PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 45-53

Farshid Hajir

On exponents of class groups in towers of number fields

Written by Marine Rougnant

The Talk is based on a joint work with Christian Maire.

1 Ideal class groups

The ideal class group of a number field K, denoted Cl_K, is the quotient of the fractional ideals of the integer ring $\mathcal{O}_K$ by the the subgroup of principal ideals. Its cardinality h_K, called the class number of K, measures how far $\mathcal{O}_K$ is from a principal ring, and is also a measure of the obstruction to the uniqueness of a decomposition of an ideal into a product of prime ideals.

The ideal class groups are quite simple to define but they are still very mysterious. It is known that the class number of a number field K is always finite and Minkowski's bound permits to compute the class group of a given field K. Despite this, most of the questions on infinite families of fields are still open. For example, are there infinitely many number fields K (up to isomorphism) with principal integer ring or, at least, with h_K bounded by a given number? Or can we show that there are infinitely many number fields with cyclic class group, or even with class group generated by, say, 2017 elements?

Even if we are no able yet to give an answer to any of these questions, we can point to some great advances in understanding variation of class groups in towers. We must first quote Iwasawa's formula, which gives asymptotically the growth of the p-part of ideal class groups in a $\mathbb{Z}_p$-extension. On the other hand, Cohen-Lenstra heuristics give an overall approach to predicting the distributions of class groups in certain situations; recent advances by Bhargava and his collaborators have verified a growing body of Cohen-Lenstra type predictions.

One is quickly led to study ideal class groups one p-part at a time. Let us fix notations for the rest of the paper. Let $p > 2$ be an odd prime number; let K be a number field. We will denote by Cl_K the ideal class group of K and by $A(K)$ the p-Sylow subgroup of Cl_K, that we call p-class group of K.

2 Average exponent

Throughout, we take $p > 2$ to be an odd prime. The structure theorem of finite abelian groups says that every finite abelian p-group A can be written as a product of cyclic p-groups: letting $d = d(A)$ be the dimension of the $\mathbb{F}_p$-vector space A/pA, there exist d positive integers $a_1 \geqslant \ldots \geqslant a_d$ such that

$$A \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{a_{d(A)}}\mathbb{Z}.$$

We recall that the exponent of A is defined as the maximal order p^{a_1} of its elements.

We then have:

$$|A| = \prod_{i=1}^{d(A)} p^{a_i}.$$

Definition. The logarithmic average exponent of a finite p-group A is given by

$$\mathfrak{m}_A = \log_p(|A|^{1/d(A)}).$$

In particular, it follows from this definition that $\log_p |A| = \mathfrak{m}_A d(A)$.

3 Towers of number fields

3.1 Abelian p-adic analytic extensions : Iwasawa's formulas

$$\begin{tikzcd}
L \arrow[d, dash, dotted] \\
K_{n+1} \arrow[d, dash] \\
K_n \arrow[d, dash, dotted, "p^n"] \\
K \arrow[uuu, dash, bend left, "\mathbb{Z}_p"]
\end{tikzcd}$$

Let K be a number field and $L|K$ a $\mathbb{Z}_p$-extension of K, i.e. a Galois extension of K whose Galois group is isomorphic to $\mathbb{Z}_p$. The closed subgroups of $\mathbb{Z}_p$ are exactly the groups $p^n\mathbb{Z}_p$ for $n \geqslant 0$; hence for each such n, there exists a unique subextension $K_n|K$ of $L|K$ of degree p^n.

Iwasawa's formulas give the asymptotic behavior of the p-rank and of the cardinality of the groups $A(K_n)$:

Theorem. *There exist $\mu, s_\mu, \lambda \geqslant 0$ (depending on L) and $\nu \in \mathbb{Z}$ such that for all large enough n,*

1. $\log_p |A(K_n)| = \mu p^n + \lambda n + \nu$,
2. $d(A(K_n)) = s_\mu p^n + O(1)$.

We can deduce from the second point that if μ is 0, then the p-rank is bounded. It follows that $\mathfrak{m}_{A_n}$ goes to infinity if $\mu = 0$ and $\lambda \neq 0$. This observation leads us to consider a particular $\mathbb{Z}_p$-extension.

