

INSTITUT DE MATHEMATIQUES DE JUSSIEU - PARIS RIVE GAUCHE

REPORT ON THE THESIS OF JĘDRZEJ GARNEK

"*Abelian varieties over p-adic fields.*"

Paris, 25 June 2020,

The memoir of Jędrzej Garnek consists of a chapter of preliminaries presenting material about group schemes, abelian varieties and cohomologies, followed by three chapters containing the original results. The central topic is the study of torsion points on abelian varieties defined over a number field or a p-adic field, and the fields generated by these points. A large part of the presented results is already published (Journal de théorie des nombres de Bordeaux, International Journal of Number Theory), while the other part is accessible in the form of preprint.

The first chapter contains well written and condensed preliminaries detailing various delicate arithmetic-geometric topics on group schemes, abelian varieties, cohomology theories and arithmetic Galois theory. The second chapter describes lifts of abelian varieties, reviewing Serre-Tate theory and applying it to the study of local torsion (i.e. the torsion subgroup of points rational over a local field like $\mathbb{Q}_p$). The third chapter studies the question of finding (or proving non existence of) equivariant splitting of some cohomological exact sequences. The link with the previous chapter is a criterion for an abelian scheme to be (or not) the canonical lift of its special fiber. The fourth chapter contains a study of the arithmetic of Kummer extensions associated to abelian varieties over a number fields; in particular it is proven that the class number of the fields generated by torsion points of an abelian variety is "large", under mild conditions.

Let us describe with more details the content of the three original chapters.

The first part (chapter 2) investigates the degree of extensions generated by torsion subgroups in an abelian variety A of dimension g, defined over a number field. Jędrzej Garnek defines the (n,d)-degree of A over a field K, denoted $D_{n,d} = D_{n,d}(A/K)$, as the minimal degree of an extension of K generated by a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^d$. One is actually interested in the case where K is a non archimedean completion of the base field. Notice that, over a number field, general results of Serre on Galois representations show for example that $D_{n,1} \geq c_\delta n^\delta$, where δ can be any real < 1 (or even < 2 if the abelian variety has no CM factor); similarly one knows that $D_{p^n,2g} \geq cp^{n\delta}$, with δ the dimension of the algebraic envelope of the image of the p-adic Galois representation, but these results are in

general ineffective and obtained over the ground field, not over the completion. Jędrzej Garnek observes that when d is strictly greater than the p-rank of A, one gets a lower bounds $D_{p^n,d}(A/\mathbb{Q}_p) \geq p^{2g} - 1$ and, in particular, if the p-rank is zero then $D_{p,1}(A/\mathbb{Q}_p) = p^{2g} - 1$; this is a fine observation. He then unfolds a link between these questions and the theory of canonical lifts. More precisely he shows that, if the reduction at p is not ordinary or if $A_{\mathbb{Z}/p^{n+1}\mathbb{Z}}$ is *not* the canonical lift of $A_{\mathbb{F}_p}$, then

$$D_{p^n,g}(A/\mathbb{Q}_p) \geq p - 1. \tag{1}$$

This result, combined with the theory of complex multiplication, allows for an explicit determination of $D_{p,1}(E/\mathbb{Q}_p)$, where $E/\mathbb{Q}$ is an elliptic curve. For example, when the elliptic curve has complex multiplication by an order of discriminant $-D$, when p is a good prime with Legendre symbol $\left(\frac{-D}{p}\right) = -1$, then $D_{p,1}(E/\mathbb{Q}_p) = p^2-1$ is maximal, whereas when $\left(\frac{-D}{p}\right) = +1$, one has $D_{p,1}(E/\mathbb{Q}_p) = \mathrm{ord}(\mathrm{s} \mod \mathrm{p})$ where $4p = s^2 + Dt^2$. Heuristics from analytic number theory suggest that there are infinitely many primes of the shape $1 + Dt^2$ and thus that the quantity $D_{p,1}(E/\mathbb{Q}_p)$ does not tend to infinity when p goes to infinity. However it is conjectured by Chantal David and Weston, that for $E/\mathbb{Q}$ without CM $\lim D_{p,1}(E/\mathbb{Q}_p) = +\infty$. This conjecture is left open but the results of Garnek offer a strategy to attack it.

