Mima Stanojkovski

EVOLVING GROUPS

Master thesis supervised by
Prof. Dr. Hendrik Willem Lenstra Jr.

Academic year 2012–2013

Contents

A day without laughter is a day wasted.
Charlie Chaplin.

Introduction

Let G be a finite group. We say that G is an *evolving group* if for every prime number p and for every p-subgroup I of G there exists a subgroup J of G that contains I and such that $|G : J|$ is a p-power and $|J : I|$ is coprime to p. The following theorem is the starting point of the whole paper.

Theorem A. *Let G be a finite group. Then the following are equivalent.*

1. *For every G-module M, integer q, and $c \in \widehat{\mathrm{H}}^q(G, M)$, the minimum of the set $\{|G : H| \mid H \leq G \text{ with } c \in \ker \mathrm{Res}^G_H\}$ coincides with its greatest common divisor.*

2. *For every G-module M and for every $c \in \widehat{\mathrm{H}}^0(G, M)$ the minimum of the set $\{|G : H| \mid H \leq G \text{ with } c \in \ker \mathrm{Res}^G_H\}$ coincides with its greatest common divisor.*

3. *The group G is an evolving group.*

Section 1 is devoted to the proof of this result, which allows us to translate a purely cohomological requirement in terms of a group theoretical problem. We remark that condition (1) is inspired by a phenomenon that occurs in Galois cohomology.

The following result is a simplified version of the main theorems given in Sections 2 and 3.

Theorem B. *Let G be an evolving group. Then G is supersolvable and it is isomorphic to the semidirect product of two nilpotent groups of coprime orders.*

In Section 2 we investigate the main properties of evolving groups and define some new concepts in order to prove that evolving groups are supersolvable. We show that the property of being evolving is inherited by normal subgroups and quotients and we prove moreover that every evolving group has a collection of Sylow subgroups satisfying a special condition. In Section 2 we give also a second characterization of evolving groups that involves supersolvability.

The aim of Section 3 is to give a concrete description of every evolving group by means of a directed graph associated to the group. The second part of Theorem B follows from the main theorem given in this section. We conclude the section and the paper by giving an example of an evolving group with a non-evolving subgroup, which shows that the property of being evolving is not inherited by arbitrary subgroups. This example shows moreover that the converse of Theorem B is not valid.

1 Evolving groups

In this section we state and prove our first important result, which characterizes the finite groups that satisfy a certain cohomological condition. Before stating the theorem we give a new definition.

Definition 1. *Let G be a finite group and let I be a p-subgroup of G, where p is a prime number. If J is a subgroup of G containing I, for which $|G : J|$ is a p-power and p does not divide $|J : I|$, we say that J is a p-*evolution *of I in G.*

Theorem 2. *Let G be a finite group. Then the following are equivalent.*

1. *For every G-module M, integer q, and $c \in \widehat{\mathrm{H}}^q(G, M)$, the minimum of the set $\{|G : H| \mid H \leq G \text{ with } c \in \ker \mathrm{Res}^G_H\}$ coincides with its greatest common divisor.*

2. *For every G-module M and for every $c \in \widehat{\mathrm{H}}^0(G, M)$ the minimum of the set $\{|G : H| \mid H \leq G \text{ with } c \in \ker \mathrm{Res}^G_H\}$ coincides with its greatest common divisor.*

3. *For every prime p, if I is a p-subgroup of G, then I has a p-evolution J in G.*

We will start building the proof for this theorem for the case in which the cocycles have order equal to a power of a prime. For this purpose we recall here Corollary 4 from [1, Ch. 4] and emphasize that we will mostly refer to Chapter 4 from [1] for the concepts concerning group cohomology.

Lemma 3. *Let G be a finite group, let M be a G-module, and let q be an integer. Let furthermore c be an element of $\widehat{\mathrm{H}}^q(G, M)$ and assume that, for all Sylow subgroups S of the group, c restricts to zero in $\widehat{\mathrm{H}}^q(S, M)$. Then $c = 0$.*

In the previous lemma, it suffices to choose, for every prime number p, a Sylow p-subgroup S_p of G and verify the hypothesis for the chosen family $(S_p)_p$. This is a direct consequence of the following result.

Lemma 4. *Let G be a finite group, q an integer, and M a G-module. Let moreover H be a subgroup of G and g be an element of G. Then there exists a commutative diagram*

$$\begin{tikzcd}
\widehat{\mathrm{H}}^q(G, M) \arrow[r, "\mathrm{id}"] \arrow[d, "\mathrm{Res}^G_H"'] & \widehat{\mathrm{H}}^q(G, M) \arrow[d, "\mathrm{Res}^G_{gHg^{-1}}"] \\
\widehat{\mathrm{H}}^q(H, M) \arrow[r, "f"] & \widehat{\mathrm{H}}^q(gHg^{-1}, M)
\end{tikzcd}$$

where f is an isomorphism of groups.

Proof. Let us consider the category $\mathcal{C}$ of compatible pairs defined in [5, Ch.1, §6]. Let moreover $\mathrm{F}_q^* : \mathcal{C} \to \mathrm{Ab}$ be the map which sends any object $(G, M) \in \mathcal{C}$ to $\widehat{\mathrm{H}}^q(G, M)$ and any morphism $(\varphi, \psi) : (G_1, M_1) \to (G_2, M_2)$ to the homomorphism $(\varphi, \psi)_q^* : \widehat{\mathrm{H}}^q(G_1, M_1) \to \widehat{\mathrm{H}}^q(G_2, M_2)$ given by Proposition 2.2.3 in [4]. Thanks to Theorem 2.1.8 in [4], the map F_q^* is a functor for all q. Let us now consider the pairs (G, M), (H, M), (gHg^{-1}, M) and the morphisms that are collected in the commutative diagram

$$\begin{tikzcd}
(G, M) \arrow[r, "(\varphi,\psi)"] \arrow[d, "(i,\mathrm{id})"'] & (G, M) \arrow[d, "(i,\mathrm{id})"] \\
(H, M) \arrow[r, "(\varphi_{|gHg^{-1}},\psi)"] & (gHg^{-1}, M)
\end{tikzcd}$$

where i denotes the inclusion of H in G and $(\varphi, \psi) = (x \mapsto g^{-1}xg, m \mapsto gm)$. We now observe that $(\varphi, \psi) : (G, M) \to (G, M)$ is sent to the identity morphism in Ab, thanks to Proposition 3 in [1, Ch.4] (dimension shifting ensures the result for Tate groups), and the image under F_q^* of our commutative diagram preserves commutativity and isomorphisms because F_q^* is a functor. To conclude, we call $f = (\varphi_{|gHg^{-1}}, \psi)_q^*$ and observe it is an isomorphism because $(\varphi_{|gHg^{-1}}, \psi)$ is an isomorphism in $\mathcal{C}$. The image in Ab of the diagram we constructed gives us therefore the required commutative diagram. ∎

Given a group G and a prime number p, we will denote by $\mathrm{Syl}_p(G)$ the set of all Sylow p-subgroups of G. We now state a partial result.

