Intense automorphisms of finite groups

Stanojkovski, M.

Chapter 10

Obelisks

Let $p > 3$ be a prime number. A *p-obelisk* is a finite p-group G for which the following hold.

1. The group G is not abelian.
2. One has $|G : G_3| = p^3$ and $G_3 = G^p$.

The following proposition will immediately clarify our interest in p-obelisks.

Proposition 318. *Let $p > 3$ be a prime number and let G be a finite p-group of class at least 4. If $\mathrm{int}(G) > 1$, then G is a p-obelisk.*

Proof. Combine Theorems 164 and 189. ∎

Chapter 10 will be entirely devoted to understanding the structure of p-obelisks and that of their subgroups. Some of the results, especially coming from Section 10.4, are rather technical and their relevance will become evident in Chapter 11.

10.1 Some properties

We remind the reader that, if p is a prime number and G is a finite p-group, then $\mathrm{wt}_G(i) = \log_p |G_i : G_{i+1}|$ where $(G_i)_{i\geq 1}$ denotes the lower central series of G.

Lemma 319. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let $(G_i)_{i\geq 1}$ denote the lower central series of G. Then the following hold.*

1. *The class of G is at least 2.*
2. *One has $\mathrm{wt}_G(1) = 2$ and $\mathrm{wt}_G(2) = 1$.*
3. *The group G/G_3 is extraspecial of exponent p.*

Proof. The group G is non-abelian and thus $G_2 \neq G_3$. The index $|G : G_3|$ being equal to p^3, it follows from Lemma 31 that $\mathrm{wt}_G(1) = 2$ and $\mathrm{wt}_G(2) = 1$. We denote now $\overline{G} = G/G_3$ and use the bar notation for the subgroups of $\overline{G}$. Then $\overline{G_2}$ is contained in $\mathrm{Z}(\overline{G})$ and $\overline{G_2} = \mathrm{Z}(\overline{G})$, as a consequence of Lemma 27. The exponent of $\overline{G}$ is p, because G^p is contained in G_3. ∎

Lemma 320. *Let $p > 3$ and let G be a p-obelisk. Then G is regular.*

Proof. This follows directly from Lemma 53. ∎

Proposition 321. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let $(G_i)_{i\geq 1}$ be the lower central series of G and let c denote the class of G. Then the following hold.*

1. *For all $i \in \mathbb{Z}_{\geq 1}$, one has $\mathrm{wt}_G(i)\,\mathrm{wt}_G(i+1) \leq 2$.*
2. *If $\mathrm{wt}_G(i)\,\mathrm{wt}_G(i+1) = 1$, then $i = c - 1$.*
3. *For all positive integers k and l, not both even, one has $[G_k, G_l] = G_{k+l}$.*

Proof. Proposition 321 is a simplified version of Theorem 4.3 from [Bla61], which can also be found in Chapter 3 of [Hup67] as Satz 17.9. ∎

We remark that the term *p-obelisk* does not appear in [Bla61] or [Hup67] and is of our own invention. Moreover, originally Proposition 321(1-2) was phrased in the following way: if G is a p-obelisk, then

$$(\mathrm{wt}_G(i))_{i\geq 1} = (2, 1, 2, 1, \ldots, 2, 1, f, 0, 0, \ldots) \quad \text{where} \quad f \in \{0, 1, 2\}.$$

Lemma 322. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c denote the class of G and let $i \in \{1, \ldots, c-1\}$. Then the following hold.*

1. *The index i is odd if and only if $\mathrm{wt}_G(i) = 2$.*
2. *The index i is even if and only if $\mathrm{wt}_G(i) = 1$.*
3. *If $\mathrm{wt}_G(c) = 2$, then c is odd.*
4. *If c is even, then $\mathrm{wt}_G(c) = 1$.*

Proof. For all $j \in \{1, \ldots, c-1\}$, denote $w_j = \mathrm{wt}_G(j)$. Thanks to Lemma 319, we have $w_1 = 2$ and $w_2 = 1$. As a consequence of Proposition 321, whenever $i < c-1$, the product $w_i w_{i+1}$ is equal to 2 and, for all indices $i, j \in \{1, \ldots, c-1\}$, one has $w_i = w_j$ if and only if i and j have the same parity. It follows from Proposition 321(1) that $\mathrm{wt}_G(c)$ can be 2 only if c is odd. ∎

We recall that, if G is a p-group, then ρ denotes the map $x \mapsto x^p$ on G.

Lemma 323. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then, for all $i, k \in \mathbb{Z}_{>0}$, one has $\rho^k(G_i) = G_{2k+i}$.*

In his original proof of Proposition 321, Blackburn also proves Lemma 323. Blackburn's proof strongly relies on the fact that p-obelisks are regular and it makes use of some technical lemmas that can be found in [Hup67, Ch. III].

