Chapter 6

Tori, LUC and XTR

Recall from Example 5.1.5 that $\mathbb{F}_q^*$ satisfies our informal notion of an algebraic group. This chapter concerns certain subgroups of the multiplicative group of finite fields of the form $\mathbb{F}_{q^n}$ with $n > 1$. The main goal is to find short representations for elements. Algebraic tori give short representations of elements of certain subgroups of $\mathbb{F}_{q^n}^*$. Traces can be used to give short representations of certain algebraic group quotients in $\mathbb{F}_{q^n}^*$, and the most successful implementations of this are called LUC and XTR. These ideas are sometimes called **torus based cryptography** or **trace based cryptography**, though this is misleading: the issue is only about representation of elements and is independent of any specific cryptosystem.

6.1 Cyclotomic Subgroups of Finite Fields

Definition 6.1.1. Let $n \in \mathbb{N}$. A complex number z is an n-th **root of unity** if $z^n = 1$, and is a **primitive** n-th root of unity if $z^n = 1$ and $z^d \neq 1$ for any divisor $d \mid n$ with $1 \leq d < n$.

The n-th **cyclotomic polynomial** $\Phi_n(x)$ is the product $(x - z)$ over all primitive n-th roots of unity z.

Lemma 6.1.2. *Let $n \in \mathbb{N}$. Then*

1. $\deg(\Phi_n(x)) = \varphi(n)$.
2. $\Phi_n(x) \in \mathbb{Z}[x]$.
3. $$x^n - 1 = \prod_{d|n, 1 \leq d \leq n} \Phi_d(x).$$
4. *If $m \in \mathbb{N}$ is such that $m \neq n$ then* $\gcd(\Phi_n(x), \Phi_m(x)) = 1$.

5.

$$\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$$

where $\mu(d)$ is the Möbius function (Definition 4.3 of [468]).

Proof: Let z be a primitive n-th root of unity. Then every n-th root of unity is a power of z and, for $0 \leq i < n$, z^i is a primitive n-th root of unity if and only if $\gcd(n, i) = 1$. Therefore

$$\Phi_n(x) = \prod_{0 \leq i < n, \gcd(n,i)=1} (x - z^i)$$

and so $\deg(\Phi_n(x)) = \varphi(n)$.

Galois theory implies $\Phi_n(x) \in \mathbb{Q}[x]$ and, since z is an algebraic integer, it follows that $\Phi_n(x) \in \mathbb{Z}[x]$.[1]

The third fact follows since $x^n - 1 = \prod_{i=0}^{n-1}(x - z^i)$ and each z^i has some order $d \mid n$.

Let z be a root of $\gcd(\Phi_n(x), \Phi_m(x))$. Then z has order equal to both n and m, which is impossible if $n \neq m$.

Finally, writing z_d for some primitive d-th root of unity, note that

$$\begin{aligned}
\prod_{d|n}(x^{n/d} - 1)^{\mu(d)} &= \prod_{d|n}\prod_{j=1}^{n/d}\left(x - z_{n/d}^j\right)^{\mu(d)} \\
&= \prod_{d|n}\prod_{j=1}^{n/d}\left(x - z_n^{dj}\right)^{\mu(d)} \\
&= \prod_{i=1}^{n}(x - z_n^i)^{\sum_{d|\gcd(n,i)}\mu(d)}.
\end{aligned}$$

Since $\sum_{d|n}\mu(d)$ is 0 when $n > 1$ and is 1 when $n = 1$ (Theorem 4.7 of [468]) the result follows. □

Exercise 6.1.3. Show that $\Phi_1(x) = x - 1, \Phi_2(x) = x + 1$, $\Phi_6(x) = x^2 - x + 1$ and $\Phi_l(x) = x^{l-1} + x^{l-2} + \cdots + x + 1$ if l is prime.

Exercise 6.1.4. Prove that if $p \mid n$ then $\Phi_{pn}(x) = \Phi_n(x^p)$ and that if $p \nmid n$ then $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$. Prove that if n is odd then $\Phi_{2n}(x) = \Phi_n(-x)$.
[Hint: Use part 5 of Lemma 6.1.2.]

It is well-known that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$; we do not need this result so we omit the proof.