Lemma 5. *Let G be a finite group, let M be a G-module, and let q be an integer. Let moreover p be a prime number, $c \in \widehat{\mathrm{H}}^q(G, M)$ be of order a power of p and assume every p-subgroup of G has a p-evolution in G. Then the minimum of the set $\{|G : H| \mid H \leq G \ \text{ with } \ c \in \ker \mathrm{Res}^G_H\}$ coincides with its greatest common divisor and it is a p-power.*

Proof. If l is a prime different from p and $S_l \in \mathrm{Syl}_l(G)$, then $\mathrm{Res}^G_{S_l}(c)$ is annihilated by a power of l, but $\mathrm{Res}^G_{S_l}(c)$ is also annihilated by a power of p and so the restriction of c to S_l must be zero. Let now H_p be a p-subgroup of G such that $\mathrm{Res}^G_{H_p}(c) = 0$ and the order of H_p is maximal; then by assumption we can find a p-evolution J_p of H_p in G. The subgroup H_p is a Sylow p-subgroup of J_p on which c vanishes and c is also zero restricted to all Sylow subgroups of J_p associated to prime numbers different from p, because they are Sylow subgroups of G. By Lemma 3, we have $\mathrm{Res}^G_{J_p}(c) = 0$. To conclude, we show that the index $|G : J_p|$ is the greatest common divisor of the set $\{|G:H| \mid H \leq G \ \text{ with } \ c \in \ker \operatorname{Res}^G_H\}$ and so it equals its minimum, too. Let us take $H \leq G$ such that $\operatorname{Res}^G_H(c) = 0$; in particular, c restricts to zero on every Sylow p-subgroup P of H. By the maximality of H_p, the order of P divides the order of H_p and so, for every prime number q, the quantity $\operatorname{ord}_q |H|$ divides $\operatorname{ord}_q |J_p|$. It follows that the order of H divides the order of J_p, in other words, $|G : J_p|$ divides $|G : H|$. Moreover, since J_p is a p-evolution of a p-group, its index in G is a power of p. ∎

Thanks to this Lemma, it is now easy to prove that (3) implies (1) in Theorem 2. Given a group G, a G-set X and an element $x \in X$, we will denote by Gx the orbit of x in X and by G_x the stabilizer of x in G. We will denote by $G\backslash X$ the set of orbits in X with respect to the left G-action.

Lemma 6. *Let G be a finite group and let $\mathcal{H}$ be a non-empty family of subgroups in which every two elements have coprime index in G. Then $|G : \bigcap_{H\in\mathcal{H}} H|$ equals $\prod_{H\in\mathcal{H}} |G : H|$.*

Proof. Let us call K the intersection of all elements of $\mathcal{H}$ and let us consider the map $G/K \to \prod_{H\in\mathcal{H}} G/H$ defined by $gK \mapsto (gH)_{H\in\mathcal{H}}$.The map is well defined because K is contained in every $H \in \mathcal{H}$. We now observe that two elements gK and fK in G/K have the same image in $\prod_{H\in\mathcal{H}} G/H$ if and only if, for every $H \in \mathcal{H}$, the element $f^{-1}g$ belongs to H, which occurs if and only if $f^{-1}g$ belongs to K. It follows that $fK = gK$ and the map is injective, in particular $|G : K| \leq \prod_{H\in\mathcal{H}} |G : H|$. We now want to show that the reversed inequality is true as well. By definition of K we know that $|G : H|$ divides $|G : K|$ for all $H \in \mathcal{H}$ and therefore, since every two elements of $\mathcal{H}$ have coprime index, the product $\prod_{H\in\mathcal{H}} |G : H|$ divides $|G : K|$. In particular, $\prod_{H\in\mathcal{H}} |G : H| \leq |G : K|$. ∎

Lemma 7. *Let G be a finite group and let M be a G-module. Furthermore, let q be an integer and let $c \in \widehat{\mathrm{H}}^q(G, M)$. Assume moreover that, for every prime p, every p-subgroup of G has a p-evolution in G. Then the minimum of the set $\{|G : H| \mid H \leq G \ \text{ with } \ c \in \ker \operatorname{Res}^G_H\}$ equals its greatest common divisor.*

Proof. The group $\widehat{\mathrm{H}}^q(G, M)$ is an abelian group of exponent dividing the order of G and therefore we can write uniquely c as $\sum_{p||G|} c_p$ where each c_p belongs to the p-primary component of $\widehat{\mathrm{H}}^q(G, M)$. By Lemma 5, for every prime p, there exists a subgroup $J_p \leq G$ such that $|G : J_p|$ is a p-power and it is both the minimum and the greatest common divisor of the set $\{|G : H| \mid H \leq G \ \text{ with } \ c_p \in \ker \operatorname{Res}^G_H\}$. We now define $L = \bigcap_{p||G|} J_p$ and we observe that $\operatorname{Res}^G_L(c) = 0$; indeed each c_p vanishes on J_p and so on $\bigcap_{p||G|} J_p$, too. We now claim that $|G:L|$ divides the index in G of every subgroup on which the restriction of c vanishes. Let indeed K be a subgroup of G such that $\mathrm{Res}^G_K(c) = 0$; in particular, for every prime p, we have that $\mathrm{Res}^G_K(c_p) = 0$. It follows, for each prime number p, that $|G : J_p|$ divides $|G : K|$ and, since J_p and J_q have coprime indices in G whenever $p \neq q$, we have that $\prod_{p||G|} |G : J_p|$ divides $|G : K|$. To conclude, by Lemma 6 we have that $|G : L| = |G : \bigcap_{p||G|} J_p| = \prod_{p||G|} |G : J_p|$ and so $|G : L|$ divides $|G : K|$. ■

To prove the other direction, we will work with a specific kind of G-modules, which we introduce here.