Proposition 324. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let $(G_i)_{i\geq 1}$ be the lower central series of G and let c denote its nilpotency class. Then $\mathrm{Z}(G) = G_c$.*

Proof. We work by induction on c. If $c = 2$, then, by Lemma 319(3), the group G is extraspecial so $G_2 = \mathrm{Z}(G)$. Assume now that $c > 2$. The subgroup G_c is central, because G has class c, and, by the induction hypothesis, $\mathrm{Z}(G/G_c) = G_{c-1}/G_c$. It follows that $G_c \subseteq \mathrm{Z}(G) \subseteq G_{c-1}$ and $\mathrm{Z}(G) \neq G_{c-1}$. Moreover, by Proposition 321(1), the width $\mathrm{wt}_G(c-1)$ is either 1 or 2. If $\mathrm{wt}_G(c-1) = 1$, then $\mathrm{Z}(G) = G_c$; we assume thus that $\mathrm{wt}_G(c-1) = 2$. By Lemma 322(1), there exists a positive integer k such that $c - 1 = 2k + 1$ so, from Lemma 323, we get $G_{c-1} = \rho^k(G)$ and $G_c = \rho^k(G_2)$. As a consequence of Proposition 321(1), the subgroup G_c has order p. Let us assume by contradiction that $\mathrm{Z}(G) \neq G_c$, in other words $|G_{c-1} : \mathrm{Z}(G)| = |\mathrm{Z}(G) : G_c| = p$. Let $N = \mathrm{C}_G(G_{c-1})$. The commutator map $G/G_2 \times G_{c-1}/G_c \to G_c$ is bilinear by Lemma 24 and it factors as a surjective non-degenerate map $G/N \times G_{c-1}/\mathrm{Z}(G) \to G_c$. It follows from Lemma 2 that G/N is cyclic of order p so, by Lemma 28, one has $G_2 = [N, G]$. Lemma 54 yields

$$\rho^k([N, G]) = [N, \rho^k(G)] = [N, G_{c-1}] = \{1\}$$

and so $G_c = \rho^k(G_2) = \{1\}$. Contradiction. ∎

Lemma 325. *Let G be a group and let N be a normal subgroup of G. Let moreover H and K be subgroups of G such that $K \subseteq H$. Then one has $(H \cap N)K = (KN) \cap H$.*

Proof. Easy exercise. ∎

Lemma 326. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then each non-abelian quotient of G is a p-obelisk.*

Proof. Let N be a normal subgroup of G such that G/N is not abelian. We claim that N is contained in G_3. Denote first $H = G/N$. Then we have $|H : H_2| \leq |G : G_2|$. Moreover, H being non-abelian, Lemma 31 yields $|H : H_2| \geq p^2$, and therefore, from Lemma 319(2), it follows that $N \subseteq G_2$. If $N \cap G_3 = N$, then N is contained in G_3 and we are done. Assume by contradiction that $N \cap G_3 \neq N$. As a consequence of Lemma 319(2), the subgroup N does not contain G_3. Let now

M be a normal subgroup of G such that $N \cap G_3 \subseteq M \subseteq G_3$ and $|G_3 : M| = p$, as given by Lemma 35. Then $\overline{G} = G/M$ has class 3 and $\overline{N} \neq \{1\}$. But, by Lemma 140, the centre of $\overline{G}$ is equal to $\overline{G_3}$ so, $\overline{G_3}$ having order p, Lemma 29 yields $\overline{G_3} \subseteq \overline{N}$. In particular, G_3 is contained in MN. Thanks to Lemma 325, we get that $G_3 = (G_3 \cap N)M = M$, which gives a contradiction. It follows that $N \subseteq G_3$, as claimed, and thus we have $|H : H_3| = |G : G_3|$. It is moreover clear that $H^p = H_3$, and so we have proven that H is a p-obelisk. ∎

Lemma 327. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then the following hold.*

1. *If H is a quotient of G of class i, then $\mathrm{Z}(H) = H_i$.*
2. *Let N be a subgroup of G. Then N is normal in G if and only if there exists $i \in \mathbb{Z}_{>0}$ such that $G_{i+1} \subseteq N \subseteq G_i$.*

Proof. (1) Let H be a quotient of G and let i denote the class of H. Let moreover c denote the class of G and note that $i \leq c$. If $i = 0$ or $i = 1$, the group H is abelian and $\mathrm{Z}(H) = H$. Assume now that $i > 1$. Then H is a non-abelian quotient of a p-obelisk so, by Lemma 326, it is a p-obelisk itself. To conclude, apply Proposition 324. For the proof of (2), we combine (1) with Lemma 30. ∎

10.2 Power maps and commutators

Throughout Section 10.2 we will faithfully follow the notation from the List of Symbols. In particular, if p is a prime number and G is a finite p-group, then ρ denotes the map $G \to G$ that is defined by $x \mapsto x^p$. We remind the reader that ρ is in general not a homomorphism.

