Intense automorphisms of finite groups

Stanojkovski, M.

Chapter 13

A generalization to profinite groups

Let G be a profinite group and let α be an automorphism of G. Then α is *topologically intense* if, for every closed subgroup H of G, there exists $x \in G$ such that $\alpha(H) = xHx^{-1}$. Topologically intense automorphisms are automatically continuous, because they stabilize each open normal subgroup of the group on which they are defined. We denote by $\mathrm{Int_c}(G)$ the group of topologically intense automorphisms of a profinite group G.

Topologically intense automorphisms are a generalization of intense automorphisms to profinite groups. In Section 13.2, we will show that, the group of topologically intense automorphisms of a profinite group is itself profinite and moreover, if p is a prime number and G is a pro-p-group, then $\mathrm{Int_c}(G)$ is isomorphic to $S \rtimes C$, where S is a pro-p-subgroup of $\mathrm{Int_c}(G)$ and C is a subgroup of $\mathbb{F}_p^*$. The *intensity* of a pro-p-group G is then defined to be the cardinality of C and it is denoted by $\mathrm{int}(G)$. The question we ask is: *What are the infinite pro-p-groups that have intensity greater than* 1*?* We answer this question with Theorem 405, which we state after fixing some notation. Let p be an odd prime number and take $t \in \mathbb{Z}_p$ to be a quadratic non-residue modulo p. We define Δ_p to be the quaternion algebra $\mathbb{Z}_p \oplus \mathbb{Z}_p\mathrm{i} \oplus \mathbb{Z}_p\mathrm{j} \oplus \mathbb{Z}_p\mathrm{k}$ with defining relations $\mathrm{i}^2 = t$, $\mathrm{j}^2 = p$, and $\mathrm{k} = \mathrm{ij} = -\mathrm{ji}$. We denote by $\mathrm{S}(\Delta_p)$ the pro-p-subgroup of the multiplicative group $(1 + \mathrm{j}\Delta_p)$ that consists of all elements $x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ satisfying $a^2 - tb^2 - pc^2 + tpd^2 = 1$.

Theorem 405. *Let p be a prime number and let G be an infinite pro-p-group. Then* $\mathrm{int}(G) > 1$ *if and only if exactly one of the following holds.*

1. *One has $p > 2$ and G is abelian.*
2. *One has $p > 3$ and G is topologically isomorphic to* $\mathrm{S}(\Delta_p)$.

Moreover, one has $\mathrm{int}(\mathrm{S}(\Delta_p)) = 2$ *and, if G is abelian, then* $\mathrm{int}(G) = p - 1$.

Let p be a prime number and let G be a pro-p-group. We will show, in Section 13.2, that $\operatorname{int}(G) = \gcd\{\operatorname{int}(G/N) : N \text{ normal open in } G,\ N \neq G\}$ and, thanks to this last characterization, we will derive the following theorem as a corollary of Theorem 405.

Theorem 406. *Let $p > 3$ be a prime number. Then, for any positive integer c, there exists a finite p-group G of class c and intensity greater than* 1*.*

The pace of Chapter 13 will be slightly faster, compared to the previous ones, in the sense that we will assume the reader is familiar with some basic facts about profinite groups (which can however all be found in Chapters 0 and 1 from [DdSMS91]). We will give some extra background in Section 13.1. In Section 13.2, we will prove several properties of topologically intense automorphisms and give an analogue of Theorem 86 for pro-p-groups. In the subsequent sections we will pave the way to proving Theorem 405. In Section 13.3, we will give some limitations, for $p > 3$, to the structure of infinite non-abelian pro-p-groups of intensity greater than 1. In Section 13.5, we will discover that, if such groups exist, they can be continuously embedded in one of two infinite pro-p-groups (one of them being $\mathrm{S}(\Delta_p)$). We will study the structure of those two groups in Section 13.4 and, in Section 13.5, we will prove that, if $p > 3$ is a prime number and G is an infinite non-abelian pro-p-group with $\operatorname{int}(G) > 1$, then G is topologically isomorphic to $\mathrm{S}(\Delta_p)$. The results from Section 13.4.2 will ensure that $\operatorname{int}(\mathrm{S}(\Delta_p)) > 1$. We will conclude the proof of Theorem 405 in Section 13.6.1 and give that of Theorem 406 in Section 13.6.2. We will close Chapter 13 with Section 13.6.3, where we will draw a bridge between Theorem 405 and Theorem 406.

13.1 Some background

This section is a collection of definitions and results from [DdSMS91]. If G is a profinite group and S is a subset of it, we denote by $\operatorname{cl}(S)$ the closure of S in G. A full list of the symbols we use can be found at the beginning of this thesis (see List of Symbols).

Definition 407. *Let G be a profinite group. A* discrete quotient *of G is a quotient of G by an open normal subgroup. A* proper quotient *of G is a quotient of G by a closed normal subgroup that is different from $\{1\}$.*

Definition 408. *Let G be a profinite group. Then a set X is a* set of topological generators *of G if $G = \operatorname{cl}(\langle X \rangle)$. The group G is* topologically finitely generated *if it admits a finite set of topological generators.*

Definition 409. *Let G be a profinite group. The* lower central series $(G_i)_{i \geq 1}$ *of G is defined by*

$$G_1 = G \quad \text{and} \quad G_{i+1} = \operatorname{cl}([G, G_i]).$$

In Section 1.2, we have defined the lower central series for any abstract group, which should not be confused with that of a profinite group. In the case of finite groups, they however coincide. We recall that, as defined in Section 8.2, the rank of a finite group H is the smallest integer r such that every subgroup of H can be generated by r elements.

Definition 410. *Let G be a profinite group. The* rank *of G is*

$$\mathrm{rk}(G) = \sup\{\mathrm{rk}(G/N) : N \textit{ is normal open in } G\}.$$

Let G be a profinite group. It follows from the definition that $\mathrm{rk}(G)$ belongs to $\mathbb{Z} \cup \{\infty\}$ and, if G has finite rank, that G is also finitely generated. Moreover, when G is finite, the definition of rank given in Section 8.2 is equivalent to the one from Definition 410. In [DdSMS91, Proposition 3.11], a series of equivalent definitions of rank is given.