Definition 8. *Let G be a group and let X be a finite G-set. We define $M = \mathbb{Z}^X$ and we give it a left G-module structure by defining, for all $f \in \mathbb{Z}^X$, $g \in G$, $x \in X$, the G-action $(gf)(x) = f(g^{-1}x)$. We call M a* permutation module *(over $\mathbb{Z}[G]$).*

Thanks to this construction we get that $f \in \mathrm{H}^0(G, M)$ if and only if, for any choice of $x \in X$ and $g \in G$, it holds $f(x) = (gf)(x) = f(g^{-1}x)$. In particular the group $\mathrm{H}^0(G, M)$ of the G-fixed elements in M equals the set of functions $X \to \mathbb{Z}$ that are constant on each G-orbit.

Proposition 9. *Let G be a finite group, X be a finite G-set and M the permutation module associated to X. Then the map $\gamma_G : \widehat{\mathrm{H}}^0(G, M) \to \bigoplus_{Gx \in G\backslash X} \mathbb{Z}/|G_x|\mathbb{Z}$ defined by $[f] \mapsto (f(x) \bmod |G_x|)_{Gx \in G\backslash X}$ is an isomorphism of groups. Moreover, if H is a subgroup of G, then the following diagram is commutative*

$$\begin{array}{ccc}
\widehat{\mathrm{H}}^0(G, M) & \xrightarrow{\gamma_G} & \bigoplus_{Gx \in G\backslash X} \mathbb{Z}/|G_x|\mathbb{Z} \\
{\scriptstyle \mathrm{Res}^G_H}\downarrow & & \downarrow{\scriptstyle \pi} \\
\widehat{\mathrm{H}}^0(H, M) & \xrightarrow{\gamma_H} & \bigoplus_{Gx \in G\backslash X} \bigoplus_{Hy \in H\backslash Gx} \mathbb{Z}/|H_y|\mathbb{Z}
\end{array}$$

where π is the projection map, which, restricted to each Gx-th direct summand, sends $m \bmod |G_x|$ to $(m \bmod |G_y|)_{Hy \in H\backslash Gx}$.

Proof. The map γ_G is well defined; indeed if $x \in X$, $\phi \in M$ and $f \in \mathrm{H}^0(G, M)$ then $(f + \sum_{g \in G} g\phi)(x) = f(x) + (\sum_{g \in G} g\phi)(x) = f(x) + \sum_{g \in G} \phi(g^{-1}x) = f(x) + \sum_{G_x g \in G_x\backslash G} |G_x|\phi(g^{-1}x) \equiv f(x) \bmod |G_x|$. Now it can be easily checked that γ_G is a group homomorphism; let us check it is injective. Let $f \in \mathrm{H}^0(G, M)$ be such that $[f] \mapsto 0$. This means that for all $Gx \in G\backslash X$ we have that $|G_x|$ divides $f(x)$, i.e. there exists some $\phi_x \in \mathbb{Z}$ such that $f(x) = |G_x|\phi_x$. Let us now choose a representative x for each orbit Gx and define $\phi : X \to \mathbb{Z}$

by sending x to ϕ_x and all other elements of its orbit to 0; we get that $[f] = [(\sum_{g\in G} g)\phi] = [0]$.

To show the map is surjective and that the above diagram is commutative is an easy exercise. ∎

From now on, to lighten the notation, we will identify every element $c \in \widehat{\mathrm{H}}^0(G, M)$, for a fixed permutation module M, with its image under γ_G and we will always consider its restriction to a subgroup H of G to be $\pi\gamma_G(c)$.

Lemma 10. *Let G be a finite group, let K be a subgroup of G and put $M = \mathbb{Z}^{G/K}$. Let $m \in \widehat{\mathrm{H}}^0(G, M)$ and let H be a subgroup of G. Then m is zero restricted to H if and only if for all $g \in G$ there is $m_g \in \mathbb{Z}/|K|\mathbb{Z}$ such that $|gKg^{-1} \cap H|m_g \equiv m \mod |K|$.*

Proof. Let $m \in \widehat{\mathrm{H}}^0(G, M)$. By Proposition 9 the group $\widehat{\mathrm{H}}^0(G, M)$ is isomorphic to $\mathbb{Z}/|K|\mathbb{Z}$ and if $H \le G$, then $\mathrm{Res}^G_H(m) = 0$ if and only if, for all $g \in G$, there is $m_g \in \mathbb{Z}/|K|\mathbb{Z}$ such that $|H_{gK}|m_g \equiv m \mod |K|$. To conclude we observe that $H_{gK} = H \cap G_{gK} = H \cap gKg^{-1}$. ∎

Lemma 11. *Let G be a finite group and assume that, for every G-module M and for every $c \in \widehat{\mathrm{H}}^0(G, M)$, the minimum and the greatest common divisor of the set $\{|G : H| \mid H \le G \text{ with } c \in \ker \mathrm{Res}^G_H\}$ coincide. Then for every prime p and for every p-subgroup I of G there exists a p-evolution of I in G.*

For the proof of this last lemma we need an auxiliary result.

Lemma 12. *Let G be a finite group, let p be a prime number and let $\alpha \in \mathbb{Z}_{\ge 0}$. Let moreover I be a subgroup of G of order p^α, let S_p be a Sylow p-subgroup of G and let $\mathcal{L} = \{L \le G \mid |L| = |I| \text{ and } L \ne gIg^{-1} \text{ for all } g \in G\}$; define $M = \mathbb{Z}^{G/S_p} \oplus \left(\bigoplus_{L\in\mathcal{L}} \mathbb{Z}^{G/L}\right)$. Furthermore, let H be a subgroup of G and define $c = (m, (m_L)_{L\in\mathcal{L}}) \in \widehat{\mathrm{H}}^0(G, M)$ by*

$$\begin{cases} m = p^\alpha \bmod |S_p| \\ m_L = p^{\alpha-1} \bmod |L| \quad \text{for all} \quad L \in \mathcal{L}. \end{cases}$$

Then $\mathrm{Res}^G_H(c) = 0$ if and only if $\mathrm{ord}_p |H| \le \alpha$ and, if the equality holds, every Sylow p-subgroup of H is conjugate to I in G.

