Intense automorphisms of finite groups

Stanojkovski, M.

Author: Stanojkovski, M.
Title: Intense automorphisms of finite groups
Issue Date: 2017-09-05

INTENSE AUTOMORPHISMS OF FINITE GROUPS

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 5 september 2017
klokke 10:00 uur

door

Mima Stanojkovski
geboren te Sarajevo, Joegoslavië, in 1989

Samenstelling van de promotiecommissie:

Promotor:

Prof. dr. Hendrik W. Lenstra	Universiteit Leiden

Overige leden:

Dr. Jon González Sánchez	Euskal Herriko Unibertsitatea
Dr. Ellen Henke	University of Aberdeen
Prof. dr. Andrea Lucchini	Università degli Studi di Padova
Prof. dr. Bart de Smit	Universiteit Leiden
Prof. dr. Aad van der Vaart	Universiteit Leiden

Mojim najdražima, mami, tati, i dragom gusaru.

The background image of the cover of this thesis has been drawn by the author. The vertices of the illustrated graph represent equivalence classes of subgroups of MC(3), as defined in Section 9.2, with respect to the equivalence relation $H \sim K$ if and only if, for each $j \in \{1, 2, 3, 4\}$, the j-th widths, as defined in Section 2.3, of H and K in MC(3) are the same. An edge is drawn between two vertices if there are representatives H and K of the given vertices such that H is contained in K with index 3 or vice versa. The color of each vertex is determined by the number of conjugates in MC(3) of any representative of the equivalence class associated to the vertex. Subgroups corresponding to white, blue, red, and yellow vertices have respectively 1, 3, 9, and 27 conjugates in MC(3).

Contents

List of Symbols

General

p, a prime number

$\mathbb{Z}$, ring of integers

$\mathbb{Z}_{\geq x}$, set of integers that are at least x

$\mathbb{Z}_{>x}$, set of integers that are larger than x

$\mathbb{Z}_p$, ring of p-adic integers

$\mathbb{F}_q$, finite field of q elements

R^*, group of units of the ring R

$|X|$, the cardinality of the set X

$\langle X \rangle$, the subgroup generated by the set X
and we write $\langle a, b, c, \ldots \rangle$ instead of $\langle \{a, b, c, \ldots\} \rangle$

id_X, the identity map on the set X

$\alpha_{|X}$, the map α restricted to the set X

$\mathrm{cl}(X)$, the closure of the set X

$\bigsqcup$, disjoint union

$\otimes = \otimes_{\mathbb{Z}}$

$\bigwedge = \bigwedge_{\mathbb{Z}}$

$\mathrm{GL}_n(k)$, the general linear group of degree n over k

$\mathrm{MC}(3)$, definition in Chapter 9

$\mathrm{SL}_2^{\triangle}(\mathbb{Z}_p)$, definition in Section 13.4.1

$\mathrm{S}(\Delta_p)$, definition in Section 13.4.2

For any group G

$[x, y] = xyx^{-1}y^{-1}$, for any $x, y \in G$

$\mathrm{Z}(G)$, the centre of G

$\Phi(G)$, the Frattini subgroup of G, see Section 1.3

$(G_i)_{i\geq 1}$, the lower central series of G, see Definitions 14 and 409

$G^n = \langle x^n \ : \ x \in G\rangle$

$\mu_n(G) = \langle x \in G \ : \ x^n = 1\rangle$

$|G : H|$, the index of H in G

$\mathrm{C}_G(X) = \bigcap_{x\in X} G_x$, where G_x is the stabilizer of x

$\mathrm{N}_G(H)$, the normalizer of H in G

$\mathrm{End}(G)$, the set of endomorphisms of G

$\mathrm{Aut}(G)$, the automorphism group of G

$\mathrm{Inn}(G)$, the inner automorphism group of G

$\mathrm{Int}(G)$, the intense automorphism group of G, see Chapter 3

$\mathrm{rk}(G)$, the rank of G, see Sections 8.2 and 13.1

For a finite p-group G

ρ, the map $x \mapsto x^p$

$\mathrm{dpt}_G(x)$, the depth of x in G, see Section 2.3

$\mathrm{wt}_H^G(j)$, the j-th width of H in G, see Section 2.3

$\mathrm{wt}_G(j) = \mathrm{wt}_G^G(j)$

χ_G, the intense character of G, see Section 3.2

$\mathrm{int}(G)$, the intensity of G, see Section 3.2

Exceptions

$(F_i)_{i\geq 1}$, the p-central series of the free group F, in Sections 5.4, 9.4, and 9.6

Introduction

Let G be a group and let $\mathrm{Aut}(G)$ denote its group of automorphisms. An automorphism $\alpha \in \mathrm{Aut}(G)$ is *intense* if it sends each subgroup of G to a conjugate, i.e., for every subgroup H of G there exists $g \in G$ such that $\alpha(H) = gHg^{-1}$. The collection of intense automorphisms is a normal subgroup of $\mathrm{Aut}(G)$, which is denoted by $\mathrm{Int}(G)$.

