Università di Roma La Sapienza

On the order of the reductions of points on abelian varieties and tori

Ph.D. Thesis

Antonella Perucca

Advisor: Prof. René Schoof, Università di Roma Tor Vergata

2008

Acknowledgements

I sincerely thank all the people who supported me during the Ph.D.

- I thank Marc Hindry. I developed a 'right guess' of him which then became one of the most important results of this thesis.
- I thank Bas Edixhoven. The mathematical discussions with him led me to generalize my results from abelian varieties to products of abelian varieties and tori.
- I thank my advisor René Schoof, Brian Conrad, Jeroen Demeyer, Emmanuel Kowalski, Qing Liu and Richard Pink for helpful discussions.
- I thank Pietro Corvaja, Andrea Ferretti, Hendrik Lenstra, Willem Jan Palenstijn, Bjorn Poonen, Jean-Pierre Serre and Olivier Wittenberg for useful remarks and explanations.

For my stay in Rome, I thank the University of La Sapienza. For my stay in Paris, I thank Jean-François Mestre and Leonardo Zapponi. For my stay in Leiden, I thank Bas Edixhoven. For my stay in Lausanne, I thank Philippe Michel.

Contents

Introduction

In this thesis, we study the order of the reductions of points on algebraic groups defined over number fields. It is a topic in between number theory and algebraic geometry.

Let G be an algebraic group defined over a number field K. We reduce G modulo the prime ideals of the ring of integers of K (which we also call the primes of K). For all but finitely many primes $\mathfrak{p}$ of K the reduction of G modulo $\mathfrak{p}$ is an algebraic group defined over the residue field $k_\mathfrak{p}$.

Let R be a K-point on G. Then the reduction $(R \bmod \mathfrak{p})$ is well-defined for all but finitely many primes $\mathfrak{p}$ of K: it is a $k_\mathfrak{p}$-point on the reduction of G modulo $\mathfrak{p}$. In particular, for all but finitely many primes $\mathfrak{p}$ of K, $(R \bmod \mathfrak{p})$ is an element of a finite group.

On the order of the reductions of points

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-point on G. We are interested in describing the values taken by $(R \bmod \mathfrak{p})$, where $\mathfrak{p}$ varies in the primes of K.

If R is a torsion point of order n then the order of $(R \bmod \mathfrak{p})$ equals n for all but finitely many primes $\mathfrak{p}$ of K. So assume that R has infinite order.

Which is the greatest integer which divides the order of $(R \bmod \mathfrak{p})$ *for all but finitely many primes* $\mathfrak{p}$ *of* K*?* We prove that it is the number of connected components of the smallest K-algebraic subgroup of G containing R. We also prove that it is the greatest integer n such that the following holds: there exist a product of an abelian variety and a torus H defined over $\bar{K}$ and a point in $H(\bar{K})$ of order n which is the image of R under an element of $\mathrm{Hom}_{\bar{K}}(G, H)$.

Do there exist infinitely many primes $\mathfrak{p}$ *of* K *with the property that the order of* $(R \bmod \mathfrak{p})$ *is coprime to a given integer* m*? ... or divisible by* m*? ... do there exist infinitely many primes* $\mathfrak{p}$ *of* K *with the property that the* ℓ*-adic valuation of the order of* $(R \bmod \mathfrak{p})$ *equals* $v_\ell(m)$ *for every* ℓ *in a given finite set of rational primes?* Call n_R the number of connected components of the smallest K-algebraic subgroup of G containing R. Let $m > 0$ be a multiple of n_R and let S be a finite set of rational primes. We prove that there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that for every ℓ in S the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$ equals $v_\ell(m)$.

We prove the above results in Chapter 4. We base our work on a method by Khare and Prasad, which combines Kummer theory and the study of the ℓ-adic representation.

We have made several improvements with respect to the results in the literature ([KP04], [Pin04], [BGK05], [Bar06]): we let G be the product of an abelian variety and a torus (rather than the multiplicative group or an abelian variety); we let m be any integer $m > 0$ (not only a prime power) and we consider finitely many valuations (rather than one valuation); we let R be any point of infinite order (not only a point such that the smallest K-algebraic subgroup of G containing it is the whole G).

For a general semi-abelian variety we prove that the greatest positive integer which divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K is a multiple of n_R. Also we prove that for any given $m > 0$ there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the order of $(R \bmod \mathfrak{p})$ is a multiple of m. See Chapter 4.

For the multiplicative group and elliptic curves, stronger results are known. For the multiplicative group, Schinzel in [Sch74] proved that for all but finitely many $m > 0$ there exists a prime $\mathfrak{p}$ of K such that the order of $(R \bmod \mathfrak{p})$ is exactly m, provided of course that R is not a torsion point. Silverman, Cheon and Hahn extended Schinzel's result to elliptic curves by using the theory of heights. See [Sil88] and [CH99]. In general, the question to be asked is if all but finitely many multiples of n_R are the order of $(R \bmod \mathfrak{p})$ for some prime $\mathfrak{p}$ of K.

Jones and Rouse in [JR07] studied arboreal Galois representations for commutative algebraic groups (which are supposed to be smooth, separated, reduced). With this approach, they showed that the set of primes $\mathfrak{p}$ of K for which the order of $(R \bmod \mathfrak{p})$ is coprime to a given prime number ℓ has a Dirichlet density and computed this density in several cases.

For abelian varieties, Pink in [Pin04] compared the order of $(R \bmod \mathfrak{p})$ with the prime p which is the characteristic of the residue field $\mathcal{O}/\mathfrak{p}$. Fix a prime number ℓ and a polynomial $f(x)$ which is the product of cyclotomic polynomials and a power of x. Pink showed that for a positive Dirichlet density of primes $\mathfrak{p}$ of K the order of $(R \bmod \mathfrak{p})$ is divisible by ℓ and it is not a divisor of $f(p)$. The method by Pink is still based on Kummer theory and the study of the ℓ-adic representations.

The support problem

Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-points on G. Suppose that the following condition is satisfied:

(SP) *The order of $(Q \bmod \mathfrak{p})$ divides the order of $(P \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.*

How are P and Q related?

The support problem was first studied for the multiplicative group and for elliptic curves by Corrales-Rodrigáñez and Schoof ([CRS97]). In the first case Q is a multiple

of P, in the second case $Q = \phi(P)$ for some K-endomorphism ϕ. Notice that condition (SP) is satisfied whenever Q is the image of P via a K-endomorphism.

For abelian varieties, partial results were obtained by Khare and Prasad in [KP02] and by Banaszak, Gajda and Krasoń in [BGK03]. Larsen in [Lar03] solved the support problem for abelian varieties. He showed that there exist a K-endomorphism ϕ and a non-zero integer c such that $\phi(P) = cQ$ ([Lar03, Theorem 1]). In general one can not take $c = 1$, even if both P and Q have infinite order ([Lar03, Proposition 2]). Wittenberg in [Wit03] gave an alternative proof of [Lar03, Theorem 1] based on [LS04].

We study two variants of the support problem, which we call respectively *ℓ-adic support problem* and *radical support problem*. We require weaker conditions on the points:

(LSP) *Let ℓ be a prime number. Suppose that the ℓ-adic valuation of the order of $(Q \bmod \mathfrak{p})$ is less than or equal to the ℓ-adic valuation of the order of $(P \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.*

(RSP) *Let S be an infinite family of prime numbers. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the following holds: for every ℓ in S the order of $(Q \bmod \mathfrak{p})$ is coprime to ℓ whenever the order of $(P \bmod \mathfrak{p})$ is coprime to ℓ.*

Let P and Q satisfy condition (LSP) or condition (RSP). We prove that there exist a K-endomorphism ϕ and a non-zero integer c such that $\phi(P) = cQ$. See Theorems 6.1.1 and 7.1.1. These results strengthen and generalize Larsen's result on the support problem.

For abelian varieties, our results have alternative proofs: the proof by Larsen of [Lar03, Theorem 1] only requires condition (RSP); the proof by Wittenberg of [Lar03, Theorem 1] which is in [Wit03] only requires condition (LSP); for simple abelian varieties, Theorem 6.1.1 is equivalent to a result by Barańczuk ([Bar06, Theorem 8.2]).

Let G be the product of an abelian variety and a torus defined over a number field K and let P and Q satisfy one of the three conditions above. Let c be the least positive integer such that cQ belongs to the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by P.

Assuming condition (SP), c divides an integer m which depends only on G and K. For abelian varieties, this result has an alternative proof by Larsen, see [LS04].

Assuming condition (LSP), the ℓ-adic valuation of c is less than or equal to the ℓ-adic valuation of an integer m which depends only on G and K (notice that m does not depend on ℓ).

Assuming condition (RSP), there exist two integers n and m depending only on G and K such that the following holds: for every ℓ in S coprime to n the ℓ-adic valuation of c is less than or equal to the ℓ-adic valuation of m.

See sections 5.3, 6.1 and 7.1 for more results concerning c under conditions (SP), (LSP) and (RSP) respectively.

In Chapter 8 we discuss the *multilinear support problem*, which is a variant of the support problem introduced by Barańczuk in [Bar06]. The points P and Q are replaced by n-tuples of points and the following condition is required:

(MSP) *Suppose that for all but finitely many primes* $\mathfrak{p}$ *of* K *the following holds: for all integers* $m_1, \ldots, m_n$ *the point* $(m_1Q_1 + \ldots + m_nQ_n \bmod \mathfrak{p})$ *is zero whenever the point* $(m_1P_1 + \ldots + m_nP_n \bmod \mathfrak{p})$ *is zero.*

Condition (MSP) is stronger than requiring condition (SP) on each pair of points (P_i, Q_i) so we know that there exist K-endomorphisms ϕ_i and an integer c such that $\phi_i(P_i) = cQ_i$. One would like to prove that there exists a K-endomorphism ϕ such that $\phi(P_i) = cQ_i$ for every i. This is true if the endomorphism ring is $\mathbb{Z}$ (see [Bar06]) but in general it is false (see Chapter 8).

The problem of detecting linear dependence

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $G(K)$ and let Λ be a finitely generated subgroup of $G(K)$. Suppose that $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. Does R belong to Λ?

The problem of detecting linear dependence is still unsolved. Schinzel in [Sch75, Theorem 2] solved it for the multiplicative group. Partial results for abelian varieties were obtained by Banaszak, Gajda, Górnisiewicz, Kowalski, Krasoń, Weston in the papers [Wes03], [Kow03], [BGK05], [GG07], [Ban07]. See section 9.1.

The strongest result is due to Weston: for abelian varieties with commutative endomorphism ring there exists a torsion point T such that $R + T$ belongs to Λ ([Wes03]).

We study the problem of detecting linear dependence as an application of the other results of our thesis. We prove three results on the problem of detecting linear dependence for the product of an abelian variety and a torus, see Theorems 9.2.1, 9.3.1 and 9.4.1.

First we prove that there exists a non-zero multiple of R which belongs to the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by Λ.

Second, we solve the problem of detecting linear dependence in the case where Λ is a free left $\mathrm{End}_K G$-submodule of $G(K)$ or if Λ has a set of generators (as a group) which is also a basis of a free left $\mathrm{End}_K G$-submodule of $G(K)$. This result strengthens [GG07, Theorem B] and [Ban07, Theorem 1]: in both cases we remove the assumption on the point R and generalize the statement to products of abelian varieties and tori.

Third, we solve the problem of detecting linear dependence in the case where Λ is cyclic. This third result was known so far only for elliptic curves and the multiplicative group, see [Kow03, Theorem 3.3] by Kowalski.

The results in Chapter 4 will appear in the Journal of Number Theory ([Per09]). The other results are submitted for publication.

Part I

The reductions

Chapter 1

Reductions of algebraic groups

1.1 The model of an algebraic group

A projective system of schemes

Let K be a number field, let $\mathcal{O}$ be the ring of integers of K. Following EGA, we adopt the following notations: $A = K$; $A_0 = \mathcal{O}$; $S = \operatorname{Spec} K$; $S_0 = \operatorname{Spec} \mathcal{O}$.

Let L be the set consisting of the following elements: the finite subsets of the support of S_0 not containing $\{0\}$. Then L with the inclusion relation is a partially ordered directed set.

For every λ in L we define A_λ as follows: A_λ is obtained from A by inverting the prime ideals corresponding to the element λ. If λ is a singleton corresponding to a prime ideal $\mathfrak{p}$, let a be the generator of some power of $\mathfrak{p}$ (the class group of K is finite hence there exists a power of $\mathfrak{p}$ which is a principal ideal). Then A_λ is is obtained by localizing A_0 to the multiplicative set generated by a. Now let λ correspond to some prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and let $a_1, \ldots, a_n$ be defined analogously to a. Then A_λ is is obtained by localizing A_0 to the multiplicative set generated by the element $a_1 \cdots a_n$. Notice that the prime spectrum of A_λ consists of the complement of λ in $\operatorname{Spec} \mathcal{O}$.

Let λ and μ be in L. There are inclusion maps from A_λ to A_μ whenever $\mu > \lambda$. Define $S_\lambda = \operatorname{Spec} A_\lambda$. Correspondingly, there are scheme morphisms from S_μ to S_λ whenever $\mu > \lambda$. We have an inductive limit of algebras and the corresponding projective limit of their spectra:

$$A = \varinjlim A_\lambda \qquad S = \varprojlim S_\lambda.$$

Existence of a model

Definition 1.1.1. *Let X be a K-scheme. Let Z be a scheme such that* $\operatorname{Spec} K$ *is a Z-scheme. Then a Z-scheme $\mathcal{X}$ is a Z-model for X if the generic fiber of $\mathcal{X}$ is X i.e.*

$$X = \mathcal{X} \times_Z \operatorname{Spec} K.$$

In our setting, [Gro66, Théorème 8.8.2 (ii)] says the following:

Theorem 1.1.2. *Let X be an algebraic group defined over a number field K. Let $\mathcal{O}$ be the ring of integers of K. Then there exists a non-empty open subscheme A_λ of* $\operatorname{Spec}\mathcal{O}$ *and a model X_λ over A_λ for X which is of finite type over A_λ.*

Lift of a morphism

Definition 1.1.3. *Let X and Y be K-schemes. Let Z be a scheme such that* $\operatorname{Spec}K$ *is a Z-scheme. Let $\mathcal{X}$ and $\mathcal{Y}$ be Z-models of X and Y respectively. Let ϕ be a K-morphism from X to Y. Call π_1,π_2 the projections of a fibered product of schemes. Then a Z-morphism Φ from $\mathcal{X}$ to $\mathcal{Y}$ is said to be a lift of ϕ if the following relation holds:*

$$\phi = (\Phi \circ \pi_1) \times_Z \pi_2.$$

In our setting, [Gro66, Théorème 8.8.2 (i)] says the following:

Theorem 1.1.4. *Let X and Y be algebraic groups defined over a number field K. Call $\mathcal{O}$ the ring of integers of K and let A_α be a non-empty open subscheme of* $\operatorname{Spec}\mathcal{O}$ *such that there exists a model X_α (respectively Y_α) for X (respectively Y) over A_α of finite type over A_α. Then for every K-morphism f from X to Y there exists a non-empty open subscheme* $\operatorname{Spec}B$ *of* $\operatorname{Spec}\mathcal{O}$ *such that $B \supseteq A_\alpha$ and such that the following holds: there exists a unique B-morphism $\tilde{f}$ from $X_\alpha \times_{A_\alpha} B$ to $Y_\alpha \times_{A_\alpha} B$ which induces f on the generic fibers.*

Lemma 1.1.5. *The lift of the composition of two morphisms is the composition of their lifts.*

Proof. This is an immediate consequence of the unicity of the lift in Theorem 1.1.4. □

Properties of the lift of a morphism

It is remarkable that some properties of the K-morphisms are preserved by the lift on a sufficiently small non-empty open subscheme of $\operatorname{Spec}\mathcal{O}$. In our setting, [Gro66, Théorème 8.10.5] says the following:

Theorem 1.1.6. *Consider the property of being: (i) an isomorphism; (ibis) a monomorphism; (ii) an immersion; (iii) an open immersion; (iv) a closed immersion; (v) 'séparé'; (vi) surjective; (vii) 'radiciel'; (viii) 'affine'; (ix) 'quasi-affine'; (x) 'fini'; (xi) 'quasi-fini'; (xii) 'propre'; (xiii) 'projectif'; (xiv) 'quasi-projectif'. Let $\mathcal{P}$ be one of the previous properties. With the notations of Theorem 1.1.4, let f be a K-morphism between X and Y and let f_B be a lift to f to the models of X and Y over B. Then f has the property $\mathcal{P}$ if and only if f_B has the property $\mathcal{P}$ for every sufficiently small* $\operatorname{Spec}B$.

In the previous theorem, by 'sufficiently small $\operatorname{Spec}B$' we mean the following: there exists α in S such that for every $\lambda \geq \alpha$ the property $\mathcal{P}$ holds for the model over S_λ.

On the unicity of the model

The following result is a consequence of [Gro66, Corollaire 8.8.2.5]. We prove it for the convenience of the reader.

Theorem 1.1.7. *Let X be an algebraic group defined over a number field K. Call $\mathcal{O}$ the ring of integers and let* $\operatorname{Spec} A_\alpha$ *be a non-empty open subscheme of* $\operatorname{Spec} \mathcal{O}$ *such that there exist two models X_α, Y_α for X over A_α and of finite type over A_α. Then there exists a non-empty open subscheme* $\operatorname{Spec} B$ *of* $\operatorname{Spec} \mathcal{O}$ *such that $B \supseteq A_\alpha$ and such that the following holds: there exists a B-isomorphism from $X_B = X_\alpha \times_{A_\alpha} B$ to $Y_B = Y_\alpha \times_{A_\alpha} B$ which induces the identity on the generic fibers.*

Proof. Apply Theorem 1.1.4 with $X = Y$ and $f = \mathrm{id}_{XY}$. We can then lift f and f^{-1} and their composition, which is id_X. We can lift these morphisms to morphisms on the models X_B and Y_B (where the choice of B clearly depends on A_α, f and f^{-1}). The identity on X_B induces the identity on X hence (by unicity) it is the lift of id_X. Then by Lemma 1.1.5 the composition of the lift of f and f^{-1} is the identity on X_B. Analogously the composition of the lift of f^{-1} and f is the identity on Y_B. Then the lift of f is a B-isomorphism from X_B to Y_B which induces the identity on the generic fibers. □

Clearly if two models are isomorphic so are their generic fibers.

Group scheme structure of the model of an algebraic group

Let G be a group scheme over K. Then the group scheme structure on G is defined by a triple m, i, e of K-morphisms where $m : G \times G \to G$ is the multiplication, $i : G \to G$ is the inverse and $e : \operatorname{Spec} K \to G$ is the identity. The morphisms m, i, e should satisfy the following relations:

$$\begin{aligned} m \circ (m \times \mathrm{id}_G) &= m \circ (\mathrm{id}_G \times m) \\ m \circ (e \times \mathrm{id}_G) &= \pi_2 \\ m \circ (\mathrm{id}_G \times e) &= \pi_1 \end{aligned}$$

where

$$\pi_2 : \operatorname{Spec} K \times_K G \to G\,; \quad \pi_1 : G \times_K \operatorname{Spec} K \to G$$

are the projections of the fiber products. The group scheme is said to be commutative if $m = m \circ s$, where s is the map switching the two factors of $G \times G$.

Let G be an algebraic group defined over a field K. We can find a non-empty open subscheme $\operatorname{Spec} B$ of $\operatorname{Spec} \mathcal{O}$ such that there is a model $\mathcal{G}$ for G and there are lifts of the maps m, i, e, j_1, j_2. The lifts of the maps m, i, e are the candidates for a B-group scheme structure on $\mathcal{G}$. We only have to check that these maps satisfy the relations as above. This is an immediate consequence of the unicity of the lift and the fact that the lift of the composition is the composition of the lifts (see Lemma 1.1.5). Analogously,

one proves that for a commutative algebraic group one can find a model which is a commutative group scheme.

The group structure on $\mathcal{G}$ induces a group scheme structure on every fiber. For the generic fiber G we find (as expected) the K-group scheme structure given by m, i, e. For the special fiber $\mathcal{G}_{\mathfrak{p}}$ over the residue field $k_{\mathfrak{p}}$ (where $\mathfrak{p}$ is a non-zero prime ideal in the support of $\operatorname{Spec} B$) we find a $k_{\mathfrak{p}}$-group scheme structure.

Let $\mathfrak{p}$ be a non-zero prime ideal in the support of $\operatorname{Spec} B$. Call $\mathcal{O}_{\mathfrak{p}}$ the localization of $\mathcal{O}$ to $\mathfrak{p}$ and consider the extension $\mathcal{G} \times_B \mathcal{O}_{\mathfrak{p}}$. Then $\mathcal{G} \times_B \mathcal{O}_{\mathfrak{p}}$ has a $\mathcal{O}_{\mathfrak{p}}$-group scheme structure induced by $\mathcal{G}$.

We showed that we can lift morphisms in an essentially unique way. Restricting the lift of a morphism to a special fiber gives the reduction of the morphism modulo the corresponding prime ideal.

Lemma 1.1.8. *A morphism of group schemes reduces to a morphism of group schemes for all but finitely many fibers.*

Proof. A morphism of group schemes X and Y defined over K is a morphism f of K-schemes such that $f \circ m_X = m_Y \circ (f \times f)$, where m_X and m_Y are the multiplication morphisms on X and Y respectively. Let $\mathcal{X}$ and $\mathcal{Y}$ be models for X and Y which are group-schemes. By Lemma 1.1.5 and by the unicity of the lift we can prove the analogous formula for the lift of f to the models (provided that the base scheme is sufficiently small). This implies the desired formula for all but finitely many fibers of the model. □

Proposition 1.1.9. *Let G be an algebraic group defined over K. Then there exist a non-empty open subscheme B of* $\operatorname{Spec} \mathcal{O}$ *and a model for G on B which is a B-group scheme and whose fibers are algebraic groups.*

Proof. Since the model is of finite type, its fibers are also of finite type. In this section we have shown that the model of an algebraic group is a group scheme (provided that the base scheme is sufficiently small). Then the fibers of such a model are algebraic groups over the residue field. □

Model for an algebraic subgroup

Let X be an algebraic group defined over a number field K. A K-algebraic subgroup Y of X is in particular a K-scheme which admits a closed immersion to X. The K-group scheme structure of Y is obtained by restricting the K-morphisms m, i, e which define the K-group scheme structure on X.

Lemma 1.1.10. *Let X be an algebraic group defined over a number field K. Let Y be a K-algebraic subgroup of X. Then there exists a model for Y which is a closed subgroup scheme of a model for X.*

Proof. Call f the closed immersion from Y to X. By considering a sufficiently small non-empty open subscheme $\operatorname{Spec} B$ of $\operatorname{Spec} \mathcal{O}$ (where $\mathcal{O}$ is the ring of integers of K) we

can find a B-model for X and for Y and we can lift f to the models. Provided that $\operatorname{Spec} B$ is sufficiently small the lift of f is a closed immersion from the model of Y to the model of X (see Theorem 1.1.6). Also, provided that $\operatorname{Spec} B$ is sufficiently small the two models of X and Y are B-group schemes. Then it suffices to show that the closed immersion of the model of Y into the model of B is a morphism of B-group schemes. This is true for sufficiently small $\operatorname{Spec} B$ (see Lemma 1.1.8). □

Model for products and for affine algebraic groups

The product of group schemes behaves well with respect to the model.

Lemma 1.1.11. *A model for the product is the product of the models.*

Proof. This is a straight-foreward check: the product of two group schemes of finite type over a base S is still of finite type over S and its generic fiber is the product of the generic fibers. □

The following remark follows immediately from the definitions:

Remark 1.1.12. *An affine algebraic group admits an affine model and its special fibers are affine schemes.*

Extending the base field

Let K be a number field and call $\mathcal{O}$ the ring of integers of K. Let F be a finite extension of K and call $\mathcal{O}_F$ the ring of integers of F. Let λ be a finite subset of non-zero prime ideals of $\mathcal{O}$ and let λ_F be the set of prime ideals of $\mathcal{O}_F$ which are over the primes of λ. Call $\operatorname{Spec} B$ the open subscheme of $\operatorname{Spec} \mathcal{O}$ associated to λ and $\operatorname{Spec} B_F$ the open subscheme of $\operatorname{Spec} \mathcal{O}_F$ associated to λ_F. Remark that there is an inclusion of B into B_F which makes $\operatorname{Spec} B_F$ a scheme over $\operatorname{Spec} B$. Then one can extend a B-scheme to a B_F-scheme. For models of K-algebraic groups one has the following:

Lemma 1.1.13. *The extension of the model is a model for the extension.*

Proof. The proof is a straightforward check: we consider the extension of the model and verify that it is still of finite type (immediate from the definition) and that its generic fiber is the extension of the given algebraic group. For this, it suffices to apply the following property about fibered products of schemes (see [Gro60, Corollary 3.3.10]) where S is a scheme and X, Y, S' are S-schemes:

$$(X \times_S S') \times_{S'} (Y \times_S S') \simeq (X \times_S Y) \times_S S'.$$

□

1.2 Reductions of points

Let G be an algebraic group defined over a number field K and let R be a K-point on G. By definition, R is a morphism from $\operatorname{Spec} K$ to G. The point R induces also a morphism from $\operatorname{Spec} B$ to G, where $\operatorname{Spec} B$ is some non-empty open subscheme of $\operatorname{Spec} \mathcal{O}$. This can be easily proven by considering an affine open subscheme of G to which R belongs. By taking $\operatorname{Spec} B$ sufficiently small we may assume that there is a model $\mathcal{G}$ for G over B which is a B-group scheme. Let $\mathfrak{p}$ be a non-zero prime ideal in the support of $\operatorname{Spec} B$.

