $i \geq 1$. Then, $o(\sigma) \mid p$, that is, $o(\sigma) = p$ since $\sigma \neq 1$, and then, $|G| = p^{r(p-1)} p = p^{r(p-1)+1}$.

Now, of course, $\gamma_{r(p-1)+1}(G) = 1$, and by *iv*), we deduce that the nilpotency class of G is $r(p-1)$, in other words, G is a p-group of maximal class.

vi) Finally, we consider the group $G/\gamma_i(G)$ with $2 \leq i \leq r(p-1)+1$, and obviously it is of maximal class since $\gamma_j(\overline{G}) = \overline{\gamma_j(G)}$. Moreover, the order of $\overline{G}$ is p^{i+1}, and since r is arbitrary, i can be any number greater than 2. Thus, we have finished. □

Exercise 9. Prove that the p-group $P_n = \langle a, b \mid a^{p^n} = b^{p^{n-1}} = 1, a^b = a^{1+p} \rangle$ is nilpotent of class n and also that P_n is powerful.

Solution. First of all, we note that $P_n = \langle a \rangle \rtimes \langle b \rangle$, via the automorphism $\alpha : \langle a \rangle \to \langle a \rangle$ such that $\alpha(a) = a^b = a^{1+p}$. Thus, $o(a) = p^n$, $o(b) = p^{n-1}$ and $|P_n| = p^{2n-1}$.

We will prove by induction that $\gamma_i(P_n) = \langle a^{p^{i-1}} \rangle$. For $i=2$, we use again Theorem 1.23 and then,

$$P_n' = \langle [a,b]^g \mid g \in P_n \rangle.$$

We calculate the value of the commutator:

$$[a,b] = a^{-1} a^b = a^{-1} a^{p+1} = a^p.$$

Furthermore, the subgroup $\langle a^p \rangle$ is normal in P_n since $\langle a^p \rangle$ is characteristic in $\langle a \rangle$ and $\langle a \rangle$ is normal in P_n, so $P_n' = \langle a^p \rangle$. For a general i, it suffices to calculate

$$\gamma_i(P_n) = [\gamma_{i-1}(P_n), P_n] = [\langle a^{p^{i-2}} \rangle, \langle a, b \rangle].$$

So, by Theorem 1.13, since the subgroup $\langle a^{p^{i-1}} \rangle$ is normal in P_n,

$$\gamma_i(P_n) = \langle [a^{p^{i-2}}, b]^g \mid g \in P_n \rangle = \langle a^{p^{i-1}} \rangle,$$

and we are done. We have prove that the nilpotency class of P_n is exactly n.

Furthermore, since $P_n' = \langle a^p \rangle \leq (P_n)^p$, it follows that P_n is powerful. □

Exercise 10. Let G be a finite p-group. Then:

i) If N is a powerfully embedded subgroup of G and $N = \langle Y \rangle^G$, prove that $N = \langle Y \rangle$.

ii) If $G = \langle X \rangle$ is powerful, what system of generators do we get for the terms of the lower central series of G by applying the previous result?

Solution. i) The result will be proved for $p > 2$ since the proof for the case $p = 2$ is very similar. We observe that

$$N = \langle Y \rangle^G = \langle y^g \mid y \in Y, g \in G \rangle = \langle y[y, g] \mid y \in Y, g \in G \rangle \leq \langle Y \rangle [N, G],$$

and since N is powerfully embedded in G, we have $N \leq \langle Y \rangle [N, G] \leq \langle Y \rangle N^p$. The other inclusion is trivial, so $N = \langle Y \rangle N^p$.