Lemma 6.1.5. *Let $n \in \mathbb{N}$. The greatest common divisor of the polynomials $(x^n - 1)/(x^d - 1)$ over all $1 \leq d < n$ such that $d \mid n$ is $\Phi_n(x)$.*

Proof: Define $I = \{d \in \mathbb{N} : 1 \leq d < n, d \mid n\}$. By part 3 of Lemma 6.1.2 we have $\Phi_n(x) = (x^n - 1)/f(x)$ where $f(x) = \prod_{d \in I}\Phi_d(x) = \operatorname{lcm}(x^d - 1 : d \in I)$. Hence

$$\Phi_n(x) = \frac{x^n - 1}{\operatorname{lcm}(x^d - 1 : d \in I)} = \gcd\left(\frac{x^n - 1}{x^d - 1} : d \in I\right).$$

□

[1] One can find elementary proofs of this fact in any book on polynomials.

Definition 6.1.6. Let $n \in \mathbb{N}$ and q a prime power. Define the **cyclotomic subgroup** $G_{q,n}$ to be the subgroup of $\mathbb{F}_{q^n}^*$ of order $\Phi_n(q)$.

The subgroups $G_{q,n}$ are of interest as most elements of $G_{q,n}$ do not lie in any subfield of $\mathbb{F}_{q^n}$ (see Corollary 6.2.3 below). In other words, $G_{q,n}$ is the "hardest part" of $\mathbb{F}_{q^n}^*$ from the point of view of the DLP. Note that $G_{q,n}$ is trivially an algebraic group, by virtue of being a subgroup of the algebraic group $\mathbb{F}_{q^n}^* = G_m(\mathbb{F}_{q^n})$ (see Example 5.1.5). The goal of this subject area is to develop compact representations for the groups $G_{q,n}$ and efficient methods to compute with them.

The two most important cases are $G_{q,2}$, which is the subgroup of $\mathbb{F}_{q^2}^*$ of order $q+1$, and $G_{q,6}$, which is the subgroup of $\mathbb{F}_{q^6}^*$ of order $q^2 - q + 1$. We give compact representations of these groups in Sections 6.3 and 6.4.

6.2 Algebraic Tori

Algebraic tori are a classical object in algebraic geometry and their relevance to cryptography was first explained by Rubin and Silverberg [503]. An excellent survey of this area is [504].

Recall from Theorem 5.7.7 that the Weil restriction of scalars of $\mathbb{A}^1$ with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$ is $\mathbb{A}^n$. Let $n > 1$ and let $f : \mathbb{A}^n(\mathbb{F}_q) \to \mathbb{F}_{q^n}$ be a bijective $\mathbb{F}_q$-linear function (e.g., corresponding to the fact that $\mathbb{F}_{q^n}$ is a vector space of dimension n over $\mathbb{F}_q$). For any $d \mid n$ define the norm $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g) = \prod_{i=0}^{n/d-1} g^{q^{di}}$. The equation $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(f(x_1, \ldots, x_n)) = 1$ defines an algebraic set in $\mathbb{A}^n$.

Definition 6.2.1. The **algebraic torus**[2] $\mathbb{T}_n$ is the algebraic set

$$V(\{\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(f(x_1, \ldots, x_n)) - 1 : 1 \leq d < n, d \mid n\}) \subset \mathbb{A}^n.$$

Note that there is a group operation on $\mathbb{T}_n(\mathbb{F}_q)$, given by polynomials, inherited from multiplication in $\mathbb{F}_{q^n}^*$. Hence (at least, ignoring for the moment the inverse map) $\mathbb{T}_n(\mathbb{F}_q)$ satisfies our informal definition of an algebraic group.

Lemma 6.2.2. *Let the notation be as above.*

1. $G_{q,n} = \{g \in \mathbb{F}_{q^n}^* : \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g) = 1$ *for all* $1 \leq d < n$ *such that* $d \mid n\}$.
2. $\mathbb{T}_n(\mathbb{F}_q)$ *is isomorphic as a group to* $G_{q,n}$.
3. $\#\mathbb{T}_n(\mathbb{F}_q) = \Phi_n(q)$.

Proof: For the first statement note that

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g) = \prod_{i=0}^{n/d-1} g^{q^{di}} = g^{(q^n-1)/(q^d-1)}.$$

Recall that $\Phi_n(q) \mid (q^n - 1)/(q^d - 1)$ and, by Lemma 6.1.5, $\gcd((q^n - 1)/(q^d - 1) : 1 \leq d < n, d \mid n) = \Phi_n(q)$. Hence, all the norms are 1 if and only if $g^{\Phi_n(q)} = 1$, which proves the first claim. The second and third statements follow immediately. □

Corollary 6.2.3. *Let* $n \in \mathbb{N}$ *and* q *a prime power. Suppose* $g \in G_{q,n}$ *has order* $r > n$. *Then* g *does not lie in any proper subfield of* $\mathbb{F}_{q^n}$.

