RESEARCH PLAN

ARNAUD PLESSIS

My research lies in the areas of both algebraic number theory and diophantine geometry, more precisely ramification groups, Property (B) and localization of points of small height.

1. Algebraic Number Theory

We are interested in the explicit computation of the ramification groups of radical extensions, which are the easiest examples of non-abelian Galois extensions.

The proofs of the three next examples use different methods, although the authors consider almost the same problem. Viviani [19] computed the sequence of ramification groups of any extension of the shape $\mathbb{Q}_p(\zeta_{p^r}, a^{1/p^s})/\mathbb{Q}_p$ where p is odd, r and s denote two positive integers such that $r \geq s$ and $a \in \mathbb{Q}_p$ such that $v_p(a) \in \{0,1\}$. Later, Obus [9] managed to compute the condutor of this extension if $p = 2$. Furthemore, he removed the technical condition on $v_p(a)$. But, I did not compute all the sequence of the ramification groups.

Sharifi [17] computed the sequence of the ramification groups of the (finite) extension $\mathbb{Q}_p(\zeta_{p^r}, V^{1/p^s}, ((1-p)p^k)^{1/p^t})/\mathbb{Q}_p$ where r, s and t denote three positive integers with $r \geq s, t$ and V the unit group of $\mathbb{Z}_p$.

Let $K/\mathbb{Q}_p$ be a finite extension such that $\zeta_p \in K$. Hecke [6, Theorem 10.2.9] computed the ramification groups of any radical extension L/K of degree p. Using this theorem and some recurrences, we get [12]:

Let $F/\mathbb{Q}_p$ be an unramified extension of finite degree. If $p \neq 2$, we can compute explicitly the sequence of the ramification group of any radical extension L/F.

For $p = 2$, it is also possible to compute the ramification groups, making some additional technical hypotheses. This result has several interesting consequences. Assume that p is odd. If L/F is an radical extension like above, it is possible to compute explicitly the Artin conductor of any character belonging to $\mathrm{Gal}(L/F)$. Furthemore, we are also able to compute its different ideal and its discriminant.

2. The Property (B)

Let $L/\mathbb{Q}$ be an algebraic extension and write μ_∞ the set of the roots of the unity. We say that L satisfies the Property (B) if there exists $c > 0$ such that $\mathrm{h}(\alpha) \geq c$, for all $\alpha \in L^* \backslash \mu_\infty$.

A theorem of Northcott shows that number fields satisfy the Property (B). Later, Amoroso and Zannier [2] proved that K^{ab} satisfies the Property (B) for any number field K.

Let $(K_n)_n$ be a sequence of number fields with uniformly bounded degree. Is it true that the compositum $K_1^{ab}K_2^{ab}\cdots$ satisfies the Property (B)? Naturally, this problem extends the previous quoted result.

As a first approximation to solving this problem, we can consider, instead of the abelian closure, its Hilbert class field, that we denote by $H(K)$. Under some additional hypotheses, we give a positive answer to this question [11]:

Let $(K_n/\mathbb{Q})_n$ be a sequence of finite extensions with uniformly bounded degree. Assume that for some rational prime p, there exists an unique prime ideal $\mathfrak{p}_n$ of $\mathcal{O}_{K_n}$ above p, for all n. Then, the compositum $H(K_1)H(K_2)\cdots$ satisfies the Property (B).

In fact, we prove a more general result where the Hilbert class field is replaced by a ray class field. Furthemore, our lower bounds are explicit.

3. Localization of points of small height

Let $\mathbb{G}$ denote either the torus $\mathbb{G}_m$ or an elliptic curve E defined over $\mathbb{Q}$. We write h for the Weil height if $\mathbb{G}=\mathbb{G}_m$ or the Néron-Tate height if $\mathbb{G}=E$. Let Γ be a group of finite rank ($=\dim_{\mathbb{Q}}\mathbb{Q}\otimes_{\mathbb{Z}}\Gamma$). Let S be a set of rational primes, and write $\Gamma_{\text{div},S}$ the set of $g\in A$ such that there exists $n\in\mathbb{N}^*$, whose prime factors are in S, and for which $[n].g\in\Gamma$. In addition, when S is the set of all primes, we simply write $\Gamma_{\text{div}}=\Gamma_{\text{div},S}$. We study a particular case of a conjecture of Rémond [10]:

Conjecture. *There exists $c>0$, depending only on Γ, such that $\mathrm{h}(\alpha)>c$, for all $\alpha\in A(\mathbb{Q}(\Gamma))\backslash\Gamma_{\text{div}}$.*

This conjecture is true in the case when Γ is a finitely generated group since $\mathbb{Q}(\Gamma)$ is then a number field (it is a consequence of a theorem of Northcott).