Such automorphisms come to light in the field of Galois cohomology, as we will see at the end of this introductory section. Additionally, they give rise to a very rich theory. We study the case in which G is a finite p-group and show that, if $\mathrm{Int}(G)$ is not itself a p-group, then the structure of G is almost completely determined by its "class".

If G is a finite abelian group, then the inversion map $x \mapsto x^{-1}$ is an intense automorphism of G and therefore, unless the exponent of G divides 2, the order of $\mathrm{Int}(G)$ is even. It follows, for example, that if G is non-trivial abelian of odd order, then G always has a non-trivial intense automorphism of order coprime to its order. In Chapter 3 we prove the following result for groups of prime power order.

Theorem A. *Let p be a prime number and let G be a finite p-group. Then* $\mathrm{Int}(G)$ *is isomorphic to a semidirect product $S_G \rtimes C_G$, where S_G is a Sylow p-subgroup of* $\mathrm{Int}(G)$ *and C_G is a subgroup of the unit group $\mathbb{F}_p^*$ of the finite field $\mathbb{F}_p$. Moreover, if G is non-trivial abelian, then $C_G = \mathbb{F}_p^*$.*

Theorem A is the same as Theorem 86 and is proven in Section 3.3. If p is an odd prime number, then Theorem A guarantees the existence of infinitely many p-groups, up to isomorphism, whose group of intense automorphisms is not itself a p-group. Moreover, it is also clear from Theorem A that the order of the intense automorphism group of a 2-group can never have prime divisors other than 2. We define the *intensity* of a finite p-group G to be the order of C_G and we denote it by $\mathrm{int}(G)$. The main goal of this thesis is to classify all pairs (p, G) such that p is a prime number and G is a finite p-group of intensity greater than 1. Theorem A classifies all such pairs (p, G) for which G is abelian... but what happens in general?

We proceed by separating into cases based on "how non-abelian" a group is. We define the *lower central series* $(G_i)_{i\geq 1}$ of a group G by

$$G_1 = G \quad \text{and} \quad G_{i+1} = [G, G_i] = \langle xyx^{-1}y^{-1} \ : \ x \in G, y \in G_i\rangle$$

and we define the *(nilpotency) class* of G to be

$$\mathrm{cl}(G) = \#\{k \in \mathbb{Z}_{\geq 1} : G_k \neq 1\}.$$

In other words, the class of a group G is the number of non-trivial elements of the lower central series. The only group of class 0 is the trivial group and the groups of class 1 are the non-trivial abelian groups. It is a classical result that, for any finite p-group, the lower central series stabilizes at $\{1\}$ and so the class is finite.

In Chapter 4 we look at finite p-groups of class 2 – the first non-abelian case we treat – and prove the following result.

Theorem B. *Let p be a prime number and let G be a finite p-group of class 2. Then the following are equivalent.*

1. *One has* $\mathrm{int}(G) > 1$.
2. *One has* $\mathrm{int}(G) = p - 1$ *and p is odd.*
3. *The group G is extraspecial of exponent p.*

Theorem B is the same as Theorem 105 and is proven in Section 4.3. As we explain in Chapter 4, *extraspecial groups* of exponent p are exactly those of the form $(\mathbb{F}_p^{2n+1}, *)$, where $*$ is a twist of the usual $+$ by an inner product on $\mathbb{F}_p^n$. Thanks to their pleasant shape, it is not a surprise that they carry intense automorphisms of order coprime to p. Moreover, they provide, for each odd prime p, an infinite class of examples of p-groups of class 2 and intensity different from 1.

Passing to class at least 3, things drastically change: in Chapter 5, we prove the following very restrictive result.