Definition 411. *A* p-adic analytic *group is a profinite group that contains an open pro-p-subgroup of finite rank.*

Our definition of a p-adic analytic group is not among the standard ones, but it serves our purposes the best. In general, p-adic analytic groups are defined to be topological groups that present the structure of a p-adic manifold. The equivalence of the two definitions, for profinite groups, is given by Corollary 9.35 from [DdSMS91]. For more information about the topic, see [DdSMS91, Ch. 9].

Definition 412. *A profinite group is* just-infinite *if it is infinite and each of its proper quotients is finite.*

Definition 413. *Let p be a prime number and let G be a pro-p-group. The* Frattini subgroup *of G is $\Phi(G) = \mathrm{cl}(G^p[G,G])$.*

As for the case of finite p-groups, the Frattini subgroup $\Phi(G)$ of a pro-p-group G is the unique closed normal subgroup of G minimal with the property that $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$.

Lemma 414. *Let p be a prime number and let G be a pro-p-group. Then G is topologically finitely generated if and only if $\Phi(G)$ is open in G.*

Proof. This is Proposition 1.14 from [DdSMS91]. ∎

In Chapter 3 of [DdSMS91] it is proven that, if G is a finitely generated group, then the cardinality of a minimal set of topological generators of G is equal to $\dim_{\mathbb{F}_p}(G/\Phi(G))$.

Definition 415. *Let p be an odd prime number and let U be a pro-p-group. Then U is* uniform *if the following hold.*

1. *The group U is topologically finitely generated.*

2. *The quotient $U/\operatorname{cl}(U^p)$ is abelian.*

3. *The group U is torsion-free.*

The definition of uniform group we give is slightly different from the one that is given in [DdSMS91]. However, the equivalence of the two is proven in [DdSMS91, Theorem 4.8].

Definition 416. *Let p be an odd prime number and let U be a uniform pro-p-group. The* dimension *of U is the cardinality of a minimal set of topological generators of U. The dimension of U is denoted* $\dim(U)$.

Lemma 417. *Let p be an odd prime number and let G be a pro-p-group of finite rank. Then G has a characteristic open uniform subgroup.*

Proof. See Corollary 4.3 from [DdSMS91]. ∎

Lemma 418. *Let p be an odd prime number and let G be a pro-p-group. Then all open uniform subgroups of G have the same dimension.*

Proof. See [DdSMS91, Corollary 4.6]. ∎

Definition 419. *Let p be an odd prime number and let G be a pro-p-group of finite rank. The* dimension *of G is the dimension of any of its open uniform subgroups.*

Lemmas 417 and 418 guarantee the consistency of Definition 419.

13.2 Properties and intensity

In Section 13.2 we give several properties of topologically intense automorphisms and, for a given prime number p, we define the intensity of a pro-p-group.

Lemma 420. *Let G be a profinite group and let α be a topologically intense automorphism of G. Then α induces an intense automorphism on each discrete quotient of G.*

Proof. Let N be an open normal subgroup of G. Then $\alpha(N) = N$ and α induces an automorphism $\overline{\alpha}$ of G/N. Now each subgroup $\overline{H}$ of G/N corresponds to an open subgroup H of G, which is sent to a conjugate by α. As a consequence, also $\overline{\alpha}(\overline{H})$ and $\overline{H}$ are conjugate in G/N and, the choice of $\overline{H}$ being arbitrary, it follows that $\overline{\alpha}$ is intense. ∎

If G is a profinite group and Υ denotes the set of open normal subgroups of G, then $\mathrm{Aut}(G)$ has a natural topology, the "congruence topology", for which a basis of open neighbourhoods of the identity is given by

$$\{\Gamma(N) = \{\alpha \in \mathrm{Aut}(G) : \alpha \equiv \mathrm{id} \bmod N\}\}_{N \in \Upsilon}.$$

For more information on the subject see for example [DdSMS91, Ch. 5.2].

Lemma 421. *Let G be a profinite group and let Υ denote the collection of open normal subgroups of G. Then one has*

$$\mathrm{Int_c}(G) = \varprojlim_{N \in \Upsilon} \mathrm{Int}(G/N).$$

Proof. Let Υ denote the collection of open normal subgroups of G. Then, thanks to Lemma 420, we have a natural homomorphism

$$\pi : \mathrm{Int_c}(G) \to \prod_{N \in \Upsilon} \mathrm{Int}(G/N).$$

The map π is injective, because $\ker \pi$ is contained in $\cap_{N \in \Upsilon} \Gamma(N) = \{1\}$, and the image of π is equal to $\varprojlim_{N \in \Upsilon} \mathrm{Int}(G/N)$, thanks to Lemma 88(2). ∎

Lemma 422. *Let $\{X_\lambda\}_{\lambda \in \Lambda}$ be an inverse system of finite non-empty sets over a directed set Λ. Then $\varprojlim X_\lambda$ is non-empty.*

Proof. This is Proposition 1.4 from [DdSMS91]. ∎

Proposition 423. *Let G be a profinite group and let α be an automorphism of G. Then the following are equivalent.*

1. *The automorphism α is topologically intense.*
2. *For every open subgroup H of G, there exists an element $x \in G$ such that $\alpha(H) = xHx^{-1}$.*

Proof. As every open subgroup is also closed, (1) clearly implies (2). Assume now (2) and let H be a closed subgroup of G. We will construct $x \in G$ such that $\alpha(H) = xHx^{-1}$. Let Λ denote the collection of all discrete quotients of G and let moreover Υ be the collection of all open normal subgroups of G. Then there is a natural bijection $\Upsilon \to \Lambda$, given by $N \mapsto G/N$. Now, thanks to Lemma 420, the automorphism α induces an intense automorphism on each element of Λ. Hence, if $\overline{G}$ is an element of Λ and $\overline{H}$ denotes the image of H in $\overline{G}$, then there exists $x \in \overline{G}$ such that $\overline{\alpha(H)} = x\overline{H}x^{-1}$. For each $\overline{G} \in \Lambda$ define $X_{\overline{G}} = \{x \in \overline{G} : \overline{\alpha(H)} = x\overline{H}x^{-1}\}$ and observe that $X_{\overline{G}}$ is finite and non-empty. Let now $\overline{G}$ and $\overline{G}'$ be elements of Λ such that $\overline{G}'$ is a quotient of $\overline{G}$. Then the natural projection $\overline{G} \to \overline{G}'$