We now define the reduction modulo $\mathfrak{p}$ for R. Call $\mathcal{O}_\mathfrak{p}$ the localization of $\mathcal{O}$ to $\mathfrak{p}$ and consider the extension $\mathcal{G} \times_B \mathcal{O}_\mathfrak{p}$. The point R also induces a morphism from $\operatorname{Spec} \mathcal{O}_\mathfrak{p}$ to G. The reduction of R modulo $\mathfrak{p}$ is a morphism from $\operatorname{Spec} k_\mathfrak{p}$ (where $k_\mathfrak{p}$ is the residue field) to the special fiber $G_\mathfrak{p} = \mathcal{G} \times_B k_\mathfrak{p}$ obtained in the following way:

1)extend R as a map from $\operatorname{Spec} \mathcal{O}_\mathfrak{p}$ to G;

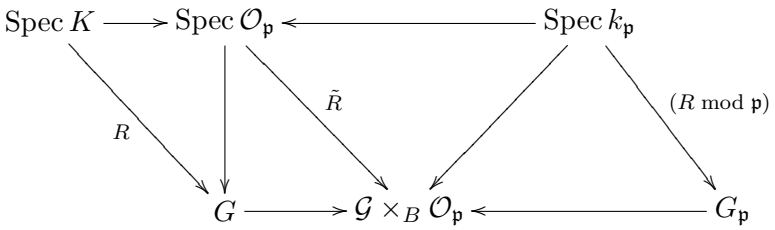
2)compose with the inclusion of G in $\mathcal{G} \times_B \mathcal{O}_\mathfrak{p}$ (call this point $\tilde{R}$);

3)compose with the morphism from $\operatorname{Spec} k_\mathfrak{p}$ to $\operatorname{Spec} \mathcal{O}_\mathfrak{p}$ induced by the quotient map from $\mathcal{O}_\mathfrak{p}$ to $k_\mathfrak{p}$;

4)restrict the image to $G_\mathfrak{p}$.

For 4) we just have to exclude that the image of the point $\mathcal{G} \times_B \mathcal{O}_\mathfrak{p}$ lies on the generic fiber of $\mathcal{G} \times_B \mathcal{O}_\mathfrak{p}$. This can be proven by comparing the characteristics: the elements in the support of the generic fiber have residue field of characteristic zero (since any affine open subscheme of the generic fiber has for ring of sections a K-algebra) while a $k_\mathfrak{p}$-point of a scheme (see [Har77, Chapter II, Exercise 2.7]) has for image an element in the support of the scheme whose residue field is $k_\mathfrak{p}$.

The following diagram illustrates the above procedure:



We call $(R \bmod \mathfrak{p})$ the reduction of the point R modulo $\mathfrak{p}$. Notice that on a point of $G(K)$ the reduction maps are defined for all but finitely many primes of K. In general, unless the algebraic group is projective the set of excluded primes depends on the point. This is because we have to exclude the prime ideals containing some denominators of the coordinates of the point. Nevertheless, we can define all but finitely many reduction maps on a finitely generated subgroup of $G(K)$.

In what follows we may assume that $G_\mathfrak{p}$ is an algebraic group over $k_\mathfrak{p}$ since this holds for all but finitely many primes $\mathfrak{p}$ of K.

Lemma 1.2.1. *The reduction map modulo $\mathfrak{p}$ induces a group homomorphism from the K-points of G which have a lift to $\operatorname{Spec} \mathcal{O}_\mathfrak{p}$ to the points in $G_\mathfrak{p}(k_\mathfrak{p})$.*

Proof. Let R_1 and R_2 be two K-points on G which can be lifted to morphisms from $\operatorname{Spec}\mathcal{O}_\mathfrak{p}$ to G. Extend their image and call $\tilde{R}_1$ and $\tilde{R}_2$ the lifts of R_1 and R_2 as morphisms from $\operatorname{Spec}\mathcal{O}_\mathfrak{p}$ to $\mathcal{G}\times_B\mathcal{O}_\mathfrak{p}$. Call m the multiplication of G and $\tilde{m}$ the multiplication of $\mathcal{G}\times_B\mathcal{O}_\mathfrak{p}$. By the unicity of the lifts and by Lemma 1.1.5, the point $m(R_1,R_2)$ lifts to $\tilde{m}(\tilde{R}_1,\tilde{R}_2)$. Call $m_\mathfrak{p}$ the multiplication in the special fiber. Since $m_\mathfrak{p}$ is induced by $\tilde{m}$, we deduce that

$$(m(R_1,R_2) \bmod \mathfrak{p}) = m_\mathfrak{p}((R_1 \bmod \mathfrak{p}),(R_2 \bmod \mathfrak{p})).$$

We draw a diagram to illustrate the situation:

$$\begin{array}{ccccc}
\operatorname{Spec}K & \xrightarrow{(R_1,R_2)} & G\times G & \xrightarrow{m} & G \\
\downarrow & & \downarrow & & \downarrow \\
\operatorname{Spec}\mathcal{O}_\mathfrak{p} & \xrightarrow{(\tilde{R}_1,\tilde{R}_2)} & (\mathcal{G}\times_B\mathcal{O}_\mathfrak{p})\times(\mathcal{G}\times_B\mathcal{O}_\mathfrak{p}) & \xrightarrow{\tilde{m}} & \mathcal{G}\times_B\mathcal{O}_\mathfrak{p} \\
\uparrow & & \uparrow & & \uparrow \\
\operatorname{Spec}k_\mathfrak{p} & \xrightarrow{((R_1 \bmod \mathfrak{p}),(R_2 \bmod \mathfrak{p}))} & G_\mathfrak{p}\times G_\mathfrak{p} & \xrightarrow{m_\mathfrak{p}} & G_\mathfrak{p}
\end{array}$$

□

We assume that $G_\mathfrak{p}$ is a $k_\mathfrak{p}$-algebraic group since this property holds for all but finitely many primes $\mathfrak{p}$ of K. Then in particular $G_\mathfrak{p}(k_\mathfrak{p})$ is a group. By the previous lemma, the identity of $G(K)$ goes to the identity of $G_\mathfrak{p}(k_\mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.

Lemma 1.2.2. *The group $G_\mathfrak{p}(k_\mathfrak{p})$ is finite. For every K-point R on G the reduction $(R \bmod \mathfrak{p})$ has finite order.*

Proof. Since the point $(R \bmod \mathfrak{p})$ belongs to $G_\mathfrak{p}(k_\mathfrak{p})$, the second assertion follows from the first. The scheme $G_\mathfrak{p}$ is of finite type over $k_\mathfrak{p}$. Then to prove the first assertion it suffices to show that $X(k_\mathfrak{p})$ is a finite set for every affine scheme X of finite type over $k_\mathfrak{p}$. The set $X(k_\mathfrak{p})$ is obviously a finite set since $k_\mathfrak{p}$ is a finite field. □

Extending the base field

Let L be a finite extension of K. Then we can identify the K-points on G with a subgroup of the L-points on $G\times_K L$. Let $\mathfrak{p}$ be a non-zero prime ideal of the ring of integers of K and let $\mathfrak{q}$ be a non-zero prime ideal of the ring of integers of L lying over $\mathfrak{p}$. Since we can choose for $G\times_K L$ a model which is the extension of the model of G (on a sufficiently small non-empty open subscheme of $\operatorname{Spec}\mathcal{O}$), the reduction modulo $\mathfrak{p}$ is encoded in the reduction modulo $\mathfrak{q}$. Then for all but finitely many primes $\mathfrak{p}$ of K the reduction of $G(L)$ modulo $\mathfrak{q}$ extends the reduction of $G(K)$ modulo $\mathfrak{p}$. The following

diagram is commutative

$$\begin{array}{ccc} G(L) \supseteq & G(\mathcal{O}_{L,\mathfrak{q}}) & \xrightarrow{\text{mod } \mathfrak{q}} G_{\mathfrak{q}}(k_{\mathfrak{q}}) \\ & \uparrow & \uparrow \\ G(K) \supseteq & G(\mathcal{O}_{K,\mathfrak{p}}) & \xrightarrow{\text{mod } \mathfrak{p}} G_{\mathfrak{p}}(k_{\mathfrak{p}}). \end{array}$$

where the horizontal maps are the reduction maps and the vertical maps are the inclusions. Notice that the maps in the diagram are group homomorphisms.

Lemma 1.2.3. *Let K be a number field and let G be an algebraic group over K. Let L be a finite extension of K. Let R be a K-point of G. For all but finitely many primes $\mathfrak{p}$ of K the following holds: for any prime $\mathfrak{q}$ of L lying over $\mathfrak{p}$ the order of $(R \bmod \mathfrak{q})$ equals the order of $(R \bmod \mathfrak{p})$.*

Proof. The assertion is an easy consequence of the following fact: we can define the reductions of G and of $G \times_K L$ by using two models such that one is obtained from the other by a base change. □

1.3 Reductions of morphisms

Let G be an be algebraic group defined over a number field K. In the last section we showed that for all but finitely many primes $\mathfrak{p}$ of K the multiplication by n commutes with the reduction modulo $\mathfrak{p}$ (see Lemma 1.2.1). The endomorphism $[n]$ induces for all but finitely many primes $\mathfrak{p}$ of K the endomorphism $[n]$ on the fiber $G_{\mathfrak{p}}$ and it lifts to the endomorphism $[n]$ on the model $\mathcal{G}$ (provided that the base scheme of the model is sufficiently small). More generally the following holds:

Proposition 1.3.1. *Let G_1 and G_2 be algebraic groups defined over a number field K and let ϕ be a K-morphism from G_1 to G_2. Then ϕ induces a $k_{\mathfrak{p}}$-morphism $\phi_{\mathfrak{p}}$ from $G_{1\mathfrak{p}}$ to $G_{2\mathfrak{p}}$ for all but finitely many primes $\mathfrak{p}$ of K.*

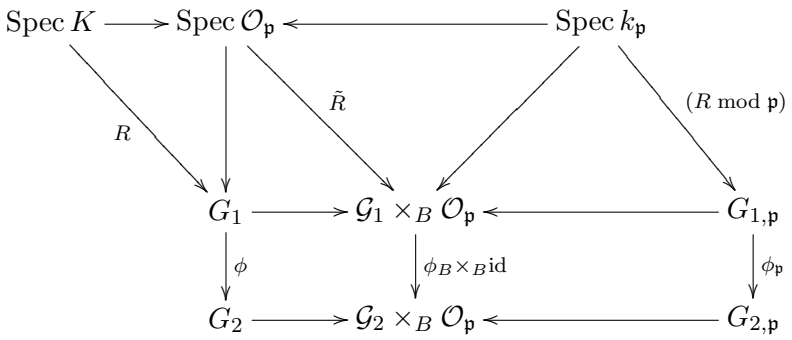
Proof. In section 1.1 we showed that ϕ lifts to a B-morphism ϕ_B between the models, where B is an open subscheme of the spectrum of the ring of integers of K. Then the specialization of ϕ_B to the special fiber corresponding to a prime $\mathfrak{p}$ provides the requested morphism $\phi_{\mathfrak{p}}$. □

By excluding finitely many primes $\mathfrak{p}$ of K we may assume that the models $\mathcal{G}_1$ and $\mathcal{G}_2$ of G_1 and G_2 (and hence the fibers $G_{1\mathfrak{p}}$ and $G_{2\mathfrak{p}}$) are group schemes. Suppose that the reduction modulo $\mathfrak{p}$ is defined on every K-point of G_1 and G_2 (for example this happens if G_1 and G_2 are abelian varieties). Then the following diagram of abelian groups is

commutative:

$$\begin{array}{ccc} G_1(K) & \xrightarrow{\bmod \mathfrak{p}} & G_{1,\mathfrak{p}}(k_\mathfrak{p}) \\ \Big\downarrow{\scriptstyle \phi} & & \Big\downarrow{\scriptstyle \phi_\mathfrak{p}} \\ G_2(K) & \xrightarrow[\bmod \mathfrak{p}]{} & G_{2,\mathfrak{p}}(k_\mathfrak{p}). \end{array}$$

In general we have to restrict to suitable subgroups of G_1 and G_2. See section 1.2. We illustrate the situation with the following diagram:



Corollary 1.3.2. *Let G_1 and G_2 be algebraic groups defined over a number field K. Let ϕ be a K-morphism from G_1 to G_2. Let R be in $G_1(K)$. Then for all but finitely many primes $\mathfrak{p}$ of K the order of $(\phi(R) \bmod \mathfrak{p})$ divides the order of $(R \bmod \mathfrak{p})$.*

Proof. The statement is an elementary property of finite groups because Proposition 1.3.1 implies the following: for all but finitely many primes $\mathfrak{p}$ of K the point $(\phi(R) \bmod \mathfrak{p})$ is the image of $(R \bmod \mathfrak{p})$ via a group homomorphism. □

Corollary 1.3.3. *Let G_1 and G_2 be algebraic groups defined over a number field K. Let ϕ be an invertible K-morphism from G_1 to G_2. Let R be in $G_1(K)$. Then for all but finitely many primes $\mathfrak{p}$ of K the order of $(R \bmod \mathfrak{p})$ equals the order of $(\phi(R) \bmod \mathfrak{p})$.*

Proof. It suffices to apply the previous corollary to ϕ and ϕ^{-1}. □

Lemma 1.3.4. *Let A and B be smooth, separated, reduced algebraic groups defined over a number field K. Let α be a K-isogeny from A to B. Let R be in $A(K)$. Let d be the exponent of the kernel of α (notice that d divides the degree of α). Then there exists $\hat{\alpha}$ in $\mathrm{Hom}_K(B, A)$ such that $\hat{\alpha} \circ \alpha = [d]$.*

Proof. We use the equivalence between K-group schemes and the functors from K-schemes to groups. See [vdGM, Proposition 3.6]. Let Z be a K-scheme. Then α and $[d]$ induce group homomorphisms α_Z and $[d]_Z$ from $A(Z)$ to $B(Z)$. The exponent of the kernel of α_Z divides d hence there exists a unique group homomorphism $\hat{\alpha}_Z$ such that $\hat{\alpha}_Z \circ \alpha_Z = [d]_Z$. It is easy to check that the group homomorphisms $\hat{\alpha}_Z$ are functorial in Z. Then they determine a unique morphism $\hat{\alpha}$ from B to A satisfying $\hat{\alpha} \circ \alpha = [d]$. A priori, $\hat{\alpha}$ is defined over a finite extension L of K (which we may suppose to be Galois).

For every $\sigma \in \mathrm{Gal}(L/K)$ we have $\hat{\alpha}^\sigma \circ \alpha = [d]$. By unicity, we conclude that $\hat{\alpha}$ is defined over K. □

Lemma 1.3.5. *Let A and B be smooth, separated, reduced algebraic groups defined over a number field K. Let α be an isogeny in $\mathrm{Hom}_K(A, B)$ and let d be the exponent of the kernel of α. Let R be a K-point of A. For all but finitely many primes $\mathfrak{p}$ of K the following holds: the order of $(dR \bmod \mathfrak{p})$ divides the order of $(\alpha(R) \bmod \mathfrak{p})$.*

Proof. Corollary 1.3.2 says that for every ψ in $\mathrm{Hom}_K(B, A)$ and for every point W in $B(K)$ the following holds: the order of $(\psi(W) \bmod \mathfrak{p})$ divides the order of $(W \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. Then it suffices to take $\psi = \hat{\alpha}$ and $W = \alpha(R)$ where $\hat{\alpha}$ is the isogeny in $\mathrm{Hom}_K(B, A)$ such that $\hat{\alpha} \circ \alpha = [d]$ (see Lemma 1.3.4). □

Chapter 2

Reductions of abelian varieties and tori

2.1 Algebraic subgroups of a semi-abelian variety

Let G be a semi-abelian variety defined over a number field K. In this section we prove that the group $G(\bar{K})$ is divisible (see Lemma 2.1.4) and that every connected K-algebraic subgroup of G is a semi-abelian variety (see Proposition 2.1.3).

Lemma 2.1.1. *Let A and T be respectively an abelian variety and a torus defined over a number field K. Then $\mathrm{Hom}_{\bar{K}}(A,T) = \{0\}$ and $\mathrm{Hom}_{\bar{K}}(T,A) = \{0\}$.*

Proof. We may obviously assume that A and T are non-zero. Since A is a complete variety and T is affine, there are no non-trivial morphisms from A to T. For the second equality to hold, it suffices to prove that every $\bar{K}$-morphism from $\mathbb{G}_m$ to A is zero. Let ϕ be in $\mathrm{Hom}_{\bar{K}}(\mathbb{G}_m, A)$. Since ϕ is a continuous map, the image of $\mathbb{G}_m$ is connected. Since $\phi(\mathbb{G}_m)$ is a connected algebraic subgroup of $A \times_K \bar{K}$, it is an abelian subvariety of $A \times_K \bar{K}$. The dimension of $\phi(\mathbb{G}_m)$ is less than or equal to the dimension of $\mathbb{G}_m$ hence it can only be zero or one. If it is zero then ϕ is zero. Now suppose that the image of ϕ has dimension one, which is to say that $\phi(\mathbb{G}_m)$ is an elliptic curve. Then the kernel of ϕ is an algebraic subgroup of $\mathbb{G}_m$ of dimension zero and ϕ is an isogeny (see the proof of [vdGM, Proposition 5.2]). We conclude because the multiplicative group is not isogenous to an elliptic curve (by the Hurwitz formula in [Sil86, Chapter II Theorem 5.9]). □

It is well-known that a connected algebraic subgroup of a torus is a torus and that a connected algebraic subgroup of an abelian variety is an abelian variety. We now prove that connected algebraic groups of the product of an abelian variety and a torus are again products of abelian varieties and tori.

Proposition 2.1.2. *Let K be a number field. Let $G = A \times T$ be the product of an abelian variety and a torus defined over K. Then a connected algebraic K-subgroup of G is the product of a K-abelian subvariety of A and a K-subtorus of T.*

Proof. Let V be an algebraic subgroup of G. Call π_A and π_T the projections of V on A and T respectively. Remark that $\pi_A(V)$ is a connected K-subgroup of A therefore it is an abelian subvariety of A. Similarly $\pi_T(V)$ is a connected K-subgroup of T therefore it is a subtorus of T. By replacing G with $\pi_A(V) \times \pi_T(V)$, we may assume that $\pi_A(V) = A$ and $\pi_T(V) = T$.

Write $N_T = \pi_T(V \cap (\{0\} \times T))$ and $N_A = \pi_A(V \cap (A \times \{0\}))$. Remark that N_A and N_T are K-algebraic subgroups of A and T respectively. It suffices to show that $N_A = A$ and $N_T = T$ because in that case $V = A \times T$ and we are done. To prove the assertion, we make a base change to $\bar{K}$. Since the category of commutative algebraic $\bar{K}$-schemes is abelian ([Gro70, Theorem p. 315 §5.4 Expose VI_A]) it suffices to see that the quotients $\hat{A} = A/N_A$ and $\hat{T} = T/N_T$ are zero. The quotient A/N_A^0 is an abelian variety (see [Pol03, §9.5]) and then the quotient of A/N_A^0 by the image of N_A in A/N_A^0 is an abelian variety (see [Mum70, Theorem 4 p.72]). Hence $\hat{A}$ is an abelian variety. Because of [Bor91, Corollary §8.5] the algebraic group T/N_T^0 is a torus. The quotient of T/N_T^0 by the image of N_T in T/N_T^0 is an affine algebraic group (see [Bor91, Theorem §6.8]). Hence $\hat{T}$ is an affine algebraic group.

Call α the composition of π_A and the quotient map from A to $\hat{A}$. Similarly call β the composition of π_T and the quotient map from T to $\hat{T}$. The product map $\alpha \times \beta$ is a map from V to $\hat{A} \times \hat{T}$. Now we show that the projection $\pi_{\hat{A}}$ from $\alpha \times \beta(V)$ to $\hat{A}$ is an isomorphism. Clearly $\pi_{\hat{A}}$ is an epimorphism. Since we are working in an abelian category, it suffices to show that $\pi_{\hat{A}}$ is a monomorphism. Because the map $\alpha \times \beta$ from V to $\alpha \times \beta(V)$ is an epimorphism, it suffices to check that the maps $\pi_{\hat{A}} \circ (\alpha \times \beta)$ and $\alpha \times \beta$ have the same kernel. The kernel of the first map is $V \cap (N_A \times T)$. The kernel of the second map is $V \cap (N_A \times T) \cap (A \times N_T)$. We show that these two group schemes are isomorphic because they have the same groups of Z-points for every $\bar{K}$-scheme Z. The Z-points of the first kernel are the pairs (a, b) in $V(Z)$ such that a lies in $N_A(Z)$. Since $(a, 0)$ belongs to $V(Z)$ we deduce that $(0, b)$ lies in $V(Z)$ and so b belongs to $N_T(Z)$. Then the two kernels have the same Z-points. The proof that $\alpha \times \beta(V)$ is isomorphic to $\hat{T}$ is analogous. We deduce that $\hat{A}$ and $\hat{T}$ are isomorphic. Since $\hat{A}$ is a complete variety while $\hat{T}$ is affine the only possible morphism from $\hat{A}$ to $\hat{T}$ is zero. Then $\hat{A}$ and $\hat{T}$ are zero. □

Now we prove that the connected algebraic subgroups of a semi-abelian variety are semi-abelian varieties.

Proposition 2.1.3. *Let G be a semi-abelian variety defined over a number field K. Let H be a connected subgroup of G. Then H is a semi-abelian variety.*

Proof. Let G be defined by the following sequence:

$$0 \longrightarrow T \xrightarrow{f} G \xrightarrow{g} A \longrightarrow 0.$$

We prove that H is a semi-abelian variety by showing that the following sequence is exact, that $(T \cap H)$ is a torus and that $g(H)$ is an abelian variety:

$$0 \longrightarrow (T \cap H) \xrightarrow{f} G \xrightarrow{g} g(H) \longrightarrow 0.$$

The maps f and g are here the restrictions of the maps defining G. It is evident that the kernel of the restriction of g to H is $T \cap H$. By definition, H is mapped to $g(H)$. Since we are working with smooth, separated and reduced algebraic groups, this is sufficient to prove that the sequence is exact. It is left to show that $g(H)$ is an abelian variety and $H \cap T$ is a torus. Since H is connected, $g(H)$ is connected. Then $g(H)$ is a connected algebraic subgroup of the abelian variety A hence it is an abelian variety. Since H and T are connected, the intersection $H \cap T$ is a connected algebraic subgroup of T. Then $H \cap T$ it is a torus. This concludes the proof. □

Let G be a semi-abelian variety defined over a number field K. We now prove that $G(\bar{K})$ is a divisible group.

Lemma 2.1.4. *Let G be a semi-abelian variety defined over a number field K. Then $G(\bar{K})$ is a divisible group.*

Proof. The statement is obvious for $\mathbb{G}_m$ hence it is true for tori. Also the statement is well known for abelian varieties. Let G be defined by the following sequence:

$$0 \longrightarrow T \xrightarrow{f} G \xrightarrow{g} A \longrightarrow 0.$$

We then have

$$0 \longrightarrow T(\bar{K}) \xrightarrow{f} G(\bar{K}) \xrightarrow{g} A(\bar{K}) \longrightarrow 0.$$

Let R be a point in $G(\bar{K})$. Call P a point in $A(\bar{K})$ such that $nP = g(R)$. Let Q be a point in $g^{-1}(P)$. Then $nQ - R$ is in the kernel of g therefore it belongs to $T(\bar{K})$. Call Z a point in $T(\bar{K})$ such that $nZ = nQ - R$. Then the point $Q - Z$ is in $G(\bar{K})$ and $n(Q - Z) = nQ - (nQ - R) = R$. □

2.2 Models of abelian varieties and tori

Models for tori

Let K be a number field, let $\mathcal{O}$ be the ring of integers of K. If $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}$, call $k_\mathfrak{p}$ the residue field.

Lemma 2.2.1. *The multiplicative group $\mathbb{G}_{m,K}$ admits a model $\mathcal{G}$ over $\mathcal{O}$ such that for every prime $\mathfrak{p}$ of $\mathcal{O}$ the special fiber of $\mathcal{G}$ over $\mathfrak{p}$ is the multiplicative group $\mathbb{G}_{m,k_\mathfrak{p}}$.*

Proof. The proof is immediate. □

Proposition 2.2.2. *Let G be the product $\mathbb{G}_{m,K}^n$ of copies of the multiplicative group. Then G admits a model $\mathcal{G}$ over $\mathcal{O}$ such that for every prime $\mathfrak{p}$ of $\mathcal{O}$ the special fiber of $\mathcal{G}$ over $\mathfrak{p}$ is the algebraic group $\mathbb{G}_{m,k_\mathfrak{p}}^n$.*

Proof. By Lemma 1.1.11, the statement is a consequence of Lemma 2.2.1. □

Proposition 2.2.3. *Let G be a torus of dimension $n \geq 1$. Then G admits a model $\mathcal{G}$ over an open subscheme U of* $\mathrm{Spec}(\mathcal{O})$ *such that for every prime $\mathfrak{p}$ of U the special fiber of $\mathcal{G}$ over $\mathfrak{p}$ is a torus of dimension n.*

Proof. Let L be a finite extension of K where G splits. Then a model for $G \times_K L$ is isomorphic to the model of $\mathbb{G}^n_{m,L}$ (on a non-empty open subscheme of the spectrum of the ring of integers of L). We deduce that for all but finitely many primes $\mathfrak{q}$ of L the fiber of the model of $G \times_K L$ is a split torus of dimension n (this fiber being $k_\mathfrak{q}$-isomorphic to the fiber $\mathbb{G}^n_{m,k_\mathfrak{q}}$ of the model of $\mathbb{G}^n_{m,L}$). Call $\mathcal{G}$ a model for G. Since the extension of $\mathcal{G}$ is a model for $G \times_K L$, by Theorem 1.1.7 we deduce that the extension of the fiber $G_\mathfrak{p}$ is a split torus of dimension n for all but finitely many primes $\mathfrak{p}$ of K. Then the fiber $G_\mathfrak{p}$ is a torus of dimension n for all but finitely many primes $\mathfrak{p}$ of K. □

Néron models for abelian varieties

Abelian varieties admit a special model, called the (global) Néron model. It is a model over the ring of integers $\mathcal{O}$ uniquely defined by an universal property. It makes sense to use the Néron model whenever we want to make reductions of an abelian variety. In any case, by Lemma 1.1.7 some of the properties of the Néron model extend to properties of any model. A peculiarity of the Néron model is that with this model we can reduce A modulo $\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}$.