Lemma 328. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then the following hold.*

1. *For all $i, k \in \mathbb{Z}_{>0}$ the map $\rho^k : G_i \to G_i$ induces a surjective homomorphism $\rho_i^k : G_i/G_{i+1} \to G_{2k+i}/G_{2k+i+1}$.*
2. *For all $h, k \in \mathbb{Z}_{>0}$ not both even, the commutator map induces a bilinear map $\gamma_{h,k} : G_h/G_{h+1} \times G_k/G_{k+1} \to G_{h+k}/G_{h+k+1}$ whose image generates G_{h+k}/G_{h+k+1}.*

Proof. (1) Let i and k be positive integers and, without loss of generality, assume that $G_{2k+i+1} = \{1\}$. We work by induction on k and we start by taking $k = 1$. As a consequence of Lemma 20, the group $[G_i, G_i]$ is contained in G_{2i} so, from Lemma 323, it follows that $[G_i, G_i]^p$ is contained in G_{2i+2}. The index i being positive, G_{2i+2} is contained in $G_{i+3} = \{1\}$. Now, the prime p is larger than 3 so G_{ip} is also

contained in $G_{i+3} = \{1\}$. It follows from Lemma 20, that $(G_i)_p$ is contained in G_{ip}, and so, thanks to Corollary 48, the map $\rho : G_i \to G_i$ is a homomorphism. The function ρ factors as a surjective homomorphism $\rho_i^1 : G_i/G_{i+1} \to G_{i+2}$, thanks to Lemma 323. This finishes the proof for $k = 1$. Assume now that $k > 1$ and define

$$\rho_i^k = \rho_{2k+i-1}^1 \circ \rho_{2k+i-3}^1 \circ \ldots \circ \rho_{i+2}^1 \circ \rho_i^1.$$

As a consequence of the base case, the map ρ_i^k is a surjective homomorphism $\rho_i^k : G_i/G_{i+1} \to G_{2k+i}/G_{2k+i+1}$ and, by its definition, it is induced by ρ^k. This proves (1). To prove (2) combine Proposition 321(3) with Lemma 23. ∎

Corollary 329. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c be the class of G. Let moreover i and j be integers of the same parity such that $1 \leq i \leq j \leq c$ and one of the following holds.*

1. *The number j is even.*
2. *One has $\mathrm{wt}_G(j) = 2$.*

Define $m = \frac{j-i}{2}$. Then the map $\rho^m : G_i \to G_i$ induces an isomorphism of groups $\rho_i^m : G_i/G_{i+1} \to G_j/G_{j+1}$.

Proof. By Lemma 328(1), the map $\rho^m : G_i \to G_i$ induces a surjective homomorphism $\rho_i^m : G_i/G_{i+1} \to G_j/G_{j+1}$. Now, i and j having the same parity, it follows from Lemma 322 that $\mathrm{wt}_G(i) = \mathrm{wt}_G(j)$ and ρ_i^m is a bijection. ∎

Lemma 330. *Let $p > 3$ be a prime number and let G be a p-obelisk. Denote by c the class of G. Let moreover h and k be positive integers, not both even, such that $h + k \leq c$. Assume additionally that, if $h + k$ is odd, then $\mathrm{wt}_G(h + k) = 2$. Then the map $\gamma_{h,k}$ from Lemma 328 is non-degenerate.*

Proof. Without loss of generality, assume that $c = h + k$ and so $G_{h+k+1} = \{1\}$. We prove non-degeneracy of $\gamma_{h,k}$ by looking at the parity of $h + k$. Assume first that $h + k$ is odd and, without loss of generality, h is odd and k is even. From Lemma 322, it follows that $\mathrm{wt}_G(h) = 2$ and $\mathrm{wt}_G(k) = 1$. Moreover, by assumption, $\mathrm{wt}_G(h + k) = 2$. Since the image of $\gamma_{h,k}$ generates G_{h+k}, the map $\gamma_{h,k}$ is non-degenerate. Let now $h + k$ be even. The numbers h and k are both odd so $\mathrm{wt}_G(h) = \mathrm{wt}_G(k) = 2$, by Lemma 322(2). Assume without loss of generality that $h \leq k$. Then, by Lemma 323, the set $\rho^{\frac{k-h}{2}}(G_h)$ coincides with the subgroup G_k. Let now $C = \mathrm{C}_{G_h}(G_k)$ and $D = \mathrm{C}_{G_k}(G_h)$. Since $\gamma_{h,k} \neq 1$, Lemma 20 yields that $G_{h+1} \subseteq C \subsetneq G_h$ and $G_{k+1} \subseteq D \subsetneq G_k$. The commutator map induces a non-degenerate map $G_h/C \times G_k/D \to G_{h+k}$ so, $\mathrm{wt}_G(h+k)$ being equal to 1, Lemma 2 yields that $|G_h : C| = |G_k : D|$. Now, by Lemma 320, the group G is regular, and therefore so is C. Thanks to Lemma 52(1), the set $\rho^{\frac{k-h}{2}}(C)$ is a subgroup of C and

