UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica

Dottorato di Ricerca in Matematica e Modelli

Ciclo XXXVI

Local-global divisibility in some commutative algebraic groups

SSD: MAT/02

Dottoranda:
Jessica Alessandrì

Coordinatore del corso:
Prof. **Davide Gabrielli**

Tutor:
Prof. **Riccardo Aragona**
Relatori:
Prof. **Rocco Chirivì**
Prof.ssa **Laura Paladino**

Anno Accademico 2022/2023

Contents

Abstract

In this thesis we study a local-global principle in algebraic groups that was first introduced by Dvornicich and Zannier in 2001, called the *local-global divisibility problem*. The problem is the following: given a commutative algebraic group $\mathcal{G}$ defined over a number field k and given q a positive integer, if $P \in \mathcal{G}(k)$ is such that for all but finitely many places v of k there exists $D_v \in \mathcal{G}(k_v)$ such that $P = qD_v$; can we conclude that there exists $D \in \mathcal{G}(k)$ such that $P = qD$? The algebraic groups considered in this thesis are algebraic tori and elliptic curves.

The problem was answered by Dvornicich and Zannier in the case $q = p$ for tori of prescribed dimension and then a sharp bound on the dimension was given by Illengo. He proved that, if a torus has dimension $< 3(p-1)$ the answer is positive and he showed a counterexample of exact dimension $3(p-1)$.

In the work presented in the first part of this thesis, which was recently published in the Bulletin of the London Mathematical Society, we complete the answer for any power of an odd prime p. We show that if the torus have dimension $< p-1$, then the local-global divisibility by any odd p^l holds. We also prove that this bound is best possible, by exhibiting a counterexample of higher dimension. In addition, we show that, if the base field has some additional properties, then it is still possible to prove the local-global divisibility by any odd p^l, for tori of dimension $< 3(p-1)$. All the proofs are done via Galois cohomology, by using criteria introduced by Dvornicich and Zannier.

In the second part, which was published in the European Journal of Mathematics, we study the 7–division fields of some families of elliptic curves with CM. The study of these fields is related to the local-global divisibility problem, since they (and their Galois groups) appear in the cohomology groups used for the above mentioned criteria.

The elliptic curves studied have Weierstrass form $y^2 = x^3 + bx$ and $y^2 = x^3 + c$, with b, c in the field k. We find explicit generators of the exensions and then, using this explicit description, we classify them according to their possible degree and Galois groups. We give two applications of the results achieved. Thanks to the description of such Galois groups, we are able to deduce the minimal cardinality of a *finite* set S of places of k where to check the local divisibility by 7 for the elliptic curves of the mentioned families. Since the local-global divisibility by a prime number holds for elliptic curves, this results assures that, if a rational point is 7–divisibile in k_v, for every $v \in S$, then it is also 7–divisibile in k. The other application concerns modular curves.

Acknowledgements

This thesis, and overall this achievement, could not be done without the great support of some awesome people. I wish to thank a few of them and I hope that anyone that may feel left out can forgive me, blaming the lack of space.

Firstly, I thank Prof. Riccardo Aragona for his enourmous patience and understanding. Thank you for giving me the opportunity to following my passions and for all your kindness and advices. I can surely say that without you this thesis would not exist.

I deeply thank Prof. Laura Paladino for suggesting a topic that I love studying, but most importantly for guiding me in the first steps of this wonderful (but sometimes intimidating) world of mathematical research. Thank you also for the great support that you gave (and still give) me throughout these years, for your great advices, inside and outside academics.

A big "thank you" goes to Prof. Rocco Chirivì, who I did not thank enough during our almost ten (TEN?!) years of knowing each other. Thanks for pushing me to do my best, for your unconditional help (even at the most incovenient time) and for all the maths done on small tables of random cafes.

I am grateful to my family: my mum Emily, my dad Michele, my sister Simona and my nonna Nzina. Thank you for supporting me everytime – and everywhere – with proudness and love. I don't always show how grateful I am to have a family that believes in me more than I do, and pushes me to always aim high. I love you.

I am grateful also to my "other" – or rather *extended* – family: Egidio, Concetta e Gianmarco. I feel so lucky to have found such wonderful people, who welcomed me immediately as one of them. I thank you for your kindness and love, for being there whenever I needed, as you would do for a daughter (or a sister).

I thank my friend Martina: although our days together in Pisa are over, we supported each other, especially in the difficulties of the PhD, and I know that we will do it always.

A warm hug and thank you goes to my friend Sara. You taught me what that real friendship does not care about distance or frequency, we will always be there for each other.

I feel the need to thank also Gess, the long-distance-friend and collegue that I wish I met earlier! These last months of the PhD life would have been much more difficult

and boring without you. Because of you, I also met Carlotta (that probably will never read these lines), who helped me more than she could ever imagine.

To the love of my life, Vincenzo, goes the biggest thanks. I know how difficult it could be to stay by my side, but you did it no matter what. Words cannot express how thankful I am to you and to life, for giving me you. Thank you for being my light when everything around me seemed black, for supporting me in every situation, even when it was impossible for anyone else to be around me. I hope you forgive me for everytime that I forgot how beatiful life is, with you by my side, for letting bad things – and thoughts – take over our moments, for not thanking you enough for all the smiles that I put on my face during these years. I am so proud of how much we grew and I cannot wait to see what the future holds for us.

Introduction

In this thesis we study an arithmetic property of *algebraic groups*, which can be thought as algebraic varieties endowed with a group law. In fact, the two main characters of this thesis are *algebraic tori* and *elliptic curves*, which are probably the first two examples that come to mind when thinking about a group law over a variety. For the first ones, one has just to think to classical multiplication between numbers; the second one is – slightly – more complicated, but has a nice (and well known) geometric representation.

The property that we are going to focus on lies in the realm of *local-global principles*. These principles arise from the idea that sometimes it is easier to find solutions of an equation in a *local* field than in a *global* field. Indeed, *Hilbert's Tenth Problem*, which asks whether there is an algorithm to decide if a diophantine equation has solutions in a certain ring (originally in $\mathbb{Z}$), has been solved for all the completions of $\mathbb{Q}$, i.e. $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p, but it is still unknown for $\mathbb{Q}$ itself. Therefore, it is quite natural to ask if we can somehow relate the solutions found in $\mathbb{Q}_v$, where v is a place (even infinite) of $\mathbb{Q}$, to the ones lying in $\mathbb{Q}$.

In general, given a global field k, if a property holding in (almost all) every completion k_v holds also in k, we say that there is a *Hasse principle* or a *local-global principle*. These kind of problems have been widely studied during the last century. For example, one of the most famous local-global principles is the Albert–Brauer–Hasse–Noether Theorem on central simple algebras (see e.g. [Roq06]). Connected to this theorem, there is the study of the failure of the Hasse principle for a variety, which is done via the study of the Brauer group of the variety (cf. [CS21] for more details).

The local-global principle that we investigate in this thesis originated by a particular case of the following famous theorem, that is also known as *Hasse principle for quadratic forms*, proved by Minkowski in the case of rational numbers and generalized by Hasse for any number field k. We denote with M_k the set of places of k.

Theorem 1 (Hasse-Minkowski)**.** *A quadratic form in $k[X_1, \dots, X_n]$ has nontrivial zeros in k if and only if it has nontrivial zeros in k_v, for every $v \in M_k$.*

One can replace the hypothesis "for every $v \in M_k$" with "for all but finitely many $v \in M_k$" to get a stronger form of the principle. For example, for $k = \mathbb{Q}$, if we fix $r \in \mathbb{Q}$ and we consider the quadratic form $X^2 - rY^2$, we are asking if a rational number that is a square modulo all but a finite number of primes is also a square in $\mathbb{Q}$ (the converse is clearly true).

Generalizing further, in the example above we can take q–powers instead of squares. Hence, we are asking if a point in $\mathbb{Q}^\times$, that is q–power for almost every completion of $\mathbb{Q}$, is also a q–power in $\mathbb{Q}$. An answer to this question, not only for $\mathbb{Q}$ but for any number field (actually, global field), is given by the Grunwald-Wang Theorem (see [Wan50] or Section 2.2). Observe that taking a point in $\mathbb{Q}^\times$ is equivalent to taking a point in the split torus $\mathbb{G}_m$ over $\mathbb{Q}$.

Motivated by this kind of questions, in 2001 Dvornicich and Zannier asked: *for which algebraic groups $\mathcal{G}$ over k and natural numbers q, the divisibility of a point P by q in $\mathcal{G}(k)$ is equivalent to local divisibility by q in almost every completion*? They indeed formulated the so called **local-global divisibility problem**, that we state below. Let q be a fixed positive integer and let $\mathcal{G}$ be a commutative algebraic group defined over k.

Problem 1 (Dvornicich and Zannier, [DZ01])**.** *If we assume that the point $P \in \mathcal{G}(k)$ has the following property: for all but finitely many $v \in M_k$ there exists $D_v \in \mathcal{G}(k_v)$ such that $P = qD_v$; can we conclude that there exists $D \in \mathcal{G}(k)$ such that $P = qD$?*

Observe that, by the Bézout identity and the unique factorization in $\mathbb{Z}$, it is sufficient to answer the problem when q is a power of a prime.

Answers to Problem 1 have been established in several cases. In the case of elliptic curves, the problem was long studied. For $q = p$ a prime number there is an affirmative answer over any number field k, proved in [DZ01] (this was also proved in [Won00, Theorem 1]). For powers p^n, with $n \geqslant 1$, Paladino, Ranieri and Viada gave an affirmative answer for p greater than a constant $C([k : \mathbb{Q}])$ that depends only on the absolute degree of k. In particular, if $k = \mathbb{Q}$ we have $p > 3$, and in general if $k \neq \mathbb{Q}$, we have $C([k : \mathbb{Q}]) = (3^{[k:\mathbb{Q}]/2}+1)^2$ (see [PRV12; PRV14] and the recent result [CL23]). Whereas for $q = p^n$, with $p = 2, 3$ and $n \geqslant 2$, there exist counterexamples over $\mathbb{Q}$ (see [Cre16; DZ04; Pal11]) and over $\mathbb{Q}(\zeta_3)$ (see [Cre13; GR17]). These counterexamples give also counterexamples in a finite extension of k, for each k linearly disjoint over L from the field $L(\mathcal{E}[p^n])$, where $L = \mathbb{Q}$ or $L = \mathbb{Q}(\zeta_3)$, respectively (see Remark 2.4.5 for further details).

For principally polarized abelian surfaces, in [GR18] Gillibert and Ranieri proved sufficient conditions for the local-global divisibility by any prime power p^n; while in [GR20] they generalized these conditions in order to answer the case of GL_2–type varieties (see also [GR17]). Furthermore, in [Pal19], Paladino produced conditions for the local-global p–divisibility for a general commutative algebraic group. We remark that in the case of abelian varieties, the problem is also linked to a classical question posed by Cassels in 1962 on the p–divisibility of the Tate-Shafarevich group (see [Cas62; ÇS15; Cre16]).

The central part of this thesis is devoted to the study of the local-global divisibility in the case when the algebraic group is an algebraic torus.

As mentioned, the classical case of the multiplicative group $\mathcal{G} = \mathbb{G}_m$ has a complete answer given by the Grunwald-Wang Theorem: positive for q not divisible by 8 and negative for $q = 2^n$ with $n \geqslant 3$. In general, the local-global divisibility by $q = p$ a prime number in an algebraic torus T was proved first in [DZ01], provided that $\dim(T) \leqslant \max\{3, 2(p-1)\}$. Later in [Ill08], Illengo improved the bound, showing that the answer is affirmative for tori of dimension strictly smaller that $3(p-1)$ and negative otherwise.

In this thesis and in particular in Chapter 2, we give a complete answer to Problem 1 when the algebraic group is a torus, for every power of odd primes. In particular, we

show that for every odd prime p the local-global divisibility by p^n for $n \geqslant 1$ holds for algebraic tori of dimension $r < p-1$, while for $r \geqslant p-1$ the local-global divisibility by p^n is no longer assured. Our results can be summarized in the following theorem.

Theorem 2. *Let p be an odd prime.*

(a) Let k be a number field and let T be a torus defined over k. If T has dimension less than $p-1$, then the local-global divisibility by p^n holds for $T(k)$, for every $n \geqslant 1$.

(b) For every $n \geqslant 2$ and for every $r \geqslant p-1$ there exists a torus defined over $k = \mathbb{Q}(\zeta_p)$ of dimension r and a finite extension L/k such that the local-global divisibility by p^n does not hold for $T(L)$.

Nevertheless, we also show that under certain conditions on the base field k, satisfied for example by adjoining a primitive p^n–th root of unity to k, we can say something more when $p-1 \leqslant \dim(T) < 3(p-1)$. In general, for every commutative algebraic group $\mathcal{G}$, we denote with $\mathcal{G}[q]$ the set of q–torsion points of $\mathcal{G}$ and with $k(\mathcal{G}[q])$ the field obtained by adjoining to k the coordinates of these points.

Theorem 3. *Let p be an odd prime and let $n \geqslant 1$ be an integer. Suppose that T is a torus defined over k with $p-1 \leqslant \dim(T) < 3(p-1)$ and p does not divide the degree $[k(T[p^n]) \cap k(\zeta_{p^n}) : k]$, where ζ_{p^n} is a p^n–th root of unity. Then the local-global divisibility by p^n holds for $T(k)$.*

The tools that we use to prove both the theorems come from Galois cohomology. In fact, a classical way to answer to local-global problems is to translate them into problems in cohomology. For example, we already mentioned that the study of the Hasse principle on a variety X is done through the Brauer group, that is defined as $\mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$ (c.f. [CS21], Definition 3.2.1 and Chapter 2 for the étale cohomology), which provides an obstruction to the principle (often the *only obstruction*, see e.g. [Col88; SS91]). In our case (and also for almost all the cited results over other algebraic groups), we use the cohomological criteria developed by Dvornicich and Zannier. They showed that the answer to Problem 1 is linked to the triviality of a subgroup of the first cohomology group $\mathrm{H}^1(\mathrm{Gal}(k(\mathcal{G}[q])/k), \mathcal{G}[q])$. Such a subgroup is called the *first local cohomology group* and, setting $G = \mathrm{Gal}(k(\mathcal{G}[q])/k)$, is defined as

$$\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q]) = \bigcap_{v \in \Sigma} (\ker \mathrm{H}^1(G, \mathcal{G}[q]) \xrightarrow{\mathrm{res}_v} \mathrm{H}^1(G_v, \mathcal{G}[q])), \tag{1}$$

where: Σ is the set of places of k unramified in $k(\mathcal{G}[q])$, the group G_v is the Galois group of the extension $k(\mathcal{G}[q])_w/k_v$ obtained localizing k at v and $k(\mathcal{G}[q])$ at a place w extending v, while res_v is the usual restriction map. We present in details the criteria introduced by Dvornicich and Zannier in Section 2.1.

From the description just given, it is clear that the answer to the local-global divisibility is linked to the behaviour of the field extensions $k(\mathcal{G}[q])/k$. Therefore, the study and classification of these extensions, which has an interest of its own, could also have applications in local-global divisibility.

In particular, in the case of elliptic curves (and abelian varieties) for any positive integer m, the field $k(\mathcal{E}[m])$ is called the m–**division field** of the curve $\mathcal{E}$ over k and

we denote it with k_m. We recall that the extension k_m/k is finite and Galois: in fact, the abscissas of the m–torsion points of $\mathcal{E}$ are the roots of the *m–th division polynomial* of $\mathcal{E}$, while the ordinates are obtained by solving the equations given by substituing the abscissas in the Weierstrass equation of $\mathcal{E}$.

In this thesis we classify the 7–division fields for the families of CM elliptic curves $\mathcal{F}_1 : y^2 = x^3 + bx$ and $\mathcal{F}_2 : y^2 = x^3 + c$, with $b, c \in k$.

The properties of the extensions k_m/k are a relevant topic in the study of elliptic curves. In fact, they are related to Galois representations on the total Tate module, to Iwasawa theory, to modularity and to the proof of the Mordell-Weil theorem. Moreover, there are many potential applications of the description of the extensions k_m/k: besides the local-global divisibility problem (cf. Section 3.7.1), they are used in Galois representation (see e.g. [Sha17]), descent problems (see [SS04] or, for a particular case, [Ban04]), points on modular curves ([BP12]) and on Shimura curves.

We know that, by Artin's Primitive Element Theorem, the extension k_m/k is monogeneous, but finding an explicit single generator is not as easy as it may seem. Since $\mathcal{E}[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, a generating set for k_m is given by $\{x_1, x_2, y_1, y_2\}$, where $\{P_1 = (x_1, y_1), P_2 = (x_2, y_2)\}$ is a generating set for $\mathcal{E}[m]$. We want to find explicit generators and generating sets that are as easy as possibile to be used in the applications mentioned above.

We notice that, by the properties of the Weil pairing, the field k_m contains ζ_m, a primitive m–th root of unity. Therefore, when $k = \mathbb{Q}$ we have $\mathbb{Q}(\mathcal{E}[m]) \neq \mathbb{Q}$ for every $m \geqslant 3$ and the extension $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is "as minimal as possible" when $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\zeta_m)$. Merel and Rebolledo proved that, when $m = p$ is a prime, such an equality holds only if $p \leqslant 5$ (see [Mer96; Reb03]). For $m = 3, 5$ a classification of all elliptic curves satisfying this equality is given in [Pal10] and in [GL16], respectively. In the latter, the authors also investigate the cases when $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is an abelian extension for all elliptic curves: among other important results, in particular they prove that if $\mathcal{E}$ is a CM elliptic curve and $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is abelian, then $m \in \{2, 3, 4, 5, 6, 8\}$.

For $m = 3$ and $m = 4$, a complete description of the fields k_m in terms of generators, degrees and Galois groups, was given in [BP16] (see also [BP12]) for $m = 3$ and $m = 4$ for arbitrary elliptic curves and in [Pal18] for $m = 5$ for the families of CM elliptic curves mentioned above, namely $\mathcal{F}_1 : y^2 = x^3 + bx$ and $\mathcal{F}_2 : y^2 = x^3 + c$, with $b, c \in k$. Furthermore, the case of 8–torsion is studied in [Yel17]: the author produced generators for the fields k_8 and gave information on the action of certain elements of the Galois groups.

As mentioned, in the work presented in Chapter 3, we continue this description and classification, studying the case when $m = 7$ for the elliptic curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$. We find explicit generators of the extensions k_7/k: they are described in Theorem 3.1.1 for the family $\mathcal{F}_1$ and Theorem 3.4.1 for the family $\mathcal{F}_2$. Thanks to these results, we classify the extensions k_7/k according to their possible degree and Galois group. In particular we find that for the family $\mathcal{F}_1$ the maximum possible degree is 96 (all the other possibilities are listed in Table 3.1 of Theorem 3.2.1). In this case, the Galois group is a semidirect product $\mathrm{Dic}_4 \rtimes \mathbb{Z}/6\mathbb{Z}$ (cf. Theorem 3.3.1), where Dic_4 is the dicyclic group of order 16. We also list all the other possibilities in Section 3.3. In the same way, for the family $\mathcal{F}_2$, we find that the maximum possible degree is 72 (and all the other possibilities are listed in Table 3.2 of Theorem 3.5.1). In this case, the Galois group is again a semidirect product $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$ (cf. Therem 3.6.1), where Dic_3 is the

dicyclic group of order 12, and the other possibilities are listed in Section 3.6.

Finally, we give two applications of these results, the first concerning the local-global divisibility problem. By the mentioned result [DZ01, Theorem 3.1], the local-global divisibility by a prime number holds for elliptic curves, therefore also for $q = 7$. In particular, the first local cohomology group $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{E}[7])$ (defined in (1)) is trivial. Observe that in the definition (1), the groups G_v are cyclic, since every $v \in \Sigma$ is unramified. By the Čebotarev Density Theorem, the local Galois group G_v varies over *all* cyclic subgroups of G as v varies in Σ. However, to apply the theorem, it suffices to take a subset S of Σ such that G_v varies over all cyclic subgroups of G as v varies in S. In particular we can choose a finite set S (on the contrary Σ is not finite): the local divisibility for all $v \in S$ implies the local divisibility for almost all places v. By looking at the description of the possible Galois groups and counting all of their cyclic subgroups, we are able to deduce the minimal cardinality of a finite set S of places of k where to check the local divisibility by 7 for the elliptic curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$ (in [Pal18] an answer was given when $q = 5$ for the curves of the same families). More precisely, we show that for elliptic curves in the family $\mathcal{F}_1$ we have $|S| \leqslant 18$ (cf. Theorem 3.7.1), while for elliptic curves in the family $\mathcal{F}_2$ we have $|S| \leqslant 15$ (cf. Theorem 3.7.2).

The other application concerns some remarks on CM-points on modular curves. For example, we show that if the field k contains ζ_3 and ζ_7, then the modular curves associated to the level 7 congruence groups $\Gamma(7)$, $\Gamma_0(7)$ and $\Gamma_1(7)$ (for the definitions, see Section 3.7.2) have a k–rational CM point (cf. Proposition 3.7.3).

The thesis is structured as follows.

- In Chapter 1 we give all the preliminary definitions and results about algebraic groups. After giving some general background, we focus first on algebraic tori, with particular emphasis on the norm-one torus, and then on elliptic curves.

- In Chapter 2 we study the local-global divisibility in algebraic tori. We give the cohomological interpretation of the problem and a detailed description of the known results in this case; then we prove Theorem 2 and Theorem 3. The results of this chapter are collected in the paper [ACP24], published in the *Bulletin of the London Mathematical Society*.

- Finally, in Chapter 3 we study the 7–division fields of the CM elliptic curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$, describing all the fields k_7 and their Galois groups and deducing the applications described above. All these results are collected in the paper [AP23], published in the *European Journal of Mathematics*.

Chapter 1

Preliminaries on algebraic groups

1.1 Basic definitions

In this section we present a few basic definitions and results about algebraic groups. They are all well known and they appear in vast literature. About definitions and basic properties of algebraic groups and their morphisms we refer to [Mil17; Ser12; Vos98]. We give here only some definitions that are central to our work. For the definitions using category theory we refer to [Mac13].

From now on we fix k to be a field. We will often consider number fields, but most of the results in this chapter apply to every field. We also fix an algebraic closure $\overline{k}$ of k. We let $* = \mathrm{Spm}(k)$, i.e. the maximal spectrum of k.

Definition 1.1.1. Let $\mathcal{G}$ be an algebraic scheme over k and let $m : \mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}$ be a morphism. The pair $(\mathcal{G}, m)$ (when it is clear we shall omitt the map m) is an **algebraic group** over k if there exist morphisms

$$e : * \longrightarrow \mathcal{G}, \quad \mathrm{inv} : \mathcal{G} \longrightarrow \mathcal{G}$$

such that the following diagrams commute.

$$\begin{array}{ccc} \mathcal{G}\times\mathcal{G}\times\mathcal{G} & \xrightarrow{\mathrm{Id}\times m} & \mathcal{G}\times\mathcal{G} \\ {\scriptstyle m\times\mathrm{Id}}\downarrow & & \downarrow{\scriptstyle m} \\ \mathcal{G}\times\mathcal{G} & \xrightarrow[m]{} & \mathcal{G} \end{array} \qquad \begin{array}{ccccc} *\times\mathcal{G} & \xrightarrow{e\times\mathrm{Id}} & \mathcal{G}\times\mathcal{G} & \xleftarrow{\mathrm{Id}\times e} & G\times * \\ & \searrow^{\simeq} & \downarrow{\scriptstyle m} & \swarrow_{\simeq} & \\ & & \mathcal{G} & & \end{array}$$

$$\begin{array}{ccccc} \mathcal{G} & \xrightarrow{(\mathrm{inv},\mathrm{Id})} & \mathcal{G}\times\mathcal{G} & \xleftarrow{(\mathrm{Id},\mathrm{inv})} & \mathcal{G} \\ \downarrow & & \downarrow{\scriptstyle m} & & \downarrow \\ * & \xrightarrow[e]{} & \mathcal{G} & \xleftarrow{e} & * \end{array}$$

When $\mathcal{G}$ is a variety we call $(\mathcal{G}, m)$ a **group variety**; when $\mathcal{G}$ is an affine scheme we call $(\mathcal{G}, m)$ an **affine algebraic group**.

Example 1.1.2. Consider $\mathrm{SL}_n := \mathrm{Spec}(k[T_{11}, T_{12}, \ldots, T_{nn}]/(\det(T_{ij}) - 1))$; it is an affine group variety with the usual matrix multiplication.

We recall that an **algebraic variety** X **over** k is an algebraic scheme over k that is separated (i.e. the diagonal is closed) and geometrically reduced ($X_{\overline{k}}$ is reduced, i.e. $\mathcal{O}_P$ has no nilpotent elements for every $P \in \overline{k}$). Moreover, if X is irreducible, all the rings $\mathcal{O}_X(U)$ for U affine open subset of X have a common ring of fractions, denoted $k(X)$ and called the ring of **rational functions** on X.

Remark 1.1.3. By Proposition 1.22 of [Mil17] all algebraic groups are separated, thus a **group variety** is a geometrically reduced algebraic group. By Proposition 1.26 of [Mil17], for an algebraic group being geometrically reduced is equivalent to being smooth; also, by Corollary 8.39 of [Mil17], if the field is of characteristic zero, every algebraic group is smooth. Therefore in characteristic zero every algebraic group is a group variety.

A useful way to study algebraic groups is to regard them as functors.

Algebraic groups as functors. Denote with $\mathbf{Alg}_k$ the category of finitely generated k–algebras. An algebraic scheme X over k defines a functor:

$$\widetilde{X} : \mathbf{Alg}_k \longrightarrow \mathbf{Set}, \quad R \longmapsto X(R).$$

If X is affine, e.g. $X = \mathrm{Spec}(A)$ for a k–algebra A, then

$$X(R) = \mathrm{Hom}_{k\text{–algebra}}(A, R).$$

By Yoneda's lemma (cf. [Mac13, Ch. III, §2]) the functor that associates $\widetilde{X}$ to X is fully faithful, i.e. for every X and Y algebraic schemes over k there is an isomorphism between $\mathrm{Hom}(X, Y)$ and the set of natural transformations $\mathrm{Nat}(\widetilde{X}, \widetilde{Y})$. We say that a functor from k–algebras to sets is **representable** if it is isomorphic to $\widetilde{X}$ for an algebraic scheme X over k, and we call X the **representing object** of the functor. Observe that, again by Yoneda's lemma, the representing object X is uniquely determined up to unique isomorphism.

An algebraic group $(\mathcal{G}, m)$ is a functor from the category of k–algebras to the category of groups whose underlying functor to sets is representable by an algebraic scheme. Let us present examples of algebraic groups, which will appear recurrently throughout this thesis.

Example 1.1.4. The algebraic group SL_n defined above can be represented as the algebraic group sending a k–algebra A to the group $\mathrm{SL}_n(A)$ of $n \times n$ matrices with entries in A and determinant equal to 1.

Example 1.1.5. Let $\mathbb{G}_m$ be the functor from the category of k–algebras to the category of groups such that for every k–algebra A the group $\mathbb{G}_m(A)$ is the group $A^\times$ of the units of A. The functor $\mathbb{G}_m$ is representable by $\mathrm{Spec}(k[T, T^{-1}])$, since $A^\times \simeq \mathrm{Hom}_k(k[T, T^{-1}], A)$. Hence $\mathbb{G}_m$ is an affine algebraic group called the **multiplicative group**. We sometimes write $\mathbb{G}_{m,k}$ to specify the field over which it is defined.

Example 1.1.6. Another example of an affine algebraic group is given by the functor $\mathbb{G}_a$, which associates to a k–algebra A the group given by $(A, +)$. It is called the **additive group** and it is representable by $\mathrm{Spec}(k[T])$.

Example 1.1.7. Let $n \geqslant 1$ be an integer and let μ_n be the functor such that $\mu_n(A) = \{a \in A \mid a^n = 1\}$ for every k–algebra A. It is representable by $\mathrm{Spec}(k[t]/(t^n - 1))$ and so it is an (affine) algebraic group. It is not irreducible and, depending on the field k, we may have that it is not reduced (if $\mathrm{char}(k)$ divides n).

Example 1.1.8. The **general linear group** GL_n is the functor that associates to every k–algebra A the multiplicative group $\mathrm{GL}_n(A)$ of invertible $n \times n$ matrices with entries in A. It is representable by

$$\mathrm{Spec}(k[T_{11}, T_{12}, \ldots, T_{nn}, T]/(\det(T_{ij})T - 1))$$

and thus it is affine. The algebraic group SL_n is a subgroup of GL_n.

Definition 1.1.9. An algebraic group $\mathcal{G}$ is said to be **linear** if it admits an isomorphism onto a (closed) algebraic subgroup of GL_n for some n.

Every linear algebraic group is affine (since it is a subgroup of the affine group GL_n, c.f. [Mil17, p. 1.43]) and the converse also holds, see [Mil17, Corollary 4.10]. Thus the linear algebraic groups are precisely the affine algebraic groups.

Example 1.1.10. Some example of algebraic subgroups of GL_n, i.e. linear algebraic groups:

- $\mathbb{T}_n : A \longmapsto \{(a_{ij}) \mid a_{ij} = 0 \text{ for } i > j\}$, the upper triangular matrices;
- $\mathbb{U}_n : A \longmapsto \{(a_{ij}) \mid a_{ij} = 0 \text{ for } i > j, a_{ii} = 1\}$, called the **unipotent group**;
- $\mathbb{D}_n : A \longmapsto \{(a_{ij}) \mid a_{ij} = 0 \text{ for } i \neq j\}$, the diagonal matrices.

Let $\mathcal{G}$ be an algebraic group over k; then $\mathcal{O}(\mathcal{G})$, the ring of global sections, is a k–algebra and if $\mathcal{G}$ is affine we have $\mathcal{G} \simeq \mathrm{Spec}(\mathcal{O}(\mathcal{G}))$. If $\mathcal{O}(\mathcal{G}) = k$, i.e. $\mathcal{G}$ has no global section other than the constant ones, we say that $\mathcal{G}$ is **anti-affine**. In particular, projective varieties are anti-affine.

Example 1.1.11. The simplest anti-affine algebraic groups are **elliptic curves**: smooth cubic curves in $\mathbb{P}^2_k$. On an elliptic curve $\mathcal{E}$ the morphism m is given in the following way: fix a point $O \in \mathcal{E}(\overline{k})$ (assumed to exist); for $P, Q \in \mathcal{E}(\overline{k})$ draw the line through P and Q, it meets $\mathcal{E}$ in a third point $R \in \mathcal{E}(\overline{k})$. Let $P + Q$ be the third point of intersection of the line through O and R with $\mathcal{E}$, the morphism $m : \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$ is defined as $m(P, Q) = P + Q$. We will give more details about elliptic curves in Section 1.3.

A complete connected group variety $\mathcal{G}$ is anti-affine (see A.75 of [Mil17]) and such a group variety is called **abelian variety**. They are commutative and projective (c.f. 8.45 of [Mil17]), but they are not the only anti-affine algebraic groups. An abelian variety of dimension 1 is an elliptic curve. They are widely studied in mathematics, for some references, see the classic book [Mum74], the course notes [Mil08] and also [Sil09; Sil94] for the specific case of elliptic curves. We will see later in this section that every connected algebraic group is an extension of an affine algebraic group (in fact, a *linear* algebraic group) by an anti-affine algebraic group, i.e. an abelian variety. This is true also in general without the hypothesis of being connected (see Section 8.i of [Mil17]).