Theorem C. *Let p be a prime number and let G be a finite p-group of class at least 3. Then the following hold.*

1. *One has* $\mathrm{int}(G) \leq 2$.
2. *If* $\mathrm{int}(G) = 2$, *then p is odd and* $|G : G_2| = p^2$.

Theorem C is a reformulation of Theorem 125, which is proven in Section 5.2. Moreover, Theorem C tells us that, for class greater than 2, a p-group G always has intensity 1 or 2; in the latter case, if p is odd, then the order of the abelianization of G is "small".

Starting from class 3, we want to understand the structure of the groups from Theorem C(2). To this end, let p be an odd prime number and let G be a finite p-group of class 3 with $|G : G_2| = p^2$. In Section 5.2, we prove that G/G_3 is extraspecial of exponent p and that the order of G is p^4 or p^5. Moreover, if we write $w_i = \log_p |G_i : G_{i+1}|$, then either $(w_1, w_2, w_3) = (2, 1, 1)$ or $(w_1, w_2, w_3) = (2, 1, 2)$. As a consequence, for the given prime number p, there are, up to isomorphism, only finitely many possibilities for G (for a sharp bound see for example [Ben27]) and so, contrarily to what happens for class 1 and 2, there are only finitely many isomorphism classes of finite p-groups of class 3 and intensity greater than 1. The fortunate outcome of our investigation in class 3 is the following.

Theorem D. *Let p be an odd prime number and let G be a finite p-group of class 3. Then the following are equivalent.*

1. *One has* $\mathrm{int}(G) = 2$.
2. *One has* $|G : G_2| = p^2$.

The last theorem is a simplification of Theorem 124, whose proof is given in Section 5.4. Thanks to Theorem D, we now know that the only condition, given an odd prime number p, for a finite p-group of class 3 to have intensity 2 is just that of having an abelianization of order p^2. The most urgent problem at this point is that of constructing examples of p-groups of class greater than 3 and intensity 2: those will serve as a model for further investigation.

Example. Let $p > 3$ be a prime number and let $\mathbb{Z}_p$ denote the ring of p-adic integers. Let t be a quadratic non-residue modulo p and denote by Δ_p the quaternion algebra $\Delta_p = \mathbb{Z}_p + \mathbb{Z}_p\mathrm{i} + \mathbb{Z}_p\mathrm{j} + \mathbb{Z}_p\mathrm{ij}$ with defining relations $\mathrm{i}^2 = t$, $\mathrm{j}^2 = p$, and $\mathrm{ji} = -\mathrm{ij}$. The algebra Δ_p is equipped with a *standard involution*, which is given by

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

and which is an anti-ring-automorphism of Δ_p. Moreover, $\mathfrak{m} = \Delta_p\mathrm{j}$ is the unique (2-sided/left/right) maximal ideal of Δ_p and the residue field $\Delta_p/\mathfrak{m}$, as well as every quotient $\mathfrak{m}^k/\mathfrak{m}^{k+1}$, has cardinality p^2. Via the natural isomorphisms of groups $(1 + \mathfrak{m}^k)/(1 + \mathfrak{m}^{k+1}) \to \mathfrak{m}^k/\mathfrak{m}^{k+1}$, the multiplicative group $1 + \mathfrak{m}$ is then seen to be a pro-p-subgroup of Δ_p^*. We define $\mathrm{S}(\Delta_p)$ to be the subgroup of $1 + \mathfrak{m}$ consisting of those elements x satisfying $\overline{x} = x^{-1}$. Being closed in $1+\mathfrak{m}$, the group

$\mathrm{S}(\Delta_p)$ is itself a pro-p-subgroup of Δ_p^* and, if $(\mathrm{S}(\Delta_p)_i)_{i\geq 1}$ denotes the lower central series of $\mathrm{S}(\Delta_p)$, then

$$(\log_p |\,\mathrm{S}(\Delta_p)_i : \mathrm{S}(\Delta_p)_{i+1}|)_{i\geq 1} = (2, 1, 2, 1, 2, 1, \ldots).$$

We prove in Section 13.4.2 that each non-trivial discrete quotient of $\mathrm{S}(\Delta_p)$ has intensity greater than 1.

Because of the last example, we know that, whenever p is a prime larger than 3 and c is a positive integer, then there always exists a finite p-group of class c and intensity greater than 1. We cannot however use the same strategy to build examples of high class 3-groups of intensity 2. As a matter of fact, even though the group $\mathrm{S}(\Delta_p)$ can be defined also for $p = 3$, the image of the 3-torsion of $\mathrm{S}(\Delta_3)$ in $\mathrm{S}(\Delta_3)/\,\mathrm{S}(\Delta_3)_2$ is non-trivial. The next result, which is obtained by combining Theorem 164 and Lemma 206(1), explains why this is a problem.