Proof. By Proposition 9 we have that $\widehat{\mathrm{H}}^0(G, M) \cong \mathbb{Z}/|S_p|\mathbb{Z} \oplus \left(\bigoplus_{L\in\mathcal{L}} \mathbb{Z}/|L|\mathbb{Z}\right)$ and if $\alpha = 0$ the collection $\mathcal{L}$ is empty. It follows that c is well defined and if $c = (m, (m_L)_{L\in\mathcal{L}}) \in \widehat{\mathrm{H}}^0(G, M)$, then the subgroups for which it restricts to zero are those for which each component restricts to zero. Now, by Lemma 10, we have that $\mathrm{Res}^G_H(m) = 0$ if and only if, for all $g \in G$, the order of

$H \cap gS_pg^{-1}$ divides p^α; in other words $\mathrm{Res}_H^G(m) = 0$ if and only if $\mathrm{ord}_p(H)$ is at most α. If $\alpha = 0$ we are clearly done, otherwise let us fix $L \in \mathcal{L}$. Then $\mathrm{Res}_H^G(m_L) = 0$ if and only if, for all $g \in G$, the order of $H \cap gLg^{-1}$ divides $p^{\alpha-1}$. If $\mathrm{ord}_p |H| \leq \alpha - 1$, this last condition is always satisfied; if $\mathrm{ord}_p |H| = \alpha$ it occurs if and only if H does not contain any conjugate of L. To conclude, we prove that, if $\mathrm{ord}_p |H| = \alpha$ then $\mathrm{Res}_H^G(c) = 0$ if and only if every Sylow p-subgroup of H is G-conjugate to I. In this case, by intersecting all the conditions, we get that $\mathrm{Res}_H^G(c) = 0$ if and only if, for every $L \in \mathcal{L}$, the subgroup H does not contain any G-conjugate of L; in other words, since the Sylow p-subgroups of H have the same order as I and $\mathcal{L}$ is the set of all subgroups of G that have the same order as I but are not G-conjugate to it, the Sylow p-subgroups of H must be G-conjugate to I. ∎

Proof of Lemma 11. Let p be a prime number and let I be a subgroup of order p^α for some $\alpha \in \mathbb{Z}_{\geq 0}$; we want to construct a p-evolution J of I. Let us fix a Sylow p-subgroup S_p of G and let $\mathcal{L}$ be as in Lemma 12. We want indeed to construct a module M and a cocycle $c \in \widehat{\mathrm{H}}^0(G, M)$ that give rise to a p-evolution of I; a good choice is to define $M = \mathbb{Z}^{G/S_p} \oplus \left(\bigoplus_{L\in\mathcal{L}} \mathbb{Z}^{G/L}\right)$ and get $\widehat{\mathrm{H}}^0(G, M) \cong \mathbb{Z}/|S_p|\mathbb{Z} \oplus \left(\bigoplus_{L\in\mathcal{L}} \mathbb{Z}/|I|\mathbb{Z}\right)$. Let now $c \in \widehat{\mathrm{H}}^0(G, M)$ be as in Lemma 12. From that lemma, we know that $\mathrm{Res}_I^G(c) = 0$, but the restriction is not zero for subgroups of higher p-power order, and $\mathrm{Res}_{S_l}^G(c) = 0$ for every prime number $l \neq p$ and for every $S_l \in \mathrm{Syl}_l(G)$. It follows that the greatest common divisor of the set $\{|G : H| \mid H \leq G \text{ with } c \in \ker \mathrm{Res}_H^G\}$ is $p^{\mathrm{ord}_p |G| - \alpha}$ and so by assumption there is a subgroup J' with index $|G : J'| = p^{\mathrm{ord}_p |G| - \alpha}$ such that $\mathrm{Res}_{J'}^G(c) = 0$. Moreover, J' does not contain any p-subgroup of order p^α which is not G-conjugate to I, thanks to Lemma 12. Hence, since $\mathrm{ord}_p |J'| = \alpha$, there is some $g \in G$ such that $gIg^{-1} \leq J'$; to conclude define $J = g^{-1}J'g$. ∎

Proof of Theorem 2. (1) ⇒ (2) Trivial. (2) ⇒ (3) Lemma 11. (3) ⇒ (1) Lemma 7. ∎

Definition 13. *Let G be a finite group. We say that G is an* evolving group *if it satisfies one of the equivalent conditions in* Theorem 2.

2 The supersolvability of evolving groups

In this section we prove some important properties of evolving groups and give a first characterization.

Definition 14. *Let G be a finite group and let $\mathcal{P}$ be the set of prime numbers that divide its order. We say that $(S_p)_{p\in\mathcal{P}}$ is a* Sylow family *of G if each S_p is a Sylow p-subgroup of G and S_q normalizes S_p whenever $q < p$.*

To lighten the notation, for every prime p dividing the order of G, when $(S_q)_{q\in\mathcal{P}}$ is a Sylow family, we will write L_p meaning $\langle S_q \mid p < q\rangle$ and T_p meaning $\langle S_q \mid q < p\rangle$. It is an easy exercise to show that, if $\mathcal{Q}$ is a subset of $\mathcal{P}$, then the subgroup $\langle S_q \mid q \in \mathcal{Q}\rangle$ has order $\prod_{q\in\mathcal{Q}} |S_q|$. It follows that, if G is a finite group with a Sylow family $(S_p)_{p\in\mathcal{P}}$, we have $G \cong L_p \rtimes (S_p \rtimes T_p)$. We will write simply $G = L_p \rtimes S_p \rtimes T_p$.

We give here a short summary of the properties of Sylow families we will use.

Definition 15. *Let G be a finite group. Then G is* supersolvable *if it has a series $1 = N_0 \leq N_1 \leq \ldots \leq N_t = G$ such that every N_i is a normal subgroup of G and, for all $i = 0, \ldots, t-1$, the quotient N_{i+1}/N_i is cyclic.*

Proposition 16. *Let G be a finite group. Then the following hold.*

1. *If G is supersolvable, then G has a Sylow family.*
2. *If G has a Sylow family, then it is unique up to conjugation. In other words, if $(S_p)_{p\in\mathcal{P}}$ and $(R_p)_{p\in\mathcal{P}}$ are two Sylow families then there exists $g \in G$ such that, for all $p \in \mathcal{P}$, we have $R_p = gS_pg^{-1}$.*