1.1.1 Extension and restrictions of scalars

Having defined algebraic groups as functors, it is clear what we mean when we say that we are taking the points of an algebraic group $\mathcal{G}$ in some field extension F of the base field k: we are associating to the k–algebra F the group $\mathcal{G}(F)$. If we think of affine groups, defined by some polynomial equations, this is just taking the solutions in F

of equations with coeffiecients in k. We can read these equations in some extension or subextension of k and get different equations: for example, an irreducible polynomial in k could split in its factors. We formalize this concept of *base change* with the following two definitions.

Definition 1.1.12. Let $\mathcal{G}$ be an algebraic group over k, with representing object $\mathcal{O}_{\mathcal{G}}$. For any field $F \supseteq k$ the **extension of scalars** of $\mathcal{G}$ is the algebraic group $\mathcal{G}_F$ over F with representing object $\mathcal{O}_{\mathcal{G}_F} = \mathcal{O}_{\mathcal{G}} \otimes_k F$.

For example, the algebraic group SL_2 over k is represented by $k[a,b,c,d]/(ad-bc-1)$ and its extension of scalars $(\mathrm{SL}_2)_F$ is represented by $F[a,b,c,d]/(ad-bc-1)$.

Given a finite field extension F/k and an algebraic group $\mathcal{G}$ defined over F, we want to define an algebraic group $\mathrm{R}_{F/k}\mathcal{G}$ defined over k that "behaves" like $\mathcal{G}$ over F. In particular, we want that $\mathrm{R}_{F/k}\mathcal{G}(k) \simeq \mathcal{G}(F)$. Thinking of the extension $\mathbb{C}/\mathbb{R}$, the idea is to regard a n–dimensional complex variety as a $2n$–dimensional real variety.

Definition 1.1.13. Let F/k be a finite field extension and let X be an algebraic scheme over F. The **Weil restriction** of X to k, if it exists, is an algebraic scheme $\mathrm{R}_{F/k}X$ such that $\mathrm{R}_{F/k}X(A) = X(F \otimes A)$ for all k–algebras A.

If X is quasi-projective, the Weil restriction of X always exists (c.f. [Wei82, p. 6]). For $\mathcal{G}$ an algebraic group, the Weil restriction of $\mathcal{G}$ is defined in the same way. We remark that all algebraic groups over a field are quasi-projective ([Mil17, B.38]), so that the Weil restriction always exists. Notice that on k–points we have:

$$\mathrm{R}_{F/k}\mathcal{G}(k) = \mathcal{G}(k \otimes F) \simeq \mathcal{G}(F).$$

Let $\mathcal{G}$ be an algebraic group over k. For A a k–algebra we have a group homomorphism $A \longrightarrow F \otimes A$ that sends a to $a \otimes 1$ and defines a group homomorphism $\mathcal{G}(A) \longrightarrow \mathcal{G}(F \otimes A) = \mathrm{R}_{F/k}\mathcal{G}_F(A)$. It is natural, so it arises from a homomorphism $i_{\mathcal{G}} : \mathcal{G} \longrightarrow \mathrm{R}_{F/k}\mathcal{G}_F$ of algebraic groups that has the following universal property.

> For any algebraic group $\mathcal{H}$ over F and homomorphism $\varphi : \mathcal{G} \longrightarrow \mathrm{R}_{F/k}\mathcal{H}$ there exists a unique homomorphism $\theta : \mathrm{R}_{F/k}\mathcal{G}_A \longrightarrow \mathcal{H}$ such that $\mathrm{R}_{F/k}(\theta) \circ i_{\mathcal{G}} = \varphi$.

This shows that the functor $\mathrm{R}_{F/k}$ is right adjoint to the functor "extension of scalar" $(-)_F$:

$$\mathrm{Hom}_k(\mathcal{G}, \mathrm{R}_{F/k}\mathcal{H}) \simeq \mathrm{Hom}_F(\mathcal{G}_F, \mathcal{H}).$$

We can describe explicitly the Weil restriction if the algebraic group $\mathcal{G}$ is affine. For example, suppose that

$$\mathcal{G} = \mathrm{Spec}\left(\frac{F[x_1, \dots, x_n]}{(f_1, \dots, f_r)}\right).$$

Choosing a k–basis $e_1, \dots e_d$ of F, where $d = [F : k]$, we can change variables, considering $x_i = \sum_{j=1}^{d} y_{ij} e_j$ for every $1 \leqslant i \leqslant n$. By substituting, we can rewrite each polynomial $f_h(x_1, \dots, x_n)$ as combination of d polynomials with coefficients in k in the variables y_{ij}: $f_h(x_1, \dots, x_n) = F_{h,1}e_1 + \cdots + F_{h,d}e_d$, with $F_{h,l} \in k[\{y_{ij}\}]$. We obtained that

$$\mathrm{R}_{F/k}\mathcal{G} = \mathrm{Spec}\left(\frac{k[\{y_{ij}\}]}{(\{F_{h,l}\})}\right).$$

Example 1.1.14. Let $k = \mathbb{R}$, $F = \mathbb{C}$ and consider the multiplicative group $\mathcal{G} = \mathbb{G}_m = \mathrm{Spec}\,(\mathbb{C}[x,y]/(xy-1))$ over $\mathbb{C}$. We choose the $\mathbb{R}$–basis $1, i$ of $\mathbb{C}$ and write $x = a + bi$, $y = c + di$. By substituting these relations in $xy - 1 = 0$ we get the equations

$$\begin{aligned} ac - bd &= 1, \\ ad + bc &= 0. \end{aligned}$$

Thus $\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m = \mathrm{Spec}\,(\mathbb{R}[a,b,c,d]/(ac - bd - 1, ad + bc))$. We will go back to this example later.

The description above can be seen in terms of the Galois action, as we are going to describe. This can be helpful in understanding what the Weil restriction is and its properties, in particular when the field extension is Galois.

Suppose that F/k is separable of degree d (this is not necessary for some of the properties that we are going to list, see Section 2.i of [Mil17]) and let k^s be the separable closure of k in $\overline{k}$. Let $\sigma_1, \ldots, \sigma_d$ be distinct embeddings of F into $\overline{k}$.

Given $\mathcal{G}$ an algebraic group over F, for each $1 \leqslant j \leqslant d$ we denote with $\mathcal{G}_{\sigma_j}$ the group obtained by extension of scalars by the k–homomorphism σ_j: it is the fibered product

$$\begin{array}{ccc} \mathcal{G}_{\sigma_j} & \longrightarrow & \mathcal{G} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(F) & \xrightarrow{\sigma_j} & \mathrm{Spec}(F). \end{array}$$

It is called the *base change of* $\mathcal{G}$ *along* σ_j.
In the affine case, we have that if $\mathcal{G} = \mathrm{Spec}\,(F[x_1, \ldots, x_n]/(f_1, \ldots, f_r))$, then $\mathcal{G}_{\sigma_j} = \mathrm{Spec}\,\big(F[x_1, \ldots, x_n]/(f_1^{\sigma_j}, \ldots, f_r^{\sigma_j})\big)$, where $f_k^{\sigma_j}$ is the polynomial whose coefficients are the conjugates of the coefficients of f_k by σ_j.

Proposition 1.1.15. *Let L be the Galois closure of F/k. Then we have*

$$(\mathrm{R}_{F/k}\mathcal{G})_L \simeq \prod_{j=1}^{d} \mathcal{G}_{\sigma_j}.$$

Proof. See Theorem 1.3.1 of [Wei82] and the paragraphs after that, or 2.61 of [Mil17]. □

We now list some properties of the Weil restriction that follow from the discussions above. For a more detailed proof, see for example [Vos98] or [Wei82].

1. If $k \subseteq E \subseteq F$, then $\mathrm{R}_{F/k}\mathcal{G} = \mathrm{R}_{E/k}(\mathrm{R}_{F/E}\mathcal{G})$.
2. Let L be an extension of k, then $L \otimes_k F = k_1 \times \ldots \times k_t$, for some positive integer t, where every k_i is a field. There is a canonical isomorphism
$$(\mathrm{R}_{F/k}\mathcal{G})_L \simeq \prod_{i=1}^{t} \mathrm{R}_{k_i/L}(\mathcal{G}_{k_i}).$$
3. We have $\dim(\mathrm{R}_{F/k}\mathcal{G}) = [F : k] \cdot \dim(\mathcal{G})$.

4. If $\mathcal{G}$ is affine, then $\mathrm{R}_{F/k}\mathcal{G}$ is also affine; if $\mathcal{G}$ is smooth, then $\mathrm{R}_{F/k}\mathcal{G}$ is also smooth.

5. The functor $\mathrm{R}_{F/k}$ is an exact functor from the category of algebraic F–groups to the category of algebraic k–groups.

Given an algebraic group $\mathcal{G}$ over F, the group $G_k = \mathrm{Gal}(k^s/k)$ acts on $\mathcal{G}_{k^s}$ and we have an induced action on $(\mathrm{R}_{F/k}\mathcal{G})_{k^s}$.

By the Primitive Element Theorem, $F = k(\alpha)$ for some $\alpha \in k^s$. If $\mu_\alpha(x)$ is the minimal polynomial of α over k, then we also have that $F \simeq k[x]/(\mu_\alpha(x))$. We denote with $\alpha_1 = \alpha, \ldots, \alpha_d$ the d distinct roots of $\mu_\alpha(x)$ in k^s. We can assume that $\sigma_j(\alpha) = \alpha_j$ for every $1 \leqslant j \leqslant d$, where $\sigma_1, \ldots, \sigma_d$ are the distinct embeddings $F \hookrightarrow \overline{k}$. We have that

$$k^s \otimes_k F \simeq k^s \otimes_k \frac{k[x]}{(\mu_\alpha(x))} \simeq \frac{k^s[x]}{(\mu_\alpha(x))}.$$

Since $\mu_\alpha(x)$ splits completely as $(x-\alpha_1)\cdots(x-\alpha_d)$ in k^s, using the Chinese Reminder Theorem, we get that

$$k^s \otimes_k F \simeq L_1 \oplus \ldots \oplus L_d, \quad \text{where} \quad L_i \simeq \frac{k^s[x]}{(\mu_{\alpha_i}(x))} \simeq k^s \quad \text{for } i = 1, \ldots, d.$$

This decomposition is equivalent to the decomposition of the unity with idempotent elements: for every $1 \leqslant j \leqslant d$ there exists $e_j \in L_j$ such that

$$e_1 + \ldots + e_d = 1, \quad e_j^2 = e_j, \quad e_j e_h = 0, \quad \text{for all } 1 \leqslant j, h \leqslant d.$$

The Galois group G_k acts transitively on $\{e_1, \ldots, e_d\}$ and we can write its action on $k^s \otimes_k F$ in this way: an element a of $k^s \otimes_k F$ can be written using the decomposition above as $a = a_1 e_1 + \ldots + a_d e_d$, so for all $\sigma \in G_k$

$$\sigma(a) = \sigma(a_1)\sigma(e_1) + \ldots + \sigma(a_d)\sigma(e_d). \tag{1.1}$$

The group $G_F = \mathrm{Gal}(k^s/F)$ fixes $\alpha = \alpha_1$, so we get that $k^s \otimes F$ is isomorphic to the induced module $k^s \otimes_{k[G_F]} k[G_k]$.

Remark 1.1.16. The previous arguments hold also taking the normal closure of F/k, instead of k^s and we get Proposition 1.1.15.

Therefore, the Galois action on $\mathrm{R}_{F/k}\mathcal{G}(k^s)$ can be described in the following way. For every $1 \leqslant j \leqslant d$ choose $\overline{\sigma}_j \in G_k$ a representative of σ_j, thus an element of G_k is of the form $\overline{\sigma_j}\tau$, for some j and $\tau \in G_F$. Every $x \in \mathrm{R}_{F/k}\mathcal{G}(k^s) \simeq \prod_{i=1}^d \mathcal{G}_{\sigma_j}(k^s)$ can be written as $x = (x_1, \ldots, x_d)$, therefore for each $1 \leqslant h \leqslant d$ we have that

$$\tau\overline{\sigma}_j \cdot x_h = \tau\sigma_j(x_l), \tag{1.2}$$

where $1 \leqslant l \leqslant d$ is such that $\sigma_j^{-1}\sigma_h = \sigma_l$. In other words, the G_k acts on the product $\prod_{i=1}^d \mathcal{G}_{\sigma_j}(k^s)$ by permuting the factors and then acting on each component (see also the proof of Theorem 1.3.3 of [Wei82]).

Example 1.1.17. We describe the Galois action on Example 1.1.14. We have $\mathcal{G} = \mathbb{G}_{m,\mathbb{C}}$ and by the results above

$$\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m(\mathbb{C}) = \left(\mathbb{G}_m \times (\mathbb{G}_m)_\varepsilon\right)(\mathbb{C}) \simeq \mathbb{C}^\times \times \mathbb{C}^\times,$$

where ε is the complex conjugation. On $x = (x_1, x_2) \in \mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m(\mathbb{C})$, the complex conjugation acts as:

$$\varepsilon \cdot (x_1, x_2) = (\varepsilon(x_2), \varepsilon(x_1)) = (\overline{x_2}, \overline{x_1}).$$

Since the $\mathbb{R}$–points of $\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m$ are the points of $\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m(\mathbb{C})$ fixed by $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, we deduce that

$$\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m(\mathbb{R}) = \{(x_1, \overline{x_1}) \mid x_1 \in \mathbb{C}^\times\} \simeq \mathbb{C}^\times.$$

We remark that this description can be easy generalized to any algebraic group over $\mathbb{C}$.

1.1.2 The m–torsion points

The set of the torsion points of an algebraic group will be of great importance in the next chapters. In Chapter 3 we will study the fields of definition (together with the classification of their Galois group over k) of the 7–torsion points of some families of elliptic curves. We will amply discuss torsion points in elliptic curves in Section 1.3, in particular we will show how we can explicitly compute their coordinates. Also in Chapter 2 we will deal with torsion points: we will need them to give the cohomological interpretation of the problem that we will study. In particular (but actually in both chapters), we will use the Galois representation of these points. That is why we are interested in the description given in this subsection, where we assume k to be a number field.

Given a commutative and connected algebraic group $\mathcal{G}$ over k we denote with O the image of $e : * \longrightarrow \mathcal{G}$ in $\mathcal{G}(k)$, which is the identity element of the group; sometimes it is also called the **origin** of $\mathcal{G}$. If m is a positive integer, let

$$\mathcal{G}[m] = \{P \in \mathcal{G}(\overline{k}) \mid mP = O\},$$

be the set of the m–torsion points of $\mathcal{G}(\overline{k})$. We are going to show that there exists an integer n, depending only on $\mathcal{G}$, such that $\mathcal{G}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^n$.

Theorem 1.1.18 (Barsotti-Chevalley Theorem)**.** *Every connected group variety $\mathcal{G}$ over a perfect field contains a unique normal subgroup R such that*

- *the group R is connected and linear;*
- *the quotient group $\mathcal{G}/R$ is an abelian variety.*

Proof. See [Mil17, Theorem 8.27] □

Working in characteristic zero, we saw in Remark 1.1.3 that every algebraic group is a group variety. Therefore we have an exact sequence of algebraic groups

$$0 \longrightarrow R \longrightarrow \mathcal{G} \longrightarrow \mathcal{A} \longrightarrow 0,$$

with $\mathcal{A} = \mathcal{G}/R$ is an abelian variety and R is a connected linear group.

We recall that a unipotent group is an algebraic group isomorphic to $\mathbb{U}_n$ (for some n), that we defined in Example 1.1.10.

Theorem 1.1.19. *A connected commutative linear group is a product of $\mathbb{G}_m^s$, for some s, and a unipotent group.*

Proof. See [Mil17, Corollary 16.15] or [Ser12, Chap. III, §2.7, Proposition 12]. □

Proposition 1.1.20. *In characteristic zero, every commutative unipotent group is isomorphic to $\mathbb{G}_a^r$ for some r.*

Proof. See [Mil17, Chap.14, Section d] or [Ser12, Chap. VII, §2.7]. □

Putting all together we get the following exact sequence

$$0 \longrightarrow \mathbb{G}_a^r \times \mathbb{G}_m^s \longrightarrow \mathcal{G} \longrightarrow \mathcal{A} \longrightarrow 0,$$

that leads, thanks to the divisibility of $\mathbb{G}_a^r \times \mathbb{G}_m^s$, to the exact sequence

$$0 \longrightarrow (\mathbb{G}_a^r \times \mathbb{G}_m^s)[m] \longrightarrow \mathcal{G}[m] \longrightarrow \mathcal{A}[m] \longrightarrow 0.$$

We notice that $(\mathbb{G}_a^r \times \mathbb{G}_m^s)[m] \simeq (\mathbb{Z}/m\mathbb{Z})^s$; in fact, $(\mathbb{G}_a^r \times \mathbb{G}_m^s)[m] \simeq (\mathbb{G}_m^s)[m]$, which is by definition $\mathbb{G}_m^s(\overline{k})[m]$, thus it is the product of s copies of the set of the m–th roots of unity in $\overline{k}$. If $\mathcal{A}$ has dimension t, the map

$$\begin{array}{rccc} [m]: & \mathcal{A} & \longrightarrow & \mathcal{A} \\ & P & \longmapsto & mP \end{array}$$

has degree m^{2t} and hence $\mathcal{A}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2t}$ (we will deal with the case of elliptic curves in Section 1.3, for the general case see p. 63 of [Mum74]). We get that $\mathcal{G}[m]$ is an abelian group with order m^{s+2t} and, since it has exponent m and can be generated by at most $s+2t$ elements, we have that $\mathcal{G}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{s+2t}$, as claimed.

Observe that, given an action of the absolute Galois group G_k on the points of $\mathcal{G}$, we have an induced action on the m–torsion points. By the isomorphism $\mathcal{G}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^n$, with $n = s+2t$, we have that G_k acts on these points as a subgroup of $\mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$:

$$G_k \longrightarrow \mathrm{Aut}(\mathcal{G}[m]) \simeq \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z}).$$

It is easy to see that the image of this representation is isomorphic to the Galois group $\mathrm{Gal}(k(\mathcal{G}[m])/k)$. Therefore, the Galois representation above will be a key tool, both for answering the local-global divisibility problem and for the study of the Galois groups of the division fields of elliptic curves.

1.1.3 Characters

Definition 1.1.21. Let $\mathcal{G}$ be an algebraic group over k. A **character** of $\mathcal{G}$ is a morphism of algebraic groups $\chi : \mathcal{G} \longrightarrow \mathbb{G}_m$.

Let χ and χ' be two characters of $\mathcal{G}$; the sum $\chi + \chi'$ is defined as

$$(\chi + \chi')(g) = \chi(g) \cdot \chi'(g), \quad g \in \mathcal{G}(A),$$

for every k–algebra A. Hence the set of the characters of $\mathcal{G}$ is an abelian group, that we denote $X(\mathcal{G})$ (in the literature it is also denoted as $\hat{\mathcal{G}}$).

Example 1.1.22. Let $\mathcal{G} = \mathbb{G}_m$. Each integer $n \in \mathbb{Z}$ defines a character of $\mathbb{G}_m$: for every k–algebra A we have

$$\begin{array}{ccc} \mathbb{G}_m(A) & \longrightarrow & \mathbb{G}_m(A) \\ t & \longmapsto & t^n. \end{array}$$

Thus we get an isomorphism $X(\mathbb{G}_m) \simeq \mathbb{Z}$ (cf. [Ono61, §1], this also follow from Theorem 1.1.30 and Example 1.1.27 below).

If $f : \mathcal{G} \longrightarrow \mathcal{H}$ is a homomorphism of algebraic group, then we have a homomorphism of abelian groups $\varphi : X(\mathcal{H}) \longrightarrow X(\mathcal{G})$. We also have that

$$X(\mathcal{G} \times \mathcal{H}) = X(\mathcal{G}) \times X(\mathcal{H}).$$

Remark 1.1.23. One can think of $X(-) = \mathrm{Hom}_{\mathrm{AlgGp}_k}(-, \mathbb{G}_m)$ (homomorphisms of algebraic groups defined over k) as a contravariant functor from the category of algebraic k–groups to the category of abelian groups.

In the literature, $X(\mathcal{G})$ is also called the group of the *rational characters*. In fact, in our definition, characters are defined over k, while, for example in [PR93], they are defined over $\overline{k}$. Given an extension L/k, one can define the group of L–rational characters as

$$X_L^*(\mathcal{G}) = \mathrm{Hom}(\mathcal{G}_L, \mathbb{G}_{m,L}),$$

which in our notation is equal to $X(\mathcal{G}_L)$. So our $X(\mathcal{G})$ is equal to $X_k^*(\mathcal{G})$, and we denote with $X^*(\mathcal{G})$ the group $X(\mathcal{G}_{k^s})$ of characters defined over the separable closure k^s.

The group $\Gamma = \mathrm{Gal}(k^s/k)$ (endowed with the Krull topology) acts on $X^*(\mathcal{G})$ under the usual action

$$\sigma(\chi)(g) = \sigma(\chi(\sigma^{-1}g)), \quad \sigma \in \Gamma,\ \chi \in X^*(\mathcal{G}),\ g \in \mathcal{G}.$$

The action is continuous since every homomorphism $\mathcal{G}_{k^s} \longrightarrow \mathbb{G}_m$ is defined over a finite extension of k, thus $X^*(\mathcal{G})$ is a Γ–module, so also a $\mathbb{Z}[\Gamma]$–module. We observe that

$$X^*(\mathcal{G})^\Gamma = X(\mathcal{G}).$$

Example 1.1.24. Let L/k be a Galois extension and let $\mathcal{G} = \mathbb{G}_{m,k}$. Then $\mathcal{G}_L = \mathbb{G}_{m,L}$, so $X(\mathcal{G}_L) \simeq \mathbb{Z}$. To be more precise:

$$\begin{array}{ccccccc} X(\mathcal{G}_L) \simeq & \mathrm{Hom}_{\mathrm{Alg}_L}(L[t,t^{-1}], k[t,t^{-1}] \otimes L) \simeq & (k[t,t^{-1}] \otimes L)^\times \simeq & (L[t,t^{-1}])^\times \simeq & \mathbb{Z} \\ & (x \mapsto x^n \otimes 1) & x^n \otimes 1 & x^n & n \end{array}$$

The action of $\mathrm{Gal}(L/k)$ is defined in terms of the action on the L–part of the tensor $x^n \otimes 1$, thus it is trivial and $X(\mathcal{G}_L)$ is a trivial $\mathrm{Gal}(L/k)$–module. We conclude that $X^*(\mathbb{G}_m)$ is a trivial Γ–module.

The functor $X^*(-)$ will be very important when dealing with algebraic tori, which is the main object of Chapter 2. In particular, we will see that $X^*(-)$ will give us a correspondance between algebraic tori and finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ (see Section 1.2). To do so, we need to introduce the following definitions.

Definition 1.1.25. Let M be a finitely generated commutative group. We define the functor $D(M)$ as the functor that associates to every k–algebra A the group $D(M)(A) = \mathrm{Hom}(M, A^\times)$.

For every M as in the definition, the functor $D(M)(-)$ is representable by the algebraic group $\mathrm{Spec}(k[M])$, where $k[M]$ is the group algebra of M. Thus $D(M)$ is an affine algebraic group.

Definition 1.1.26. We say that an algebraic group is **diagonalizable** if it is isomorphic to $D(M)$ for some finitely generated commutative group M.

Example 1.1.27. The algebraic k–group $\mathbb{G}_m$ is a diagonalizable group with $M = \mathbb{Z}$: indeed, for every k–algebra A we have $D(\mathbb{Z})(A) = \mathrm{Hom}(\mathbb{Z}, A^\times) \simeq A^\times = \mathbb{G}_m(A)$.

Example 1.1.28. Let $M = \mathbb{Z}/m\mathbb{Z}$, for some positive integer m. The group algebra $k[M]$ is isomorphic to $k[t]/(t^m - 1)$, thus $\mu_m = D(\mathbb{Z}/m\mathbb{Z})$ (c.f. Example 1.1.7) and it is a diagonalizable group.

Remark 1.1.29. There are different definitions of diagonalizable groups. For instance, in [Mil17, Definition 12.7] or [Wat12], a diagonalizable group $\mathcal{G}$ is defined using the *group-like elements* of the Hopf algebra $\mathcal{O}(\mathcal{G})$; while for example in [Spr94] it is defined as a group isomorphic to a closed subgroup of $\mathbb{D}_n$, for some n (where $\mathbb{D}_n$ is the group of diagonal matrices, c.f. Example 1.1.10). These definitions are equivalent, by [Mil17, Theorem 12.8] or by [Mil17, Theorem 12.12], observing that $\mathbb{D}_n$ is isomorphic to n copies of $\mathbb{G}_m$.

Notice that the definition implies that diagonalizable groups are finite products of copies of $\mathbb{G}_m$ and various μ_n. The functors introduced in this section are closely related, as the following theorem shows.

Theorem 1.1.30. *The functor $M \longmapsto D(M)$ is a contravariant equivalence from the category of finitely generated commutative groups to the category of diagonalizable algebraic groups, with quasi-inverse $\mathcal{G} \longmapsto X^*(\mathcal{G})$. Furthermore the functors $D(-)$ and $X^*(-)$ are exact.*

Proof. See [Mil17, Theorem 12.9]. □

1.2 Algebraic tori

In this section we introduce the definitions and the main tools concerning algebraic tori that we will use in Chapter 2. Most of them are well known and the main references for this section are [Ono61; Mil17; Vos98].

Definition 1.2.1. An algebraic group $\mathcal{G}$ over k is a **k–torus** (of finite rank) if it becomes isomorphic to a product of r copies of $\mathbb{G}_m$ over the separable closure k^s of k for some positive integer r. Such r is called the **rank** or **dimension** of the torus.

Example 1.2.2. Some algebraic tori that we already encountered:

- clearly $\mathbb{G}^r_{m,k}$ is an algebraic torus of rank r over k;
- the algebraic group $\mathbb{D}_n$ of the diagonal matrices is k–torus of rank n;
- the Weil restriction $\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m$ is an algebraic torus of rank 2, by example 1.1.17 (see also Proposition 1.2.12 below).

For an algebraic torus T of rank k, by the definition we have $T_{k^s} \simeq \mathbb{G}^r_m$.

Definition 1.2.3. Let T be an algebraic torus of rank r over k. Let F/k be a field extension. We say that T is **split over** F if the extension of scalars T_F is isomorphic to $\mathbb{G}^r_m$. If T is isomoprhic to $\mathbb{G}^r_m$ over k we say that T is **split**, otherwise we say that T is **non-split**.

The split tori are the smooth connected diagonalizable algebraic groups, since μ_n is not connected (see e.g. Example 1.6 of [Mil17]) and, if $n = \mathrm{char}(k) > 0$, it is not smooth too (in this case, it is not reduced and one can use Proposition 1.28 of [Mil17]). Moreover, under the equivalence of categories described in Theorem 1.1.30, the split tori correspond to free $\mathbb{Z}$–modules of finite rank.

1.2.1 Groups of multiplicative type

Definition 1.2.4. An algebraic group over k is of **multiplicative type** if it becomes diagonalizable over some field containing k.

By [Mil17, Theorem 12.18] a group is of multiplicative type if and only if it becomes diagonalizable over the separable closure k^s of k. Therefore $\mathcal{G}$ is of multiplicative type if there is a finitely generated abelian group M such that

$$\mathcal{G}_{k^s} \simeq D(M)_{k^s} = \mathrm{Spec}(k^s[M]).$$

By the equivalence of categories of Theorem 1.1.30, the group M is the group of characters $X^*(\mathcal{G})$.

So, if $\mathcal{G}$ is of multiplicative type, then $X^*(\mathcal{G})$ is finitely generated. Every homomorphism $\mathcal{G}_{k^s} \longrightarrow \mathbb{G}_m$ is defined over some finite extension of k, therefore there exists a finite extension L of k over which all the elements of $X^*(\mathcal{G})$ are defined, i.e. $X^*(\mathcal{G}) = X(\mathcal{G}_L)$. In this case we have $\mathcal{G}_L = D(X^*(\mathcal{G}))_L$ ($\mathcal{G}$ becomes diagonalizable over L) and the field L is called **a splitting field** of $\mathcal{G}$.

Recall that $X^*(\mathcal{G})$ is a continuous $\Gamma = \mathrm{Gal}(k^s/k)$–module and that $X^*(\mathcal{G})^\Gamma = X(\mathcal{G})$.

Theorem 1.2.5. *The functor $X^*(-)$ is a contravariant equivalence from the category of groups of multiplicative type over k to the category of finitely generated abelian groups equipped with a continuous Γ–action, with quasi inverse $D(-)$. Moreover, under this equivalence, short exact sequences correspond to short exact sequences.*

Proof. Given M a finitely generated abelian group with a continuous Γ–action, we can construct $D(M_0)$ the diagonalizable group over k^s attached to M: in other words, $D(M_0) = \mathrm{Spec}(k^s[M])$. The action of Γ on $k^s[M]$ is given by the action on M, induced by a representation $h : \Gamma \longrightarrow \mathrm{Aut}(M)$ and the natural Galois action on k^s. Let $\mathcal{G} = \mathrm{Spec}(k^s[M]^\Gamma)$, it is a k–group that becomes isomorphic to $D(M_0)$ over k^s, so it is of multiplicative type.
This, together with Theorem 1.1.30 and the arguments above, implies the claims. □

Remark 1.2.6. Algebraic tori are group of multiplicative type such that their group of characters is torsion free. Moreover, from the theorem above we have that split tori correspond to free abelian groups of finite rank with trival Γ–action. We also remark that the equivalence preserves the rank: a torus of rank r corresponds to a free abelian group of rank r.

Given $\mathcal{G}$ an algebraic group of multiplicative type over k we have that $\mathcal{G} = D(X^*(\mathcal{G}))$. So for every extension $k \subseteq F \subset k^s$, we have

$$\mathcal{G}(F) = \mathrm{Hom}(X^*(\mathcal{G}), (k^s)^\times)^{\Gamma_F},$$

i.e. the homomorphism from $X^*(\mathcal{G})$ to $(k^s)^\times$ that commutes with the action of Γ_F and we recall that Γ_F is the subgroup of Γ of elements fixing F, that is $\mathrm{Gal}(k^s/F)$.

Example 1.2.7. Let $k = \mathbb{R}$, so that $\Gamma = \mathrm{Gal}(\mathbb{C}, \mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$, and let T be a $\mathbb{R}$–torus of rank 1. We have that $X^*(T) = \mathbb{Z}$ and two possible actions of Γ (hence two possible $\mathbb{R}$–tori of rank 1):

- the trivial action: in this case T is split, so $T = \mathbb{G}_m$;

- the nontrivial element ε of Γ acts on $\mathbb{Z}$ as $n \longmapsto -n$. Then $X(T) = X^*(T)^\Gamma = 0$ and $T(\mathbb{R})$ consists of the elements $z \in \mathbb{C}^\times$ fixed under the action: $\varepsilon z = \overline{z}^{-1}$. Thus

$$T(\mathbb{R}) = \{z \in \mathbb{C}^\times \mid z\overline{z} = 1\},$$

  which is not split.

Remark 1.2.8. In general, an algebraic torus with $X(T) = 0$, as in the example above, is called **anisotropic**, otherwise is called **isotropic**. It follows from the definition that anisotropic tori are non-split.