so, thanks to Lemma 54, one has $[\rho^{\frac{k-h}{2}}(C), G_h] = [C, \rho^{\frac{k-h}{2}}(G_h)] = [C, G_k] = \{1\}$. In particular, $\rho^{\frac{k-h}{2}}(C) \subseteq D$. Since $|G_h : C| = |G_k : D|$ and $\mathrm{wt}_G(h) = \mathrm{wt}_G(k) = 2$, we derive from Corollary 329 that $\rho^{\frac{k-h}{2}}(C) = D$. Assume now by contradiction that there exists $x \in G_h$ such that $G_h = \langle x, C\rangle$. Then $G_k = \langle \rho^{\frac{k-h}{2}}(x), D\rangle$ and therefore, the commutator map being alternating, one has $G_{h+k} = [G_k, G_h] = \langle [x, \rho^{\frac{k-h}{2}}(x)]\rangle = \{1\}$. Contradiction to the class of G being $h + k$. It follows that the quotient G_h/C is not cyclic and so $C = G_{h+1}$ and $D = G_{k+1}$. In particular, $\gamma_{h,k}$ is non-degenerate. ∎

Corollary 331. *Let $p > 3$ be a prime number and let G be a p-obelisk. Denote by c the class of G. Let moreover $l \in \{1, \ldots, c-1\}$ be such that $c - l$ is odd. Then the map $G_{c-l}/G_{c-l+1} \to \mathrm{Hom}(G_l/G_{l+1}, G_c)$ that is defined by*

$$t\, G_{c-l+1} \quad \mapsto \quad (x\, G_{l+1} \mapsto [t, x])$$

is a surjective homomorphism of groups.

Proof. As a consequence of Lemma 323, the groups G_l/G_{l+1}, G_{c-l}/G_{c-l+1}, and G_c are elementary abelian and the map $\gamma_{c-l,l}$ from Lemma 328 is thus a bilinear map of $\mathbb{F}_p$-vector spaces. Respecting the notation from Section 1.1, we define

$$\delta : G_{c-l}/G_{c-l+1} \to \mathrm{Hom}(G_l/G_{l+1}, G_c)$$

to be the map sending each element $v \in G_{c-l}/G_{c-l+1}$ to ${}_v(\gamma_{c-l,l})$. In other words, if $v = t\, G_{c-l+1}$, then $\delta(v) : G_l/G_{l+1} \to G_c$ is defined by $x\, G_{l+1} \mapsto [t, x]$. As a consequence of Lemma 328(2), the function δ is a homomorphism of groups and δ differs from the zero map. Let us now, for all $i \in \{1, \ldots, c\}$, denote $w_i = \mathrm{wt}_G(i)$. It follows that the dimension of $\mathrm{Hom}(G_l/G_{l+1}, G_c)$ is equal to $w_l w_c$ and, if $w_l w_c = 1$, then δ is surjective. We assume that $w_l w_c \neq 1$. The index $c-l$ being odd, it follows that either l or c is even. Proposition 321 yields $w_{c-l} = w_l w_c$ and, if l is even, then $w_c = 2$. As a consequence of Lemma 330, the map δ is injective and so δ is also surjective. ∎

10.3 Framed obelisks

Let $p > 3$ be a prime number and let G be a p-obelisk. Then G is *framed* if, for each maximal subgroup M of G, one has $\Phi(M) = G_3$.

Lemma 332. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let moreover $h, k \in \mathbb{Z}_{>0}$, with h odd and k even, and $n \in \mathbb{Z}_{\geq 0}$. Then the following diagram is commutative.*

$$\begin{array}{ccc} G_h/G_{h+1} \times G_k/G_{k+1} & \xrightarrow{\gamma_{h,k}} & G_{h+k}/G_{h+k+1} \\ \downarrow{\scriptstyle (\mathrm{id}_{G_h/G_{h+1}},\ \rho_k^n)} & & \downarrow{\scriptstyle \rho_{h+k}^n} \\ G_h/G_{h+1} \times G_{k+2n}/G_{k+2n+1} & \xrightarrow{\gamma_{h,k+2n}} & G_{h+k+2n}/G_{h+k+2n+1} \end{array}$$

Proof. The maps from the above diagram are defined in Lemma 328. Assume without loss of generality that $G_{h+k+2n+1} = \{1\}$ so that G_{h+k+2n} is central. The diagram is clearly commutative for $n = 0$. We will prove the most delicate case, i.e. when $n = 1$, and leave the general case to the reader. Set $n = 1$. Let $(x, y) \in G_h \times G_k$. We will show, and that suffices, that $[x, y^p] = [x, y]^p$. Thanks to Lemma 18(4), one gets