Theorem E. *Let p be an odd prime number and let G be a finite p-group. Let $(G_i)_{i\geq 1}$ denote the lower central series of G and write $w_i = \log_p |G_i : G_{i+1}|$. Assume that the class of G is at least 4 and that $\mathrm{int}(G) = 2$. Then the following conditions are satisfied.*

1. *One has $(w_1, w_2, w_3, w_4) = (2, 1, 2, 1)$.*
2. *The map $x \mapsto x^p$ induces a bijection $\overline{\rho} : G/G_2 \to G_3/G_4$.*

Relying on results coming from Section 1.5, one can prove that, whenever $p > 3$, the map $\overline{\rho}$ from Theorem E is a group isomorphism, while in the case of 3-groups it never is: because of this structural difference, we separate the two cases.

We define a *κ-group* to be a finite 3-group G such that $|G : G_2| = 9$ and such that cubing induces a bijection $\kappa : G/G_2 \to G_3/G_4$. In particular, κ coincides with $\overline{\rho}$ from Theorem E(2). In Chapter 9, we prove several structural results about κ-groups: we show, for example, that in class 3 there is, up to isomorphism, a unique κ-group and that the minimal extensions of that group to class 4 (which then have order 729) have an elementary abelian commutator subgroup. The just-mentioned results are presented in the form of Theorems 233 and 234. Our investigation of κ-groups leads to the construction of the following example.

Example. Let $R = \mathbb{F}_3[\epsilon]$ be of cardinality 9, with $\epsilon^2 = 0$. Denote by Δ the quaternion algebra $\Delta = R + R\mathrm{i} + R\mathrm{j} + R\mathrm{ij}$ with defining relations $\mathrm{i}^2 = \mathrm{j}^2 = \epsilon$ and $\mathrm{ji} = -\mathrm{ij}$. Let moreover the *standard involution* on Δ be the R-linear map that is given by $(\overline{1}, \overline{\mathrm{i}}, \overline{\mathrm{j}}, \overline{\mathrm{ij}}) = (1, -\mathrm{i}, -\mathrm{j}, -\mathrm{ij})$. Then, for each $x, y \in \Delta$, one has $\overline{xy} = \overline{y}\,\overline{x}$. We write $\mathfrak{m} = \Delta\mathrm{i} + \Delta\mathrm{j}$, which is a nilpotent maximal 2-sided ideal of Δ with $\Delta/\mathfrak{m}$ isomorphic to $\mathbb{F}_3$. We define additionally $\mathrm{MC}(3)$ to be the subgroup of the multiplicative group $1 + \mathfrak{m}$ consisting of those elements x satisfying $\overline{x} = x^{-1}$. The group MC(3) has order 729, class 4, and it is a κ-group. Moreover, $\mathrm{int}(\mathrm{MC}(3)) = 2$.

In Chapter 9 we prove the following result, which is a simplified version of Theorem 231.

Theorem F. *Let G be a finite 3-group of class at least 4. Then the following conditions are equivalent.*

1. *One has* $\mathrm{int}(G) = 2$.
2. *The group G is isomorphic to* MC(3).

Theorem F concludes the classification of finite 3-groups of intensity greater than 1. Except for the two infinite families of finite non-trivial abelian 3-groups and extraspecial 3-groups of exponent 3, there are, up to isomorphism, exactly 17 groups in class 3 (specifically 4 of order 81 and 13 of order 243), and 1, namely MC(3), in class 4. In class higher than 4, there are no 3-groups of intensity greater than 1.

To continue our investigation, we let $p > 3$ be a prime number. In Chapter 10, we define a *p-obelisk* to be a finite non-abelian p-group G such that $|G : G_3| = p^3$ and $G^p = G_3$. Among other things, we prove that p-obelisks of class at least 4 satisfy both (1) and (2) from Theorem E and it is in fact true that, for each p-obelisk G, one has

$$(\log_p |G_i : G_{i+1}|)_{i \geq 1} = (2, 1, 2, 1, \ldots, 2, 1, f, 0, 0, \ldots) \quad \text{with} \quad f \in \{0, 1, 2\},$$

where the index $i \in \{\mathrm{cl}(G), \mathrm{cl}(G) + 1\}$ to which f corresponds is odd and larger than 2. We will see in Chapter 13 that, for every prime number $p > 3$, each non-abelian quotient of $\mathrm{S}(\Delta_p)$ is a special kind of p-obelisk that we call "framed".