[2]The plural of "torus" is "tori".

Proof: Suppose $g \in \mathbb{F}_{q^d}$ for some $1 \leq d < n$ such that $d \mid n$. Then $1 = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(g) = g^{n/d}$, but this contradicts the order of g being $> n$. □

It follows from the general theory that $\mathbb{T}_n$ is irreducible and of dimension $\varphi(n)$. Hence, $\mathbb{T}_n$ is a variety and one can speak of birational maps from $\mathbb{T}_n$ to another algebraic set. We refer to Section 5 of [504] for details and references.

Definition 6.2.4. The torus $\mathbb{T}_n$ is **rational** if there is a birational map from $\mathbb{T}_n$ to $\mathbb{A}^{\varphi(n)}$.

If $\mathbb{T}_n$ is rational then $\mathbb{A}^{\varphi(n)}(\mathbb{F}_q)$ is a compact representation for $G_{q,n}$. Performing discrete logarithm cryptography by transmitting elements of $\mathbb{A}^{\varphi(n)}(\mathbb{F}_q)$ is called **torus based cryptography** and was developed by Rubin and Silverberg [503].

If $\mathbb{T}_n$ is rational then there is an induced "partial" group operation on $\mathbb{A}^{\varphi(n)}$, given by rational functions. This is not an algebraic group in general since there is not usually a one-to-one correspondence between $\mathbb{A}^{\varphi(n)}(\mathbb{F}_q)$ and $G_{q,n}$. Nevertheless, "most" of the elements of the group $G_{q,n}$ appear in $\mathbb{A}^{\varphi(n)}(\mathbb{F}_q)$ and, for many cryptographic purposes, the partial group law is sufficient. In practice, however, working with the partial group operation on $\mathbb{A}^{\varphi(n)}$ is not usually as efficient as using other representations for the group. The main application of tori is therefore the compact representation for elements of certain subgroups of $\mathbb{F}_{q^n}^*$.

It is not known if $\mathbb{T}_n$ is rational for all $n \in \mathbb{N}$ (we refer to [504] for more details and references about when $\mathbb{T}_n$ is known to be rational). The cryptographic applications of $\mathbb{T}_2$ and $\mathbb{T}_6$ rely on the well-known fact that these tori are both rational. The details are given in the following sections.

As mentioned in Section 4.3, sometimes it is convenient to consider quotients of algebraic groups by an equivalence relation. In the following sections we describe algebraic group quotients (more commonly known by the names LUC and XTR) for $G_{q,2}$ and $G_{q,6}$, but we construct them directly without using the theory of tori.

6.3 The Group $G_{q,2}$

Define $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta)$ where

$$\theta^2 + A\theta + B = 0 \tag{6.1}$$

for some $A, B \in \mathbb{F}_q$ such that $x^2 + Ax + B$ is irreducible over $\mathbb{F}_q$ (e.g., if q is odd then $A^2 - 4B$ is not a square in $\mathbb{F}_q$). In practice there are performance advantages from using a simpler equation, such as $\theta^2 = B$ or $\theta^2 + \theta = B$ where B is "small". Every element of $\mathbb{F}_{q^2}$ is of the form $u + v\theta$ where $u, v \in \mathbb{F}_q$.

The **conjugate** of θ is $\overline{\theta} = \theta^q = -A - \theta$. We have $\theta + \overline{\theta} = -A$ and $\theta\overline{\theta} = B$. The conjugate of an element $g = u + v\theta \in \mathbb{F}_{q^2}$ is $u + v\overline{\theta}$ and g has **norm**

$$\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = (u + v\theta)(u + v\overline{\theta}) = u^2 - Auv + Bv^2. \tag{6.2}$$

The group $G_{q,2}$ is defined to be the set of elements $g \in \mathbb{F}_{q^2}$ such that $g^{q+1} = 1$. Equivalently this is the set of $u + v\theta$ such that $u^2 - Auv + Bv^2 = 1$.

Exercise 6.3.1. Show that if $g = u + v\theta \in G_{q,2}$ then $g^{-1} = g^q = u + v\overline{\theta} = (u - Av) + (-v)\theta$. Hence, inversion in $G_{q,2}$ is cheaper than a general group operation (especially if $A = 0$ or A is "small").