Now, since N is powerfully embedded, it is, in particular, powerful, so by Theorem 2.25 we have $\Phi(N) = N^p$, and by Theorem 2.13, we conclude that $N = \langle Y \rangle$.

ii) By Theorem 1.23, we have

$$\gamma_i(G) = \langle [x_1, \ldots, x_i] \mid x_1, \ldots, x_i \in X \rangle^G,$$

and since every $\gamma_i(G)$ is powerfully embedded in G, by i) we deduce that

$$\gamma_i(G) = \langle [x_1, \ldots, x_i] \mid x_1, \ldots, x_i \in X \rangle.$$

□

Exercise 11. Let G be a finite p-group. We say that G is *metacyclic* if there exists $N \trianglelefteq G$ such that both N and G/N are cyclic. Observe that a metacyclic group can be generated by two elements.

i) If G is metacyclic and $p > 2$, prove that G is powerful.

ii) Give an example showing that the previous result is not generally true for $p = 2$.

iii) If G is powerful and $d(G) = 2$, prove that G is metacyclic, without restrictions on the prime p.

Solution. i) Since $p > 2$, we have to check that $[G, G] \leq G^p$. Since G is metacylclic, there exist N such that $N = \langle a \rangle$ and $G/N = \langle b \rangle$ for some $a, b \in G$. Then, by Lemma 3.10, $[G, G] = [G, N]$, and since G is nilpotent and N is normal in G, we have $[G, N] < N$. Thus, $[G, N] = \langle a^{p^j} \rangle$ for some $1 \leq j < o(a)$, and obviously $a^{p^j} \in G^p$. Therefore, $[G, G] = [G, N] < N \leq G^p$, and we are done.

ii) For $p = 2$ we consider the group $D_{2^n} = \langle a, b \mid a^{2^{n-1}} = b^2 = 1, a^b = a^{-1} \rangle$ for some $n \geq 3$. It is easy to see that it is metacyclic since $\langle a \rangle$ is normal in D_{2^n}, and $D_{2^n}/\langle a \rangle = \langle \overline{b} \rangle$. However, it is not powerful. Indeed, by Exercise 3, $[D_{2^n}, D_{2^n}] = \langle a^2 \rangle$, and obviously this subgroup is not contained in $D_{2^n}^4$.

iii) Let $G = \langle a, b \rangle$. By Exercise 10, $G' = \langle [a, b] \rangle$, so G' is cyclic. We write $G' = \langle c^{p^k} \rangle$ with k as large as possible. Then, $c \notin G^p$. Indeed, otherwise, since G is powerful, by Theorem 3.13, $c = g^p$ for some $g \in G$, and so, $G' = \langle g^{p^{k+1}} \rangle$, which is absurd because of the way in which we have taken k.

Since G is powerful, by Theorem 2.25 $\Phi(G) = G^p$, and we consider the factor group $\overline{G} = G/G^p$, which is a vector-space of dimension 2. Thus, $\overline{c} \neq \overline{1}$, and we can take a basis $\{\overline{c}, \overline{d}\}$ of $\overline{G}$. Therefore, $G = \langle c, d \rangle$, and we notice that

$$[G, \langle c \rangle] \leq [G, G] = \langle c^{p^k} \rangle \leq \langle c \rangle,$$

that is, $\langle c \rangle$ is normal in G. Since $G/\langle c \rangle = \langle \overline{b} \rangle$, we have finished. □

Bibliography

[1] M. Erickson, Pearls of Discrete Mathematics, CRC Press, 2010.

[2] G. A. Fernández-Alcober, Notes of the PhD Course "Advanced Group Theory", Leioa, 2001.

[3] G. A. Fernández-Alcober, Omega subgroups of powerful p-groups, Israel Journal of Mathematics **162** (2007), 75-79.

[4] G. A. Fernández-Alcober, p-taldeen eta talde abeldarren arteko antzekotasun batzuk, Ekaia **5** (1996), 161-175.

[5] P. Hall, A contribution to the theory of groups of prime-power order, Proc. London Math. Soc. (1934), 29-95.

[6] E. I. Khukhro, p-Automorphisms of Finite p-Groups, Cambridge University Press, 1998.

[7] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, Journal für die reine und angewandte Mathematik **44** (1852), 93–146.

[8] A. Mann, F. Posnick-Fradkin, Subgroups of powerful groups, Israel Journal of Mathematics **138** (2003), 19-28.

[9] M. Suzuki, Group Theory II, Springer, 1986.