induces a well-defined map $X_{\overline{G}} \to X_{\overline{G}'}$. It follows that $\{X_{\overline{G}}\}_{\overline{G}\in\Lambda}$ is an inverse system of finite non-empty sets so, by Lemma 422, the set $X = \varprojlim X_{\overline{G}}$ is non-empty. Let $x \in X$. As a consequence of the definition of X, for each element N of Υ, the element xN belongs to $X_{G/N}$ and thus, for each $N \in \Upsilon$, we have $\alpha(HN) = xHx^{-1}N$. The map α is continuous, because it stabilizes each open normal subgroup, and so it follows that

$$\alpha(H) = \mathrm{cl}(\alpha(H)) = \bigcap_{N\in\Upsilon} \alpha(H)N = \bigcap_{N\in\Upsilon} \alpha(HN) =$$

$$= \bigcap_{N\in\Upsilon} xHx^{-1}N = \mathrm{cl}(xHx^{-1}) = xHx^{-1}.$$

This proves (1), and therefore the proof is complete. ■

In the proof of the following result we will use the generalization to profinite groups of Schur-Zassenhaus's theorem (see for example Theorem 2.3.15 from [RZ10]).

Proposition 424. *Let p be a prime number and let G be a pro-p-group. Then*

$$\mathrm{Int_c}(G) = S \rtimes C,$$

where S is a Sylow pro-p-subgroup of $\mathrm{Int_c}(G)$ and C is isomorphic to a subgroup of $\mathbb{F}_p^*$. Moreover, one has

$$|C| = \gcd\{\mathrm{int}(G/N) : N \text{ normal open in } G,\ N \neq G\}.$$

Proof. Let Υ denote the collection of open normal subgroups of G. For each $N \in \Upsilon$, denote by $\pi_N : \mathrm{Int}(G/N) \to \mathrm{Int}((G/N)/\Phi(G/N))$ the map from Lemma 88(2) and set $K_N = \ker \pi_N$ and $I_N = \pi_N(\mathrm{Int}(G/N))$. For each $N \in \Upsilon$, we then get a short exact sequence

$$1 \to K_N \to \mathrm{Int}(G/N) \to I_N \to 1$$

which induces, thanks to Lemma 421 and the exactness of $\varprojlim$, the short exact sequence

$$1 \to \varprojlim_{N\in\Upsilon} K_N \to \mathrm{Int_c}(G) \to \varprojlim_{N\in\Upsilon} I_N \to 1.$$

Define $S = \varprojlim_{N\in\Upsilon} K_N$ and $C = \varprojlim_{N\in\Upsilon} I_N$. As a consequence of Lemma 101, whenever $M, N \in \Upsilon \setminus \{G\}$ and $N \subseteq M$, the natural map $I_N \to I_M$ is injective and therefore, $\varprojlim_{N\in\Upsilon} \mathrm{Int}((G/N)/\Phi(G/N))$ being equal to $\mathrm{Int}(G/\Phi(G))$, Lemma 89 yields that C is isomorphic to a subgroup of $\mathbb{F}_p^*$. Moreover, thanks to Lemma 97, the group S is a pro-p-subgroup of $\mathrm{Int_c}(G)$. The order of C being coprime to p, it follows that in fact S is a Sylow pro-p-subgroup of $\mathrm{Int_c}(G)$ and, from the generalization of

Schur-Zassenhaus's theorem to profinite groups, that $\mathrm{Int_c}(G) = S \rtimes C$. Moreover, the fact that $|C|$ is equal to the greatest common divisor of the $\mathrm{int}(G/N)$, as N varies in $\Upsilon \setminus \{G\}$, is a direct consequence of Lemma 101. ∎

Let p be a prime number and let G be a pro-p-group. Let moreover C be as in Proposition 424. The *intensity* $\mathrm{int}(G)$ of G is defined to be the cardinality of C. Thanks to Proposition 424, the intensity of G is also equal to the greatest common divisor of the set $\{\mathrm{int}(G/N) : N \text{ normal open in } G,\ N \neq G\}$.

Corollary 425. *Let p be a prime number and let G be an abelian pro-p-group. If G is non-trivial, then* $\mathrm{int}(G) = p - 1$.

Proof. If G is non-trivial, then Theorem 86 yields $\mathrm{int}(G) = p - 1$. ∎

13.3 Non-abelian groups, part I

The main purpose of Section 13.3 is to give a proof of Proposition 426. We refer to Section 13.1 for the definitions of just-infinite profinite groups and of p-adic analytic groups and their dimensions.

Proposition 426. *Let $p > 3$ be a prime number and let G be a non-abelian infinite pro-p-group. Assume that* $\mathrm{int}(G) > 1$. *Then G is a just-infinite p-adic analytic group of dimension* 3.

The following assumptions will be valid until the end of Section 13.3. Let p be an odd prime number and let G be an infinite non-abelian pro-p-group of intensity greater than 1. Let $(G_i)_{i \geq 1}$ denote the lower central series of G, as defined in Section 13.1, and let α be a topologically intense automorphism of G of order 2. The existence of α is guaranteed by the combination of Propositions 424 and 133.

Lemma 427. *The automorphism α induces an intense automorphism of order* 2 *on each non-trivial discrete quotient of G.*

Proof. Let C be as in proposition 424 and, without loss of generality, assume that $\alpha \in C$. Then, as a consequence of Lemma 420, given any open normal subgroups N and M of G such that $N \subseteq M \neq G$, we get a commutative diagram

$$\begin{tikzcd} C \arrow[r] \arrow[d] & \mathrm{Int}(G/M) \\ \mathrm{Int}(G/N) \arrow[ur] & \end{tikzcd} .$$

Moreover, the map α being non-trivial, there exists a discrete quotient of G on which α induces an automorphism of order 2. The choice of M and N being arbitrary, it follows that α induces an intense automorphism of order 2 on each non-trivial discrete quotient of G. ∎

Lemma 428. *Assume that $p > 3$. Then each discrete quotient of G of class at least 4 is a p-obelisk.*