The second part (chapter 3) has two intertwined themes: criteria for an abelian variety to be a canonical lift of its reduction modulo p and criteria for an equivariant Hodge-de Rham exact sequence to split G-equivariantly. The latter means that one consider a finite group G acting on a smooth projective curve X, and asks for example if the exact sequence:

$$0 \to H^0(X, \Omega_X) \to H^1_{\mathrm{dR}}(X) \to H^1(X, \mathcal{O}_X) \to 0 \tag{2}$$

splits G-equivariantly. Jędrzej Garnek studies in detail the case $G = \mathbb{Z}/p\mathbb{Z}$, over an algebraically closed field k of characteristic p. The link is provided by the interesting fact that if the pair (X, G) lifts to the truncated Witt ring $W_2(k)$, then the exact sequence (2) splits G-equivariantly. This has several consequences. First one deduces that, when X is *ordinary*, the sequence (2) splits G-equivariantly; secondly, assuming p odd, if the sequence (2) splits G-equivariantly, then the action of G is weakly ramified (this means that the second ramification group is trivial). Jędrzej Garnek also illustrates the fact that the hypothesis p odd is necessary by exhibiting, over a field of characteristic 2, a pair (X, G) with weakly ramified action for which the sequence (2) does not split G-equivariantly. Finally this shows that if the action of G is not weakly ramified, then the curve has no lift to $W_2(k)$.

The study of class numbers of number fields has a rich history, let us mention Gauss conjecture (first proven by Heilbronn) that the class number of an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ goes to infinity when squarefree D goes to infinity, and the fact that the class number of the cyclotomic field $\mathbb{Q}(\exp(2\pi i/n))$ goes to infinity with n. The main theorem of the thesis third chapter can be viewed as a partial analog of the latter; it can be stated as follows. For an abelian variety A defined over a number field K and a prime number p, denote $K_n := K(A[p^n])$ the field extension obtained by adding coordinates of points of order p^n. Assume $A(K)$ is infinite, there exists two integers $a, b \geq 0$ depending on A/K such that

$$\mathrm{ord_p}(\sharp\mathrm{Pic}(\mathcal{O}_{\mathrm{K_n}})) \geq \mathrm{an} - \mathrm{b}, \tag{3}$$

further, when say $K = \mathbb{Q}$, the constant a is ≥ 1 as soon as the rank of $A(\mathbb{Q})$ over $\mathrm{End}(A)$ is large enough, or the abelian variety has good reduction at p and positive p-rank. As an obvious corollary, one gets, providing $a \geq 1$, that the class number of K_n (even its p-component) goes to infinity with n. The strategy to prove this beautiful result is to show that the Kummer extension L_n/K_n obtained by adding coordinates of p^n-division points of points in $A(K)$ contains a large unramified subextension; using class field theory and the fact that L_n/K_n is an abelian p-extension, this yields a large p-subgroup of $\mathrm{Pic}(\mathcal{O}_{\mathrm{K_n}})$. It is relatively easy to see that L_n/K_n is unramified at archimedean places and places of good reduction not dividing p. It is much more subtle to control the ramification at bad places and even more for places that divide p, this is the core of the proof of the main theorem. The computation of the constant "a"is straightforward and, as mentioned, one gets $a \geq 1$ under mild conditions on the rank of $A(K)$ or the type of reduction at places above p. The computation of the constant "b"is trickier, it involves controlling the finite index of failure of surjectivity of the p-adic Kummer map and is, in general, not effectively computable. However Jędrzej Garnek provides, as a nice complement, conditions that guarantee the surjectivity of the Kummer map. When those conditions can be checked (in fact they are not always satisfied, but they are in some sense "generic"), the whole result becomes therefore effective and even explicit. To illustrate this, he gives a numerical example of the jacobian of a concrete curve of genus two where everything is computed explicitly (one finds the values $a = 4$ and $b = 24$).

