ON p-CLASS GROUPS AND THE FONTAINE-MAZUR CONJECTURE

May 28, 2013

JOCHEN GÄRTNER

ABSTRACT. We show that for an infinite unramified p-extension of a number field k, the p-class numbers of the finite subextensions $K|k$ tend to infinity. This is proven by means of a group theoretical result on compact p-adic analytic groups. Furthermore we provide an equivalent formulation of the Fontaine-Mazur conjecture for p-extensions unramified outside a finite set of primes not containing any prime above p.

1. GROUP THEORETICAL RESULTS

Let p be a prime number. For a profinite group G, by $(G_i)_{i\geq 1}$ we denote the lower p-central series, i.e.

$$G_1 = G,\ G_{i+1} = G_i^p[G_i, G].$$

By $G^{ab} = G/[G,G]$ we denote the abelianization of G. Finally, if G is abelian, let $Tor(G)$ be the torsion subgroup and $exp(Tor(G))$ its exponent.

Theorem 1. *Let G be a compact p-adic analytic group. Then either*

(i) *There exists an open subgroup $H_0 \subseteq G$ such that H^{ab} is torsion free for all open subgroups $H \subseteq H_0$, or*
(ii) *If $U \subseteq G$ is an open powerful pro-p subgroup, then*

$$\lim_{k\to\infty} exp(Tor((U_k)^{ab})) = \infty.$$

Remark 2. The above result seems to be known to the experts, however we could not find it in the literature. It has been remarked by Benjamin Klopsch that condition (i) is equivalent to the following: G is virtually abelian, i.e. there exists an open abelian subgroup of G.

We need the following Lemma which follows as a special case from [3], Cor.3.5:

Lemma 3. *Let G be a powerful pro-p group. Then for all $k, k' \geq 1, i, j \geq 0$*

$$[G_k, G_{k'}]^{p^{i+j}} = [(G_k)^{p^i}, (G_{k'})^{p^j}] = [G_{k+i}, G_{k'+j}].$$

Proof of Th.1. First assume that (i) holds. By [2], Cor.8.34. there exists an open uniform pro-p subgroup $U \subseteq H_0$. By assumption $Tor((U_l)^{ab})$ is trivial for all $l \geq 1$, hence (ii) does not hold.

Conversely assume that we are not in case (i). Let $U \subseteq G$ be an open powerful pro-p subgroup. By [2], Th.4.2 we may assume that U is uniform. Suppose that there exists $n \geq 0$ such that

$$exp(Tor((U_k)^{ab})) \mid p^n$$

for all $k \geq 1$. By assumption, there exists an open subgroup $H \subseteq U_{n+1}$ of U_{n+1} such that $Tor(H^{ab})$ is non-trivial. Let $g \in H$ such that $g[H,H] \in Tor(H^{ab})$ is not the identity. Furthermore, let $r \geq n+1$ be maximal such that $g \in U_r$, i.e. $g \in U_r \setminus U_{r+1}$. Since

$$g^{p^n} \in [U,U],$$

for $t = r-(n+1)$ it follows by Lemma 3 that

$$g^{p^{n+2t}} \in [H,H]^{p^{2t}} \subseteq [U_{n+1},U_{n+1}]^{p^{2t}} = [(U_{n+1})^{p^t},(U_{n+1})^{p^t}] = [U_r,U_r],$$

i.e. $g[U_r,U_r] \in Tor((U_r)^{ab})$. However, this implies that

$$g^{p^n} \in [U_r,U_r] \subseteq U_{2r}.$$

On the other hand, since U is uniform, the map $x \mapsto x^p$ induces an isomorphism

$$U_i/U_{i+1} \xrightarrow{\sim} U_{i+1}/U_{i+2}$$

for all $i \geq 1$ and therefore $g^{p^n} \in U_{r+n} \setminus U_{r+n+1}$. It follows that $r+n \geq 2r$ which yields a contradiction[1]. □

We now want to apply this result to the study of the subgroup growth in *fab* pro-p groups.

Definition 4. A finitely generated pro-p group G is called *fab* if for every open subgroup $H \subseteq G$ the abelianization $H^{ab} = H/[H,H]$ is finite.

As an immediate consequence of Theorem 1 we obtain the following

Corollary 5. *Let G be an infinite fab p-adic analytic pro-p group. Then*

$$exp(Tor(H^{ab})) \longrightarrow \infty$$

if H runs through the open normal subgroups of G.

For arbitrary (i.e. not necessarily p-adic analytic) fab pro-p groups we will prove the following

Theorem 6. *Let G be an infinite fab pro-p group. Then*

$$\#H^{ab} \longrightarrow \infty$$

if H runs through the open normal subgroups of G.