The Néron model is a general construction in scheme theory. We refer to the book of Bosh, Lütkebohmert Raynaud [SBR90], which is the standard reference for the subject.

Let A be an abelian variety defined over a number field K. Call $\mathcal{O}$ the ring of integers of K.

Definition 2.2.4 (Néron model)**.** *The Néron model of A over* $\mathrm{Spec}\,\mathcal{O}$ *is an $\mathcal{O}$-model of A which is smooth, separated, of finite type over $\mathcal{O}$ and such that it satisfies the so-called Néron mapping property: for any smooth $\mathcal{O}$-scheme Y and for any K-morphism from the generic fiber of Y to A there exists unique an $\mathcal{O}$-morphism from Y to $\mathcal{A}$ extending it.*

The $\mathcal{O}$-Néron model $\mathcal{A}$ of A exists and it is unique up to canonical isomorphism. The uniqueness follows from the fact that the Néron mapping property is a universal property. Notice that the Néron model of a product of abelian varieties is the product of their Néron models.

The Néron model $\mathcal{A}$ is an $\mathcal{O}$-group scheme hence it induces a group scheme structure on each fiber. The K-group scheme structure on A coincides with the group scheme structure induced by the $\mathcal{O}$-Néron model. Because of the universal property, there exists a group isomorphism between $A(K)$ and $\mathcal{A}(\mathcal{O})$.

Call $\mathcal{O}_\mathfrak{p}$ the localization of $\mathcal{O}$ to the complement of $\mathfrak{p}$. A prime $\mathfrak{p}$ of $\mathcal{O}$ is said to be of good reduction for A if the $O_\mathfrak{p}$-scheme $\mathcal{A} \otimes_\mathcal{O} \mathcal{O}_\mathfrak{p}$ is proper. This implies that for the residue field $k_\mathfrak{p}$ the $k_\mathfrak{p}$-group scheme $\mathcal{A}_{k_\mathfrak{p}} = \mathcal{A} \otimes_\mathcal{O} \mathrm{Spec}\, k_\mathfrak{p}$ is an abelian variety over $k_\mathfrak{p}$ of the same dimension of A. All but finitely many primes of $\mathcal{O}$ are of good reduction (see [SBR90, Theorem 3 p. 19]). As a consequence of Lemma 1.1.7 we have the following:

Remark 2.2.5. *Let A be an abelian variety defined over a number field K. Call $\mathcal{O}$ the ring of integers of K. Fix a model $\mathcal{A}$ for A on a non-empty open subscheme of* $\operatorname{Spec}\mathcal{O}$. *Then for almost all primes $\mathfrak{p}$ of $\mathcal{O}$ the fiber $A_{\mathfrak{p}}$ is an an abelian variety defined over the residue field $k_{\mathfrak{p}}$ and it has the same dimension of A.*

Now we describe how we can use equations to define the reduction maps for an abelian variety. There is a non-empty open subscheme $\operatorname{Spec} B$ of $\operatorname{Spec}\mathcal{O}$ such that the extension of the Néron model to $\operatorname{Spec} B$ is projective. Thanks to the projectivity, one can write down equations for this model. These equations also describe A while the reduction modulo $\mathfrak{p}$ of these equations describe the fiber $A_{\mathfrak{p}}$. Let R be an element of $A(K)$ and consider projective coordinates of R such that the $\mathfrak{p}$-adic valuation is zero for at least one coordinate. Then one obtaines coordinates for the reduction of R modulo $\mathfrak{p}$ simply by reducing each coordinate modulo $\mathfrak{p}$.

Model for the product of an abelian variety and a torus

Proposition 2.2.6. *Let $G = A \times T$ be the product of an abelian variety of dimension n and a torus of dimension m defined over a number field K. Then G admits a model $\mathcal{G}$ over an open subscheme U of* $\operatorname{Spec}(\mathcal{O})$ *such that for every prime $\mathfrak{p}$ of U the fiber of $\mathcal{G}$ over $\mathfrak{p}$ is the product of an abelian variety of dimension n and a torus of dimension m.*

Proof. By Lemma 1.1.11, the statement is an immediate consequence of Proposition 2.2.3 and of Remark 2.2.5 (where the statement is proven for a torus and for an abelian variety respectively). □

2.3 The reductions of torsion points

We first prove a very simple but useful property of the reduction maps: a non-zero point is in the kernel of only finitely many reduction maps.

Proposition 2.3.1. *Let G be a semi-abelian variety defined over a number field K. Let R be a K-point on G. There are only finitely many prime ideals $\mathfrak{p}$ of K such that* $(R \bmod \mathfrak{p})$ *is zero.*

Proof. Let G be the extension of an abelian variety A by a torus T:

$$0 \longrightarrow T \longrightarrow G \xrightarrow{\pi} A \longrightarrow 0.$$

First we show that it suffices to prove the assertion for A and for T respectively. Suppose that there are infinitely many primes $\mathfrak{p}$ such that $(R \bmod \mathfrak{p})$ is zero. By Corollary 1.3.2 we deduce that there are infinitely many primes $\mathfrak{p}$ such that $(\pi(R) \bmod \mathfrak{p})$ is zero. If the assertion is true for A we deduce that $\pi(R)$ is zero. Then R is a K-point on T and it suffices to apply the statement for T.

Now we prove the statement for T. Since T is an affine scheme its reduction can be described by equations (see section 1.1). Then we can consider the coordinates of R and

of the zero-point. By a translation we may assume that the coordinates of the zero point are all zero. We conclude because of the well-known statement about number fields that a non-zero element of the ring of integers belongs only to finitely many prime ideals of the ring of integers.

Now we prove the statement for A. Since A is a projective scheme, there exists an affine open subscheme containing R and the zero point (see [Liu02, Proposition 3.36 (b)]). Now we can analogously use the equations to conclude. □

Corollary 2.3.2. *Let G be a semi-abelian variety defined over a number field K. If R_1 and R_2 are distinct points of $G(K)$ then there are only finitely many prime ideals $\mathfrak{p}$ of K such that $(R_1 \bmod \mathfrak{p})$ equals $(R_2 \bmod \mathfrak{p})$.*

Proof. By excluding finitely many primes $\mathfrak{p}$ of K, we may assume the following: the reduction modulo $\mathfrak{p}$ is defined on R_1, R_2, $R_1 - R_2$ and on the identity of $G(K)$; the points R_1 and R_2 belong to $G(\mathcal{O}_\mathfrak{p})$. Since G is a group scheme then the reduction map modulo $\mathfrak{p}$ gives a group homomorphism from $G(\mathcal{O}_\mathfrak{p})$ to $G_\mathfrak{p}(k_\mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K (see Lemma 1.2.1). In particular the reduction modulo $\mathfrak{p}$ of the identity of $G(K)$ is the identity of $G_\mathfrak{p}(k_\mathfrak{p})$. Then we may assume that $R_2 = 0$ (by replacing R_1 by $R_1 - R_2$) and we can apply the previous proposition. □

Corollary 2.3.3. *Let G be a semi-abelian variety defined over a number field K. Let R be a point in $G(K)$ of infinite order. Then the order of $(R \bmod \mathfrak{p})$ cannot assume the same value for infinitely many primes $\mathfrak{p}$ of K.*

Proof. Suppose that the order of $(R \bmod \mathfrak{p})$ equals some integer $n > 0$ for infinitely many primes $\mathfrak{p}$ of K. From the proposition we deduce that $nR = 0$. Since R has infinite order, we have a contradiction. □

Corollary 2.3.4. *Let G be a semi-abelian variety defined over a number field K. For all but finitely many primes $\mathfrak{p}$ of K the reduction modulo $\mathfrak{p}$ restricted to the torsion of $G(K)$ is injective. In particular, let R be a torsion point in $G(K)$. Then the order of $(R \bmod \mathfrak{p})$ equals the order of R for all but finitely many primes $\mathfrak{p}$ of K.*

Proof. The torsion subgroup of $G(K)$ is a finite group. Then to prove the first assertion it suffices to apply Corollary 2.3.2 to every pair of points in the torsion subgroup of $G(K)$.

Call n the order of R. The point $(nR \bmod \mathfrak{p})$ is zero for almost all primes $\mathfrak{p}$ of K because of Lemma 1.2.1. Suppose that there exist infinitely many primes such that the order of $(R \bmod \mathfrak{p})$ is not the order of R. We deduce that there exists an integer d dividing n and different from n such that $(dR \bmod \mathfrak{p})$ is zero for infinitely many primes $\mathfrak{p}$ of K. By Proposition 2.3.1 we deduce that $dR = 0$, a contradiction. □

Lemma 2.3.5. *Let A be an abelian variety defined over a number field K. Let m be a non-zero integer such that $A[m]$ is defined over K. Then for all but finitely many primes $\mathfrak{p}$ of K the reduction modulo $\mathfrak{p}$ induces an isomorphism from $A[m]$ to $A_\mathfrak{p}[m]$ (where $A_\mathfrak{p}$ is the reduction of A modulo $\mathfrak{p}$).*

Proof. For all but finitely many primes $\mathfrak{p}$ of K, m is coprime to the characteristic of $k_\mathfrak{p}$ and $A_\mathfrak{p}$ is an abelian variety of the same dimension of K. Then $A[m]$ and $A_\mathfrak{p}[m]$ have the same cardinality. For all but finitely many primes $\mathfrak{p}$ of K the reduction modulo $\mathfrak{p}$ is a group homomorphism (see Lemma 1.2.1) hence it maps $A[m]$ to $A_\mathfrak{p}[m]$. By the previous corollary, for all but finitely many primes $\mathfrak{p}$ of K the reduction modulo $\mathfrak{p}$ restricted to the torsion of $A(K)$ is injective. An injective map between finite sets of the same cardinality is a bijection hence the statement follows. □

Lemma 2.3.6. *Let T be a torus defined over a number field K. Let m be a non-zero integer such that $T[m]$ is defined over K. Then for all but finitely many primes $\mathfrak{p}$ of K the reduction modulo $\mathfrak{p}$ induces an isomorphism from $T[m]$ to $T_\mathfrak{p}[m]$ (where $T_\mathfrak{p}$ is the reduction of T modulo $\mathfrak{p}$).*

Proof. By Lemma 1.2.1, the reduction modulo $\mathfrak{p}$ induces a group homomorphism from $T(K)$ to $T_\mathfrak{p}(k_\mathfrak{p})$ and hence from $T[m]$ to $T_\mathfrak{p}[m]$. By Corollary 2.3.4, the reduction modulo $\mathfrak{p}$ is injective on $T[m]$ for all but finitely many primes $\mathfrak{p}$. It suffices to prove the surjectivity. We do this by showing that the finite groups $T[m]$ and $T_\mathfrak{p}[m]$ have the same cardinality for all but finitely many primes $\mathfrak{p}$ of K. We may assume that T is split therefore by Lemma 1.1.11 it suffices to prove the statement for $\mathbb{G}_m$. The statement for $\mathbb{G}_m$ is immediate. □

Proposition 2.3.7. *Let G be a semi-abelian variety defined over a number field K. Let m be a non-zero integer such that $G[m]$ is defined over K. Then for all but finitely many primes $\mathfrak{p}$ of K the reduction modulo $\mathfrak{p}$ induces an isomorphism from $G[m]$ to $G_\mathfrak{p}[m]$ (where $G_\mathfrak{p}$ is the reduction of G modulo $\mathfrak{p}$).*

Proof. This result is proven in [Kow03, Lemma 4.4]. □

Let G be a semi-abelian variety defined over a number field K. In general the reduction map modulo $\mathfrak{p}$ does not give a surjection from $G(K)$ to $G_\mathfrak{p}(k_\mathfrak{p})$, as the following example shows.

Example 2.3.8. Let E be an elliptic curve defined over $\mathbb{Q}$ and suppose that $E(K)$ is a finite group. By varying $\mathfrak{p}$ into the rational primes we know by the Hasse-Weil bound that the cardinality of $E_\mathfrak{p}(k_\mathfrak{p})$ is not bounded. Then for sufficiently large primes $\mathfrak{p}$ the reduction map from $E(K)$ to $E_\mathfrak{p}(k_\mathfrak{p})$ is not surjective.

Chapter 3

Independent points on semi-abelian varieties

3.1 The algebraic subgroup generated by a point

Let G be a connected, smooth, separated, reduced algebraic group defined over a number field K. Let Λ be a subgroup of $G(K)$. We now describe the Zariski closure of Λ in G.

Fix an algebraic closure $\bar{K}$ of K and call $G_{\bar{K}}$ the extension of G to $\bar{K}$. Define $H_{\bar{K}}$ as the smallest closed subscheme of $G_{\bar{K}}$ (with reduced structure) whose set of $\bar{K}$-points contains Λ. Notice that $H_{\bar{K}}$ is the intersection of all closed subschemes of $G_{\bar{K}}$ whose set of $\bar{K}$-points contains Λ. We say that $H_{\bar{K}}$ is the Zariski closure of Λ in $G_{\bar{K}}$ since Λ is Zariski-dense in $H_{\bar{K}}(\bar{K})$ and $H_{\bar{K}}$ is the smallest closed subscheme of $G_{\bar{K}}$ with this property.

Since Λ is a set of K-points, $H_{\bar{K}}(\bar{K})$ contains a dense subset consisting of K-points. Therefore $H_{\bar{K}}$ is defined over K. We write $H_{\bar{K}}$ as H_K when we consider it as a K-scheme. We call H_K the *Zariski closure* of Λ in G. Notice that H_K is the smallest closed subscheme of G whose set of K-points contains Λ.

Let L be an algebraic extension of K and let G_L denote the extension of G to L. We can see Λ as a subgroup of G_L and analogously define H_L as the the Zariski closure of Λ in G_L. It is then obvious that H_L is the extension of H_K obtained by changing the base from K to L. In this sense we say that the Zariski closure of Λ in G does not depend on the base field. The following remark shows that H_K is the algebraic subgroup of G generated by Λ (i.e. the smallest algebraic subgroup of G that contains the points in Λ).

Remark 3.1.1. *H_K is a K-algebraic subgroup of G.*

Proof. It suffices to prove that the K-morphisms e, i and m which define the group structure of $G_{\bar{K}}$ can be restricted to $H_{\bar{K}}$.

Because Λ is a subgroup then $H_{\bar{K}}(\bar{K})$ contains the identity of G. We now prove that the inverse map i of G maps $H_{\bar{K}}$ to $H_{\bar{K}}$. Equivalently we can show that that $f \circ i = 0$ on $H_{\bar{K}}$ for every f defining $H_{\bar{K}}$. Because the base field is algebraically closed and the scheme $H_{\bar{K}}$ is reduced it suffices to check that $f \circ i$ is zero on $H_{\bar{K}}(\bar{K})$. Thus it suffices to

show that i maps $H_{\bar{K}}(\bar{K})$ to $H_{\bar{K}}(\bar{K})$. This fact follows immediately by continuity since Λ is stable by inversion (recall that Λ is Zariski-dense in $H_{\bar{K}}(\bar{K})$).

We are left to prove that m carries $H_{\bar{K}} \times H_{\bar{K}}$ into $H_{\bar{K}}$. Because the base field is algebraically closed and the scheme $H_{\bar{K}} \times H_{\bar{K}}$ is reduced (since $H_{\bar{K}}$ is reduced) it suffices to check that $f \circ m$ is zero on $H_{\bar{K}} \times H_{\bar{K}}(\bar{K})$. Thus it suffices to show that m maps $H_{\bar{K}} \times H_{\bar{K}}(\bar{K})$ to $H_{\bar{K}}(\bar{K})$.

For every R in Λ the set $\Lambda \times \{R\}$ is carried by m into $H_{\bar{K}}(\bar{K})$. Since Λ is Zariski-dense in $H_{\bar{K}}(\bar{K})$, by continuity of the multiplication the set $H_{\bar{K}}(\bar{K}) \times \{R\}$ is also carried by m into $H_{\bar{K}}(\bar{K})$. So for every $P \in H_{\bar{K}}(\bar{K})$ the set $\{P\} \times \Lambda$ is mapped by m into $H_{\bar{K}}(\bar{K})$. Again by continuity of m, the set $\{P\} \times H_{\bar{K}}(\bar{K})$ is carried into $H_{\bar{K}}(\bar{K})$. This proves the assertion. □

From the previous remark it follows that H_L is the smallest algebraic subgroup of G_L whose set of K-points contains Λ, for every algebraic extension L of K.

Let G be a connected, smooth, separated, reduced algebraic group defined over a number field K. Let R be a K-point on G. The algebraic subgroup of G generated by R (the smallest algebraic subgroup of G that contains the points R) is also the algebraic subgroup of G generated by the group $\mathbb{Z}R$. Thus it is the Zariski closure of $\mathbb{Z}R$ in $G \times_K \bar{K}$. We call it G_R. For every algebraic extension L of K we have that G_R is the smallest algebraic L-subgroup of G such that R is an L-point. Write G_R for the algebraic subgroup of G generated by R and G_R^0 for the connected component of the identity of G_R. In particular, G_R^0 is an algebraic K-subgroup of G defined over K. Write n_R for the number of connected components of G_R. The number n_R does not get affected by a change of ground field: since $\mathbb{Z}R$ is Zariski-dense in $G_R(\bar{K})$ then every connected component of G_R is a translate of G_R^0 by a K-point therefore it is also defined over K.

Lemma 3.1.2. *For every integer $d \neq 0$ we have $G_{dR}^0 = G_R^0$. In particular the dimension of G_{dR} equals the dimension of G_R.*

Proof. Since G_R contains dR we have by definition $G_{dR} \subseteq G_R$. Therefore $G_{dR}^0 \subseteq G_R^0$. Since these algebraic groups are connected, it suffices to prove that they have the same dimension. Clearly the dimension of G_{dR}^0 is less or equal than the dimension of G_R^0. To prove the other inequality it suffices to show that the multiplication by $[d]$ (which is an isogeny) maps G_R into G_{dR}. It suffices to prove that the preimage $[d]^{-1}G_{dR}$ contains G_R. This is true because this preimage is an algebraic subgroup of G which contains the point R. □

Remark 3.1.3. *Let G and G' be connected, smooth, separated, reduced algebraic groups defined over a number field K. Let R be in $G(K)$ and let α be in $\mathrm{Hom}_K(G, G')$. Then $G_{\alpha(R)} \subseteq \alpha(G_R)$. If α is an isogeny then $G_{\alpha(R)}$ and $\alpha(G_R)$ have the same dimension.*

Proof. Since $\alpha(G_R)$ is an algebraic group containing $\alpha(R)$, by definition we have $G_{\alpha(R)} \subseteq \alpha(G_R)$. Then clearly the dimension of $G_{\alpha(R)}$ is less than or equal to the dimension of $\alpha(G_R)$. Now suppose that α is an isogeny. Then the dimension of $\alpha(G_R)$ equals the

dimension of G_R. So it suffices to prove that the dimension of G_R is less than or equal to the dimension of $\alpha(G_R)$. Let $\hat{\alpha}$ be the isogeny in $\mathrm{Hom}_K(G', G)$ such that $\hat{\alpha} \circ \alpha = [d]$ where $d \neq 0$ is the degree of α, see Lemma 1.3.4. Then we have $G_{dR} = G_{\hat{\alpha}\circ\alpha(R)} \subseteq G_{\alpha(R)} \subseteq \alpha(G_R)$. By Lemma 3.1.2, the dimension of G_R equals the dimension of G_{dR} and we conclude. □

Lemma 3.1.4. *Let G be a connected, smooth, separated, reduced algebraic group defined over a number field K. Let R be a K-point on G such that $G_R^0(\bar{K})$ is divisible (e.g. if G is a semi-abelian variety, see Lemma 2.1.4). Then $G_{n_R R} = G_R^0$. Furthermore, let H be a connected component of G_R. Then there exists a torsion point X in $G_R(\bar{K})$ such that $H = X + G_R^0$.*

Proof. Clearly G_R^0 contains $G_{n_R R}$. In particular G_R^0 contains $G_{n_R R}^0$. By Lemma 3.1.2 the last two algebraic groups have the same dimension. Since they are connected and one is contained in the other they are equal. It follows that G_R^0 is contained in $G_{n_R R}$. So we have $G_{n_R R} = G_R^0$.

Let P be any point in $H(\bar{K})$. Then $P + G_R^0 = H$. The point $n_R P$ is in $G_R^0(\bar{K})$. Since $G_R^0(\bar{K})$ is divisible, there exists a point Q in $G_R^0(\bar{K})$ such that $n_R Q = n_R P$. Set $X = P - Q$, thus X is a torsion point in $G_R(\bar{K})$. Then we have:

$$H = P + G_R^0 = P - Q + G_R^0 = X + G_R^0.$$

□

The following lemma shows in particular that the group of components G/G_R^0 is cyclic of order n_R.

Lemma 3.1.5. *Let G be a connected, smooth, separated, reduced algebraic group defined over a number field K. Let R be a K-point on G. Call W the connected component of G_R containing R and let X be a torsion point in $G(\bar{K})$ such that $W = X + G_R^0$. Then $n_R X$ is the least positive multiple of X belonging to G_R^0. Furthermore the connected components of G_R are the translated of G_R^0 of the form $W_d = dX + G_R^0$ where $1 \leq d \leq n_R$.*

Proof. By definition of n_R, $n_R W = G_R^0$ hence $n_R X$ belongs to G_R^0. Thus the first assertion is a consequence of the second assertion, which we now prove. Since X does not belong to G_R^0 we have $W_d \neq W_d'$ whenever $d \neq d'$. Then the set of the W_d's has the same cardinality of the set of the connected components of G_R. So it suffices to show that any connected component of G_R is of the form W_d for some d in $\{1, \ldots, n_R\}$. Let C be a connected component of G_R. Consider the intersection $C \cap W_d$ for some fixed d in $\{1, \ldots, n_R\}$. Then $C \cap W_d$ is either empty or it has the dimension of G_R^0 because C is a translate of G_R^0 by Lemma 3.1.4. Suppose that $C \neq W_d$ is not empty. Since C (respectively W_d) is connected, it follows that $C \cap W_d$ coincides with C (respectively W_d). This concludes the proof. □

Lemma 3.1.6. *Let G be a connected, smooth, separated, reduced algebraic group defined over a number field K. Let R be a K-point on G. Call W the connected component of*

G_R containing R and let X be a torsion point in $G(\bar{K})$ such that $W = X + G_R^0$. Let L be a finite extension of K where X is defined. Then for all but finitely many primes $\mathfrak{q}$ of L the point $(n_R X \bmod \mathfrak{q})$ is the least multiple of $(X \bmod \mathfrak{q})$ belonging to $(G_R^0 \bmod \mathfrak{q})$.

Proof. Call x the order of X. To prove the statement, we may assume that the points in $G_R[x]$ are defined over L. Suppose that the statement is not true and let d be an integer not divisible by n_R such that for infinitely many primes $\mathfrak{q}$ of L the point $(dX \bmod \mathfrak{p})$ belongs to $(G_R^0 \bmod \mathfrak{q})$. Up to excluding finitely many primes $\mathfrak{q}$, we may assume that the reduction modulo $\mathfrak{q}$ maps injectively $G_R[x]$ to $(G_R \bmod \mathfrak{q})[x]$ and that it maps surjectively $G_R^0[x]$ onto $(G_R^0 \bmod \mathfrak{q})[x]$. See [Kow03, Lemma 4.4]. We deduce that dR belongs to $G_R^0[x]$. We have a contradiction since by Lemma 3.1.5 $n_R X$ is the least positive multiple of X which belongs to $G_R^0(\bar{K})$. □

3.2 A bound on the number of connected components

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-point on G. In the following proposition we bound the number of connected components of the algebraic subgroup of G generated by R with a constant depending only on G and K. We apply this proposition in Chapters 6 and 7. To prove it, we use the results of Chapter 4.

Lemma 3.2.1. *Let A be an abelian variety defined over a number field K. There exists a non-zero integer t such that the following holds: for every K-point R on A there exists an abelian subvariety Z of A defined over K such that $G_R^0 + Z = A$ and $G_R^0 \cap Z$ has finite order dividing t.*

Proof. This Lemma is proven in [Ber87, Appendix, Proposition 2]. Its proof can also be found in [RU07, Appendix, Proposition 5.1]. □

Proposition 3.2.2. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-point on G. Then n_R divides a constant which depends only on G and K.*

Proof. Write $G = A \times T$ and $R = (R_A, R_T)$. Since $G_R \subseteq G_{R_A} \times G_{R_T}$ we have $G_R^0 \subseteq (G_{R_A} \times G_{R_T})^0 = G_{R_A}^0 \times G_{R_T}^0$. The algebraic group G_R^0 is the product of an abelian subvariety A' of $G_{R_A}^0$ and a subtorus T' of $G_{R_T}^0$ by Proposition 2.1.2. We have $A' = G_{R_A}^0$ because A' is connected and contains a non-zero multiple of R_A. Analogously $T' = G_{R_T}^0$ because T' is connected and contains a non-zero multiple of R_T. So $G_R^0 = (G_{R_A} \times G_{R_T})^0$. Then n_R divides $n_{R_A} \cdot n_{R_T}$, which is the number of connected components of $G_{R_A} \times G_{R_T}$. Consequently, it suffices to prove the statement for A and for T respectively.