More interesting, when $\Gamma=\{1\}_{\text{div}}=\mu_\infty$ (and so $\mathbb{Q}(\Gamma)=\mathbb{Q}^{ab}$ by Kronecker's Theorem), this conjecture is true since $\mathbb{Q}^{ab}$ satisfying Property (B) which was proven by Amoroso and Dvornicich [1]. However, the case $\Gamma=\langle 2\rangle_{\text{div}}$ is still unknow.

The next result (see [14]) shows that this conjecture is true for $\Gamma=\langle 2\rangle_{\text{div},S}$, where S is any finite set of odd rational primes.

Let $G\subset\overline{\mathbb{Q}}^*$ be a group finitely generated and S a finite set of odd rational prime. Assume that for any $p\in S$, p does not divide the discriminant of $\mathbb{Q}(G)$. Then, the conjecture holds for $\Gamma=G_{\text{div},S}$.

Let $S=\mathbb{G}_m\times E$ be a split semiabelian variety and let h denote the height on S defined by the sum of the heights on $\mathbb{G}_m$ and E. An extension of this conjecture can be given by replacing A by S.

In this direction, Habegger [8] proved that the conjecture holds if E is not CM and $\Gamma=\{1\}\times E_{\text{tors}}$. The case $\Gamma=(\mathbb{G}_m)_{\text{tors}}\times\{0\}$ is a consequence of Amoroso-Dvornicich [1] and Silverman [18] (resp. Baker [3]) if E is not CM (resp. is CM).

In this examples, we have $\Gamma_{\text{div}}=(\mathbb{G}_m)_{\text{tors}}\times E_{\text{tors}}$. The next result (see [13]) give an example of a group Γ such that $\Gamma_{\text{div}}\neq(\mathbb{G}_m)_{\text{tors}}\times E_{\text{tors}}$.

Let $p\geq 5$ be a rational prime and E an elliptic curve defined over $\mathbb{Q}$ such that p is a supersingular prime. Put $b\geq 2$ an integer such that $p\nmid b$ and $p^2\nmid(b^{p-1}-1)$. Then, the conjecture holds for $A=\mathbb{G}_m\times E$ and $\Gamma=\langle b\rangle_{\text{div},p}\times\{0\}$.

4. Future plans

To find a lower bound for both Néron-Tate and Weil heights, the classical method is split into two steps. The first one consists in etablishing some local metric estimate and the second one consists in a descent method.

For instance, let $E/\mathbb{Q}$ be an elliptic curve no CM. In [8], the author considers a sequence $(P_i)_i$ of points in $E(\mathbb{Q}(E_{\text{tors}}))\backslash E_{\text{tors}}$. For all i, he constructs an explicit $\sigma_i\in\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that, thanks to some local metric estimate, there exists $c>0$

satisfying $\hat{\mathrm{h}}(\sigma_i P_i - P_i) \geq c$ for all i. Thus, points of small height in $E(\mathbb{Q}(E_{\mathrm{tors}}))$ are torsion points because $4\hat{\mathrm{h}}(P_i) \geq \hat{\mathrm{h}}(\sigma P_i - P_i)$.

In the future, I plan to find a lower bound on an elliptic curve without using a metric inequality argument, but only equidistribution arguments. For purpose, I think to use a variation of the Habegger's idea above. Let's condider this idea using an example. Let $E/\mathbb{Q}$ be an elliptic curve no CM, $Q \in E(\mathbb{Q})$ and p a rational prime such that E has bad reduction at p. I plan to localize the points of small height in $E(\langle Q\rangle_{\mathrm{div},\{p\}})$ (it is an analog of the first result of the section 3 in the elliptic case). To find them, I plan to put a sequence $(P_i)_i$ in $E(\langle Q\rangle_{\mathrm{div},\{p\}})$ such that $\lim\limits_{i\to+\infty} \hat{\mathrm{h}}(P_i) = 0$. Then, I construct a "good $\sigma_i \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$" such that the sequence $(\sigma_i P_i - P_i)_i$ isn't equidistribued using the equidistribution theorem of Chambert-Loir [7, Corollaire 5.5]. Hence, $\sigma_i P_i - P_i \in E_{\mathrm{tors}}$ for all i large enough. Next, by a descent method, I will show that the points of small height of $E(\langle Q\rangle_{\mathrm{div},\{p\}})$ are in $\langle Q\rangle_{\mathrm{div},\{p\}}$. Naturally, the same proof works if we consider a finite set of $E(\mathbb{Q})$ instead of just one point Q.