Let p be a prime number and let G be a finite p-group. The *Frattini subgroup* of G is $\Phi(G) = [G, G]G^p$; then $G/\Phi(G)$ is the largest possible quotient of G that is vector space over $\mathbb{F}_p$. If $p > 3$, then a p-obelisk G is *framed* if the Frattini subgroup of each maximal subgroup of G coincides with G_3, i.e. for each maximal subgroup M of G, one has $\Phi(M) = G_3$. Though it might not be evident at first sight, asking for a p-obelisk to be framed is equivalent to imposing strong limitations to the interaction of commutator maps and power maps in the group.

Using a wide range of techniques, we are able to prove the following characterization for p-groups of class at least 4, which coincides with the combination of

Theorems 343, 375, and 390. We denote by $\mathrm{C}_G(G_4)$ the centralizer of G_4 in the group G, i.e. $\mathrm{C}_G(G_4) = \bigcap_{g \in G_4} \{x \in G : [x, g] = 1\}$.

Theorem G. *Let $p > 3$ be a prime number and let G be a finite p-group of class at least 4. For each $i \in \mathbb{Z}_{\geq 1}$, write $w_i = \log_p |G_i : G_{i+1}|$. Then $\mathrm{int}(G) = 2$ if and only if there exists $\alpha \in \mathrm{Aut}(G)$ of order 2 such that α induces the inversion map $x \mapsto x^{-1}$ on G/G_2 and one of the following holds.*

1. *The group G is a p-obelisk of class 4.*
2. *The group G is a p-obelisk with $w_5 = 1$ and $\Phi(\mathrm{C}_G(G_4)) = G_3$.*
3. *The group G is a framed p-obelisk with $w_5 = 2$.*

Theorem G makes the role of p-obelisks in our theory clear and it can be used to prove that any p-group of class at least 6 and intensity greater than 1 is a framed p-obelisk. Class 5 is the highest class in which there still exist p-obelisks of intensity greater than 1 that are not framed ... but "semi-framed". More precisely, if, as in Theorem G(2), the group G is a p-obelisk with $w_5 = 1$, then the class is 5, the order of G_5 is p, and $\mathrm{C}_G(G_4)$ is a maximal subgroup; it is the only maximal subgroup whose Frattini subgroup is required to coincide with G_3.

Theorem G completes the classification of prime power order groups of intensity greater than 1, modulo the existence of some special automorphism. Because of their relevance in the theory of intense automorphisms, we give a name to such an automorphism. If G is a group, we call an automorphism $\alpha \in \mathrm{Aut}(G)$ *concrete* if it has order 2 and the automorphism of G/G_2 that is induced by α coincides with the inversion map $x \mapsto x^{-1}$. To the present day, we know very little about concrete automorphisms and how to construct them in general: finding necessary and sufficient conditions for a p-obelisks to possess a concrete automorphism is an interesting problem that we have not yet addressed.

In the following table, we summarize the results we have formulated so far. We denote by p a prime number and by G a finite p-group of class c.
We now have a clear picture of the intensity of groups of prime power order, according to their (finite) class. However, the theory of intense automorphisms can be extended to a larger family of groups with a striking result. In Chapter 13, we complete the picture by moving to infinite class and computing the "intensity" of infinite pro-p-groups.

We call an automorphism α of a profinite group G *topologically intense* if, for each closed subgroup H of G, there exists an element g in G such that $\alpha(H) = gHg^{-1}$. The group of topologically intense automorphisms of a profinite group G is denoted by $\mathrm{Int_c}(G)$ and it is itself profinite. As a consequence, several results concerning