$$[x, y]^{-p}[x, y^p] = \prod_{r=1}^{p-1} [[y^r, x], y].$$

Applying Lemma 20 twice, one gets that, for each index r, the element $[[y^r, x], y]$ belongs to G_{h+2k}, which is itself contained in the central subgroup G_{h+k+2}. Moreover, the group G_{h+k} being central modulo G_{h+k+1}, Lemma 22 yields $[y^r, x] \equiv [y, x]^r \bmod G_{h+k+1}$. Thanks to Lemma 23, the commutator map on G induces a bilinear map $G_{h+k}/G_{h+k+1} \times G_k/G_{k+1} \to G_{h+2k}$ and therefore we get $[[y^r, x], y] = [[y, x]^r, y] = [[y, x], y]^r$. It follows that

$$[x, y]^{-p}[x, y^p] = \prod_{r=1}^{p-1} [[y^r, x], y] = \prod_{r=1}^{p-1} [[y, x], y]^r = [[y, x], y]^{\binom{p}{2}}$$

and, the prime p being larger than 2, the number $\binom{p}{2}$ is a multiple of p. Since $[[y, x], y]$ belongs to G_{h+k+2}, it follows from Lemma 323 that $[x, y^p] = [x, y]^p$. This concludes the case $n = 1$. ∎

Lemma 333. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let moreover $h, k \in \mathbb{Z}_{>0}$, with h odd and k even, and $m \in \mathbb{Z}_{\geq 0}$. Then the following diagram is commutative.*

$$\begin{array}{ccc} G_h/G_{h+1} \times G_k/G_{k+1} & \xrightarrow{\gamma_{h,k}} & G_{h+k}/G_{h+k+1} \\ \downarrow{\scriptstyle (\rho_h^m,\ \mathrm{id}_{G_k/G_{k+1}})} & & \downarrow{\scriptstyle \rho_{h+k}^m} \\ G_{h+2m}/G_{h+2m+1} \times G_k/G_{k+1} & \xrightarrow{\gamma_{h+2m,k}} & G_{h+k+2m}/G_{h+k+2m+1} \end{array}$$

Proof. The maps in the diagram are as in Lemma 328 and they are well-defined. Assume without loss of generality that $G_{h+k+2m+1} = \{1\}$ and so G_{h+k+2m} is central. Let $(x, y) \in G_h \times G_k$. The diagram is clearly commutative if $m = 0$; we will prove commutativity when $m = 1$, the most difficult case, and we will leave the general case to the reader. Set $m = 1$. We will prove, and that suffices, that $[x^p, y] = [x, y]^p$. Applying Lemma 18(3) twice, we get

$$[x^p, y][x, y]^{-p} = \prod_{s=1}^{p-1} [x, [x^{p-s}, y]] \prod_{s=1}^{p-1} \Big[x\,,\, \Big(\prod_{j=1}^{p-s-1} [x\,,\, [x^{p-s-j}, y]] \Big) [x, y]^{p-s} \Big].$$

Thanks to Lemma 20, each element $[x, [x^{p-s-j}, y]]$ belongs to G_{k+2h} and, the group G_{h+k+3} being trivial, G_{k+2h} centralizes G_{h+k}. Again by Lemma 20, for each index s, the element $[x, y]^{p-s}$ belongs to G_{h+k} and applying Lemma 18(1) twice yields

$$\begin{aligned}[x^p, y][x, y]^{-p} &= \prod_{s=1}^{p-1} \Big[x\,,\, \prod_{j=1}^{p-s-1} [x, [x^{p-s-j}, y]]\Big] \prod_{s=1}^{p-1} [x, [x, y]^{p-s}] \\ &= \prod_{s=1}^{p-1} \Big[x\,,\, \prod_{j=1}^{p-s-1} [x, [x^{p-s-j}, y]]\Big] \prod_{s=1}^{p-1} [x, [x, y]]^{p-s}.\end{aligned}$$

Thanks to Lemma 23, given any two positive integers i and j, the commutator map induces a bilinear map $G_i/G_{i+1} \times G_j/G_{j+1} \to G_{i+j}/G_{i+j+1}$. By taking consecutively $(i, j) = (h, k)$ and $(i, j) = (h, h + k)$, we get respectively that $[x^{p-s-j}, y] \equiv [x, y]^{p-s-j} \bmod G_{h+k+1}$ and so

$$[x, [x^{p-s-j}, y]] \equiv [x, [x, y]^{p-s-j}] \equiv [x, [x, y]]^{p-s-j} \bmod G_{2h+k+1}.$$

By taking $(i, j) = (h, 2h + k)$, we derive that

$$\begin{aligned}[x^p, y][x, y]^{-p} &= \prod_{s=1}^{p-1} \Big[x\,,\, \prod_{j=1}^{p-s-1} [x, [x, y]]^{p-s-j}\Big] \prod_{s=1}^{p-1} [x, [x, y]]^{p-s} \\ &= \prod_{s=1}^{p-1} \Big[x, [x, [x, y]]^{\binom{p-s}{2}}\Big] \prod_{s=1}^{p-1} [x, [x, y]]^{p-s} \\ &= \prod_{s=1}^{p-1} [x, [x, [x, y]]]^{\binom{p-s}{2}} \prod_{s=1}^{p-1} [x, [x, y]]^{p-s} = [x, [x, [x, y]]]^{\binom{p}{3}} [x, [x, y]]^{\binom{p}{2}}.\end{aligned}$$

