UNIVERSITY OF UDINE

SCHOOL OF ADVANCED STUDIES OF TOPPO WASSERMANN

Master's degree in Mathematics

Discrete log–cryptography and twisting commutative algebraic groups

Supervisor:
Prof. Mario Mainardis

Presented by:
Nicola Dal Cin

ACADEMIC YEAR 2021 – 2022

Contents

Notation

Here is a summary of the most common notations and conventions used throughout this work.

- The nonzero elements of $\mathbb{Z}_p$, and $\mathbb{F}_p$ are respectively denoted by $\mathbb{Z}_p^\times$, and $\mathbb{F}_p^\times$.
- When finite fields are considered, the characteristic is different from 2.
- Let $x \in \mathbb{R}$, the smallest integer grater than x is $\lceil x \rceil$, while the bigger integer less than x is $\lfloor x \rfloor$.
- The Euler totient function is indicated by $\varphi(\cdot)$.
- If the element a is randomly chosen from the set X, we will write $a \in_R X$.
- Let G be a group acting on X by conjugation, we adopt the exponential notation, i.e. the action of $g \in G$ over $x \in X$ is x^g.
- If R is a commutative ring, and G a finite group, we denote the *group ring* as $R[G] := \{\sum_{g \in G} a_g g \mid a_g \in R\}$.
- We use $\Phi_d(x) \in \mathbb{Z}[x]$ to indicate the cyclotomic polynomial whose complex roots are the primitive d–roots of unity.
- If d is a positive divisor of N, we denote

$$\Psi_{n,d}(x) := \frac{x^n - 1}{\Phi_d(x)} \in \mathbb{Z}[x],$$

  and

$$\Psi_d(x) := \Psi_{d,d} = \frac{x^d - 1}{\Phi_d(x)} \in \mathbb{Z}[x].$$

- Let R be a ring, while M and N respectively a right and left R– module; we denote $M \otimes_R N$ the *tensor product* of M and N.

Chapter 1

Introduction

In this work, we recall a few basic concepts about cryptography, such as the definition of a cryptosystem, and the difference between private and public–key encryption. We will then focus on the latter, in particular on discrete log–cryptosystems. The former example is the system introduced by Taher Elgamal in 1985, which is indeed based on the difficulty of finding the logarithm modulo a prime in polynomial time. In particular, we prove how the security of *El Gamal cryptosystem* also depends on the choice of the chosen prime p (in particular on $(p-1)$ factorization).

Discrete log problem can be formulated in an analog guise for a generic group; following Elgamal's construction leads to a generalization of the former case which keeps the denomination of *discrete log–cryptography*.

We conclude Chapter 2 with a particular example of a discrete log–cryptosystem that arises by choosing, as the group in the above–mentioned definition, an elliptic curve over a finite field. The *Elliptic Curve Cryptosystem* (ECC) is, actually, one of the most used (e.g. in Bitcoin signatures), and therefore of big interest in modern research.

There are also recent examples of discrete log–cryptosystems defined over an abelian variety, in particular over the $\mathbb{F}_q$–points of the variety (e.g. the multiplicative group $\mathbf{G_m}$).

It is then interesting, also in order to study the security of the system, the study of its algebraic structure. We will see how this leads to the definition of a *primitive subgroup* of an algebraic group.

More explicitly, considering V, an algebraic group over k, the algebraic variety obtained with the Weil restriction of scalars of V from L to k (where L is a finite abelian extension of k) is isogenous to the direct sum of primitive subgroups of V. In other words, the security of a cryptosystem defined on V actually relies on the security of the restriction in those subgroups.

Chapter 2

Cryptography bases

In this chapter we introduce a few basic concepts concerning cryptography, with the seek of giving a general understanding of the topic, and without the pretense of being either self contained or complete (for further readings see [1]).

After giving the definition of a cryptosystem, we briefly talk about the difference of symmetric ones respect to the asymmetric. Then, we concentrate on the latter case (the more interesting, especially nowadays), and in particular on examples of discrete log–based cryptosystems. These particular cases are widely studied for themselves, because of their wide application. However, at present are being studied some generalizations which use advanced abstract algebra (and not only). In this work we will present an example that relies on primitive subgroups of an algebraic group.

2.1 Basics definitions

Suppose Alice and Bob are two friends who want to communicate through a (public) channel[1], but ensure that their secret are safe from an evil Eve who can possibly intercept the message they shared.

The natural method they can adopt is to agree on an invertible procedure to convert their messages into other strings, and send the latter in the channel. This lead to:

Definition 2.1.1. A **cryptosystem** is a tuple $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, e, d)$ where:

- $\mathcal{X}$ is a finite set of **plaintexts**;
- $\mathcal{Y}$ is a finite set of **ciphertexts**;
- $\mathcal{K}$ is a finite set of **keys**;
- $e = \{e_k : \mathcal{X} \to \mathcal{Y}\}_{k \in \mathcal{K}}$ is a family of **encryption maps**;
- $d = \{d_k : \mathcal{X} \to \mathcal{Y}\}_{k \in \mathcal{K}}$ is a family of **decryption maps**;

such that for all $k \in \mathcal{K}$

$$d_k(e_k(x)) = x. \tag{2.1}$$

[1] More precisely, a channel that could be eavesdropped, but in which the receiver always knows, with certainty, who sent a message.

In practical cases the sets considered are often numerical ones, those are put in correspondence with strings by opportune functions.

Example 2.1.1. (Hill cryptosystem) Take for instance $\mathcal{H} = (\mathcal{X}, \mathcal{Y}, \mathcal{K}, e, d)$ of the form: $\mathcal{X} = \mathcal{Y} = (\mathbb{Z}_n)^m$, the keys $K = GL_m(\mathbb{Z}_n)$, i.e. the general linear group of $m \times m$ matrices which are invertible modulo n, $e_k(x) = k \cdot x$, and $d_k(y) = k^{-1} \cdot y$.

2.1.1 Private–key cryptosystems

A crucial step in the above procedure, is sharing the key (or the keys) before beginning the communication. If the exchange is done privately (e.g. in person) before, the cryptosystem adopted is a **private–key** one, and is also said **symmetric**.

It is know that, provided choosing a suitable key–set, a symmetric system is perfectly secure, i.e. there are no attacks that Eve can attempt only based on knowing the ciphertext (this is why symmetric cryptosystems are also employed in military framework). Despite not being a central topic in this work, and therefore can be ignored, the proof of this classical result is discussed in the next subsection.

Shannon's theorem

In this section we consider a probabilistic experiment defining X and K, two independent random variables with values respectively in $\mathcal{X}$ and $\mathcal{K}$, i.e.

$$P(X = x \wedge K = k) = P(X = x)P(K = k). \tag{2.2}$$

Notice that these two random variables defines a third one, namely $Y := e(K, X) : \Omega \to \mathcal{Y}$. Moreover, we will assume $P(X = x) > 0$ and $P(Y = y) > 0$. Since

$$P(Y = y \mid X = x) = P(K \in \{k : e_k(x) = y\}) \tag{2.3}$$

we have

$$P(Y = y) = \sum_{x \in \mathcal{X}} P(Y = y \wedge X = x) = \sum_{x \in \mathcal{X}} P(Y = y \mid X = x)P(X = x) \tag{2.4}$$

$$= \sum_{x \in \mathcal{X}} P(K \in \{k : e_k(x) = y\})P(X = x). \tag{2.5}$$

Definition 2.1.2. A cryptosystem is said **Shannon perfectly secure** if X and Y are independent, i.e.

$$P(X = x \mid Y = y) = P(X = x). \tag{2.6}$$

In other words, the perfect security we can aspire to is finding an encryption method which leads to a ciphertext that doesn't reveal anything about the original secret.

Theorem 2.1.1. Let $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, e, d)$ be a cryptosystem such that $|\mathcal{X}| = |\mathcal{Y}| = |\mathcal{K}|$, let's consider the above probabilistic experiment, and assume

- X and K are independent,
- $P(Y = y) > 0$ for all $y \in \mathcal{Y}$.

Then the cryptosystem is perfectly secure if and only if

(i) For all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $\exists! k$ such that $e_k(x) = y$, (we denote it as k_{xy}).

(ii) $P(K = k) = 1/|\mathcal{K}|$.

Proof. First of all, notice that (i) implies

$$k_{xy} = k_{x'y'} \iff \text{either } x = x' \wedge y = y' \text{ or } x \neq x' \wedge y \neq y'. \tag{2.7}$$

($\Leftarrow$) Let's verify the definition

$$P(X = x \mid Y = y) = \frac{P(X = x \wedge Y = y)}{P(Y = y)} \overset{(2.5)}{=} \frac{P(X = x \wedge K \in \{k : e_k(x) = y\})}{\sum_{x' \in \mathcal{X}} P(K \in \{k : e_k(x') = y\}) P(X = x')} \tag{2.8}$$

$$\overset{(2.2)}{=} \frac{P(X = x)P(K = k_{xy})}{\sum_{x' \in \mathcal{X}} P(K = k_{x'y}) P(X = x')} \overset{(i)}{=} \frac{P(X = x) 1/|\mathcal{K}|}{1/|\mathcal{K}| \cdot \sum_{x' \in \mathcal{X}} P(X = x')} \tag{2.9}$$

$$= P(X = x). \tag{2.10}$$

($\Rightarrow$) Fix and x and notice that for all $y \in \mathcal{Y}$

$$0 < P(Y = y) \overset{\text{ind}}{=} P(Y = y \mid X = x) \overset{(2.3)}{=} P(K \in \{k : e_k(x) = y\}), \tag{2.11}$$

so for all x and y the set $\{k : e_k(x) = y\} \neq \emptyset$. We deduce that for each x the functions

$$f_x : \mathcal{K} \to \mathcal{Y} \tag{2.12}$$

$$k \mapsto y := e_k(x) \tag{2.13}$$

are surjective and, since $|\mathcal{K}| = |\mathcal{Y}|$, also injective, i.e. we have proved (i).