<table>
<tr><th colspan="4">Intensity</th></tr>
<tr><th>c \ p</th><th>2</th><th>3</th><th>≥ 5</th></tr>
<tr><td>0</td><td rowspan="6">1</td><td colspan="2">1</td></tr>
<tr><td>1</td><td colspan="2">$p-1$</td></tr>
<tr><td>2</td><td colspan="2">$p-1$ if G extraspecial of exponent p;
1 otherwise</td></tr>
<tr><td>3</td><td colspan="2">2 if $|G:G_2|=p^2$;
1 otherwise</td></tr>
<tr><td>4</td><td>2 if $G \cong \mathrm{MC}(3)$;
1 otherwise</td><td>2 if G is a p-obelisk with a concrete automorphism;
1 otherwise</td></tr>
<tr><td>≥ 5</td><td>1</td><td>2 if G is a p-obelisk with $|G_5|=p$, $\Phi(\mathrm{C}_G(G_4))=G_3$,
and G has a concrete automorphism;
2 if G is framed p-obelisk with $|G_5:G_6|=p^2$
and G has a concrete automorphism;
1 in all other cases</td></tr>
</table>

intense automorphisms of finite p-groups can be generalized to topologically intense automorphisms of pro-p-groups. For example, Theorem 424 asserts that, if p is a prime number and G is a pro-p-group, then $\mathrm{Int_c}(G)$ decomposes as

$$\mathrm{Int_c}(G) = S_G \rtimes C_G,$$

where S_G is a Sylow pro-p-subgroup of $\mathrm{Int_c}(G)$ and C_G is isomorphic to a subgroup of $\mathbb{F}_p^*$. Similarly to the finite case, we define the intensity $\mathrm{int}(G)$ of a pro-p-group G to be the order of C_G and we ask which are the infinite pro-p-groups of intensity greater than 1. Surprisingly, this question can be answered much more exhaustively than in the finite case, as follows.

Theorem H. *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* $\mathrm{int}(G) = p - 1$.

Theorem H tells us that, "in the limit", for a given prime number $p > 3$, there is a unique non-abelian pro-p-group, up to isomorphism, of intensity greater than 1. From the point of view of finite groups, this last statement translates into saying that, if $p > 3$ is a prime number, then 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 $\mathrm{S}(\Delta_p)$. In a more definite way, we present this result in Section 13.6.3, under the name of Proposition 451.

We conclude our introductory section by giving a "cohomological context" to intense automorphism. As we already mentioned at the beginning of this thesis, intense automorphisms arise naturally as solutions to certain problems coming from the field of Galois cohomology and we would like, with these last lines, to make this statement a little less vague. We start by looking at some examples.

Example. Let k be a field and let n be a positive integer. Moreover, let a be a non-zero element of k. Then the least degree of the irreducible factors of $x^n - a$ divides all other degrees.

Example. Let k be a field and let $\mathrm{Br}(k)$ denote the group of similarity classes of central simple algebras over k, endowed with the multiplication $\otimes_k$. If $[A] \in \mathrm{Br}(k)$, then an extension ℓ/k is said to *split* A if $[A \otimes_k \ell] = [\ell]$. In [GT06, Ch. 4.5], it is proven that the minimal degree of finite separable extensions of k that split a given central simple algebra A over k divides all other degrees.

Example. Let k be a field and let C be a smooth projective absolutely irreducible curve of genus 1 over k. As a consequence of the Riemann-Roch theorem, as explained for example in [LT58, §2], the least degree of the finite extensions of k for which C has a rational point divides all other degrees.

In a quite simplified manner, the last three examples suggest the following question: *When does it happen that "a problem", defined on a base field k, is solvable over a field extension ℓ/k whose degree divides the degrees of all extensions m/k over which the given problem can be solved?* The difficulty of translating this last question into rigorous mathematics is given by the fact that the known examples are quite diverse; however, we can try to unify them from the perspective of Galois cohomology. A first attempt of getting closer to the observed phenomena is Theorem I(1) from [Sta13].

Theorem I. *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 $\{\, |G : H| \; : \; H \leq G \text{ with } \mathrm{Res}^G_H(c) = 0 \,\}$ coincides with its greatest common divisor.*
2. *There exist nilpotent groups N and T of coprime orders and a homomorphism $\phi : T \to \mathrm{Int}(N)$ such that $G \cong N \rtimes_\phi T$.*

A way to interpret (1) from Theorem I is the following. In some sense, the non-zero elements of a cohomology group are the obstructions to having solutions so, ideally, each subgroup H of G for which $\mathrm{Res}^G_H(c) = 0$ corresponds to a field extension "solving the problem". The merit of Theorem I is that of giving a splendid correspondence between a rather technical cohomological condition and a very concrete requirement regarding intense automorphisms. More about Theorem I and its proof can be found in [Sta13].

Generalizing Theorem I to profinite groups is an intriguing problem that is to the present day still open.