Example 1.2.9. We saw that the Weil restriction $T = \mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m$ is an $\mathbb{R}$–torus of rank two, so $X^*(T)$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. The complex conjugation acts on $X^*(T)$ by $(n_1, n_2) \longmapsto (-n_2, n_1)$, thus

$$X(T) = X^*(T)^\Gamma = \{(n_1, -n_1) \mid n_1 \in \mathbb{Z}\} \simeq \mathbb{Z}.$$

Therefore the $\mathbb{R}$–rational points are

$$\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m(\mathbb{R}) = \{(x_1, \overline{x_1}) \mid x_1 \in \mathbb{C}^\times\},$$

as seen in Example 1.1.17.

Theorem 1.2.10. *Let T be an algebraic k–torus. There exists a unique minimal finite Galois extension L over k such that T is split over L.*

Proof. We have seen that T is split over a (separable) extension F if and only if all the characters of T are defined over F, so if and only if $X^*(T) = X(T_F)$. Observe that $X(T_F) = X^*(T)^{\Gamma_F}$, where $\Gamma_F = \mathrm{Gal}(k^s/F)$, so T splits over F if and only if the open subgroup Γ_F of Γ acts trivially on $X^*(T)$. The conclusion follows by observing that the kernel of the action is an open normal subgroup of Γ (and then using Galois correspondence). □

The field L in Theorem 1.2.10 is called the **minimal** splitting field of T. It is the minimal field where the isomorphism between T and $\mathbb{G}_m^r$ is defined.

Given a group of multiplicative type G over k defined by a representation $h : \Gamma \longrightarrow \mathrm{Aut}(X^*(\mathcal{G}))$, as in the proof of Theorem 1.2.5, we have that $h(\Gamma) \subseteq \mathrm{Aut}(X^*(\mathcal{G}))$ is a finite group. In fact, h is continuous, Γ is compact and $\mathrm{Aut}(M)$ is discrete. It is called the **splitting group** of $\mathcal{G}$. Therefore, as we saw for tori in Theorem 1.2.10, the field fixed by $\ker(h)$, i.e. $L = (k^s)^{\ker(h)}$, is a finite Galois extension of k and is the intersection of all splitting fields of $\mathcal{G}$ contained in k^s. Moreover, we have $\mathrm{Gal}(L/k) \simeq \Gamma/\ker(h)$ and the degree of L/k is equal to the order of the splitting group of $\mathcal{G}$. We notice that given an algebraic k–torus T with (minimal) splitting field L, if $G = \mathrm{Gal}(L/k)$ then $X^*(T)$ becomes a G–module in the usual way.
Conversely, given a finite Galois extension L/k with Galois group G, we can define an associated algebraic torus in the following way. Let M be a torsion-free G–module of finite rank. Then the functor that associated to every k–algebra A the group of G–equivariant homomorphisms $\mathrm{Hom}_G(M, A_L^\times)$, where $A_L = A \otimes_k L$, is an algebraic torus defined over k and split over L.

Therefore we have shown the following (see also Proposition 1.2.3 and Proposition 1.2.4 of [Ono61]).

Theorem 1.2.11. *Let L/k be a finite Galois extension with Galois group G. There is a contravariant equivalence of categories between algebraic k–tori split over L and finitely generated free G–modules.*

In conclusion, an algebraic torus T is uniquely determined by the Γ–module $X^*(T)$, i.e. by the integral representation

$$\rho : \Gamma \longrightarrow \mathrm{Aut}(X^*(T)) \simeq \mathrm{GL}_r(\mathbb{Z}),$$

where r is the rank of T. Moreover, $\ker(\rho) = \Gamma_L$ and $\Delta = \rho(\Gamma) \simeq \mathrm{Gal}(L/k)$, where L is the minimal splitting field of T. We point out that the splitting group Δ is defined only up to conjugation, since $\mathrm{Aut}(X^*(T)) \simeq \mathrm{GL}_r(\mathbb{Z})$ depends on the choice of a basis.

1.2.2 The norm-one torus

Given a finite separable extension F/k of degree d, we want to define an associated algebraic torus, which will result as a subgroup of the Weil restriction of the one-dimensional split torus over F, that is $\mathrm{R}_{F/k}\mathbb{G}_m$. Using the properties of the Weil restriction that we showed in Section 1.1.1, it is easy to prove the following.

Proposition 1.2.12. *Let L be the normal closure of F/k. Then $\mathrm{R}_{F/k}\mathbb{G}_m$ is a k–torus of rank d with minimal splitting field L.*

Remark 1.2.13. Clearly, if T is an algebraic torus over F (not necessarily split) of rank r, then $\mathrm{R}_{F/k}(T)$ is an algebraic torus defined over k of rank dr.

As seen in the previous section, an algebraic torus is uniquely determined by its character module, so let us decribe $X^*(\mathrm{R}_{F/k}\mathbb{G}_m)$. To ease the notation, let $T = \mathrm{R}_{F/k}\mathbb{G}_m$. Recall that $\mathrm{R}_{F/k}\mathbb{G}_m(k^s) = (k^s \otimes_k F)^\times$ and we saw that $k^s \otimes_k F$ is isomorphic to the induced $k[\Gamma]$–module $k^s \otimes_{k[\Gamma_F]} k[\Gamma]$, where Γ acts by permutation. Therefore the Γ–module $X^*(T)$ is of the form $\mathbb{Z} \otimes_{\Gamma_F} \mathbb{Z}[\Gamma] \simeq \mathbb{Z}[\Gamma/\Gamma_F]$, i.e. the induced module $\mathrm{Ind}_{\Gamma_F}^{\Gamma} X^*(\mathbb{G}_m)$ (see Example 18 of [Vos98, Ch. 1, §3]). In particular, the action of Γ on $X^*(T) \simeq \mathbb{Z}^d$ is by permuting the factors. Since the Γ–action is not trivial, it follows that the Weil restriction $\mathrm{R}_{F/k}\mathbb{G}_m$ is a non-split torus (and the splitting field is L, the normal closure of F/k).

The norm map. Given the one-dimensional algebraic tori $\mathbb{G}_{m,F}$ and $\mathbb{G}_{m,k}$, we have that $\mathrm{R}_{F/k}\mathbb{G}_{m,F}(k) = F^\times$ and $\mathbb{G}_{m,k}(k) = k^\times$, so there is the usual norm map $N_{F/k} : F^\times \longrightarrow k^\times$. We can extend $N_{F/k}$ to a "generalized" norm map which is a morphism of algebraic k–groups. Let us show how it is constructed. Let A be a k–algebra and let $A_F = F \otimes_k A$ be its extension of scalars, which has the structure of an A–module. For every $x \in A_F$, let $\lambda_x : A_F \longrightarrow A_F$ be the (left) multiplication by x. We have the left regular representation

$$\begin{array}{rccc} \lambda : & A_F & \longrightarrow & \mathrm{End}_k(A_F) \\ & x & \longmapsto & \lambda_x. \end{array}$$

Since λ_x is also A–linear for every $x \in A_F$, we can regard λ as $A_F \longrightarrow \mathrm{End}_A(A_F)$. On the units we get:

$$\begin{array}{rccc} \lambda : & A_F^\times & \longrightarrow & \mathrm{GL}_A(A_F) \\ & x & \longmapsto & \lambda_x, \end{array}$$

and therefore we can define the generalized norm map as

$$\begin{array}{rccc} N_{A_F} = \det \circ \lambda : & A_F^\times & \longrightarrow & A^\times \\ & x & \longmapsto & \det(\lambda_x). \end{array}$$

We want to describe the image of this norm map in the case of a Galois extension. Let L/k be a Galois extension of degree d and fix an embedding $\iota : k \hookrightarrow k^s$. Let A be a k^s–algebra. We have the following diagram.

$$\begin{array}{ccc} L^\times & \xrightarrow{N_{L/k}} & k^\times \\ {\scriptstyle \iota\otimes 1}\downarrow & & \downarrow{\scriptstyle \iota} \\ (A^\times)^d & \xrightarrow[N_A]{} & A^\times \end{array}$$

The vertical map $\iota \otimes 1$ can be described as

$$L^\times \longrightarrow (k^{s\times})^d \hookrightarrow (A^\times)^d \qquad l \longmapsto (\sigma_1(l), \ldots, \sigma_d(l)),$$

where $\sigma_1, \ldots, \sigma_d$ are the elements of $\mathrm{Gal}(L/k)$. The left regular representation of $(A^\times)^d$ is

$$(A^\times)^d \longrightarrow \mathrm{GL}_d(A^\times), \quad (a_1, \ldots, a_d) \longmapsto \mathrm{diag}(a_1, \ldots, a_d),$$

therefore the norm map is given by

$$N_A : (A^\times)^d \longrightarrow A^\times, \quad (a_1, \ldots, a_d) \longmapsto \prod_{i=1}^{d} a_i.$$

Taking $A = k^s$, by the above diagram we have $N_{k^s}(\sigma_1(l), \ldots, \sigma_d(l)) = \prod_{i=1}^d \sigma_i(l) = N_{L/k}(l)$. In particular, taking L to be the normal closure of F/k, this show that the map N is an extension of the usual norm map.

From the definition, it follows that for every k–algebra A, the norm map N_A is a group homomorphism. To conclude that the defined N is a morphism of algebraic groups, we have to check that it is a natural transformation, i.e. for every $f : A \longrightarrow B$ morphism of k–algebras the following diagram commutes

$$\begin{array}{ccc} \mathrm{R}_{L/k}\mathbb{G}_m(A) & \xrightarrow{N_A} & \mathbb{G}_m(A) \\ {\scriptstyle \mathrm{R}_{L/k}\mathbb{G}_m(f)}\downarrow & & \downarrow{\scriptstyle \mathbb{G}_m(f)} \\ \mathrm{R}_{L/k}\mathbb{G}_m(B) & \xrightarrow[N_B]{} & \mathbb{G}_m(B). \end{array}$$

This is equivalent to check that the following diagram commutes:

$$\begin{array}{ccc} A_L^\times & \xrightarrow{N_A} & A^\times \\ {\scriptstyle (f\otimes 1)|_{A_L^\times}}\downarrow & & \downarrow{\scriptstyle f|_{A^\times}} \\ B_L^\times & \xrightarrow[N_B]{} & B^\times. \end{array}$$

To see that, we first write, for every $x \in A_L$, the image $N_A(x)$ in terms of an A–basis of $A_L = A \otimes_k L$. If $\{\alpha_1, \ldots, \alpha_d\}$ is a k–basis for L, an A–basis for A_L is given by

$\{1_A \otimes \alpha_i \mid i = 1, \dots d\}$. For $1 \leqslant i, j, h \leqslant d$ we define $\beta_{i,j}^h$ to be the elements in k such that $\alpha_i \alpha_i = \sum_{h=1}^d \beta_{i,j}^h \alpha_h$. Thus, if we write $x = \sum_{i=1}^d x_i \otimes \alpha_i$, we have that λ_x acts on the A–basis of A_L as follows: for every $1 \leqslant j \leqslant d$

$$\begin{aligned}\lambda_x (1_A \otimes \alpha_j) &= \big(\sum_{i=1}^d x_i \otimes \alpha_i\big)(1 \otimes \alpha_j) = \sum_{i=1}^d x_i \otimes \alpha_i \alpha_j \\ &= \sum_{i=1}^d x_i \otimes \sum_{h=1}^d \beta_{i,j}^h \alpha_h = \sum_{h=1}^d \big(\sum_{i=1}^d x_i \beta_{i,j}^h\big) \otimes \alpha_h.\end{aligned}$$

Therefore the multiplication by x is represented by the matrix $\big(\sum_{i=1}^d x_i \beta_{i,j}^h\big)_{j,h}$ and so $N_A(x) = \det\Big(\big(\sum_{i=1}^d x_i \beta_{i,j}^h\big)_{j,h}\Big)$. Since $(f \otimes 1)(x) = \sum_{i=1}^d f(x_1) \otimes \alpha_i$, we have that (with the same arguments on B_L)

$$N_B((f \otimes 1)(x)) = \det\Big(\big(\sum_{i=1}^d f(x_i) \beta_{i,j}^h\big)_{j,h}\Big).$$

On the other hand, since f is a homomorphism of k–algebras,

$$f(N_A(x)) = f\Big(\det\Big(\big(\sum_{i=1}^d x_i \beta_{i,j}^h\big)_{j,h}\Big)\Big) = \det\Big(\big(\sum_{i=1}^d f(x_i) \beta_{i,j}^h\big)_{j,h}\Big) = N_B((f \otimes 1)(x)),$$

and this proves the naturality of the norm map.

Proposition 1.2.14. *Let F/k be a finite separable extension of degree $d > 1$. Let $N : \mathrm{R}_{F/k}\mathbb{G}_{m,F} \longrightarrow \mathbb{G}_{m,k}$ be the (generalized) norm map and let T be the kernel of N. Then T is a torus of rank $d - 1$.*

Proof. Since T is defined as the kernel of a homomorphism of algebraic groups, it is a (normal) algebraic subgroup of $\mathrm{R}_{F/k}\mathbb{G}_{m,F}$. We need to show that T_{k^s} is isomorphic to $\mathbb{G}_m^{d-1}$. This is equivalent to show that for every k^s–algebra A

$$T_{k^s}(A) \simeq \mathbb{G}_m^{d-1}(A) = (A^\times)^{d-1}.$$

Let A be k^s–algebra. By definition, $T(A) = \ker(N_A)$, where (as showed above)

$$N_A : (A^\times)^d \longrightarrow A^\times, \quad (a_1, \dots, a_d) \longmapsto \prod_{i=1}^d a_i.$$

Therefore we can write

$$T(A) = \{(a_1, \dots, a_d) \in (A^\times)^d \mid a_1 \cdots a_d = 1\} \simeq \{(a_1, \dots, a_{d-1}) \in (A^\times)^{d-1}\} \simeq (A^\times)^{d-1}.$$

□

Definition 1.2.15. The algebraic torus defined in Proposition 1.2.14 is called the **norm-one torus** and in literature is often denoted as $\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m$.

Here are examples of norm-one tori for some field extensions.

Example 1.2.16. Let $k = \mathbb{R}$, $F = \mathbb{C}$ and let T be the norm-one torus. On $\mathbb{C}$–points we have $\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{m,\mathbb{C}}(\mathbb{C}) = (\mathbb{C}^\times)^2$ and the norm map is just $N_{\mathbb{C}} : (\mathbb{C}^\times)^2 \longrightarrow \mathbb{C}^\times$, $(z, w) \longmapsto zw$, thus

$$T(\mathbb{C}) = \ker N_{\mathbb{C}} = \{(z, z^{-1}) \mid z \in \mathbb{C}\} \simeq \mathbb{C}^\times.$$

On $\mathbb{R}$ we have: $\mathrm{R}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{m,\mathbb{C}}(\mathbb{R}) = (\mathbb{R}\otimes_{\mathbb{R}}\mathbb{C})^\times \simeq \mathbb{C}^\times$ and the norm map is $N_{\mathbb{R}} : \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$, $z \longmapsto |z|$. Therefore

$$T(\mathbb{R}) = \ker N_{\mathbb{R}} = \{z \in \mathbb{C}^\times \mid |z| = 1\},$$

which is the torus found in Example 1.2.7.

Example 1.2.17. Let us generalize the above example. Let k be a perfect field and $F = k(\sqrt{d})$, with d not a square in k. A k–basis for F is given by $\{1, \sqrt{d}\}$ and so the left regular representation of $F^\times$ in terms of this basis is given by

$$\lambda_1(a + b\sqrt{d}) = a + b\sqrt{d} = \begin{pmatrix} a \\ b \end{pmatrix},$$

$$\lambda_{\sqrt{d}}(a + b\sqrt{d}) = a\sqrt{d} + bd = \begin{pmatrix} bd \\ a \end{pmatrix};$$

therefore

$$\begin{array}{rccc} \lambda : & L^\times & \longrightarrow & \mathrm{GL}_2(k) \\ & a + b\sqrt{d} & \longmapsto & \begin{pmatrix} a & bd \\ b & a \end{pmatrix}. \end{array}$$

Thus, on k–points we have $N_k : F^\times \longrightarrow k^\times$, $a + b\sqrt{d} \longmapsto a^2 - db^2$ and the norm-one torus on these points is

$$T(k) = \ker N_k = \{(a, b) \in k \mid a^2 - db^2 = 1\}.$$

If L is the normal closure of a finite separable extension F/k, then $\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m$ splits over L, since $\mathrm{R}_{F/k}\mathbb{G}_m$ is split over L. It is not immediate from the definition if the norm-one torus associated to F/k is split.

Proposition 1.2.18. *Let F/k be finite separable extension of degree $d > 1$. Then the associated norm-one torus $\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m$ is a non-split k–torus.*

Proof. We have the following exact sequence of algebraic k–groups:

$$1 \longrightarrow \mathrm{R}^{(1)}_{F/k}\mathbb{G}_m \longrightarrow \mathrm{R}_{F/k}\mathbb{G}_m \xrightarrow{N} \mathbb{G}_m.$$

Since $X^*(-)$ is an exact (contravariant) functor, we get the following exact sequence of abelian groups:

$$X^*(\mathbb{G}_m) \xrightarrow{N^*} X^*(\mathrm{R}_{F/k}\mathbb{G}_m) \longrightarrow X^*(\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m) \longrightarrow 1.$$

So $X^*(\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m) \simeq \mathbb{Z}^{d-1}$ is isomorphic to the cokernel of the map N^*. Recall that, as $\mathbb{Z}[\Gamma]$–modules, $X^*(\mathrm{R}_{F/k}\mathbb{G}_m)$ is isomorphic to $\mathbb{Z}[\Gamma/\Gamma_F]$: if $\sigma_1, \ldots, \sigma_d$ are representatives of Γ/Γ_F (i.e. they are d distinct embeddings of F in k^s), then $X^*(\mathrm{R}_{F/k}\mathbb{G}_m) \simeq \mathbb{Z}\sigma_1 +$

$\ldots + \mathbb{Z}\sigma_d$ and Γ acts by permuting the factors $\mathbb{Z}\sigma_i$.
The norm map $N : \mathrm{R}_{F/k}\mathbb{G}_m \longrightarrow \mathbb{G}_m$ induces on the character modules the map

$$\begin{array}{rccc} N^* : & \mathbb{Z} & \longrightarrow & \mathbb{Z}[\Gamma/\Gamma_F] \\ & m & \longmapsto & \sum_{i=1}^{d} m\sigma_i. \end{array}$$

Therefore, if we let $\gamma = \sum \sigma_i$, we have that $\mathrm{Im}(N^*) = \mathbb{Z}\gamma$ and so $X^*(\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m) \simeq \mathbb{Z}[\Gamma/\Gamma_F]/\mathbb{Z}\gamma$. The module $\mathbb{Z}\gamma$ is the submodule of $\mathbb{Z}[\Gamma/\Gamma_F]$ fixed by the action of Γ. Thus we conclude that, since $d > 1$, the action of Γ on $X^*(\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m)$ is not trivial. So the k–torus $\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m$ is non-split (it is actually anisotropic).

□

From the proof one also gets that the minimal splitting field of $\mathrm{R}^{(1)}_{F/k}\mathbb{G}_m$ is the normal closure L of F/k and that $\mathrm{Gal}(L/k)$ acts by left multiplication.

Remark 1.2.19. The proof can be done using the same arguments, by taking the groups $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/F)$ instead of Γ and Γ_F, respectively (c.f. p. 54 of [PR93]). In fact $X^*(\mathrm{R}_{F/k}\mathbb{G}_m)$ is also a $\mathbb{Z}[G]$–module. In this setting, the group obtained as the cokernel of the map N^* is called the *Chevallay module of* G/H.

1.3 Elliptic curves

In this section we present some well-know definitions and results about elliptic curves. The main reference is [Sil09].

Elliptic curves are non-singular curves of genus 1 with a specific base point. Thanks to the Riemann-Roch Theorem, every such curve can be written as the locus in $\mathbb{P}^2_k$ of a cubic equation with only one point (the base point) on the line at ∞ (as defined in Example 1.1.11), i.e. as an equation of the form (using non-homogeneous coordinates for ease of notation)

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.3}$$

with the basepoint $O = [0, 1, 0]$, called the **Weierstrass equation** of the curve. If $a_1, \ldots, a_6 \in k$, we say that $\mathcal{E}$ is **defined over** k.

If the characteristic of the field is different from 2 and 3, we can change coordinates to get a shorter equation:

$$\mathcal{E} : y^2 = x^3 + Ax + B\,. \tag{1.4}$$

This equation has associated quantities $\Delta(\mathcal{E}) := -16(4A^3+27B^2)$ and $j(\mathcal{E}) := \dfrac{1728(4A^3)}{\Delta(\mathcal{E})}$ called, respectively, the **discriminant** of the Weierstrass equation and the j–**inviariant** of $\mathcal{E}$. Since we will deal with number fields, from now on we will define elliptic curves by their short Weierstrass equation.

We have seen in Example 1.1.11 that we can define an operation on the points of $\mathcal{E}$, the sum of two points, that make $\mathcal{E}$ an abelian group with identity element O.

Isogenies. Given two elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$, an **isogeny** from $\mathcal{E}_1$ to $\mathcal{E}_2$ is a morphism of curves $\phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ such that $\phi(O_1) = O_2$. By [Sil09, Ch. II, Theorem 2.3], an isogeny is either constant or surjective. Thus either $\phi(\mathcal{E}_1) = \{O_2\}$ (so that ϕ is the map

$[0]P = O$) or $\phi(\mathcal{E}_1) = \mathcal{E}_2$.
The set $\mathrm{Hom}(\mathcal{E}_1, \mathcal{E}_2)$ of isogenies from $\mathcal{E}_1$ to $\mathcal{E}_2$ forms a group, with the sum defined as $(\phi + \psi)(P) = \phi(P) + \psi(P)$. If $\mathcal{E}_1 = \mathcal{E}_2 = \mathcal{E}$, then $\mathrm{End}(\mathcal{E}) = \mathrm{Hom}(\mathcal{E}, \mathcal{E})$ is also a ring (since we can compose isogenies) and it is called the **endomorphism ring of** $\mathcal{E}$. The invertible elements of $\mathrm{End}(\mathcal{E})$ form a group $\mathrm{Aut}(\mathcal{E})$.
By Ch. III, Corollary 4.9 and Theorem 4.10 of [Sil09], isogenies have finite kernel and, if ϕ is separable (meaning that the field extension $\overline{k}(\mathcal{E}_1)/\phi^*\overline{k}(\mathcal{E}_2)$ is separable), we have that $\deg\phi = |\ker(\phi)|$.

For each $m \in \mathbb{Z}$ we can sum a point P with itself m–times, if $m \geqslant 0$, or sum $-P$ $(-m)$–times, if $m < 0$. We denote this operation, **the multiplication-by-m isogeny**, by $[m] : \mathcal{E} \longrightarrow \mathcal{E}$, i.e.

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ terms}} \text{ for } m > 0,$$

$$[0]P = O, \quad \text{and} \quad [m]P = [-m](-P) \text{ for } m < 0.$$

It can be proven (cf. [Sil09, Ch. III, Proposition 4.2]) that if $m \neq 0$, then $[m]$ is non-constant. If $\mathcal{E}$ is defined over k, then $[m]$ is defined over k.

Definition 1.3.1. Given $\mathcal{E}$ an elliptic curve over a field k, we denote by $\mathrm{End}(\mathcal{E})$ the endomorphism ring of an elliptic curve. The map

$$\begin{array}{rccc} [\ ]: & \mathbb{Z} & \longrightarrow & \mathrm{End}(\mathcal{E}) \\ & m & \longmapsto & [m] \end{array}$$

gives an injection $\mathbb{Z} \hookrightarrow \mathrm{End}(\mathcal{E})$. If $\mathbb{Z} \subsetneq \mathrm{End}(\mathcal{E})$, we say that $\mathcal{E}$ **has complex multiplication** (shortly, we say that $\mathcal{E}$ has CM or it is with CM).

The following theorem tells us that $\mathrm{End}(\mathcal{E})$ can be of three forms.

Theorem 1.3.2 ([Sil09, Ch. III, Corollary 9.4])**.** *The endomorphism ring of an elliptic curve $\mathcal{E}/k$ is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If* $\mathrm{char}(k) = 0$*, then only the first two are possible.*

Remark 1.3.3. With a few more details, $\mathrm{End}(\mathcal{E})$ is one of the following:

(i) the ring $\mathbb{Z}$;

(ii) a finite index subgring of $\mathbb{Z}[\sqrt{-d}]$ if $-d \not\equiv 1 \mod 4$ or of $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ if $-d \equiv 1 \mod 4$, with $\mathrm{End}(\mathcal{E}) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[\sqrt{-d}]$;

(iii) a ring such that it is free of rank 4 as $\mathbb{Z}$–module and that $\mathrm{End}(\mathcal{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra.

If $\mathrm{char}(k) = 0$, then, by Ch. III, Corollary 5.6 of [Sil09], case (iii) does not appear, since $\mathrm{End}(\mathcal{E})$ is commutative. On the other hand, if k is a finite field, from [Sil09, Ch. V, Theorem 3.1] we get that $\mathrm{End}(\mathcal{E})$ is always larger than $\mathbb{Z}$, i.e. every elliptic curve has CM.

The next two are examples of elliptic curves with CM that we will consider in Chapter 3.

Example 1.3.4. Let k field with $\mathrm{char}(k) \neq 2$ and let $\mathcal{E}/k$ be the curve defined by $y^2 = x^3 + bx$, with $b \in k$. Let $i \in \overline{k}$ be a primitive fourth root of unity, then there is a map $[i]$ in $\mathrm{End}(\mathcal{E})$, given by

$$[i] : (x, y) \longmapsto (-x, iy).$$

Therefore, if $\mathrm{char}(k) = 0$, the curve $\mathcal{E}$ has CM and we have that $\mathrm{End}(\mathcal{E})$ is isomorphic to the ring of Gaussian integers $\mathbb{Z}[i]$: the homomorphism between $\mathbb{Z}[i]$ and $\mathrm{End}(\mathcal{E})$ sending $a + ib$ to $[a] + [i][b]$ for every $a, b \in \mathbb{Z}$ is an isomorphism.

Example 1.3.5. Let k be a number field and let $\mathcal{E}/k$ be the curve defined by $y^2 = x^3 + c$, with $c \in k$. Let $\zeta_3 \in \overline{k}$ be a primitive third root of unity. Then in $\mathrm{End}(\mathcal{E})$ we find the endomorphism

$$\phi : (x, y) \longmapsto (\zeta_3 x, y)$$

and thus $\mathcal{E}$ has CM. It is easy to see that $\mathrm{End}(\mathcal{E})$ is isomorphic to $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, which is the ring of integers of $\mathbb{Q}\left(\sqrt{-3}\right) = \mathbb{Q}(\zeta_3)$.

1.3.1 The m–torsion subgroup of $\mathcal{E}$

The m-torsion subgroup of $\mathcal{E}$ was defined in Subsection 1.1.2 to be the set of points of $\mathcal{E}$ of order m:

$$\mathcal{E}[m] = \{P \in \mathcal{E}(\overline{k}) \mid [m]P = O\}.$$

When $\mathrm{char}(k) = 0$ or if m is prime to $\mathrm{char}(k)$, then $\mathcal{E}[m]$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. This follows from the fact that $\mathcal{E}[m]$ is the kernel of the isogeny $[m]$ multiplication by m, which has degree m^2 (for more details, see Ch. III, Theorem 6.2 and Corollary 6.4 of [Sil09]). An elementary, but rather long, proof of this fact can be given using the so-called **division polynomials**, that we are going to introduce. They are a useful tool in finding explicit m–torsion points.

Division Polynomials. Suppose that $\mathrm{char}(k) \neq 2, 3$, so that we can put $\mathcal{E}$ in Weierstrass form $y^2 = x^3 + Ax + B$. We define the division polynomials recursively:

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Ax - A^2,\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2),
\end{aligned}$$

and then

$$\begin{aligned}
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 && \text{for } n \geqslant 2,\\
\psi_2\psi_{2n} &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) && \text{for } n \geqslant 3,\\
\psi_{-n} &= -\psi_n.
\end{aligned}$$

Furthermore, we define

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1},$$

$$\omega_n = \frac{\psi_{2n}}{2\psi_n}.$$

With these definitions, one can prove inductively, with some easy computations, that ψ_n, ϕ_n, $y^{-1}\omega_n$, for n odd, and $(2y^{-1})\psi_n$, ϕ_n, ω_n, for n even, are polynomials in $\mathbb{Z}[x, y^2, A, B]$. Moreover, by substituting $y^2 = x^3 + Ax + B$, we may consider them as polynomials in $\mathbb{Z}[x, A, B]$ and we have that

$$\begin{aligned}\phi_n(x) &= x^{n^2} + (\text{lower order terms}),\\ \psi_n(x) &= n^2 x^{n^2-1} + (\text{lower order terms}).\end{aligned}$$

One can also easily prove that for any $P = (x_0, y_0)$ the multiplication by m can be written as

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right).$$

We deduce that $[m]$ has degree m^2 and that a point $P = (x_0, y_0)$ (except from the origin O) is m–torsion if and only if $\psi_m(x_0) = 0$. To find the x–coordinates of those points we just need to find the roots of the m–th division polynomial. Then, it suffices to substitute these roots into to the Weierstrass equation of the elliptic curve to dermine the corresponding y–coordinate.

Definition 1.3.6. The field $k_m = k(\mathcal{E}[m])$, obtained by adjoining to k all the m–torsion points of $\mathcal{E}$, is called the m–**th division field** of $\mathcal{E}$.

Remark 1.3.7. From the observation above we get that, if $\mathrm{char}(k)$ does not divide m, then the extension k_m/k given by the m–division field of $\mathcal{E}$ over k is a (finite) Galois extension. Furthermore, since $\mathcal{E}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$, we only need the coordinates of two points, the ones that we choose as a basis for $\mathcal{E}[m]$, to generate k_m (more details in Chapter 3).

In Chapter 3 we will study the 7–division fields of the CM curves of Example 1.3.4 and 1.3.5, in the case when k is a number field. We will use repeatedly the following result to retrieve information about the Galois group of the extension k_7/k.

Theorem 1.3.8 ([Sil94, Chap. II, Theorem 2.3])**.** *Let $\mathcal{E}/\mathbb{C}$ be an elliptic curve with complex multiplication by the ring of integers of the quadratic imaginary field K, and let*

$$L = K(j(\mathcal{E}), \mathcal{E}_{\mathrm{tors}})$$

be the field generated over K by the j–invariant of $\mathcal{E}$ and the coordinates of all the torsion points of $\mathcal{E}$. Then L is an abelian extension of $K(j(\mathcal{E}))$.

In particular, the elliptic curves that we will study in Chapter 3 have j–invariants lying in $\mathbb{Q}$: in fact, for the curves of Example 1.3.4 it is equal to 1728, while for the curves of Example 1.3.5 it is equal to 0. Therefore, in this setting, the field L is equal to $K(\mathcal{E}_{\mathrm{tors}})$. Observe that this field is the compositum of all the fields $K_m = K(\mathcal{E}[m])$ and so, the extensions K_m/K are abelian. We will use this fact to classify all the possible Galois groups of the extensions k_7/k of the mentioned curves.