In my conclusion I will add some personal impressions. There are two things I particularly appreciate in this excellent thesis: I'm quite fond of the theorem about class numbers of fields of division of an abelian variety (third chapter) and I'm impressed by the variety of mathematics skillfully used in the memoir: group theory (represention theory, group schemes, p-divisible and formal groups), abelian varieties (complex multiplication, Néron models, Serre-Tate lifts), cohomology theories (sheaf, de Rham, group cohomology), Galois number theory, algebraic geometry. The memoir of Jędrzej Garnek contains nice arithmetic-geometric constructions and a variety of new results around the arithmetic of abelian varieties, the thesis is nicely written and the motivation coming from the study of local torsion is clearly explained. It is a very welcome addition to the literature. It certainly meets the standard to be awarded a PhD degree and ranks very well among the thesis I have seen.

Marc Hindry
Professeur Université de Paris (Paris Diderot)
Institut de mathématiques de Jussieu – Paris rive gauche
Email: marc.hindry@imj-prg.fr

Appendix: miscellaneous remarks, misprints, queries.

The thesis is very carefully and nicely written in general. I have just a few minor remarks on details, which I list below.

(1) (misprint or unclear notation) In the beginning of the proof of proposition 1.1.5, I fail to understand how $\Gamma(spec(R), --)$ can not depend on R (in the notation).
(2) (reference) Lemma 1.2.8 is not trivial but is stated without proof or reference. I think it can be extracted from Shimura-Taniyama original book on complex multiplication.
(3) (missing sentence + additional reference) Section 1.2.5 starts with a sentence that has been cut : "together with an isomorphism is". Also it seems fair to add to the reference to Katz ([Kat81]) the original (unpublished) notes of Serre-Tate (by Lubin, as quoted in Katz paper) are available at https://web.ma.utexas.edu/users/voloch/lst.html
(4) (clarification) In Corollary 3.3.7 it would clarify the statement to remind the reader that you assume ramification (i.e. $n_P \geq 1$) otherwise I believe the formula fails.
(5) (misprint) In Corollary 4.1.5 $r(A_{\mathfrak{p}}) > 0$ should be $r(A_p) > 0$.
(6) (misprint) bottom of page 62, the notation $\mathcal{A}(R')$ does not make sense; it should be, I guess, $\mathcal{A}(\mathcal{O}^{\mathrm{ur}})$.
(7) Page 64 "One sees easily that $|H_n| = p^{nh_{\mathfrak{p}}}$", this is essentially the definition of $h_{\mathfrak{p}}$.
(8) Page 64 "By Néron-Ogg-Shafarevich"; in fact this criterion does not apply here since $\mathfrak{p}$ divides p, instead you merely want to use the defining property of the inertia group.
(9) Page 64 for some $a_i \in \mathbb{Z}$ should be : "for some $a_{ij} \in \mathbb{Z}$".
(10) (query) Bottom of page 65 you claim that the $\mathbb{F}_p[\mathrm{Sp}_{2g}(\mathbb{F}_p)]$-module is simple. For tiny values (I mean for $g = 1$ and $p \leq 3$) this is a bit surprising since the group $\mathrm{Sp}_{2g}(\mathbb{F}_p)$ is solvable. This has no incidence on the proof of the example you work out (there $g = 2$ and $p \neq 2, 3$), but it should be checked with the Suprunenko-Zalesskii paper you invoke. For example $\mathrm{Sp}_2(\mathbb{F}_2)$ is isomorphic to $\mathcal{S}_3$ and the only irreducible representations have dimension 1 and 2. Since you invoke the theory of quadratic forms, assuming $p \neq 2$ would perhaps be safer.