Proof. We will work by induction on the order of G. If G is the trivial group then $\mathcal{P}$ is empty and so we are done in both cases; we assume therefore G is non-trivial. Let us first prove (1). Let p be the largest prime dividing the order of G; since G is supersolvable, it has a unique normal Sylow p-subgroup S_p (see [3, Ch.10, §5]). By the Schur-Zassenhaus theorem, S_p has a complement T_p in G, which is isomorphic to G/S_p and so T_p is supersolvable. By induction, T_p has a Sylow family $(S_q)_{q\in\mathcal{P}\setminus\{p\}}$. By adding S_p to the Sylow family of T_p, we get a Sylow family of G. Let us now prove (2). Let p be the largest prime dividing the order of G; then G has a unique Sylow p-subgroup, so $S_p = R_p$. Moreover $T = \langle S_q \mid q < p\rangle$ and $T' = \langle R_q \mid q < p\rangle$ are complements of S_p in G; by the Schur-Zassenhaus theorem there is therefore $g \in G$ such that $T' = gTg^{-1}$. Now $(R_q)_{q<p}$ and $(gS_qg^{-1})_{q<p}$ are Sylow families of T' and so, by the inductive hypothesis, there is $t \in T'$ such that, for all $q < p$, we have $R_q = (tg)S_q(tg)^{-1}$. The subgroup R_p is normal in G and so $R_p = (tg)R_p(tg)^{-1} = (tg)S_p(tg)^{-1}$. ∎

Definition 17. *Let p be a prime number and let S be a finite p-group. Let moreover H be a finite group acting on S. We say that S has the* correction property *with respect to the action of H if for every subgroup I of S there is $\alpha \in S$ such that $\alpha I\alpha^{-1}$ is stable under the action of H.*

We give here an equivalent definition of correction property of a group with respect to a *coprime action*, i.e. an action of which the involved groups have coprime orders. We will need the following auxiliary result from [2, Lemma 3.24].

Lemma 18 (Glauberman's lemma)**.** *Let A and G be finite groups with coprime orders such that at least one of them is solvable. Assume A acts on G and that each of them acts on some non-empty set X, where the action of G is transitive. Finally, assume the three actions are compatible, i.e. for all $g \in G$, $a \in A$ and $x \in X$ it holds $a(gx) = (ag)(ax)$. Then there exists an A-invariant element in X.*

Lemma 19. *Let p be a prime number and let S be a finite p-group. Let moreover H be a finite group acting on S such that it has order coprime to the order of S. Then the following are equivalent.*

1. *The group S has the correction property with respect to the action of H.*

2. *For every subgroup I of S and for every $h \in H$ there is $\alpha \in S$ such that $h(I) = \alpha I \alpha^{-1}$.*

Proof. (1) $\Rightarrow$ (2) Let I be a subgroup of S and h an element of H. By assumption we know there is $\alpha \in S$ such that $h(\alpha I \alpha^{-1}) = \alpha I \alpha^{-1}$. To conclude we observe that $h(\alpha I \alpha^{-1}) = h(\alpha)h(I)h(\alpha)^{-1}$ and so $h(I)$ and I are conjugate in S.

(2) $\Rightarrow$ (1) Let I be a subgroup of S and let us define $X = \{\alpha I \alpha^{-1} \mid \alpha \in S\}$. Then S acts transitively on X by conjugation; moreover, it follows from the assumption that H acts on X, too. Now, since the two actions are compatible, we get, by Glauberman's lemma, that there is an element in X that is fixed by H. In other words there is an element α in S such that $\alpha I \alpha^{-1}$ is H-stable. ∎

Definition 20. *Let G be a finite group with a Sylow family $(S_p)_{p\in\mathcal{P}}$. We say that G has the* correction property *if for every prime $p \in \mathcal{P}$ the subgroup S_p has the correction property with respect to the action of T_p on S_p.*

We observe that the definition of correction property does not depend on the choice of the Sylow family of the group, thanks to Proposition 16.

We state here the main theorem of this second part and we will work, through this whole section, in order to prove it.

Theorem 21. *Let G be a finite group. Then the following are equivalent.*

1. *The group G is an evolving group.*

2. *The group G is a supersolvable group with the correction property.*

One direction does not need any preparation, so we prove it immediately.

Lemma 22. *Every supersolvable group with the correction property is an evolving group.*

Proof. Let us fix a prime p; we need to prove that every p-subgroup has a p-evolution in G. The group G is supersolvable, so by Proposition 16 it has a Sylow family $(S_p)_{p\in\mathcal{P}}$. Let now I be a p-subgroup of G; by the Sylow theorems there is an element $g \in G$ such that $gIg^{-1} \leq S_p$. Now we recall that G has the correction property and therefore there is an element $\alpha \in S_p$ such that T_p normalizes $\alpha gI(\alpha g)^{-1}$. We now define $\tilde{J} = L_p \rtimes (\alpha gI(\alpha g)^{-1} \rtimes T_p)$ and observe that $|G : \tilde{J}|$ is a p-power and $|\tilde{J}|/|I|$ is not divisible by p. If we now call $J = (\alpha g)^{-1}\tilde{J}\alpha g$, then the order of J equals the order of $\tilde{J}$ and J contains I. We conclude by observing that $|G : J| = |G : \tilde{J}|$ and $|J : I| = |\tilde{J}|/|I|$ and hence the subgroup J is a p-evolution of I in G. ■

Lemma 23. *Let G be an evolving group and let N be a normal subgroup of G. Then both N and G/N are evolving groups.*

Proof. Let I be a subgroup of N of order a power of p; we want to construct a subgroup J of N satisfying the properties described in Definition 1. We observe that I is a subgroup of G, which is evolving. There is therefore a subgroup J' of G such that $I \leq J'$, the index $|J' : I|$ is coprime with p and $|G : J'|$ is a p-power. If we now define $J = J' \cap N$ we get that $I \leq J$ and p does not divide $|J : I|$, because $|J : I|$ divides $|J' : I|$. Moreover we have that $|N : J| = |J'N : J'|$ and, by the normality of N, we know that $|J'N : J'|$ divides $|G : J'|$. It follows that $|N : J|$ is a p-power and so J is a p-evolution of I in N.