(i) implies $\{k : e_k(x) = y\} = \{k_{xy}\}$ for all (x, y), moreover from above follows that

$$P(K = k_{xy}) = P(K = k_{x'y}) = P(Y = y) > 0, \quad \text{for all } x, x' \in \mathcal{X} \tag{2.14}$$

and so, fixing y and using (2.7), we have:

$$k_{xy} = k_{x'y} \Leftrightarrow x = x', \tag{2.15}$$

and so the function $g_y : \mathcal{X} \to \mathcal{K}$ s.t. $g_y(x) = k_{xy}$ is injective (and also bijective).

We deduce

$$1 = \sum_{x \in \mathcal{X}} P(X = x) = \sum_{x \in \mathcal{X}} P(X = x \mid Y = y) = \sum_{x \in \mathcal{X}} P(K = g_y(x)) = \tag{2.16}$$

$$= \sum_{x \in \mathcal{X}} P(K = k_{xy}) = |X| P(Y = y) \tag{2.17}$$

and, since $|\mathcal{X}| = |\mathcal{K}|$, we can conclude

$$P(K = k) = P(Y = y) = 1/|\mathcal{K}|. \tag{2.18}$$

□

2.1.2 Public–key cryptosystems

In the years, modern practical applications required the possibility to privately communicate (e.g. by email or WhatsApp) with people without sharing symmetrically a private key before.

The problem was solved by Diffie and Hellman who proposed the following DH–scheme [2], based on the assumption that there are certain algebraic functions and problems (see appendix A for basic definitions) that are computationally easy to solve, but their inverse is not.

The DH–scheme uses two keys (a private and a public one) that are mathematically related to each other. The strength of security lies in these keys' properties since it is computationally infeasible to calculate one key using the other. Each sender and receiver will have their private-public key pair in this system.

More explicitly, if Alice wants to send a message to Bob, she will need to use his public key to encrypt the message, and Bob will decrypt the message using his private key. In practice, when we communicate only, we share a key in a asymmetric way and then we use the latter to continue the encryption symmetrically.

A rigorous definition of the above procedure is the following:

Definition 2.1.3. The family $\{\mathcal{X}, \mathcal{Y}, \mathcal{K}, e, d, u, \mathcal{U}\}$ is an **asymmetric cryptosystem with security parameter** $\eta = |\theta|$ if

(i) $u : \mathcal{K} \to \mathcal{U}$ is a PT publication function $u(k)$, called **public key of** k.

(ii) The family $\{e_{u(k)} : \mathcal{X} \to \mathcal{Y}\}_\theta$ is a one–way family with trapdoor k.

(iii) $d_k(e_{u(k)}(x)) = x$ for all $x \in \mathcal{X}$.

(iv) it should be efficient to sample $\mathcal{K}$ as $|\theta|$ grows.

The fourth condition imposes that it should be easy to sample a random key for each parameter θ.

Example 2.1.2 (RSA). The following system is widely adopted and known; it is based on the hardness of finding the square roots modulo $\theta = n = pq$, with p and q large primes. It is easy to show, indeed, that this problem is as difficult as factoring n.

Taking $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$, $\mathcal{K} = \{(a, b) : ab = 1 \mod \varphi(n) = (p-1)(q-1)\}$, $u(a, b) = a$, and

$$e_a(x) = x^a \mod n, \quad \text{and} \quad d_{(a,b)}(y) = y^b \mod n \tag{2.19}$$

The idea is simply using the fact $\mathbb{Z}_{pq} = \mathbb{Z}_p \times \mathbb{Z}_q$ and so

$$x = (a, b) = 0 \mod n = pq \iff a = 0 \mod p, \quad \text{and} \quad b = 0 \mod q. \tag{2.20}$$

2.2 Discrete log–cryptography

Now, we focus on a particular class of public–key cryptosystems, which takes inspiration by El Gamal, who first introduced a scheme based on the hardness of finding the discrete logarithm modulo a large prime. We will first look at this remarkable example, and then see an analog problem related to elliptic curves.

2.2.1 El Gamal system

It is well known, and also easy to show, that the following problem is, in general, in the $\mathcal{NP}$ class. In fact, it has been showed that for a lot of primes it is actually in $\mathcal{P}$.

Problem 2.2.1. Let p be a prime, α a generator of $\mathbb{Z}_p^\times$ and $\beta \in \mathbb{Z}_p^\times$. Find $0 \leq a \leq p-2$ such that

$$\alpha^a = \beta \mod p. \tag{2.21}$$

As anticipated, the security of the following one is based on the (assumed) hardness of problem 2.2.1.

Definition 2.2.1. Let p be a prime for which the discrete log problem is hard (e.g. $p = 2q+1$ with q a large prime) and α a public known primitive element of $\mathbb{Z}_p^\times$. The **El Gamal cryptosystem** is defined taking

- $\mathcal{X} = \mathbb{Z}_p^\times$ (plaintext space);
- $\mathcal{Y} = \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$ (ciphertext space);
- $\mathcal{K} = \{(a, \beta) : \alpha^a = \beta\}$ (key space)
- $u : \mathcal{K} \to \mathbb{Z}_p^\times$ with $u(a, \beta) = \beta$ the publication map;
- $e_\beta(x) = (y_1, y_2) := (\alpha^r \mod p\ ,\ x\beta^r \mod p)$ where $r \in_R \mathbb{Z}_{p-1}$ is randomly taken;
- $d_{(a,\beta)}(y_1, y_2) = y_2(y_1^a)^{-1} \mod p$.

The above condition on the prime p, follows from various attacks that Eve can attempt, in particular trying to factor $p - 1$. In the following subsection we present an example of attack, which offers a connection with a more general case that we will encounter in Chapter 3.

Pohlig–Hellman theorem

The key observation to perform the following attack is that if $p - 1$ is a product of prime which are "small enough", then El Gamal is vulnerable since we can compute the logarithm in the single p–groups (see proof below for the algorithm). This also motivate the following:

Definition 2.2.2. A number is said to be **n–smooth** if the prime number in its decomposition are not larger that n.

Theorem 2.2.1 (Pohlig–Hellman)**.** If p is a prime such that $(p-1)$ is $O(\text{polylog}(p))$ – smooth[2], then there is a polynomial algorithm to compute the discrete log of p.

Proof. Given (α, β) we want to compute $a = \log_\alpha \beta \mod p$, with p prime, and $p - 1 = \prod_{i=1}^s q_i^{e_i}$ (with q_i polylog bounded). Notice that $a \in \mathbb{Z}_{p-1} \cong \mathbb{Z}_{q_1^{e_1}} \times \cdots \times \mathbb{Z}_{q_s^{e_s}}$, so it's enough to determine $a \mod q_i^{e_i}$ for $i = 1, \ldots, s$.

Fix a i, by hypothesis $e_i \in O(\log p)$ and $q_i \in O(\text{polylog}(p))$. Moreover, since $p - 1 = 0 \mod q_i^{e_i}$ and so we can write $a \mod q_i^{e_i}$ in base q_i with at most e_i symbols:

$$a \mod q_i^{e_i} = [a_{e_i-1} \cdots a_1 a_0]_{q_i} = \sum_{j=1}^{e_i-1} a_j q_i^j, \tag{2.22}$$

Lemma 2.2.1. We have that a_0 is the element that satifies $\beta^{(p-1)/q_i} = \alpha^{(p-1)a_0/q_i} \mod p$.

Proof. Modulo p we have

$$\beta^{(p-1)/q_i} = \alpha^{\left(dq_i^{e_i} + \sum_{j=0}^{e_i-1} a_j q_i^j\right)(p-1)/q_i} = \alpha^{\left(dq_i^{e_i-1} + \sum_{j=1}^{e_i-1} a_j q_i^{j-1}\right)(p-1)} \alpha^{\frac{p-1}{q_i} a_0} = 1 \cdot \alpha^{\frac{p-1}{q_i} a_0}. \tag{2.23}$$

□

[2]We write polylog(x) to indicate a polynomial evaluated in $\log x$.

So to determine a_0 it is sufficient to check the equality above for $a \in \{0, \dots, q-2\}$, remember that the Power Mod can be computed in PT. Found a_0, it's sufficient to subtract a_0 from a mod $q_i^{e_i}$ and then divide by q_i to apply recursively the lemma above. To compute the overall complexity, notice

1) the number of primes s is clearly $O(\log(p))$.

2) Each $e_i \in (\log(p))$.

3) By hypothesis $q_i \in O(\text{polylog}(p))$ as $p-1$ is polylog smooth.

So the overall complexity is polynomial in the number of bits of p. □

Remark 2.2.1. Notice that the above algorithm uses the fact that we can consider the singles q_i–groups to compute the discrete log. Thus, in this sense, we can say that the security of the system depends on the dimension of those groups.