The prime p being larger than 3, both $\binom{p}{2}$ and $\binom{p}{3}$ are multiples of p. As both $[x, [x, y]]$ and $[x, [x, [x, y]]]$ belong to G_{h+k+1}, it follows from Lemma 323 that $[x^p, y] = [x, y]^p$. This concludes the proof for $m = 1$. ∎

Proposition 334. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let moreover $h, k \in \mathbb{Z}_{>0}$, with h odd and k even, and let $m, n \in \mathbb{Z}_{\geq 0}$. Then the following diagram is commutative.*

$$\begin{array}{ccc} G_h/G_{h+1} \times G_k/G_{k+1} & \xrightarrow{\gamma_{h,k}} & G_{h+k}/G_{h+k+1} \\ \downarrow{\scriptstyle (\rho_h^m\ ,\ \rho_k^n)} & & \downarrow{\scriptstyle \rho_{h+k}^{m+n}} \\ G_{h+2m}/G_{h+2m+1} \times G_{k+2n}/G_{k+2n+1} & \xrightarrow{\gamma_{h+2m,k+2n}} & G_{h+k+2(m+n)}/G_{h+k+2(m+n)+1} \end{array}$$

Proof. Combine Lemmas 332 and Lemma 333. ∎

Lemma 335. *Let $p > 3$ be a prime number and let G be a p-obelisk of class at least 3. Let moreover M be a maximal subgroup of G. Then $[M, M] = [M, G_2]$ and, whenever $\mathrm{wt}_G(3) = 2$, the following are equivalent.*

1. *One has $\Phi(M) \neq G_3$.*
2. *One has $[M, M] = M^p = \Phi(M)$.*

Proof. The subgroups M^p and $[M, M]$ are both characteristic in the normal subgroup M; thus both M^p and $[M, M]$ are normal in G. By Lemma 319(2), the quotient G/G_2 has order p^2 and so $|G : M| = |M : G_2| = p$. It follows from Lemma 28 that $[M, M] = [M, G_2]$ and so, as a consequence of Corollary 329 and Lemma 330, the least jumps of $[M, M]$ and M^p in G are both equal to 3 and of width 1. In particular, $\Phi(M)$ is contained in G_3 and Lemma 327(2) yields $G_4 \subseteq M^p \cap [M, M]$. If the third width of G is equal to 2, then it follows that $\Phi(M) \neq G_3$ if and only if $[M, M] = \Phi(M) = M^p$. ∎

We remark that, as a consequence of Lemma 323, quotients of consecutive elements of the lower central series of a p-obelisk are vector spaces over $\mathbb{F}_p$ and therefore, in (2) and (3) from Proposition 336, it makes sense, for each positive integer i, to talk about subspaces of G_i/G_{i+1}.

Proposition 336. *Let $p > 3$ be a prime number and let G be a p-obelisk. Then the following conditions are equivalent.*

1. *The p-obelisk G is framed.*
2. *For each 1-dimensional subspace ℓ of G/G_2, the quotient G_3/G_4 is generated by $\rho_1^1(\ell)$ and $\gamma_{1,2}(\{\ell\} \times G_2/G_3)$.*
3. *For each $h, k \in \mathbb{Z}_{>0}$, with h odd and k even, and for each 1-dimensional subspace ℓ in G_h/G_{h+1}, the spaces $\rho_h^{k/2}(\ell)$ and $\gamma_{h,k}(\{\ell\} \times G_k/G_{k+1})$ generate G_{h+k}/G_{h+k+1}.*

Proof. (1) $\Leftrightarrow$ (2) Let $\pi : G \to G/G_2$ denote the natural projection. Then, through π, there is a bijection between the maximal subgroups of G and the 1-dimensional subspaces of G/G_2. For any maximal subgroup M of G, we know from Lemma 335 that $[M, G_2] = [M, M]$ and therefore (2) holds if and only if, given any maximal subgroup M of G, one has $\Phi(M)G_4 = G_3$. Lemma 327(2) yields that (2) is satisfied if and only if, for any maximal subgroup M of G, one has $\Phi(M) = G_3$. We now deal with (2) $\Leftrightarrow$ (3). The implication $\Leftarrow$ is proven by taking $h = 1$ and $k = 2$, so we will prove that (2) implies (3). Let ℓ be a 1-dimensional subspace of G_h/G_{h+1}. Define moreover $m = \frac{h-1}{2}$, $n = \frac{k-2}{2}$, and $S = m + n = \frac{h+k-3}{2}$. Thanks to Lemma 328(1), there exists a 1-dimensional subspace ℓ' of G/G_2 such that $\rho_1^m(\ell') = \ell$ and, moreover, $\rho_2^n(G_2/G_3) = G_k/G_{k+1}$. By assumption G_3/G_4 is generated by $\rho_1^1(\ell')$ and $\gamma_{1,2}(\{\ell'\} \times G_2/G_3)$, so it follows from Lemma 328(1) that $\rho_3^S(\rho_1^1(\ell'))$ and $\rho_3^S(\gamma_{1,2}(\{\ell'\} \times G_2/G_3))$ together span G_{h+k}/G_{h+k+1}. We now have