For A the statement is proven in [McQ95, Lemma 2.2.4]. Now we prove the statement for T: we reduce at once to the case $T = \mathbb{G}_m^n$ since for any R in $T(K)$ the number n_R is not affected by an algebraic extension of the ground field. Write $R = (R_1, \ldots, R_n)$ and let e be the exponent of $\mathbb{G}_m(K)_{tors}$. Since n_R divides e times n_{eR}, we reduce at once to the case where for every i the point R_i is either zero or has infinite order. It

suffices to prove that in this case for every rational prime ℓ one has $v_\ell(n_R) = 0$. Fix a rational prime ℓ. Remark that $R_1, \ldots, R_n$ generate a torsion-free subgroup of $\mathbb{G}_m(K)$ and that $\mathrm{End}_K \mathbb{G}_m = \mathbb{Z}$. Then an elementary argument on abelian groups shows that there exists a set $J = \{j_1, \ldots, j_s\}$ and points $P_{j_1}, \ldots, P_{j_s}$ in $\mathbb{G}_m(K)$ such that the point $R' = (P_{j_1}, \ldots, P_{j_s})$ is independent in $\mathbb{G}_m^s(K)$ and the order of $(R \bmod \mathfrak{p})$ equals the order of $(R' \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. By Theorem 4.2.1 there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(R' \bmod \mathfrak{p})] = 0$. Then for infinitely many primes $\mathfrak{p}$ of K we have $v_\ell[\mathrm{ord}(R \bmod \mathfrak{p})] = 0$. By Theorem 4.1.1 it follows that $v_\ell(n_R) = 0$. □

Notice that the above proof shows that if G is a torus then n_R is bounded by the exponent of $\mathbb{G}_m(L)$ (where L is any extension of K where G splits).

3.3 Equivalent definitions of independent point

Let G be a semi-abelian variety defined over a number field K. Let R be a K-point on G of infinite order. The point R is independent if the algebraic subgroup generated by R in G (i.e. the smallest algebraic subgroup of G containing R) is G itself.

Definition 3.3.1. *Let G be a semi-abelian variety defined over a number field K. Let R be a non-zero K-point on G. We say that R is independent if $G_R = G$.*

Notice that by this definition an independent point has infinite order. Also notice that this definition does not depend on the choice of the number field K such that R belongs to $G(K)$.

For the convenience of the reader we prove the following remark. It shows (in the case of the product of an abelian variety and a torus) that our definition of independent point is equivalent to the one used in [Rib79], [BGK05] and [Bar06]. By proving this equivalence, we show in particular that the hypothesis considered by Pink in [Pin04, Theorem 4.1] is the same hypothesis of independence considered in [BGK05] and [Bar06]. In particular, some of the results in [BGK05] and [Bar06] are consequences of the results in [Pin04].

Remark 3.3.2. *Let $G = A \times T$ be the product of an abelian variety and a torus defined over a number field K. Then a non-zero K-point R on G is independent if and only if the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by R is free.*

Proof. The 'only if' part is straightforward: if ϕ is a non-zero element of $\mathrm{End}_K G$ such that $\phi(R) = 0$ then $\ker(\phi)$ is an algebraic subgroup of G different from G and containing R hence containing G_R. Now we prove the 'if' part. Suppose that R is not independent. Because of [Rib79, Proposition 1.5] (see Lemma 3.3.3) the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by R is free if and only if the left $\mathrm{End}_{\bar{K}} G$-submodule of $G(\bar{K})$ generated by R is free. Then to conclude we construct a non-zero element of $\mathrm{End}_{\bar{K}} G$ whose kernel contains the point R.

Clearly we may assume that R has infinite order. So G_R^0 is non-zero and since R is not independent we have $G_R^0 \neq G$. By Proposition 2.1.2, G_R^0 is the product of an abelian subvariety A' of A and a subtorus T' of T. Then either A' or T' are non-zero and either $A \neq A'$ or $T \neq T'$. If A' is zero set $\phi_A = \mathrm{id}_A$, if $A' = A$ set $\phi_A = 0$. Otherwise by the Poincaré Reducibility Theorem there exists a non-zero abelian subvariety B of A such that A' and B have finite intersection and such that the map

$$\alpha : A' \times B \to A \quad \alpha(x, y) = x + y$$

is an isogeny. Call d the degree of α and remark that d is the order of $A' \cap B$. Call $\hat{\alpha}$ the isogeny from A to $A' \times B$ such that $\alpha \circ \hat{\alpha} = [d]$. Call π the projection from $A' \times B$ to $\{0\} \times B$. Set $\phi_A = \alpha \circ [d] \circ \pi \circ \hat{\alpha}$. Remark that if $\alpha(x, y)$ is a point on A' then both x and y are points on A'. Then it is immediate to see that ϕ_A is a non-zero element of $\mathrm{End}_{\bar{K}} A$ and that its kernel contains A'.

If T' is zero set $\phi_T = \mathrm{id}_T$, if $T' = T$ set $\phi_T = 0$. Otherwise, because a subtorus is a direct factor there exists a non-zero ϕ_T in $\mathrm{End}_{\bar{K}} T$ such that T' is contained in $\ker(\phi_T)$. Then by construction $(\phi_A \times \phi_T) \circ [n_R]$ is a non-zero element of $\mathrm{End}_{\bar{K}} G$ whose kernel contains G_R. □

For the convenience of the reader we quote the result by Ribet ([Rib79, Proposition 1.5]) which we used to prove the previous remark.

Lemma 3.3.3. *Let G be the product of an abelian variety and a torus defined on a number field K. Let R be a K-point on G. Then the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by R is free if and only if the left $\mathrm{End}_{\bar{K}} G$-submodule of $G(\bar{K})$ generated by R is free.*

Proof. Since $\mathrm{End}_{\bar{K}} G$ equals $\mathrm{End}_L G$ for some finite extension L of K, it suffices to prove the following: we suppose that R is such that the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by R is free and deduce that the left $\mathrm{End}_L G$-submodule of $G(K)$ generated by R is free. We may assume that L is sufficiently large so that T splits and that L/K is a Galois extension. Let d be the degree of the extension L/K.

Suppose that $\phi(R) = 0$ for some ϕ in $\mathrm{End}_L G$ and that R generates a free left $\mathrm{End}_K G$-submodule of $G(K)$. Let α be an element of $\mathrm{End}_L G$. Consider the trace

$$\tau(\alpha \circ \phi) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha \circ \phi).$$

This is an element of $\mathrm{End}_K G$. Since $\alpha \circ \phi(R) = 0$ and both R and 0 are K-points we have:

$$\tau(\alpha \circ \phi)(R) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha \circ \phi)(R) = [d] \circ \alpha \circ \phi(R) = 0.$$

Since the left End_K-module generated by R is free, it follows that $\tau(\alpha \circ \phi) = 0$. Then we conclude by proving that the trace τ is non-degenerate: $\tau(\alpha \circ \phi) = 0$ for every α in $\mathrm{End}_L G$ implies $\phi = 0$.

Let $G = A \times T$ where A is an abelian variety and T is a torus. By Lemma 2.1.1, $\mathrm{End}_L G = \mathrm{End}_L A \times \mathrm{End}_L T$ and it suffices to prove that the trace τ is non-degenerate on A and T respectively.

Let Tr be the trace associated to the ℓ-adic representation of A (notice that this trace does not depend on ℓ). The fact that the trace Tr is non-degenerate on A follows from the positivity of the Rosati involution attached to a polarization of A, see [Mum70, Theorem 1 p.192]. Then τ is non-degenerate since for every α in $\mathrm{End}_L A$ we have $\mathrm{Tr}(\tau(\alpha)) = d\,\mathrm{Tr}(\alpha)$.

Let n be the dimension of T. Since T is split over L and $\mathrm{End}_L \mathbb{G}_m = \mathbb{Z}$, we can write the elements of $\mathrm{End}_L T$ as $n \times n$ matrices with integer entries. Let Tr be the usual trace of matrices. For every α in $\mathrm{End}_L T$ we have $\mathrm{Tr}(\tau(\alpha)) = d\,\mathrm{Tr}(\alpha)$. Then the fact that the trace τ is non-degenerate on T follows from the well-known fact that the trace Tr of matrices with integer entries is non-degenerate. □

In the previous remark we proved that if G is the product of an abelian variety and a torus then R is independent if and only if it is non-zero and the left $\mathrm{End}_K G$-module generated by R is free. Then the K-points of infinite order on the multiplicative group or on a K-simple abelian variety are independent (since the non-zero endomorphisms are isogenies and in particular have finite kernel). The following two examples are also an easy consequence of Remark 3.3.2:

Example 3.3.4. Let A_1 and A_2 be abelian varieties defined on a number field K. Suppose that $\mathrm{Hom}_K(A_1, A_2) = \mathrm{Hom}_K(A_1, A_2) = \{0\}$ (this happens for example when A_1 and A_2 are K-simple and not K-isogenous). Let S_1 and S_2 be points on A_1 and A_2 respectively. Then the point (S_1, S_2) is independent in $A_1 \times A_2$ if and only if S_1 and S_2 are independent on A_1 and A_2 respectively.

Example 3.3.5. Let A be an abelian variety defined on a number field K and K-simple. Let S be a point in $A(K)$, let T be a torsion point of $A(K)$ and let ϕ be in $\mathrm{End}_K A$. The following points are not independent in A^2: $(S, 0)$; $(S, \phi(S))$; $(S, S + T)$.

Let G be a semi-abelian variety defined over a number field K. If R is a point in $G(K)$ which is independent then in particular the smallest algebraic subgroup of G containing R is connected. This means that $n_R = 1$. However it is not true that if $n_R = 1$ then the point R is independent. Indeed, let H be a semi-abelian subvariety of G different from G and suppose that R is a K-point on H. Then by Lemma 3.1.4 the point $n_R R$ is such that $G_{n_R R}$ is connected but $G_{n_R R}$ is contained in H hence the point $n_R R$ is not independent.

Some authors use the notion of independent points:

Definition 3.3.6. *Let G be a semi-abelian variety defined over a number field K. For every $i = 1, \ldots, n$ let R_i be a point in $G(K)$. The points $R_1, \ldots, R_n$ are independent if they generate a non-zero free left $\mathrm{End}_K G$-submodule of $G(K)$.*

To avoid confusing 'a set of points each of which is independent' and 'a set of independent points' we only speak of one independent point at a time. This is possible because of the following observation:

Remark 3.3.7. *Let G be a semi-abelian variety defined over a number field K. For every $i = 1, \dots, n$ let R_i be a point in $G(K)$. The points $R_1, \dots, R_n$ are independent if and only if the point $(R_1, \dots, R_n)$ is independent in G^n.*

3.4 Some properties of the independent points

In this section we prove some properties of the independent points.

Lemma 3.4.1. *Let G be a semi-abelian variety defined over a number field K. Let R be a K-point on G of infinite order. Then the point $n_R R$ is independent in G^0_R. Furthermore, let X be a torsion point in $G(K)$ and suppose that R is independent in G. Then $R + X$ is independent in G.*

Proof. By Lemma 3.1.4 we have $G_{n_R R} = G^0_R$ therefore $n_R R$ is independent in G^0_R. For the second assertion, we have to prove that $G_{R+X} = G$. Call t the order of X. Clearly $G_{R+X} \supseteq G_{t(R+X)} = G_{tR}$. Because $G_R = G$ it suffices to show that $G_{tR} = G_R$. Remark that G_R contains G_{tR} and that G_R is mapped to G_{tR} by $[t]$. Because $[t]$ has finite kernel, G_R and G_{tR} have the same dimension. Because G_R is connected it follows that $G_{tR} = G_R$. □

The following lemma allows us to estimate the order of a point with the order of an independent point.

Lemma 3.4.2. *Let K be a number field and let $I = \{1, \dots, n\}$. Let $G = \prod_{i \in I} B_i$ where for every i B_i is either $\mathbb{G}_m$ or a K-simple abelian variety and for every i, j either $B_i = B_j$ or $\mathrm{Hom}_K(B_i, B_j) = \{0\}$. Let $P = (P_1, \dots, P_n)$ be a point on $G(K)$ of infinite order. Then there exist a subset $J = \{j_1, \dots, j_s\}$ of I and a non-zero integer d such that the point $P' = (P_{j_1}, \dots, P_{j_s})$ is independent in $G' = \prod_{j \in J} B_j$ and such that the order of $(P \bmod \mathfrak{p})$ divides d times the order of $(P' \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.*

Proof. We prove the statement by induction on n. If $n = 1$, the point P_1 is independent in B_1 so take $J = \{1\}$, $d = 1$. Now we prove the inductive step. Let $P = (P_1, \dots, P_n)$ and set $\tilde{P} = (P_1, \dots, P_{n-1})$. If $\tilde{P}$ is a torsion point then P_n is independent in B_n and we easily conclude. So assume that $\tilde{P}$ has infinite order and let $\tilde{J} = \{j_1, \dots, j_{\tilde{s}}\}$ and $\tilde{d}$ be as in the statement. If the point $(P_{j_1}, \dots, P_{j_{\tilde{s}}}, P_n)$ is independent in $\prod_{j \in \tilde{J} \cup \{n\}} B_j$ take $J = \tilde{J} \cup \{n\}$ and $d = \tilde{d}$. Otherwise, by definition of $\tilde{J}$ and since $\mathrm{Hom}_K(B_n, B_j)$ is zero whenever $B_j \neq B_n$ we have

$$\psi(P_n) = \sum_{j \in \tilde{J}} \psi_j(P_j)$$

for some non-zero ψ in $\mathrm{End}_K B_n$ and for some ψ_j in $\mathrm{Hom}_K(B_j, B_n)$. Since ψ is an isogeny there exist $\hat{\psi}$ in $\mathrm{End}_K B_n$ and a non-zero integer r such that $[r] = \hat{\psi} \circ \psi$. Consequently $r(P_n) = \sum_{j \in \tilde{J}} \hat{\psi} \circ \psi_j(P_j)$ and we can take $J = \tilde{J}$, $d = \mathrm{l.c.m.}(\tilde{d}, r)$. □

Let G be a semi-abelian variety defined over a number field K. How many points of $G(K)$ are independent in G? It may occur that $G(K)$ contains no independent points, even if $G(K)$ has non-zero rank, see Example 3.4.3. Since G is connected, by Lemma 3.1.2 we immediately deduce the following: if a point is independent in G then all its multiples are independent in G. Then if $G(K)$ contains a point independent in G, it contains infinitely many of such points.

Example 3.4.3. Let E be an elliptic curve defined over a number field K and such that the rank of $E(K)$ is n. Then the abelian variety E^{n+1} is such that $E^{n+1}(K)$ contains no independent point.

Let G be a semi-abelian variety defined over a number field K. What is the maximum n such that $G^n(K)$ contains a point which is independent in G^n? Let r be the rank of $G(K)$. Then we clearly have $n \leq r$.

Example 3.4.4. If G is an abelian variety, the maximum n such that $G^n(K)$ contains an independent point is finite (being at most the rank of $G(K)$). If G is the multiplicative group, the maximum n such that $G^n(K)$ contains an independent point is infinite: since $\mathrm{End}_K \mathbb{G}_m = \mathbb{Z}$ and $\mathbb{G}_m(K)$ has infinite rank, the group $\mathbb{G}_m^n(K)$ contains an independent point for every $n > 0$.

Because of the following proposition, to study independent points on abelian varieties it suffices to consider the case of product of powers of simple abelian variety. Since the definition of independent point does not depend on the base field, to study independent points on tori it suffices to study independent points on $\mathbb{G}_m^n$.

Proposition 3.4.5. *Let G_1 and G_2 be semi-abelian varieties defined over a number field K. Let α be an isogeny in $\mathrm{Hom}_K(G_1, G_2)$. Let R_1 be a point in $G_1(K)$. Then R_1 is independent in G_1 if and only if $\alpha(R_1)$ is independent in G_2.*

Proof. Call $R_2 = \alpha(R_1)$. We have to show that $G_{R_1} = G_1$ if and only if $G_{R_2} = G_2$. Since G_1 and G_2 are connected, it suffices to show that the dimensions of G_{R_1} and G_1 are equal if and only if the dimensions of G_{R_2} and G_2 are equal. Because α is an isogeny, G_1 and G_2 have the same dimension so it suffices to show that G_{R_1} and G_{R_2} have the same dimension. Then we have $G_{\alpha(R_1)} \subseteq \alpha(G_{R_1})$ so in particular the dimension of G_{R_2} is less than or equal to the dimension of G_{R_1}. By Lemma 1.3.4, there exists an isogeny $\hat{\alpha}$ in $\mathrm{Hom}_K(G_2, G_1)$ such that $\hat{\alpha} \circ \alpha = [d]$ for some non-zero integer d. We clearly have $G_{\hat{\alpha}(R_2)} \subseteq \hat{\alpha}(G_{R_2})$ so the dimension of G_{dR_1} is less than or equal to the dimension of G_{R_2}. Since by Lemma 3.1.2 the dimension of G_{dR_1} equals the dimension of G_{R_1}, we deduce that G_{R_1} and G_{R_2} have the same dimension. □

Chapter 4

On the order of the reductions of points

4.1 Introduction

First consider the additive group and the multiplicative group defined over $\mathbb{Q}$. The restriction of their reduction maps give the well-known reductions for the integers:

Let p be a prime number. For every integer a, the order of $(a \bmod p)$ in $\mathbb{Z}/p\mathbb{Z}$ is 1 if p divides a and it is p otherwise. If a is coprime to p then $(a \bmod p)$ lies in $(\mathbb{Z}/p\mathbb{Z})^*$, which is the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$. The order of $(a \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is a divisor of $p-1$. Suppose that $a \geq 2$. The values of $(a \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})^*$ by varying p are all the positive integers unless $a = 2$ (1 and 6 are excluded) or $a = 2^h - 1$ for $h \geq 2$ (2 is excluded). This was proven by Bang in 1886 ([Ban86]).

Now consider the additive group and the multiplicative group defined over a number field. Their reduction maps give the well-known reductions of number fields:

Let K be a number field and let $\mathcal{O}$ be the ring of integers of K. Let $\mathfrak{p}$ be a prime of K, i.e. a prime ideal of $\mathcal{O}$. The reduction of $\mathcal{O}$ modulo $\mathfrak{p}$ is the quotient map onto the residue field $\mathcal{O}/\mathfrak{p}$.

Let a be an element of K. Then $a = \frac{x}{y}$ for some x, y in $\mathcal{O}$, $y \neq 0$. We can reduce x and y modulo $\mathfrak{p}$ and y is contained only in finitely many primes $\mathfrak{p}$. Then we can define $(a \bmod \mathfrak{p})$ for all but finitely many $\mathfrak{p}$ as the fraction $(x \bmod \mathfrak{p})/(y \bmod \mathfrak{p})$. If $a \neq 0$ then also x is contained only in finitely many primes $\mathfrak{p}$. Hence $(a \bmod \mathfrak{p})$ belongs to the multiplicative group $(\mathcal{O}/\mathfrak{p})^*$ for all but finitely many primes $\mathfrak{p}$.

Let p^n be the cardinality of the finite field $\mathcal{O}/\mathfrak{p}$. The order of $(a \bmod \mathfrak{p})$ in $\mathcal{O}/\mathfrak{p}$ is either 1 or p. The order of $(a \bmod \mathfrak{p})$ in $(\mathcal{O}/\mathfrak{p})^*$ is a divisor of $p^n - 1$. Schinzel in [Sch74] proved that if a is not zero or a root of unity then the order of $(a \bmod \mathfrak{p})$ in $(\mathcal{O}/\mathfrak{p})^*$ takes all but finitely many values of $\mathbb{N}$ by varying $\mathfrak{p}$ in the primes of K.

Let G be a semi-abelian variety defined over a number field K. It is easy to see that if R is non-zero then for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ is non-zero. A first consequence is that if R is a torsion point of order n then for all

but finitely many primes $\mathfrak{p}$ of K the order of $(R \bmod \mathfrak{p})$ is n. A second consequence is that if R has infinite order then the order of $(R \bmod \mathfrak{p})$ cannot take the same value for infinitely many primes $\mathfrak{p}$ of K.

The main result of this chapter is the following:

Theorem 4.1.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-point on G of infinite order. Call n_R the number of connected components of the smallest K-algebraic subgroup of G containing R. Then n_R is the greatest positive integer which divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. Furthermore, let $m > 0$ be a multiple of n_R and let S be a finite set of rational primes. Then there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that for every ℓ in S the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$ equals $v_\ell(m)$.*

We base our work on a method by Khare and Prasad, which combines Kummer theory and the study of the ℓ-adic representation.

For semi-abelian varieties, we prove that for every integer $m > 0$ there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the order of $(R \bmod \mathfrak{p})$ is a multiple of m (see Corollary 4.4.2). Also for all but finitely many primes $\mathfrak{p}$ the order of $(R \bmod \mathfrak{p})$ is a multiple of n_R (see Proposition 4.3.1).

Theorem 4.1.1 and the results in section 4.3 and section 4.4 (Proposition 4.3.2, Proposition 4.3.3 and Corollary 4.4.2) strengthen results which are in the literature: [KP04, Lemma 5]; [Pin04, Theorem 4.1 and Theorem 4.4]; [BGK05, Theorem 3.1] and [Bar06, Theorem 5.1] (in the case of abelian varieties).

4.2 The method by Khare and Prasad

In this section we prove the following result, which will be used in section 4.3 to prove the Theorem 4.1.1. To prove this result we generalize a method by Khare and Prasad (see [KP04, Lemma 5]).

Theorem 4.2.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let F be a finite extension of K. Let R be an F-point on G such that G_R is connected. Fix a non-zero integer m. There exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that the order of $(R \bmod \mathfrak{q})$ is coprime to m.*

Remark that if $F = K$ the theorem simply says that there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the order of $(R \bmod \mathfrak{p})$ is coprime to m.

Let G be a semi-abelian variety defined over a number field K. For n in $\mathbb{N}$ call K_{ℓ^n} the smallest extension of K over which every point of $G[\ell^n]$ is defined. Let R be in $G(K)$. Then for n in $\mathbb{N}$ call $K(\frac{1}{\ell^n}R)$ the smallest extension of K_{ℓ^n} over which the ℓ^n-th roots of R are defined. Clearly the extensions $K_{\ell^{n+1}}/K_{\ell^n}$ and $K(\frac{1}{\ell^n}R)/K_{\ell^n}$ are Galois.

Lemma 4.2.2. *Let G be a semi-abelian variety defined over a number field K. Let ℓ be a rational prime and let n be a positive integer. Suppose that $G(K)$ contains $G[\ell]$. Then*

the degree $[K_{\ell^n} : K]$ *is a power of* ℓ *and for every* R *in* $G(K)$ *the degree* $[K(\frac{1}{\ell^n}R) : K]$ *is a power of* ℓ.

Proof. Since the points of $G[\ell]$ are defined over K, we can embed $\mathrm{Gal}(K_{\ell^n}/K)$ into the group of the endomorphisms of $G[\ell^n]$ fixing $G[\ell]$. The order of this group is a power of ℓ since $G[\ell^n]$ is a finite abelian group whose order is a power of ℓ. Now we only have to prove that the degree $[K(\frac{1}{\ell^n}R) : K_{\ell^n}]$ is a power of ℓ. We can map the Galois group of the extension $K(\frac{1}{\ell^n}R)/K_{\ell^n}$ into $G[\ell^n]$, whose order is a power of ℓ. This is accomplished via the Kummer map

$$\phi_n : \mathrm{Gal}(K(\frac{1}{\ell^n}R)/K_{\ell^n}) \to G[\ell^n]; \quad \phi_n(\sigma)(R) = \sigma(\frac{1}{\ell^n}R) - (\frac{1}{\ell^n}R),$$

where $\frac{1}{\ell^n}R$ is an ℓ^n-th root of R. Since two such ℓ^n-th roots differ by a torsion point of order dividing ℓ^n, it does not matter which root we take. This also implies that ϕ_n is injective. This proves the assertion. □

Lemma 4.2.3. *Let* G *be the product of an abelian variety and a torus defined over a number field* K. *Let* R *be a* K*-point of* G *which is independent. Then for all sufficiently large* n *we have:*

$$K(\frac{1}{\ell^n}R) \cap K_{\ell^{n+1}} = K_{\ell^n}.$$

Proof. Consider the map

$$\alpha_n : \mathrm{Gal}(K(\frac{1}{\ell^{n+1}}R)/K_{\ell^{n+1}}) \to \mathrm{Gal}(K(\frac{1}{\ell^n}R)/K_{\ell^n})$$

given by the restriction to $K(\frac{1}{\ell^n}R)$. To prove this lemma, it suffices to show that α_n is surjective for sufficiently large n.