2.2.2 Elliptic curves discrete log problem

A natural generalization of El Gamal cryptosystem is the following:

Definition 2.2.3. Let $(G, \cdot)$ be a commutative group such that H is a cyclic subgroup with order n, and generator α. We take

- $\mathcal{X} = G$ (plaintext space);
- $\mathcal{Y} = H \times G$ (ciphertext space);
- $\mathcal{K} = \{(a, \beta) : \alpha^a = \beta\} \subset \mathbb{Z}_n \times H$ (key space)
- $u : \mathcal{K} \to H$, where $u(a, \beta) = \beta$ is the publication map;
- $e_\beta(x) = (y_1, y_2)$ with
  - $r \in_R \mathbb{Z}_n$ is randomly chosen,
  - $y_1 = \alpha^r$, and $y_2 = x\beta^r$.
- $d_{(a,\beta)}(y_1, y_2) = y_2(y_1^a)^{-1} \mod p$.

Now, since the following problem is considered to be hard, elliptic curves are a natural candidate for a cryptosystem of this guise.

Problem 2.2.2. (Discrete log problem for elliptic curves) Let $(E, +)$ be an elliptic curve defined over $\mathbb{F}_p$. Let then $P \in E$ be a generator of a large subgroup[3] H in G, given $Q \in H$, find m integer such that $mP = Q$.

Given an elliptic curve E on $\mathbb{F}_p$ (p a large prime), definition 2.2.3 describes the so called **Elliptic curve cryptosystem** or **ECC** (notice that in this case the notation is additive). ECC is widely used in application, for example in the implementation of Bitcoin signature scheme. As in El Gamal example, is proven that problem 2.2.2 is not always in $\mathcal{NP}$, and there are attacks analogue to Pohlig–Hellman's one.

[3] A good introduction to elliptic curves, and in particular a proof that such a cyclic subgroup always exists can be found in [3]

Example 2.2.1. (Diffie–Hellman key agreement) Suppose Alice and Bob want to share a secret using ECC. Let the public parameters of the system be the elliptic curve E, on $\mathbb{F}_p$, and the subgroup generator $P \in E$. Moreover, the two are both given a key, respectively (P, n_A) and (P, n_B), whose first part is public (is actually the generator) and the second is a private and random integer (also said *exponent*).

If they compute respectively points $Q_A := n_A G$, and $Q_B := n_B G$. The secret that they can share (and later possibly use to encrypt their conversation) is the point $S = n_B Q_A = n_A Q_B$. In fact, is sufficient that they send Q_A, and Q_B to each other and multiply what received by their private key. Notice that Bob can't deduce n_A from Q_A (unless solving problem 2.2.2), and vice versa. In particular Eve, even intercepting the messages Q_A and Q_B, has no (obvious) way to find S.

Remark 2.2.2. A point that we haven't stressed in this work, but is crucial, is that the operations in the procedure need to be computationally efficient[4].

[4]If interested, the reader can find here my implementation of ECC in PYTHON (but I suggest to look for better ones).

Chapter 3

Twisting commutative algebraic groups

In the previous chapter we described a few standard examples of discrete log–based cryptography, in particular El Gamal and ECC. Now, we move to a more general framework, what are considered in this setting are $\mathbb{F}_q$–points of the multiplicative group $\mathbf{G_m}$, or the $\mathbb{F}_q$–points of an abelian variety A over $\mathbb{F}_q$ (usually an elliptic curve). Our scope is to show how discrete log-based cryptography over extension fields can be reduced to cryptography in primitive subgroups; this generalization was suggested in [4], and interesting examples were presented in [5].

3.1 Primitive subgroups

Despite applications are of course implemented over finite fields (in particular in the above two cases), it is useful to work in a more general setting. Thus, in this section we will assume that V is a commutative algebraic group over a field k, and L is an abelian extension of k of finite degree n, i.e. $\mathrm{Gal}(L/k)$ is commutative. We will also use some notation introduced in Appendix B.

3.1.1 Weil restriction of scalars

Restriction of scalars is a way to associate an algebraic variety X over L another variety $\mathrm{Res}_{L/k}(X)$ over k[1].

Definition 3.1.1. The **restriction of scalars** of V from L to k is a commutative algebraic group over k, that we denote $Res_{L/k}(V)$, together with a homomorphism over L

$$\eta_{L/k} : \mathrm{Res}_{L/k}(V) \longrightarrow V \tag{3.1}$$

with the universal property that for every variety X over k, the map

$$\begin{aligned} \mathrm{Hom}_k(X, \mathrm{Res}_{L/k}(V)) &\longrightarrow \mathrm{Hom}_L(X, V) \\ f &\longmapsto \eta_{L/k} \circ f \end{aligned} \tag{3.2}$$

is an isomorphism.

[1] Weil restriction of scalars variety actually represents a functor from k–schemes to sets but, for our purposes and consistency, it is convenient to give a more practical definition.

Remark 3.1.1. Notice that for every k–algebra A, by taking $X = \mathrm{Spec}(A)$ in condition (3.2), one finds that $\eta_{L/k} : (\mathrm{Res}_{L/k}(V))(A) \longrightarrow V(A \otimes_k L)$ is an isomorphism. In particular

$$(\mathrm{Res}_{L/k}(V))(k) \cong V(L). \tag{3.3}$$

To clear the above definition, consider the following.

Example 3.1.1. Let's consider V as defined by a system of polynomial equations:

$$f_l(x_1, \ldots, x_r) = 0, \quad f_l \in L[x_1, \ldots, x_r] \text{ for } 1 \leq l \leq s. \tag{3.4}$$

Fixing a basis $\{v_1, \ldots, v_n\}$ of the extension L over k, and introuducing new variables y_{ij} expressing the combinations $x_i = \sum_{j=1}^{n} y_{ij} v_j$, leads to a system of s equations in the rn unknowns $\{y_{ij}\}$. The latter defines a $n \cdot \dim(V)$–dimensional variety over k which is in fact $\mathrm{Res}_{L/k}(V)$.

As anticipated above, the aim of this chapter is to generalize discrete log–based cryptography viewpoint to a more algebraic one. To this scope is convenient to introduce a couple of examples.

The multiplicative group and quadratic extensions

Assume $D \in k^\times$ is a non–square, let $L = k(\sqrt{D})$, and $G = \mathrm{Gal}(L/k)$ with generator σ. One can consider the multiplicative group $\mathbf{G_m}$ as the variety in $\mathbb{A}^2$ defined by the equations $xy = 1$. In this case,

Proposition 3.1.1. $\mathrm{Res}_{L/k}(\mathbf{G_m})$ is the variety R in $\mathbb{A}^3$ defined by $(x_1^2 - Dx_2^2)y = 1$ with the commutative operation

$$(x_1, x_2, y) \cdot_{\mathbf{G_m}} (w_1, w_2, z) = (x_1 w_1 + D x_2 w_2, x_1 w_2 + x_2 w_1, yz). \tag{3.5}$$

Proof. Define $\eta_{L/k} : R \to \mathbf{G_m}$ as

$$(x_1, x_2, y) \mapsto (x_1 + x_2\sqrt{D}, (x_1 - x_2\sqrt{D})y) \tag{3.6}$$

Given X a variety over k and $\psi \in \mathrm{Hom}_L(X, \mathbf{G_m})$ we can define

$$= \left(\frac{\psi + \psi^\sigma}{2}, \frac{\psi - \psi^\sigma}{2\sqrt{D}}, \frac{1}{\psi\psi^\sigma} \right) \in \mathrm{Hom}_k(X, R). \tag{3.7}$$

and also check that $\eta_{L/k} \circ \tilde{\psi} = \psi$. In this case, showing that the map (3.2) is an isomorphism follows from the fact that $\eta_{L/k} \circ f = f$. □

Elliptic curves and quadratic extensions

Suppose $E : y^2 = f(x)$ is an elliptic curve on k, thus $\deg(f) = 3$, and that $D \in k^\times$ is a non–square. As above, let $L = k(\sqrt{D})$, and $G = \mathrm{Gal}(L/k)$ with generator σ.

The **quadratic twist** of E by D is the curve $E^{(D)} : Dy^2 = f(x)$, and the two are isomorphic over L by

$$\begin{aligned} \phi : \quad & E \longrightarrow E^{(D)} \\ & (x, y) \longmapsto (x, y/\sqrt{D}). \end{aligned} \tag{3.8}$$

Proposition 3.1.2. With the above assumptions, $\mathrm{Res}_{L/k}(E)$ is $(E \times E^{(D)})/T$, where

$$T := \{(P, \phi(P) \in E \times E^{(D)} : 2P = O\} = \ker(f_0) \cap \ker([2]), \tag{3.9}$$

where [2] is the multiplication by two in E, and

$$\begin{aligned} f_0 : E \times E^{(D)} &\longrightarrow E \\ (P, Q) &\longmapsto P - \phi^{-1}(Q) \end{aligned} \tag{3.10}$$

In this case $\eta_{L/k} : (P, Q) \mapsto P + \phi^{-1}(Q)$.

3.1.2 Definition of primitive subgroup

We conclude this section giving the definition of a primitive subgroup V_F of V and enunciating some of his properties, whose proofs exile from the scopes of this script and can be find in [4].

As above, L/k is a finite abelian extension of k. Our aim is to associate to each intermediate field F (i.e. $k \subseteq F \subseteq L$) such that F/k is cyclic, a commutative algebraic group V_F over k.