Let us now choose $I/N \leq G/N$, where $|I : N|$ is a p-power, and let us show there is a subgroup J of G containing N, such that J/N is a p-evolution of I/N in G/N. Let us take I_p a Sylow p-subgroup of I. It is a p-subgroup of G and so it has a p-evolution J in G. We now prove that J contains I by showing that every Sylow subgroup of J contains a Sylow subgroup of I; it will follow that J contains N, too. By definition of J, the subgroup I_p belongs to $\mathrm{Syl}_p(J)$ and to $\mathrm{Syl}_p(I)$. Let now $q \neq p$ be a prime number and let $J_q \in \mathrm{Syl}_q(J)$. Since the group J is a p-evolution of a p-group, J_q is a Sylow subgroup of G. Now, by the normality of N, the subgroup $J_q \cap N$ is a Sylow subgroup of N and it is also a Sylow subgroup of I because $|I : N|$ is a p-power. This completes the proof of $I \leq J$. In conclusion, we show that the condition on the indices is satisfied. By definition of J, the number $|J : I_p|$ is coprime to p and $|G : J|$ is a p-power; moreover, by the isomorphism theorems, we have that $|G/N : J/N| = |G : J|$ and $|J/N : I/N| = |J : I|$, which divides $|J : I_p|$. The subgroup J/N is thus a p-evolution of I/N in G/N. ∎

We point out that an arbitrary subgroup of an evolving group is not in general an evolving group. We will give a counterexample at the end of Section 3. Meanwhile, we start laying the ground for proving that every evolving group has the properties announced in Theorem 21.

Lemma 24. *Let G be a non-trivial evolving group and let p be the largest prime dividing the order of G. Then every Sylow p-subgroup of G is normal.*

Proof. Let us work by induction on the order of G and let r be the smallest prime dividing it. If $p = r$, the group G equals its Sylow p-subgroup and therefore it is normal. We now consider the case $p > r$. Let R be a Sylow r-subgroup of G and let T be a subgroup of index r in R. The group G is evolving and so there is an r-evolution J of T in G; in particular J has index r in G. The subgroup J is normal in G, since r is the smallest prime dividing the order of G. Hence, by Lemma 23, it is evolving. By induction, there is therefore a unique Sylow p-subgroup P in J, which is also characteristic in J. In conclusion, since P is a characteristic subgroup of a normal subgroup, it is normal in G. ∎

Proposition 25. *Let G be an evolving group. Then G has a Sylow family.*

Proof. We will work by induction on the order of G. If G is the trivial group then the statement is clearly true. Let now G be non-trivial and let p be the largest prime dividing its order. By Lemma 24 the group G has a unique Sylow p-subgroup S_p and by the Schur-Zassenhaus theorem S_p has a complement T_p in G, which is isomorphic to G/S_p. Now, by Lemma 23, the group G/S_p is an evolving group and therefore so is T_p. By induction, T_p has a Sylow family $(S_q)_{q\in\mathcal{P}\setminus\{p\}}$. We get a Sylow family for G by taking $(S_q)_{q\in\mathcal{P}}$. ∎

Lemma 26. *Let G be an evolving group. Then G has the correction property.*

Proof. If G is the trivial group, it has clearly the correction property; we can thus assume G is non-trivial. Let first p be the largest prime dividing the order of G and let us write $G = S_p \rtimes T_p$. Let moreover I be a subgroup of S_p; we want to find an element $\alpha \in S_p$ such that T_p is contained in $\mathrm{N}_G(\alpha I \alpha^{-1})$. The subgroup I is a p-subgroup of G and so it has a p-evolution J. Moreover, by an order argument, we have $G = S_pJ$ and $S_p \cap J = I$, from which it follows that I is normal in J. By the Schur-Zassenhaus theorem, I has a complement

T in J, which is thus a complement for S_p in G, too. There is therefore an element $\alpha \in S_p$ such that $T_p = \alpha T \alpha^{-1}$ and hence $\alpha I \alpha^{-1}$ is normalized by T_p.

Let now p be any prime number dividing the order of G and let us write $G = L_p \rtimes S_p \rtimes T_p$. The subgroup L_p is normal in G and $S_p \rtimes T_p$ is isomorphic to G/L_p; by Lemma 23 the group $S_p \rtimes T_p$ is evolving. Now p is the largest prime which divides the order of $S_p \rtimes T_p$ and so we can conclude, as in the previous case, that for every subgroup I of S_p there is $\alpha \in S_p$ such that T_p normalizes $\alpha I \alpha^{-1}$. ∎

Lemma 27. *Let G be a finite group with a Sylow family $(S_p)_{p \in \mathcal{P}}$. Assume moreover that G has the correction property. Then G is supersolvable.*

Proof. We will work by induction on the order of G. If G is the trivial group, then G is supersolvable. Let us now assume G is non-trivial and let p be the largest prime dividing the order of G. The Sylow p-subgroup of G is normal and T_p has the correction property; by induction T_p is supersolvable. To conclude it suffices to get a series of subgroups $1 = I_0 \leq I_1 \leq \cdots \leq I_r = S_p$ which are normal in G and such that $|I_{j+1} : I_j| = p$ for every $j \in \{1, \ldots, r\}$. The subgroup S_p is supersolvable because it is a p-group and therefore it has such a chain of normal subgroups in S_p. Let us now fix $j \in \{0, \ldots, r\}$: by assumption there is an element $\alpha \in S_p$ such that T_p normalizes $\alpha I_j \alpha^{-1}$, but I_j is normal in S_p and so $I_j = \alpha I_j \alpha^{-1}$. The subgroup I_j is normalized by both S_p and T_p and therefore it is normal in G. ∎

Proof of Theorem 21. (2) $\Rightarrow$ (1) Lemma 22. (1) $\Rightarrow$ (2) Lemma 26 and Lemma 27. ∎

3 The structure of an evolving group

In this section we give a concrete description of every evolving group and construct a directed graph describing the interaction between the elements of an arbitrarily chosen Sylow family of the group.

Definition 28. *A* directed graph *$\mathcal{G}$ is an ordered pair (V, A), where V and A are sets respectively called the set of* vertices *and the set of* arcs*, together with two maps $s, t : A \to V$. For any $a \in A$, we call $s(a)$ the* source *of a and $t(a)$ the* target *of a.*

Definition 29. *Let G be an evolving group, let $\mathcal{P}$ be the set of primes dividing its order and let $(S_p)_{p \in \mathcal{P}}$ be a Sylow family of G. We define the* graph associated *to G as the directed graph $\mathcal{G} = (V, A)$ where $V = \mathcal{P}$ and $A = \{(p, q) \mid p, q \in V,\ p < q$ and the action of S_p on $S_q/\Phi(S_q)$ is non-trivial$\}$. The maps $s, t : A \to V$ are defined by $s(p, q) = p$ and $t(p, q) = q$.*

Definition 30. *Let G be an evolving group, let $\mathcal{P}$ be the set of prime numbers dividing its order and let $\mathcal{G} = (V, A)$ be its associated graph. We define the subsets $\mathcal{T}$, $\mathcal{S}$ and $\mathcal{I}$ of V as follows.*

· *The set $\mathcal{T}$ equals $t(A)$ and its elements are called* target primes.