It is not difficult to check that the following diagram is well-defined and commutative (ϕ_n is the Kummer map defined in the proof of Lemma 4.2.2 and β_n is induced by the diagram):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Gal}(K(\frac{1}{\ell^{n+1}}R)/K_{\ell^{n+1}}) & \xrightarrow{\phi_{n+1}} & G[\ell^{n+1}] & \longrightarrow & \mathrm{coker}\,\phi_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle [\ell]} & & \downarrow{\scriptstyle \beta_n} & & \\
0 & \longrightarrow & \mathrm{Gal}(K(\frac{1}{\ell^n}R)/K_{\ell^n}) & \xrightarrow{\phi_n} & G[\ell^n] & \longrightarrow & \mathrm{coker}\,\phi_n & \longrightarrow & 0
\end{array}$$

If β_n is injective then α_n is surjective. Since β_n is surjective, it suffices to prove that $\mathrm{coker}\,\phi_{n+1}$ and $\mathrm{coker}\,\phi_n$ have the same order for sufficiently large n. Since the order of $\mathrm{coker}\,\phi_n$ increases with n, it is equivalent to show that the order of $\mathrm{coker}\,\phi_n$ is bounded by a constant which does not depend on n. Since we assumed that $G_R = G$, this assertion is a special case of a result by Bertrand ([Ber88, Theorem 1]). □

Lemma 4.2.4. *Let K be a number field. Let $G = A \times T$ be the product of an abelian variety defined over K and a torus split over K. Fix a rational prime ℓ. If $T = 0$ or if $A = 0$ or if ℓ is odd then for every sufficiently large $n > 0$ there exists an element h_ℓ in $\mathrm{Gal}(\bar{K}/K)$ which acts on $G[\ell^\infty]$ via an automorphism whose set of fixed points is $G[\ell^n]$. If A and T are non-zero and $\ell = 2$ then for every sufficiently large $n > 0$ there exists an element h_2 in $\mathrm{Gal}(\bar{K}/K)$ which acts on $G[2^\infty]$ via an automorphism whose set of fixed points is $A[2^n] \times T[2^{n+1}]$.*

Proof. If $T = 0$ then the assertion is a consequence of a result by Bogomolov ([Bog80, Corollaire 1]). If $A = 0$, because T is split over K then it suffices to remark the following fact: for every sufficiently large $n > 0$ the field obtained by adjoining to K the $\ell^{(n+1)}$-th roots of unity is a non-trivial extension of the field obtained by adjoining to K the ℓ^n-th roots of unity. Now assume that A and T are non-zero. Call $\hat{A}$ the dual abelian variety of A. By applying a result of Bogomolov ([Bog80, Corollaire 1]) to $A \times \hat{A}$ we know that if $n > 0$ is sufficiently large, there exists an element h_ℓ in $\mathrm{Gal}(\bar{K}/K)$ which acts on $A \times \hat{A}[\ell^\infty]$ as a homothety with factor h in $\mathbb{Z}_\ell^*$ such that $h \equiv 1 \pmod{\ell^n}$ and $h \not\equiv 1 \pmod{\ell^{n+1}}$. For every n the Weil paring

$$e_{\ell^n} : A[\ell^n] \times \hat{A}[\ell^n] \to \mu_{\ell^n}$$

is bilinear, non-degenerate and Galois invariant. Since e_{ℓ^n} is bilinear and non-degenerate its image contains a root of unity ζ of order ℓ^n. Choose $X_1 \in A[\ell^n]$, $X_2 \in \hat{A}[\ell^n]$ such that $e_{\ell^n}(X_1, X_2) = \zeta$. By Galois invariance and bilinearity we have:

$$\sigma(\zeta) = \sigma\big(e_{\ell^n}(X_1, X_2)\big) = e_{\ell^n}(\sigma(X_1), \sigma(X_2)) = e_{\ell^n}(h \cdot X_1, h \cdot X_2) = \zeta^{h^2}.$$

Because ζ generates μ_{ℓ^n} then σ acts on μ_{ℓ^n} as a homothety with factor $h^2 \pmod{\ell^n}$. Clearly $h^2 \equiv 1 \pmod{\ell^n}$ and $h^2 \not\equiv 1 \pmod{\ell^{n+1}}$ if ℓ is odd. If $\ell = 2$ and $n > 1$ then $h^2 \equiv 1 \pmod{2^{n+1}}$ and $h^2 \not\equiv 1 \pmod{2^{n+2}}$. Because T is split over K we deduce the following: if ℓ is odd the set of fixed points for the automorphism of $G[\ell^\infty]$ induced by h_ℓ is $G[\ell^n]$; if $\ell = 2$ the set of fixed points for the automorphism of $G[2^\infty]$ induced by h_2 is $A[2^n] \times T[2^{n+1}]$. □

Proof of Theorem 4.2.1. By Proposition 2.1.2, G_R is the product of an abelian variety A and a torus T defined over F. Let R' be a point in $G_R(\bar{F})$ such that $2R' = R$. Since R is independent in G_R, the point R' is independent in G_R. Call S the the set of the prime divisors of m. Let K' be a finite extension of F over which R' is defined, over which T is split and over which $G_R[\ell]$ is split for every ℓ in S. Apply Lemma 4.2.3 to the point R', the algebraic group G_R and with base field K'. Then for all sufficiently large n and for every ℓ in S the intersection of $K'(\frac{1}{\ell^n}R')$ and $K'_{\ell^{n+1}}$ is K'_{ℓ^n}. Apply Lemma 4.2.4 to G_R with base field K': we can choose $n > 0$ such that the previous assertion holds and such that for every ℓ in S there exists h_ℓ as in Lemma 4.2.4. Call L the compositum of the fields $K'(\frac{1}{\ell^n}R')$ and the fields $K'_{\ell^{n+1}}$ where ℓ varies in S. By Lemma 4.2.2, the fields $K'(\frac{1}{\ell^n}R') \cdot K'_{\ell^{n+1}}$ where ℓ varies in S are linearly disjoint over K'. Then we can construct

σ in $\mathrm{Gal}(L/K)$ such that for every ℓ in S the restriction of σ to $K'(\frac{1}{\ell^n}R')$ is the identity and such that the restriction to $K'_{\ell^{n+1}}$ of σ and of h_ℓ coincide.

Let $\mathfrak{p}$ be a prime of K which does not ramify in L and such that there exists a prime $\mathfrak{w}$ of L which is over $\mathfrak{p}$ and such that $\mathrm{Frob}_{L/K}\,\mathfrak{w} = \sigma$. By Chebotarev's Density Theorem there exists a positive Dirichlet density of prime ideals $\mathfrak{p}$ of K which satisfy the above conditions. Let $\mathfrak{q}$ be the prime of F lying under $\mathfrak{w}$. Fix a prime ℓ in S and suppose that the order of $(R \bmod \mathfrak{q})$ is a multiple of ℓ. Up to discarding finitely many primes $\mathfrak{p}$ the order of $(R \bmod \mathfrak{w})$ is a multiple of ℓ. Let Z be an element of $G_R(L)$ such that $\ell^n Z = R'$. Then the order of $(Z \bmod \mathfrak{w})$ is a multiple of ℓ^{n+1} (respectively of ℓ^{n+2} if $\ell = 2$). Let $a \geq 1$ be such that the order of $(aZ \bmod \mathfrak{w})$ is exactly ℓ^{n+1} (respectively ℓ^{n+2} if $\ell = 2$). Up to discarding finitely many primes $\mathfrak{p}$ there exists a torsion point X in $G_R(L)$ of order ℓ^{n+1} (respectively ℓ^{n+2} if $\ell = 2$) and such that $(aZ \bmod \mathfrak{w}) = (X \bmod \mathfrak{w})$. See [Kow03, Lemma 4.4].

Up to excluding finitely many primes $\mathfrak{p}$, the action of the Frobenius $\mathrm{Frob}_{L/K}\,\mathfrak{w}$ commutes with the reduction modulo $\mathfrak{w}$ of G hence we deduce the following: the point $(Z \bmod \mathfrak{w})$ is fixed by the Frobenius of $\mathfrak{w}$ while $(X \bmod \mathfrak{w})$ is not fixed. Then the point $(aZ \bmod \mathfrak{w})$ is fixed by the Frobenius of $\mathfrak{w}$ and we get a contradiction. □

4.3 Prescribing valuations of the order of points

In this section we prove Theorem 4.1.1 and other applications of Theorem 4.2.1.

Proposition 4.3.1. *Let G be a semi-abelian variety defined over a number field K. Let R be a K-point on G. Then n_R divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.*

Proof. Because of Lemma 3.1.4 there exists a torsion point X in $G_R(\bar{K})$ and a point P in $G_R^0(\bar{K})$ such that $R = P + X$. Then clearly $n_R X$ is the least multiple of X which belongs to $G_R^0(\bar{K})$. Call t the order of X. Let F be a finite extension of K where P is defined and $G_R[t]$ is split. Fix a prime $\mathfrak{p}$ of K and let $\mathfrak{q}$ be a prime of F over $\mathfrak{p}$. Call m the order of $(R \bmod \mathfrak{p})$. Up to excluding finitely many primes $\mathfrak{p}$ of K, we may assume that the order of $(R \bmod \mathfrak{q})$ is also m. The equality $(mX \bmod \mathfrak{q}) = (-mP \bmod \mathfrak{q})$ implies that $(mX \bmod \mathfrak{q})$ belongs to $(G_R^0(F) \bmod \mathfrak{q})$. Then $(mX \bmod \mathfrak{q})$ belongs to $(G_R^0 \bmod \mathfrak{q})[t]$.

Up to excluding finitely many primes $\mathfrak{p}$ of K, we may assume that the reduction modulo $\mathfrak{q}$ maps injectively $G_R[t]$ to $(G_R \bmod \mathfrak{q})[t]$ and that it maps surjectively $G_R^0[t]$ onto $(G_R^0 \bmod \mathfrak{q})[t]$. See [Kow03, Lemma 4.4]. We deduce that mX belongs to $G_R^0[t]$. Then m is a multiple of n_R. This shows that for all but finitely many primes $\mathfrak{p}$ the order of $(R \bmod \mathfrak{p})$ is a multiple of n_R. □

Proposition 4.3.2. *Let K be a number field. For every $i = 1, \ldots, n$ let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$ of infinite order. Suppose that the point $R = (R_1, \ldots, R_n)$ in $G = G_1 \times \ldots \times G_n$ is such*

that G_R is connected. Fix a non-zero integer m. For every $i = 1, \dots, n$ fix a torsion point X_i in $G_i(\bar{K})$ such that the point $X = (X_1, \dots, X_n)$ is in $G_R(\bar{K})$. Let F be a finite extension of K over which X is defined. Then there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that for every $i = 1, \dots, n$ the order of $(R_i - X_i \bmod \mathfrak{q})$ is coprime to m.

Proof. By Lemma 3.4.1 the point R is independent in G_R and the point $R' = R - X$ is independent in G_R. Since $G_{R'} = G_R$, by Proposition 2.1.2 the algebraic group $G_{R'}$ is the product of an abelian variety and a torus defined over K. Apply Theorem 4.2.1 to R' and find a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that the order of $(R' \bmod \mathfrak{q})$ is coprime to m. This clearly implies the statement. □

Proposition 4.3.3. *Let K be a number field. For every $i = 1, \dots, n$ let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$ of infinite order. Suppose that the point $R = (R_1, \dots, R_n)$ in $G = G_1 \times \dots \times G_n$ is independent. Fix a finite set S of rational primes. For every $i = 1, \dots, n$ fix a non-zero integer m_i. Then there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that for every $i = 1, \dots, n$ and for every ℓ in S the ℓ-adic valuation of the order of $(R_i \bmod \mathfrak{p})$ is $v_\ell(m_i)$.*

Proof. For every $i = 1, \dots, n$ choose a torsion point X_i in $G_i(\bar{K})$ of order m_i and call $X = (X_1, \dots, X_n)$. Let F be a finite extension of K over which X is defined. Call m the product of the primes in S. Apply Proposition 4.3.2 to R and find a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that the order of $(R - X \bmod \mathfrak{q})$ is coprime to m. Fix $\mathfrak{p}$ as above. Up to discarding finitely many primes $\mathfrak{p}$, for every $i = 1, \dots, n$ the order of $(X_i \bmod \mathfrak{q})$ equals m_i. This implies that for every $i = 1, \dots, n$ and for every ℓ in S the ℓ-adic valuation of the order of $(R_i \bmod \mathfrak{q})$ equals $v_\ell(m_i)$. Then up to discarding finitely many primes $\mathfrak{p}$, the ℓ-adic valuation of the order of $(R_i \bmod \mathfrak{p})$ equals $v_\ell(m_i)$ for every $i = 1, \dots, n$ and for every ℓ in S. □

Proof of Theorem 4.1.1. Call n the largest positive integer which divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. By Proposition 4.3.1 we know that n_R divides n. Now we prove that n divides n_R. By Lemma 3.4.1, $G_{n_R R}$ is connected hence by Proposition 2.1.2 it is the product of an abelian variety and a torus defined over K. Let ℓ be a rational prime. Apply Theorem 4.2.1 to $n_R R$ and find infinitely many primes $\mathfrak{p}$ of K such that the ℓ-adic valuation of the order of $(n_R R \bmod \mathfrak{p})$ is 0. Thus there exist infinitely many primes $\mathfrak{p}$ of K such that the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$ is less than or equal to $v_\ell(n_R)$. This shows that n divides n_R. Now we prove the second assertion.

Apply Proposition 4.3.3 to $n_R R$ in $G_{n_R R}$ and find a positive density of primes $\mathfrak{p}$ of K such that for every ℓ in S the ℓ-adic valuation of the order of $(n_R R \bmod \mathfrak{p})$ is $v_\ell(\frac{m}{n_R})$. Because of the first assertion, we may assume that n_R divides the order of $(R \bmod \mathfrak{p})$.

Then for every ℓ in S the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$ is $v_\ell(m)$. □

By adapting this proof straightforwardly we may remark that n_R is also the largest positive integer which divides the order of $(R \bmod \mathfrak{p})$ for a set of primes $\mathfrak{p}$ of K of Dirichlet density 1.

4.4 A divisibility result for semi-abelian varieties

Lemma 4.4.1. *Let K be a number field. For every $i = 1, \dots, n$ let G_i be the product of an abelian variety and a torus defined over K. Let H be an algebraic subgroup of $G_1 \times \dots \times G_n$ such that the projection π_i from H to G_i is non-zero for every $i = 1, \dots, n$. Let ℓ be a rational prime. Then there exists X in $H[\ell^\infty]$ such that $\pi_i(X)$ is non-zero for every $i = 1, \dots, n$.*

Proof. By Proposition 2.1.2, up to replacing H with H^0 we may assume that H is the product of an abelian variety and a torus. For every $i = 1, \dots, n$ since the projection π_i is non-zero, it is easy to see that there exists Y_i in $H[\ell^\infty]$ such that $\pi_i(Y_i)$ is non-zero. The assertion is immediate for abelian varieties and tori and to combine the two cases it suffices to remark that there are no non-zero homomorphisms between abelian varieties and tori. The point Y_1 is not in the kernel of π_1. So if $n = 1$ we conclude. Otherwise let $1 < r \leq n$ and suppose that $\sum_{j=1}^{r-1} Y_j$ is not in the kernel of π_i for every $i = 1, \dots, r-1$. Up to replacing Y_r with an element in $\frac{1}{\ell^\infty} Y_r$, we may assume that for every $i = 1, \dots, r$ either $\pi_i(Y_r)$ is zero or the order of $\pi_i(Y_r)$ is greater than the order of $\pi_i(\sum_{j=1}^{r-1} Y_j)$. Then $\sum_{j=1}^{r} Y_j$ is not in the kernel of π_i for every $i = 1, \dots, r$. We conclude by iterating the procedure up to $r = n$.

Corollary 4.4.2. *Let K be a number field. For every $i = 1, \dots, n$ let G_i be a semi-abelian variety defined over K and let R_i be a point on $G_i(K)$ of infinite order. Then for every integer $m > 0$ there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that for every $i = 1, \dots, n$ the order of $(R_i \bmod \mathfrak{p})$ is a multiple of m.*

Proof. First we prove the case where G_i is the product of an abelian variety A_i and a torus T_i for every $i = 1, \dots, n$. Call S the set of prime divisors of m. Consider the point $R = (R_1, \dots, R_n)$ in $G = G_1 \times \dots \times G_n$. We may assume that $n_R = 1$ by replacing R_i with $n_R R_i$ and we may assume that m is square-free by replacing R_i with $(m/\prod_{\ell \in S} \ell) R_i$ for every $i = 1, \dots, n$. Since G_R contains R, the projection from G_R to G_i is non-zero for every $i = 1, \dots, n$ so we can apply Lemma 4.4.1. Then for every ℓ in S there exists X_ℓ in $G_R[\ell^\infty]$ such that all the coordinates of X_ℓ are non-zero. Write $Y = \sum_{\ell \in S} X_\ell$. By construction Y belongs to $G_R(\bar{K})_{tors}$ and for every $\ell \in S$ the order of every coordinate of Y is a multiple of ℓ. Let F be a finite extension of K where Y is defined. By Proposition 4.3.2, there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that the order of $(R - Y \bmod \mathfrak{q})$ is coprime to m. Then up to discarding finitely many primes $\mathfrak{p}$ the order of $(R_i \bmod \mathfrak{p})$ is a multiple of ℓ for every ℓ in S and for every $i = 1, \dots, n$. This concludes the proof for this case.

For every $i = 1, \ldots, n$ let G_i be an extension of an abelian variety A_i by a torus T_i and call π_i the quotient map from G_i to A_i. If $\pi_i(R_i)$ does not have infinite order let R_i' be a non-zero multiple of R_i which belongs to $T_i(K)$. If $\pi_i(R)$ has infinite order then let $R_i' = 0$. Then $(\pi_i R_i, R_i')$ is a K-point of $A_i \times T_i$ of infinite order. Clearly for all but finitely many primes $\mathfrak{p}$ of K the following holds: the order of $(R_i \bmod \mathfrak{p})$ is a multiple of m whenever the order of $((\pi_i R_i, R_i') \bmod \mathfrak{p})$ is a multiple of m. Then we reduced to the previous case. □

4.5 Remarks

Let G be an algebraic group defined over a number field K. Let R be a K-point on G. Let n be the greatest integer which divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. We proved in Theorem 4.1.1 that n is the number of connected components of the algebraic subgroup of G generated by R. We now give another characterization of n.

Proposition 4.5.1. *Let G be the product of an abelian variety and a torus defined over a number field K. The greatest integer which divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K is the greatest integer n such that there exists a product of an abelian variety and a torus H defined over $\bar{K}$ and a torsion point X in $H[n]$ such that X belongs to $\mathrm{Hom}_{\bar{K}}(G, H) \cdot R$.*

Proof. Let H be a product of an abelian variety and a torus H defined over $\bar{K}$. From Corollary 1.3.2 and Lemma 1.2.3 we deduce the following: if a point X on H of order n is such that X belongs to $\mathrm{Hom}_{\bar{K}}(G, H) \cdot R$ then n divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.

In view of Theorem 4.1.1, it suffices to prove that there exist H and X as in the statement where X has order n_R.

Let G be the product of an abelian variety A and a torus T. Let H be the quotient of G by G_R^0. By Theorem 2.1.2, G_R^0 is the product $A' \times T'$ of an abelian subvariety of A and a subtorus of T. As we showed in the proof of Theorem 2.1.2, the quotient A/A' is an abelian variety defined over $\bar{K}$ and the quotient T/T' is a torus defined over $\bar{K}$. Hence H equals $A/A' \times T/T'$ and in particular it is the product of an abelian variety and a torus defined over $\bar{K}$.

Call W the connected component of G_R containing the point R. By Lemma 3.1.5, there exists a torsion point Y in $G(\bar{K})$ such that $W = Y + G_R^0$ and $n_R Y$ is the least positive multiple of Y contained in G_R^0. Let X be the image of Y in H. Since $n_R Y$ belongs to G_R^0, we have $n_R X = n_R[Y] = [n_R Y] = 0$. Then the order of X is some divisor d of n_R. Suppose that $d \neq n_R$. Then $dX = [dY] = 0$ hence dY belongs to G_R^0. We have a contradiction. □

In [Kow03] Kowalski gives the definition of *fairly well spread* point:

Definition 4.5.2. *Let G be a semi-abelian variety defined over a number field K. Let R be a K-point on G. Then R is fairly well-spread if the following conditions are satisfied: R has infinite order; for all prime number ℓ and for all $n \geq 1$ there exists a prime $\mathfrak{p}$ of K such that ℓ^n divides the order of $(R \bmod \mathfrak{p})$; the greatest common divisor of the order of $(R \bmod \mathfrak{p})$ where $\mathfrak{p}$ ranges over any family containing almost all primes of K is 1.*

Proposition 4.4.2 implies that if R is a point of infinite order then R satisfies the first two conditions of the above definition. Proposition 4.3.1 implies that if the third condition is satisfied then the algebraic subgroup of G generated by R is connected.

If G is the product of an abelian variety and a torus, Theorem 4.1.1 implies that the fairly well spread points are the points of infinite order which generate a connected algebraic subgroup of G. In particular, independent points are fairly well-spread.

Let G be the product of an abelian variety and a torus defined over a number field K. In Proposition 4.3.2 and in Proposition 4.3.3 it is important to know which torsion points of $G(\bar{K})$ are contained in G_R. It is easy to see that the point R is independent in G if and only if every torsion point of $G(\bar{K})$ is contained in G_R.

We now give an application of Proposition 4.3.3.

Corollary 4.5.3. *Let E be an elliptic curve defined over a number field K and without complex multiplication. Let P and Q be points in $E(K)$ which generate a subgroup H of $E(K)$ of rank 2. Let n be a positive integer. Then there exist infinitely many primes $\mathfrak{p}$ of K such that $(H \bmod \mathfrak{p})$ contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Proof. We may assume that $E[n]$ is contained in $E(K)$. Let T_1 and T_2 be points in $E[n]$ without a non-zero common multiple. By Proposition 4.3.3 there exist infinitely many primes $\mathfrak{p}$ of K such that the order of $(P - T_1 \bmod \mathfrak{p})$ and the order of $(Q - T_2 \bmod \mathfrak{p})$ are coprime to n. Up to excluding finitely many primes $\mathfrak{p}$, we may assume that $(E[n] \bmod \mathfrak{p}) = (E \bmod \mathfrak{p})[n]$ and that this group is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Let $\mathfrak{p}$ be a prime of K as above. The group $(H \bmod \mathfrak{p})$ contains $(T_1 \bmod \mathfrak{p})$ and $(T_2 \bmod \mathfrak{p})$ hence it contains $(E[n] \bmod \mathfrak{p})$. This proves the statement. □

Part II

Local-global principles

Chapter 5

The support problem

5.1 A question by Erdős

Pál Erdős in 1988 asked the following question:

Question. Let a and b be positive integers with the property that for every $n > 0$ the set of prime numbers dividing $a^n - 1$ is equal to the set of prime numbers dividing $b^n - 1$. Is then $a = b$?

The *support* of an integer m is the set of primes dividing m. So Erdős's condition can be rephrased as follows: the support of $a^n - 1$ and of $b^n - 1$ coincide for every $n > 0$. For this reason, the above question was called 'the support problem'.

In 1997 Corrales-Rodrigáñez and Schoof answered affirmatively to Erdős's question. They proved a stronger statement:

Proposition 5.1.1. *Let a and b be positive integers with the property that for every $n > 0$ the support of $a^n - 1$ is contained in the support of $b^n - 1$. Then a is a power of b.*

Erdős's condition can be also rephrased as follows: for every prime number p and for every $n > 0$

$$a^n \equiv 1 (\mathrm{mod} p) \quad \textit{if and only if} \quad b^n \equiv 1 (\mathrm{mod} p).$$

Corrales-Rodrigáñez and Schoof generalized the above condition to number fields. For the reductions of number fields, see section 4.1. The support problem for number fields is solved by the following result:

Theorem 5.1.2 (Theorem 1, [CRS97])**.** *Let K be a number field and let a, $b \in K^*$. If for almost all primes $\mathfrak{p}$ of K and for all $n > 0$ one has*

$$a^n \equiv 1 (\mathrm{mod} \mathfrak{p}) \quad \textit{whenever} \quad b^n \equiv 1 (\mathrm{mod} \mathfrak{p})$$

then a is a power of b.

Another rephrasing of Erdős condition is the following: for almost all prime numbers p the order of $(b \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})^*$ divides the order of $(a \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})^*$. It is with this last formulation that the support problem has been generalized to algebraic groups, see section 5.3.

In 1975, Andrej Schinzel answered to Erdős's question!

Theorem 5.1.3 ([Sch75, Theorem 2])**.** *Let K be a number field. Let a be a non-zero element of K and let B be a subgroup of K^*. Suppose that for almost all prime ideals $\mathfrak{p}$ of K $(a \bmod \mathfrak{p})$ belongs to $(B \bmod \mathfrak{p})$. Then a belongs to B.*

We now show why Schinzel's result answers to Erdős's question for the integers. Consider the group generated by b. Since the multiplicative group of a finite field is *cyclic*, the following conditions are equivalent for a prime $\mathfrak{p}$ of K: the order of $(a \bmod \mathfrak{p})$ divides the order of $(b \bmod \mathfrak{p})$; the point $(a \bmod \mathfrak{p})$ lies in the subgroup generated by $(b \bmod \mathfrak{p})$. Furthermore, to prove that a lies in the subgroup of K^* generated by b is to prove that a is a power of b.

5.2 The support problem for the integers and the abc-conjecture

A refinement of the support problem for the integers is the following:

Conjecture 5.2.1. *Let a and b be positive integers with the property that for infinitely many positive integers n the set of prime numbers dividing $a^n - 1$ is contained in the set of prime numbers dividing $b^n - 1$. Then b is a power of a.*

The *radical* of an integer number is the product of the primes in its support.