Galois representations. Let $\mathcal{E}$ be an elliptic curve over a field k and let $m \geqslant 2$ be an integer such that $\mathrm{char}(k) \nmid m$. As already seen, in this setting there is an isomorphism $\mathcal{E}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$. In addition, we have an action of the absolute Galois group G_k on $\mathcal{E}$,

given by the action on its coordinates. Since for every point P and every integer m we have $[m](P^\sigma) = ([m]P)^\sigma$ for all $\sigma \in G_k$, the Galois group G_k also acts on the m–torsion points. Thus, by choosing a basis for $\mathcal{E}[m]$, we obtain a Galois representation

$$\rho_{\mathcal{E},m} : G_k \longrightarrow \mathrm{Aut}\left(\mathcal{E}[m]\right) \simeq \mathrm{GL}_2\left(\mathbb{Z}/m\mathbb{Z}\right),$$

which is called the **mod m Galois representation attached to $\mathcal{E}$**.

Remark 1.3.9. We remark that, although these representations are $\bmod m$, we can deduce a representation in characteristic 0. Indeed, if $m = l$ is a prime, we define the **l–adic Tate module $T_l(\mathcal{E})$ of $\mathcal{E}$** as the inverse limit of all $\mathcal{E}[l^n]$ (with respect to the multiplication by l map $\mathcal{E}[l^{n+1}] \longrightarrow \mathcal{E}[l^n]$). The homomorphism

$$\rho_l : G_k \longrightarrow \mathrm{Aut}\left(T_l(\mathcal{E})\right)$$

is called the **l–adic Galois representation attached to $\mathcal{E}$** and it encodes many of the arithmetic properties of the elliptic curve.

Theorem 1.3.10 (Serre's Open Image Theorem [Ser72, Theorem 2, §4.2])**.** *Let $\mathcal{E}$ be an elliptic curve without CM. Then, for all but finitely many primes l, the l–adic Galois representation ρ_l is surjective.*

Weil pairing. Let $\mathcal{E}/k$ be an elliptic curve and fix m an integer coprime with $p = \mathrm{char}(k)$, if $\mathrm{char}(k) > 0$. We can define a paring on $\mathcal{E}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$, denoted with e_m and called the **Weil e_m–pairing**, taking values in the group of the m–th roots of unity (for the definition, see [Sil09, Ch. III, §8])

$$e_m : \mathcal{E}[m] \times \mathcal{E}[m] \longrightarrow \mu_m.$$

The Weil e_m–pairing is bilinear, alternating, nondegenerate, Galois invariant and compatible (c.f. [Sil09, Ch. III, Proposition 8.1]) and all of these properties imply its surjectivity.

Proposition 1.3.11. *There exists points $S, T \in \mathcal{E}[m]$ such that $e_m(S,T)$ is a primitive m–th root of unity. In particular, if $\mathcal{E}[m] \subset \mathcal{E}(k)$, then $\mu_m \subset k^*$.*

Proof. See Ch. III, Corollary 8.1.1 of [Sil09]. □

Chapter 2

The local-global divisibility problem in algebraic tori

In this chapter we consider the local-global divisibility problem stated in the Introduction (c.f. Problem 1). In particular, after recalling the cohomological interpretation of the problem, we focus on the case of algebraic tori. We present some known results and then show that the problem has an affirmative answer for all powers of an odd prime, provided that the dimension of the torus is bounded or the field of definition has some additional properties. Furthermore, we show that our bound is sharp, by giving examples of higher dimension where the local-global divisibility fails.

This chapter is an expanded version of the paper "Local-global divisibility on algebraic tori" [ACP24], published in the Bulletin of the London Mathematical Society.

Let us recall the problem that we are considering. We let k to be a number field and we denote with M_k the set of places of k and with k_v the completion of k at a place $v \in M_k$. Let q be a fixed positive integer and $\mathcal{G}$ an algebraic group defined over k.

Problem 2.1 (Dvornicich and Zannier, [DZ01]). *If we assume that the point $P \in \mathcal{G}(k)$ has the following property: for all but finitely many $v \in M_k$ there exists $D_v \in \mathcal{G}(k_v)$ such that $P = qD_v$; can we conclude that there exists $D \in \mathcal{G}(k)$ such that $P = qD$?*

2.1 Cohomological interpretation

As mentioned in the introduction, a classical method in dealing with local-global problems is to reinterpret them into cohomological problems.

Notation. From now on we fix k a number field with algebraic closure $\overline{k} = \overline{\mathbb{Q}}$ and we denote by $G_k = \mathrm{Gal}(\overline{k}/k)$ its absolute Galois group. If $v \in M_k$ is a discrete valuation, then we will call it a prime and we will denote by k_v the completion of k at v.

Since it is sufficient to give an answer to Problem 2.1 for powers of a prime, we fix $q = p^l$, where p is a prime number and $l \geqslant 1$ is an integer. In a similar way to what we have seen for elliptic curves, the field $K = k(\mathcal{G}[q])$, obtained by adjoining the coordinates of the q–torsion points of $\mathcal{G}(\overline{k})$ to k, is a finite Galois extension of k. As

seen in Section 1.1.2, the group $\mathcal{G}[q]$ is a finite abelian p–group isomorphic to $(\mathbb{Z}/q\mathbb{Z})^n$, for some $n = n_{\mathcal{G}}$ depending only on $\mathcal{G}$. We also mentioned that, for this reason, the absolute Galois group G_k acts on $\mathcal{G}[q]$ as a subgroup of $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$:

$$\xi : G_k \longrightarrow \mathrm{Aut}(\mathcal{G}[q]) \simeq \mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z}).$$

The image of G_k through this action is a group G isomorphic to $\mathrm{Gal}(K/k)$.

Fix $P \in \mathcal{G}(k)$ and let $D \in \mathcal{G}[q]$ be such that $P = qD$. Call $F = k(D)$ the field generated by adjoining the (coordinates of the) point D to k and consider the composite $L = KF$, with Galois group $\Gamma = \mathrm{Gal}(L/k)$. Then, for each $\gamma \in \Gamma$ we have that $\gamma(D)$ is also a q–divisor of P. So we can define a cocycle

$$\begin{array}{rccl} c: & \Gamma & \longrightarrow & \mathcal{G}[q] \\ & \gamma & \longmapsto & Z_\gamma \quad = \gamma(D) - D. \end{array} \tag{2.1}$$

Let $[c]$ be the class of this cocycle in $\mathrm{H}^1(\Gamma, \mathcal{G}[q])$. By the following proposition, we have that if $[c]$ is zero then the point P has a k–rational q–divisor.

Proposition 2.1.1 ([DP22a, Proposition 3.1])**.** *The class of the cocycle defined in* (2.1) *vanishes in* $\mathrm{H}^1(\Gamma, \mathcal{G}[q])$ *if and only if there exists* $\widetilde{D} \in \mathcal{G}(k)$ *such that* $P = q\widetilde{D}$.

The hypotheses of Problem 2.1 can be translated in a cohomological way as follows. Let v be a prime of k unramified in L. If w is a prime of L extending v, let L_w be the completion of L at w. The extension L_w/k_v is cyclic, generated by a Frobenius authomorphism σ of v. By the hypotheses of the problem, there exists $D_v \in \mathcal{G}(k_v)$ such that $P = qD_v$, therefore the restriction of $[c]$ to $\mathrm{H}^1(\mathrm{Gal}(L_w/k_v), \mathcal{G}[q])$ is zero. This means that there exists $W \in \mathcal{G}[q]$ such that $c(\sigma) = Z_\sigma = (\sigma - 1)W$. By the Čebotarev Density Theorem, the group $\mathrm{Gal}(L_w/k_v)$ varies over all the cyclic subgroups of Γ, as w varies over all but finitely many primes in L (actually, we only need a set of primes of Dirichlet density 1 to apply the theorem). Thus we can give the following definition, first introduced by Dvornicich and Zannier in [DZ01].

Definition 2.1.2. Let G be a group and let M be a G–module. We say that a cocycle $\{Z_g\}_{g\in G}$ of G with values in M **satisfies the local conditions** if there exist $W_g \in M$ such that $Z_g = (g-1)W_g$ for all $g \in G$. We denote by $\mathrm{H}^1_{\mathrm{loc}}(G, M)$ the subgroup of $\mathrm{H}^1(G, M)$ of the classes of these cocycles, called the **first local cohomology group**.

Equivalently, $\mathrm{H}^1_{\mathrm{loc}}(G, M)$ is the intersection of the kernels of the restriction maps $\mathrm{H}^1(G, M) \longrightarrow \mathrm{H}^1(C, M)$, as C varies over all the cyclic subgroups of G:

$$\mathrm{H}^1_{\mathrm{loc}}(G, M) = \bigcap_{\substack{C \leqslant G \\ C \text{ cyclic}}} \ker\left(\mathrm{H}^1(G, M) \longrightarrow \mathrm{H}^1(C, M)\right).$$

In our problem, the first local cohomology group that we are considering is therefore

$$\mathrm{H}^1_{\mathrm{loc}}(\Gamma, \mathcal{G}[q]) = \bigcap_{\substack{v \in M_k \\ v \text{ unramified in } L}} \ker\left(\mathrm{H}^1(\Gamma, \mathcal{G}[q]) \xrightarrow{\mathrm{res}_v} \mathrm{H}^1(\mathrm{Gal}(L_w/k_v), \mathcal{G}[q])\right).$$

By using again Proposition 2.1.1, we deduce that if $\mathrm{H}^1_{\mathrm{loc}}(\Gamma, \mathcal{G}[q])$ is trivial, then Problem 2.1 has an affirmative answer. Dvornicich and Zannier proved in [DZ01, Proposition 2.1] that one can replace the group Γ with $\mathrm{Gal}(K/k)$.

Proposition 2.1.3. *Assume that* $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{G}[q]) = 0$. *Let* $P \in \mathcal{G}(k)$ *be a rational point with the following property: for all but finitely many primes* v *of* k, *there exists* $D_v \in \mathcal{G}(k_v)$ *such that* $P = qD_v$. *Then there exists* $D \in \mathcal{G}(k)$ *such that* $P = qD$.

Thus we have a sufficient condition to answer affirmatively to Problem 2.1.

Remark 2.1.4. If we take all valuations, instead of almost all, in the definition of the group $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{G}[q])$, then we get a group isomorphic to the Tate-Shafarevich group $Ш(k, \mathcal{G}[q])$ (c.f. [DP22a, Section 4]). Thus, the vanishing of $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(K/k), \mathcal{G}[q])$ implies the vanishing of $Ш(k, \mathcal{G}[q])$, which is a sufficient condition to give an affirmative answer to the local–global divisibility problem in the case when v runs over all valuations of k (see, e.g., [Cre16]).

In the following, for ease of notation, we will denote with G the group $\mathrm{Gal}(K/k)$.

Observe that, by [DZ01, Proposition 2.5], we can restrict ourselves to study the vanishing of the first local cohomology group relative to a p–Sylow subgroup of G.

Proposition 2.1.5. *Let* G_p *be a* p*-Sylow subgroup of* G. *An element of* $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ *is zero if and only if its restriction to* $\mathrm{H}^1_{\mathrm{loc}}(G_p, \mathcal{G}[q])$ *is zero.*

In order to find counterexamples for the local-global divisibility, one can ask if the converse of Proposition 2.1.3 holds. By [DZ07, Theorem 3] this is true, but in general only up to a field extension.

Theorem 2.1.6. *Suppose that* $\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{G}[q])$ *is not trivial. Then there exists a number field* L *such that* $L \cap K = k$ *and a point* $P \in \mathcal{G}(L)$ *which is divisible by* q *in* $\mathcal{G}(L_w)$ *for all places* w *of* L *but is not divisible by* q *in* $\mathcal{G}(L)$.

2.2 Known results for algebraic tori

In this section we present the already known answers to Problem 2.1 in the case when $\mathcal{G} = T$ is an algebraic torus.

2.2.1 The split case

As mentioned in the introduction, for the one-dimensional split torus $T = \mathbb{G}_m$ we have a complete answer to the local-global divisibility problem by any integer m, given by the Grunwald-Wang Theorem. Actually, the theorem gives conditions on a more general global field k. We state it as in [AT67, Theorem 1, Chap. X] (see [Wan50] for the original statement). For each $r \geqslant 1$, let $\hat{\zeta_{2^r}}$ be a 2^r–th root of unity choosen so that $\hat{\zeta}^2_{2^{r+1}} = \hat{\zeta}_{2^r}$ and let $\eta_r = \hat{\zeta}_{2^r} + \hat{\zeta}^{-1}_{2^r}$.

Theorem 2.2.1 (Grunwald-Wang)**.** *Let* k *be a global field,* m *a positive integer,* S *a finite set of primes and* $P(m, S)$ *the group of all* $\alpha \in k^\times$ *such that* $\alpha \in k_p^m$ *for all* $p \notin S$. *Then* $P(m, S) = k^{\times m}$ *except under the following conditions:*

- k *is a number field;*
- -1, $2 + \eta_r$ *and* $-(2 + \eta_r)$ *are non-squares in* k, *where* $r \geqslant 2$ *is an integer such that* $\eta_r \in k$ *and* $\eta_{r+1} \notin k$;
- $m = 2^t m'$, *where* m' *is odd and* $t > r$;

- *the set S_0 of primes p such that $p|2$ and -1, $2+\eta_r$ and $-(2+\eta_r)$ are non-squares in k_p is contained in S.*

In this case, $P(m,S) = k^m \cup \alpha_0 k^m$, where $\alpha_0 = ((2+\eta_r)^{2^{t-1}})^{m'}$.

In our case, with k a number field, we have that if the highest power of 2 dividing m is 4, then the answer is affirmative. For higher powers of 2, i.e. for m divisible by 8, the answer is negative. The first counterexample was found by Trost (see [Tro34]) and it is given by taking $k = \mathbb{Q}$, $m = 8$ and $P = 16$, i.e. considering the equation $x^8 - 16 = 0$, which has solutions in $\mathbb{Q}_p$ for all odd primes p, but has no solution in $\mathbb{Q}$ (and in $\mathbb{Q}_2$). The same equation gives a counterexample in other number fields, e.g. in $k = \mathbb{Q}(\sqrt{7})$: indeed, 16 is a 8–th power in k_p for all primes, even in $k_2 = \mathbb{Q}_2(\sqrt{7})$ and in the archimedean completions of k (which are both equal to $\mathbb{R}$), but it is not a 8–th power in k. In this last case we have that the local divisibility holds for all primes p, whereas the global divisibility fails.

Remark 2.2.2. One can construct examples similar to Trost's for all powers 2^n with $n \geqslant 3$ and, therefore, for all integers $m = 2^n m'$, with $n \geqslant 3$ and m' odd. These (and other) examples can be easily constructed by looking at the conditions listed in Theorem 2.2.1. Moreover, one can find counterexamples to the local-global divisibility in every dimension, by taking direct products of copies of $\mathbb{G}_m$.

2.2.2 The general case

For an algebraic torus T, not necessarly split over k, the local-global divisibility by a prime number p was proved by Dvornicich and Zannier already in [DZ01], for tori of certain dimensions.

Theorem 2.2.3 ([DZ01, Theorem 4.1])**.** *Let T be an algebraic k–torus of dimension $n \leqslant \max(3, 2(p-1))$. Then if a point $P \in T(k)$ is divisible by p in all but finitely many $T(k_v)$, it is divisible by p in $T(k)$.*

They proved this statement by showing that the group $\mathrm{H}^1_{\mathrm{loc}}(G, (\mathbb{Z}/p\mathbb{Z})^n)$ is trivial. They also proved that the local-global divisibility does not in general hold for all algebraic tori. Indeed, they showed that for $n = p^4 - p^2 + 1$ and a suitable subgroup G of $\mathrm{GL}_n(\mathbb{Z})$, isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, the first local cohomology group $\mathrm{H}^1_{\mathrm{loc}}(G, (\mathbb{Z}/p\mathbb{Z})^n)$ is nonzero. By choosing $k = \mathbb{Q}(\zeta_{p^3})$, and considering an extension L/k with $\mathrm{Gal}(L/k) \simeq G$, we know by Theorem 1.2.11 that there exists a k–torus T with splitting field L. This choice of k allows to produce a k–rational point P which is p–divisible in all but finitely many $T(k_v)$, but not globally (c.f. [DZ01, Example 5.1]). A similar example can be built over $\mathbb{Q}$ by increasing the dimension: consider the restriction $\widetilde{T} = R_{k/\mathbb{Q}}(T)$ of the torus in the previous example; it has dimension $p^2(p-1)\dim T$ and there is a bijection between $T(k)$ and $\widetilde{T}(\mathbb{Q})$. They also pointed out that the conclusion $\mathrm{H}^1_{\mathrm{loc}}(G, (\mathbb{Z}/p\mathbb{Z})^n) = 0$ could possibly be obtained under weaker assumptions. In 2008 in [Ill08], Illego indeed improved the condition $n \leqslant 2(p-1)$ with the weaker one $n < 3(p-1)$, proving the following.

Theorem 2.2.4 ([Ill08, Theorem 1])**.** *Let $p \neq 2$ be a prime and let $n < 3(p-1)$. For every p–group G in $\mathrm{SL}_n(\mathbb{Z})$ the projection $\mathrm{H}^1(G, \mathbb{F}_p^n) \longrightarrow \prod \mathrm{H}^1(C, \mathbb{F}_p^n)$, the product being taken on all cyclic subgroups C of G, is injective.*

This, together with Proposition 2.4.3, shows that the local-global divisibility by p holds for tori of dimension smaller than $3(p-1)$.

Remark 2.2.5. In the statement of his theorem, Illengo considered only matrices in $\mathrm{SL}_n(\mathbb{Z})$, while above we have seen that we are interested in $G \subseteq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Nevertheless, as Dvornicich and Zannier showed in the proof of Theorem 2.2.3, in the case of the p–divisibility, every p–Sylow subgroup of G actually comes from a p–group of integer matrices, and therefore it suffices to study those. Moreover, being p odd, any p–group of $\mathrm{GL}_n(\mathbb{Z})$ is contained in $\mathrm{SL}_n(\mathbb{Z})$.

Illengo also showed in the same paper that this bound is best possible, by building an example with $r = 3(p-1)$ for which the local-global divisibility by p fails. He defined a p–group G of matrices in $\mathrm{SL}_n(\mathbb{Z})$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ and a cocycle with values in $\mathbb{F}_p^n$ that satisfies the local conditions but it is not a coboundary. The existence of a torus with $\mathrm{Gal}(k(T[p])/k)$ isomorphic to G is guaranteed by Theorem 1.2.11 again.

2.3 Local-global divisibility by p^n in algebraic tori

In the mentioned papers by Dvornicich and Zannier [DZ01] and by Illengo [Ill08], answers to Problem 2.1 were given only for $q = p$ and the question remained open for higher powers of primes p^n in (non-split) algebraic tori. In this part of the thesis we give a complete answer to Problem 2.1 for every power of odd primes. We recall that our aim is to show that if a k–torus T has dimension smaller that $p-1$, then the local-global divisibility by p^n, for any $n \geqslant 1$, holds in $T(k)$. Whereas, for tori of dimension greater than or equal to $p-1$ the local-global divisibility by p^n is no longer assured. For the latter, we will construct a counterexample of dimension $p-1$ for which the local-global divisibility by every p^n with $n \geqslant 2$ does not hold. We remark that, starting from this construction, one can build a counterexample of any dimension $r \geqslant p-1$, by taking the product of the torus that we build (in Lemma 2.4.1) with the split torus of dimension $r-(p-1)$.
Our goal in this section is to prove Theorem 2, a result which we state again for the reader's convenience.

Theorem 2.3.1. *Let p be an odd prime.*

(a) Let k be a number field and let T be a torus defined over k. If T has dimension less than $p-1$, then the local-global divisibility by any power p^n holds for $T(k)$, for every $n \geqslant 1$.

(b) For every $n \geqslant 2$ and for every $r \geqslant p-1$, there exists a torus T defined over $k = \mathbb{Q}(\zeta_p)$ of dimension r and a finite extension L/k such that the local-global divisibility by p^n does not hold for $T(L)$.

Moreover, we also show that under certain condition on the base field k, we can still prove that the local-global divisibility by every p^n, for $n \geqslant 1$, holds for tori of dimension $p-1 \leqslant \dim(T) < 3(p-1)$.

Theorem 2.3.2. *Let p be an odd prime. Suppose that T is a torus defined over k with $p-1 \leqslant \dim(T) < 3(p-1)$ and p does not divide the degree $[k(T[p^n]) \cap k(\zeta_{p^n}) : k]$, where ζ_{p^n} is a p^n–th root of unity. Then the local-global divisibility by p^n holds for $T(k)$.*

2.3.1 Notation

Let us now introduce some notation for algebraic tori that we will use from now on. We adopt the same notation as in Section 4 of [DZ01].

Let T be an algebraic torus defined over a number field k, of dimension r. By definition, there exists an isomorphism of algebraic groups $\phi : T \longrightarrow \mathbb{G}_m^r$, that is defined over a finite extension L of k, the splitting field of T, as seen in Section 1.2. Consider the following map:

$$\begin{array}{rccc} \psi: & G_k & \longrightarrow & \mathrm{Aut}(\mathbb{G}_m^r) \simeq \mathrm{GL}_r(\mathbb{Z}) \\ & \sigma & \longmapsto & \phi \circ (\phi^\sigma)^{-1}, \end{array}$$

where ϕ^σ is the twist of ϕ by $\sigma \in G_k$, i.e. $\phi^\sigma(x) = \sigma(\phi(\sigma^{-1}(x)))$ for every $x \in T$. We notice that ψ is a 1–cocycle, but since the action of G_k on $\mathrm{Aut}(\mathbb{G}_m^r)$ is trivial, the cocycle ψ is actually a group homomorphism. The image $\Delta := \psi(G_k)$ is identified with a finite subgroup of $\mathrm{GL}_r(\mathbb{Z})$ and we have that $\Delta \simeq \mathrm{Gal}(L/k)$.

Let $\zeta := \zeta_{p^n}$ be a primitive p^n–th root of unity and let χ be the cyclotomic character

$$\begin{array}{rccc} \chi: & G_k & \longrightarrow & (\mathbb{Z}/p^n\mathbb{Z})^\times \\ & \sigma & \longmapsto & j_\sigma, \end{array}$$

where j_σ is such that $\sigma(\zeta) = \zeta^{j_\sigma}$. Let $T[p^n]$ be the group of the p^n–torsion points of T. We have $T[p^n] = T(\overline{k})[p^n] \simeq \left\{ (\zeta^{j_1}, \ldots, \zeta^{j_r}) \in \left(\overline{k}^\times\right)^r \mid j_h \in \mathbb{Z}/p^n\mathbb{Z} \right\}$ and we fix the following isomorphism

$$\begin{array}{ccc} T[p^n] & \longrightarrow & (\mathbb{Z}/p^n\mathbb{Z})^r \\ (\zeta^{j_1}, \ldots, \zeta^{j_r}) & \longmapsto & (j_1, \ldots, j_r). \end{array} \tag{2.2}$$

By this isomorphism, the natural action of G_k on $T[p^n]$ induces the following action on $(\mathbb{Z}/p^n\mathbb{Z})^r$: $\sigma \cdot v = j_\sigma \widetilde{\psi(\sigma)} v$ for all $v \in (\mathbb{Z}/p^n\mathbb{Z})^r$, where the tilde denotes the reduction mod p^n. Therefore, we have the homomorphism

$$\begin{array}{rccc} \xi: & G_k & \longrightarrow & \mathrm{GL}_r(\mathbb{Z}/p^n\mathbb{Z}) \\ & \sigma & \longmapsto & j_\sigma \widetilde{\psi(\sigma)}. \end{array} \tag{2.3}$$

It is easy to check that the field fixed by $\ker\xi$ is $K := k\left(T[p^n]\right)$; thus the image G of ξ in $\mathrm{GL}_r(\mathbb{Z}/p^n\mathbb{Z})$ is a finite subgroup isomorphic to $G_k/\ker\xi \simeq \mathrm{Gal}(K/k)$. Denote by $G_{k(\zeta)}$ the subgroup $\mathrm{Gal}\left(\overline{k}/k\left(\zeta\right)\right)$ of G_k. We have $L = \overline{k}^{\ker\psi}$ and $K = \overline{k}^{\ker\xi}$ and, since $\ker\xi \supseteq \ker\psi \cap G_{k(\zeta)}$, we also get $K \subseteq L\left(\zeta\right)$. The kernel of the restriction of ξ to $G_{k(\zeta)}$ is contained both in $\ker\xi$ and in $\ker\widetilde{\psi}$. It follows that the image of $G_{k(\zeta)}$ via ξ is a normal subgroup G' of G, which is also a normal subgroup of the reduction $\widetilde{\Delta}$ modulo p^n of Δ. In particular, we have the following tower of extensions:

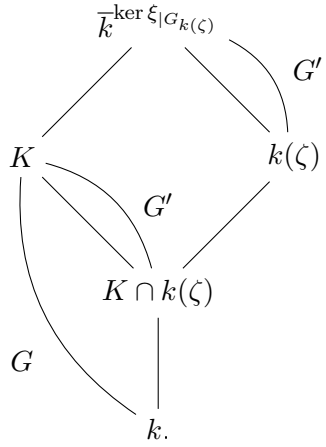

Figure 2.1

We have obtained that G and $\widetilde{\Delta}$ have a common normal subgroup G', with $[G : G'] \mid p^{n-1}(p-1)$ and $[\widetilde{\Delta} : G'] \mid p^{n-1}(p-1)$. In [DZ01], studying the local-global divisibility by p, the authors can easily conclude that G and $\widetilde{\Delta}$ also have the same p–Sylow subgroups (since in their situation both $[G : G']$ and $[\widetilde{\Delta} : G']$ are coprime with p). Thus they only need to study the p–Sylow subgroups in $\widetilde{\Delta}$, which all come from reduction modulo p of p–subgroups of $\Delta \subseteq \mathrm{GL}_r(\mathbb{Z})$. Instead, in our general setting for the divisibility by p^n, we have to distinguish two cases: either $p \mid [G : G']$ or $p \nmid [G : G']$. Observe that in the first case a p–Sylow subgroup of G could not come from a p–group of integer matrices and we cannot use the techniques used in [DZ01] and in [Ill08]. Nevertheless, in the proof of Theorem 2.3.1 we will use the following key result from [Ill08].

Lemma 2.3.3 ([Ill08, Lemma 4]). *Let p be a prime and let Γ be a p–group of matrices in $\mathrm{SL}_r(\mathbb{Q})$. If $r < p(p-1)$ then Γ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^b$, for some $b \leqslant r/(p-1)$.*

The following theorem (see [Sco87, Theorem 6.1.16]) will be a precious tool in proving part (a) of Theorem 2.3.1.

Theorem 2.3.4. *A subgroup of a quotient is a p–Sylow subgroup if and only if it is the image through the canonical projection homomorphism of a p–Sylow subgroup.*

2.4 Proof of Theorem 2.3.1

In this section we give a proof of Theorem 2.3.1. We use the notation above and in particular we denote by G_p a p–Sylow subgroup of G. We show that:

(a) let p be an odd prime number and let $n \geqslant 1$ be an integer, then for every algebraic torus T of dimension $r < p-1$ we have $\mathrm{H}^1_{\mathrm{loc}}(G_p, T[p^n]) = 0$. Hence by Proposition 2.1.5 and Proposition 2.1.3 Problem 2.1 has affirmative answer;

(b) for every odd prime number p and every positive integer $n \geqslant 2$, there exists a torus T defined over $\mathbb{Q}(\zeta_p)$ of dimension $p-1$ such that $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) \neq 0$. Thus by Theorem 2.1.6, there exists a finite extension F of k such that the local-global divisibility by p^n does not hold in $T(F)$.

The counterexample in (b) shows that the bound on the dimension of T is best possible.

Since point (b) requires more efforts we start by showing a few results that we will use for its proof. The first step is building a torus such that G is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$.

Lemma 2.4.1. *Let p be an odd prime and let $n \geqslant 2$. There exists an algebraic torus T of dimension $r = p-1$ defined over $k = \mathbb{Q}(\zeta_p)$ such that G is isomorphic to $Z/p\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$. In particular, we can construct a torus for wich $G \subseteq \mathrm{GL}_r(\mathbb{Z}/p^n\mathbb{Z})$ is generated by*

$$\gamma_1 = \begin{pmatrix} 0 & & & & -1 \\ 1 & 0 & & & -1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & 0 & -1 \\ & & & 1 & -1 \end{pmatrix} \quad \textit{and} \quad \gamma_2 = \begin{pmatrix} p+1 & & & \\ & \ddots & & \\ & & & p+1 \end{pmatrix}.$$

Proof. Let L be a Kummer extension of k, such that $[L:k] = p$ and a prime other than p ramifies. For example, we can take $L = k(\sqrt[p]{2})$. Then $L \cap \mathbb{Q}(\zeta_{p^n}) = k$ and L/k is a cyclic extension of degree p. Let σ be a generator of $\mathrm{Gal}(L/k)$.
Consider the split torus $\mathbb{G}_m = \mathbb{G}_{m,L}$ defined over L. We denote the group $\mathbb{G}_m[p^n]$ by $V \simeq \mathbb{Z}/p^n\mathbb{Z}$ using additive notation. The Galois action on V is given by the cyclotomic character $\chi : G_k \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$. Let $X = R_{L/k}\mathbb{G}_m$ be the Weil restriction of $\mathbb{G}_m$ (see Definition 1.1.13). By Proposition 1.2.12, it is an algebraic torus defined over k of dimension p, split over L. The group $X[p^n]$ of the p^n–torsion points of X is a free $\mathbb{Z}/p^n\mathbb{Z}$–module of rank p. By the properties of the Weil restriction, in particular by Proposition 1.1.15, we have that

$$X[p^n] \simeq \prod_{j=0}^{p-1} V_j,$$

where V_j is an isomorphic copy of V, for every j. The Galois action on $X[p^n]$ is given in the following way. Let us choose a lifting $\overline{\sigma} \in G_k$ of σ. For every $\tau \in G_L = \mathrm{Gal}(\overline{k}/L)$ and $0 \leqslant h \leqslant p-1$, recall from (1.1) that an element $\gamma = \tau\overline{\sigma}^h \in G_k$ acts on $(x_0, x_1 \ldots, x_{p-1}) \in X[p^n]$ by

$$\begin{aligned} \gamma \cdot (x_0, x_1 \ldots, x_{p-1}) &= \tau\overline{\sigma}^h \cdot (x_0, x_1 \ldots, x_{p-1}) \\ &= \chi(\gamma)(x_{-h}, x_{-h+1}, \ldots, x_{-h-1}), \end{aligned} \tag{2.4}$$

where we are considering the indices of the coordinates as integers modulo p.

