PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 17-22

Christian Maire

Pro-p-extensions of number fields and relations

Written by Zouhair Boughadi

This note presents a summary of the talk of Christian Maire at the fourth mini symposium of the Roman number theory association based on a joint work with F. Hajir and R. Ramakrishna. The main results of the talk are a new record to the constant of Martinet and the answer to a question asked by Ihara. The construction of infinite unramified pro-p-extension of a number field plays a crucial role in the proof of these results.
Let G be a pro-p-group, we denote $h^i(G) = dim_{\mathbb{F}_p} H^i(G, \mathbb{F}_p)$, $d(G) = h^1(G)$, and $r(G) = h^2(G)$

Theorem 0.1 (Golod-Shafarevich) *Let G be a non trivial finite p-group. Then*

$$r(G) > \frac{d(G)^2}{4}.$$

For a number field K, let's denote by K' the maximal pro-p-extension of K which is unramified everywhere and $G = Gal(K'/K)$ its Galois group. We know that the group G is a finitely presented pro-p-group. Moreover, by class field theory, we know that $d(G)$ is exactly the p-rank of the class group of K. We also have bounds for the number of relations of G, obtained by Koch and Shafarevich :

$$d(G) \leq r(G) \leq d(G) + r_2 + r_1 - 1 + \delta_{K,p},$$

where r_2 (resp. r_1) is the number of complex (resp. real) embeddings and $\delta_{K,p}$ is equal 1 or 0 depending on whether K contains or not the pth root of unity μ_p.

Theorem 0.2 *If $d(Cl_K) \geq 2+2\sqrt{r_2 + r_1 + \delta_{K,p}}$, then K'/K is infinite.*

Let G be a pro-p-group, and let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

be a minimal presentation of G, then the pro-p-group F is a free group with $d(G)$ generators.
Let $\Lambda := \mathbb{F}_p[[F]]$ be the Iwasawa algebra of F and

$$I = ker(\Lambda \rightarrow \mathbb{F}_p)$$

be the augmentation ideal of Λ.
The depth $\omega(g)$ of an element g of $F \setminus \{1\}$ is defined as

$$\omega(g) = max\{n, g - 1 \in I^n\}.$$

The Zassenhaus filtration of F is given by

$$F_n = \{g \in F,\ \omega(g) \geq n\}.$$

It is well known that $R/R^p[F,R] \simeq H^2(G, \mathbb{F}_p)$. Let $(\rho_i)_i$ be a set of generators of $R/R^p[F,R]$, for $n \geq 1$ we set

$$r_n = |\{\rho_i,\ \omega(\rho_i) = n\}|.$$

Note that r_1 always equals zero because of the following isomorphism

$$G/G^p[G,G] \simeq F/F^p[F,F].$$

Theorem 0.3 (Vinberg, 1965) *If the series* $1 - d(G)t + \sum_n r_n t^n$ *has a zero for a given* $t \in [0, 1]$*, then the pro-p-group G is infinite.*

As an application, if one has no information on the relations, we take $r_2 = r(G)$ to obtain the Golod Shafarevich theorem. More generally if we suppose that $r_2 = \cdots = r_{k-1} = 0$ we get a refinement of Golod Shafarevich bound; namely, if G is finite then

$$r(G) > \frac{d(G)^k}{k^k}(k-1)^{k-1}.$$

A similar result was proven by Koch-Venkov and Schoof, when p is an odd prime and K a quadratic field. Then $r_2(G) = 0$, furthermore if $h^1(G) \leq 3$, K'/K is infinite. More generally Kisilevsky-Labute asserts that this result remains true when K is a CM field.

The main results of the talk can be viewed as further applications. We start with the new record of Martinet's constant. Let K be a number field and (r_1, r_2) its signature ($[K : \mathbb{Q}] = r_1 + 2r_2$). We define the root discriminant of K to be

$$Rd_K := |Disc_K|^{1/[K:\mathbb{Q}]},$$

where $Disc_K$ is the discrimant of K. For number fields with $[K : \mathbb{Q}] >> 0$ and by classical methods we have

$$Rd_K \geq A^t B^{1-t}$$

where $t = r_1/[K : \mathbb{Q}]$ denotes the type of K.