· *The set $\mathcal{S}$ equals $s(A)$ and its elements are called* source primes.

· *The set $\mathcal{I}$ is the set of prime numbers belonging to $\mathcal{P} \setminus (\mathcal{T} \cup \mathcal{S})$, which are called* isolated primes.

We state here the result which gives us the structure of an evolving group by means of its associated graph. We will use the symbol $\prod$ to denote a direct product of groups.

Theorem 31. *Let G be an evolving group and let $(S_p)_{p\in\mathcal{P}}$ be a Sylow family. Let moreover $\mathcal{P}$, $\mathcal{S}$, $\mathcal{T}$ and $\mathcal{I}$ be as in Definitions 29 and 30. Then*

$$G = \left(\prod_{p\in\mathcal{T}} S_p \rtimes \prod_{p\in\mathcal{S}} S_p \right) \times \prod_{p\in\mathcal{I}} S_p.$$

Corollary 32. *Let G be an evolving group. Then G is the semidirect product of two nilpotent groups of coprime orders.*

The converse of Corollary 32 is not valid and we will soon give a counterexample.

The proof of Theorem 31 will follow as a corollary of the following two results.

Lemma 33. *Let G be a non-trivial evolving group and let p be a prime number dividing the order of G. Then $\mathbb{F}_p^*$ is contained in $\mathrm{Aut}(S_p/\Phi(S_p))$ as the subgroup of scalar multiplications and the image of the action $T_p \to \mathrm{Aut}(S_p/\Phi(S_p))$ is a subgroup of $\mathbb{F}_p^*$.*

Proof. Let us take p to be the largest prime number dividing the order of G and let S_p be the unique Sylow p-subgroup of G; then the action of T_p on S_p induces an action on the $\mathbb{F}_p$-vector space $V = S_p/\Phi(S_p)$ and so clearly $\mathbb{F}_p^* \le \mathrm{Aut}(S_p/\Phi(S_p))$. We will use the "bar convention" for subgroups of S_p projected to the quotient $S_p/\Phi(S_p)$. By assumption G is an evolving group and thus, by Lemma 26, it has the correction property. In other words for every subgroup I of S_p we can find $\alpha \in S_p$ such that $\alpha I \alpha^{-1}$ is normalized by T_p. In particular, since V is abelian and $\overline{\alpha I \alpha^{-1}} = \overline{I}$, every subspace $\overline{I}$ of V is stable under the action of T_p and therefore every single vector is an eigenvector. Let us now fix $f \in T_p$ and call λ_u the eigenvalue of a given

$u \in V \setminus \{0\}$ with respect to f. Let moreover $v, w \in V \setminus \{0\}$ be two linearly independent vectors (so in particular $v + w \neq 0$); we must have $\lambda_v v + \lambda_w w = f(v) + f(w) = f(v + w) = \lambda_{v+w}(v + w) = \lambda_{v+w} v + \lambda_{v+w} w$, because the action of T_p is linear. Equivalently we have $(\lambda_v - \lambda_{v+w})v + (\lambda_w - \lambda_{v+w})w = 0$ and so, since v and w are linearly independent, we get $\lambda_v = \lambda_w = \lambda_{v+w}$. If v and w are linearly dependent they belong to the same eigenspace. It follows that, for any choice of $v, w \in V \setminus \{0\}$, the two vectors must have the same eigenvalue with respect to f and hence all the elements of V belong to the same eigenspace; in other words applying f is the same as multiplying by the common eigenvalue. Since the choice of f was arbitrary, every element of T_p acts by scalar multiplication on V and so the image of T_p in $\mathrm{Aut}(S_p/\Phi(S_p))$ is equal to a subgroup of $\mathbb{F}_p^*$.

If p is an arbitrary prime number, we write $G = L_p \rtimes S_p \rtimes T_p$. The group L_p is normal in G and so, by Lemma 23, the group G/L_p is evolving and we can apply the previous case to $S_p \rtimes T_p$. ∎

Proposition 34. *Let $\mathcal{G}$ be the graph associated to an evolving group G. Then $\mathcal{S}$ and $\mathcal{T}$ have empty intersection, i.e. the graph has no consecutive arcs.*

Proof. Let $p, q, r \in \mathcal{P}$ such that $p < q < r$ and $(q, r) \in A$; we will show that the action of S_p on $S_q/\Phi(S_q)$ is trivial. By Proposition 25 we have an action of $S_q \rtimes S_p$ on S_r, which induces an action on the Frattini quotient of S_r. By Lemma 33 we write this last action as $S_q \rtimes S_p \longrightarrow \mathbb{F}_r^*$. We observe that this is not the trivial map because of the choice of (q, r). We choose now $s \in S_q$ such that s does not map to the identity in $\mathbb{F}_r^*$ and choose $g \in S_p$; we have then, since $\mathbb{F}_r^*$ is abelian, that $[s, g]$ maps to 1. In particular, if we call $\phi_q : S_q \longrightarrow \mathbb{F}_r^*$ the map identifying the action of S_q on $S_r/\Phi(S_r)$, then $gsg^{-1} \equiv s \bmod \ker \phi_q$. Now, since the action of S_q on $S_r/\Phi(S_r)$ is non-trivial, the kernel of ϕ_q is a proper subgroup of S_q and therefore so is the subgroup $L = (\ker \phi_q)\Phi(S_q)$; moreover $gsg^{-1} \equiv s \bmod L$. It follows that S_q/L is a non-zero quotient space of $S_q/\Phi(S_q)$ on which every eigenvalue equals 1. By Lemma 33 we get that $S_p \longrightarrow \mathbb{F}_q^*$ is trivial. ∎

We observe that, in the case of an evolving group G with associated graph $\mathcal{G}$, the set $\{\mathcal{T}, \mathcal{S}, \mathcal{I}\}$ is a partition of V thanks to the previous proposition. The proof of Theorem 31 follows now directly from Corollary 3.29 in [2], which we state here.