Adjoining to the field K all the roots of unity with order a power of p, we define a Galois extension $K(\mu_{p^\infty})|K$. We call cyclotomic $\mathbb{Z}_p$-extension of K the unique subfield $K_\infty|K$ corresponding to the maximal pro-p quotient of $\mathrm{Gal}(K(\mu_{p^\infty})|K)$. This $\mathbb{Z}_p$-extension of K is wildly ramified at least at one prime above p.

$$\begin{tikzcd}
 & K(\zeta_p) \arrow[r, dash] & K(\zeta_{p^2}) \arrow[r, dash] & K(\zeta_{p^3}) \arrow[r, dotted, dash] & \, \\
K \arrow[ur, dash, "\text{degree}|(p-1)"] \arrow[r, dash, "p"] & F_1 \arrow[ur, dash] \arrow[r, dash, "p"] & F_2 \arrow[ur, dash] \arrow[r, dotted, dash] & \,
\end{tikzcd}$$

Iwasawa conjectured that the invariant μ of the cyclotomic $\mathbb{Z}_p$-extension of a number field would be 0 and proved it in the case where K is $\mathbb{Q}$. This theorem was extended by Ferrero and Washington for abelian extensions of $\mathbb{Q}$. The last conjecture we have to mention about cyclotomic $\mathbb{Z}_p$-extensions is the following, due to Ralph Greenberg:

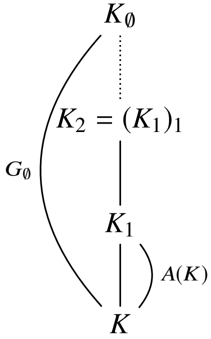
Conjecture. *If K is totally real and if K_∞ is the $\mathbb{Z}_p$-cyclotomic extension of K, then $\lambda = \mu = 0$. In particular $|A(K_\infty)|$, $d(A(K_\infty))$ and $\mathfrak{m}_{K_\infty}$ are bounded.*

3.2 Class field towers : the unramified case

Let K be a number field and let S, T be two finite disjoint sets of places of K. The compositum of all finite p-extensions of K unramified outside S and totally split at the primes of T is still unramified outside S and T-split: this is the maximal pro-p extension of K unramified outside S and T-split. This extension that we denote by K_S^T is Galois (by maximality). Denote by G_S^T (or $G_S^T(K)$) its Galois group. Recall that if $S' \subset S$ and $T \subset T'$, we have $K_{S'}^{T'} \subset K_S^T$.

The study of the unramified case, where S and T are the empty set, was first motivated by geometry: indeed $G_\emptyset$” = ”$\pi_1(Spec\mathcal{O}_K)$. Moreover, the pro-p group $G_\emptyset$ is linked to the class group of K by class field theory: Artin's symbole gives and isomorphism between its abelianized $G_\emptyset^{ab}$ and $A(K)$ (we can see $G_\emptyset$ as a non-abelian generalisation of $A(K)$). We denote by K_1 and we call p-Hilbert of K the subfield of $K_\emptyset$ corresponding to $G_\emptyset^{ab}$.

For $n \geqslant 2$, let K_n be the Hilbert of K_{n-1}: $K_n = (K_{n-1})_1$. The tower $K \subset K_1 \subset K_2 \subset \ldots$ is called Hilbert tower of K.



Remark. The question of the finiteness of Hilbert class field towers had been discussed by Artin and Hasse in their correspondence. It appears that Artin doubted the existence of an infinite Hilbert tower.

By construction, for every index $n \geqslant 2$, the intermediate Galois group $\mathrm{Gal}(K_n|K_{n-1})$ is isomorphic to the p-class group $A(K_{n-1})$ of the field K_{n-1}. The Fontaine Mazur conjecture predicts that the p-rank of $A(K_n)$ goes to infinity. Is its growth due to the growths of both $|A(K_n)|$ and $\mathfrak{m}_{A(K_n)}$, or can we find some situations where the average exponent is bounded?

The aim of this last part is to construct an example of an infinite tower of unramified Galois extensions $K \subset K_1 \subset \ldots$ such that $\mathfrak{m}_{A(K_n)}$ remains bounded above. Recall that the average exponent $\mathfrak{m}_{A(K_n)}$ is defined as the quotient $\log_p(|A(K_n)|)/d(A(K_n))$. This idea is then simple: the first step is to make $d(A(K_n))$ grow as fast as possible, and the second step is to find an upper bound for the numerator.

3.2.1 Growth of the denominator

Let $K \subset K_1 \subset \ldots \subset K_n \subset \ldots \subset K_\emptyset$ be an infinite tower of unramified Galois extensions. For any n, the Galois group H_n of the extension $K_\emptyset | K_n$ is a normal subgroup of $G_\emptyset$. We can first use the following result from group theory to show that its p-rank grows at most linearly with the degree of the extension $K_n | K$:

Proposition.*F*or a pro-p group G and an open subgroup H, $d(H) - 1 \leqslant [G : H](d(G) - 1)$, with equality if G is free.

Furthermore, Burnside's basis theorem gives $d(H_n) = d(H_n^{ab})$ so we have finally the following inequality for every n:

$$d(A(K_n)) - 1 \leqslant [K_n : K](d(G_\emptyset) - 1).$$

The p-rank $d(A(K_n))$ can grow at most linearly with the index of H_n in $G_\emptyset$. We now have to make sure that it will grow as fast as possible. Genus theory (and a trick invented by Iwasawa) permits to find a tower where $d(A(K_n))$ grows linearly in $[K_n : K]$ (cf section 3.3).