Conjecture (abc-conjecture)**.** Let ϵ be a real number such that $\epsilon > 0$. There exists a real number $C_\epsilon > 0$ such that for every abc-triple (i.e. positive integers (a, b, c) such that $a + b = c$ and $(a, b) = 1$)

$$c \leq C_\epsilon(\mathrm{rad}(abc))^{1+\epsilon}.$$

We prove Conjecture 5.2.1 by assuming the abc-conjecture: we refine an unpublished proof by Corrales-Rodrigáñez and Schoof (in which they answer to Erdős's question by assuming the abc-conjecture). We apply the following result by Bugeaud, Corvaja and Zannier:

Theorem 5.2.2. *[Theorem, [BCZ03]] Let a,b be multiplicatively independent integers ≥ 2 and let $\epsilon > 0$. Then provided n is sufficiently large we have*

$$\gcd(a^n - 1, b^n - 1) < \exp(\epsilon n).$$

Corollary 5.2.3. *[Remark(1), [BCZ03]] Let a,b be integers ≥ 2. If b is not a power of a then for sufficiently large n we have* $\gcd(a^n - 1, b^n - 1) < a^{(n/2)}$.

Proof of Conjecture 5.2.1 by assuming the abc-conjecture. Let S be the infinite set of natural numbers such that the condition in the statement holds. Let n be in S. If $a = 1$ then the support of $a^n - 1$ is the set of all primes. This clearly forces $b = 1$ so the assertion holds. If $b = 1$ then b is trivially a power of a. Now assume that $a, b > 2$.

Fix $\epsilon < 1$ and consider the following *abc*-triples: $(a^n - 1, 1, a^n)$ where n varies in S. By assuming the *abc*-conjecture, we find:

$$a^n \leq C_\epsilon(\mathrm{rad}((a^n-1)a^n))^{1+\epsilon} = C_\epsilon(\mathrm{rad}((a^n-1)a))^{1+\epsilon}.$$

Since (a^n-1) and a are coprime, $\mathrm{rad}((a^n-1)a)$ is the product of $\mathrm{rad}(a^n-1)$ and $\mathrm{rad}(a)$. Then

$$(\mathrm{rad}(a^n-1))^{1+\epsilon} \geq C'_\epsilon a^n \tag{5.1}$$

where $C'_\epsilon = C_\epsilon^{-1}\,\mathrm{rad}(a)^{-(1+\epsilon)}$.

Suppose that b is not a power of a and let n be in S. From Corollary 5.2.3 we know that $\gcd(a^n - 1, b^n - 1) < a^{(n/2)}$ for every sufficiently large n. Because n is in S, $\mathrm{rad}(a^n - 1)$ divides $\mathrm{rad}(b^n - 1)$ hence

$$\mathrm{rad}(a^n - 1) \mid \gcd(a^n - 1, b^n - 1).$$

Then

$$(\mathrm{rad}(a^n-1))^{1+\epsilon} \leq (\gcd(a^n - 1, b^n - 1))^{1+\epsilon} \leq a^{(n/2)(1+\epsilon)}. \tag{5.2}$$

Let $\nu = (n/2)(1+\epsilon)$. By combining (5.1) and (5.2) we have that for every n in S sufficiently large

$$a^\nu \geq C'_\epsilon a^n.$$

This formula only holds for finitely many n since $a > 1$, $\nu < n$ and C'_ϵ is a positive constant not depending on n. We find a contradiction. □

5.3 State of the art of the support problem

The support problem

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-point on G and let ϕ be a K-endomorphism of G. Then the order of $(\phi(R) \bmod \mathfrak{p})$ divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. The *support problem* is concerned with the converse:

Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-points on G. Suppose that the following condition is satisfied:

(SP) *The order of $(Q \bmod \mathfrak{p})$ divides the order of $(P \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.*

How are P and Q related?

Results on the support problem

The support problem was first studied for the multiplicative group and for elliptic curves by Corrales-Rodrigáñez and Schoof ([CRS97]). In the both cases they proved that Q is the image of P via a K-endomorphism. For the multiplicative group this means that Q is a power of P.

For abelian varieties, partial results were obtained by Khare and Prasad in [KP02] and by Banaszak, Gajda and Krasoń in [BGK03].

Larsen in [Lar03] solved the support problem for abelian varieties. He showed that there exist a K-endomorphism ϕ and a non-zero integer c such that $\phi(P) = cQ$ ([Lar03, Theorem 1]). His result is optimal since in general one can not take $c = 1$, even if both P and Q have infinite order ([Lar03, Proposition 2]).

We extend Larsen's result to products of abelian varieties and tori, see Theorems 6.1.1 and 7.1.1.

The integer c of the support problem

Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-points on G satisfying condition (SP). Call c the minimal positive integer c such that cQ belongs to $\mathrm{End}_K G \cdot P$. Recall that c in general is not 1, even if both P and Q have infinite order ([Lar03, Proposition 2]).

Khare and Prasad proved that for a simple abelian variety $c = 1$ if the point P has infinite order, see [KP04, Theorem 1]. We generalize their result to the product of an abelian variety and a torus, under the assumption that P is independent. This is a consequence of Proposition 6.3.1.

Larsen in [LS04] proved that for abelian varieties c divides a constant which depends only on G and K. We generalize this last result to the product of an abelian variety and a torus by using a different method, see Theorem 6.1.2.

Larsen in [LS04] proved something more precise: in every K-isogeny class of abelian varieties there is an abelian variety such that c divides the exponent of the Mordell-Weil group, see [LS04, Corollary 4.4 and Theorem 5.2].

The refined support problem

Larsen and Schoof investigated whether it is true for abelian varieties that assuming condition (SP) there exist a K-endomorphism ϕ and a K-point T of finite order such that $\phi(P) = Q + T$. They called this question *refined support problem*.

They asked a meaningful question because what they looked for is weaker than requiring $\phi(P) = Q$ (which is in general false) and it is stronger than requiring $\phi(P) = cQ$ for some non-zero integer c (which is known to be true).

Larsen and Schoof in [LS06] constructed an example of an abelian variety for which the question of the refined support problem has a negative answer. Nevertheless, there are abelian varieties for which the answer is positive. Indeed, there is one such variety in every K-isogeny class ([LS04, Corollary 4.4 and Theorem 5.2]). More precisely, the

answer is positive for every abelian variety such that $T_\ell G$ is integrally semisimple ([LS04, Definition 4.1]) for every rational prime ℓ and in every K-isogeny class of abelian varieties there is an abelian variety with this property, see [LS04, Theorem 5.2 and Corollary 4.4].

Unpublished references

In her master thesis with advisor Bart de Smit, Ana Lukić analyzed which are the hypotheses really used in the proof by Corrales-Rodrigáñez and Schoof of [CRS97, Theorem 1]. She made some original remarks. See [Luk03].

In her master thesis with advisors David McKinnon and Eva Bayer Fluckiger, Anna Devic analyzed the paper by Corrales-Rodrigáñez and Schoof [CRS97]. She gave more details for the proof of [CRS97, Theorem 2] in the case of complex multiplication and explicitly wrote Larsen's proof of [Lar03, Theorem 1] in the case of elliptic curves. See [Dev07].

In a manuscript, Olivier Wittenberg presented the history of the support problem. He also gave an alternative proof of Larsen's theorem ([Lar03, Theorem 1]) inspired by a work of Larsen and Schoof ([LS04]). See [Wit03].

Chapter 6

The ℓ-adic support problem

6.1 Introduction

In this chapter we study a variant of the support problem which we call the *ℓ-adic support problem*. Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-points on G. We require the following condition on the points P and Q:

(LSP) *Let ℓ be a prime number. Suppose that the ℓ-adic valuation of the order of $(Q \bmod \mathfrak{p})$ is less than or equal to the ℓ-adic valuation of the order of $(P \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.*

We strengthen Larsen's result on the support problem by proving the following:

Theorem 6.1.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-points of G satisfying condition (LSP). Then there exist a K-endomorphism ϕ of G and a non-zero integer c such that $\phi(P) = cQ$.*

For the multiplicative group, the above result was proven by Khare in [Kha03, Proposition 3] by applying a method by Corrales-Rodrigañez and Schoof [CRS97]. For simple abelian varieties, an equivalent result was proven by Baranczuk in [Bar06, Theorem 8.2]. For abelian varieties, our result has an alternative proof by Wittenberg, see [Wit03, proof of Theorem 1.3].

Theorem 6.1.2. *Under the assumptions of Theorem 6.1.1, one can take c such that $v_\ell(c) \leq v_\ell(m)$ where m is a non-zero integer depending only on G and K (in particular not depending on ℓ).*

In Theorem 6.1.1, one cannot take c coprime to ℓ even if P and Q have infinite order (the counterexample in [Lar03, Proposition 2] works for $\ell = 2$ but it can be generalized straight-forwardly to any ℓ). One can take c coprime to ℓ if the smallest algebraic subgroup of G containing P is G itself, see Proposition 6.3.1. This happens in particular if G is a simple abelian variety and P is a point of infinite order.

If G is a one-dimensional torus or a split torus, one can take c coprime to ℓ. For a general torus, one can take c such that $v_\ell(c) \leq v_\ell([L : K])$ where L is a finite Galois extension of K where the torus splits, see Remark 6.3.2. I do not know whether one can take c coprime to ℓ also for non-split tori.

6.2 The proof of Theorem 6.1.1

Lemma 6.2.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let L be a finite Galois extension of K of degree d. Let P and Q be K-points of G. If Q belongs to $\mathrm{End}_L G \cdot P$ then dQ belongs to $\mathrm{End}_K G \cdot P$.*

Proof. Let ψ be in $\mathrm{End}_L G$ and such that $\psi(P) = Q$. Set $\phi = \sum_{\sigma \in \mathrm{Gal}(L/K)} \psi^\sigma$. Then ϕ is in $\mathrm{End}_K G$ and we have:

$$\phi(P) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \psi^\sigma(P) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \psi(P)^\sigma = \sum_{\sigma \in \mathrm{Gal}(L/K)} Q^\sigma = dQ.$$

□

Lemma 6.2.2. *Let A and B be products of an abelian variety and a torus defined over a number field K and K-isogenous. If Theorem 6.1.1 is true for B, then it is true for A.*

Proof. Suppose that Theorem 6.1.1 holds for B. Let α be a K-isogeny from A to B, call d the degree of α and call $\hat{\alpha}$ the isogeny in $\mathrm{Hom}_K(B, A)$ satisfying $\hat{\alpha} \circ \alpha = [d]$. Take P, Q in $A(K)$ satisfying the condition of Theorem 6.1.1. Because of Lemma 1.3.5 and the hypotheses on P and Q, for all but finitely many primes $\mathfrak{p}$ of K we have

$$v_\ell[\mathrm{ord}(\alpha(P) \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(dP \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(dQ \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(\alpha(dQ) \bmod \mathfrak{p})]$$

therefore $\alpha(P)$ and $\alpha(dQ)$ satisfy the condition of Theorem 6.1.1. Thus

$$\psi\big(\alpha(P)\big) = r\big(\alpha(dQ)\big)$$

where ψ is in $\mathrm{End}_K B$ and r is a non-zero integer. Set $\phi = \hat{\alpha} \circ \psi \circ \alpha$, $c = rd^2$. Then ϕ is in $\mathrm{End}_K A$, c is a non-zero integer and we have:

$$\phi\big(P\big) = \hat{\alpha} \circ \psi \circ \alpha\big(P\big) = \hat{\alpha} \circ [r] \circ \alpha\big(dQ\big) = rd^2Q = cQ.$$

□

Proof of Theorem 6.1.1. First step. We reduce to the case $G = \prod_{i \in I} B_i$ where for every $i \in I$ the factor B_i is either $\mathbb{G}_m$ or a K-simple abelian variety and for any two indices i, j either $B_i = B_j$ or $\mathrm{Hom}_K(B_i, B_j) = \{0\}$. By the Poincaré Reducibility Theorem, any abelian variety is K-isogenous to a product of K-simple abelian varieties which are in

pairs either equal or non-isogenous. Also there are no non-zero homomorphisms between abelian varieties and tori. Then it suffices to combine two things: the statement holds for G if it holds for $\alpha(G)$ where α is a K-isogeny (see Lemma 6.2.2); the statement holds for G if it holds for $G \times_K L$, where L is a finite Galois extension of K (see Lemma 6.2.1).

Second step. Now let $I = \{1, \dots, n\}$ and write $P = (P_1, \dots, P_n)$, $Q = (Q_1, \dots, Q_n)$. Call π_i the projection from G to B_i. It suffices to show that for every $i \in I$ there exist ψ_i in $\mathrm{Hom}_K(G, B_i)$ and a non-zero integer c such that $\psi_i(P) = c \cdot \pi_i(Q)$. Without loss of generality we prove this for $i = 1$. Then we may clearly replace Q by $(Q_1, 0, \dots, 0)$.

Now we reduce to the case where both P and Q have infinite order. We may assume that Q has infinite order (otherwise take $\phi = 0$ and $c = \mathrm{ord}\, Q$). We may assume that for every $i \in I$ the point P_i is either zero or has infinite order (replace P and Q by dP and dQ for a suitable non-zero integer d). Then it suffices to remark that P is non-zero: since Q has infinite order, by Corollary 4.4.2 there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] > 0$ so if $P = 0$ we have a contradiction with the hypotheses of Theorem 6.1.1.

Third step. Apply Lemma 3.4.2 to P and let J, d, P', G' be as in Lemma 3.4.2. Since P' is a projection of P, it suffices to prove that there exist ψ in $\mathrm{Hom}_K(G', B_1)$ and a non-zero integer c such that $\psi(P') = cQ_1$.

The point (P', Q_1) is not independent in $G' \times B_1$. Otherwise, by Proposition 4.3.3 there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(Q_1 \bmod \mathfrak{p})] = v_\ell(d) + 1$ and $v_\ell[\mathrm{ord}(P' \bmod \mathfrak{p})] = 0$. We find a contradiction since by definition of d we may assume that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] \leq v_\ell(d) + v_\ell[\mathrm{ord}(P' \bmod \mathfrak{p})]$.

Since (P', Q_1) is not independent in $G' \times B_1$, we have $F(P', Q_1) = 0$ for some non-zero F in $\mathrm{End}_K(G' \times B_1)$. Recall that G' is the product of some B_i's such that either $B_i = B_1$ or $\mathrm{Hom}_K(B_1, B_i) = \{0\}$. Then since P' is independent in G' we deduce that $f(P') = g(Q_1)$ for some f in $\mathrm{Hom}_K(G', B_1)$ and some non-zero g in $\mathrm{End}_K B_1$. Since g is an isogeny, g factors a non-zero integer in $\mathrm{End}_K B_1$ and we easily conclude. □

The following corollary is the analogue to [Lar03, Corollary 6].

Corollary 6.2.3. *Let G_1 and G_2 be products of an abelian variety and a torus defined over a number field K. Let P and Q be K-points on G_1 and G_2 respectively. Fix a rational prime ℓ. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the ℓ-adic valuation of the order of $(P \bmod \mathfrak{p})$ is greater than or equal to the ℓ-adic valuation of the order of $(Q \bmod \mathfrak{p})$. Then there exist ϕ in $\mathrm{Hom}_K(G_1, G_2)$ and a non-zero integer c such that $\phi(P) = cQ$.*

Proof. Apply Theorem 6.1.1 to $G_1 \times G_2$ and its K-points $(P, 0)$ and $(0, Q)$. □

6.3 On the integer c of the ℓ-adic support problem

The following proposition is the generalization of a result by Khare and Prasad ([KP04, Theorem 1]).

Proposition 6.3.1. *Under the assumptions of Corollary 6.2.3, one can take c coprime to ℓ if P is independent in G_1.*

Proof. We have $\phi P = cQ$ for some ϕ in $\mathrm{Hom}_K(G_1, G_2)$ and some non-zero integer c. By iteration, it suffices to prove that if c is divisible by ℓ there exists ψ in $\mathrm{Hom}_K(G_1, G_2)$ such that $\psi P = \frac{c}{\ell}Q$. Suppose that c is divisible by ℓ.

First we prove that $\phi = [\ell] \circ \psi$ for some ψ in $\mathrm{Hom}_K(G_1, G_2)$. Suppose that this is false, thus let T be a point in $G_1[\ell] \setminus \ker(\phi)$. Write L for a finite extension of K over which $G_1[\ell]$ is split. Since P is independent in G_1, by Proposition 4.3.2 there exist infinitely many primes $\mathfrak{q}$ of L such that $v_\ell[\mathrm{ord}(P - T \bmod \mathfrak{q})] = 0$. Fix such a prime $\mathfrak{q}$. We may assume that the order of $(T \bmod \mathfrak{q})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 1$. Since T is not in the kernel of ϕ, the order of $(\phi(T) \bmod \mathfrak{q})$ is ℓ. Since $cQ - \phi(T) = \phi(P - T)$, we have $v_\ell[\mathrm{ord}(cQ - \phi(T) \bmod \mathfrak{q})] = 0$. Then $v_\ell[\mathrm{ord}(cQ \bmod \mathfrak{q})] = 1$. Because ℓ divides c, it follows that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})]$ is at least 2. Then there are infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})]$ is 1 while $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})]$ is at least 2 so we have a contradiction.

Write ϕ as $[\ell] \circ \psi$ for some ψ in $\mathrm{Hom}_K(G_1, G_2)$. Then we have $\psi(P) = \frac{c}{\ell}Q + T'$ for some T' in $G_1[\ell]$. It suffices to prove that $T' = 0$. Suppose not. By Theorem 4.2.1, there exist infinitely many primes $\mathfrak{q}$ of L such that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 0$. We may assume that $v_\ell[\mathrm{ord}(T' \bmod \mathfrak{q})] = 1$ so we deduce that $v_\ell[\mathrm{ord}(\frac{c}{\ell}Q \bmod \mathfrak{q})] = 1$. Consequently, for infinitely many primes $\mathfrak{q}$ of L we have $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 0$ while $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})]$ is at least 1. We have a contradiction. □

Proof of Theorem 6.1.2. We first reduce to the case $G = A \times \mathbb{G}_m^n$ where A is an abelian variety. To accomplish this, it suffices to combine two things: the statement holds for G if it holds for $\alpha(G)$ where α is a K-isomorphism; the statement holds for G if it holds for $G \times_K L$ where L is a finite Galois extension of K. The first of the two assertions is trivial. The second assertion can be deduced from the proof of Lemma 6.2.1: if m' is such that $v_\ell(c) \leq v_\ell(m')$ for $G \times_K L$ then one can take $m = [L : K]m'$.

We reduce at once to the case where G_P is connected: replace P and Q by dP and dQ (where n_P divides d and d depends only on G and K, see Proposition 3.2.2). Now assume that G_P is connected. By Proposition 2.1.2 we have $G_P = A' \times T'$ where A' is an abelian subvariety of A and T' is a sub-torus (hence a direct factor) of $\mathbb{G}_m^n$. If P is zero then Q is a torsion point coprime to ℓ by Corollary 4.4.2 and the statement clearly holds. So assume that P has infinite order and hence that P is independent in G_P. By Proposition 6.3.1 there exist ψ in $\mathrm{Hom}_K(G_P, G)$ and an integer c_ℓ coprime to ℓ such that $\psi(P) = c_\ell Q$.

Write $P = (P_A, P_T)$ and remark that $A' = G_{P_A}$ (see the proof of Proposition 3.2.2). Apply Lemma 3.2.1 to P_A. Let Z and t be as in Lemma 3.2.1. The map

$$j : A' \times Z \to A\,;\ (x, y) \mapsto x + y.$$

is a K-isogeny in $\mathrm{Hom}_K(A' \times Z, A)$ of degree dividing t. Call $\hat{j}$ the isogeny in $\mathrm{Hom}_K(A, A' \times Z)$ satisfying $\hat{j} \circ j = [t]$. We have:

$$\hat{j}\big(P_A\big) = \hat{j} \circ j\big((P_A, 0)\big) = (tP_A, 0).$$

Since T' is a direct factor of $\mathbb{G}_m^n$, we can then construct Π in $\mathrm{Hom}_K(G, G_P)$ such that $\Pi(P) = tP$. The map $\phi = \psi \circ \Pi$ is in $\mathrm{End}_K A$ and we have $\phi(P) = tc_\ell Q$. Since t depends only on G and K and c_ℓ is coprime to ℓ, this concludes the proof. □

In Theorem 6.1.1, one can take c such that $v_\ell(c) \leq v_\ell(m)$ where m depends only on G and K, see Theorem 6.1.2. Unless $G(K)$ is finite, one clearly cannot bound $v_p(c)$ for any rational prime p different from ℓ.

Remark 6.3.2. *In Theorem 6.1.1, let G be a torus. If G is split or 1-dimensional then one can take c coprime to ℓ. In general one can take c such that $v_\ell(c) \leq v_\ell([L : K])$ where L is any finite Galois extension of K where G splits.*

Proof. We may assume that $G = \mathbb{G}_m^n$: see the proof of Lemma 6.2.1 and notice that if G is 1-dimensional every $\bar{K}$-endomorphism is already defined over K.

Thus assume that $G = \mathbb{G}_m^n$ and recall that $\mathbb{G}_m[a] \simeq \mathbb{Z}/a\mathbb{Z}$ for every $a \geq 1$. Without loss of generality we may assume that $Q = (Q_1, 0, \ldots, 0)$. If P is a torsion point then (since $\phi(P) = cQ$) Q_1 is also a torsion point and the statement easily follows from condition (LSP). Now assume that P has infinite order. Since $\mathrm{End}_K \mathbb{G}_m \simeq \mathbb{Z}$, we may assume that P is of the following form:

$$P = (R_1, \ldots, R_h, T, 0, \ldots, 0)$$

where the point $(R_1, \ldots, R_h)$ is independent in $\mathbb{G}_m^h$, $h \geq 1$ and T is a torsion point. Call t the ℓ-adic valuation of the order of T. We have

$$aT + \sum_{i=1}^{h} a_i R_i = cQ_1 \tag{6.1}$$

for some $a, a_1, \ldots, a_h$ in $\mathbb{Z}$ and for some non-zero integer c. Suppose that c is divisible by ℓ. It suffices to find an expression analogous to (6.1) where c is replaced by $\frac{c}{\ell}$ and we conclude by iteration.

Now we prove that a is divisible by ℓ. Suppose not. We may clearly assume that $t \neq 0$, otherwise we can multiply every coefficient of (6.1) by an integer coprime to ℓ and replace a by zero. By Proposition 4.3.3 there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(R_i \bmod \mathfrak{p})] = 0$ for every i. We may assume that $v_\ell[\mathrm{ord}(T \bmod \mathfrak{p})] = t$. We deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] \geq t + 1$ and that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] = t$ so we find a contradiction.

Without loss of generality we prove that a_h is divisible by ℓ. Suppose not. The point $(R_1, \ldots, a_h R_h + aT)$ is independent in $\mathbb{G}_m^h$. Thus by Proposition 4.3.3 there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(R_i \bmod \mathfrak{p})] = 0$ for every $i \neq h$ and $v_\ell[\mathrm{ord}(a_h R_h + aT \bmod \mathfrak{p})] = t + 1$. We easily deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] \geq t + 2$ and that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] = t + 1$, contradiction.

Now we can write

$$\frac{a}{\ell} T + \sum_{i=1}^{m} \frac{a_i}{\ell} R_i = \frac{c}{\ell} Q_1 + W$$

where W is in $\mathbb{G}_m[\ell]$.

If $t \geq 1$ then W is a multiple of T and we conclude. If $W = 0$ we also conclude. Now suppose that $t = 0$ and $W \neq 0$. By Proposition 4.3.3 there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(R_i \bmod \mathfrak{p})] = 0$ for every i. We may assume that the order of $(W \bmod \mathfrak{p})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] = 0$ and $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] \geq 1$, a contradiction. □

Condition (LSP) is trivially satisfied for any P in $G(K)$ if and only if Q is a torsion point of order coprime to ℓ (see Corollary 4.4.2). If Q is not a torsion point of order coprime to ℓ, it is possible to choose ϕ non-zero: this is obvious if Q has infinite order (since $cQ \neq 0$); if Q is a torsion point then it suffices to show that P is not independent, which is an immediate consequence of Theorem 4.2.1.

From the equality $\phi(P) = cQ$ we deduce that if P is a torsion point, then Q is also a torsion point. In general Q can be a torsion point and P a point of infinite order. Indeed, the left $\mathrm{End}_K G$-module generated by a K-point of infinite order may contain torsion points.

Notice that condition (LSP) is equivalent to the following: the order of $(\ell^n Q \bmod \mathfrak{p})$ is coprime to ℓ whenever the order of $(\ell^n P \bmod \mathfrak{p})$ is coprime to ℓ for all $n \in \mathbb{N}$ and for all but finitely many primes $\mathfrak{p}$ of K.

Remark 6.3.3. *In Theorem 6.1.1, it suffices to require that there exists an integer $d \geq 0$ such that for all but finitely many primes $\mathfrak{p}$ of K one has*

$$v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] - d.$$

Proof. It suffices to show that P and $\ell^d Q$ satisfy the hypotheses of Theorem 6.1.1. Obviously $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(\ell^d Q \bmod \mathfrak{p})]$ whenever the right hand side of this inequality is zero. Otherwise for almost all primes $\mathfrak{p}$ we have:

$$v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] \geq v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] - d = v_\ell[\mathrm{ord}(\ell^d Q \bmod \mathfrak{p})].$$

□

Notice that in Theorem 6.1.1 (respectively in the other results of this chapter) it suffices to require the condition for 'all primes of K outside a set of Dirichlet density zero' rather then 'for all but finitely many primes of K'.