Recall that for a pro-p group G the *rank* $\mathrm{rk}(G)$ is defined as

$$\mathrm{rk}(G) = \limsup \{\dim_{\mathbb{F}_p} H^1(H,\mathbb{F}_p) \mid H \leq G \text{ closed subgroup}\}.$$

[1]This conclusion is inspired by an argument given by John Labute in the proof of [9], Lemma 3.2.

By results of Lubotzky and Mann [10],

$$\begin{aligned} \mathrm{rk}(G) &= \limsup \{\dim_{\mathbb{F}_p} H^1(H, \mathbb{F}_p) \mid H \leq G \text{ open subgroup}\} \\ &= \limsup \{\dim_{\mathbb{F}_p} H^1(H, \mathbb{F}_p) \mid H \trianglelefteq G \text{ open normal subgroup}\}. \end{aligned}$$

We have the following characterization of p-adic analytic pro-p groups, cf. [10], Th.A:

Lubotzky-Mann: A pro-p group G is p-adic analytic if and only if $\mathrm{rk}(G) < \infty$.

We can now prove Theorem 6.

Proof of Th.6. If $exp(H^{ab})$ is unbounded for H running over the open normal subgroups of G, we are done. Hence assume $exp(H^{ab}) \mid p^n$ for some $n \in \mathbb{N}$ and all open normal subgroups H. By Corollary 5 we deduce that G is not p-adic analytic. Now the above result due to Lubotzky and Mann yields $\mathrm{rk}(G) = \infty$ which in particular implies $\#H^{ab} \to \infty$ and concludes the proof. □

2. Number theoretical results

Let k be a number field. We denote by $h_k(p)$ the p-class number, i.e.

$$h_k(p) = \#Cl(k)(p).$$

From Theorem 6, we immediately deduce the following

Theorem 7. *Let k be a number field and $k'|k$ be an infinite unramified p-extension. Then $h_K(p) \to \infty$ if K runs through the finite normal subextensions of $k'|k$.*

Remark 8.

(i) The above statement would also follow as a consequence of the *Fontaine-Mazur conjecture*. In fact, even more is true: If $k'|k$ is an infinite unramified p-extension, the conjecture predicts that $\mathrm{Gal}(k'|k)$ is not p-adic analytic and hence the *p-class ranks* of the finite normal subextensions $K|k$ are unbounded, i.e.

$$\dim_{\mathbb{F}_p} Cl(K)/p \longrightarrow \infty.$$

Conversely, this growth behavior implies the Fontaine-Mazur conjecture for unramified p-extensions ([6]). The only explicit examples of infinite unramified pro-p-extensions we have at hand use (variations) of the *Golod-Šafarevič inequality*. In particular, their Galois groups are not p-adic analytic. However, e.g. it is not known whether for a given number field with infinite p-class field tower $k'|k$, there exists a finite subextension $K|k$ such that $\mathrm{Gal}(k'|K)$ satisfies the Golod-Šafarevič inequality, cf. [6]. Against this background, it seems useful to have the unconditional statement in Theorem 7. Furthermore, Corollary 5 gives rise to a equivalent formulation of the Fontaine-Mazur conjecture. We will make a precise formulation in 12.

(ii) Theorem 7 suggests that p-class numbers in unramified p-extensions behave rather differently from p-adic Lie extensions that naturally arise in Iwasawa theory. For example, in the most classical case where $k_\infty|k$ is the cyclotomic $\mathbb{Z}_p$-extension of a totally real number field k, Greenberg's *pseudo-null conjecture* [5] predicts that for the Iwasawa μ- and λ-invariants we have

$$\mu(k_\infty|k) = \lambda(k_\infty|k) = 0,$$

i.e. the size of the p-ideal class groups stays bounded along $k_\infty|k$.

In order to study the relation between our group theoretical statements and the Fontaine-Mazur Conjecture, we need some results from class field theory.

Let S be a set of primes of the number field k. We denote by k_S (resp. $k_S(p)$) the maximal extension (resp. maximal pro-p-extension) of k unramified outside S and set

$$G_{k,S} := \mathrm{Gal}(k_S|k),\ G_{k,S}(p) := \mathrm{Gal}(k_S(p)|k).$$

In this section we recall some facts from class field theory to estimate the exponent $exp(G_{k,S}(p)^{ab})$ where S is a finite set of finite primes of k not containing any primes above p.

Let I_k denote the idèle class group of k. Recall that a *modulus* $\mathfrak{m}$ of k is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$$

where $\mathfrak{p}$ runs through all primes of k and $n_\mathfrak{p} \geq 0$ is an integer for all $\mathfrak{p}$ such that

(i) $n_\mathfrak{p} = 0$ for all but finitely many $\mathfrak{p}$,
(ii) $n_\mathfrak{p} \in \{0, 1\}$ if $\mathfrak{p}$ is an infinite prime.