Now let T be the norm 1 subtorus of X, that is $T = R^{(1)}_{L/k}\mathbb{G}_m = \ker(R_{L/k}\mathbb{G}_m \xrightarrow{N_{L/k}} \mathbb{G}_m)$, the kernel of the (generalized) norm map on X. As seen in Proposition 1.2.14, it is an algebraic torus over k of dimension $r = p-1$, split over L. We are going to show that $k(T[p^n]) = L(\zeta_{p^n})$.
Through the isomorphism (2.2) applied to $X[p^n]$, we can regard $T[p^n]$ as the submodule W of $X[p^n]$ of those vectors $(x_0, x_1 \ldots, x_{p-1})$ such that the sum of all coordinates is equal to zero (we are using the additive notation here). The Galois action on $T[p^n]$ is given by $\xi : G_k \longrightarrow \mathrm{Aut}(W)$, that is, by the action on the points of $X[p^n]$ that lie in W (see (2.3)). We have that $k(T[p^n]) = \overline{k}^{\ker\xi}$. Thus, in order to determine this field, we need to find the elements of G_k that act trivially on W. Since $p \geqslant 3$, by

(2.4) we see that $\gamma = \tau\overline{\sigma}^h$ fixes every $(x_0, x_1 \ldots, x_{p-1})$ in W if and only if $h = 0$ and $\chi(\gamma) = \chi(\tau) = 1$, i.e. if and only if γ lies in $G_L \cap G_{\mathbb{Q}(\zeta_{p^n})} = G_{L(\zeta_{p^n})}$. We therefore conclude that $k\left(T[p^n]\right) = L(\zeta_{p^n})$ as claimed.

Note that $L \cap \mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}(\zeta_p) = k$, so the extension $k\left(T[p^n]\right)/k$ has Galois group $\mathrm{Gal}\left(k\left(T[p^n]\right)/k\right)$ and

$$\mathrm{Gal}\left(k\left(T[p^n]\right)/k\right) \ni \varphi \longmapsto (\varphi_{|L}, \varphi_{|k(\zeta_{p^n})}) \in \mathrm{Gal}\left(L/k\right) \times \mathrm{Gal}\left(k(\zeta_{p^n})/k\right) \tag{2.5}$$

is an isomorphism. Further, it is clear that the last group is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$.

Let $\eta \in \mathrm{Gal}\left(k(\zeta_{p^n})/k\right)$ be the automorphism sending ζ_{p^n} to $\zeta_{p^n}^{p+1}$; the two elements σ and η are generators of $\mathrm{Gal}\left(L/k\right) \times \mathrm{Gal}\left(k(\zeta_{p^n})/k\right)$. As noticed in the previous section, the group $\mathrm{Gal}\left(k\left(T[p^n]\right)/k\right)$ is isomorphic to $G = \xi(G_k) \subseteq \mathrm{GL}_{p-1}(\mathbb{Z}/p^n\mathbb{Z})$. So we want to represent σ and η as matrices in $\mathrm{GL}_{p-1}(\mathbb{Z}/p^n\mathbb{Z})$. We can choose the lifting $\overline{\sigma} \in G_k$ of σ such that, when restricted to $k\left(T[p^n]\right)$, it corresponds to the pair $(\sigma, 1)$ in the isomorphism (2.5); in particular $\chi(\overline{\sigma}) = 1$ (i.e. it lies in $G_{\mathbb{Q}(\zeta_{p^n})}$). With respect to the the basis $v = (1, -1, 0, \ldots, 0, 0)$, $\overline{\sigma}(v)$, $\overline{\sigma}^2(v), \ldots, \overline{\sigma}^{p-2}(v)$ of W, we can write the matrix $\gamma_1 = \xi(\overline{\sigma})$ corresponding to σ, as

$$\gamma_1 = \begin{pmatrix} 0 & & & & -1 \\ 1 & 0 & & & -1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & 0 & -1 \\ & & & 1 & -1 \end{pmatrix}.$$

To conclude the proof, we observe that, with a similar reasoning, we can lift η to $\overline{\eta} \in G_k$ in such a way that, when restricted to $k\left(T[p^n]\right)$, the element $\overline{\eta}$ corresponds to the pair $(1, \eta)$ and, clearly, $\chi(\overline{\eta}) = p + 1$. Hence the action of $\overline{\eta}$ on W is just by multiplication by $p + 1$; so if $\gamma_2 = \xi(\overline{\eta})$ we have

$$\gamma_2 = \begin{pmatrix} p+1 & & \\ & \ddots & \\ & & p+1 \end{pmatrix}.$$

□

Remark 2.4.2. In the proof, we have explicitly described the homomorphism ξ in (2.3) of Section 2.3 in the particular case where T is the norm torus.

Recall from (2.2) that $T[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{p-1}$, hence we have a natural identification of $\mathrm{H}^1_{\mathrm{loc}}\left(G, T[p^n]\right)$ with $\mathrm{H}^1_{\mathrm{loc}}\left(G, (\mathbb{Z}/p^n\mathbb{Z})^{p-1}\right)$ by inducing the action of G on $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ via the same isomorphism. In the following proposition we show that these groups are non-trivial.

Proposition 2.4.3. *Let p be an odd prime and let $n \geqslant 2$. Consider the action of G on $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ induced by the isomorphism $T[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ of (2.2). There exists a (unique) extension of*

$$\gamma_1 \longmapsto v_1 = \begin{pmatrix} p^{n-2}(p-1) \\ 0 \\ \vdots \\ 0 \\ p^{n-2} \end{pmatrix}, \quad \gamma_2 \longmapsto v_2 = \begin{pmatrix} p^{n-1} \\ \vdots \\ p^{n-1} \\ 0 \end{pmatrix}$$

to a cocycle in $\mathrm{H}^1\left(G,(\mathbb{Z}/p^n\mathbb{Z})^{p-1}\right)$ *and it is a non-trivial element of* $\mathrm{H}^1_{\mathrm{loc}}\left(G,(\mathbb{Z}/p^n\mathbb{Z})^{p-1}\right)$.

Proof. Let $\underline{0}$ be the vector with all coordinates equal to zero. To check that the assigned vectors define a cocycle, we have to prove that in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$

$$(1+\gamma_1+\cdots+\gamma_1^{p-1})v_1=\underline{0} \tag{2.6}$$

$$(1+\gamma_2+\cdots+\gamma_2^{p^{n-1}-1})v_2=\underline{0} \tag{2.7}$$

$$(1-\gamma_2)v_1+(\gamma_1-1)v_2=\underline{0} \tag{2.8}$$

Indeed these conditions must be true since $\gamma_1^p=\gamma_2^{p^{n-1}}=\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}=1$ in G. A lifting of γ_1 to $\mathrm{GL}_{p-1}(\mathbb{Q})$ is the matrix γ_1 itself. It solves the polynomial x^p-1 and it is easy to see that 1 is not an eigenvalue. Thus the minimal polynomial of γ_1 is $x^{p-1}+x^{p-2}+\cdots+x+1$ and so condition (2.6) holds. Using $\gamma_2=(p+1)\mathrm{Id}$, we have that

$$(1+\gamma_2+\ldots+\gamma_2^{p-1})v_2=(1+(p+1)+\ldots+(p+1)^{p-1})v_2\equiv\underline{0}\mod p^n.$$

Since $n\geqslant 2$, we can collect the factor $1+\gamma_2+\ldots+\gamma_2^{p-1}$ on the left-hand side of (2.7), hence (2.7) holds. For (2.8) we have:

$$\begin{aligned}(1-\gamma_2)v_1+(\gamma_1-1)v_2&=-pv_1+\begin{pmatrix}-1&&&&-1\\1&-1&&&-1\\&\ddots&\ddots&&\vdots\\&&1&-1&-1\\&&&1&-2\end{pmatrix}v_2\\&\equiv\begin{pmatrix}p^{n-1}\\0\\\vdots\\0\\-p^{n-1}\end{pmatrix}+\begin{pmatrix}-p^{n-1}\\0\\\vdots\\0\\p^{n-1}\end{pmatrix}\equiv\underline{0}\mod p^n\end{aligned}$$

Thus we can extend v_1 and v_2 to a cocycle $Z=\{Z_\gamma\}_{\gamma\in G}$, with $Z_{\gamma_1}=v_1$ and $Z_{\gamma_2}=v_2$. We now prove that Z is not trivial. Suppose that it is a coboundary, then there exists $w\in(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ such that for all $\gamma\in G$ we have $Z_\gamma=(\gamma-1)w$, in particular $v_1=(\gamma_1-1)w$ and $v_2=(\gamma_2-1)w$. We denote with $w^{(i)}$ the i–th coordinate of w. From $v_2=(\gamma_2-1)w$ we have $v_2=pw$, so that $pw^{(p-1)}=0$. On the other hand, from $v_1=(\gamma_1-1)w$ we have

$$v_1=\begin{pmatrix}p^{n-2}(p-1)\\0\\\vdots\\0\\p^{n-2}\end{pmatrix}=\begin{pmatrix}-1&&&&-1\\1&-1&&&-1\\&\ddots&\ddots&&\vdots\\&&1&-1&-1\\&&&1&-2\end{pmatrix}\begin{pmatrix}w^{(1)}\\w^{(2)}\\\vdots\\\vdots\\w^{(p-1)}\end{pmatrix}. \tag{2.9}$$

Thus we obtain the system

$$\begin{cases} -w^{(1)} - w^{(p-1)} = p^{n-2}(p-1) \\ w^{(1)} - w^{(2)} - w^{(p-1)} = 0 \\ \vdots \\ w^{(p-3)} - w^{(p-2)} - w^{(p-1)} = 0 \\ w^{(p-2)} - 2w^{(p-1)} = p^{n-2}. \end{cases} \tag{2.10}$$

By adding the equations in (2.10) we get $p^{n-1} = -pw^{(p-1)}$, in contradiction with $pw^{(p-1)} = 0$. Therefore Z is not a trivial cocycle in $\mathrm{H}^1\left(G, (\mathbb{Z}/p^n\mathbb{Z})^{p-1}\right)$.
We are left to show that Z satisfies the local conditions. It is easy to see that the elements γ_2^h and $\gamma_1\gamma_2^h$, for $h = 0, 1, \ldots, p^{n-1}-1$ are generators of all the cyclic subgroups of G. So it is enough to show that there exist $W_{\gamma_2^h}$ and $W_{\gamma_1\gamma_2^h}$ in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ such that $Z_{\gamma_2^h} = (\gamma_2^h - 1)W_{\gamma_2^h}$ and $Z_{\gamma_1\gamma_2^h} = (\gamma_1\gamma_2^h - 1)W_{\gamma_1\gamma_2^h}$ for all $h \in \{0, 1, \ldots, p^{n-1}-1\}$. First, since $\gamma_2 - 1 = p\mathrm{Id}$, we have that the image of $\gamma_2 - 1$ is the submodule M of $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ of vectors with each coordinate divisible by p. The vector v_2 satisfies this condition, so there exists $W_{\gamma_2} \in (\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ such that $v_2 = Z_{\gamma_2} = (\gamma_2 - 1)W_{\gamma_2}$. Furthermore, since $Z_{\gamma_2^h} = (1 + \gamma_2 + \ldots + \gamma_2^{h-1})v_2$, we have that $Z_{\gamma_2^h}$ also lies in M and $Z_{\gamma_2^h} = (\gamma_2^h - 1)W_{\gamma_2}$.
Now we fix $h \in \{0, 1, \ldots, p^{n-1}-1\}$ and define

$$V = \left\{ \begin{pmatrix} v^{(1)} \\ \vdots \\ v^{(p-1)} \end{pmatrix} \in (\mathbb{Z}/p^n\mathbb{Z})^{p-1} \;\middle|\; \sum_{j=1}^{p-1} v^{(j)} \equiv 0 \mod p \right\} \subseteq (\mathbb{Z}/p^n\mathbb{Z})^{p-1}.$$

We claim that the image of $\gamma_1\gamma_2^h - 1$ is equal to V. Since $\gamma_2^h = (p+1)^h\mathrm{Id} \equiv (1+pl)\mathrm{Id} \mod p^n$ for some $l \in \mathbb{Z}/p^n\mathbb{Z}$, we can rewrite

$$\gamma_1\gamma_2^h - 1 = (1+pl)\gamma_1 - 1 = \begin{pmatrix} -1 & & & & -1-pl \\ 1+pl & -1 & & & -1-pl \\ & \ddots & \ddots & & \vdots \\ & & \ddots & -1 & -1-pl \\ & & & 1+pl & -2-pl \end{pmatrix}$$

and thus $\mathrm{Im}(\gamma_1\gamma_2^h - 1) \subseteq V$.
We check that the determinant of $\gamma_1\gamma_2^h - 1$ is equal to p modulo p^2. For every $j = 2, \ldots, p-1$ let M_j be the determinant of the j–th principal minor of $\gamma_1\gamma_2^h - 1$. We have that

$$\begin{aligned} \det(\gamma_1\gamma_2^h - 1) = M_{p-1} &= -M_{p-2} + (1+pl)^{p-1} \\ &= M_{p-3} + (1+pl)^{p-2} + (1+pl)^{p-1} \\ &\vdots \\ &= M_2 + \sum_{j=1}^{p-3} (1+pl)^{p-j} \\ &= 2 + pl + (1+pl)^2 + \sum_{j=1}^{p-3} (1+pl)^{p-j} \end{aligned}$$

$$\begin{aligned}&\equiv 2 + pl + \sum_{j=2}^{p-1}(1 + plj) \mod p^2\\ &= pl + p - pl = p.\end{aligned}$$

Take a lifting of $\gamma_1\gamma_2^h - 1$ to an integer matrix; this integer matrix has still determinant equal to p modulo p^2. Since $\mathbb{Z}$ is a principal ideal domain, we can consider its Smith normal form $\mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_{p-1})$, and we get that $p \mid \alpha_{p-1}$ while $p^2 \nmid \alpha_{p-1}$ and $p \nmid \alpha_j$ for every $j = 1, \ldots, p-2$.
Its projection $\mathrm{diag}(\widetilde{\alpha}_1, \widetilde{\alpha}_2, \ldots, \widetilde{\alpha}_{p-1})$ modulo p^n is such that $\widetilde{\alpha}_j$ is invertible, for $j = 1, \ldots, p-2$, and $\widetilde{\alpha}_{p-1} \neq 0$ is equal to 0 modulo p. Therefore, up to basis changes in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$, the map $\gamma_1\gamma_2^h - 1$ is

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & p \end{pmatrix}.$$

It follows that $\mathrm{Im}(\gamma_1\gamma_2^h - 1)$ has index equal to p in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$. The submodule V has also index equal to p in $(\mathbb{Z}/p^n\mathbb{Z})^{p-1}$ and so, from the inclusions $\mathrm{Im}(\gamma_1\gamma_2^h - 1) \subseteq V \subseteq \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{p-1}$, we get the equality $V = \mathrm{Im}(\gamma_1\gamma_2^h - 1)$. To conclude that Z satisfies the local conditions it only remains to verify that $Z_{\gamma_1\gamma_2^h}$ lies in V. We have $Z_{\gamma_1\gamma_2^h} = v_1 + \gamma_1 Z_{\gamma_2^h}$, with $v_1 \in V$ and, as mentioned above, $Z_{\gamma_2^h} \in M$ (and also $\gamma_1 Z_{\gamma_2^h} \in M$). Since M is contained in V, we get that $Z_{\gamma_1\gamma_2^h} \in V$. □

We can finally give the proof of Theorem 2.3.1.

Proof of Theorem 2.3.1. Let p be an odd prime.

(a) Let T be an algebraic torus of dimension $r < p-1$ defined over a number field k and let $n \geqslant 1$ be an integer. With the notation of Section 2.3.1, since the inclusion $K \subseteq L(\zeta)$ holds, it is clear that G is isomorphic to the quotient $\mathrm{Gal}(L(\zeta)/k)/\mathrm{Gal}(L(\zeta)/K)$. Being p an odd prime, any p–Sylow subgroup of the group $\Delta \simeq \mathrm{Gal}(L/k)$ is contained in $\mathrm{SL}_r(\mathbb{Q})$; hence by the condition $r < p-1$ and Lemma 2.3.3, we have that Δ has no nontrivial p–Sylow subgroups. By standard Galois theory we have the inclusion

$$\mathrm{Gal}(L(\zeta)/k) \hookrightarrow \mathrm{Gal}(L/k) \times \mathrm{Gal}(k(\zeta)/k).$$

Thus any p–Sylow subgroup of $\mathrm{Gal}(L(\zeta)/k)$ is isomorphic to a subgroup of $\mathrm{Gal}(k(\zeta)/k)$. The latter is isomorphic to a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$, hence it is cyclic. Thus $\mathrm{Gal}(L(\zeta)/k)$ contains only one cyclic p–Sylow subgroup. Now let G_p be a p–Sylow subgroup of G. By Theorem 2.3.4, it is the image through the projection to the quotient of the p–Sylow subgroup of $\mathrm{Gal}(L(\zeta)/k)$, hence it is cyclic too. By the definition of the first local cohomology group we immediately conclude that $\mathrm{H}^1_{\mathrm{loc}}(G_p, T[p^n])$ is trivial and by Proposition 2.1.3 and Proposition 2.1.5 we get an affirmative answer to Problem 2.1 in this case.

(b) Let $n \geqslant 2$ be an integer. As we remarked at the beginning of Section 2.3, it is enough to prove the statement for $r = p-1$. By Lemma 2.4.1 and Proposition 2.4.3 there exists an algebraic torus T defined over $k = \mathbb{Q}(\zeta_p)$ of dimension $p-1$ such that the group $\mathrm{Gal}(k(T[p^n])/k)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$ and $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) \neq 0$. By Theorem 2.1.6, there exists a finite extension F/k such that $F \cap k(T[p^n]) = k$ and the local-global divisibility by p^n does not hold for $T(F)$. □

Remark 2.4.4. The example built in Lemma 2.4.1 is defined over the number field $k = \mathbb{Q}(\zeta_p)$, but we can use it to construct an example over $\mathbb{Q}$ of dimension $(p-1)^2$. Indeed, let $\widetilde{T} = R_{k/\mathbb{Q}}(T)$ be the Weil restriction of T. It has dimension $\dim(\widetilde{T}) = [k:\mathbb{Q}]\dim(T) = (p-1)^2$ and for every number field F containing k we have $\widetilde{T}(F) = R_{k/\mathbb{Q}}(T)(F) = T(k \otimes_{\mathbb{Q}} F) \simeq T(F)^{p-1}$. In particular, if $P \in T(F)$ is a point such that the local-global divisibility fails, we have the failure of the the local-global divisibility also for the corresponding point on $\widetilde{T}(F)$ (given by $p-1$ copies of P).

Remark 2.4.5. Let T be a torus defined over a number field k, with non-trivial first local cohomology group $\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k(T[p^n])/k), T[p^n])$. If L is a finite extension of k linearly disjoint from $k(T[p^n])$ over k, then

$$\mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(L(T[p^n])/L), T[p^n]) \simeq \mathrm{H}^1_{\mathrm{loc}}(\mathrm{Gal}(k(T[p^n])/k), T[p^n])$$

is non-trivial too. Thus by Theorem 2.1.6 we have a counterexample over a finite extension of L. In this way, we have counterexamples over infinitely many number fields; in particular this applies to $k = \mathbb{Q}$. Moreover, this argument works not only for tori, but for every commutative algebraic group.

2.5 Proof of Theorem 2.3.2

In this section we will prove Theorem 2.3.2 by showing that, with the hypotheses of the theorem, we have $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) = 0$. To do so, we will need the following well known result (see p. 197 of [Min87]) whose proof we include for the reader's convenience (for a more general result see [Ser61]).

Lemma 2.5.1. *Let p be an odd prime and let $\pi : \mathrm{GL}_r(\mathbb{Z}) \longrightarrow \mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$ be the reduction modulo p. Then π is injective on finite subgroups of $\mathrm{GL}_r(\mathbb{Z})$.*

Proof. It is enough to show that if $A \in \ker\pi$ and A has finite order m, then $A = \mathrm{Id}$. Suppose that instead $A \neq \mathrm{Id}$. If $p \nmid m$, then write $A = 1 + p^k B$, with $k \geqslant 1$ and $B \in \mathrm{Mat}_r(\mathbb{Z})$ such that p does not divide at least one of the entries of B. We have

$$1 = A^m = \sum_{j=0}^{m} \binom{m}{j} p^{jk} B^j = 1 + mp^k B + \sum_{j=2}^{m} \binom{m}{j} p^{kj} B^j.$$

Thus $mp^k B = -p^{k+1}C$, for some $C \in \mathrm{Mat}_r(\mathbb{Z})$ and so $mB = -pC$, which is a contradiction. On the other hand, if $p \mid m$, then $\overline{A} := A^{m/p}$ has order p and lies in $\ker\pi$. We have $\overline{A} = 1 + p^k\overline{B}$ with $k \geqslant 1$ and $\overline{B} \in \mathrm{Mat}_r(\mathbb{Z})$ such that p does not divide at least one of the entries of $\overline{B}$. We have

$$1 = \overline{A}^p = \sum_{j=0}^{p} \binom{p}{j} p^{jk} \overline{B}^j = 1 + p^{k+1}\overline{B} + \sum_{j=2}^{p-1} \binom{p}{j} p^{kj} \overline{B}^j + p^{pk}\overline{B}^p.$$

Since $p \neq 2$ and $k \geqslant 1$, we get $p^{k+1}\overline{B} = -p^{k+2}\overline{C}$, for some $\overline{C} \in \mathrm{Mat}_r(\mathbb{Z})$, so $B = -p\overline{C}$ and we have again a contradiction.

□

We can now prove Theorem 2.3.2. We remark that the dimension of the torus cannot be greater then $3(p-1)$, since already the local-global divisibility by p would fail (by Illengo's result).

Proof of Theorem 2.3.2. We proceed by induction on $n \geqslant 1$ proving that $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) = 0$. The base of the induction $n = 1$ is proven in [Ill08]. Thus, suppose $n \geqslant 2$ and $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^m]) = 0$, for every $m \leqslant n-1$. With the notation of Section 2.3.1, let $F = K \cap k(\zeta)$. We have that $[F : k] = [G : G']$, thus it is coprime with p by the assumptions of the theorem (see Figure 2.1). Therefore the p–Sylow subgroups of G are contained in G', hence in $\widetilde{\Delta}$. For any $j = 1, \ldots, n-1$, using a similar construction as in Section 2.3.1 for G, we can define a group $G^{(j)} \subseteq \mathrm{GL}_r(\mathbb{Z}/p^j\mathbb{Z})$ that is isomorphic to $\mathrm{Gal}(k\left(T[p^j]\right)/k)$. If we denote with χ_j the cyclotomic character $G_k \longrightarrow (\mathbb{Z}/p^j\mathbb{Z})^\times$, then the elements of $G^{(j)}$ are of the form $\chi_j(\sigma)\widetilde{\psi(\sigma)}^j$, where $\widetilde{\psi(\sigma)}^j$ denotes the reduction modulo p^j and σ varies in G_k. Let $\pi_j : \mathrm{GL}_r(\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow \mathrm{GL}_r(\mathbb{Z}/p^j\mathbb{Z})$ be the reduction modulo p^j and let $H^{(j)}$ be the intersection of G with $\ker \pi_j$. It is easy to prove that $G^{(j)} = \pi_j(G) \simeq \mathrm{Gal}(k\left(T[p^j]\right)/k)$ for every $j = 1, \ldots, n-1$: in fact, one only has to check that $\pi_j(\chi(\sigma)) = \chi_j(\sigma)$, for every $\sigma \in G_k$, and this is true by construction of the cyclotomic character. Consequently, $H^{(j)} \simeq \mathrm{Gal}(K/k\left(T[p^j]\right))$.
We claim that $H^{(1)}$ is trivial. Every $h \in H^{(1)}$ can be written as $h = 1 + pA$, for some $A \in \mathrm{Mat}_r(\mathbb{Z}/p^n\mathbb{Z})$, so we have $h^{p^{n-1}} \equiv \mathrm{Id} \mod p^n$. Hence the subgroup $H^{(1)}$ is a p–group, and thus, it is contained in a p–Sylow subgroup G_p of G. Since every p–Sylow subgroup of G is contained in G', we have that $H^{(1)}$ is contained in a p–Sylow subgroup G'_p of G' too. Thus, $H^{(1)} \subseteq \widetilde{\Delta}_p$, where $\widetilde{\Delta}_p$ is a p–Sylow subgroup of $\widetilde{\Delta}$. Let $H \subset \mathrm{GL}_r(\mathbb{Z})$ be a subgroup of Δ such that its image via the reduction modulo p^n is $H^{(1)}$. Consider $\pi : \mathrm{GL}_r(\mathbb{Z}) \longrightarrow \mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$ the reduction modulo p. We have that H is contained in $\ker(\pi) \cap \Delta$. So, by using Lemma 2.5.1 we find that H and, consequently, $H^{(1)}$ are trivial. Our claim is proved and we get that also every $H^{(j)}$ is trivial since they are all contained in $H^{(1)}$. Therefore $G \simeq G^{(n-1)} \simeq \cdots \simeq G^{(1)}$ via the relative projections.

Consider the following short exact sequence

$$1 \longrightarrow T[p] \xrightarrow{\iota} T[p^n] \xrightarrow{\varepsilon} T[p^{n-1}] \longrightarrow 1,$$

where ι is the inclusion and ε is the p–power map (here we are using the multiplicative notation for $T[p], T[p^{n-1}]$ and $T[p^n]$). The group G acts on $T[p^n]$ and, via the projection, on $T[p]$ and $T[p^{n-1}]$ and, by these actions, the above short exact sequence is a sequence of G–modules. Thus we have the following long exact sequence:

$$1 \to T[p]^G \to T[p^n]^G \to T[p^{n-1}]^G \to \mathrm{H}^1(G, T[p]) \to \mathrm{H}^1(G, T[p^n]) \to \mathrm{H}^1(G, T[p^{n-1}]) \to \ldots$$

Let C be a cyclic subgroup of G and for $i = 1, n-1, n$ let res_i be the restriction $\mathrm{H}^1(G, T[p^i]) \longrightarrow \mathrm{H}^1(C, T[p^i])$. We have the following diagram with exact rows

$$\begin{array}{ccccc}
\ker(\mathrm{res}_1) & \longrightarrow & \ker(\mathrm{res}_n) & \longrightarrow & \ker(\mathrm{res}_{n-1}) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{H}^1(G, T[p]) & \longrightarrow & \mathrm{H}^1(G, T[p^n]) & \to & \mathrm{H}^1(G, T[p^{n-1}]) \\
\downarrow \mathrm{res}_1 & & \downarrow \mathrm{res}_n & & \downarrow \mathrm{res}_{n-1} \\
\mathrm{H}^1(C, T[p]) & \longrightarrow & \mathrm{H}^1(C, T[p^n]) & \to & \mathrm{H}^1(C, T[p^{n-1}])
\end{array}$$

where the central row is given by the long exact sequence above, the lower row is obtained from the same exact sequence by restriction to the subgroup C, whereas the upper one is induced by the commutativity of the diagram given by the last two rows. Since the group G is isomorphic to $G^{(1)}$ and to $G^{(n-1)}$, we have that the cyclic subgroups of $G^{(1)}$ and $G^{(n-1)}$ are the images of the projections of the cyclic subgroups of G. Therefore, by taking the intersection over all the cyclic subgroups of G, from the first row of the diagram we have the exact sequence

$$\mathrm{H}^1_{\mathrm{loc}}(G, T[p]) \longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^n]) \longrightarrow \mathrm{H}^1_{\mathrm{loc}}(G, T[p^{n-1}]).$$

Since by inductive hypothesis $\mathrm{H}^1_{\mathrm{loc}}(G, T[p]) = \mathrm{H}^1_{\mathrm{loc}}(G, T[p^{n-1}]) = 0$, we also have that $\mathrm{H}^1_{\mathrm{loc}}(G, T[p^n])$ is trivial. Again, by Theorem 2.1.3 we conclude that the local-global divisibility by p^n holds for $T(k)$.

□

Remark 2.5.2. We remark that in Lemma 2.4.1 we have $k = \mathbb{Q}(\zeta_p)$ and $F := k\left(T[p^n]\right) \cap k(\zeta_{p^n}) = k(\zeta_{p^n})$, so $[F : k] = [k(\zeta_{p^n}) : k] = [\mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}(\zeta_p)] = p^{n-1}$. Moreover, we notice that the automorphism η in the proof of Lemma 2.4.1 is a generator of the subgroup $H^{(1)} \simeq \mathrm{Gal}\left(k\left(T[p^n]\right)/k\left(T[p]\right)\right)$, defined in the proof of Theorem 2.3.2 above. In particular, for the torus defined in Lemma 2.4.1 we have that $H^{(1)}$ is not trivial.

Remark 2.5.3. Notice that it is always possible to construct an algebraic torus T, not split over k, that satisfies the conditions of Theorem 2.3.2. An example is obtained by taking a number field k that contains a p^n–th root of unity, any finite extension L/k of degree d, with $p-1 \leqslant d < 3(p-1)$ and considering $T = R_{L/k}\mathbb{G}_{m,L}$, the Weil restriction of the split torus $\mathbb{G}_{m,L}$ over L. The torus T is defined over k, it is split over L and it has dimension d. Thus $F = K \cap k(\zeta)$ is equal to k and the hypotheses of the theorem are satisfied.

Chapter 3

On 7-division fields of CM elliptic curves

As seen in the previous chapters, the division fields play a fundamental role in the local-global divisibility. Therefore, this motivated us to study division fields and their properties, which already have an interest of their own due to the many applications related to these extensions. In this chapter we present a classification of the 7–division fields of some families of CM elliptic curves. As an application of these results, we show a minimal bound for the number of completions such that the local divisibility implies the global one in some cases when the principle holds.

These results also appear in the paper "On 7–division fields of CM elliptic curves" [AP23], published in the European Journal of Mathematics.

We use the notation of Chapter 1. Let k be a number field with algebraic closure $\overline{k}$ and let $\mathcal{E}$ be an elliptic curve defined over k. For every positive integer m, we denote by $\mathcal{E}[m]$ the m–torsion subgroup of $\mathcal{E}$ and by k_m the m–th division field $k(\mathcal{E}[m])$.

Recall from Remark 1.3.7 that k_m/k is a finite Galois extension. Moreover, from the properties of the Weil pairing (see Proposition 1.3.11) we have that $k(\zeta_m) \subseteq k_m$, where ζ_m is a primitive m–th root of unity. Thus one may wonder if ζ_m can be used as a generators of the field k_m. Indeed, we have the following result by Bandini and Paladino.

Theorem 3.0.1 ([BP16, Theorem 1.1]). *Let $m > 2$ and let $\{P_1 = (x_1, y_1), P_2 = (x_2, y_2)\}$ be a basis for $\mathcal{E}[m]$, then*

$$k_m = k(x_1, x_2, \zeta_m, y_1).$$

Moreover, when $m \geqslant 4$ we have $k_m = k(x_1, \zeta_m, y_2)$.

When $m = p$ is a prime number, this generating set is minimal among the subsets of $\{x_1, x_2, \zeta_m, y_1, y_2\}$. Indeed, $[k(x_1, \zeta_p, y_2) : k] \geqslant (p^2 - 1)(p^2 - p) = |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|$ and by Serre's Open Image Theorem (see Theorem 1.3.10), for almost every prime p we have that $\mathrm{Gal}(k_p/k) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, for a curve without CM. Therefore, if k is a generic number field (not containing ζ_p or any coordinate of any generator of $\mathcal{E}[p]$, see [BP16, Theorem 4.3]) the equality holds for almost every prime. When $m = p^n$, with $n \geqslant 2$ we can replace ζ_{p^n} with ζ_p, as the next theorem shows.