Proof. Let $\overline{G}$ be a discrete quotient of class at least 4 of G. By Lemma 427, the map α induces an intense automorphism of order 2 of $\overline{G}$. It follows from Proposition 318 that $\overline{G}$ is a p-obelisk. ∎

Lemma 429. *Let c be a non-negative integer. Then G has a discrete quotient of class c.*

Proof. Assume by contradiction that there exists an upper bound on the class of the discrete quotients of G and let $C \in \mathbb{Z}_{\geq 0}$ be minimal with this property. Since G is non-abelian, one has $C \geq 2$. Let us now denote by Υ the collection of open normal subgroups of G. Then $G = \varprojlim_{N \in \Upsilon} G/N$ and so G has class C. The group G being infinite, it follows from Theorem 165 that $C < 3$ and so $C = 2$. Let now $M, N \in \Upsilon$ be such that G/N has class 2 and $M \subsetneq N$. Let $K = G/M$ and let $\pi : G \to K$ denote the canonical projection. Then K has class 2 and, as a consequence of Lemma 427, the intensity of K is greater than 1. By Theorem 105, the group K is extraspecial and, $\pi(N)$ being non-trivial and normal in K, it follows from Lemma 29 that $\pi(N)$ contains $\mathrm{Z}(K) = [K, K]$. In particular, $K/\pi(N)$ is abelian and therefore so is G/N. Contradiction. ∎

Lemma 430. *The set $\{G_i\}_{i \geq 1}$ is a base of open neighbourhoods of 1 in G.*

Proof. Let moreover Υ denote the collection of all open normal subgroups N of P with the property that G/N has class at least 3. As a consequence of Lemma 429, the group G is equal to $\varprojlim_{N \in \Upsilon} G/N$. Moreover, each subgroup G_i being closed, we also have $G_i = \varprojlim_{N \in \Upsilon} (G/N)_i$. Thanks to Lemma 427, whenever $N \in \Upsilon$, the quotient G/N has intensity greater than 1 and so Theorem 218 yields that $\{G_i\}_{i \geq 1}$ is a base of open neighbourhoods of 1 in G. ∎

Lemma 431. *Assume that $p > 3$. Then $\mathrm{rk}(G) = 3$ and G is p-adic analytic.*

Proof. By Lemma 427, the automorphism α induces an intense automorphism of order 2 on each non-trivial discrete quotient of G and, as a consequence of Lemma 429, the group G has finite quotients of any possible class. It follows that $\mathrm{rk}(G) = \sup\{\mathrm{rk}(G/N) : G/N \text{ has class at least } 4\}$ and hence Proposition 222 yields $\mathrm{rk}(G) = 3$. The group G being a pro-p-group of finite rank, it is p-adic analytic. ■

Lemma 432. *Assume that $p > 3$. Let N be a non-trivial closed subgroup of G. Then the following are equivalent.*

1. *The subgroup N is normal.*
2. *There exists $l \in \mathbb{Z}_{\geq 1}$ such that $G_{l+1} \subseteq N \subseteq G_l$.*

Moreover, P is just-infinite.

Proof. The implication (2) ⇒ (1) is clear; we prove (1) ⇒ (2). Thanks to Lemma 430, every element of the lower central series of G is open and $\{G_i\}_{i\geq 1}$ is a base of open neighbourhoods of 1. For all $k \in \mathbb{Z}_{\geq 1}$, denote by $\pi_k : G \to G/G_k$ the canonical projection and set $l = \max\{k : \pi_k(N) = 1\}$. The index l is well-defined, because $N \neq 1$, and N is contained in G_l, but not in G_{l+1}, by the maximality of l. In particular, for each $k > l$, the minimum jump of $\pi_k(N)$ in G/G_k is l. Now, by Lemma 428, whenever $k \geq 5$, the quotient G/G_k is a p-obelisk. It follows from Lemma 327(2) that, whenever $k > \max\{l, 5\}$, the subgroup G_{l+1} is contained in NG_k, and therefore

$$G_{l+1} \subseteq \bigcap_{k>\max\{l,5\}} NG_k = \bigcap_{k\geq 1} NG_k = \mathrm{cl}(N) = N.$$

We have proven that $G_{l+1} \subseteq N \subseteq G_l$ and thus also that (1) implies (2). To conclude, since each G_k is open in G, the subgroup N is open and the quotient G/N is finite. Because of the arbitrary choice of N, the group G is just-infinite. ■

Lemma 433. *Assume that $p > 3$. Then G is torsion-free.*

Proof. By Lemma 428, whenever k is at least 5, the quotient G/G_k is a p-obelisk. It follows from Corollary 329 that, for each non-negative integer i, raising to the power p induces a well-defined isomorphism $G_i/G_{i+1} \to G_{i+2}/G_{i+3}$. By Lemma 429, there is no bound on the class of the finite quotients of G, and therefore G is torsion-free. ■

Lemma 434. *Assume that $p > 3$. Then G_2 is open, uniform, and has dimension 3.*

Proof. Let $\overline{G}$ be a discrete quotient of class at least 5 of G, which exists by Lemma 429. As a consequence of Lemma 428, the group $\overline{G}$ is a p-obelisk and so Lemma 322 yields $|\overline{G}_2 : \overline{G}_4| = p^3$. The subgroup $\overline{G}_2^p$ is equal to $\overline{G}_4$, thanks to Lemma 323, and so, as a consequence of Lemma 20, the quotient $\overline{G}_2/\overline{G}_2^p = \overline{G}_2/\overline{G}_4$ is elementary abelian. It follows that each generating set of $\overline{G}_2$ has at least 3 elements. However, the rank of G is equal to 3, thanks to Lemma 431, and therefore $\overline{G}_2$ is generated by exactly 3 elements. Since $\overline{G}$ was chosen arbitrarily, the quotient $G_2/\operatorname{cl}(G_2^p)$ is abelian and any minimal set of topological generators of G_2 has 3 elements. Now, as a consequence of Lemma 433, the torsion of G_2 is trivial and hence G_2 is uniform of dimension 3. Moreover, the subgroup G_2 is open thanks to Lemma 430. ∎

We conclude Section 13.3 by giving the proof of Proposition 426. Assume that $p > 3$. Then G is p-adic analytic, by Lemma 431, and it has dimension 3 thanks to Lemma 434. Moreover, G is just-infinite by Lemma 432. The proof of Proposition 426 is now complete.