Before giving the definition, we have to describe some context and notations. Let $G := \mathrm{Gal}(L/k)$, if $g \in G$ we have that $\eta_{L/k}^g \in \mathrm{Hom}_L(\mathrm{Res}_{L/k}(V), V)$ and by (3.2) applied to $\mathrm{Res}_{L/k}(V)$, exists a unique $g_{L/k,V} \in \mathrm{End}_k(\mathrm{Res}_{L/k}(V))$ such that $\eta_{L/k} \circ g_{L/k,V} = \eta_{L/k}^g$. Now we have the correspondence $g \mapsto g_{L/k,V}$, which can be linearly extended to a ring homomorphism: writing $\alpha = \sum_{g \in G} a_g\, g$ (with $a_g \in \mathbb{Z}$) and imposing

$$\begin{aligned} \mathbb{Z}[G] &\longrightarrow \mathrm{End}_k(\mathrm{Res}_{L/k}(V)) \\ \alpha &\longmapsto \alpha_{L/k,V} := \sum_{g \in G} a_g\, g_{L/k,V} \end{aligned} \tag{3.11}$$

Considering k–points and identifying $(\mathrm{Res}_{L/k}(V))(k)$ with $V(L)$ as in the remark 3.1.1, if $\alpha = \sum_{g \in G} a_g\, g \in \mathbb{Z}[G]$, and $v \in (\mathrm{Res}_{L/k}(V))(k) \cong V(L)$ then $\alpha_{L/k,V}(v) = \prod_{g \in G} g(x)^{a_g}$.

Example 3.1.2. The map (3.11) is injective if the natural application $\mathbb{Z} \longrightarrow \mathrm{End}_k(V)$ is injective. For instance, taking $V = \mathbf{G_m}$ (or another abelian variety) leads to an injective map, while $V = \ker[n]$ (with $[n]$ the multiplication by n on an elliptic curve) does not.

Now, if $k \subseteq M \subseteq F$, let

$$N_{F/M} := \sum_{h \in \mathrm{Gal}(F/M)} h \quad \in \mathbb{Z}[\mathrm{Gal}(F/M)] \subseteq \mathbb{Z}[\mathrm{Gal}(F/k)]. \tag{3.12}$$

Theorem–Definition 3.1.1. Assume V is a commutative algebraic group over k, F is a field extension of k, and F/k is cyclic. Fix a generator τ of $\mathrm{Gal}(F/k)$, and consider $\Phi_d(\tau), \Psi_d(\tau) \in \mathbb{Z}[\mathrm{Gal}(F/k)]$ and $\Phi_d(\tau)_{F/k,V}, \Psi_d(\tau)_{F/k,V} \in \mathrm{End}_k(\mathrm{Res}_{F/k}(V))$ as above. Then, the following are equivalent conditions and they define a **primitive subgroup** V_F, associated with the field F, of the group V.

(i) $V_F = \ker(\Phi_d(\tau)_{F/k,V}) \subseteq \mathrm{Res}_{F/k}(V)$,

(ii) $V_F = \bigcap_{M \in \Omega_{F/k}} \ker((N_{F/M})_{F/k,V}) = \bigcap_{M \in \Omega'_{F/k}} \ker((N_{F/M})_{F/k,V}) \subseteq \mathrm{Res}_{F/k}(V)$,

(iii) $V_F = \bigcap_{M \in \Omega_{F/k}} \ker(R_{F/M/k,V}) = \bigcap_{M \in \Omega'_{F/k}} \ker(R_{F/M/k,V}) \subseteq \mathrm{Res}_{F/k}(V)$,

(iv) if $F \subseteq L$, with L/k abelian[2], $[L:k] = n$, and $\sigma \in G := \mathrm{Gal}(L/k)$ such that its restriction on $\mathrm{Gal}(F/k)$ is one of its generators, i.e. $\mathrm{Gal}(F/k) = \langle \sigma|_F \rangle$. Then

(a) $V_F = (N_{L/F} \cdot \Psi_d(\sigma))_{L/k,V}(\mathrm{Res}_{L/k}(V)) \subseteq \mathrm{Res}_{F/k}(V)$,

(b) $V_F = \mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V$ (see following sections).

To handle this intricate definition, let's consider our two "quadratic" examples. In this framework (taking $L = F$) we have $d = 2$, $\Phi_d(\sigma) = \sigma + 1 = N_{L/k}$, and $\Psi_d(\sigma) = \sigma - 1$.

Example 3.1.3 ($(\mathbf{G_m})_L$ with quadratic L). Let then $V = \mathbf{G_m}$. The image of σ under the map (3.11) is $\sigma_{L/k,\mathbf{G_m}} \in \mathrm{End}_k(R)$, recalling that $R = \mathrm{Res}_{L/k}(\mathbf{G_m})$ described as before. More explicitly,

$$\sigma_{L/k,\mathbf{G_m}}(x_1, x_2, y) = (x_1, -x_2, y). \tag{3.13}$$

Moreover, after a few calculations, we write

$$\Phi_2(\sigma) = (N_{L/k})_{L/k,\mathbf{G_m}} = (\sigma + 1)_{L/k,\mathbf{G_m}} : R \longrightarrow R \tag{3.14}$$

as

$$\Phi_2(\sigma) : \left(x_1, x_2, \frac{1}{x_1^2 - Dx_2^2}\right) \longmapsto \left(x_1^2 - Dx_2^2, 0, \frac{1}{(x_1^2 - Dx_2^2)^2}\right); \tag{3.15}$$

while $R_{L/k/k,\mathbf{G_m}} : R \longrightarrow \mathbf{G_m}$ is given by

$$R_{L/k/k,\mathbf{G_m}} : \left(x_1, x_2, \frac{1}{x_1^2 - Dx_2^2}\right) \longmapsto \left(x_1^2 - Dx_2^2, \frac{1}{x_1^2 - Dx_2^2}\right), \tag{3.16}$$

and $(N_{L/k} \cdot \Phi_2(\sigma))_{L/k,\mathbf{G_m}} = (\sigma - 1)_{L/k,\mathbf{G_m}} : R \longrightarrow R$ by

$$\left(x_1, x_2, \frac{1}{x_1^2 - Dx_2^2}\right) \longmapsto \left(\frac{x_1^2 + Dx_2^2}{x_1^2 - Dx_2^2}, \frac{-2x_1x_2}{x_1^2 - Dx_2^2}, 1\right). \tag{3.17}$$

Then $(\mathbf{G_m})_L = (\sigma - 1)_{L/k,\mathbf{G_m}}(R) = \ker((\sigma + 1)_{L/k,\mathbf{G_m}})$, and $(\mathbf{G_m})_L$ is the sub–variety[3] of $R \subseteq \mathbb{A}^3$ defined by $x_1^2 - Dx_2^2 = y$. Also, notice that its k–points are the norm one elements of L (viewed as vector space on k).

Example 3.1.4. (Elliptic curve E and quadratic L) Recalling $\mathrm{Res}_{L/k}(E) = (E \times E^{(D)})/T$, one can show $\sigma_{L/k,E} \in \mathrm{End}(E \times E^{(D)})/T)$ and

$$\sigma_{L/k,E} : (P, Q) \longmapsto (P, -Q). \tag{3.18}$$

Moreover, to determine the image of $E^{(D)}$ into $(E \times E^{(D)})/T$, considering the inclusion of E and its quadratic twist into $(E \times E^{(D)})/T$ is enough. Applying the first definition leads to the conclusion:

$$E_L = \ker((\sigma + 1)_{L/k,E}) = (\sigma - 1)_{L/k,E}((E \times E^{(D)})/T) = E^{(D)}. \tag{3.19}$$

3.2 Decomposition of groups rings

It is possible to construct a decomposition of $\mathrm{Res}_{L/k}$ into primitive subgroups, starting from the one of $\mathbb{Q}[\mathrm{Gal}(L/k)]$ into direct sum of irreducible rational representations (for instance see [7]).

In this section we will assume that G is a finite abelian group. We will also consider the group rings $\mathbb{Z}[G]$, $\mathbb{Q}[G]$, and $\mathbb{C}[G]$ and derive their decomposition. Beginning with the latter, let's consider the character group of G, namely $\hat{G} = \mathrm{Hom}_{\mathbb{C}}(G, \mathbb{C}^\times)$.

[2]Notice that V_F is independent on the choice of the field extension L.

[3]In the literature $(\mathbf{G_m})_L$ is also denoted by $\mathbb{T}_{L,k}$ or $\mathbb{T}_2$, e.g. see [6].

Proposition 3.2.1. (Decomposition of $\mathbb{C}[G]$) Fix $\chi \in \hat{G}$, and let

$$e_\chi := \frac{1}{|G|}\sum_{g\in G}\chi(g)g^{-1} = \frac{1}{|G|}\sum_{g\in G}\chi^{-1}(g)g \in \mathbb{C}[G]. \tag{3.20}$$

Then

(i) $e_\chi^2 = e_\chi$;

(ii) if $\chi \neq \psi$, $e_\chi e_\psi = 0$;

(iii) $\sum_{\chi\in\hat{G}} e_\chi = 1_G$;

(iv) $e_\chi\mathbb{C}[G] = e_\chi\mathbb{C}$ is a one–dimensional $\mathbb{C}$–vector space;

(v) $\mathbb{C}[G] = \sum_{\chi\in\hat{G}}(e_\chi\cdot\mathbb{C}[G]) = \bigoplus_{\chi\in\hat{G}}(e_\chi\cdot\mathbb{C}[G]) = \bigoplus_{\chi\in\hat{G}} e_\chi\mathbb{C}$, in other words $\mathbb{C}[G]$ is decomposable into a direct sum of irreducible rational representations.