3.2.2 A bound for the numerator of $\mathrm{m}_{A_{K_n}}$

By definition, $|A(K_n)|$ is at most h_{K_n}. The well-known Brauer-Siegel theorem gives an asymptotic relation between it and the discriminant of K_n:

Theorem. *(*Brauer-Siegel) Let k be a field ranging over a sequence $\mathcal{K} = (k_n)$ of Galois extensions of $\mathbb{Q}$ such that the root discriminant $rd_{k_n} = |d_{k_n}|^{1/[k_n:\mathbb{Q}]}$ tends to infinity, where $d_(k_n)$ is the discriminant of the field k_n.

Then $B(\mathcal{K}) = \lim_{n \to +\infty} \dfrac{\log(h_{k_n} R_{k_n})}{\log(\sqrt{|d_{K_n}|})}$ exists and is equal to 1.

Unfortunately, the root discriminant rd_{k_n} is constant in an infinite tower of unramified extensions so Brauer-Siegel's theorem cannot apply in our context. Instead, we will use one of its generalizations, due to Tsfasman-Vladut:

Theorem[3]. *If we do not assume the condition on rd_{k_n}, then $B(\mathcal{K})$ exists and is bounded by $1 + C$, where $C \leqslant 0.1588$. If K is totally complex, we can take $C = 1.0764$.*

By definition of $A(K_n)$, we have :

$$\log_p(|A(K_n)|) \leqslant \log_p h_{K_n} = \log_p(h_{K_n} R_{K_n}) - \log_p(R_{K_n}).$$

Tsfasman-Vladut's theorem gives an asymptotic bound of the first summand. It remains to minimize $\log_p(R_{K_n})$, which we get via a fundamental result of Friedman giving an absolute lower bound for the regulator of all numbers fields.

3.3 Example

Let k be a number field and let $T = \{p_1, \ldots, p_t\}$ be a finite set of prime numbers. Let (k_n) be a sequence of unramified extensions in which every element of T splits, i.e. such that $k_n \subset k_{\emptyset}^T$ for every n. Consider the imaginary quadratic field $K = k(\sqrt{-p_1 \ldots p_t})$ and, for every n, denote by K_n the compositum Kk_n. In particular, as the extension $K|k$ is linearly disjoint of any unramified extension of k, the degrees $[K_n : K]$ and $[k_n : k]$ are equal.

$$\begin{tikzcd}
 & & & & k_\emptyset \\
 & K_n \arrow[dl, dash] \arrow[dr, dash] & & k_\emptyset^T \arrow[ur, dash] & \\
K \arrow[dr, dash] & & k_n \arrow[ur, dash] \arrow[dl, dash] & & \\
 & k \arrow[d, dash] & & & \\
 & \mathbb{Q} & & &
\end{tikzcd}$$

Under these hypothesis, for all $n \geqslant 1$, $d(A(K_n))$ is bounded from below by $t[k_n : k] - 1$. By section 3.2.1, we then know that $d(A(K_n))$ grows linearly with the degree of the extension $K_n|K$. Using what has been done before, we obtain for the numerator the following:

$$\begin{aligned}
\log_p(|A(K_n)|) &\leqslant \log_p(h_{K_n} R_{K_n}) - \log_p R_{K_n} \\
&\leqslant 1.0765 \log_p(\sqrt{|d_{K_n}|}) \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|})[K_n : K] \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|})[k_n : k] \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|})\frac{d(A_{K_n})}{t}.
\end{aligned}$$

Finally :

$$\begin{aligned}
\mathfrak{m}_{A(K_n)} = \frac{\log_p(|A(K_n)|)}{d(A(K_n))} &\leqslant \frac{1.0765 \log_p(\sqrt{|d_K|})\frac{d(A_{K_n})}{t}}{d(A(K_n))} \\
&\leqslant \frac{1.0765 \log_p(\sqrt{|d_K|})}{t}.
\end{aligned}$$

Remark. By using refined results of Tsfasman and Vladut, we are able to create an example of an infinite unramified tower of p-extensions, with $p = 2$, for which $\mathfrak{m}_{A(K_n)} \leqslant 8,858$; it would be very interesting to see how to refine such constructions further to make $\mathfrak{m}_{A(K_n)}$ as small as possible.

References

[1] G. Gras, Class Field Theory, From Theory to practice, Springer-Verlag, Berlin, 2003.

[2] F. Hajir and C. Maire, *On the invariant factors of class groups in towers of number fields*, preprint.

[3] M. Tsfasman and S. Vladut, *Infinite global fields and the generalized Brauer-Siegel theorem.* Dedicated to Yuri I. Manin on the occasion of his 65th birthday. Mosc. Math. J. **2**(2002), no.2, 329–402.

Marine Rougnant
Laboratoire de Mathématiques de Besançon
Université de Bourgogne Franche-Comté
16 route de Gray
25000 Besançon, France.
email: `marine.rougnant@univ-fcomte.fr`