13.4 Two infinite groups

In Section 13.4 we present two infinite pro-p-groups, which are p-adic analytic. We will see, in Section 13.5, the role they play in the proof of Theorem 405.

13.4.1 The first group

Let $p > 3$ be a prime number and let $\pi : \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{F}_p)$ be the canonical projection. Let $\mathrm{SL}_2^{\triangle}(\mathbb{F}_p)$ denote the subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ consisting of those elements of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{where} \quad x \in \mathbb{F}_p.$$

We define $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p) = \pi^{-1}(\mathrm{SL}_2^{\triangle}(\mathbb{F}_p))$ and remark that $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ is a pro-p-group. Our notation is consistent with that of [GSK09]; however, we will make use of several facts coming from [Hup67, Ch. III.17], where the group $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ is denoted by $\mathfrak{M}_{0,1,1}$.

Lemma 435. *Let $p > 3$ be a prime number and let $G = \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for each $k \in \mathbb{Z}_{\geq 3}$, the quotient G/G_k is a p-obelisk.*

Proof. This is a reformulation of Satz 17.8 from [Hup67, Ch. III]. ∎

Lemma 436. *Let $p > 3$ be a prime number and let $G = \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then there exist $x \in G \setminus G_2$ and $a \in G_2 \setminus G_3$ such that $[x, a] \in \operatorname{cl}(\langle x \rangle)$.*

Proof. This proof relies on several lemmas from [Hup67, Ch. III.17]; we will respect Huppert's notation. Let

$$x = B(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad a = D(1+p) = \begin{pmatrix} (1+p)^{-1} & 0 \\ 0 & (1+p) \end{pmatrix}.$$

Satz 17.4 from [Hup67, Ch. III.17] gives a concrete characterization of the lower central series of G, from which it directly follows that $x \in G \setminus G_2$ and $a \in G_2 \setminus G_3$. As a consequence of Hilfssatz 17.2(a), the element x generates topologically the subgroup $\mathfrak{B}_0$ consisting of all matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{where} \quad x \in \mathbb{Z}_p.$$

To conclude, Hilfssatz 17.3 guarantees that there exists an element $b \in \mathbb{Z}_p$ such that

$$[x,a] = \begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix}$$

so, in particular, $[x,a]$ belongs to the subgroup $\mathfrak{B}_0 = \mathrm{cl}(\langle x \rangle)$. ∎

We recall that a p-obelisk is a non-abelian finite p-group G satisfying $G_3 = G^p$ and $|G : G_3| = p^3$. A p-obelisk G is framed if, given any maximal subgroup M of G, one has $\Phi(M) = G_3$. For more information about p-obelisks, we refer to Chapter 10.

Lemma 437. *The group* $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ *has a discrete quotient of class* 6 *that is not a framed* p*-obelisk.*

Proof. Let $G = \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ and denote by $(G_i)_{i \geq 1}$ the lower central series of G, as defined in Section 13.1. We define $\overline{G} = G/G_7$ and we use the bar notation for subgroups and elements of $\overline{G}$. The group $\overline{G}$ has class 6 and it is a p-obelisk, by Lemma 435. Let now $x \in G$ be as in Lemma 436 and set $\ell = \langle \overline{xG_2} \rangle$, which is a 1-dimensional subspace of $\overline{G}/\overline{G}_2$. Let moreover

$$\rho_1^1 : \overline{G}/\overline{G}_2 \to \overline{G_3}/\overline{G}_4$$

and

$$\gamma_{1,2} : \overline{G}/\overline{G}_2 \times \overline{G_2}/\overline{G_3} \to \overline{G}_3/\overline{G}_4$$

denote the maps from Lemma 328. As a consequence of Lemma 436, the elments $\rho_1^1(\ell)$ and $\gamma_{1,2}(\{\ell\} \times \overline{G}_2/\overline{G}_3)$ generate a 1-dimensional subspace ℓ' of $\overline{G}_3/\overline{G}_4$. By Lemma 322(1), the width $\mathrm{wt}_{\overline{G}}(3)$ is equal to 2 so ℓ' is different from $\overline{G}_3/\overline{G}_4$. Proposition 336 yields that $\overline{G}$ is not framed. ∎

13.4.2 The second group

Let $p > 3$ be a prime number and let $t \in \mathbb{Z}_p$ be a quadratic non-residue modulo p. Define Δ_p to be $\left(\frac{t\,,\,p}{\mathbb{Z}_p}\right)$, i.e., the quaternion algebra

$$\Delta_p = \mathbb{Z}_p \oplus \mathbb{Z}_p\mathrm{i} \oplus \mathbb{Z}_p\mathrm{j} \oplus \mathbb{Z}_p\mathrm{k}$$

with defining relations

$$\mathrm{i}^2 = t,\ \mathrm{j}^2 = p,\ \text{ and } \mathrm{k} = \mathrm{ij} = -\mathrm{ji}.$$

The quaternion algebra Δ_p is equipped with a bar map, defined by

$$x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \ \mapsto\ \overline{x} = a - b\mathrm{i} - c\mathrm{j} - d\mathrm{k},$$

which is an anti-homomorphism of order 2. The algebra Δ_p has, in addition, a unique maximal (left/right/two-sided) ideal $\mathfrak{m}$, which is principal generated by j, i.e. $\mathfrak{m} = \Delta_p\,\mathrm{j}$. It follows that an element $x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ belongs to $\mathfrak{m}$ if and only if both a and b belong to $p\mathbb{Z}_p$. Moreover, for each $k \in \mathbb{Z}_{\geq 1}$, the ideal $\mathfrak{m}^k$ is principal generated by j^k and therefore, for each $s \in \mathbb{Z}_{\geq 0}$, one has

$$\mathfrak{m}^{2s} = p^s\Delta_p \ \text{ and } \ \mathfrak{m}^{2s+1} = p^s\mathfrak{m}.$$

As a result, for each $k \in \mathbb{Z}_{\geq 1}$, the quotient $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a vector space over $\mathbb{F}_p$ of dimension 2. Now, for each $k \in \mathbb{Z}_{\geq 1}$, the set $1+\mathfrak{m}^k$ is easily seen to be a subgroup of Δ_p^* and the natural map $(1+\mathfrak{m}^k)/(1+\mathfrak{m}^{k+1}) \to \mathfrak{m}^k/\mathfrak{m}^{k+1}$ is an isomorphism of groups. It follows that $1+\mathfrak{m}$ is a pro-p-subgroup of Δ_p^*. Define

$$\mathrm{S}(\Delta_p) = (1+\mathfrak{m}) \cap \{x \in \Delta_p : \overline{x} = x^{-1}\}.$$

Then $\mathrm{S}(\Delta_p)$ is a closed subgroup of $1+\mathfrak{m}$ and thus a pro-p-group itself. We have here lightened the notation from [GSK09], where the group $\mathrm{S}(\Delta_p)$ is denoted by $\mathrm{SL}_1^1(\Delta_p)$.