Theorem 3.0.2 ([DP22b, Theorem 1.1]). *Let $p > 3$ be a prime number and let $n \geqslant 1$. If $\{P_1 = (x_1, y_1), P_2 = (x_2, y_2)\}$ is a basis for $\mathcal{E}[p^n]$, then*

$$k_{p^n} = k(x_1, \zeta_p, y_2).$$

We are going to exhibit some explicit generators for this extension when $m = 7$ and the curve belongs to one of the families of CM elliptic curves $\mathcal{F}_1 : y^2 = x^3 + bx$, with $b \in k$, and $\mathcal{F}_2 : y^2 = x^3 + c$, with $c \in k$. After finding generators, we will study the extensions k_7/k, classifying them according to their possible degree and Galois groups. We conclude the chapter giving some applications to modular curves and, as mentioned above, to the local-global divisibility.

3.1 Generators of $k(\mathcal{E}[7])$ for elliptic curves of $\mathcal{F}_1$

Let $\mathcal{E}$ be an elliptic curve. For every positive integer m, let $\psi_m(x)$ be the m–th division polynomial of $\mathcal{E}$ (for its definition we refer to Section 1.3.1 in Chapter 1). It has degree $\frac{m^2-1}{2}$ when m is odd and $\frac{m^2-4}{2}$ when m is even. Let $\mathcal{E}_1$ be an elliptic curve defined over k with Weierstrass form $y^2 = x^3 + bx$. We saw in Example 1.3.4 that $\mathcal{E}_1$ has CM and its ring of automorphism is isomorphic to the ring of Gaussian integers $\mathbb{Z}[i]$. We denote by ϕ_1 the complex multiplication of $\mathcal{E}_1$ (that we denoted by $[i]$ in Example 1.3.4), i.e. for every point $P = (x, y) \in \mathcal{E}_1$ we have $\phi_1((x, y)) = (-x, iy)$. Since ϕ_1 is an automorphism of $\mathcal{E}_1$, we have that ψ_m is a polynomial in x^2. By the use of a software of computational algebra, one can find explicitly the m–division polynomial for small m. We used the software AXIOM to compute the 7–division polynomials for the curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$. When $m = 7$, the 7–th division polynomial of $\mathcal{E}_1$ is the polynomial

$$\begin{aligned} q_7(x) =& 7x^{24} + 308bx^{22} - 2954b^2x^{20} - 19852b^3x^{18} - 35231b^4x^{16} - 82264b^5x^{14} - 111916b^6x^{12} \\ & - 42168b^7x^{10} + 15673b^8x^8 + 14756b^9x^6 + 1302b^{10}x^4 + 196b^{11}x^2 - b^{12}. \end{aligned}$$

We can set $t := x^2$ and consider the polynomial $q_7(t)$ of degree 12 to look for the abscissas of the 7–torsion points of $\mathcal{E}_1$. For every $\alpha \in k_7$, we denote by $\overline{\alpha}$ its complex conjugate. Let i be a root of $x^2 + 1 = 0$, let σ_1 be the automorphism of the extension $\mathbb{Q}(\zeta_7, i)/\mathbb{Q}$ mapping ζ_7 to ζ_7^5 and let

$$\begin{aligned} \omega_1 &:= (6i+4)\zeta_7^5 + (6i-2)\zeta_7^4 + (2i-2)\zeta_7^3 + (2i+4)\zeta_7^2 + 8i\zeta_7 + 4i - 3; \\ \omega_3 &:= \sigma_1(\omega_1) = (2i+2)\zeta_7^5 + 6\zeta_7^4 + (-4i+6)\zeta_7^3 + (-6i+2)\zeta_7^2 - 4i\zeta_7 - 2i - 1; \\ \omega_5 &:= \sigma_1(\omega_3) = (4i-6)\zeta_7^5 + (-2i-4)\zeta_7^4 + (6i-4)\zeta_7^3 - 6\zeta_7^2 + 4i\zeta_7 + 2i - 7; \\ \omega_{s+1} &:= \overline{\omega_s}, \quad \text{for } s \in \{1,3,5\}; \\ \theta_1 &:= \frac{1}{7}\big((-3520i - 1568)\zeta_7^5 + (-4800i + 2352)\zeta_7^4 + (-256i + 2352)\zeta_7^3 \\ &\qquad + (-1536i - 1568)\zeta_7^2 - 5056i\zeta_7 - 2528i + 3584\big); \\ \theta_3 &:= \sigma_1(\theta_1) = \frac{1}{7}\big((-256i - 2352)\zeta_7^5 + (1280i - 3920)\zeta_7^4 + (3264i - 3920)\zeta_7^3 \\ &\qquad + (4800i - 2352)\zeta_7^2 + 4544i\zeta_7 + 2272i + 1232\big); \\ \theta_5 &:= \sigma_1(\theta_3) = \frac{1}{7}\big((-3264i + 3920)\zeta_7^5 + (1536i + 1568)\zeta_7^4 + (-3520i + 1568)\zeta_7^3 \\ &\qquad + (1280i + 3920)\zeta_7^2 - 1984i\zeta_7 - 992i + 5152\big); \\ \theta_{s+1} &:= \overline{\theta_s}, \quad \text{for } s \in \{1,3,5\}. \end{aligned}$$

With the use of a software of computational algebra (we used AXIOM, that is also implemented in SAGE), one can verify that $q_7(t)$ factors over $k(i,\zeta_7)$ as follows:

$$q_7(t) = 7\prod_{j=1}^{6}\left(t-\left(\omega_j b+\frac{1}{2}b\sqrt{\theta_j}\right)\right)\left(t-\left(\omega_j b-\frac{1}{2}b\sqrt{\theta_j}\right)\right).$$

Thus the roots of $q_7(x)$, i.e. the abscissas of the 7-torsion points of $\mathcal{E}_1$, are

$$\pm x_{2j-1} = \pm\sqrt{\omega_j b+\frac{1}{2}b\sqrt{\theta_j}}; \qquad \pm x_{2j} = \pm\sqrt{\omega_j b-\frac{1}{2}b\sqrt{\theta_j}};$$

for $1\leqslant j\leqslant 6$. By using the equation $y^2=x^3+bx$, we can calculate the corresponding ordinates. For ease of notation, we denote by iP the point $\phi_1(P)=(-x,iy)$, where $P=(x,y)\in\mathcal{E}_1$.

It turns out that the 48 points of exact order 7 of $\mathcal{E}_1$ are the following:

$$\pm P_{2j-1} := (x_{2j-1},\pm y_{2j-1}) = \left(\sqrt{\omega_j b+\frac{1}{2}b\sqrt{\theta_j}}, \pm\sqrt{\left(\omega_j+\frac{1}{2}\sqrt{\theta_j}+1\right)b\sqrt{\omega_j b+\frac{1}{2}b\sqrt{\theta_j}}}\right);$$

$$\pm P_{2j} := (x_{2j},\pm y_{2j}) = \left(\sqrt{\omega_j b-\frac{1}{2}b\sqrt{\theta_j}}, \pm\sqrt{\left(\omega_j-\frac{1}{2}\sqrt{\theta_j}+1\right)b\sqrt{\omega_j b-\frac{1}{2}b\sqrt{\theta_j}}}\right);$$

$$\pm iP_{2j-1} := (-x_{2j-1},\pm iy_{2j-1}), \quad \text{and} \quad \pm\, iP_{2j} := (-x_{2j},\pm iy_{2j});$$

for $1\leqslant j\leqslant 6$. Having found the coordinates of all the 7–torsion points of $\mathcal{E}_1$, we also have the generators of the extension k_7/k. The following theorem tells us that we just need the ordinate of a (nontrivial) point, together with the roots of unity i and ζ_7.

Theorem 3.1.1. *Let θ_j and ω_j be as above, for $1\leqslant j\leqslant 6$, and let $\varepsilon\in\{+,-\}$ fixed. Then we have*

$$k_7 = k\left(i,\zeta_7,y_j\right) = k\left(i,\zeta_7,\sqrt{\left(\omega_j+\varepsilon\frac{1}{2}\sqrt{\theta_j}+1\right)b\sqrt{\omega_j b+\varepsilon\frac{1}{2}b\sqrt{\theta_j}}}\right).$$

Proof. If P is a nontrivial 7–torsion point, then iP is a 7–torsion point too. If iP is not a multiple of P, then a basis for $\mathcal{E}_1[7]$ is given by $\{P,iP\}$. Observe that $iP=nP$, for some integer $n>0$, if and only if $(i-n)P=O$. Since the ring of automorphisms of $\mathcal{E}_1$ is $\mathbb{Z}[i]$ and 7 is inert in $\mathbb{Z}[i]$ (because of $7\equiv 3 \bmod 4$), we see that iP is not a multiple of P, for every $P\in\mathcal{E}_1[7]$ of exact order 7. Therefore we can choose $\{P_j,iP_j\}$ as a generating set of $\mathcal{E}_1[7]$, for any $1\leqslant j\leqslant 12$. We have

$$k_7 = k(x_j,y_j,-x_j,iy_j) = k(x_j,y_j,i).$$

On the other hand, by Theorem 3.0.1, the field k_7 is equal to $k(x_j,\zeta_7,iy_j)$. Then in particular $k_7=k(x_j,i,\zeta_7,y_j)$. By calculating y_j^2 and y_j^4, one can verify that $\sqrt{\theta_j}$ lies in $k(i,\zeta_7,y_j^4)$. Thus $x_j\in k(i,\zeta_7,y_j)$ and we get the conclusion

$$k_7 = k(i,\zeta_7,y_j) = k\left(i,\zeta_7,\sqrt{\left(\omega_j+\varepsilon\frac{1}{2}\sqrt{\theta_j}+1\right)b\sqrt{\omega_j b+\varepsilon\frac{1}{2}b\sqrt{\theta_j}}}\right),$$

for every $1\leqslant j\leqslant 6$ and $\varepsilon\in\{+,-\}$. □

Now that we have explicit generators of the extension k_7/k, in the following two sections we are going to show its possible degree and Galois group, depending of the base field k.

3.2 Degrees $[k_7 : k]$ for the curves of $\mathcal{F}_1$

For ease of notation, from now on we will fix the generating set $\{P_1, iP_1\}$ for $\mathcal{E}_1[7]$. By Theorem 3.1.1 we have $k_7 = k\left(i, \zeta_7, \sqrt{\left(\omega_1 + \frac{1}{2}\sqrt{\theta_1} + 1\right) b\sqrt{\omega_1 b + \frac{1}{2}b\sqrt{\theta_1}}}\right)$. As explained in the proof of Theorem 3.1.1, such a choice is without loss of generality and all the results that we are going to show about the degree $[k_7 : k]$ and the Galois group $\mathrm{Gal}\,(k_7/k)$ hold as well for every other generating set of the extension k_7/k listed in Theorem 3.1.1.

Theorem 3.2.1. *Let $\mathcal{E}_1 : y^2 = x^3 + bx$, with $b \in k$. Let*

$$y_1 = \sqrt{\left(\omega_1 + \frac{1}{2}\sqrt{\theta_1} + 1\right) b\sqrt{\omega_1 b + \frac{1}{2}b\sqrt{\theta_1}}}$$

and consider the conditions

A.	$i \notin k$;	**C.**	$\sqrt{\theta_1} \notin k(i, \zeta_7)$;
B1.	$\zeta_7 + \zeta_7^{-1} \notin k(i)$;	**D.**	$\sqrt{\omega_1 b + \frac{1}{2}b\sqrt{\theta_1}} \notin k(i, \zeta_7, \sqrt{\theta_1})$;
B2.	$\zeta_7 \notin k(i, \zeta_7 + \zeta_7^{-1})$;	**E.**	$y_1 \notin k\left(i, \zeta_7, \sqrt{\omega_1 b + \frac{1}{2}b\sqrt{\theta_1}}\right)$.

The possible degrees of the extension k_7/k are listed in the following table.

d	*holding conditions*	*d*	*holding conditions*
96	**A**, **B1**, **B2**, **C**, **D**, **E**	*8*	**E** and two of **A**, **B2**, **C**, **D** or **A**, **B2** and **C**
48	**B1**, **E**, and three of **A**, **B2**, **C**, **D**	*6*	**B1** and one of **A**, **B2**, **C**, **E**
32	**A**, **B2**, **C**, **D**, **E**	*4*	two of **A**, **B2**, **C** or **E** and one of **A**, **B2**, **C**, **D**
24	**B1**, **E** and two of **A**, **B2**, **C**, **D** or **A**, **B1**, **B2** and **C**	*3*	**B1**
16	**E** and three of **A**, **B2**, **C**, **D**	*2*	one of **A**, **B2**, **C**, **E**
12	**B1**, **E** and one of **A**, **B2**, **C**, **D** or **B1** and two of **A**, **B2**, **C**	*1*	no condition hold

Table 3.1: Conditions for the family $\mathcal{F}_1$

Proof. Consider the tower of extensions

$$k \subseteq k(i) \subseteq k(i, \zeta_7 + \zeta_7^{-1}) \subseteq k(i, \zeta_7) \subseteq k(i, \zeta_7, \sqrt{\theta_1}) \subseteq$$
$$\subseteq k\left(i, \zeta_7, \sqrt{\omega_1 b + \frac{1}{2}b\sqrt{\theta_1}}\right) \subseteq k\left(i, \zeta_7, y_1\right).$$

The degree $d := [k_7 : k]$ is the product of the degrees of the intermediate extensions appearing in the tower. Each extension gives a contribution to the degree less than or equal to 2, except for the extension $k(i) \subseteq k(i, \zeta_7 + \zeta_7^{-1})$ which gives a contribution dividing 3. With the use of the software of computational algebra AXIOM, we have verified that if k is linearly disjoint from $\mathbb{Q}(i, \zeta_7)$ over $\mathbb{Q}$, then θ_1 is not a square in $k(i, \zeta_7)$. A priori we can have all the possible combinations of the conditions **A**, **B1**, **B2**, **C**, **D** and **E**. However, some of the cases do not occur. The extensions $\mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_7)$ are linearly disjoint over $\mathbb{Q}$, so condition **A** is independent of conditions **B1** and **B2**. On the other hand, the extensions $\mathbb{Q}\left(i, \zeta_7, \sqrt{\theta_1}\right)$, $\mathbb{Q}\left(i, \zeta_7, \sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}\right)$ and $\mathbb{Q}(i, \zeta_7, y_1)$ are not linearly disjoint over $\mathbb{Q}(i, \zeta_7)$. Therefore conditions **C**, **D** and **E** might be dependent on each other. We show that **D** depends on **E**.

Suppose that **E** does not hold. Then $y_1 \in k\left(i, \zeta_7, \sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}\right)$ and we can write $y_1 = \alpha + \beta\sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}$, with $\alpha, \beta \in k\left(i, \zeta_7, \sqrt{\theta_1}\right)$. From the equation $y_1^2 = x_1^3 + b x_1$ of $\mathcal{E}_1$, we deduce

$$\begin{cases} 2\alpha\beta = b\omega_1 + b + \dfrac{b}{2}\sqrt{\theta_1} \\ \alpha^2 + \beta^2\left(\omega_1 b + \dfrac{b}{2}\sqrt{\theta_1}\right) = 0 \end{cases}$$

(recall that $b \neq 0$, otherwise the curve would be singular and we would not have an elliptic curve, hence $\alpha\beta \neq 0$). Therefore we get

$$\begin{cases} \alpha = \dfrac{b\omega_1 + b + \dfrac{b}{2}\sqrt{\theta_1}}{2\beta} \\ \dfrac{b^2\left(\omega_1 + 1 + \dfrac{1}{2}\sqrt{\theta_1}\right)^2 + 4\beta^4\left(\omega_1 b + \dfrac{b}{2}\sqrt{\theta_1}\right)}{4\beta^2} = 0. \end{cases}.$$

Hence $b^2\left(\omega_1 + 1 + \frac{1}{2}\sqrt{\theta_1}\right)^2 + 4\beta^4\left(\omega_1 b + \frac{b}{2}\sqrt{\theta_1}\right) = 0$, i.e.

$$\omega_1 b + \frac{b}{2}\sqrt{\theta_1} = -\frac{b^2\left(\omega_1 + 1 + \frac{1}{2}\sqrt{\theta_1}\right)^2}{4\beta^4}$$

is a square in $k\left(i, \zeta_7, \sqrt{\theta_1}\right)$ and condition **D** does not hold too. Therefore we cannot have cases when condition **D** holds and condition **E** does not hold and in particular this implies that condition **E** may not hold only when $d \leqslant \frac{96}{4} = 24$. On the contrary, one can easily see that the assumption that condition **D** does not hold (i.e. $\sqrt{\omega_1 b + \frac{b}{2}\sqrt{\theta_1}} = \alpha + \beta\sqrt{\theta_1}$ with $\alpha, \beta \in k\left(i, \zeta_7\right)$), in general gives no contradiction with the holding of condition **C**. There are no similar dependences for other possible combinations of the conditions, thus all the other cases may take place. The final computation that gives the degree and the corresponding conditions in Table 3.1 is straightforward. □

Remark 3.2.2. One can get examples of extensions realizing the scenarios given by all the possible combinations by considering the curve in the family $\mathcal{F}_1$ with $b = 1$ and setting the base field k as the extension of $\mathbb{Q}$ whose generators are the ones of k_7/k appearing in the conditions which do not hold.

Notice that $[k_7 : k] \leqslant 96 < 2016 = |\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})|$ and the Galois representation

$$\rho_{\mathcal{E}_1,7} : \mathrm{Gal}(\overline{k}/k) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$$

is not surjective, in accordance with $\mathcal{E}_1$ having CM.

3.3 Galois groups $\mathrm{Gal}(k_7/k)$ for the curves of $\mathcal{F}_1$

Let $\mathcal{E}_1$ be a curve of the family $\mathcal{F}_1$, let $G := \mathrm{Gal}(k_7/k)$ and let d be the order of the group G. We denote by Q_{16} the generalized quaternion group of order 16, which has the following presentation

$$\langle x, y \mid x^4 = y^2,\, y^{-1}xy = x^{-1} \rangle.$$

Theorem 3.3.1. *Let k be a field with $\mathrm{char}(k) \neq 2, 3$ and let $\mathcal{E}_1$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx$, where $b \in k$. Then $\mathrm{Gal}(k_7/k)$ is isomorphic to a subgroup of $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$. In particular, if $[k_7 : k] = 96$, then $\mathrm{Gal}(k_7/k) \simeq Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$.*

Proof. Assume that all the conditions in Theorem 3.2.1 hold; then $[k_7 : k] = 96$. The image of $\mathrm{Gal}(\overline{k}/k)$ via the Galois representation $\rho_{\mathcal{E}_1,7}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ isomorphic to $G = \mathrm{Gal}(k_7/k)$. We denote by G both $\mathrm{Gal}(k_7/k)$ and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. As a consequence of the properties of the Weil pairing (see the relevant part in Section 1.3.1), the action of $\mathrm{Gal}(k_7/k)$ on ζ_7 is via determinant, i.e. $\sigma(\zeta_7) = \zeta_7^{\det(\sigma)}$, where σ denotes both an element of G and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. Consider the tower of extensions

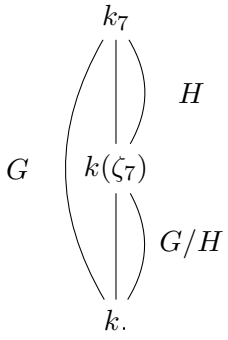

Figure 3.1

We denote by H both the group $\mathrm{Gal}(k_7/k(\zeta_7))$ and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. We have that the Galois group $\mathrm{Gal}(k(\zeta_7)/k) \simeq G/H$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. If σ fixes ζ_7, then it has determinant equal to 1 and so it lies $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. Therefore H is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ of order 16. Since $|\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})| = 336 = 16 \cdot 21$, the image of H in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is a 2–Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. By Sylow's Theorems, the 2–Sylow subgroups are all conjugate and in particular they are all isomorphic. So it suffices to determine the structure of a 2–Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ to get H

up to isomorphism. The structure of such a group is known; however, according to our knowledge, there is no explicit reference in the literature. So, for the reader's convenience, we are going to describe it.
We know that one of the automorphisms of G is the complex multiplication ϕ_1. We consider again $\{P_1, iP_1\}$ as a generating set of $\mathcal{E}_1[7]$ and we have

$$P_1 \overset{\phi_1}{\longmapsto} iP_1 \overset{\phi_1}{\longmapsto} -P_1 \overset{\phi_1}{\longmapsto} -iP_1 \overset{\phi_1}{\longmapsto} P_1.$$

Then the representation of ϕ_1 in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is

$$\phi_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and $\det(\phi_1) = 1$. Therefore ϕ_1 is an element of H and we observe that $\phi_1^2 = -\mathrm{Id}$.
Consider the matrix

$$\tau_1 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Since it has determinant equal to 1, we have that $\tau_1 \in \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. In addition, τ_1 has order 8 and in particular $\tau_1^4 = -\mathrm{Id}$. One can easily verify that $\phi_1\tau_1 = \tau_1^{-1}\phi_1$. Therefore the group generated by ϕ_1 and τ_1 has the following presentation

$$\langle \phi_1, \tau_1 \,|\, \phi_1^2 = \tau_1^4 = -\mathrm{Id},\ \phi_1\tau_1 = \tau_1^{-1}\phi_1 \rangle$$

and it is then isomorphic to the generalized quaternion group Q_{16}, i.e. the dicyclic group Dic_4. This is a group of order 16, hence it is a 2–Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. Thus H is isomorphic to Q_{16} too. We have

$$H = \langle \phi_1, \varphi_1 | \phi_1^2 = \varphi_1^4 = -\mathrm{Id}, \phi_1\varphi_1 = \varphi_1^{-1}\phi_1 \rangle,$$

where φ_1 is a conjugate of τ_1. To deduce the structure of G, we have to look more closely at the automorphism generating $G/H \simeq \mathbb{Z}/6\mathbb{Z}$. In fact, since $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) \simeq \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \rtimes (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \rtimes \mathbb{Z}/6\mathbb{Z}$, we have that G is isomorphic to $H \rtimes \mathbb{Z}/6\mathbb{Z} \simeq Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$. Our goal is now to show that this semidirect product is not a direct product. The group $\mathrm{Gal}(k(\zeta_7)/k) \simeq G/H$ is generated by an automorphism ψ_1 corresponding to the automorphism σ_1 of $\mathbb{Q}(\zeta_7, i)/\mathbb{Q}$ mapping ζ_7 to ζ_7^5. Since $\sigma_1(\omega_1) = \omega_3$ and $\sigma_1(\theta_1) = \theta_3$, we have that ψ_1 acts on the basis $\{P_1, iP_1\}$ by mapping P_1 to one of the points $\pm P_s$, $\pm iP_s$, for $s = 5$ or $s = 6$. Observe that if x_1 is sent to x_s (respectively $-x_s$), for $s = 5$ or $s = 6$, then $-x_1$ is sent to $-x_s$ (respectively x_s). Therefore if ψ_1 maps the point P_1 to P_s (respectively $-P_s$) then ψ_1 maps the point iP_1 to one of the points $\pm iP_s$. Similarly, if ψ_1 maps the point P_1 to iP_s (respectively $-iP_s$), then ψ_1 maps the point iP_1 to one of the points $\pm P_s$. We get that if $\psi_1(P_1) = \alpha P_1 + \beta iP_1$, with $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$, then $\psi_1(iP_1) = \pm(-\beta P_1 + \alpha iP_1)$, i.e.

$$\psi_1 = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} \quad \text{or} \quad \psi_1 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}.$$

Suppose that ψ_1 and ϕ_1 commute. Since $iP_1 = \phi_1(P_1)$, we have that $\psi_1(iP_1) = \phi_1(\psi_1(P_1)) = \alpha iP_1 - \beta P_1$. In this case the representation of ψ_1 in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is $\psi_1 = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$. Observe that every power of ψ_1 is a matrix of the same type

$$\psi_1^n = \begin{pmatrix} \alpha_n & -\beta_n \\ \beta_n & \alpha_n \end{pmatrix},$$

for some $\alpha_n, \beta_n \in \mathbb{Z}/7\mathbb{Z}$. In particular we have

$$\psi_1^3 = \begin{pmatrix} \alpha^3 - 3\alpha\beta^2 & \beta^3 - 3\alpha^2\beta \\ -\beta^3 + 3\alpha^2\beta & \alpha^3 - 3\alpha\beta^2 \end{pmatrix} = \begin{pmatrix} \alpha_3 & -\beta_3 \\ \beta_3 & \alpha_3 \end{pmatrix},$$

for some $\alpha_3, \beta_3 \in \mathbb{Z}/7\mathbb{Z}$. Since $G/H \simeq \mathbb{Z}/6\mathbb{Z}$ and $G = H \rtimes G/H$, we have that $\psi_1^6 = \mathrm{Id}$. Hence

$$(\psi_1^3)^2 = \begin{pmatrix} \alpha_3^2 - \beta_3^2 & -2\alpha_3\beta_3 \\ 2\alpha_3\beta_3 & \alpha_3^2 - \beta_3^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus $\alpha_3\beta_3 = 0$, implying $\alpha_3 = 0$ or $\beta_3 = 0$ in $\mathbb{Z}/7\mathbb{Z}$. Therefore $\alpha^3 - 3\alpha\beta^2 = 0$ or $\beta^3 - 3\alpha^2\beta = 0$, i.e. $\alpha = 0$ or $\beta = 0$ or $\alpha^2 = 3\beta^2$ or $\beta^2 = 3\alpha^2$. The last two equalities have no nontrivial solutions in $\mathbb{Z}/7\mathbb{Z}$ and thus $\alpha = 0$ or $\beta = 0$. Assume $\alpha = 0$, then

$$\psi_1 = \begin{pmatrix} 0 & -\beta \\ \beta & 0 \end{pmatrix} = \beta\phi_1.$$

Since $\psi_1^6 = \mathrm{Id}$ and $\phi_1^2 = -\mathrm{Id}$, we have $-\beta^6 = 1$ and we get a contradiction with Fermat's Little Theorem. If $\beta = 0$, then we see that the automorphism ψ_1 is represented by a scalar matrix $\alpha \cdot \mathrm{Id}$. Since ψ_1 acts on ζ_7 via determinant and we are assuming that ψ_1 is the automorphism of order 6 induced by the automorphism σ_1 mapping ζ_7 to ζ_7^5, we have that $\det(\psi_1) = 5$ i.e. $\alpha^2 = 5$. This equality has no solutions in $\mathbb{Z}/7\mathbb{Z}$. Therefore we must have that ψ_1 is represented by the other matrix

$$\psi_1 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$$

and ψ_1 and ϕ_1 do not commute. Hence G is not isomorphic to $Q_{16} \times \mathbb{Z}/6\mathbb{Z}$. Finally, if $[k_7 : k] < 96$, then G is isomorphic to a proper subgroup of $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$.

□

We are going to describe the Galois group $G = \mathrm{Gal}(k_7/k)$ (up to isomorphism), for all possible $d := [k_7 : k] \leqslant 96$. We firstly state a few general remarks.

Remark 3.3.2.

(i) In the last part of the proof of Theorem 3.3.1 we have shown that the automorphism ψ_1 in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is of the form $\psi_1 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$. Hence $\psi_1^2 = \begin{pmatrix} \alpha^2 + \beta^2 & 0 \\ 0 & \alpha^2 + \beta^2 \end{pmatrix} = -\det(\psi_1)\mathrm{Id}$ and so ψ_1^2 and ψ_1^4 commute with every element of G. Observe that instead $\psi_1^3 = -\det(\psi_1)\psi_1$ does not commute with ϕ_1.

(ii) We recall that every subgroup of a generalized quaternion group is cyclic or it is a (generalized) quaternion group itself. The only proper non abelian subgroup of Q_{16} is Q_8 (and there are two isomorphic copies of it). The other proper nontrivial subgroups of Q_{16} are isomorphic to the groups $\mathbb{Z}/m\mathbb{Z}$, with $m \in \{2, 4, 8\}$.

(iii) By Theorem 1.3.8 and the remarks after the theorem, the extension $k_7/k(i)$ is abelian. Therefore, when condition **A** does not hold, we have that G is an abelian group. If conditions **C**, **D** and **E** hold, then $\mathrm{Gal}(k_7/k(i,\zeta_7))$ is an abelian group of order 8, which is a subgroup of Q_{16}, i.e. it is isomorphic to $\mathbb{Z}/8\mathbb{Z}$. In this case we have $\mathrm{Gal}(k_7/k(i,\zeta_7)) = \langle\varphi_1\rangle$. In addition, $\mathrm{Gal}(k_7/k(i)) = \langle\varphi_1,\psi_1\rangle \simeq \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. In particular, we find that ψ_1 commutes with φ_1. Moreover, we deduce that the existence of any power of φ_1 in G is related to the holding of at least some of the conditions **C**, **D** and **E**.

(iv) Furthermore, we deduce that if **A** does not hold, then $\phi_1 \notin G$. On the other hand, if **A** holds and at least one of **C**, **D** and **E** holds, then G has a subgroup of order 4, which is isomorphic to a subgroup of Q_{16} that is not generated by any power of φ_1. Hence in this case ϕ_1 is an element of G.

(v) The automorphism ϕ_1 does not commute with φ_1^n of φ_1, for every $n \not\equiv 0 \pmod 4$; in fact for such n we have $\phi_1\varphi_1^n = \varphi_1^{-n}\phi_1$. Thus if Q_8 is a subgroup of G under certain conditions, then we have that $\phi_1 \in H$.

(vi) Observe that $\phi_1^2 = \varphi_1^4 = -\mathrm{Id}$ is an element of $\mathrm{Gal}(k_7/k(i))$.

Galois groups $\mathrm{Gal}(k(\mathcal{E}_1[7])/k)$.

$d = 96$. If the degree d of the extension k_7/k is 96, then all the conditions in Table 3.1 hold. We have already proved in Theorem 3.3.1 that $G \simeq Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$.

$d = 48$. If the degree d of the extension k_7/k is 48, then condition **B1** holds, because d is divisible by 3. If **E** does not hold, then as stated in the proof of Theorem 3.2.1 we have that **D** does not hold and we would have an extension of degree $d < 48$. Therefore condition **E** holds.

- If **A** does not hold then, as mentioned above, G is abelian. We have $G = \langle\varphi_1,\psi_1\rangle \simeq \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.
- If **A** holds, we have that ϕ_1 is an element of order 4 of G (recall that condition **E** holds too) and G is not abelian (recall that ϕ_1 does not commute with any element in Q_{16} except its powers). We have two more cases.
  - If **B2** holds, then ψ_1 has order 6 and $G \simeq Q_8 \rtimes \mathbb{Z}/6\mathbb{Z}$.
  - If **B2** does not hold, then $G/H \simeq \mathbb{Z}/3\mathbb{Z}$ is generated by ψ_1^2, which is represented by a scalar matrix, as we have observed above. Thus $G \simeq Q_{16}\times\mathbb{Z}/3\mathbb{Z}$.

$d = 32$. If the degree d of the extension k_7/k is 32, then all the conditions hold but **B1**. Thus we have that $G/H \simeq \mathbb{Z}/2\mathbb{Z}$ is generated by the automorphism ψ_1^3 mapping ζ_7 to ζ_7^{-1} and G is isomorphic to $Q_{16} \rtimes \mathbb{Z}/2\mathbb{Z}$.

$d = 24$. If the degree d of the extension k_7/k is 24, again we have that condition **B1** must hold in all cases, since d is divisible by 3.

- If **B2** holds, then G/H is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ and we have the following cases.
  - If **A** does not hold, then G is abelian and we have $G \simeq \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

- Assume that **A** holds. Since **B2** holds, we have that either **C** or **E** also holds and $\phi_1 \in G$. Therefore $H = \langle \phi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ and $G = \langle \phi_1, \psi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z} \simeq D_8 \times \mathbb{Z}/3\mathbb{Z}$ (recall that ϕ_1 does not commute with ψ_1).