Treating the cases of $\mathbb{Q}[G]$, and $\mathbb{Z}[G]$ is not as straightforward, indeed $\chi(g)$ does not belong to $\mathbb{Q}$ in general, i.e. $e_\chi \notin \mathbb{Q}[G]$.

Lemma 3.2.1. Denote $G_\mathbb{Q} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, let $C_G := \{H \leq G \mid G/H \text{ is cyclic}\}$, R_G be the set of irreducible rational representation of G, and X_G be the set of $G_\mathbb{Q}$–orbits of $\hat{G}$. Then C_G, R_G, and X_G are in natural one–to–one correspondence.

Proof. Firstly, let's prove the correspondence between C_G and X_G. If we fix $H \in C_G$ it is sufficient to consider $Y_H := \{\chi \in \hat{G} \mid \ker(\chi) = H\}$, i.e. the annihilator of H in G, and notice it is in X_G. Vice versa, if $Y \in X_G$, let $H_Y := \bigcap_{\chi\in Y}\ker(\chi)$; it follows that $G/H_Y \cong \chi(G)$ is a finite, and so cyclic, subgroup of $\mathbb{C}^\times$. We then conclude $H_Y \in C_G$.

Finally, let's consider X_G and R_G. If $Y \in X_G$, by definition $\sum_{\chi\in Y} e_\chi \in \mathbb{Q}[G]$, and and G's action on $\sum_{\chi\in Y}(e_\chi)\mathbb{Q}[G]$ is an irreducible rational representation ρ_Y of G which belongs to R_G. Conversely, if $\rho \in R_G$, we can decompose ρ over $\mathbb{C}$ into a direct sum of characters of G. From the fact that ρ is rational and irreducible it follows that it corresponds to a single $G_\mathbb{Q}$–orbit of $\hat{G}$. □

This result gives us the following

Proposition 3.2.2. (Decomposition of $\mathbb{Q}[G]$) Using the above notations, if $H \in C_G$ and defining $e_H := \sum_{\chi\in Y_H} e_\chi \in \mathbb{Q}[G]$, then

(i) $e_H^2 = e_H$;

(ii) if H_1 and H_2 are two distinct elements of C_G, $e_{H_1}e_{H_2} = 0$;

(iii) $\sum_{H\in C_G} e_H = 1_G$.

Moreover, if we define $\mathbb{Q}[G]_H := e_H\cdot\mathbb{Q}[G]$, then it is a simple $\mathbb{Q}[G]$–submodule of $\mathbb{Q}[G]$, and also the unique irreducible rational representation of G contained in $\mathbb{Q}[G]$ having kernel H. Finally, it hols

$$\mathbb{Q}[G] = \bigoplus_{H\in C_G}(e_H\cdot\mathbb{Q}[G]) = \bigoplus_{H\in C_G}\mathbb{Q}[G]_H. \tag{3.21}$$

Remark 3.2.1. If we consider the restriction $\mathbb{Z}[G]_H := \mathbb{Q}[G]_H \cap \mathbb{Z}[G]$, from the fact that it is a sub–module of $\mathbb{Z}[G]$ follows it is also a free $\mathbb{Z}$–module.

We can now finally prove an important auxiliary result.

Lemma 3.2.2. Suppose G is a finite abelian group, $H \in C_G$, $\sigma \in G$ is such that σH is a generator of G/H, $d = |G/H|$ and $N_H := \sum_{h\in H} h$. Then

(i) $\mathbb{Z}[G]_H = N_H \cdot \Psi_d(\sigma) \cdot \mathbb{Z}[G] \cong \mathbb{Z}[x]/(\Phi_d(x))$,

(ii) $\mathbb{Z}[G]_H \otimes_{\mathbb{Z}} \mathbb{Q} = N_H \cdot \Psi_d(\sigma) \cdot \mathbb{Q}[G] = \mathbb{Q}[G]_H$,

(iii) $\mathrm{rank}_{\mathbb{Z}}(\mathbb{Z}[G]_H) = \varphi(d)$, where $\varphi(\cdot)$ is the Euler totient function;

(iv) $\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[G] = \bigoplus_{H\in C_G}(\mathbb{Z}[G]_H \otimes \mathbb{Q})$;

(v) $\mathbb{Z}[G]/\bigoplus_{H\in C_G} \mathbb{Z}[G]_H$ is annihilated by $|G|$.

(vi) If G is also cyclic, of order n, and generated by σ (i.e. $G = \langle\sigma\rangle$), then we have

$$\mathbb{Z}[G]_H = \Psi_{n,d}(\sigma) \cdot \mathbb{Z}[G] = \ker(\Phi_d(\sigma)), \tag{3.22}$$

where $\Phi_d(\sigma)$ is viewed as endomorphism of $\mathbb{Z}[G]$.

Proof. Call $\beta = N_H \cdot \Psi_d(\sigma)$. Consider a character $\chi \in \hat{G}$, if $\ker(\chi) = H$ then

$$e_\chi \cdot \beta \cdot \mathbb{C}[G] = e_\chi \cdot \mathbb{C} = e_\chi \cdot e_H \cdot \mathbb{C}[G], \tag{3.23}$$

whereas if $\ker(\chi) \neq H$ then $e_\chi \cdot \beta \cdot \mathbb{C}[G] = 0 = e_\chi \cdot e_H \cdot \mathbb{C}[G]$ and so

$$\beta \cdot \mathbb{C}[G] = e_H \cdot \mathbb{C}[G] = \mathbb{Q}[G]_H. \tag{3.24}$$

Since $N_H\mathbb{Q}[G] \cap \mathbb{Z}[G] = N_H\mathbb{Z}[G]$, and it follows that $Z[G]/N_H\mathbb{Z}[G]$ is a torsion free $\mathbb{Z}$–module. Using the fact that the isomorphism of $\mathbb{Z}[G]$–modules

$$\begin{aligned} \pi_H \ : \ & N_H\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G/H], \\ & N_H \sum_{g\in G} a_g g \longmapsto \sum_{g\in G} a_g(gH) \end{aligned} \tag{3.25}$$

induces another isomorphism between torsion–free $\mathbb{Z}$–modules (Ψ_d is indeed monic):

$$N_H\mathbb{Z}[G]/\beta\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G/H]/\Psi_d(\sigma H)\mathbb{Z}[G/H] \cong \mathbb{Z}[x]/(\Psi_d(x)). \tag{3.26}$$

By the exact sequence

$$0 \longrightarrow N_H\mathbb{Z}[G]/\beta\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]/\beta\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]/N_H\mathbb{Z}[G] \longrightarrow 0 \tag{3.27}$$

one deduces that also $\mathbb{Z}[G]/\beta\mathbb{Z}[G]$ is a torsion–free $\mathbb{Z}$–module, and using (3.24) concludes

$$\beta \cdot \mathbb{Z}[G] = \mathbb{Z}[G]_H. \tag{3.28}$$

Moreover, using π_H we can write the following isomorphisms' chain

$$\beta\mathbb{Z}[G] \longrightarrow \Psi_d(\sigma H)\mathbb{Z}[G/H] \longrightarrow \Psi_d(x)(\mathbb{Z}[x]/(x^d - 1)) \cong (\Phi_d(x)). \tag{3.29}$$

In conclusion we have proved points (i) and (ii). Furthermore, points (iii) and (iv) follow, respectively, by the fact that $\mathrm{rank}_{\mathbb{Z}}(\mathbb{Z}[x]/\Phi_d(x)) = \varphi(d)$, and by applying (ii) and (3.21).

Let's now focus ourselves on the last two statements. If we fix $\alpha \in \mathbb{Z}[G]$, then

$$|G| \cdot \alpha = \sum_{H \in C_G} e_H \, |G| \, \alpha \in \bigoplus_{H \in C_G} \mathbb{Z}[G]_H; \tag{3.30}$$

thus

$$|G| \cdot \mathbb{Z}[G] \subseteq \bigoplus_{H \in C_G} \mathbb{Z}[G]_H \subseteq \mathbb{Z}[G] \tag{3.31}$$

and we have (v). Finally, assuming $G = \langle \sigma \rangle$, we can consider its action (which is actually a multiplication by x) on $\mathbb{Z}[x]/(x^n - 1)$. From

$$\Psi_{n,d}(x) = (1 + x^d + x^{2d} + \cdots + x^{n-d})\Psi_d(x) \tag{3.32}$$

it follows that $\Psi_{n,d} = N_H \Psi_d(\sigma)$, and using (i) we also have

$$\mathbb{Z}[G]_H = \Psi_{n,d}(\sigma)\mathbb{Z}[G] \cong \Psi_{n,d}(x)(\mathbb{Z}[x]/(x^n - 1)). \tag{3.33}$$

Notice that the latter is the kernel of multiplication by $\Phi_d(x)$ in $\mathbb{Z}[x]/(x^n - 1)$, and so $\Psi_{n,d}(\sigma)\mathbb{Z}[G]$ is the kernel of multiplication by $\Phi_d(\sigma)$ in $\mathbb{Z}[G]$.