Remark 6.3.4. *Under the assumptions of Corollary 6.2.3, one can take c such that $v_\ell(c) \leq v_\ell(m)$ where m is a non-zero integer depending only on G_1, G_2 and K.*

Proof. Apply Theorem 6.1.2 to $G_1 \times G_2$ and its K-points $P' = (P, 0)$ and $Q' = (0, Q)$. Then there exist a K-endomorphism ψ of $G_1 \times G_2$ and an integer c such that $\psi(P') = cQ'$ and one can take c such that $v_\ell(c) \leq v_\ell(m)$ where m is a non-zero integer depending only on $G_1 \times G_2$ and K. Consequently, there exists a K-homomorphism ϕ from G_1 to G_2 such that $\phi(P) = cQ$. Notice that c is a non-zero integer such that $v_\ell(c) \leq v_\ell(m)$ where m is a non-zero integer depending only on G_1, G_2 and K. □

Chapter 7

The radical support problem

7.1 Introduction

In this chapter we study a variant of the support problem which we call *radical support problem*. Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-points on G. We require the following condition on P and Q:

(RSP) *Let S be an infinite family of prime numbers. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the following holds: for every ℓ in S the order of $(Q \bmod \mathfrak{p})$ is coprime to ℓ whenever the order of $(P \bmod \mathfrak{p})$ is coprime to ℓ.*

This condition is in particular satisfied if the radical of the order of $(Q \bmod \mathfrak{p})$ divides the radical of the order of $(P \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.

Theorem 7.1.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let P and Q be K-points of G satisfying condition (RSP). Then there exist a K-endomorphism ϕ of G and a non-zero integer c such that $\phi(P) = cQ$.*

For abelian varieties, the previous result has an alternative proof by Larsen (see [Lar03, proof of Theorem 1]). If the set S is finite then the statement is no longer true, see Example 7.3.4.

Theorem 7.1.2. *Under the assumptions of Theorem 7.1.1, there exist two integers n and m depending only on G and K such that the following holds: one can take c such that $v_\ell(c) \leq v_\ell(m)$ for every ℓ in S coprime to n.*

If P is independent (for example if P is a point of infinite order on the multiplicative group or on a simple abelian variety) one can take $n = 1$, see Proposition 7.3.1.

In general for a split torus or for an abelian variety one cannot take $n = 1$, even if P and Q have both infinite order, see Example 7.3.2. A reason for this is the following: if the order of $(P \bmod \mathfrak{p})$ is divisible by some prime ℓ in S for all but finitely many primes $\mathfrak{p}$ of K then the condition of Theorem 7.1.1 is trivial for the prime ℓ.

Finally notice that whenever $G(K)$ is infinite one cannot bound $v_\ell(c)$ for any prime ℓ which is not in S, see Example 7.3.3.

7.2 The proof of Theorem 7.1.1

Proof of Theorem 7.1.1. First step. We reduce to prove Theorem 7.1.1 for $G = \prod_{i\in I} B_i$ where for every i the factor B_i is either $\mathbb{G}_m$ or a K-simple abelian variety and for every i, j either $B_i = B_j$ or $\mathrm{Hom}_K(B_i, B_j) = \{0\}$. To accomplish this, it suffices to combine two things: the statement holds for G if it holds for $\alpha(G)$ where α is a K-isogeny; the statement holds for G if it holds for $G \times_K L$, where L is a finite Galois extension of K. The second assertion is a consequence of Lemma 6.2.1. For the first assertion, let G' be the product of an abelian variety and a torus defined over K which is K-isogenous to G. We suppose that Theorem 7.1.1 holds for G' and prove it for G. Let α be a K-isogeny of degree a from G to G' and call $\hat{\alpha}$ the K-isogeny from $\alpha(G)$ to G satisfying $\hat{\alpha} \circ \alpha = [a]$. Call S' the complement in S of the divisors of a. Then by Corollary 1.3.2 and Lemma 1.3.5 the points $\alpha(P)$ and $\alpha(Q)$ satisfy the condition of Theorem 7.1.1 (the set of primes now being S'). We deduce that

$$\psi\big(\alpha(P)\big) = r\big(\alpha(aQ)\big)$$

where ψ is in $\mathrm{End}_K G'$ and r is a non-zero integer. We conclude because $\hat{\alpha} \circ \psi \circ \alpha$ is in $\mathrm{End}_K G$ and we have

$$\hat{\alpha} \circ \psi \circ \alpha\big(P\big) = \hat{\alpha} \circ [r] \circ \alpha\big(aQ\big) = ra^2 Q.$$

Second step. Let $G = \prod_{i\in I} B_i$ where for every $i \in I$ the factor B_i is either $\mathbb{G}_m$ or a K-simple abelian variety and for every i, j either $B_i = B_j$ or $\mathrm{Hom}_K(B_i, B_j) = \{0\}$. Write $P = (P_1, \ldots, P_n)$, $Q = (Q_1, \ldots, Q_n)$. Without loss of generality we may replace Q by $(Q_1, 0, \ldots, 0)$. We may assume that Q has infinite order (otherwise take $\phi = 0$ and $c = \mathrm{ord}\, Q$). Then we may assume that also P has infinite order. Otherwise let ℓ be a prime of S coprime to the order of P. We find a contradiction by Corollary 4.4.2 (there exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{p})] > 0$).

Apply Lemma 3.4.2 to P and let J, d, P', G' be as in Lemma 3.4.2. Since P' is a projection of P, it suffices to prove that there exist ψ in $\mathrm{Hom}_K(G', B_1)$ and a non-zero integer c such that $\psi(P') = cQ_1$.

The point (P', Q_1) is not independent in $G' \times B_1$. Indeed, let ℓ be a prime in S coprime to d and apply Proposition 4.3.3. There exist infinitely many primes $\mathfrak{p}$ of K such that $v_\ell[\mathrm{ord}(P' \bmod \mathfrak{p})] = 0$ and $v_\ell[\mathrm{ord}(Q_1 \bmod \mathfrak{p})] = 1$. We find a contradiction since by definition of d we have $v_\ell[\mathrm{ord}(P \bmod \mathfrak{p})] \leq v_\ell(d) + v_\ell[\mathrm{ord}(P' \bmod \mathfrak{p})] = 0$.

Third step. Since (P', Q_1) is not independent, we have $f(P') = g(Q_1)$ for some f and g in $\mathrm{End}_K(G' \times B_1)$ such that not both f and g are zero.

Recall that G' is the product of some B_i's such that for every i, j either $B_i = B_j$ or $\mathrm{Hom}_K(B_i, B_j) = \{0\}$. Then since P' is independent in G' we deduce that $\tilde{f}(P') = \tilde{g}(Q_1)$ for some $\tilde{f}$ in $\mathrm{Hom}_K(G', B_1)$ and some $\tilde{g}$ in $\mathrm{End}_K B_1$, where not both $\tilde{f}$ and $\tilde{g}$ are zero. Since P' is independent in G' and B_1 is a factor of G', if $\tilde{g} = 0$ then $\tilde{f} = 0$. We deduce that $\tilde{g}$ is non-zero. Since B_1 is either $\mathbb{G}_m$ or a K-simple abelian variety, $\tilde{g}$ is an isogeny and therefore it factors a non-zero integer in $\mathrm{End}_K B_1$. This concludes the proof. □

Corollary 7.2.1. *Let G_1 and G_2 be products of an abelian variety and a torus defined over a number field K. Let P and Q be K-points on G_1 and G_2 respectively. Let S be an infinite family of rational primes. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the following holds: for every ℓ in S the order of $(Q \bmod \mathfrak{p})$ is coprime to ℓ whenever the order of $(P \bmod \mathfrak{p})$ is coprime to ℓ. Then there exist ϕ in $\mathrm{Hom}_K(G_1, G_2)$ and a non-zero integer c such that $\phi(P) = cQ$.*

Proof. Apply Theorem 7.1.1 to $G_1 \times G_2$ and its K-points $(P, 0)$ and $(0, Q)$. □

7.3 On the integer c of the radical support problem

The following result is the generalization of a result by Khare and Prasad ([KP04, Lemma 5]).

Proposition 7.3.1. *Under the assumptions of Corollary 7.2.1, if P is independent in G_1 then one can take c coprime to ℓ for every ℓ in S.*

Proof. We have $\phi P = cQ$ for some ϕ in $\mathrm{Hom}_K(G_1, G_2)$ and some non-zero integer c. By iteration, it suffices to prove that if c is divisible by ℓ for some ℓ in S there exists ψ in $\mathrm{Hom}_K(G_1, G_2)$ such that $\psi P = \frac{c}{\ell} Q$. So suppose that c is divisible by ℓ for some fixed prime ℓ in S. Let P' be a point in $G_1(\bar{K})$ such that $\ell P' = P$. We then have $\phi(P') = \frac{c}{l} Q + Z$ for some Z in $G_1[\ell]$. Write L for a finite extension of K over which $G_1[\ell]$ is split and where P' is defined. Notice that P' is also independent in G_1. The condition of Corollary 7.2.1 clearly implies that for all but finitely many primes $\mathfrak{q}$ of L the order of $(Q \bmod \mathfrak{q})$ is coprime to ℓ whenever the order of $(P \bmod \mathfrak{q})$ is coprime to ℓ.

First we prove that $\phi = [\ell] \circ \psi$ for some ψ in $\mathrm{Hom}_K(G_1, G_2)$. Suppose not and then let T be a point in $G_1[\ell] \setminus \ker(\phi)$.

Suppose that $\phi(T) \neq Z$. By Proposition 4.3.2 there exist infinitely many primes $\mathfrak{q}$ of L such that $v_\ell[\mathrm{ord}(P' - T \bmod \mathfrak{q})] = 0$. We deduce that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 0$ and that the point $(\phi(P') - \phi(T) \bmod \mathfrak{q})$ has order coprime to ℓ. Then

$$r_\mathfrak{q} \phi(T) = r_\mathfrak{q} \phi(P') = r_\mathfrak{q}(\frac{c}{l} Q + Z) \ (\mathrm{mod} \mathfrak{q})$$

for some integer $r_\mathfrak{q}$ coprime to ℓ. Therefore

$$r_\mathfrak{q} \frac{c}{l} Q = r_\mathfrak{q}(\phi(T) - Z) \ (\mathrm{mod} \mathfrak{q}).$$

By discarding finitely many primes $\mathfrak{q}$ we may assume that the order of $(\phi(T) - Z \bmod \mathfrak{q})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})] > 0$ and we find a contradiction.

Now suppose that $\phi(T) = Z$. Then $\phi(P') = \frac{c}{l} Q + \phi(T)$. By Proposition 4.3.2 there exist infinitely many primes $\mathfrak{q}$ of L such that $v_\ell[\mathrm{ord}(P' \bmod \mathfrak{q})] = 0$. Then $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 0$. By discarding finitely many primes $\mathfrak{q}$ we may assume that the order of $(\phi(T) \bmod \mathfrak{q})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})] > 0$ and we find a contradiction.

So we can factor ϕ as $[\ell] \circ \psi$ for some ψ in $\mathrm{Hom}_K(G_1, G_2)$. Then $\psi(P) = \frac{c}{\ell}Q + T'$ for some T' in $G_1[\ell]$. It suffices to prove that $T' = 0$. By Theorem 4.2.1, there exist infinitely many primes $\mathfrak{q}$ of L such that $v_\ell[\mathrm{ord}(P \bmod \mathfrak{q})] = 0$.

If $T' \neq 0$ then by discarding finitely many primes $\mathfrak{q}$ we may assume that the order of $(T' \bmod \mathfrak{q})$ is ℓ. We deduce that $v_\ell[\mathrm{ord}(Q \bmod \mathfrak{q})] > 0$ and we have a contradiction. □

We are now able to prove Theorem 7.1.2.

Proof of Theorem 7.1.2. We first reduce to the case $G = A \times T$ where A is an abelian variety and T is a split torus. For this, it suffices to show that the statement holds for G if it holds for $G \times_K L$ where L is a finite Galois extension of K. This is a consequence of Lemma 6.2.1 since we can ignore the primes in S which divide the degree of the extension L/K.

We may replace P by $n_P P$: by Proposition 3.2.2, we can ignore the primes of S which divide n_P. In this way we reduce to the case where G_P is connected.

If P is zero then by Corollary 4.4.2 we immediately deduce that Q is a torsion point. Then the order of Q is coprime to every prime ℓ in S and the statement holds since we can take $c = \mathrm{ord}\, Q$.

Now we may assume that G_P is connected and non-zero. Then P is independent in G_P so by Proposition 7.3.1 there exist ψ_ℓ in $\mathrm{Hom}_K(G_P, G)$ and an integer r coprime to every ℓ in S such that $\psi_\ell(P) = rQ$.

By Proposition 2.1.2, $G_P = A' \times T'$ where A' is an abelian subvariety of A and T' is a sub-torus of T. Write $P = (P_{A'}, P_{T'})$ and apply Lemma 3.2.1 to $P_{A'}$. Notice that A' is the algebraic subgroup of A generated by $P_{A'}$. Let Z and t be as in Lemma 3.2.1. Then the map

$$j : A' \times Z \to A\,;\ (x, y) \mapsto x + y.$$

is a K-isogeny in $\mathrm{Hom}_K(A' \times Z, A)$ of degree dividing t. Call $\hat{\jmath}$ the isogeny in $\mathrm{Hom}_K(A, A' \times Z)$ satisfying $\hat{\jmath} \circ j = [t]$. We have

$$\hat{\jmath}\big(P_{A'}\big) = \hat{\jmath} \circ j\big((P_{A'}, 0)\big) = (tP_{A'}, 0).$$

Then there is an element π_A in $\mathrm{Hom}_K(A, A')$ mapping $P_{A'}$ to $tP_{A'}$. Since T' is a direct factor of T, there exists π_T in $\mathrm{Hom}_K(T, T')$ such that $\pi_T(P_{T'}) = tP_{T'}$. Let Π be $\pi_A \times \pi_T$. Then Π is in $\mathrm{Hom}_K(G, G_P)$ and $\Pi(P) = tP$. The map $\phi = \psi \circ \Pi$ is in $\mathrm{End}_K G$ and we have $\phi(P) = rtQ$. Consequently in this case one can take $m = t$, $n = 1$. This concludes the proof. □

Example 7.3.2. Let ℓ be a rational prime. Let E be an elliptic curve defined over a number field K such that $E(K)$ contains a point R of infinite order and a torsion point T of order ℓ. Consider the points $P = (\ell^n R, T)$ and $Q = (R, 0)$ on E^2, for some n in $\mathbb{N}$. Then the points P and Q satisfy the condition of Theorem 7.1.1 where S is the set of all primes but one has to take c such that $v_\ell(c) \geq n$. By varying n, we see at once that that one cannot bound $v_\ell(c)$ with a constant depending only on E and K.

Example 7.3.3. Let G be the product of an abelian variety and a torus defined over a number field K and such that $G(K)$ is infinite. Let R be a point in $G(K)$ of infinite order and let ℓ be a rational prime. The points $P = \ell^n R$ and $Q = R$ satisfy the condition of Theorem 7.1.1 where S is the set of primes different from ℓ. By varying n, we see at once that one cannot bound $v_\ell(c)$ for the prime ℓ with a constant depending only on G and K.

Example 7.3.4. Let S be a finite family of prime numbers and let m be the product of the primes in S. Let G be the product of an abelian variety and a torus defined on a number field K such that the following holds: $G(K)$ contains a torsion point T of order m; $G(K)$ contains two points R, W of infinite order such that the point (R, W) is independent in G^2. Consider the points $P = (R, T)$, $Q = (W, 0)$ in G^2. Then the order of P is a multiple of m for almost all prime $\mathfrak{p}$ of K hence the points P and Q satisfy the condition of Theorem 7.1.1 for the set S. Nevertheless, since (R, W) is independent in G^2 no non-zero multiple of Q lies in the left $\mathrm{End}_K G^2$-submodule of $G^2(K)$ generated by P.

Chapter 8

The multilinear support problem

8.1 Introduction

In this chapter we discuss the *multilinear support problem*, introduced by Barańczuk in [Bar06]. This variant of the support problem concerns several points. The points P and Q are replaced by n-tuples $P_1, \ldots, P_n$ and $Q_1, \ldots, Q_n$.
Let G be the product of an abelian variety and a torus defined over a number field K.

(MSP) *Suppose that for all but finitely many primes* $\mathfrak{p}$ *of* K *the following holds: for all integers* $m_1, \ldots, m_n$ *the point* $(m_1Q_1 + \ldots + m_nQ_n \bmod \mathfrak{p})$ *is zero whenever the point* $(m_1P_1 + \ldots + m_nP_n \bmod \mathfrak{p})$ *is zero.*

This condition is strong: if $n > 1$ it is stronger than the condition of the support problem on each pair of points (P_i, Q_i).

Assuming condition (MSP), we know that there exist K-endomorphisms ϕ_i and an integer c such that $\phi_i(P_i) = cQ_i$. One would like to prove that ϕ_i and ϕ_j are related for $i \neq j$. This is true if the endomorphism ring is $\mathbb{Z}$. In this case $\phi_i = \phi_j$ for every i, j. See [Bar06, Theorem 7.3]. The same proof holds for the multiplicative group, hence for 1-dimensional tori. In general ϕ_i and ϕ_j are not related for $i \neq j$, see Example 8.2.2.

One can also consider the ℓ-adic analogous of condition (MSP), which is stronger than the condition of the ℓ-adic support problem on each pair of points (P_i, Q_i).

(LMSP) *Suppose that for all but finitely many primes* $\mathfrak{p}$ *of* K *the following holds: for all integers* $m_1, \ldots, m_n$ *the order of* $(m_1Q_1 + \ldots + m_nQ_n \bmod \mathfrak{p})$ *is coprime to* ℓ *whenever the order of* $(m_1P_1 + \ldots + m_nP_n \bmod \mathfrak{p})$ *is coprime to* ℓ.

Assuming condition (LMSP), we know that there exist K-endomorphisms ϕ_i and an integer c such that $\phi_i(P_i) = cQ_i$. One would like to prove that ϕ_i and ϕ_j are related if $i \neq j$. This is true if the endomorphism ring is $\mathbb{Z}$. In this case ϕ_i and ϕ_j are two integers with the same ℓ-adic valuation, see [Bar06, proof of Theorem 7.3]. The same proof holds for the multiplicative group, hence for 1-dimensional tori. We show in Example 8.2.3 that ϕ_i and ϕ_j are in general not related, not even for elliptic curves.

We can also weaken condition (MSP) by imposing that $m_1 = 1$. Then one would like to prove that for every i there exist K-endomorphisms ϕ_i and an integer c_i such that $\phi_i(P_i) = c_i Q_i$. Without loss of generality, it suffices to consider two pairs of points:

(WMSP) *Suppose that for all but finitely many primes* $\mathfrak{p}$ *of* K *and for all integers* m *the point* $(Q_1 + mQ_2 \bmod \mathfrak{p})$ *is zero whenever the point* $(P_1 + mP_2 \bmod \mathfrak{p})$ *is zero.*

If G is a simple abelian variety, under condition (WMPS) Barańczuk proved that for $i = 1, 2$ there exist a K-endomorphism ϕ_i and an integer c_i such that $\phi_i(P_i) = c_i Q_i$, see [Bar06, Theorem 8.1]. The same proof holds for the multiplicative group hence for 1-dimensional tori. This result is in general false for a non-simple abelian variety or for a torus of dimension > 1, see Example 8.2.4.

8.2 The counterexamples

We first show that condition (MSP) is stronger than the condition of the support problem on every pair of points, even if one requires $m_1, \ldots, m_n$ to be positive (as in [Bar06]).

Remark 8.2.1. *Assuming condition (MSP) where* $m_1, \ldots, m_n$ *are positive, the following holds: for every* $i = 1, \ldots, n$ *the order of* $(Q_i \bmod \mathfrak{p})$ *divides the order of* $(P_i \bmod \mathfrak{p})$ *for all but finitely many primes* $\mathfrak{p}$ *of* K*.*

Proof. Without loss of generality it suffices to prove the claim for P_1 and Q_1. Let $\mathfrak{p}$ be a prime ideal of K such that condition (MSP) holds. For every $i \neq 1$ take m_i such that $(m_i P_i \bmod \mathfrak{p}) = 0$ and $(m_i Q_i \bmod \mathfrak{p}) = 0$. Then for every positive integer m_1 we have $(m_1 Q_1 \bmod \mathfrak{p}) = 0$ whenever $(m_1 P_1 \bmod \mathfrak{p}) = 0$. Consequently, the order of $(Q_1 \bmod \mathfrak{p})$ divides the order of $(P_1 \bmod \mathfrak{p})$. □

By reasoning as we did for the previous remark, it is immediate to see that [Bar06, Theorem 8.2] is equivalent to Theorem 6.1.1 for simple abelian varieties.

Example 8.2.2. Let E be an elliptic curve defined over a number field K. Let R_1, R_2 be points in $E(K)$ and let ψ_1,ψ_2 be in $\mathrm{End}_K E$. The following points in $E \times E(K)$ satisfy condition (MSP):

$$P_1 = (R_1, 0)\,;\ P_2 = (0, R_2)\,;\ Q_1 = (\psi_1(R_1), 0)\,;\ Q_2 = (0, \psi_2(R_2)).$$

Example 8.2.3. Let E be an elliptic curve defined over a number field K such that $\mathrm{End}_K E = \mathbb{Z}[i]$. Let ϕ_1 and ϕ_2 be in $\mathrm{End}_K E$ and let P_1 be in $E(K)$. The following points satisfy condition (LMSP) for $\ell = 3$:

$$P_1\,;\ P_2 = i(P_1)\,;\ Q_1 = \phi_1(P_1)\,;\ Q_2 = \phi_2(P_2).$$

Indeed, let $\mathfrak{p}$ be a prime of K of good reduction for E not over 3 and suppose that $(m_1 P_1 + m_2 P_2 \bmod \mathfrak{p})$ has order coprime to 3. It is sufficient to show that both $(m_1 P_1 \bmod \mathfrak{p})$ and $(m_2 P_2 \bmod \mathfrak{p})$ have order coprime to 3. By multiplying P_1 and P_2 by an integer

coprime to 3, we may assume that $(P_1 \bmod \mathfrak{p}) = (R \bmod \mathfrak{p})$ for a point R in $E[3^\infty]$. Let L be a finite extension of K where R is defined and let $\mathfrak{q}$ be a prime of L over $\mathfrak{p}$. Then we have $(m_1R + m_2i(R) \bmod \mathfrak{q}) = 0$ and by the injectivity of the reduction modulo $\mathfrak{q}$ on $E[3^\infty]$ we deduce that $m_1R + m_2i(R) = 0$. We have to show that $m_1R = 0$. Let 3^h be the order of R. Then the annihilator of R is an ideal of $\mathbb{Z}[i]$ containing 3^h but not 3^{h-1}. Since 3 is prime in $\mathbb{Z}[i]$, the annihilator of R is (3^h). Since $m_1 + m_2i$ belongs to (3^h), we can write $(m_1 + m_2i) = 3^h(a_1 + a_2i)$ for some integers a_1, a_2. Therefore $m_1R = 3^h a_1 R = 0$.

Example 8.2.4. Let G be either an elliptic curve without complex multiplication or the multiplicative group defined over a number field K. Suppose that the rank of $G(K)$ is greater than 1. Then let (R, W) be a K-point on G^2 which is independent. Consider the following points in $G^2(K)$:

$$P_1 = Q_1 = Q_2 = (R, 0)\,; P_2 = (0, W).$$

These points satisfy condition (WMSP) but there does not exist a K-endomorphism ϕ of G^2 and a non-zero integer c such that $\phi(P_2) = cQ_2$.

Chapter 9

The problem of detecting linear dependence

9.1 State of the art of the problem of detecting linear dependence

The problem of detecting linear dependence investigates whether the property for a point to belong to a group is a local-global principle.

Problem. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-point on G and let Λ be a finitely generated subgroup of $G(K)$. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Does R belong to Λ?*

The problem of detecting linear dependence was first formulated by Gajda in 2002 in a letter to Ken Ribet.

We first concentrate on the case of abelian varieties, for two reasons: the problem has mainly been studied for abelian varieties; the problem is still unsolved for abelian varieties.

- The strongest result is by Weston in [Wes03]: if G is such that $\mathrm{End}_K G$ is commutative then there exists a K-point T of finite order such that $R + T$ belongs to Λ. Since the torsion of the Mordell-Weil group is finite, Weston basically solved the problem for abelian varieties with commutative endomorphism ring. It is not known how to get rid of this torsion point, unless $\mathrm{End}_K G$ is $\mathbb{Z}$.
- If the endomorphism ring of the abelian variety is not commutative, we are able to prove the following: there exists a non-zero integer m (depending only on G and K) such that mR belongs to the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by Λ. See Theorem 9.2.1 and Remark 9.2.2.
- We solve the problem of detecting linear dependence in the case where Λ is a free $\mathrm{End}_K G$-submodule of $G(K)$ or it has a set of generators (as a group) which is also

a basis of a free left $\mathrm{End}_K G$-submodule of $G(K)$. With an extra assumption on the point R (that R generates a free $\mathrm{End}_K G$-submodule of $G(K)$), these two results are respectively proven by Gajda and Górnisiewicz in [GG07, Theorem B] and by Banaszak in [Ban07, Theorem 1.1]. We remove the assumption on the point R in Theorem 9.2.1 and in Theorem 9.3.1 respectively.

- If Λ is cyclic, we solve the problem of detecting linear dependence. This result was known only for elliptic curves, see [Kow03, Theorem 3.3] by Kowalski.