$$\rho_3^S(\rho_1^1(\ell')) = \rho_1^{S+1}(\ell') = \rho_h^{k/2}(\ell)$$

and, thanks to Proposition 334, we also have

$$\rho_3^S(\gamma_{1,2}(\{\ell'\} \times G_2/G_3)) = \gamma_{h,k}(\rho_1^m(\ell') \times \rho_2^n(G_2/G_3)) = \gamma_{h,k}(\{\ell\} \times G_k/G_{k+1}).$$

This completes the proof. ∎

10.4 Subgroups of obelisks

The major goal of this section is to link structural properties of subgroups of a p-obelisk to the parities and widths of their jumps. The importance of Section 10.4 will become clear in Chapter 13.

Proposition 337. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let H be a subgroup of G that is itself a p-obelisk. Then $H = G$.*

Proof. The subgroup H is non-abelian, by definition of a p-obelisk, and it is in particular non-trivial. Let l denote the least jump of H in G. Then, as a consequence of Lemma 20, the subgroup $H_2 = [H, H]$ is contained in G_{2l}. Moreover, since H^p is equal to H_3, the subgroup H^p is contained in H_2. It follows from Corollary 329 that the minimum jump of H_2 is at most $l+2$: we get that $2l \leq l+2$ and therefore $l \leq 2$. We will show that $HG_2 = G$. Assume by contradiction that $G \neq HG_2$. Then, as a consequence of Lemma 319(2), the width $\mathrm{wt}_H^G(l)$ is equal to 1 and so Lemma 28 yields that $H_2 = [H, H \cap G_{l+1}]$. Thanks to Lemma 20, the subgroup H_2 is contained in G_{2l+1} and therefore $2l + 1 \leq l + 2$. It follows that $l = 1$ and that H_2 is contained in G_3. Define now $\overline{G} = G/G_4$ and use the bar notation for the subgroups of $\overline{G}$. By the isomorphism theorems, the groups $\overline{H}$ and $H/(H \cap G_4)$ are isomorphic and so, as a consequence of Lemma 326, the group $\overline{H}$ is abelian or

a p-obelisk. The minimum jump of H^p in G being equal to 3, we have that 3 is a jump of $\overline{H_2}$ in $\overline{G}$ and so $\overline{H}$ is a p-obelisk. Now, the group $\overline{G_3}$ is central in $\overline{G}$ and so, the group $\overline{H_2}$ being non-trivial, the quotient $\overline{H}/(\overline{H} \cap \overline{G_3})$ is not cyclic. It follows that 2 is a jump of $\overline{H}$ in $\overline{G}$ and, from the combination of Lemmas 322 and 328(2), that $\overline{H_2}$ has order p. Since $\overline{H_2}$ contains $\overline{H}^p$, we get $\overline{H_2} = \overline{H}^p = \overline{H_3}$. Contradiction to $\overline{H}$ being non-abelian. We have proven that $G = HG_2$, from which we derive $G = H\Phi(G)$. Lemma 33 yields $H = G$. ∎

Lemma 338. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let H be a cyclic subgroup of G. Then all jumps of H in G have the same parity and width 1.*

Proof. Let H be a cyclic subgroup of G. Then, for all $i \in \mathbb{Z}_{>0}$, there exists $k \in \mathbb{Z}_{\geq 0}$ such that $H \cap G_i = H^{p^k}$. Moreover, $i \in \mathbb{Z}_{>0}$ is a jump of H in G if and only if there exists $k \in \{0, 1, \ldots, \log_p |H| - 1\}$ such that $H \cap G_i = H^{p^k}$ and $H \cap G_{i+1} = H^{p^{k+1}}$. We conclude thanks to Lemma 328(1). ∎

Lemma 339. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c denote the nilpotency class of G and assume that one of the following holds.*

1. *The number c is even.*
2. *One has $\mathrm{wt}_G(c) = 2$.*

If H is a subgroup such that all of its jumps in G have the same parity and width 1, then H is cyclic.