By $I_k^\mathfrak{m} \subset I_K$ we denote the subgroup of all idèles $\alpha = (\alpha_\mathfrak{p})_\mathfrak{p}$ such that

(i) $\alpha_\mathfrak{p} \in U_\mathfrak{p}^{n_\mathfrak{p}}$ for all finite primes $\mathfrak{p}$ where $U_\mathfrak{p}^{n_\mathfrak{p}}$ denotes the $n_\mathfrak{p}$-th higher unit group and we set $U_\mathfrak{p}^{n_\mathfrak{p}} = U_\mathfrak{p}$ if $n_\mathfrak{p} = 0$.
(ii) $\alpha_\mathfrak{p} \in \mathbb{R}_+^\times$ if $\mathfrak{p}$ is a real prime such that $n_\mathfrak{p} = 1$.

The quotient $I_k/I_k^\mathfrak{m} k^\times$ is the Galois group of the *ray class field of k modulo $\mathfrak{m}$*. We denote by $\mathrm{supp}(S)$ the set of all moduli $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$ of k such that $n_\mathfrak{p} = 0$ for all $\mathfrak{p} \notin S$. By the Existence Theorem of global class field theory, we have an isomorphism

$$G_{k,S}^{ab} \xrightarrow{\sim} \varprojlim_{\mathfrak{m} \in \mathrm{supp}(S)} I_k/I_k^\mathfrak{m} k^\times$$

Definition 9. Let S be a finite set of finite primes of k not containing any prime above p. We set

$$e(S) := \max_{\mathfrak{p} \in S} \{v_p(N(\mathfrak{p}) - 1)\}.$$

Proposition 10. *Let S be a finite set of primes of k not containing any prime above p. Then*

$$exp(G_{k,S}(p)^{ab}) \leq p^{e(S)} \cdot exp(Cl_k(p))$$

Proof. Let $\mathfrak{m} \in \mathrm{supp}(S)$ and consider the exact sequence of abelian groups

$$\prod_{\mathfrak{p}\in S} U_{\mathfrak{p}} \longrightarrow I_k/I_k^{\mathfrak{m}}k^{\times} \longrightarrow I_k/I_k^1 k^{\times} \longrightarrow 1.$$

Here $I_k^1 = \prod_{\mathfrak{p}\in S_\infty} k_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}\notin S_\infty} U_{\mathfrak{p}}$, i.e. we have a canonical isomorphism

$$I_k/I_k^1 k^{\times} \cong Cl_K.$$

Furthermore,

$$U_{\mathfrak{p}} \cong \mu_{N(\mathfrak{p})-1} \times U_{\mathfrak{p}}^1$$

and $U_{\mathfrak{p}}^1$ is a $\mathbb{Z}_{l_{\mathfrak{p}}}$-module where $l_{\mathfrak{p}} \neq p$ is the residue characteristic of the prime $\mathfrak{p}$. Hence the claim follows by taking pro-p-quotients and passing to the projective limit over all $\mathfrak{m} \in \mathrm{supp}(S)$. □

3. On the Fontaine-Mazur conjecture

Let k be a number field, $\overline{k}$ its algebraic closure. A continuous irreducible p-adic representation

$$\rho : \mathrm{Gal}(\overline{k}|k) \longrightarrow \mathrm{GL}_n(\mathbb{Q}_p)$$

is called *geometric*, if it is unramified outside a finite set of primes of k and its restriction $\rho_{|G_{\mathfrak{p}}}$ to the decomposition group $G_{\mathfrak{p}}$ of $\mathfrak{p}$ is potentially semi-stable for all primes $\mathfrak{p}$ of k dividing p. In [4], Fontaine and Mazur make the following fundamental conjecture: ρ is geometric if and only if it comes from algebraic geometry, i.e. it arises from the Galois action on an étale cohomology group $H^i_{et}(V_{\overline{k}}, \mathbb{Q}_p(j))$ of a smooth projective variety V over k. It has been proven in the GL_2-case (under some further assumptions) by Kisin [7]. Using further conjectures by Tate and Grothendieck-Serre [8], it implies the following

Conjecture 11 (Fontaine-Mazur)**.** *Let k be a number field and*

$$\rho : \mathrm{Gal}(\overline{k}|k) \longrightarrow \mathrm{GL}_n(\mathbb{Q}_p)$$

a continuous irreducible presentation which is unramified outside a finite set S of primes of k not containing any prime above p. Then ρ factors through a finite quotient of $\mathrm{Gal}(\overline{k}|k)$.