The constants A and B are still unknown, but lower bounds are given

	Minkowski	Odlyzko	Odlyzko (GRH)
$A \geq$	7.3	60.8	215.3
$B \geq$	5.8	22.3	44.7

Two upper bounds for the constants A and B are the constants of Martinet

$$\alpha(0,1) := \lim_n \inf \min\{Rd_K, [K : \mathbb{Q}] = 2n, K \text{totally imaginary}\}$$

$$\alpha(1,0) := \lim_n \inf \min\{Rd_K, [K : \mathbb{Q}] = n, K \text{totally real}\}$$

It is well known that we have

$$A \leq \alpha(1,0) \text{ and } B \leq \alpha(0,1).$$

On the other hand, upper bounds for $\alpha(.,.)$ occur using the discriminant formula and infinite unramified extensions. The first one was given by Jaques Martinet in 1978; he proved that the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{-23}, \cos(2\pi/11))$ has an infinite unramified extension, and so

$$\alpha(0,1) \leq Rd_K \sim 92.4\cdots$$

	Martinet (1978)	Hajir-Maire (2002)
$\alpha(1,0) \leq$	$1058.6\cdots$	$954.3\cdots$
$\alpha(1,0) \leq$	$92.4\cdots$	$82.2\cdots$

The new record is given in this talk

$$\alpha(1,0) \leq 857.5\cdots \quad (1)$$

$$\alpha(0,1) \leq 78.5\cdots \quad (2)$$

This record is obtained by observing that the totally imaginary example of Hajir-Maire improving Martinet's record gives an infinite unramified extension with root discriminant less than 78.5. This extension is obtained by cutting the maximal unramified extension outside a prime ideal of norm equal to 9, by a fourth power of its generator of its inertia group.

The second application is the answer to Ihara's question. Given an infinite unramified extension L/K, denote by $\mathcal{S}(L/K)$ the set of prime ideals of K that decompose completely in L/K.

$$\sum_{\mathfrak{p}\in\mathcal{S}(L/K)} \frac{\log N(\mathfrak{p})}{\sqrt{\log N(\mathfrak{p})}} < \infty$$

Can $\mathcal{S}(L/K)$ be infinite?

An answer is the following

Theorem 0.4 (HMR, 2018) *Suppose that* $d(Cl_K) > 2+2\sqrt{r_1 + r_2 + 1}$*. Then there exists an infinite unramified pro-p-extension* L/K *for which* $\mathcal{S}(L/K)$ *is infinite.*

The last one is about p-rational fields. Let K_p be the maximal pro-p-extension of K unramified outside p. Class field theory gives a description of the abelianization of G_p

$$G_p/[G_p, G_p] \simeq \mathbb{Z}_p^{r_2+1+\delta_K}$$

where δ_K is the Leopoldt defect, conjecturally null (Leopoldt conjecture)

Definition 0.5 *When* G_p *is pro-p-free, the number field* K *is said p-rational.*

In 2016, Gras gave the following

Conjecture 1 *Every number field* K *is p-rational for all* $p \geq C(K)$*.*

Theorem 0.6 *Let* $K/\mathbb{Q}$ *be a totally imaginary extension of degree at least 12. Choose* $p > 2$ *such that:*

i) p *splits totally in* $K/\mathbb{Q}$*;*

ii) K *is p-rational.*

Then there exists a finite extension F/K *in* K_p/K *such that* $F^{ur,p}/F$ *is infinite.*

References

[1] F. Hajir, C. Maire and R. Ramakrishna, *Cutting towers of number fields*. *arXiv:1901.04354*, preprint 2018.

[2] F. Hajir and C. Maire, *Unramified Subextensions of Ray Class Field Towers*. *Journal of Algebra*, 249:528–543, 2002.

[3] J. Martinet, *Tours de corps de classes et estimations de discriminants*. *Inventiones math.*, 44:65–73, 1978.

[4] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field ?*. *J. Math. Soc. Japan*, 35(4):693–709, 1983.

Zouhair Boughadi
department of mathematics and informatics
Moulay Ismail university
B.P. 11201 Zitoune Meknes
50070, Morocco.
email: z.boughadi@edu.umi.ac.ma