Lemma 438. *Let $p > 3$ be a prime number and let $G = \mathrm{S}(\Delta_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for each $k \in \mathbb{Z}_{\geq 1}$, one has $G_k = (1+\mathfrak{m}^k) \cap G$.*

Proof. We sketch here the proof, but leave out the computations. For all $i \in \mathbb{Z}_{\geq 1}$, denote $M_i = (1+\mathfrak{m}^i) \cap G$. We remark that all M_i are normal in G and they form a base of open neighbourhoods of 1 in G. It is easy to check that $(M_i)_{i\geq 1}$ is a central series, in other words for all $i \in \mathbb{Z}_{\geq 1}$ the subgroup $[M_1, M_i]$ is contained in M_{i+1}. As a consequence of Lemma 22, for each index i, the commutator map induces a bilinear map $\gamma_i : M_1/M_2 \times M_i/M_{i+1} \to M_{i+1}/M_{i+2}$. Next, by direct computation, one gets that, for every $i \in \mathbb{Z}_{\geq 1}$, the image of γ_i generates M_i/M_{i+1}, and therefore $M_{i+1} = [M_1, M_i]M_{i+2}$. Fix i. By induction one shows that, for each positive integer n, one has $M_{i+1} = [M_1, M_i]M_{i+n}$, and hence

$$M_{i+1} = \bigcap_{n\geq 1} [M_1, M_i]M_{i+n} = \mathrm{cl}([M_1, M_i]).$$

Since $M_1 = G$, we get that $M_{i+1} = \mathrm{cl}([G, G_i]) = G_{i+1}$. The choice of i being arbitrary, the proof is complete. ∎

Lemma 439. *Let $p > 3$ be a prime number and let $G = \mathrm{S}(\Delta_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for each $i \in \mathbb{Z}_{\geq 1}$, the map $x \mapsto x^p$ on G induces an isomorphism $\rho_i : G_i/G_{i+1} \to G_{i+2}/G_{i+3}$.*

Proof. By Lemma 438, given any positive integer i, one has $G_i = (1 + \mathfrak{m}^i) \cap G$. Fix $i \in \mathbb{Z}_{\geq 1}$ and let $1 + x$ be an element of G_i. One shows that $(1 + x)^p \equiv 1 + px \bmod G_{i+3}$. It is now easy to conclude. ∎

Lemma 440. *Let $p > 3$ be a prime number and let $G = \mathrm{S}(\Delta_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Let $x \in G \setminus G_2$ and let $y \in G_2 \setminus G_3$. Then G_3 is generated by x^p and $[x, y]$ modulo G_4.*

Proof. Straightforward computation. ∎

We remind the reader that, as defined in Chapter 10, a p-obelisk is a finite non-abelian p-group G such that $|G : G_3| = p^3$ and $G^p = G_3$. A p-obelisk is said to be framed if, for each maximal subgroup M of G, one has $\Phi(M) = G_3$.

Lemma 441. *Let $p > 3$ be a prime number and let $G = \mathrm{S}(\Delta_p)$. Denote by $(G_i)_{i\geq 1}$ the lower central series of G. Then, for each $k \in \mathbb{Z}_{\geq 3}$, the quotient G/G_k is a framed p-obelisk.*

Proof. Let $k \in \mathbb{Z}_{\geq 3}$ and denote $\overline{G} = G/G_k$. The group $\overline{G}$ is non-abelian and it is finite. Moreover, as a consequence of Lemma 438, one can easily compute that $|\overline{G} : \overline{G}_3| = |G : G_3| = p^3$ and, thanks to Lemma 439, one has $\overline{G}^p = \overline{G}_3$. It follows that $\overline{G}$ is a p-obelisk. To show that $\overline{G}$ is framed, combine Lemma 440 and Proposition 336. ∎

Lemma 442. *Let $p > 3$ be a prime number and let $G = \mathrm{S}(\Delta_p)$. Let moreover $\alpha : G \to G$ be defined by*

$$a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \;\mapsto\; a + b\mathrm{i} - c\mathrm{j} - d\mathrm{k}.$$

Then α is a continuous automorphism of G and the map $G/G_2 \to G/G_2$ that is induced by α is equal to the inversion map $a \mapsto a^{-1}$.

Proof. The map α coincides with conjugation by i and it is therefore a continuous automorphism. Moreover, thanks to Lemma 438, the subgroup G_2 coincides with $(1+\mathfrak{m}^2)\cap G$. Since each element x of G can be written in the form $x = 1+c\mathrm{j}+d\mathrm{k}+m$, with $c, d \in \mathbb{Z}_p$ and $m \in \mathfrak{m}^2$, we get that $\alpha(x) \equiv \overline{x} \bmod G_2$. The elements $\overline{x}$ and x^{-1} being equal, it follows that $\alpha(x) \equiv x^{-1} \bmod G_2$. ∎

Lemma 443. *Let $p > 3$ be a prime number and let $G = \mathrm{S}(\Delta_p)$. Define moreover $\alpha : G \to G$ by*

$$a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \;\mapsto\; a + b\mathrm{i} - c\mathrm{j} - d\mathrm{k}.$$

Then α is a topologically intense automorphism of G of order 2 and $\mathrm{int}(G) = 2$.