□

3.3 Another viewpoint on primitive subgroups

Consider, as always in this section, L/k a finite abelian extension, $G := \mathrm{Gal}(L/k)$, and $k \subseteq F \subseteq L$, with F/k cyclic, $d = [F : k]$, and $H := \mathrm{Gal}(L/F)$. In order to remember the intermediate field fixed by the Galois group that determines the sub–module, let's denote

$$\mathbb{Z}[G]_F := \mathbb{Z}[G]_H \quad \text{and} \quad \mathbb{Q}[G]_F := \mathbb{Q}[G]_H. \tag{3.34}$$

Suppose that V is the usual commutative, algebraic group over k. If we consider $\mathbb{Z}[G]_F$ as a G_k–module, then $\mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V$ is also a commutative algebraic group over k.

Assuming $k \subseteq M \subseteq F$, and letting

$$R_{F/M/k} : \mathbb{Z}[\mathrm{Gal}(F/k)] \longrightarrow \mathbb{Z}[\mathrm{Gal}(M/k)] \tag{3.35}$$

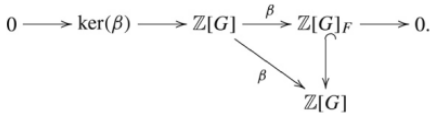
be the projection map of $R_{F/M/k,V} \in \mathrm{Hom}_k(\mathrm{Res}_{F/k}(V), \mathrm{Res}_{M/k}(V))$.

Proposition 3.3.1. With the same assumptions of theorem 3.1.1, we have that

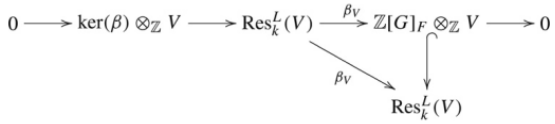
$$\mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V = \beta_{L/k,V}(\mathrm{Res}_{L/k}(V)), \tag{3.36}$$

where $\beta_{L/k,V} = N_{L/F} \cdot \Psi_d(\sigma) \in \mathbb{Z}[G]$. In other words, points (a) and (b) of of theorem 3.1.1 are equivalent.

Proof. From lemma 3.2.2 we deduce the diagram Since $\ker(\beta) \subseteq \mathbb{Z}[G]$, it is torsion–free, and



therefore it is also a free $\mathbb{Z}$–module. By Theorem B.1.1, it is induced the following diagram that shows $\mathbb{Z}[G]_F \otimes_{\mathbb{Z}} V = \beta_V(\mathrm{Res}_{L/k}(V)) = \beta_{L/k,V}(\mathrm{Res}_{L/k}(V))$. □



Now we can finally prove the following important results.

Proposition 3.3.2. V_F is isomorphic over F to $V^{\varphi(d)}$.

Proof. As said before, $\mathbb{Z}[G]_F$ is a free $\mathbb{Z}$–module of rank $\varphi(d)$ and G_F acts trivially on $\mathbb{Q}[G]_F$, so we conclude $\mathbb{Z}[G]_F \cong \mathbb{Z}^{\varphi}(d)$ as $\mathbb{Z}[G_F]$–modules. Finally, the thesis follows from point (v) of Theorem B.1.1. □

Proposition 3.3.3. The algebraic varieties $\mathrm{Res}_{L/k}(V)$ and $\bigoplus_{\substack{k\subseteq F\subseteq L \\ F/k \text{ cyclic}}} V_F$ are k–isogenous, via isogenies whose kernels are annihilated by $|G|$.

Proof. Let's use lemma 3.2.2 and point (v) of theorem B.1.1 when $\mathcal{O} = \mathbb{Z}, \mathcal{I} = \mathbb{Z}[G]$, and $\{\mathcal{J}_i\} = \{\mathbb{Z}[G]_F\}$. Then, inclusions 3.31 induce a sequence of isogenies

$$\mathrm{Res}_{L/k}(V) \longrightarrow \bigoplus_{\substack{k\subseteq F\subseteq L \\ F/k \text{ cyclic}}} V_F \longrightarrow \mathrm{Res}_{L/k}(V). \tag{3.37}$$

We conclude noticing that the composition of the above two is, indeed, the exponentiation to the power of $|G|$. □

Let's see now some special examples of primitive subgroups.

Trace zero subgroups

In the usual framework, and also assuming $d = [F : k]$ is a prime, from theorem 3.1.1 follows that V_F is the norm one subgroup of $\mathrm{Res}_{F/k}(V)$ if the group law on V is viewed multiplicatively. While, in the additive notation, it is the trace zero subgroup[4]. Moreover, $\mathrm{Res}_{F/k}(V)$ is k–isogenous to $V \times V_F$.

Decomposition of $\mathrm{Res}_{L/k}(\mathbf{G_m})$

Considering our first example (recall L/k is quadratic and $R = \mathrm{Res}_{L/k}(\mathbf{G_m}) \subset \mathbb{A}^3$) we have that the decomposition (up to isogeny) of R into $\mathbf{G_m}\times(\mathbf{G_m})_L$ is explicitly given by the homomorphism

$$\begin{aligned} \mathbf{G_m} \times (\mathbf{G_m})_L &\longrightarrow \mathrm{Res}_{L/k}(\mathbf{G_m}) \\ ((x, y), (a, b, 1)) &\longmapsto (xa, xb, y^2). \end{aligned} \tag{3.38}$$

Le latter has a rank 2 kernel generated by

$$\{((1, 1), (1, 0, 1)), ((-1, -1), (-1, 0, 1))\}. \tag{3.39}$$

As proved in proposition 3.3.3, the composition of (3.38) with

$$\begin{aligned} \mathrm{Res}_{L/k}(\mathbf{G_m}) &\longrightarrow \mathbf{G_m} \times (\mathbf{G_m})_L \\ (x_1, x_2, y) &\longmapsto ((y^{-1}, y), ((x_1^2 + Dx_2^2)y, 2x_1x_2y, 1)) \end{aligned} \tag{3.40}$$

gives the squaring map (G has indeed order 2).

[4] More details about trace zero subgroups can be found in [8].

3.3.1 Algebraic tori over finite fields

Consider again $V = \mathbf{G_m}$. The following result concerns algebraic tori on finite fields (case of most relevance in cryptography) and provides a better understanding of the relevance of the above dissertation in the cryptography's framework.

Proposition 3.3.4. Suppose $k = \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$ and $F = \mathbb{F}_{q^d}$, where q is a prime and d a divisor of n. Then:

(i) $(\mathbf{G_m})_F(k) \subseteq F^\times$;

(ii) the group $(\mathbf{G_m})_F(k)$ is isomorphic to the subgroup of $F^\times$ of order $\Phi_d(q)$;

(iii) if $v \in (\mathbf{G_m})_F(k)$ and v has a prime order not dividing d, then for all proper intermediate fields M, in symbols $k \subseteq M \subset F$, we have $v \notin M$.

Proof. Point (i) follows directly by theorem 3.1.1. Call $\sigma \in G := \mathrm{Gal}(L/k) = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ the element that induces Frobenius endomorphism $x \mapsto x^q$. Then, the map (3.11) becomes

$$\begin{aligned} \mathbb{Z}[G] &\longrightarrow \mathrm{End}_k(\mathrm{Res}_{L/k}(\mathbf{G_m})) \\ \sum_{i=0}^{n-1} a_i \sigma^i &\longmapsto \left\{ v \mapsto v^{\sum a_i q^i} \right\} \end{aligned} \tag{3.41}$$

Moreover,

$$(\mathbf{G_m})_F(\mathbb{F}_q) = \ker(\Phi_d(\sigma)_{L/k,\mathbf{G_m}}) = \ker(v \mapsto v^{\Phi_d(q)}), \tag{3.42}$$

the latter is a subgroup of $\mathbb{F}_{q^d}^\times$ of order $\Phi_d(q)$, and so e have (ii). For the last statement see Lemma 1 of [9].

□

In some literature, e.g. [6], the primitive subgroup $(\mathbf{G_m})_{\mathbb{F}_{q^d}}$ is denoted $\mathbb{T}_d$, so we shall adopt this convention.

Remark 3.3.1. Notice that by proposition 3.3.3 and (3.3) follows that $\mathbb{F}_{q^d}^\times$ can be seen as "almost isomorphic" to $\bigoplus_{d|n} \mathbb{T}_d(\mathbb{F}_q)$. Thus, cryptography in $\mathbb{F}_{q^n}^\times$ — intended as crypto–system sophistication — reduces[5] to cryptography in primitive subgroups $\mathbb{T}_d(\mathbb{F}_q)$ (for the divisors d of n). In particular, the first point of previous proposition shows how attacks (e.g. index calculus attacks as those described in [10]) to discrete log problem in $\mathbb{F}_{q^d}^\times$ can be used to attack $\mathbb{T}_d(\mathbb{F}_q)$.

The last point of proposition 3.3.4 implies that, in order to attack the primitive subgroup $\mathbb{T}_d$, one can't reduce to the multiplicative group of a sub–field of $\mathbb{F}_{p^n}$, he has to deal with the whole group, i.e. a lot of complexity. This suggest how the subgroup $\mathbb{T}_n(\mathbb{F}_q) \subseteq \mathbb{F}_{q^n}^\times$ (of order $\Phi_n(q)$) is, from this prospective, the most cryptographycally secure.

3.4 Conclusion

The construction of the previous sections, shows how the security of a discrete log–cryptosystem in $V(\mathbb{F}_{q^n})$, where V is a commutative algebraic group over $\mathbb{F}_q$, reduces to those of its primitive subgroups $V_{\mathbb{F}_{q^d}}(\mathbb{F}_q)$, — with d divisor of n.