- If **B2** does not hold, then G/H is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and we have the following cases.
  - If **A** does not hold, then G is abelian and we have $G \simeq \mathbb{Z}/24\mathbb{Z}$.
  - Assume that **A** holds. Since we are assuming that **B2** does not hold, then **E** holds (otherwise $d < 24$). We have that $\phi_1 \in G$. Therefore H is a subgroup of Q_{16} of order 8, which is not abelian (recall again that ϕ_1 does not commute with any map in Q_{16} except its powers), i.e. $H \simeq Q_8$. The group G/H is generated by ψ_1^2 or ψ_1^4. Since these two maps commute with every element in G, we have $G \simeq Q_8 \times \mathbb{Z}/3\mathbb{Z}$.

$d = 16$. If the degree d of the extension k_7/k is 16, then condition **B1** does not hold and **E** holds. Only one of the other conditions does not hold.

- If **B2** does not hold, then G/H is trivial and therefore $G \simeq Q_{16}$.
- If **B2** holds, then $G/H = \langle \psi_1^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and H has order 8. We have two possibilities.
  - If **A** does not hold, then we have an abelian extension and $G \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  - Assume that **A** holds. Since **E** holds, we have that $\phi_1 \in G$ and H is not abelian. Therefore $G \simeq Q_8 \rtimes \mathbb{Z}/2\mathbb{Z}$ (recall that ψ_1^3 does not commute with ϕ_1).

$d = 12$. If the degree d of the extension k_7/k is 12, then Q_8 cannot be a subgroup of G. Condition **B1** holds because of 3 divides d and we have the following cases.

- If **B2** holds, then $G/H \simeq \mathbb{Z}/6\mathbb{Z}$ and $H \simeq \mathbb{Z}/2\mathbb{Z}$. Thus G is abelian and $G \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.
- If **B2** does not hold, then G/H has order 3 and it is generated by ψ_1^2 or ψ_1^4. In this case H has order 4. Since every abelian subgroup of Q_{16} is cyclic and both ψ_1^2 and ψ_1^4 commute with every other element of G, we have $G \simeq \mathbb{Z}/12\mathbb{Z}$.

$d = 8$. If the degree d of the extension k_7/k is 8, then **B1** does not hold.

- If **A** does not hold, then we have an abelian extension.
  - If **B2** holds, then G/H has order 2, H has order 4 and G is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  - If **B2** does not hold, then $G = H \simeq \mathbb{Z}/8\mathbb{Z}$.
- If condition **A** holds we have the following cases.
  - If **B2** does not hold, then $G = H$ has order 8. In this case **E** holds, hence ϕ_1 is an automorphism of G and $G \simeq Q_8$.
  - If **B2** holds, we have that one of **C** and **E** holds too. Hence $G/H = \langle \psi_1^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and $H = \langle \phi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. The complex multiplication ϕ_1 is an element of G which does not commute with ψ_1^3. Then $G \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

$d = 6$. If the degree d of the extension k_7/k is 6, then condition **B1** must hold in all cases, as listed in the table of Theorem 3.2.1, and G/H has order divisible by 3. In every case we have an abelian group of order 6, i.e. $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d = 4$. If the degree d of the extension k_7/k is 4, then **B1** does not hold. We have the following cases.

- If **B2** does not hold, then G/H is trivial and $G = H$ is isomorphic to a subgroup of Q_{16} of order 4. Thus G is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
- If **B2** holds, then $G/H \simeq \mathbb{Z}/2\mathbb{Z}$ and G is isomorphic to the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d \leqslant 3$. If the degree d of the extension k_7/k is 3, 2 or 1, the Galois group G is isomorphic to, respectively, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ or $\{\mathrm{Id}\}$.

3.4 Generators of $k(\mathcal{E}[7])$ for elliptic curves of $\mathcal{F}_2$

Let $\mathcal{E}_2$ be an elliptic curve with Weierstrass form $y^2 = x^3 + c$, with $c \in k$. As seen in Example 1.3.5, in $\mathrm{End}(\mathcal{E}_2)$ we have the complex multiplication ϕ_2, which maps (x, y) to $(\zeta_3 x, y)$. As a consequence, the m–th division polynomial $\psi_m(x)$ of $\mathcal{E}_2$ is a polynomial in x^3. If $m = p$ is an odd prime, then $\psi_p(x)$ has degree $\dfrac{p^2-1}{2}$ and we observe that 3 divides $p^2 - 1$. Set $t := x^3$, then $\psi_p(t)$ is a polynomial of degree $\dfrac{p^2-1}{6}$ in the variable t. For $1 \leqslant j \leqslant \dfrac{p^2-1}{6}$, let δ_j be the roots of $\psi_p(t)$. The $p^2 - 1$ abscissas of the p–torsion points of $\mathcal{E}_2$ of exact order p are $\left\{ \sqrt[3]{\delta_j c}, \zeta_3 \sqrt[3]{\delta_j c}, \zeta_3^2 \sqrt[3]{\delta_j c} \;\middle|\; 1 \leqslant j \leqslant (p^2-1)/6 \right\}$. We also have that the ordinates of the points with abscissas in $\left\{ \sqrt[3]{\delta_j}, \zeta_3 \sqrt[3]{\delta_j}, \zeta_3^2 \sqrt[3]{\delta_j} \right\}$ are $\pm\sqrt{(\delta_j + 1)c}$. The point $\phi_2\left(\left(\sqrt[3]{\delta_j c}, \sqrt{\delta_j + c}\right)\right) = \left(\zeta_3 \sqrt[3]{\delta_j c}, \sqrt{\delta_j + c}\right)$ is still a p–torsion point of $\mathcal{E}_2$, for every δ_j. If $P_j = \left(\sqrt[3]{\delta_j c}, \sqrt{\delta_j + c}\right)$ and $\phi_2(P_j)$ are linearly independent, then $\{P_j, \phi_2(P_j)\}$ is a generating set for $\mathcal{E}_2[p]$. In this case, we have both $k(\mathcal{E}_2[p]) = k\left(\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j + 1)\, c}\right)$ and $k(\mathcal{E}_2[p]) = k\left(\sqrt[3]{\delta_j c}, \zeta_p, \sqrt{(\delta_j + 1)\, c}\right)$ (this last equality following by Theorem 3.0.1). We now make these generating sets explicit for $p = 7$, by producing the coordinates of the points in $\mathcal{E}_2[7]$.

We denote by $r_7(x)$ the 7–th division polynomial of a curve $\mathcal{E}_2 \in \mathcal{F}_2$. We have

$$\begin{aligned} r_7(x) =& 7x^{24} + 3944cx^{21} - 42896c^2x^{18} - 829696c^3x^{15} - 928256c^4x^{12} \\ & - 1555456c^5x^9 - 2809856c^6x^6 - 802816c^7x^3 + 65536c^8. \end{aligned}$$

Let σ_2 be the automorphism of $\mathbb{Q}(\zeta_3, \zeta_7)/\mathbb{Q}$ mapping ζ_7 to ζ_7^5, let φ be the automorphism of $\mathbb{Q}(\zeta_3, \zeta_7)/\mathbb{Q}$ mapping ζ_3 to ζ_3^2 and let

$$\begin{aligned} \delta_1 :=& -((-132\zeta_3 - 120)\zeta_7^5 + (-168\zeta_3 - 12)\zeta_7^4 + (-24\zeta_3 + 60)\zeta_7^3 \\ & + (-60\zeta_3 - 84)\zeta_7^2 + (-192\zeta_3 - 96)\zeta_7 - 96\zeta_3 + 52); \\ \delta_2 :=& \sigma_2(\delta_1) = -((-24\zeta_3 - 84)\zeta_7^5 + (36\zeta_3 - 108)\zeta_7^4 + (108\zeta_3 - 72)\zeta_7^3 \\ & + (168\zeta_3 + 12)\zeta_7^2 + (144\zeta_3 + 72)\zeta_7 + 72\zeta_3 + 64); \\ \delta_3 :=& \sigma_2(\delta_2) = -((108\zeta_3 + 180)\zeta_7^5 + (-60\zeta_3 + 24)\zeta_7^4 + (132\zeta_3 + 120)\zeta_7^3 \end{aligned}$$

$$
\begin{aligned}
&\quad + (-36\zeta_3 + 108)\zeta_7^2 + (72\zeta_3 + 36)\zeta_7 + 36\zeta_3 + 172);\\
\delta_4 := \sigma_2(\delta_3) &= -((132\zeta_3 + 12)\zeta_7^5 + (168\zeta_3 + 156)\zeta_7^4 + (24\zeta_3 + 84)\zeta_7^3\\
&\quad + (60\zeta_3 - 24)\zeta_7^2 + (192\zeta_3 + 96)\zeta_7 + 96\zeta_3 + 148);\\
\delta_5 := \sigma_2(\delta_4) &= -((24\zeta_3 - 60)\zeta_7^5 + (-36\zeta_3 - 144)\zeta_7^4 + (-108\zeta_3 - 180)\zeta_7^3\\
&\quad + (-168\zeta_3 - 156)\zeta_7^2 + (-144\zeta_3 - 72)\zeta_7 - 72\zeta_3 - 8);\\
\delta_6 := \sigma(\delta_5) &= -((-108\zeta_3 + 72)\zeta_7^5 + (60\zeta_3 + 84)\zeta_7^4 + (-132\zeta_3 - 12)\zeta_7^3\\
&\quad + (36\zeta_3 + 144)\zeta_7^2 + (-72\zeta_3 - 36)\zeta_7 - 36\zeta_3 + 136);\\
\delta_7 &:= \frac{12\zeta_3 + 8}{7};\\
\delta_8 := \varphi(\delta_8) &= -\frac{12\zeta_3 + 4}{7}.
\end{aligned}
$$

With the use of a software of computational algebra (we used AXIOM) one can verify that the polynomial $r_7(x)$ factors over $k(\zeta_3, \zeta_7)$ as follows:

$$r_7(x) = 7\prod_{j=1}^{8}(x^3 + \delta_j c).$$

Then, as mentioned above, the 48 torsion points of $\mathcal{E}_2$ with exact order 7 are:

$$
\begin{array}{lll}
\pm P_j & = (x_j, \pm y_j) & = \left(\sqrt[3]{\delta_j c}, \pm\sqrt{(\delta_j + 1)c}\right);\\
\pm\phi_2(P_j) & = (\zeta_3 x_j, \pm y_j) & = \left(\zeta_3\sqrt[3]{\delta_j c}\,, \pm\sqrt{(\delta_j + 1)c}\right);\\
\pm\phi_2^2(P_j) & = (\zeta_3^2 x_j, \pm y_j) & = \left(\zeta_3^2\sqrt[3]{\delta_j c}\,, \pm\sqrt{(\delta_j + 1)c}\right);
\end{array}
$$

for $1 \leqslant j \leqslant 8$.

Theorem 3.4.1. *Let $1 \leqslant j \leqslant 6$ and let δ_j be as above. Then*

$$k_7 = k\left(\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j + 1)c}\right) = k\left(\sqrt[3]{\delta_j c}, \zeta_7, \sqrt{(\delta_j + 1)c}\right).$$

Proof. We have already observed at the beginning of this section that if $\phi_2(P)$ is a 7–torsion point that is not a multiple of P, then a basis for $\mathcal{E}_2[7]$ is given by $\{P, \phi_2(P)\}$ and $k_7 = k(x(P), \zeta_3, y(P))$. However, in some cases the point $\phi_2(P)$ is a multiple of P. This happens for the points P_j and $\phi_2(P_j)$, when $j = 7$ or $j = 8$ (in fact if k does not contain ζ_7, then we have that $\zeta_7 \notin k\,(x(P_j), \zeta_3, y(P_j))$, for $j = 7$ and $j = 8$, contradicting the property of the Weil pairing of Proposition 1.3.11).
By the use of a software of computational algebra (we used AXIOM again), one can verify that $x(2P_1) = x(P_3)$ (i.e. $2P_1 = \pm P_3$) and $x(4P_1) = x(P_5)$ (i.e. $4P_1 = \pm P_5$). Suppose that $\phi_2(P_1)$ is a multiple of P_1, i.e. $\phi_2(P_1) = nP_1$ for some integer n. Since $\phi_2^2(P_1) = -P_1 - \phi_2(P_1)$, we have $(n^2+n+1)P_1 = O$. Thus n is a root of n^2+n+1 modulo 7, hence $n \equiv 2, 4 \mod 7$. But, as noticed above, we have $x(2P_1) \neq x(\phi_2(P_1))$ and $x(4P_1) \neq x(\phi_2(P_1))$. Thus $\phi_2(P_1)$ and P_1 are linearly independent. Similar arguments apply for P_3 and P_5. In addition, one can verify that $x(2P_2) = x(P_4)$ and $x(4P_2) = x(P_6)$ and repeat the arguments for those points too. Therefore P_j and $\phi_2(P_j)$ are linearly independent for $1 \leqslant j \leqslant 6$ and $\{P_j, \phi_2(P_j)\}$ is a basis of $\mathcal{E}_2[7]$, for every $1 \leqslant j \leqslant 6$. Thus $k_7 = k\left(\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j + 1)c}\right)$. As stated above, by Theorem 3.0.1 we also have $k_7 = k\left(\sqrt[3]{\delta_j c}, \zeta_7, \sqrt{(\delta_j + 1)c}\right)$. □

3.5 Degrees $[k_7 : k]$ for the curves of $\mathcal{F}_1$

By the results achieved in Theorem 3.4.1, we are going to describe the possible degrees $[k_7 : k]$ for the elliptic curves of the family $\mathcal{F}_2$. From now on we will fix the generating set $\{P_1, \phi_2(P_1)\}$ for $\mathcal{E}_2[7]$. Thus $k_7 = k\left(\sqrt[3]{\delta_1 c}, \zeta_3, \sqrt{(\delta_1+1)c}\right) = k\left(\sqrt[3]{\delta_1 c}, \zeta_7, \sqrt{(\delta_1+1)c}\right)$. Clearly, all the results that we are going to show about the degree $[k_7 : k]$ and the Galois group $\mathrm{Gal}\,(k_7/k)$ hold as well for every other generating set $\left\{\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j+1)c}\right\}$ or $\left\{\sqrt[3]{\delta_j c}, \zeta_7, \sqrt{(\delta_j+1)c}\right\}$ of the extension k_7/k, with $2 \leqslant j \leqslant 6$.

Theorem 3.5.1. *Let $\mathcal{E}_2 : y^2 = x^3 + c$, with $c \in k$, and let δ_1 be as above. Consider the conditions*

A.	$\zeta_3 \notin k$;		
B1.	$\zeta_7 + \zeta_7^{-1} \notin k(\zeta_3)$;	**C.**	$\sqrt[3]{\delta_1 c} \notin k(\zeta_3, \zeta_7)$;
B2.	$\zeta_7 \notin k(\zeta_3, \zeta_7 + \zeta_7^{-1})$;	**D.**	$\sqrt{(\delta_1+1)c} \notin k(\zeta_3, \zeta_7)$.

Then possible degrees of the extension k_7/k are listed in the following table.

d	*holding conditions*	*d*	*holding conditions*
72	**A**, **B1**, **B2**, **C**, **D**	*8*	**A**, **B2**, **D**
36	**B1**, **C** and two of **A**, **B2**, **D**	*6*	one of **B1**, **C** and one of **A**, **B2**, **D**
24	one of **B1**, **C** and **A**, **B2**, **D**	*4*	two of **A**, **B2**, **D**
18	**B1**, **C** and one of **A**, **B2**, **D**	*3*	one of **B1**, **C**
12	one of **B1**, **C** and two of **A**, **B2**, **D**	*2*	one of **A**, **B2**, **D**
9	**B1**, **C**	*1*	no conditions hold

Table 3.2: Conditions for the family $\mathcal{F}_2$

Proof. Consider the tower of extensions

$$k \subseteq k(\zeta_3) \subseteq k\left(\zeta_3, \zeta_7 + \zeta_7^{-1}\right) \subseteq k(\zeta_3, \zeta_7) \subseteq k\left(\zeta_3, \zeta_7, \sqrt[3]{\delta_1 c}\right) \subseteq k\left(\zeta_3, \zeta_7, \sqrt[3]{\delta_1 c}, \sqrt{(\delta_1+1)c}\right).$$

We have that each of the degrees $\left[k\left(\zeta_3, \zeta_7 + \zeta_7^{-1}\right) : k(\zeta_3)\right]$ and $\left[k\left(\zeta_3, \zeta_7, \sqrt[3]{\delta_1 c}\right) : k(\zeta_3, \zeta_7)\right]$ divides 3. In addition, each of the degrees $[k(\zeta_3) : k]$, $\left[k(\zeta_3, \zeta_7) : k\left(\zeta_3, \zeta_7 + \zeta_7^{-1}\right)\right]$ and $\left[k_7 : k\left(\zeta_3, \zeta_7, \sqrt[3]{\delta_1 c}\right)\right]$ divides 2. Since the fields $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_7)$ are linearly disjoint over $\mathbb{Q}$, condition **A** is independent of conditions **B1** and **B2**. Moreover, with the software AXIOM we have verified that when $k \cap \mathbb{Q}(\zeta_3, \zeta_7) = \mathbb{Q}$ neither $\delta_1 + 1$ is a square in $k(\zeta_3, \zeta_7)$, nor δ_1 is a cube in $k(\zeta_3, \zeta_7)$. Then the fields $k(\sqrt[3]{\delta_1 c})$ and $k\left(\sqrt{(\delta_1+1)c}\right)$ are linearly disjoint over $\mathbb{Q}(\zeta_3, \zeta_7)$. Hence all the conditions are independent on each other, except **B1** and **B2**, and we can have all the possible combinations of them. The conclusions follow immediately from $[k_7 : k]$ being the product of the degrees of the intermediate extensions appearing in the tower. □

Remark 3.5.2. As for the family $\mathcal{F}_1$, one can produce examples of extensions realizing the scenarios given by all the possible combinations. This can be done by considering the curve in the family $\mathcal{F}_2$ with $c = 1$ and setting the base field k as the extension of $\mathbb{Q}$ whose generators are the ones of k_7/k appearing in the conditions that do not hold.

Notice again that $[k_7 : k] \leqslant 72 < 2016 = |\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})|$ and the Galois representation

$$\rho_{\mathcal{E}_2,7} : \mathrm{Gal}(\overline{k}/k) \to \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$$

is not surjective, in accordance with $\mathcal{E}_2$ having CM.

3.6 Galois groups $\mathrm{Gal}(k_7/k)$ for the curves of $\mathcal{F}_2$

Let $\mathcal{E}_2$ be a curve of the family $\mathcal{F}_2$. We are going to show all possible Galois groups $\mathrm{Gal}(k(\mathcal{E}_2[7])/k)$, with respect to the degrees $d = [k_7 : k] \leqslant 72$. We denote by Dic_3 the dicyclic group of order 12, which is isomorphic to $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.

Theorem 3.6.1. *Let k be a field with $\mathrm{char}(k) \neq 2, 3$ and let $\mathcal{E}_2$ be an elliptic curve with Weierstrass form $y^2 = x^3 + c$, where $c \in k$. Then $\mathrm{Gal}(k_7/k)$ is isomorphic to a subgroup of $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$. In particular, if $[k_7 : k] = 72$, then $\mathrm{Gal}(k_7/k) \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$.*

Proof. Suppose that all the conditions in Theorem 3.5.1 hold, so that $[k_7 : k] = 72$. The image of $\mathrm{Gal}(\overline{k}/k)$ via the Galois representation $\rho_{\mathcal{E}_2,7}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ isomorphic to $G = \mathrm{Gal}(k_7/k)$. As for the family $\mathcal{F}_1$, we denote by G both $\mathrm{Gal}(k_7/k)$ and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. Consider the tower of extensions in Figure 3.1. We denote by H both $\mathrm{Gal}(k_7/k(\zeta_7))$ and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. The Galois group $\mathrm{Gal}(k(\zeta_7)/k)$ is then isomorphic to the quotient G/H. The group H has order 12, because $\mathrm{Gal}(k(\zeta_7)/k)$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. Since the action of $\sigma \in \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ on ζ_7 is via determinant, i.e. $\sigma(\zeta_7) := \zeta_7^{\det(\sigma)}$, then $\det(\sigma) = 1$, for every $\sigma \in H$. Thus H is indeed a subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. We are going to describe H up to isomorphism. For every positive integer n, we denote by D_{2n} the dihedral group of order $2n$. Since we are assuming that all the conditions in Theorem 3.4.1 hold, then the complex multiplication ϕ_2 and $-\mathrm{Id}$ are elements of H. The complex multiplication ϕ_2 has order 3 and acts on the basis $\{P_1, \phi_2(P_1)\}$ as

$$P_1 \overset{\phi_2}{\longmapsto} \phi_2(P_1), \quad \phi_2(P_1) \overset{\phi_2}{\longmapsto} \phi_2^2(P_1).$$

Since $\phi_2^2(P_1) = -P_1 - \phi_2(P_1)$, we can represent ϕ_2 in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ as

$$\phi_2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Then the inverse of ϕ_2 is represented by the matrix

$$\phi_2^{-1} = \phi_2^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

The automorphism $-\mathrm{Id}$, swapping the points $P \overset{-\mathrm{Id}}{\longmapsto} -P$ for every $P \in \mathcal{E}_2[7]$, corresponds to the automorphism of k_7/k that maps $\sqrt{(\delta_j + 1)c}$ to $-\sqrt{(\delta_j + 1)c}$, for all $1 \leqslant j \leqslant 8$. Clearly ϕ_2 and $-\mathrm{Id}$ commute, so H has a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$. We are going to show that H is not abelian. Suppose instead that H is abelian, then it is isomorphic to either $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$. We are going to show that neither is possible. An element σ of H commutes with ϕ_2, so

$$\sigma = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha - \beta \end{pmatrix},$$

for some $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$. If $H \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, there exists $\sigma \in H$ such that $\sigma^4 = \mathrm{Id}$ and $\sigma^2 = -\mathrm{Id}$, i.e.

$$\sigma^2 = \begin{pmatrix} \alpha^2 - \beta^2 & \beta^2 - 2\alpha\beta \\ 2\alpha\beta - \beta^2 & \alpha^2 - 2\alpha\beta \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The equality $\beta^2 - 2\alpha\beta = 0$ implies $\beta = 0$ or $\beta = 2\alpha$. If $\beta = 0$, then $\alpha^2 = -1$, which has no solutions in $\mathbb{Z}/7\mathbb{Z}$. If $\beta = 2\alpha$, then $-3\alpha^2 = -1$, which has no solutions in $\mathbb{Z}/7\mathbb{Z}$ as well. On the other hand, if $H \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, then there exists $\sigma \in H$ such that $\sigma^2 = \mathrm{Id}$ and $\sigma \neq \pm\mathrm{Id}$. By

$$\sigma^2 = \begin{pmatrix} \alpha^2 - \beta^2 & \beta^2 - 2\alpha\beta \\ 2\alpha\beta - \beta^2 & \alpha^2 - 2\alpha\beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

we get again $\beta = 0$ or $\beta = 2\alpha$. If $\beta = 0$, then $\sigma = \pm\mathrm{Id}$ and we have a contradiction. Suppose $\beta = 2\alpha$. Since σ have determinant equal to 1, we get $\alpha^2 = -2$, which has no solutions in $\mathbb{Z}/7\mathbb{Z}$. Therefore H is not abelian, as claimed. In addition, H is a group of order 12, with a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z}$. We have that either $H \simeq \mathrm{D}_{12}$ or $H \simeq \mathrm{Dic}_3$. We are going to show that the latter holds.
Suppose that $H \simeq \mathrm{D}_{12}$. We also have $H \simeq \mathrm{D}_6 \times \mathbb{Z}/2\mathbb{Z}$, thus H is generated by $-\mathrm{Id}$, ϕ_2 and another automorphism τ of order 2 such that $\phi_2\tau = \tau\phi_2^{-1}$. In other words, $\langle \phi_2, \tau \rangle \simeq \mathrm{D}_6$ and $H = \langle -\mathrm{Id} \rangle \times \langle \phi_2, \tau \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_6$, which is isomorphic to D_{12}. The relation $\phi_2\tau = \tau\phi_2^{-1}$ implies that τ is represented by a matrix of the form

$$\tau = \begin{pmatrix} \alpha & \beta \\ \alpha + \beta & -\alpha \end{pmatrix}$$

for some $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$. Since τ has order 2, we have

$$\tau^2 = \begin{pmatrix} \alpha^2 + \beta^2 + \alpha\beta & 0 \\ 0 & \alpha^2 + \beta^2 + \alpha\beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

i.e. $\alpha^2 + \beta^2 + \alpha\beta = 1$. On the other hand, since $\det(\tau) = 1$, we have that $\alpha^2 + \beta^2 + \alpha\beta = -1$ and we find a contradiction. Therefore the group H is isomorphic to $\mathrm{Dic}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ and it is generated by the complex multiplication ϕ_2, which has order 3, and an automorphism τ_2 of order 4, such that

$$H = \langle \phi_2, \tau_2 \mid \phi_2^3 = \tau_2^4 = 1,\ \phi_2\tau_2 = \tau_2\phi_2^{-1} \rangle.$$

Since $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is isomorphic to $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \rtimes \mathbb{F}_7^\times \simeq \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \rtimes \mathbb{Z}/6\mathbb{Z}$, we have that $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$. For completeness we are going to show that this last semidirect product is not a direct product (as in the case of the family $\mathcal{F}_1$).
The group G/H is generated by an element ψ_2 of order 6 corresponding to the automorphism $\sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ mapping ζ_7 to ζ_7^5. As stated in Section 3.4, we have

$$\delta_1 \overset{\sigma_2}{\longmapsto} \delta_2 \overset{\sigma_2}{\longmapsto} \delta_3 \overset{\sigma_2}{\longmapsto} \delta_4 \overset{\sigma_2}{\longmapsto} \delta_5 \overset{\sigma_2}{\longmapsto} \delta_6 \overset{\sigma_2}{\longmapsto} \delta_1.$$

Then $\psi_2(P_1)$ is one of the points $\pm\phi_2^n(P_2)$, with $0 \leqslant n \leqslant 2$ (where $\phi_2^0 = \mathrm{Id}$). Since ϕ_2 sends the abscissa x_1 of P_1 to $\zeta_3 x_1$, we have that $\psi_2(\phi_2(P_1))$ is one of the points $\pm\phi_2^{n+1}(P_2) = \pm\phi_2(\psi_2(P_1))$. Suppose that $\psi_2(P_1) = \alpha P_1 + \beta\phi_2(P_1)$, for some $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$. Thus we see that $\psi_2(\phi_2(P_1)) = \pm(\beta P_1 + (\beta - \alpha)\phi_2(P_1))$ and we have

$$\psi_2 = \begin{pmatrix} \alpha & -\beta \\ \beta & -\beta + \alpha \end{pmatrix} \quad \text{or} \quad \psi_2 = \begin{pmatrix} \alpha & \beta \\ \beta & \beta - \alpha \end{pmatrix}.$$

Only in the first case ψ_2 and ϕ_2 commute. If all the conditions in Theorem 3.4.1 hold, then the complex multiplication ϕ_2 and the automorphism ψ_2 lie in $\mathrm{Gal}(k_7/k(\zeta_3))$. By [Sil94, Chapter II, Theorem 2.3], the extension $k_7/k(\zeta_3)$ is abelian. Therefore ϕ_2 and ψ_2 must commute and we get $\psi_2 = \begin{pmatrix} \alpha & -\beta \\ \beta & -\beta+\alpha \end{pmatrix}$. Observe that ψ_2^2 maps P_1 to $\phi_2^j(P_3)$, for some $0 \leqslant j \leqslant 2$ and $\phi_2(P_1)$ to $\phi_2^{j+1}(P_3)$. As noted in the proof of Theorem 3.4.1, we have $x(P_3) = x(2P_1)$, i.e. $P_3 = 2P_1$ or $P_3 = -2P_1$. We also have $x(\phi_2(P_3)) = x(2\phi_2(P_1)) = \phi_2(x(2P_1))$. Hence the automorphism ψ_2^2 is equal to $\phi_2^j\omega$ for some j, where ω is represented by one of the following matrices

$$\omega = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{or} \quad \omega = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}.$$

The second case is not possible, since ψ_2^2 would not have order 3. Thus we have $\psi_2^2 = \phi_2^j\omega$, with $\omega = 2\mathrm{Id}$. Since $\psi_2^2 \in G/H$ and $\phi_2^j \in H$, we may assume without loss of generality that $\psi_2^2 = \omega$, by eventually changing the representative of the class ψ_2^2 in G/H. Observe that then ψ_2^2 commutes with every other element of G. Furthermore, we have

$$\psi_2^2 = \begin{pmatrix} \alpha^2-\beta^2 & \beta^2-2\alpha\beta \\ 2\alpha\beta-\beta^2 & \alpha^2-2\alpha\beta \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Thus $\beta(\beta-2\alpha) = 0$, implying $\beta = 0$ or $\beta = 2\alpha$. If $\beta = 0$, then $\det(\psi_2) = \alpha^2 = 5$ (recall that $\psi_2(\zeta_7) = \zeta_7^5 = \zeta_7^{\det(\psi_2)}$), which has no solutions in $\mathbb{Z}/7\mathbb{Z}$. So $\beta = 2\alpha$ and $-3\alpha^2 = 2$, i.e. $\alpha = \pm 2$. Thus we get

$$\psi_2 = \begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix} \quad \text{or} \quad \psi_2 = \begin{pmatrix} -2 & -3 \\ 3 & 2 \end{pmatrix} = -\begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix}.$$

Again, by eventually change the representative of the class of ψ_2 in G/H, we may assume without loss of generality that $\psi_2 = \begin{pmatrix} -2 & -3 \\ 3 & 2 \end{pmatrix}$. We consider an automorphism $\rho \in H$ induced by the automorphism of $\mathrm{Gal}(k_7/k)$ mapping ζ_3 to ζ_3^2. Thus ρ maps P_1 to $\phi_2^j(P_4)$, for some $0 \leqslant j \leqslant 2$ and we have that there exists a power ϕ_2^s of ϕ_2, with $0 \leqslant s \leqslant 2$, such that $j + s \equiv 0 \mod 3$. We call $\widetilde{\rho}$ the product $\phi_2^s\rho$ and we have that it maps P_1 to P_4. Since ψ_2^3 also maps P_1 to P_4 and

$$\psi_2^3 = \begin{pmatrix} 3 & 1 \\ -1 & 4 \end{pmatrix},$$

then we have

$$\widetilde{\rho} = \begin{pmatrix} 3 & \alpha \\ -1 & \beta \end{pmatrix},$$

for some $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$. Thus

$$\widetilde{\rho}\psi_2 - \psi_2\widetilde{\rho} = \begin{pmatrix} 3\alpha-3 & 3\beta+4\alpha-2 \\ 3\beta-5 & -3\alpha+3 \end{pmatrix},$$

and therefore $\widetilde{\rho}$ and ψ_2 commute if and only if $\alpha = 1$ and $\beta = -3$. But then in this case $\det(\widetilde{\rho}) = -1$ and we would have a contradiction with $\rho \in H$. Therefore $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$ with $G \neq \mathrm{Dic}_3 \times \mathbb{Z}/6\mathbb{Z}$.
Finally, if $d = [k_7 : k] < 72$, we have that G is isomorphic to a proper subgroup of $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$. □

Observe that the situation for the Galois groups of the family $\mathcal{F}_2$ is similar to that of the Galois groups of the family $\mathcal{F}_1$. In fact, for the curves in $\mathcal{F}_1$ we have that $G \simeq \mathrm{Dic}_4 \rtimes \mathbb{Z}/6\mathbb{Z}$, since the dicyclic group Dic_4 of order 16 is nothing but the quaternion group Q_{16}.