Proof. By Lemma 442, the map α is a continuous automorphism of G and, by its definition, it clearly has order 2. We prove that α is topologically intense. To this end, let H be an open subgroup of G. As a consequence of Lemma 430, there exists a positive integer k such that G_k is contained in H. Fix such integer k and define $K = \max\{k, 4\}$. Denote $\overline{G} = G/G_K$ and use the bar notation for the subgroups of $\overline{G}$. Denote moreover by α_K the automorphism that is induced on $\overline{G}$ by α. Then α_K induces the inversion map on $\overline{G}/\overline{G_2}$, as a consequence of Lemma 442 and the definition of α_K. Moreover, the class of $\overline{G}$ is at least 3 so, thanks to Lemma 441, the group $\overline{G}$ is a framed obelisk. It follows from Theorem 344 that α_K is intense, so there exists $g \in G$ such that $\alpha_K(\overline{H}) = \overline{gHg^{-1}}$. Furthermore, we have that $\alpha(H) = gHg^{-1}$ and, the choice of H being arbitrary, it follows from Proposition 423 that α is topologically intense. In particular, $\mathrm{int}(G)$ is even. The intensity of G is equal to 2, as a consequence of Proposition 424 and Theorem 125. ∎

13.5 Non-abelian groups, part II

The aim of this section is to give a proof of the following proposition.

Proposition 444. *Let $p > 3$ be a prime number and let P be a non-abelian infinite pro-p-group. Assume that* $\mathrm{int}(P) > 1$*. Then P is topologically isomorphic to* $\mathrm{S}(\Delta_p)$*.*

Until the end of Section 13.5, let the following assumptions be valid. Let $p > 3$ be a prime number and let P be an infinite non-abelian pro-p-group of intensity greater than 1. Let $(P_i)_{i\geq 1}$ denote the lower central series of P, as defined in Section 13.1, and let α be a topologically intense automorphism of P of order 2, which exists thanks to Proposition 424. In the proof of Proposition 444, we will make heavy use of results coming from Chapters 10 and 11.

Definition 445. *Let G be a group. The* derived series $(G^{(i)})_{i\geq 0}$ *of G is defined recursively by*

$$G^{(0)} = G \quad \textit{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

The group G is solvable *if there exists $k \in \mathbb{Z}_{\geq 0}$ such that $G^{(k)} = \{1\}$.*

Lemma 446. *Every solvable just-infinite pro-p-group other than $\mathbb{Z}_p$ has torsion.*

Proof. This is Proposition 6.1 in [GSK09]. ∎

We remind the reader that, for each prime number $p > 3$, the groups $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ and $\mathrm{S}(\Delta_p)$ have been defined in Section 13.4.

Lemma 447. *Let $p > 3$ be a prime number and let G be a p-adic analytic group. Assume that* $\dim(G) = 3$ *and that G is both torsion-free and non-solvable. Then G is topologically isomorphic to an open subgroup of* $\mathrm{S}(\Delta_p)$ *or* $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$.

Proof. See [GSK09, Section 7.3]. ∎

Lemma 448. *The group P is topologically isomorphic to an open subgroup of* $\mathrm{S}(\Delta_p)$ *or* $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$.

Proof. The group P is a just-infinite p-adic analytic group of dimension 3, by Proposition 426. By Lemma 433, the torsion of P is trivial and so, by Lemma 446, the group P is not solvable. It follows from Lemma 447 that P is isomorphic to an open subgroup of $\mathrm{S}(\Delta_p)$ or $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. ∎

Lemma 449. *The group P is topologically isomorphic to* $\mathrm{S}(\Delta_p)$ *or* $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$.

Proof. Let $G \in \{\mathrm{S}(\Delta_p), \mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)\}$ and let $(G_i)_{i\geq 1}$ denote the lower central series of G. From the combination of Lemmas 435 and 441, we know that, for each $k \geq 3$, the quotient G/G_k is a p-obelisk. Let now H be an open subgroup of G, such that P is topologically isomorphic to H. The existence of H is ensured by Lemma 448. By Lemma 429, the group H has discrete quotients of any class and, thanks to Lemma 428, each such quotient, of class at least 4, is a p-obelisk. The subgroup H being open, it follows from Lemma 430 that there exists $k \in \mathbb{Z}_{>4}$ such that G_k is contained in H so H/G_k is a p-obelisk. Proposition 337 yields $G = H$. ∎

Lemma 450. *Each discrete quotient of P of class at least* 6 *is a framed p-obelisk.*

Proof. Let $\overline{G}$ be a discrete quotient of P of class at least 6. By Lemma 427, the map α induces an intense automorphism of order 2 on $\overline{G}$ and, by Lemma 428, the group $\overline{G}$ is a p-obelisk. By Lemma 322(1), the number $\mathrm{wt}_{\overline{G}}(5)$ is equal to 2 so, by Theorem 375, the p-obelisk $\overline{G}$ is framed. ∎

We are finally ready to give the proof of Proposition 444. Thanks to Lemma 449, there are only two possibilities for the isomorphism type of P: that of $\mathrm{S}(\Delta_p)$ or that of $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$. By Lemma 450, every discrete quotient of P of class 6 is a framed p-obelisk so, in view of Lemma 437, the group $\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$ is not isomorphic to P. It follows that P is topologically isomorphic to $\mathrm{S}(\Delta_p)$ and so the proof of Proposition 444 is complete.

13.6 Proving the main theorems and more

In Sections 13.6.1 and 13.6.2 we prove respectively Theorem 405 and Theorem 406. The last two theorems are the most important results of Chapter 13: we are able to draw a bridge between the two thanks to Proposition 451, which is proven in Section 13.6.3.

13.6.1 The proof of Theorem 405

Let p be a prime number. As a consequence of Proposition 424, the intensity of a pro-p-group divides $p-1$ and so there are no pro-2-groups of intensity greater than 1. Assume now that p is odd. Then, thanks to Corollary 425, each infinite abelian pro-p-group has intensity $p-1$, which, p being odd, is greater than 1. Let now G be a non-abelian infinite pro-p-group with $\operatorname{int}(G) > 1$. Then G has a discrete quotient of any class, thanks to Lemma 429, so Theorem 231 yields that p is larger than 3. By Proposition 444, the group G is topologically isomorphic to $\mathrm{S}(\Delta_p)$, which, by Lemma 443, has indeed intensity 2. The proof of Theorem 405 is now complete.