- Gajda and Górnisiewicz in [GG07] use the theory of integrally-semisimple Galois modules to study the problem of detecting linear dependence. This theory was completely developed by Larsen in [LS04]. Gajda and Górnisiewicz prove the following result ([GG07, Theorem A]):

  Let ℓ be a prime such that $T_\ell(G)$ is integrally semisimple. Let $\hat{\Lambda}$ be a free $\mathrm{End}_K G \otimes \mathbb{Z}_\ell$-submodule of $G(K) \otimes \mathbb{Z}_\ell$ and let $\hat{R}$ in $G(K) \otimes \mathbb{Z}_\ell$ generate a free $\mathrm{End}_K G \otimes \mathbb{Z}_\ell$-submodule of $G(K) \otimes \mathbb{Z}_\ell$. Then $\hat{R}$ belongs to $\hat{\Lambda}$ if and only if $(\hat{R} \bmod \mathfrak{p})$ belongs to $(\hat{\Lambda} \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. If $\mathrm{End}_K G \otimes \mathbb{Z}_\ell$ is a maximal order in $\mathrm{End}_K G \otimes \mathbb{Q}_\ell$, the condition on $\hat{\Lambda}$ can be replaced by the following: $\hat{\Lambda}$ is torsion-free over $\mathrm{End}_K G \otimes \mathbb{Z}_\ell$.

Now we list further results on the problem of detecting linear dependence for algebraic groups. Schinzel in [Sch75, Theorem 2] solved the problem of detecting linear dependence for the multiplicative group. A generalization of Schinzel's result (Theorem 9.3.4 for the multiplicative group with no conditions on Λ) was proven by Khare in [Kha03, Proposition 3] by applying a method by Corrales-Rodrigáñez and Schoof (see [CRS97]).

Our results on the problem of detecting linear dependence (Theorems 9.2.1, 9.3.1 and 9.4.1) hold for the product of an abelian variety and a torus.

Kowalski in [Kow03] investigated for which algebraic groups the property for a point to belong to a group is a local-global principle. In particular he proved that the answer is negative whenever the additive group is embedded in G ([Kow03, Proposition 3.2]).

Papers and preprints concerning the problem of detecting linear dependence are: [Sch75], [Kha03], [Wes03], [Kow03], [BGK05], [Ban07], [Bar08].

9.2 A general result

We prove the following theorem as an application of our results on the support problem:

Theorem 9.2.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-point on G and let Λ be a finitely generated subgroup of $G(K)$. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then there exists a non-zero integer m (depending only on G, K and the rank of Λ) such that mR belongs to the left $\mathrm{End}_K G$-submodule of $G(K)$ generated by Λ. If Λ is a free left $\mathrm{End}_K G$-submodule of $G(K)$ then R belongs to Λ.*

Remark 9.2.2. *If G is an abelian variety, the integer m in Theorem 9.2.1 depends only on G and K.*

Proof. If G is an abelian variety, the rank of Λ is bounded by the rank of the Mordell-Weil group therefore m depends only on G and K. □

Lemma 9.2.3. *Let K be a number field. Let G be the product of an abelian variety and a torus defined over K. Let R be a K-point on G and let Λ be a finitely generated subgroup of $G(K)$. Fix a rational prime ℓ. Suppose that for all but finitely many primes $\mathfrak{p}$ of K there exists an integer $c_{\mathfrak{p}}$ coprime to ℓ such that $(c_{\mathfrak{p}}R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then there exists a non-zero integer c such that cR belongs to $\mathrm{End}_K G \cdot \Lambda$ and $v_\ell(c) \leq v_\ell(m)$ where m depends only on G, K and the rank of Λ. If Λ is a free left $\mathrm{End}_K G$-submodule of $G(K)$, one can take $m = 1$.*

Proof. We may clearly assume that Λ is non-zero. Let $P_1, \ldots, P_s$ generate Λ as a $\mathbb{Z}$-module. Consider G^s and its K-points $P = (P_1, \ldots, P_s)$ and $Q = (R, 0, \ldots, 0)$. The points P and Q satisfy the hypotheses of Theorem 6.1.1. Then there exist a K-endomorphism ϕ of G^s and a non-zero integer c such that $\phi(P) = cQ$ and $v_\ell(c) \leq v_\ell(m)$ (where m depends only on G^s and K). In particular cR belongs to $\mathrm{End}_K G \cdot \Lambda$. Since s depends only on G, K and the rank of Λ, the first assertion is proven. For the second assertion, let $P_1, \ldots, P_s$ be a basis of Λ as a left $\mathrm{End}_K G$-module. Since P is independent, by Proposition 6.3.1 one can take c coprime to ℓ. Consequently, one can take $m = 1$. □

Proof of Theorem 9.2.1. We apply Lemma 9.2.3 for every rational prime ℓ. Then for every ℓ there exists an integer c_ℓ such that $c_\ell R$ belongs to $\mathrm{End}_K G \cdot \Lambda$ and $v_\ell(c_\ell) \leq v_\ell(m)$, where m is a non-zero integer depending only on G, K and the rank of Λ. Since m is in the ideal of $\mathbb{Z}$ generated by the c_ℓ's, we deduce that mR belongs to $\mathrm{End}_K G \cdot \Lambda$. If Λ is a free left $\mathrm{End}_K G$-submodule of $G(K)$, one can take $m = 1$ in Lemma 9.2.3 hence R belongs to Λ. □

9.3 On a result by Banaszak

In this section we extend the result by Banaszak on the problem of detecting linear dependence ([Ban07, Theorem 1.1]) from abelian varieties to products of abelian varieties and tori. Furthermore, by adapting the proof by Banaszak we are able to remove his assumption on the point R (that R generates a free left $\mathrm{End}_K G$-submodule of $G(K)$).

Theorem 9.3.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let Λ be a finitely generated subgroup of $G(K)$ such that it has a set of generators (as a group) which is also a basis of a free left $\mathrm{End}_K G$-submodule of $G(K)$. Let R be a point of $G(K)$. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then R belongs to Λ.*

Lemma 9.3.2. *Let R be a commutative ring with 1. Let F be a free R-module. Suppose that s is an R-endomorphism of F sending every element to a multiple of itself. Then s is a scalar.*

Proof. It suffices to prove the statement if F has rank 2. Let e_1, e_2 be a basis of F. Then $s(e_1) = \lambda_1 e_1$ and $s(e_2) = \lambda_2 e_2$ and $s(e_1 + e_2) = \mu(e_1 + e_2)$ for some λ_1, λ_2, μ in R. We deduce that $\lambda_1 = \mu = \lambda_2$ therefore s is the multiplication by μ on F. □

The following proposition in the case of abelian varieties is proven in [Ban07, Step 2 of the proof of Theorem 1.1].

Proposition 9.3.3. *Let G be the product of an abelian variety and a torus defined over a number field K. Let α be a $\bar{K}$-endomorphism of G. Suppose that there exists a prime number ℓ such that the following holds: for every $n > 0$ and for every torsion point X of G of order ℓ^n the point $\alpha(X)$ is a multiple of X. Then α is a scalar.*

Proof. Apply the previous lemma to $R = \mathbb{Z}/\ell^n\mathbb{Z}$, $F = G[\ell^n]$ and taking for s the image of α in $\mathrm{End}_{\mathbb{Z}} G[\ell^n]$. We deduce that α acts as a scalar on $G[\ell^n]$. So for every n there exists an integer c_n such that α acts as the multiplication by $c_n (\bmod \ell^n)$ on $G[\ell^n]$. Since α commutes with the multiplication by ℓ we deduce that $c_{n+1} (\mathrm{mod} \ell^n) \equiv c_n (\mathrm{mod} \ell^n)$ for every n. This means that there exists c in $\mathbb{Z}_\ell$ such that $c (\mathrm{mod} \ell^n) \equiv c_n (\mathrm{mod} \ell^n)$ for every n. Then α acts on $T_\ell G$ as the multiplication by c.

Write $G = A \times T$ where A is an abelian variety and T is a torus. Since by Lemma 2.1.1 there are no non-zero morphisms between abelian varieties and tori, α is the product $\alpha_A \times \alpha_T$ of an endomorphism of A and an endomorphism of T. We prove that α_A and α_T are each the multiplication by an integer. Since it is then obvious that they are the multiplication by the same integer, we conclude. Notice that if A (respectively T) is zero then the requested property holds for α_A (respectively α_T).

Suppose that A is non-zero. We know that α_A acts on $T_\ell A$ as the multiplication by c. By [Mum70, Theorem 3 p.176], α_A is the multiplication by an integer. Consequently, c is an integer and α_A is the multiplication by c.

Suppose that T is non-zero. Let n be the dimension of T and let L be a finite extension of K such that T is L-isomorphic to $\mathbb{G}_m^n$. Call γ this isomorphism. Then α_T is the multiplication by an integer if and only if $\gamma \circ \alpha_T \circ \gamma^{-1}$ is the multiplication by an integer. Thus we may assume that T is $\mathbb{G}_m^n$. We know that $\alpha_{\mathbb{G}_m^n}$ acts on $T_\ell \mathbb{G}_m^n$ as the multiplication by c.

The endomorphism ring of $\mathbb{G}_m$ is $\mathbb{Z}$ hence we can identify the endomorphism ring of $\mathbb{G}_m^n$ with the ring of $n \times n$-matrices with integer coefficients. Since $\alpha_{\mathbb{G}_m^n}$ acts on $T_\ell \mathbb{G}_m^n$ as the multiplication by c, we deduce that $\alpha_{\mathbb{G}_m^n}$ is a scalar matrix. Hence c is an integer and $\alpha_{\mathbb{G}_m^n}$ is the multiplication by c. □

Theorem 9.3.4. *Let G be the product of an abelian variety and a torus defined over a number field K. Let Λ be a finitely generated subgroup of $G(K)$ such that it has a set of generators (as a group) which is also a basis of a free left $\mathrm{End}_K G$-submodule of $G(K)$. Let R be a point of $G(K)$. Fix a prime number ℓ. Suppose that for all but finitely many primes $\mathfrak{p}$ of K there exists an integer $c_\mathfrak{p}$ coprime to ℓ such that the point $(c_\mathfrak{p} R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then there exists an integer c coprime to ℓ such that cR belongs to Λ.*

Proof. We may clearly assume that Λ is non-zero. Let $\{P_1, ..P_n\}$ be a set of generators for Λ (as a group) which is a basis for a free left $\mathrm{End}_K G$-submodule of $G(K)$. Notice that this left-module is $\mathrm{End}_K G \cdot \Lambda$. By Lemma 9.2.3 there exists an integer c coprime to ℓ such that cR belongs to $\mathrm{End}_K G \cdot \Lambda$. So write

$$cR = \sum_{i=1}^{n} \phi_i P_i$$

for some ϕ_i in $\mathrm{End}_K A$. Without loss of generality it suffices to prove that ϕ_1 is the multiplication by an integer.

Suppose that ϕ_1 is not the multiplication by an integer and apply Proposition 9.3.3 to ϕ_1. Then there exists a torsion point T in $G(\bar{K})$ such that $\phi_1(T)$ is not a multiple of T. Let L be a finite extension of K where T is defined. The point $(P_1 - T, P_2, \ldots, P_n)$ is independent in G^n by Lemma 3.4.1. Then by Proposition 4.3.3 there are infinitely many primes $\mathfrak{q}$ of L such that the following holds: $(P_i \bmod \mathfrak{q})$ has order coprime to ℓ for every $i \neq 1$ and $(P_1 - T \bmod \mathfrak{q})$ has order coprime to ℓ. By discarding finitely many primes $\mathfrak{q}$, we may assume the following: the order of $(T \bmod \mathfrak{q})$ equals the order of T; the point $(\phi_1(T) \bmod \mathfrak{q})$ is not a multiple of $(T \bmod \mathfrak{q})$ and in particular it is non-zero; $(c_{\mathfrak{q}} R \bmod \mathfrak{q})$ belongs to $(\Lambda \bmod \mathfrak{q})$ for some integer $c_{\mathfrak{q}}$ coprime to ℓ.

Fix $\mathfrak{q}$ as above. We know that there exists an integer m coprime to ℓ such that $(mP_i \bmod \mathfrak{q}) = 0$ for every $i \neq 1$ and $(m(P_1 - T) \bmod \mathfrak{q}) = 0$. Then we have:

$$(mc_{\mathfrak{q}} cR \bmod \mathfrak{q}) = (mc_{\mathfrak{q}} \phi_1(P_1) \bmod \mathfrak{q}) = (mc_{\mathfrak{q}} \phi_1(T) \bmod \mathfrak{q}).$$

Since $v_\ell(mc_{\mathfrak{q}}) = 0$, we deduce that the point $(mc_{\mathfrak{q}} cR \bmod \mathfrak{q})$ has order a power of ℓ and it is not a multiple of $(T \bmod \mathfrak{q})$. Then $(mc_{\mathfrak{q}} cR \bmod \mathfrak{q})$ does not belong to $\sum_{i=1}^{r} \mathbb{Z}(P_i \bmod \mathfrak{q})$. Consequently, $(c_{\mathfrak{q}} R \bmod \mathfrak{q})$ does not belong to $(\Lambda \bmod \mathfrak{q})$ and we have a contradiction. □

Proof of Theorem 9.3.1. For every prime number ℓ we can apply Theorem 9.3.4. Then for every ℓ there exists an integer c_ℓ coprime to ℓ such that $c_\ell R$ belongs to Λ. Since the ideal of $\mathbb{Z}$ generated by the c_ℓ's contains 1, we deduce that R belongs to Λ. □

9.4 On a problem by Kowalski

The problem of detecting linear dependence in the case where Λ is cyclic was studied by Kowalski in [Kow03]. Kowalski solved this problem for the multiplicative group and for elliptic curves ([Kow03, Theorem 3.3]). The following result solves the problem of detecting linear dependence in the case where Λ is cyclic for products of abelian varieties and tori.

Theorem 9.4.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let Λ be a cyclic subgroup of $G(K)$. Let R be a K-point on G. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then R belongs to Λ.*

Lemma 9.4.2. *Let G be the product of an abelian variety and a torus defined over a number field K. Let Λ be a cyclic subgroup of $G(K)$ of infinite order. Let T be a K-point on G of finite order. Suppose that for all but finitely many primes $\mathfrak{p}$ of K the point $(T \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. Then T is zero.*

Proof. Suppose that T is non-zero. Then T can be uniquely written as a sum of torsion points whose orders are prime powers. These torsion points are multiples of T. Consequently, we reduce at once to the case where the order of T is the power of a prime number ℓ.

Let $\Lambda = \mathbb{Z}P$ for a point P of infinite order. The algebraic subgroup G_P of G generated by P has dimension at least 1. Call n_P the number of connected components of G_P and call G_P^0 the connected component of the identity of G_P. Thus G_P^0 is non-zero and by Proposition 2.1.2 it is the product of an abelian variety and a torus defined over K. By Lemma 3.1.4, G_P is the translation of G_P^0 by a torsion point X in $G(\bar{K})$. So we have $P = X + Z$ for some point Z in $G_P^0(\bar{K})$. The point Z is independent in G_P^0: this easily follows from Remark 3.1.3 since P and Z have a common multiple.

By Lemma 3.1.5, the point $n_P X$ is the least multiple of X which belongs to G_P^0.

Let c be the ℓ-adic valuation of the order of X. Let L be a finite extension of K where X, Z, $G[\ell^{2c}]$ are defined and such that $n_P X$ has n_P-roots in $G_P^0(L)$. Notice that for all but finitely many primes $\mathfrak{q}$ of L the point $(T \bmod \mathfrak{q})$ belongs to $(\mathbb{Z}P \bmod \mathfrak{q})$.

By Theorem 4.2.1, there exist infinitely many primes $\mathfrak{q}$ of L such that the order of $(Z \bmod \mathfrak{q})$ is coprime to ℓ. Then for infinitely many primes $\mathfrak{q}$ the point $(T \bmod \mathfrak{q})$ lies in the finite group generated by $(X \bmod \mathfrak{q})$. We deduce that $T = aX$ for some non-zero integer a.

Let T_0 be a point in G_P^0 of order ℓ^{2c}. By Theorem 4.2.1, there exist infinitely many primes $\mathfrak{q}$ of L such that the order of $(Z - T_0 \bmod \mathfrak{q})$ is coprime to ℓ. We deduce that for infinitely many primes $\mathfrak{q}$ the point $(T \bmod \mathfrak{q})$ lies in the finite group generated by $(T_0 + X \bmod \mathfrak{q})$. Then $T = b(T_0 + X)$ for some non-zero integer b.

Since $aX = b(T_0 + X)$ and because the order of T_0 is ℓ^{2c} we deduce that $v_\ell(b) \geq c$. Consequently, T is the sum of bT_0 and a torsion point of order coprime to ℓ. Then T is a multiple of T_0 and in particular it belongs to G_P^0.

Let T_1 be a point in $G_P^0(L)$ such that $n_P T_1 = -n_P X$. By Theorem 4.2.1, there exist infinitely many primes $\mathfrak{q}$ of L such that the order of $(Z - T_1 \bmod \mathfrak{q})$ is coprime to ℓ. Up to discarding finitely many primes $\mathfrak{q}$, we may assume that $(T \bmod \mathfrak{q})$ belongs to $(\mathbb{Z}P \bmod \mathfrak{q})$ and that the order of $(T \bmod \mathfrak{q})$ equals the order of T. Up to discarding finitely many primes $\mathfrak{q}$, by Lemma 3.1.6 we may assume that $(n_P X \bmod \mathfrak{q})$ is the least multiple of $(X \bmod \mathfrak{q})$ belonging to $(G_P^0 \bmod \mathfrak{q})$. Consequently, the intersection of $(G_P^0 \bmod \mathfrak{q})$ and $(\mathbb{Z}P \bmod \mathfrak{q})$ is $(\mathbb{Z}n_P P \bmod \mathfrak{q})$.

Fix a prime $\mathfrak{q}$ as above and call r the order of $(Z - T_1 \bmod \mathfrak{q})$. We have

$$(rn_P P \bmod \mathfrak{q}) = (rn_P Z + rn_P X \bmod \mathfrak{q}) = (rn_P T_1 + rn_P X \bmod \mathfrak{q}) = (0 \bmod \mathfrak{q}).$$

Since r is coprime to ℓ, it follows that $(T \bmod \mathfrak{q})$ cannot belong to the group generated by $(n_P P \bmod \mathfrak{q})$. But $(T \bmod \mathfrak{q})$ belongs to the intersection of $(G_P^0 \bmod \mathfrak{q})$ and of $(\mathbb{Z}P \bmod \mathfrak{q})$. We have a contradiction. □

Proof of Theorem 9.4.1. If Λ is finite then there exists a point P' in Λ such that for infinitely many primes $\mathfrak{p}$ of K it is $(R \bmod \mathfrak{p}) = (P' \bmod \mathfrak{p})$. Hence $R = P'$ and the statement is proven. We may then assume that $\Lambda = \mathbb{Z}P$ for a point P of infinite order.

We first prove that the statement holds in the case where the algebraic group G_P generated by P is connected. In this case, P is independent in G_P by Lemma 3.4.1. By Lemma [Kow03, Lemma 4.2], we may assume that $G_P = G$. So we may assume that P is independent in G. We conclude by applying Theorem 9.3.1.

For the general case, call n_P the number of connected components of G_P. Notice that the points $n_P P$ and $n_P R$ still satisfy the hypotheses of the theorem and that $G_{n_P P}$ is connected by Lemma 3.1.4. Therefore we know (by the special case above) that $n_P R = g n_P P$ for some integer g. Since R and P are K-points, we deduce that $R = gP + T$ for some K-point T of finite order. Since $R + T$ belongs to Λ, for all but finitely many primes $\mathfrak{p}$ of K the point $(T \bmod \mathfrak{p})$ belongs to $(\Lambda \bmod \mathfrak{p})$. By applying Lemma 9.4.2 we deduce that $T = 0$ hence R belongs to Λ. □

Bibliography

[Ban86] A. S. Bang, *Taltheoretiske undersøgelser*, Tidskrift f. Math **5** (1886), no. 4, 70–80 and 130–137.

[Ban07] G. Banaszak, *On a Hasse principle for Mordell-Weil groups*, arXiv:0712.3704, 2007.

[Bar06] S. Barańczuk, *On reduction maps and support problem in K-theory and abelian varieties*, J. Number Theory **119** (2006), no. 1, 1–17.

[Bar08] ———, *On a generalization of the support problem of Erdös and its analogues for abelian varieties and K-theory*, arXiv:0809.1991v3, 2008.

[BCZ03] Y. Bugeaud, P. Corvaja, and U. Zannier, *An upper bound for the g.c.d. of $a^n - 1$ and $b^n - 1$*, Math. Z. **243** (2003), 79–84.

[Ber87] D. Bertrand, *Minimal heights and polarizations on abelian varieties*, preprint M.S.R.I. 06220-87, 1987.

[Ber88] ———, *Galois representations and transcendental numbers*, New Advances in Trascendence Theory (Durham, 1986) (A. Baker, ed.), Cambridge University Press, Cambridge, 1988, pp. 37–55.

[BGK03] G. Banaszak, W. Gajda, and P. Krasoń, *Support problem for the intermediate Jacobians of ℓ-adic representations*, J. Number Theory **100** (2003), no. 1, 133–168.

[BGK05] ———, *Detecting linear dependence by reduction maps*, J. Number Theory **115** (2005), no. 2, 322–342.

[Bog80] F. A. Bogomolov, *Sur l'algébricité des représentations l-adiques*, C.R. Acad. Sci. Paris Sér. A–B **290** (1980), no. 15, A701–A703, presented by J.-P. Serre.

[Bor91] A. Borel, *Linear Algebraic Groups*, second ed., Graduate Texts in Mathematics, no. 126, Springer-Verlag, 1991.

[CH99] J. Cheon and S. Hahn, *The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve*, Acta Arith. **88** (1999), no. 3, 219–222.

[CRS97] C. Corrales-Rodrigáñez and R. Schoof, *The support problem and its elliptic analogue*, J. Number Theory **64** (1997), no. 2, 276–290.

[Dev07] A. Devic, *The support problem and its elliptic analogue*, March 2007, Master thesis at EPFL Lausanne, `http://alg-geo.epfl.ch/travdipl/index.html`.

[GG07] W. Gajda and K. Gornisiewicz, *Linear dependence in Mordell-Weil groups*, to appear in J. Reine Angew. Math., 2007.

[Gro60] A. Grothendieck, *Élements de géométrie algébrique III: Le langage des schémas*, Inst. Hautes Études Sci. Publ. Math. **4** (1960), pp. 228.

[Gro66] ———, *Élements de géométrie algébrique IV: Étude locale des schémas et des morphismes de schémas. III.*, Inst. Hautes Études Sci. Publ. Math. **28** (1966), pp. 255.

[Gro70] ———, *Schémas en groupes I: Propriétés génerales des schémas en groupes*, Séminaire de Géométrie Algébrique du Bois Marie - 1962/64 (SGA 3), vol. 1, Springer-Verlag, 1970, Lecture notes in mathematics 151.

[Har77] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, no. 52, Springer, 1977.

[JR07] R. Jones and J. Rouse, *Iterated endomorphisms of Abelian algebraic groups*, arXiv:0706.2384, 2007.

[Kha03] C. Khare, *Compatible systems of mod p Galois representations and Hecke characters*, Math. Res. Lett. **10** (2003), no. 1, 71–83.

[Kow03] E. Kowalski, *Some local-global applications of Kummer theory*, Manuscripta Math. **111** (2003), no. 1, 105–139.

[KP02] C. Khare and D. Prasad, *Reduction of homomorphisms mod p and algebraicity*, arXiv:0211004v1, 2002.

[KP04] ———, *Reduction of homomorphisms mod p and algebraicity*, J. Number Theory **105** (2004), no. 2, 322–332.

[Lar03] M. Larsen, *The support problem for abelian varieties*, J. Number Theory **101** (2003), no. 2, 398–403.

[Liu02] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2002.

[LS04] M. Larsen and R. Schoof, *Whitehead's lemma and Galois cohomology of abelian varieties*, `http://mlarsen.math.indiana.edu/~larsen/unpublished.html`, 2004.

[LS06] ———, *A refined counter-example to the support conjecture for abelian varieties*, J. Number Theory **116** (2006), no. 2, 396–398.

[Luk03] A. Lukić, *The support problem*, June 2003, Master thesis at the University of Utrecht. `http://www.math.leidenuniv.nl/docs/`.

[McQ95] M. McQuillan, *Division points on semi-abelian varieties*, Invent. math. **120** (1995), no. 1, 143–159.

[Mum70] D. Mumford, *Abelian varieties*, Oxford University Press, 1970, published for the Tata Institute of Fundamental Research Studies in Mathematics, Bombay.

[Per09] A. Perucca, *Prescribing valuations of the order of a point in the reductions of abelian varieties and tori*, J. Number Theory **129** (2009), no. 2, 469–476.

[Pin04] R. Pink, *On the order of the reduction of a point on an abelian variety*, Math. Ann. **330** (2004), no. 2, 275–291.

[Pol03] A. Polishchuk, *Abelian varieties, theta functions and the Fourier transform*, Cambridge Tracts in Mathematics, no. 153, Cambridge University Press, 2003.

[Rib79] K. Ribet, *Kummer theory on extensions of abelian varieties by tori*, Duke Math. J. **46** (1979), no. 4, 745–761.

[RU07] N. Ratazzi and E. Ullmo, *Galois + Équidistribution = Manin–Mumford*, `http://www.math.u-psud.fr/~ratazzi/recherche.html`, 2007.

[SBR90] W. Lütkebohmert S. Bosch and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), no. 21, Springer, 1990.

[Sch74] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. **268/269** (1974), 27–33, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II.

[Sch75] ———, *On power residues and exponential congruences*, Acta Arith. **XXVII** (1975), 397–420.

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer Verlag, 1986.

[Sil88] J. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237.

[vdGM] G. van der Geer and B. Moonen, *Abelian varieties*, `http://www.science.uva.nl/~geer/`.

[Wes03] T. Weston, *Kummer theory of abelian varieties and reductions of Mordell-Weil groups*, Acta Arith. **110** (2003), 77–88.

[Wit03] O. Wittenberg, *Le problème du support pour les variétés abéliennes, d'après Larsen*, `http://www.dma.ens.fr/~wittenberg/autres.html`, 2003.