This conjecture has been proven in the case $S = \varnothing$ in special situations, cf. [1], [11]. In this section, using Corollary 5, we give the following equivalent formulation:

Conjecture 12. *Let k be a number field and $k'|k$ a p-adic Lie extension unramified outside a finite set of primes S of k not containing any prime above p. Then the following holds:*

(i) *There exists a number $n \in \mathbb{N}$ such that $exp(Cl(K)(p)) \mid p^n$ for any finite normal subextension $K|k$ inside k'.*
(ii) *For $\mathfrak{p} \in S$ and a prime $\mathfrak{P}$ of k' lying above $\mathfrak{p}$, the local extension $k'_{\mathfrak{P}}|k_{\mathfrak{p}}$ does not contain the maximal unramified pro-p-extension of $k_{\mathfrak{p}}$.*

Theorem 13. *Conjectures 11 and 12 are equivalent.*

Proof. For a number field k, we set $S_{p,k} := \{\mathfrak{p} \text{ prime of } k \text{ such that } \mathfrak{p}|p\}$. Assume that Conjecture 11 holds. Then any p-adic Lie extension $k'|k$ unramified outside a finite set of primes S with $S \cap S_{p,k} = \varnothing$ is finite, hence Conjecture 12 holds.

Now let $k'|k$ be a p-adic Lie extension unramified outside S with $S \cap S_{p,k} = \varnothing$ and satisfying the conditions (i) and (ii) of Conjecture 12. It remains to show that $k'|k$ is finite. Set $G = \mathrm{Gal}(k'|k)$. By passing to a finite normal subextension, we may assume that G is a p-adic analytic pro-p group. Since no prime above p is ramified in $k'|k$, it follows that G is fab. For a prime $\mathfrak{p} \in S$ choose a prime $\mathfrak{P} \mid \mathfrak{p}$ of k' and let $(k'_{\mathfrak{P}})^{nr}|k_{\mathfrak{p}}$ be the maximal unramified extension inside $k'_{\mathfrak{P}}|k_{\mathfrak{p}}$. By condition (ii), the extension $(k'_{\mathfrak{P}})^{nr}|k_{\mathfrak{p}}$ is finite and we define $f_{\mathfrak{p}}$ by

$$p^{f_{\mathfrak{p}}} = [(k'_{\mathfrak{P}})^{nr} : k_{\mathfrak{p}}].$$

Set

$$f(S) := \max_{\mathfrak{p} \in S} \{f_{\mathfrak{p}}\}.$$

Let $K|k$ be a finite normal subextension of $k'|k$ and $\mathfrak{p}_K$ a prime of K lying above $\mathfrak{p}$. Then

$$v_p(N(\mathfrak{p}_K - 1) \leq v_p(N(\mathfrak{p}) - 1) + f_{\mathfrak{p}} \leq e(S) + f(S)$$

where as in section 2 we have set $e(S) = \max_{\mathfrak{p} \in S} \{v_p(N(\mathfrak{p}) - 1)\}$. If S_K denotes the set of all primes of K lying above S, the maximal abelian subextension of $k'|K$ is contained in $K_{S_K}(p)^{ab}$ and hence by Proposition 10 and condition (i) we have

$$exp(\mathrm{Gal}(k'|K)^{ab}) \leq exp(G_{K,S_K}(p)^{ab}) \leq p^{e(S)+f(S)} \cdot p^n.$$

By Corollary 5 we conclude that G is finite. □

Acknowledgement: We like to thank Kay Wingberg for valuable suggestions and comments.

References

[1] N. Boston. Some cases of the Fontaine-Mazur conjecture II. *J. Number Theory*, 75:161–169, 1999.

[2] J. Dixon, M. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups* second edition. Cambridge Stud. Adv. Math. 61, Cambridge University Press, 1999.

[3] G.A. Fernández-Alcober, J. González-Sánchez, and A. Jaikin-Zapirain. Omega subgroups of pro-p groups. *Isral J. Math.*, 166:393–412, 2008.

[4] J-M. Fontaine and B. Mazur. Geometric Galois representations. In J. Coates and S.T. Yau, editors, *Elliptic Curves, Modular Forms & Fermat's Last Theorem*, pages 41–78. International Press, Boston, 1995.

[5] R. Greenberg. On the structure of certain Galois groups. *Invent. Math.*, 47:85–99, 1978.

[6] F. Hajir. On the growth of p-class groups in p-class field towers. *J. Algebra*, 188:256–271, 1997.

[7] M. Kisin. Overconvergent modular forms and the Fontaine-Mazur conjecture. *Invent. Math.*, 153, no. 2:373–454, 2003.

[8] M. Kisin and S. Wortmann. A note on Artin motives. *Math. Res. Lett.*, 10:275–389, 2003.

[9] J. Labute. Linking numbers and the Tame Fontaine-Mazur Conjecture. *preprint*, 2012.

[10] A. Lubotzky and A. Mann. Powerful p-groups. II: p-adic analytic groups. *J. Algebra*, 105:506–515, 1987.

[11] K. Wingberg. On the Fontaine-Mazur conjecture for CM-fields. *Compositio Math.*, 131, no. 3:341–354, 2002.