13.6.2 The proof of Theorem 406

Let $p > 3$ be a prime number and let c be a positive integer. Write $P = \mathrm{S}(\Delta_p)$ and let $(P_i)_{i\geq 1}$ denote the lower central series of P, as defined in Section 13.1. Then the group P/P_{c+1} has class c and it is finite, as a consequence of Lemma 430. The group P being a pro-p-group, P/P_{c+1} is a finite p-group. Moreover, by Theorem 405, the intensity of P is greater than 1 and so, thanks to Proposition 424, we get $\operatorname{int}(P/P_{c+1}) > 1$. The number c was chosen arbitrarily and therefore Theorem 406 is proven.

13.6.3 A bridge between finite and infinite

The purpose of Section 13.6.3 is to compare, for a fixed prime $p > 3$, the finite p-groups of intensity greater than 1 with the discrete quotients of $\mathrm{S}(\Delta_p)$.

Proposition 451. *Let $p > 3$ be a prime number and write $P = \mathrm{S}(\Delta_p)$. Denote by $(P_i)_{i\geq 1}$ the lower central series of P. Then there exists a function $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ with the following properties.*

1. *One has $\lim_{c\to\infty} f(c) = \infty$.*
2. *For each finite p-group G of class c with $\operatorname{int}(G) > 1$, the quotients $G/G_{f(c)}$ and $P/P_{f(c)}$ are isomorphic.*

Proof. For each positive integer c, let $\operatorname{Int}(p, c)$ denote the collection of all finite p-groups of class c and intensity greater than 1. We define $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ by mapping each element $c \in \mathbb{Z}_{>0}$ to the maximum index $m \in \mathbb{Z}_{>0}$ for which, whenever $G \in \operatorname{Int}(p, c)$, the quotients G/G_m and P/P_m are isomorphic. The map f is well-defined, thanks to Theorem 406, and it follows directly from the definition of f that (2) is satisfied. Moreover, thanks to Lemma 101, the function f is non-decreasing. We prove (1) by contradiction. Let $C \in \mathbb{Z}_{\geq 0}$ be such that, for all $c \geq C$, one has $f(c) = f(C)$. In other words, for each $c \in \mathbb{Z}_{\geq C}$, there exists

$G \in \mathrm{Int}(p, c)$ such that $G/G_{f(C)}$ and $P/P_{f(C)}$ are isomorphic, but $G/G_{f(C)+1}$ and $P/P_{f(C)+1}$ are not. For all $c \geq C$, call X_c the collection of such G and note that, for each $c \geq C$, the set X_c is non-empty. Thanks to Lemma 101, for each $c \in \mathbb{Z}_{>C}$, we have a natural map $X_{c+1} \to X_c$, which is defined by $G \mapsto G/G_{c+1}$. The collection $\{X_c\}_{c>C}$ is thus an inverse system of non-empty sets. As a consequence of Theorem 124, the constant C is at least 3 and so, for each $c > C$, Theorem 218 yields that X_c is finite. By Lemma 422, the set $X = \varprojlim_{c>C} X_c$ is non-empty and therefore there exists an infinite non-abelian pro-p-group of intensity larger than 1 and which is, by construction, not isomorphic to P. Contradiction to Theorem 405. It follows that (2) is satisfied and the proof is complete. ∎

Proposition 451 is the last result of this thesis and, in summary, it states that, for $p > 3$, each finite p-group G with $\mathrm{int}(G) > 1$ shares a "relatively big" quotient (growing in size with the class of G) with the infinite group $\mathrm{S}(\Delta_p)$. One can then ask: if $p > 3$ and G is a finite p-group of intensity greater than 1, then "how far is G from being a quotient of $\mathrm{S}(\Delta_p)$"? More precisely, if G is a finite p-group of class c with $\mathrm{int}(G) > 1$ and f is as in Proposition 451, then what is the average size of $G_{f(c)}$? Is there an absolute constant B such that, for each $c \in \mathbb{Z}_{>0}$ and for each finite p-group G of class c and intensity greater than 1, one has $|G_{f(c)}| \leq p^B$? In view of Theorem 375, we can surely answer this question if we manage to classify, for each given prime $p > 3$, all framed p-obelisks that have an automorphism of order 2 that induces the inversion map on the Frattini quotient of the group.

Bibliography

[Ben27] H. A. Bender. A determination of the groups of order p^5. *Ann. of Math. (2) no. 1-4*, 1927.

[Bla61] N. Blackburn. Generalization of certain elementary theorems on p-groups. *Proc. London Math. Soc. (3)*, 11:1–22, 1961.

[Coh07] H. Cohen. *Number theory, Volume I: Tools and Diophantine equations.* Graduate Texts in Mathematics, 239. Springer, 2007.

[DdSMS91] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p-groups.* London Mathematical Society Lecture Note Series, 157. Cambridge University Press, 1991.

[GSK09] J. Gonzalez-Sanchez and B. Klopsch. Analytic pro-p-groups of small dimensions. *J. Group Theory*, 12:711–734, 2009.

[GT06] P. Gille and Szamuely T. *Central simple algebras and Galois cohomology.* Cambridge Studies in Advanced Mathematics, 101. Cambridge University Press, 2006.

[Hup67] B. Huppert. *Endliche Gruppen I.* Springer-Verlag, 1967.

[Isa08] M. Isaacs. *Finite group theory.* Graduate Studies in Mathematics, 92. American Mathematical Society, 2008.

[KLGP97] G. Klaas, C. R. Leedham-Green, and W. Plesken. *Linear pro-p-groups of finite width.* Lecture Notes in Mathematics, 1674. Springer-Verlag, 1997.

[Laf73] T. J. Laffey. The minimum number of generators of a finite p-group. *Bull. London Math. Soc.*, 5:288–290, 1973.

[LT58] S. Lang and J. Tate. Principal homogeneous spaces over abelian varieties. *Amer. J. Math.*, 80:659–684, 1958.

[RZ10] L. Ribes and P. Zalesski. *Profinite groups. Second edition.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 40. Springer-Verlag, 2010.

[Sta13] M. Stanojkovski. Evolving groups. Master's thesis, retrieved from http://www.math.leidenuniv.nl/nl/theses/358/, 2013.

Index