Lemma 35. *Let A and G be finite groups such that* $\gcd\{|A|, |G|\} = 1$ *and A acts on G. If the induced action of A on the Frattini quotient $G/\Phi(G)$ is trivial, then the action of A on G is trivial as well.*

As previously announced, we show here that arbitrary subgroups of evolving groups are not in general evolving. Let p be a prime number greater or equal than 3 and define the group

$$G = \left\{ \begin{pmatrix} h & u & v \\ 0 & 1 & w \\ 0 & 0 & h^{-1} \end{pmatrix} \ : \ u, v, w \in \mathbb{F}_p, h \in \mathbb{F}_p^* \right\} \ ;$$

we claim that the group G is an evolving group and that its subgroup

$$W = \left\{ \begin{pmatrix} h & u & v \\ 0 & 1 & 0 \\ 0 & 0 & h^{-1} \end{pmatrix} \ : \ u, v \in \mathbb{F}_p, h \in \mathbb{F}_p^* \right\}$$

is not evolving. First of all we call $\mathrm{Heis}(\mathbb{F}_p)$ the subgroup of G in which every entry of the diagonal is 1 and D the subgroup of G for which only the entries in the diagonal are different from zero; we then observe that D acts by conjugation on $\mathrm{Heis}(\mathbb{F}_p)$ because

$$\begin{pmatrix} h & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & h^{-1} \end{pmatrix} \begin{pmatrix} 1 & u & v \\ 0 & 1 & w \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} h^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & h \end{pmatrix} = \begin{pmatrix} 1 & hu & h^2 v \\ 0 & 1 & hw \\ 0 & 0 & 1 \end{pmatrix}$$

and moreover that $G = \mathrm{Heis}(\mathbb{F}_p) \rtimes D$. The subgroup W equals $W_H \rtimes D$ where W_H is the subgroup of $\mathrm{Heis}(\mathbb{F}_p)$ with w-th entry equal to zero. We observe that W_H is an abelian p-subgroup of $\mathrm{Heis}(\mathbb{F}_p)$ which has exponent p and therefore $\Phi(W_H)$ is trivial. The Frattini quotient of W_H is thus isomorphic to W_H. We now compute

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

and observe, since p is odd, that $1 \neq -1$ in $\mathbb{F}_p$; in other words D does not act by scalar multiplications on the Frattini quotient of W_H and so W can't be evolving by Lemma 33.

We now show that G is an evolving group, assuming Theorem 21. We notice that p is the largest prime dividing the order of G and that $\mathrm{Heis}(\mathbb{F}_p)$ is its unique Sylow p-subgroup; moreover D is abelian and therefore G has a Sylow family. By showing that G has the correction property we will get it is supersolvable (Lemma 27) and, since D is abelian, we only need to show that given a subgroup I of $S_p = \mathrm{Heis}(\mathbb{F}_p)$ there exists $\alpha \in S_p$ such that D

normalizes $\alpha I \alpha^{-1}$. It can be shown with an easy calculation that the centre Z of S_p is

$$Z = \left\{ \begin{pmatrix} 1 & 0 & v \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \ : \ v \in \mathbb{F}_p \right\}$$

and so in particular it has order p. The case in which $I = \{1\}$ is trivial and the case in which I contains Z is easy because S_p/Z is abelian; we assume therefore $I \cap Z = \{1\}$ and $I \neq \{1\}$. Let us now call $T = IZ$ and observe that, since it contains the centre, T is normal in S_p and it is D-stable. We first assume $T \neq S_p$. In this case T has order p^2 and, since it is not cyclic, it has exactly $p+1$ subgroups of order p: one is Z and we claim that the remaining p are the conjugate subgroups of I in S_p. Indeed if I were normal in S_p, which is a p-group, I would have non-trivial intersection with the centre. We now observe that the subgroup D is isomorphic to the cyclic group $\mathbb{F}_p^*$ and therefore there exists $h \in \mathbb{F}_p^*$ such that $D = \langle M_h \rangle$, where M_h is the element of D associated to h. With this definition, M_h acts on Z by scalar multiplication by h^2 and in fact Z equals the eigenspace of h^2. Moreover, h is an other eigenvalue of T and, since p is an odd prime, the values h and h^2 are distinct. Since the dimension of T as a vector space over $\mathbb{F}_p$ is only 2, we can write $T = Z \oplus L$, where L is the eigenspace of h in T. The subgroup L is a D-stable subgroup of T and it is a complement of Z in T. Since the only possible complements of Z in T are the conjugates of I in S_p, we are done. To conclude, we show that the case $T = S_p$ can never occur. Suppose indeed by contradiction that $T = S_p$; then $[IZ, IZ] = [S_p, S_p]$. But $[IZ, IZ] = [I, I]$, because Z centralizes I, and $[I, I] \leq I$. It follows that I must contain $[S_p, S_p] = [\mathrm{Heis}(\mathbb{F}_p), \mathrm{Heis}(\mathbb{F}_p)]$, which is equal to Z. Contradiction.

We remark that, from this example, it follows that the converse of Theorem B in the Introduction is not valid. The group W is indeed a non-evolving group which is however supersolvable and isomorphic to the semidirect product of two nilpotent groups of coprime orders. The subgroups W_H and D are abelian (and thus nilpotent) subgroups and W is supersolvable because it is a subgroup of the supersolvable group G.

Acknowledgements

My entire life I have never had as much fun with Mathematics as this last year, and I want to thank the people who made this possible.

A huge **THANK YOU** goes to my family for sharing my goals, for supporting me all the time, and for adding that little craziness that always drew a smile on my face.

Another big **THANK YOU** goes to my supervisor for taking me into this project, for giving me the time and the help to understand the concepts, and also for creating a jovial working atmosphere.

Last, but not least, **THANK YOU** to the Algant students who shared this adventure with me, for the endless time spent together working on problem sets and for all the joy that every day filled the Office 232 of the Mathematisch Instituut.

Index

References

[1] J.W.S. Cassels and A. Fröhlich, *Algebraic number theory.* Academic Press, 1967.

[2] I. Martin Isaacs, *Finite group theory.* American Mathematical Society, 2008.

[3] M. Hall Jr, *The theory of groups.* American Mathematical Society, 1999 (originally published in 1959).

[4] E. Weiss, *Cohomology of groups.* Academic Press, 1969 (the author in this text denotes the Tate groups with the notation we use just for cohomology groups).

[5] H. Koch, *Galoissche Theorie der p-Erweiterungen.* VEB Deutscher Verlag der Wissenschaften, 1970.