[5] Remember what discussed in remark 2.2.1 for El Gamal cryposystem.

In other words, if primitive subgroups are vulnerable by index calculus attacks, then theoretically the whole system is vulnerable, as happens to El Gamal cryptosystem if $(p-1)$ is smooth enough.

Starting by this observation, there have been a few attempts of attacks in the case of abelian varieties and elliptic curves [11].

Moreover, we saw that makes sense to think about $V_{\mathbb{F}_{q^n}}$ as the most cryptographycally secure of the subvarieties. With the sake of computational efficiency, one is therefore induced in defining a cryptosystem only upon $V_{\mathbb{F}_{q^n}}$ (instead of the whole V). For instance in the one–dimensional case, since $\dim(V_{\mathbb{F}_{q^n}}) = \varphi(n)\dim(V)$, we can represent elements in $V_{\mathbb{F}_{q^n}}$ using only a single point in $(\mathbb{F}_q)^{\varphi(n)}$.

Appendix A

Miscellanea on computability

We briefly summarize here some definitions and results that we use in Chapter 2. For further readings we also suggest [1], and [12].

A.1 Complexity and one–way functions

A (total) function $f : \mathbb{N}^n \to \mathbb{N}$ is said to be **computable** if there is algorithm (that is, a procedure that always terminates) A that upon input $(x_1, ..., x_n)$ outputs $f(x_1, ..., x_n)$.

Definition A.1.1. The **time of an algorithm** for input $(x_1, ..., x_n)$ is the number of steps that the algorithm takes to produce the output.

We represent the time of an algorithm as a function of the input size

$$\eta = \sum_{i=1}^{n} |x_i| \quad \text{where } |x_i| = \lceil \log_2(x_i + 1) \rceil \tag{A.1}$$

(i.e. $|x_i|$ is the number of bits required to write $x_i > 0$) and use asymptotic $O(\cdot)$ notation.

Remark A.1.1. In this work, contrary to what it is common in algorithmic complexity, the time–cost of the arithmetic operations and predicates over integers is not constant (since we will require arbitrary large integers and not just 64bits integers).

Assuming $x, y \in O(\eta)$, the cost of arithmetic operations and predicates is the following:

- $f(x, y) \mapsto x \pm y \in O(\eta)$,
- $f(x, y) \mapsto x \cdot y \in O(\eta^2)$,[1]
- $f(x, y) \mapsto x \div y \in O(\eta^2)$ (integer division),
- $f(x, y) \mapsto x \mod y \in O(\eta^2)$,
- $f(x, y) \mapsto x \leq y \in O(\min(|x|, |y|))$.

Definition A.1.2. A function $f : \mathbb{N}^n \to \mathbb{N}$ is said to be **computable in polynomial time** (or that f **can be computed efficiently**) if and only if there exists an algorithm A and a polynomial p such that

[1] Although this can be made more efficient with Discrete Fourier Transformation.

i) A computes f;

ii) $\text{Time}(A(x_1, ..., x_n)) \in O(p(\eta))$.

In this case, for simplicity, we will also say that f is PT–computable or PT.

Definition A.1.3. A function $f : \mathbb{N} \to \mathbb{N}$ is said to be **one–way** if:

i) it is injective;

ii) it is computed in polynomial time;

iii) its inverse is not computed in polynomial time;

iv) it's **honest**, that is if $|f(x)| \in O(|x|^n)$ and $|x| \in O(|f(x)|^{n'})$ for some constants n and n'.

Example A.1.1. If we define the PT bijection $f : \mathbb{N} \to \mathbb{N}$ as following

$$f(m) := \begin{cases} \log_2 m, & \text{if } m \text{ is a power of 2,} \\ \text{the 'next free' odd number, otherwise.} \end{cases} \tag{A.2}$$

It's easy to realize that f is not honest, since for even numbers $f(x)$ we have $|x| \notin O(|f(x)|^{n'})$ for any constant n'.

A.2 $\mathcal{P}$ and $\mathcal{NP}$

Definition A.2.1. We call $\mathcal{P}$ the family of the set A whose characteristic function χ_A can be computed in polynomial time.

Example A.2.1. In 2002 was proved that the set of prime numbers is in $\mathcal{P}$.

Definition A.2.2. The set $A \in \mathbb{N}^n$ is in $\mathcal{NP}$ if exists $B \in \mathbb{N}^{n+1}$ such that

i) $B \in \mathcal{P}$,

ii) if $(x, w) \in B$ then $|w| \in O(p(|x|))$ for some polynomial p, where $x \in \mathbb{N}^n$ and $w \in \mathbb{N}$;

iii) $x \in A$ if and only if $\exists w$ such that $(x, w) \in B$ (if $x \in A$, such w is called a **witness of x in A**).

It is an easy exercise to show that $\mathcal{P} \subseteq \mathcal{NP}$; proving or refuting the other inclusion is, maybe, one of the most challenging problems of modern mathematics. The problem $\mathcal{P} = \mathcal{NP}$ can be stated in two forms:

Conjecture A.2.1 (Decision version)**.** If $A \in \mathcal{NP}$ then $A \in \mathcal{P}$, i.e. it's characteristic function can be computed in polynomial time.

Conjecture A.2.2 (Search version)**.** If $A \in \mathcal{NP}$, let $B \in \mathcal{P}$ a set suitable for definition A.2.2, than there exists a polynomial-time function $g : \mathbb{N}^n \to \mathbb{N}$ such that $x \in A$ if and only if $(x, g(x)) \in B$. In other words if I can find quickly a witness for any element of A.

The above two formulations are actually equivalent, the proof is easy and quite instructive:

Theorem A.2.1. The decision version (DV) and the search version (SV) of the $\mathcal{P} = \mathcal{NP}$ problem are equivalent.

Proof. (SV $\Rightarrow$ DV) obvious: given x, compute in PT $g(x)$ and $x \in A \Leftrightarrow \chi_B(x, g(x)) = 1$ (also computable in PT) where B is the correspondent to A, as in the above definition.

(DV $\Rightarrow$ SV) We can then compute in PT the characteristic function of any set in NP. Let's define

$$C := \{(x, p) : x \in A \text{ and } p \text{ is the prefix of } w \text{ such that } (x, w) \in B\}, \tag{A.3}$$

we are wlog thinking $w \in \mathbb{N}$ in its binary representation. Since

$$D := \{(x, p, w) : (x, w) \in B \text{ and } p \text{ is a prefix of } w\} \tag{A.4}$$

is in $\mathcal{P}$ (because χ_B is PT) we have that $C \in \mathcal{NP}$, and so χ_C is PT. Then, we can compute g with[2] Algorithm 1, that runs in PT because both χ_C and χ_B do and $|w| \in O(p(|x|))$.

Algorithm 1 Given x, compute $g(x)$, the search function, in PT.

```
Include: χ_C, χ_B
Input: x
w = ε {ε is the empty–string}
if χ_C(x, w) == 0 then
  return w {x ∉ A}
else
  while χ_B(x, w) == 0 do
    if χ_C(x, w.0) == 1 then
      w = w.0
    else
      w = w.1
    end if
  end while
end if
return w
```

□

Theorem A.2.2. If there exists a one–way function then $\mathcal{P} \neq \mathcal{NP}$.

Proof. Let's prove the counternominal; let's assume $\mathcal{P} = \mathcal{NP}$ and show how to compute the inverse of any PT function f in PT. As before, define

$$C := \{(y, p) : p \text{ a prefix of } f^{-1}(y) \text{ in binary}\} \tag{A.5}$$

which is in NP because projection of

$$B := \{(y, p, x) : f(x) = y \text{ and } p \text{ is a prefix of } x\}. \tag{A.6}$$

We can then run Algorithm 2 in PT, and so we deduce that can't exist one–way functions.

□

[2] In this context, with the dot notation we indicate the string concatenation.

Algorithm 2 Compute the inverse of f in PT.

Include: χ_C
Input: y
$x = \varepsilon$ {ε is the empty–string}
if $\chi_C(y, x) == 0$ **then**
  return x {y has no preimage.}
else
  while $f(x) \neq y$ **do**
    if $\chi_C(y, x.0) == 1$ **then**
      $x = x.0$
    else
      $x = x.1$
    end if
  end while
end if
return x

Appendix B

Algebraic groups

B.1 General construction of $\mathcal{I} \otimes_{\mathcal{O}} V$

Here we briefly enunciate some definitions[1] and results about tensor product $\mathcal{I} \otimes_{\mathcal{O}} V$, following the same line as [4]. The scope is simply to fix some notations and ideas, not to give a complete description of the setting.

Let k_s be a separable closure of the field k, and denote $G_k := \mathrm{Gal}(k_s/k)$. We also assume that V is a commutative algebraic group over k, while $\mathcal{O}$ is a commutative ring[2], and $\mathcal{I}$ is a free $\mathcal{O}$–module with a finite rank and a continuous right action of G_k defined on it. The last assumption we make is the presence of a ring homomorphism $\mathcal{O} \to \mathrm{End}_k(V)$, so that we can regard $\mathcal{O}$ as a free rank one $\mathcal{O}$–module with trivial G_k–action.