Now we are going to describe the possible Galois groups $G = \mathrm{Gal}(k(\mathcal{E}_2[7])/k)$ when $d \leqslant 72$. Let us make some useful remarks first.

Remark 3.6.2.

(i) As seen in the proof of Theorem 3.6.1, $\psi_2^3 = 2\psi_2$ does not commute with $\widetilde{\rho}$. Therefore τ_2 does not commute neither with ψ_2 (otherwise we would get $G \simeq \mathrm{Dic}_3 \times \mathbb{Z}/6\mathbb{Z}$), nor with ψ_2^3.

(ii) As mentioned, by Theorem 1.3.8, we have that G is abelian whenever **A** does not hold.

(iii) Every nontrivial proper subgroup of $\mathrm{Dic}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$, with $m \in \{2, 3, 4, 6\}$.

(iv) In particular, if **D** does not hold, then H is abelian. Furthermore, if **D** does not hold and $\phi_2 \in H$, then we have that every other element of H commutes with ϕ_2 and it can be represented by a matrix of the form

$$\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha - \beta \end{pmatrix},$$

for some α and β in $\mathbb{Z}/7\mathbb{Z}$. Then ϕ_2 commutes with ψ_2 too. Therefore, if **D** does not hold, we have that G is abelian as well.

Galois groups $\mathrm{Gal}(k(\mathcal{E}_2[7])/k)$.

$d = 72$. If the degree d of the extension k_7/k is 72, then all the conditions hold. We have proved in Theorem 3.6.1 that in this case $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$.

$d = 36$. If the degree d of the extension k_7/k is 36, then condition **B1** and condition **C** hold.

- If one of **A** and **D** does not hold, then we have an abelian group. Since both condition **B1** and condition **B2** hold, then G/H is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ and thus $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq (\mathbb{Z}/6\mathbb{Z})^2$.
- If **B2** does not hold, then $G/H \simeq \mathbb{Z}/3\mathbb{Z}$ and G is generated by ϕ_2, τ_2, and ψ_2^2. Since ψ_2^2 is represented by a diagonal matrix and commutes with every other automorphism, we have $G \simeq \mathrm{Dic}_3 \times \mathbb{Z}/3\mathbb{Z}$.

$d = 24$. If the degree d of the extension k_7/k is 24, only one of condition **B1** and condition **C** holds and all the other conditions hold.

- If **C** does not hold, then G is generated by τ_2 and ψ_2, so it is isomorphic to $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z} \simeq \mathrm{D}_8 \times \mathbb{Z}/3\mathbb{Z}$.
- If **B1** does not hold, then G/H is generated by ψ_2^3, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Thus $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$.

$d = 18$. If the degree d of the extension k_7/k is 18, conditions **B1** and **C** hold and the automorphism ϕ_2 has order 3. Since only one of the other conditions holds, we have that at least one of **A** or **D** does not hold and G is abelian.

- If either **A** or **D** holds, then $G \simeq (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$.
- If both **A** and **D** do not hold, then **B2** holds. We have $G/H = \langle \psi_2 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$ and $H = \langle \phi_2 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$. Since ϕ_2 and ψ_2 commute, we have that $G \simeq (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$ as well.

$d = 12$. If the degree d of the extension k_7/k is 12, only one of conditions **B1** and **C** holds and two of the other conditions hold.

- If both **B1** and **B2** do not hold, then the extension G/H is trivial and $G = H$ is isomorphic to $\mathrm{Dic}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.
- If **B1** does not hold and **B2** holds, then $H \simeq \mathbb{Z}/2\mathbb{Z}$ and $G/H \simeq \mathbb{Z}/6\mathbb{Z}$. One of **A** and **D** does not hold, so the extension k_7/k is abelian with Galois group $G \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.
- If **B1** holds and **B2** does not hold, then G/H is generated by ψ_2^2 and H is generated by τ_2, so it is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Since ψ_2^2 commutes with τ_2, we get that the Galois group G is isomorphic to $\mathbb{Z}/12\mathbb{Z}$.
- If both **B1** and **B2** hold, then $G/H \simeq \mathbb{Z}/6\mathbb{Z}$ and $H \simeq \mathbb{Z}/2\mathbb{Z}$. Again, we have that one of **A** and **D** does not hold, hence k_7/k is an abelian extension with Galois group $G \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

$d = 9$. If the degree d of the extension k_7/k is 9, the only holding conditions are **B1** and **C**. Then $H = \langle \phi_2 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ and $G/H \simeq \mathbb{Z}/3\mathbb{Z}$. We have $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

$d = 8$. If the degree d of the extension k_7/k is 8, then all the conditions hold but **B1** and **C**. Thus $H = \langle \tau_2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ and $G/H = \langle \psi_2^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. We have observed that τ_2 and ψ_2^3 do not commute, hence $G \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{D}_8$.

$d = 6$. If the degree d of the extension k_7/k is 6, then either **B1** or **C** holds and one of the other condition holds. In all cases the group G is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

$d = 4$. If the degree d of the extension k_7/k is 4, then both **B1** and **C** do not hold.

- If **B2** does not hold, then G/H is trivial and $G = H$ is generated by τ_2 and it is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
- If **B2** holds, then $G/H \simeq \mathbb{Z}/2\mathbb{Z}$ and G is isomorphic to the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d \leqslant 3$. If the degree d of the extension k_7/k is 3 or 2 or 1, obviously the Galois group is isomorphic to, respectively, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ or $\{\mathrm{Id}\}$.

3.7 Some applications

In this section we will describe some applications of the results achieved in the previous sections of this chapter. The first one is an application to the local-global divisibility problem in elliptic curves. The second one regards CM points on modular curves.

3.7.1 A minimal bound for the local-global divisibility by 7

As previously mentioned, the local-global divisibility by a prime number p holds in the case of an elliptic curve $\mathcal{E}$ over k (see the Introduction and [DZ01, Theorem 3.1], among others). In particular, the local-global divisibility by 7 holds in $\mathcal{E}$ over k.
Let $G = \mathrm{Gal}(k_7/k)$ and let Σ be the set of places of k unramified in k_7. From the cohomological interpretation of the problem described in Section 2.1, for the local-global divisibility by 7 we have that

$$\mathrm{H}^1_{\mathrm{loc}}(G, \mathcal{E}[7]) = \bigcap_{v \in \Sigma} (\ker \mathrm{H}^1(G, \mathcal{E}[7]) \xrightarrow{\mathrm{res}_v} \mathrm{H}^1(G_v, \mathcal{E}[7])) = 0,$$

where we recall that the map res_v denotes the usual restriction map and G_v the Galois groups of the extension $(k_7)_w/k_v$.

By the Čebotarev Density Theorem, it suffices to consider the intersection over the places $v \in S$, with S a subset of Σ such that G_v varies over all cyclic subgroups of G as v varies in S. Observe that in particular we can choose a finite set S, whereas the set Σ is not finite.

Thus, if we are able to find such a set S and prove that the local divisibility by 7 holds for a $P \in \mathcal{E}(k)$, for all $v \in S$, then we get that P is globally divisible by 7, i.e. that P has a k–rational 7–divisor. So it suffices to have the local divisibility by 7 for a finite number of suitable places to get the global divisibility by 7.

In [DP22b] Dvornicich and Paladino produced an explicit effective version of the hypotheses of Problem 1 in all elliptic curves over number fields. In particular, they produced an explicit finite set S of places of k such that the assumption of the validity of the local divisibility for all but finite many places can be replaced with the assumption of the validity of the local divisibility for all places in S. The effective version is given by an upper bound $B(m, \mathcal{E})$ that depends only on m and $\mathcal{E}$ (and not on the field k). With such a bound it is not necessary to take into account the distinctness of the Galois groups G_v in testing the local divisibility, since it is already assured by the density of places v that are considered. However, for this reason the cardinality of the set S produced in [DP22b] is not as minimal as possible. Indeed, it is a very hard problem to obtain a similar result with an explicit set S of minimal cardinality (i.e. with the assumption that the local Galois groups G_v, corresponding to the places in S, are pairwise distinct), for all positive integers m. It is also a difficult problem just to find the minimal possible cardinality for S for every m.

In view of the results achieved for the Galois groups $\mathrm{Gal}(k_7/k)$ for the elliptic curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$, we give an answer to this last question when $m = 7$ for the curves of these families. For these curves we produce an upper bound to the cardinality of S which is surprisingly small and it is as minimal as possible when the degree $[k_7 : k]$ is maximum (that is, $[k_7 : k] = 96$ for the curves in $\mathcal{F}_1$ and $[k_7 : k] = 72$ for the curves in $\mathcal{F}_2$). With the description of the Galois groups given in Section 3.3 and Section 3.6 and with the description of the cyclic subgroups of G given in the proofs of the following Theorem 3.7.1 and Theorem 3.7.2, one can easily deduce the minimal cardinality for S, for every $\mathcal{E}_1 \in \mathcal{F}_1$ and $\mathcal{E}_2 \in \mathcal{F}_2$.

Theorem 3.7.1. *Let $\mathcal{E}_1$ be an elliptic curve defined over a number field k, with Weierstrass equation $y^2 = x^2 + bx$, for some $b \in k$. There exist sets $S \subseteq M_k$ of cardinality $s \leqslant 18$ such that if $P = 7D_v$, with $D_v \in \mathcal{E}_1(k_v)$, for all $v \in S$, then $P = 7D$, for some $D \in \mathcal{E}_1(k)$. In particular, if $[k_7 : k] = 96$, then $s = 18$.*

Proof. Let s be the number of distinct cyclic subgroups of G. As stated above, the set S can be chosen as a subset of M_k with cardinality s, such that G_v varies over all cyclic subgroups of G, as v varies in S, and G_v and G_w are pairwise distinct cyclic subgroups of G, for all $v, w \in S$, with $v \neq w$. It suffices to show that $s \leqslant 18$, i.e. that G has at most 18 cyclic subgroups. We have proved in Section 3.3, that for every $\mathcal{E}_1 \in \mathcal{F}_1$, the Galois group G is isomorphic to a subgroup of $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$. We keep the notation used in Section 3.3 for the generators of Q_{16} and $\mathbb{Z}/6\mathbb{Z}$, that is $Q_{16} = \langle \phi_1, \varphi_1 \mid \phi_1^2 = \varphi_1^4 = -\mathrm{Id}, \phi_1\varphi_1 = \varphi_1^{-1}\phi_1 \rangle$ and $\mathbb{Z}/6\mathbb{Z} = \langle \psi_1 \rangle$. The group Q_{16} has seven nontrivial cyclic subgroups: $\langle \varphi_1 \rangle \simeq \mathbb{Z}/8\mathbb{Z}$, $\langle -\mathrm{Id} \rangle = \langle \phi_1^2 \rangle = \langle \varphi_1^4 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and the five cyclic subgroups of order 4 generated respectively by ϕ_1, φ_1^2, $\phi_1\varphi_1$, $\phi_1\varphi_1^2$ and $\phi_1\varphi_1^3$. We also have the nontrivial cyclic subgroups of $\langle \psi_1 \rangle$, i.e. $\langle \psi_1^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \psi_1^2 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ and the group $\langle \psi_1 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$ itself. All of these groups are cyclic subgroups of G. In addition, we have the group $\langle \varphi_1, \psi_1^2 \rangle \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/24\mathbb{Z}$, five copies of $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ given by the direct products of the five subgroups of order 4 of Q_{16} with $\langle \psi_1^2 \rangle$, the subgroup $\langle -\mathrm{Id}, \psi_1^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and the trivial group $\langle \mathrm{Id} \rangle$. Therefore $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$ contains 18 cyclic subgroups and every subgroup G of $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$ has at most 18 cyclic subgroups. Thus $s \leqslant 18$. In particular, if $[k_7 : k] = 96$, then G has exactly 18 cyclic subgroups and in this case $s = 18$ is sharp (in fact, if $s < 18$, then the hypotheses of Problem 1 are not satisfied).

□

Theorem 3.7.2. *Let $\mathcal{E}_2$ be an elliptic curve defined over a number field k, with Weierstrass equation $y^2 = x^2 + c$, for some $c \in k$. There exist sets $S \subseteq M_k$ of cardinality $s \leqslant 15$ such that if $P = 7D_v$, with $D_v \in \mathcal{E}(k_v)$, for all $v \in S$, then $P = 7D$, for some $D \in \mathcal{E}(k)$. In particular, if $[k_7 : k] = 72$, then $s = 15$.*

Proof. Let s be the number of distinct cyclic subgroups of G. As for the proof of Theorem 3.7.1, we just have to show that G has at most 15 cyclic subgroups. As proved in Section 3.6, for every $\mathcal{E}_2 \in \mathcal{F}_2$, the Galois group G is isomorphic to a subgroup of $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$. In the notation of Section 3.6, a presentation of the group $\mathrm{Dic}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ is $\langle \phi_2, \tau_2 | \phi_2^3 = \tau_2^4 = \mathrm{Id}, \tau_2\phi_2 = \phi_2^{-1}\tau_2 \rangle$, while we denote the generator of $\mathbb{Z}/6\mathbb{Z}$ with ψ_2. We have six nontrivial cyclic subgroups of Dic_3: $\langle -\mathrm{Id} \rangle$ of order 2, $\langle \phi_2 \rangle$, of order 3, the subgroups $\langle \tau_2 \rangle$, $\langle \tau_2\phi_2 \rangle = \langle \tau_2^3\phi_2 \rangle$, and $\langle \tau_2\phi_2^2 \rangle = \langle \tau_2^3\phi_2^2 \rangle$ of order 4, and $\langle -\phi_2 \rangle = \langle -\phi_2^2 \rangle$ of order 6. We also have three nontrivial cyclic subgroups of $\langle \psi_2 \rangle$, that are $\langle \psi_2 \rangle$, $\langle \psi_2^2 \rangle$, $\langle \psi_2^3 \rangle$. In addition, we have two other cyclic subgroups of $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$ that are isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/2\mathbb{Z}$, which are $\langle \phi_2, \psi_2^3 \rangle$ and $\langle -\mathrm{Id}, \psi_2^2 \rangle$, and three subgroups isomorphic to $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, i.e. $\langle \tau_2, \psi_2^2 \rangle$, $\langle \tau_2\phi_2, \psi_2^2 \rangle$ and $\langle \tau_2\phi_2^2, \psi_2^2 \rangle$. Finally, we have the trivial subgroup $\langle \mathrm{Id} \rangle$. Thus $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$ has 15 cyclic subgroups and $s \leqslant 15$. In particular, if $[k_7 : k] = 72$, then G has exactly 15 cyclic subgroups and in this case the bound $s = 15$ is sharp.

□

3.7.2 Remarks on modular curves

In this subsection, we are going to deduce some information about CM points on modular curves by the results produced about the fields k_7. Firstly, we recall some well-known definitions concernings modular curves and CM points.

Let $\mathcal{H}$ be the complex upper half plane $\{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ via the Möbius trasformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d} \, .$$

We denote a congruence group by Γ, that is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing the **principal congruence group of level** m

$$\Gamma(m) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{m} \right\},$$

for some positive integer m. When m is minimal, the congruence group is said to be **of level** m. Important congruence groups of level m are

$$\Gamma_0(m) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{m} \right\}$$

and

$$\Gamma_1(m) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{m} \right\}.$$

The quotient $\mathcal{H}/\Gamma$ of $\mathcal{H}$ by the action of Γ, with the analytic structure induced by $\mathcal{H}$, is a Riemann surface, that is denoted by Y_Γ. The modular curve X_Γ is the compactification of Y_Γ by the addition of a finite number of cusps, that are the rational points corresponding to the orbits of $\mathbb{P}^1(\mathbb{Q})$ under Γ. The modular curves associated to the groups $\Gamma(m)$, $\Gamma_0(m)$ and $\Gamma_1(m)$ are denoted respectively by $X(m)$, $X_0(m)$ and $X_1(m)$. They are moduli spaces of families of elliptic curves with an extra structure of level m as follows (for further details see for example [KM85], [Kna92] and [Shi71]).

(i) Non cuspidal points in $X_0(m)$ correspond to pairs $(\mathcal{E}, C_m)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and C_m is a cyclic subgroup of $\mathcal{E}[m]$ of order m;

(ii) non cuspidal points in $X_1(m)$ correspond to pairs $(\mathcal{E}, P)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and P is a point of order m;

(iii) non cuspidal points in $X(m)$ correspond to triples $(\mathcal{E}, P, Q)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and P, Q are points of order m generating $\mathcal{E}[m]$.

A **CM point** on a modular curve is a point which corresponds to an elliptic curve with complex multiplication. For every modular curve X, we denote by $X(k)_{CM}$ the set of its k–rational CM points.

From what we have shown in the previous sections we can deduce the following facts (see in particular Theorem 3.4.1).

Proposition 3.7.3. *Let k be a number field. Let δ_j and P_j be as in Section 3.4, for $1 \leqslant j \leqslant 8$, and let $\mathcal{E}_{2,j,\gamma} : y^2 = x^3 + c_{j,\gamma}$, with $c_{j,\gamma} := \delta_j^2(\delta_j+1)^3\gamma^6$, for some $\gamma \in \mathbb{Q}$. If $\mathbb{Q}(\zeta_3, \zeta_7) \subseteq k$, then*

(i) the pairs $(\mathcal{E}_{2,j,\gamma}, P_j)$, $(\mathcal{E}_{2,j,\gamma}, \langle P_j \rangle)$, with $1 \leqslant j \leqslant 8$, define k–rational CM points on $X_1(7)$ and, respectively, on $X_0(7)$;

(ii) the triples $(\mathcal{E}_{2,j,\gamma}, P_j, \phi_2(P_j))$, with $1 \leqslant j \leqslant 8$, define k–rational CM points on $X(7)$.

In particular $X_0(7)(k)_{CM}$, $X_1(7)(k)_{CM}$ and $X(7)(k)_{CM}$ are nonempty.

Proof. If $1 \leqslant j \leqslant 6$, then $c_{j,\gamma}, \sqrt[3]{\delta_j c_{j,\gamma}}, \sqrt{\delta_j c_{j,\gamma}} \in \mathbb{Q}(\zeta_3, \zeta_7)$. Since $\mathbb{Q}(\zeta_3, \zeta_7) \subseteq k$, then the pairs $(\mathcal{E}_{2,j,\gamma}, P_j)$ and $(\mathcal{E}_{2,j,\gamma}, \langle P_j \rangle)$, for $1 \leqslant j \leqslant 6$, define k–rational CM points of $X_1(7)$ and, respectively, of $X_0(7)$. Furthermore, the triples $(\mathcal{E}_{2,j,\gamma}, P_j, \phi_2(P_j))$ define k–rational CM points on $X(7)$. If $j \in \{7, 8\}$, then $c_{j,\gamma} \in \mathbb{Q}(\zeta_3)$. We also have that $\sqrt[3]{\delta_j c_{j,\gamma}} = \delta_j(\delta_j + 1)\gamma^2$ lies in $\mathbb{Q}(\zeta_3)$ and $\sqrt{\delta_j c_{j,\gamma}} = \delta_j(\delta_j + 1)^2\gamma^3$ lies in $\mathbb{Q}(\zeta_3)$. Since $\mathbb{Q}(\zeta_3, \zeta_7) \subseteq k$, we have that the pairs $(\mathcal{E}_{2,j,\gamma}, P_j)$ and $(\mathcal{E}_{2,j,\gamma}, \langle P_j \rangle)$ define k–rational CM points of $X_1(7)$ and, respectively, of $X_0(7)$. Furthermore, the triples $(\mathcal{E}_{2,j,\gamma}, P_j, \phi_2(P_j))$ define k–rational CM points on $X(7)$. □

Moreover, from the results proved in Section 3.1 and Section 3.4, we can immediately deduce the following two propositions.

Proposition 3.7.4. *Let k be an extension of $\mathbb{Q}(i, \zeta_7)$. Let $\mathcal{E}_1 \in \mathcal{F}_1$ and let $P \in \mathcal{E}_1[7]$ such that $\{P, iP\}$ is a generating set of $\mathcal{E}_1[7]$. Then*

(i) the pair $(\mathcal{E}_1, \langle P \rangle)$ defines a non-cuspidal k–rational CM point of $X_0(7)$ if and only if $y(P) \in k$;

(ii) the pair $(\mathcal{E}_1, P)$ defines a non-cuspidal k–rational CM point of $X_1(7)$ if and only if $y(P) \in k$;

(iii) the triple $(\mathcal{E}_1, P, iP)$ defines a non-cuspidal k–rational CM point of $X(7)$ if and only if $y(P) \in k$.

Proposition 3.7.5. *Let k be an extension of $\mathbb{Q}(\zeta_3, \zeta_7)$. Let $\mathcal{E}_2 \in \mathcal{F}_2$ and let $P \in \mathcal{E}_2[7]$ such that $\{P, \phi_2(P)\}$ is a generating set of $\mathcal{E}_2[7]$. Then*

(i) the pair $(\mathcal{E}_2, \langle P \rangle)$ defines a non-cuspidal k–rational CM point of $X_0(7)$ if and only if $y(P) \in k$;

(ii) the pair $(\mathcal{E}_2, P)$ defines a non-cuspidal k–rational CM point of $X_1(7)$ if and only if $y(P) \in k$;

(iii) the triple $(\mathcal{E}_2, P, \phi_2(P))$ defines a non-cuspidal k–rational CM point of $X(7)$, if and only if $y(P) \in k$.

Bibliography

[ACP24] J. Alessandrì, R. Chirivì, and L. Paladino. "Local-global divisibility on algebraic tori". *Bulletin of the London Mathematical Society* 56 (2) (2024), pp. 803–816. URL: https://doi.org/10.1112/blms.12966.

[AP23] J. Alessandrì and L. Paladino. "On 7-division fields of CM elliptic curves". *European Journal of Mathematics* 9 (51) (2023). URL: https://doi.org/10.1007/s40879-023-00643-y.

[AT67] E. Artin and J. T. Tate. *Class field theory*. Vol. 366. American Mathematical Soc., 1967.

[Ban04] A. Bandini. "Three-descent and the Birch and Swinnerton-Dyer conjecture". *The Rocky Mountain Journal of Mathematics* (2004), pp. 13–27.

[BP12] A. Bandini and L. Paladino. "Number fields generated by the 3-torsion points of an elliptic curve". *Monatshefte für Mathematik* 168 (2) (2012), pp. 157–181.

[BP16] A. Bandini and L. Paladino. "Fields generated by torsion points of elliptic curves". *Journal of Number Theory* 169 (2016), pp. 103–133.

[Cas62] J.W.S. Cassels. "Arithmetic on Curves of Genus 1. IV. Proof of the Hauptvermutung". *Journal für die reine und angewandte Mathematik* 211 (1962), pp. 95–112.

[ÇS15] M. Çiperiani and J. Stix. "Weil–Châtelet divisible elements in Tate–Shafarevich groups II: On a question of Cassels". *Journal für die reine und angewandte Mathematik (Crelles Journal)* 2015 (700) (2015), pp. 175–207.

[Col88] J.-L. Colliot-Thélene. "Surfaces rationnelles fibrées en coniques de degré 4". *Séminaire de théorie des nombres, Paris* 1989 (91) (1988), p. 1990.

[CS21] J.-L. Colliot-Thélène and A. N. Skorobogatov. *The Brauer-Grothendieck group*. Vol. 71. Springer, 2021.

[Cre13] B. Creutz. "Locally trivial torsors that are not Weil–Châtelet divisible". *Bulletin of the London Mathematical Society* 45 (5) (2013), pp. 935–942.

[Cre16] B. Creutz. "On the local-global principle for divisibility in the cohomology of elliptic curves". *Mathematical Research Letters* 23 (2) (2016), pp. 377–387.

[CL23] B. Creutz and S. Lu. "The local-global principle for divisibility in CM elliptic curves". *J. Number Theory* 250 (2023), pp. 139–154.

[DP22a] R. Dvornicich and L. Paladino. "Local-global questions for divisibility in commutative algebraic groups". *European Journal of Mathematics* 8 (Suppl 2) (2022), pp. 599–628.

[DP22b] R. Dvornicich and L. Paladino. "On the division fields of an elliptic curve and an effective bound to the hypotheses of the local-global divisibility". *International Journal of Number Theory* 18 (7) (2022), pp. 1567–1590.

[DZ01] R. Dvornicich and U. Zannier. "Local-global divisibility of rational points in some commutative algebraic groups". *Bulletin de la Société Mathématique de France* 129 (3) (2001), pp. 317–338.

[DZ04] R. Dvornicich and U. Zannier. "An analogue for elliptic curves of the Grunwald–Wang example". *C. R. Acad. Sci. Paris* 338 (1) (2004), pp. 47–50.

[DZ07] R. Dvornicich and U. Zannier. "On a local-global principle for the divisibility of a rational point by a positive integer". *Bulletin of the London Mathematical Society* 39 (1) (2007), pp. 27–34.

[GR17] F. Gillibert and G. Ranieri. "On the local–global divisibility of torsion points on elliptic curves and GL_2-type varieties". *Journal of Number Theory* 174 (2017), pp. 202–220.

[GR18] F. Gillibert and G. Ranieri. "On the local-global divisibility over abelian varieties". In: *Annales de l'Institut Fourier*. Vol. 68. 2. 2018, pp. 847–873.

[GR20] F. Gillibert and G. Ranieri. "On local-global divisibility over GL_2-type varieties". *Acta Arithmetica* 193 (2020), pp. 339–354.

[GL16] E. González–Jiménez and Á. Lozano-Robledo. "Elliptic curves with abelian division fields". *Mathematische Zeitschrift* 283 (2016), pp. 835–859.

[Ill08] M. Illengo. "Cohomology of integer matrices and local-global divisibility on the torus". *Journal de théorie des nombres de Bordeaux* 20 (2) (2008), pp. 327–334.

[KM85] N.M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*. Annals of Math. Studies 108. Princeton University Press, 1985.

[Kna92] A. W. Knapp. *Elliptic curves*. Vol. 40. Princeton University Press, 1992.

[Mac13] S. Mac Lane. *Categories for the Working Mathematician*. 2nd ed. Vol. 5. Graduate Texts in Mathematics. Springer, 2013.

[Mer96] L. Merel. "Bornes pour la torsion des courbes elliptiques sur les corps de nombres". *Inventiones mathematicae* 124 (1) (1996), pp. 437–450.

[Mil17] J. S. Milne. *Algebraic groups: the theory of group schemes of finite type over a field*. Vol. 170. Cambridge University Press, 2017.

[Mil08] James S. Milne. *Abelian Varieties*. Available at www.jmilne.org/math/. 2008.

[Min87] H. Minkowski. "Zur Theorie der positiven quadratischen Formen". *Journal für die reine und angewandte Mathematik* 101 (3) (1887), pp. 196–202.

[Mum74] D. Mumford. *Abelian varieties*. 2nd ed. Studies in Mathematics 5. Published for the Tata Institute of Fundamental Research, Oxford University Press, 1974.

[Ono61] T. Ono. "Arithmetic of algebraic tori". *Annals of Mathematics* (1961), pp. 101–139.

[Pal10] L. Paladino. "Elliptic curves with $\mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9". *Journal de théorie des nombres de Bordeaux* 22 (1) (2010), pp. 139–160.

[Pal11] L. Paladino. "On counterexamples to local-global divisibility in commutative algebraic groups". *Acta Arithmetica* 148 (1) (2011), pp. 21–29.

[Pal18] L. Paladino. "On 5–torsion of CM elliptic curves". *Riv. Mat. Univ. Parma* 9 (2018), pp. 329–350.

[Pal19] L. Paladino. "Divisibility questions in commutative algebraic groups". *Journal of Number Theory* 205 (2019), pp. 210–245.

[PRV12] L. Paladino, G. Ranieri, and E. Viada. "On local–global divisibility by pn in elliptic curves". *Bulletin of the London Mathematical Society* 44 (4) (2012), pp. 789–802.

[PRV14] L. Paladino, G. Ranieri, and E. Viada. "On the minimal set for counterexamples to the local–global principle". *Journal of Algebra* 415 (2014), pp. 290–304.

[PR93] V. Platonov and A. Rapinchuk. *Algebraic groups and number theory*. Academic press, 1993.

[Reb03] M. Rebolledo Hochart. "Corps engendré par les points de 13–torsion des courbes elliptiques". *Acta Arithmetica* 109 (2003), pp. 219–230.

[Roq06] P. Roquette. *The Brauer-Hasse-Noether Theorem in Historical Perspective*. Vol. 15. Schriften der Mathematisch-naturwissenschaftlichen Klasse. Springer Berlin, 2006.

[SS91] P. Salberger and A. N. Skorobogatov. "Weak approximation for surfaces defined by two quadratic forms". *Duke Mathematical Journal* 63 (2) (1991), pp. 517–536.

[SS04] E. Schaefer and M. Stoll. "How to do a p-descent on an elliptic curve". *Transactions of the American Mathematical Society* 356 (3) (2004), pp. 1209–1231.

[Sco87] W. R. Scott. *Group Theory*. Dover, 1987.

[Ser61] J.-P. Serre. "Rigidité du foncteur de Jacobi d'échelon $n \geqslant 3$". *Appendice a l'exposé 17 du Seminaire Cartan* (1961).

[Ser72] J.-P. Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques". *Invent. math* 15 (1972), pp. 259–331.

[Ser12] J.-P. Serre. *Algebraic groups and class fields*. Vol. 117. Graduate Texts in Mathematics. Springer New York, 2012.

[Sha17] D. Sharma. "Locally indecomposable Galois representations with full residual image". *International Journal of Number Theory* 13 (05) (2017), pp. 1191–1211.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Vol. 1. Princeton University Press, 1971.

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer, 1994.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. 2nd ed. Vol. 106. Graduate Texts in Mathematics. Springer, 2009.

[Spr94] T. A. Springer. "Linear Algebraic Groups". In: *Algebraic Geometry IV: Linear Algebraic Groups Invariant Theory*. Ed. by A. N. Parshin and I. R. Shafarevich. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994.

[Tro34] E. Trost. "Zur theorie des Potenzreste". *Nieuw Arch. Wiskunde* 18 (1934), pp. 58–61.

[Vos98] V.E. Voskresenskii. *Algebraic groups and their birational invariants*. Vol. 179. American Mathematical Soc., 1998.

[Wan50] S. Wang. "On Grunwald's theorem". *Annals of Mathematics* 51 (2) (1950), pp. 471–484.

[Wat12] W. C. Waterhouse. *Introduction to affine group schemes*. Vol. 66. Graduate Texts in Mathematics. Springer New York, 2012.

[Wei82] A. Weil. *Adeles and Algebraic Groups*. Vol. 23. Progress in Mathematics. Birkhäuser, 1982.

[Won00] S. Wong. "Power residues on abelian varieties". *manuscripta mathematica* 102 (2000), pp. 129–137.

[Yel17] J. Yelton. "A note on 8–division fields of elliptic curves". *European Journal of Mathematics* 3 (2017), pp. 603–613.