Proof. Without loss of generality we assume that H is non-trivial and we take l to be the least jump of H in G. Let moreover $\mathcal{J}(H)$ denote the collection of jumps of H in G and define $J = \{l + 2k \ : \ k \in \mathbb{Z}_{\geq 0},\ k \leq (c-l)/2\}$. Let x be an element of H such that $\mathrm{dpt}_G(x) = l$; the existence of x is guaranteed by Lemma 82. Write $K = \langle x \rangle$ and let $\mathcal{J}(K)$ be the collection of jumps of K in G. By assumption J contains $\mathcal{J}(H)$ and, as a consequence of Corollary 329, the set J is contained in $\mathcal{J}(K)$. Keeping in mind that each jump of H in G has width 1, one derives

$$|K| = \prod_{j \in \mathcal{J}(K)} p^{\mathrm{wt}_K^G(j)} \geq \prod_{j \in J} p^{\mathrm{wt}_K^G(j)} \geq \prod_{j \in J} p^{\mathrm{wt}_H^G(j)} \geq \prod_{j \in \mathcal{J}(H)} p^{\mathrm{wt}_H^G(j)} = |H|.$$

It follows that $K = H$ and H is cyclic. ∎

Lemma 340. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c denote the nilpotency class of G and let H be a subgroup of G such that $H \cap G_c = \{1\}$. If all jumps of H in G have the same parity and width 1, then H is cyclic.*

Proof. We denote $\overline{G} = G/G_c$ and we will use the bar notation for the subgroups of $\overline{G}$. As a consequence of Lemma 428, the group $\overline{G}$ is abelian or it is a p-obelisk. If $\overline{G}$ is abelian, then $c = 2$ and so, by Lemma 339, the subgroup H is cyclic. Assume now that $\overline{G}$ is non-abelian and thus a p-obelisk. The group $\overline{G}$ has class $c-1$ and, as a consequence of Corollary 322, either $c-1$ is even or $\mathrm{wt}_{\overline{G}}(c-1) = 2$. It follows from Lemma 339 that $\overline{H}$ is cyclic and, the intersection $H \cap G_c$ being trivial, so is H. ∎

Lemma 341. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c denote the nilpotency class of G and let H be a non-trivial subgroup of G such that $H \cap G_c = \{1\}$. Let l be the least jump of H in G and assume that all jumps of H in G have the same parity and the same width. Then the following hold.*

1. *The group H is abelian.*
2. *One has $\Phi(H) = H \cap G_{l+1}$.*

Proof. Let $\mathcal{J}(H)$ denote the collection of jumps of H in G. We first assume $\mathrm{wt}_H^G(l) = 1$. By Lemma 340, the subgroup H is cyclic and $\Phi(H)$ has index p in H. It follows that $\Phi(H) = H \cap G_{l+1}$. Assume now that $\mathrm{wt}_H^G(l) = 2$. Then, thanks to Lemma 322(3), the jump l is odd. The subgroup $[H, H]$ is contained in G_{2l}, thanks to Lemma 20, and therefore, $2l$ being even, Lemma 328(2) yields $2l > c$. In particular, one has $[H, H] = \{1\}$ so $\Phi(H) = H^p$. Moreover, as a consequence of Lemma 328(1), the set of jumps of H^p in G is equal to $\mathcal{J}(H) \setminus \{l\}$ and each jump of H^p has width 2. It follows that $H^p = H \cap G_{l+1}$. Thanks to Proposition 321 the width $\mathrm{wt}_H^G(l)$ is either 1 or 2 and the proof is thus complete. ∎

Lemma 342. *Let $p > 3$ be a prime number and let G be a p-obelisk. Let c be the class of G and let H be a non-trivial subgroup of G such that $H \cap G_c = \{1\}$. Denote by l the least jump of H and assume that $H \cap G_{l+1} = \Phi(H)$. Finally, assume that $c-l$ is odd. Then, for each complement K of G_c in HG_c, there exists $t \in G_{c-l}$ such that $K = tHt^{-1}$.*

Proof. The subgroup G_c is central in G, because G has class c, and so, by Lemma 114, all complements of G_c in $T = HG_c$ are of the form $\{f(h)h : h \in H\}$ as f varies in $\mathrm{Hom}(H, G_c)$. The subgroup G_c is elementary abelian, as a consequence of Lemma 323, and therefore $\mathrm{Hom}(H, G_c)$ is naturally isomorphic to $\mathrm{Hom}(H/\Phi(H), G_c) = \mathrm{Hom}(H/(H \cap G_{l+1}), G_c)$. By assumption, $c - l$ is odd so, thanks to Corollary 331, the homomorphism $G_{c-l}/G_{c-l+1} \to \mathrm{Hom}(G_l/G_{l+1}, G_c)$, defined by $tG_{c-l} \mapsto (xG_{l+1} \mapsto [t, x])$, is surjective. By Lemma 323, the quotient G_l/G_{l+1} is elementary abelian and therefore the restriction map

$$\mathrm{Hom}(G_l/G_{l+1}, G_c) \to \mathrm{Hom}(HG_{l+1}/G_{l+1}, G_c)$$

is surjective. By the isomorphism theorems, HG_{l+1}/G_{l+1} and $H/(H \cap G_{l+1})$ are isomorphic and so every homomorphism $H \to G_c$ is of the form $x \mapsto [t, x]$, for some $t \in G_{c-l}$. For each complement K of G_c in T there exists thus $t \in G_{c-l}$ such that $K = \{[t, x]x \ : \ x \in H\} = \{txt^{-1} \ : \ x \in H\} = tHt^{-1}$. ∎