Definition B.1.1. Let's fix an $\mathcal{O}$–module isomorphism $j : \mathcal{O}^r \to \mathcal{I}$, where r is $\mathcal{I}$'s rank as an $\mathcal{O}$–module. If $c_{\mathcal{I}} \in H^1(k, Aut_{k_s}(V^r))$ is the image of the homomorphism

$$\gamma \mapsto j^{-1} \circ j^{\gamma}, \tag{B.1}$$

under the composition induced by the homomorphism $\mathcal{O} \to \mathrm{End}_k(V)$. Then, we denote $\mathcal{I} \otimes_{\mathcal{O}} V$ the $\mathcal{I}$–**twist of** V, i.e the twist of V^r by the cocycle $c_{\mathcal{I}}$ (see Section 3.1 of [13]). In other words, $\mathcal{I} \otimes_{\mathcal{O}} V$ is the only commutative algebraic group over k with the k_s–isomorphism

$$\phi : V^r \longrightarrow \mathcal{I} \otimes_{\mathcal{O}} V, \tag{B.2}$$

such that

$$c_{\mathcal{I}}(\gamma) = \phi^{-1} \circ \phi^{\gamma}, \text{ for every } \gamma \in G_k. \tag{B.3}$$

Example B.1.1. (Powers of V) Taking $\mathcal{I} = \mathbb{Z}^r$ with trivial Galois action, and j as the identity map on $\mathbb{Z}^r$, we find that the cocycle $c_{\mathcal{I}}$ is trivial, and therefore we can take ϕ as the identity map on V^r. Applying the above definition we get $\mathbb{Z}^r \otimes_{\mathbb{Z}} V = V^r$, and in particular $V = \mathbb{Z} \otimes_{\mathbb{Z}} V$.

Other two interesting examples in our contest are:

[1] This concept can be introduced in different ways, an alternative definition (equivalent to the one we give when they are comparable) can be found in the Appendix to [4].

[2] In the cases we consider there will always be $\mathcal{O} = \mathbb{Z}$.

Example B.1.2. (Restriction of scalars) Taking L/k a finite Galois extension, one have that $\mathbb{Z}[G] \otimes_{\mathbb{Z}} V = \mathrm{Res}_{L/k}(V)$, where $G := \mathrm{Gal}(L/k)$. Indeed, the isomorphism

$$\begin{aligned} j : \mathbb{Z}^G &\longrightarrow \mathbb{Z}[G] \\ (a_g)_{g\in G} &\longmapsto \sum_{g\in G} a_g g^{-1} \end{aligned} \tag{B.4}$$

induces an L–isomorphism $\phi : V^G \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} V$. Finally, the composition between ϕ^{-1} and the projection on the identity component of V^G (in symbols $\pi_{id_G} : V^G \to V$) gives a homomorphism that satisfies the universal property of $\mathrm{Res}_{L/k}(V)$.

Example B.1.3. (Quadratic twists of $\mathbf{G_m}$) Let's consider $V = \mathbf{G_m}$ the multiplicative group, and use the notations introduced in Chapter 3. Being $(\mathbf{G_m})_L$ its primitive subgroup, we consider the isomorphism

$$\begin{aligned} \phi : \mathbf{G_m} &\longrightarrow (\mathbf{G_m})_L \\ (x, y) &\longmapsto \left(\frac{x+y}{2}, \frac{x-y}{2\sqrt{D}}, 1 \right) \end{aligned} \tag{B.5}$$

and therefore we find that $c_{\mathcal{I}}(\gamma) = \xi_L(\gamma) = \phi^{-1} \circ \phi^{\gamma}$. Thus $\mathcal{I} \otimes_{\mathbb{Z}} \mathbf{G_m} \cong (\mathbf{G_m})_L$.

Others examples can be found in Section 3 of [5]. We conclude this section with some properties, whose proof can also be found in [4].

Theorem B.1.1. With the above assumptions and notations, the variety $\mathcal{I} \otimes_{\mathcal{O}} V$ is a commutative algebraic group over k such that:

(i) $\mathcal{I} \otimes_{\mathcal{O}} V$ is functorial in both V and $\mathcal{I}$.

(ii) For all commutative k–algebras A, and all Galois extensions F of k for which G_F acts trivially on $\mathcal{I}$, we have that

$$(\mathcal{I} \otimes_{\mathcal{O}} V)(F \otimes_k A) \cong \mathcal{I} \otimes_{\mathcal{O}} (V(F \otimes_k A)) \tag{B.6}$$

and

$$(\mathcal{I} \otimes_{\mathcal{O}} V)(A) \cong (\mathcal{I} \otimes_{\mathcal{O}} (V(F \otimes_k A)))^{\mathrm{Gal}(F/k)}, \tag{B.7}$$

where the right-hand sides are the usual tensor products of $\mathcal{O}$–modules.

(iii) Let W also be a commutative algebraic group over k and $\mathcal{J}$ a free $\mathcal{O}$–module of finite rank and a continuous right action of G_k. Then, there is a natural G_k–equivalent $\mathcal{O}$–module isomorphism:

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J}) \otimes_{\mathcal{O}} \mathrm{Hom}_{k_s}(V, W) \longrightarrow \mathrm{Hom}_{k_s}(\mathcal{I} \otimes_{\mathcal{O}} V, \mathcal{J} \otimes_{\mathcal{O}} W) \tag{B.8}$$

whose restriction to a homomorphism of $\mathcal{O}$–modules is

$$\mathrm{Hom}_{\mathcal{O}[G_k]}(\mathcal{I}, \mathcal{J}) \otimes_{\mathcal{O}} \mathrm{Hom}_k(V, W) \hookrightarrow \mathrm{Hom}_k(\mathcal{I} \otimes_{\mathcal{O}} V, \mathcal{J} \otimes_{\mathcal{O}} W). \tag{B.9}$$

(iv) If F/k is a separable extension, $\mathcal{J}$ a free $\mathcal{O}$–module of finite rank and a continuous right action of G_k, and also $\mathcal{I}$ and $\mathcal{J}$ are isomorphic as $\mathcal{O}[G_F]$–modules, the the commutative algebraic groups $\mathcal{I} \otimes_{\mathcal{O}} V$ and $\mathcal{J} \otimes_{\mathcal{O}} V$ are isomorphic over F.

(v) If F/k is a separable extension, and the action of G_F on $\mathcal{I}$ is trivial, then $\mathcal{I} \otimes_{\mathcal{O}} V$ is F–isomorphic to $V^{\mathrm{rank}_{\mathcal{O}}(\mathcal{I})}$.

(vi) If $0 \to \mathcal{I} \to \mathcal{J} \to \mathcal{K} \to 0$ is an exact sequence of free $\mathcal{O}$–modules of finite rank and with a continuous right action of G_k, then the induced sequence

$$0 \longrightarrow \mathcal{I} \otimes_{\mathcal{O}} V \longrightarrow \mathcal{J} \otimes_{\mathcal{O}} V \longrightarrow \mathcal{K} \otimes_{\mathcal{O}} V \longrightarrow 0 \tag{B.10}$$

is an exact sequence of commutative algebraic groups over k.

(vii) If $\mathcal{I}, \mathcal{J}_1, \ldots \mathcal{J}_t$ are free $\mathcal{O}$–modules of finite rank with a continuous right action of G_k, and $\mathcal{I} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \oplus_{i=1}^{t} (\mathcal{J}_i \otimes_{\mathbb{Z}} \mathbb{Q})$ as $\mathcal{O}[G_k]$–modules, then

$$\mathcal{I} \otimes_{\mathcal{O}} V \text{ is } k\text{–isogenous to } \bigoplus_{i=1}^{t} (\mathcal{J}_i \otimes_{\mathcal{O}} V). \tag{B.11}$$

Bibliography

[1] D. Boneh and V. Shoup, "A graduate course in applied cryptography," *Draft 0.5*, 2020.

[2] N. Li, "Research on diffie-hellman key exchange protocol," in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4, pp. V4–634, IEEE, 2010.

[3] L. C. Washington, *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.

[4] B. Mazur, K. Rubin, and A. Silverberg, "Twisting commutative algebraic groups," *Journal of Algebra*, vol. 314, no. 1, pp. 419–438, 2007.

[5] A. Silverberg, "Applications to cryptography of twisting commutative algebraic groups," *Discrete applied mathematics*, vol. 156, no. 16, pp. 3122–3138, 2008.

[6] K. Rubin and A. Silverberg, "Using abelian varieties to improve pairing-based cryptography," *Journal of Cryptology*, vol. 22, no. 3, pp. 330–364, 2009.

[7] J.-P. Serre *et al.*, *Linear representations of finite groups*, vol. 42. Springer, 1977.

[8] G. Frey, "Applications of arithmetical geometry to cryptographic constructions," in *Finite fields and applications*, pp. 128–161, Springer, 2001.

[9] W. Bosma, J. Hutton, and E. R. Verheul, "Looking beyond xtr," pp. 46–63, 2002.

[10] G. L. Mullen and D. Panario, "Handbook of finite fields," vol. 17, pp. 397–399, CRC press Boca Raton, 2013.

[11] P. Gaudry, "Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem," *Journal of Symbolic computation*, vol. 44, no. 12, pp. 1690–1702, 2009.

[12] O. Goldreich, "Computational complexity: a conceptual perspective," 2008.

[13] V. E. Voskresenskii, V. VoskresenskiuI, and B. Kunyavski, *Algebraic groups and their birational invariants*, vol. 179. American Mathematical Soc., 2011.