It is really interesting to know if we can prove again that $\mathbb{Q}^{ab}$ has the Property (B) with this new idea. Concretely, if $(\alpha_i)_i$ is a sequence of points in $\mathbb{Q}^{ab}$ such that $\lim\limits_{i\to+\infty} \mathrm{h}(\alpha_i) = 0$, can we construct a "good $\sigma_i \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$" such that $(\sigma_i\alpha_i/\alpha_i)_i$ is not equidistribued using the equidistribution theorem of Rumely [15] (maybe Bilu's theorem [5] is sufficient) ?

If yes, then $\sigma_i\alpha_i/\alpha_i$ is a root of the unity for all i large enough. Once again, we will conclude using a descent argument.

Finally, I also plan to prove an analog of the present result in the last paragraph of the section 3 for a group of the shape $\Gamma = \{1\} \times \langle P\rangle_{\mathrm{div},\{p\}}$, when $P \in E(\mathbb{Q})$ and when the reduction of E at p is supersingular. For purpose, I plan to use either the theory of Lubin-Tate as well as my result on ramification groups or my new method (where the theorem of Chambert-Loir quoted previously will be replaced by an equidistribution theorem for supersingular primes) .

References

[1] F. Amoroso and R. Dvornicich. *A lower bound for the height in abelian extensions*, J. Number Theory, vol. 80, no. 2, p.260–272, 2000.

[2] F. Amoroso and U. Zannier. *A uniform relative Dobrowolski's lower bound over abelian extensions*. Bull. Lond. Math. Soc., vol. 42, no. 3, p. 489–498, 2010.

[3] M. Baker. *Lower bounds for the canonical height on elliptic curves over abelian extensions*, Int. Math. Res. Not., no.29, p. 1571–1589, 2003.

[4] M. Baker and J. Silverman. *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Lett., vol. 11, no.2-3, p. 377–396, 2004.

[5] Y. Bilu. *Limit distribution of small points on algebraic tori.* Duke Math. J., vol.89, no.3, p. 465–476, 1997.

[6] H. Cohen. *Advanced topics in computational number theory*, vol. 193. Springer-Verlag, N.Y., 2000.

[7] A. Chambert-Loir. *Mesures et équidistribution sur les espaces de Berkovich.* J. Reine Angew. Math., vol.595, p. 215–235, 2006.

[8] P. Habegger. *Small height and infinite nonabelian extensions.* Duke Math. J., vol.162, no.11, p. 2027–2076, 2013.

[9] A. Obus. *Conductors of wild extensions of local fields, especially in mixed characteristic* $(0,2)$, Proc. Amer. Math. Soc., vol. 142, no. 5, p. 1485-1495, 2014.

[10] G. Rémond. *Généralisations du probléme de Lehmer et applications á la conjecture de Zilber-Pink*, Panor. Synthèses, vol.52, p. 243–284, 2017.

[11] A. Plessis. *Minoration de la hauteur de Weil dans un compositum de corps de rayon* arXiv:1805.11879v2

[12] A. Plessis. *Calcul des groupes de ramification de certaines extensions radicales* arXiv:1811.05257v2
[13] A. Plessis. *Points de petite hauteur sur une variété semi-abélienne isotriviale* arXiv:1901.07980v1
[14] A. Plessis. *Points de petite hauteur dans un corps engendré par un groupe de rang fini* in preparation
[15] R. Rumely *On Bilu's equidistribution theorem.* Contemp. Math., vol.237, p. 159–166, 1999
[16] J.P. Serre. *Corps locaux, Deuxième édition*, No. VIII. Hermann, Paris, 1968.
[17] R.T. Sharifi. *Ramification groups of nonabelian Kummer extensions* J. Number Theory, vol. 65, no. 1, p. 105–115, 1997.
[18] J. Silverman. *A lower bound for the canonical height on elliptic curves over abelian extensions*, J. Number Theory, vol. 104, no.2, p. 353–372, 2004.
[19] F. Viviani. *Ramification groups and Artin conductors of radical extensions of* $\mathbb{Q}$, *J. Théor. Nombres Bordeaux*, vol. 16, no. 3, p. 779–816, 2004.