Exercise 6.3.2. Suppose q is not a power of 2. Suppose $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta)$ where $\theta^2 + A\theta + B = 0$ and multiplying an element of $\mathbb{F}_q$ by A or B has negligible cost (e.g., $A = 0$ and $B = 1$). Show that one can compute a product (respectively: squaring; inversion) in $\mathbb{F}_{q^2}^*$

using 3 multiplications (respectively: 3 squarings; one inversion, 3 multiplications and 2 squarings) in $\mathbb{F}_q$. Ignore the cost of additions and multiplication by small constants such as 2 (since they are significantly faster to perform than multiplications etc).

Exercise 6.3.3.★ Suppose $q \equiv 3 \pmod 4$ is prime. Show that one can represent $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(\theta)$ where $\theta^2 + 1 = 0$. Show that, using this representation, one can compute a product (respectively: squaring; inversion; square root) in $\mathbb{F}_{q^2}^*$ using 3 multiplications (respectively: 2 multiplications; one inversion, 2 squarings and 2 multiplications; 2 square roots, one inversion, one Legendre symbol, one multiplication and 2 squarings) in $\mathbb{F}_q$. Ignore the cost of additions.

6.3.1 The Torus $\mathbb{T}_2$

Recall that $G_{q,2}$ can be represented as the $\mathbb{F}_q$-points of the algebraic torus $\mathbb{T}_2 = V(\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(f(x,y)) - 1) \subset \mathbb{A}^2$, where $f : \mathbb{A}^2(\mathbb{F}_q) \to \mathbb{F}_{q^2}$. By equation (6.2), an affine equation for $\mathbb{T}_2$ is $V(x^2 - Axy + By^2 - 1)$. Being a conic with a rational point, it is immediate from general results in geometry (see Exercise 5.5.14 for a special case) that $\mathbb{T}_2$ is birational with $\mathbb{A}^1$.

The next two results give a more algebraic way to show that $\mathbb{T}_2$ is rational. Rather than directly constructing a birational map from $\mathbb{T}_2$ to $\mathbb{A}^1$ we go via $G_{q,2}$. Lemma 6.3.4 provides a map from $\mathbb{A}^1(\mathbb{F}_q)$ to $G_{q,2}$ while Lemma 6.3.6 provides a map from $G_{q,2}$ to $\mathbb{A}^1(\mathbb{F}_q)$.

Lemma 6.3.4. *The set $G_{q,2} \subseteq \mathbb{F}_{q^2}^*$ is equal to the set*

$$\{(a+\theta)/(a+\overline{\theta}) : a \in \mathbb{F}_q\} \cup \{1\}.$$

Proof: Clearly, every element $g = (a+\theta)/(a+\overline{\theta})$ satisfies $g\overline{g} = 1$. It is also easy to check that $(a+\theta)/(a+\overline{\theta}) = (a'+\theta)/(a'+\overline{\theta})$ implies $a = a'$. Hence we have obtained q distinct elements of $G_{q,2}$. The missing element is evidently 1 and the result follows. □

Exercise 6.3.5. Suppose q is odd. Determine the value for a such that $(a+\theta)/(a+\overline{\theta}) = -1$.

Lemma 6.3.6. *Let $g = u + v\theta \in G_{q,2}$, $g \neq \pm 1$. Then $u + v\theta = (a+\theta)/(a+\overline{\theta})$ for the unique value $a = (u+1)/v$.*

Proof: The value a must satisfy

$$a + \theta = (u+v\theta)(a+\overline{\theta}) = ua + u\overline{\theta} + av\theta + v\theta\overline{\theta} = (ua - Au + Bv) + \theta(av - u).$$

Equating coefficients of θ gives $av = u + 1$ and the result follows as long as $v \neq 0$ (i.e., $g \neq \pm 1$). □

The above results motivate the following definition.

Definition 6.3.7. The $\mathbb{T}_2$ **decompression map** is the function $\mathrm{decomp}_2 : \mathbb{A}^1 \to G_{q,2}$ given by $\mathrm{decomp}_2(a) = (a+\theta)/(a+\overline{\theta})$.

The $\mathbb{T}_2$ **compression map** is the function $\mathrm{comp}_2 : G_{q,2} - \{1, -1\} \to \mathbb{A}^1$ given by $\mathrm{comp}_2(u + v\theta) = (u+1)/v$.

Lemma 6.3.8. *The maps* comp_2 *and* decomp_2 *are injective. The compression map is not defined at* ± 1. *If* $g \in G_{q,2} - \{1, -1\}$ *then* $\mathrm{decomp}_2(\mathrm{comp}_2(g)) = g$.

Exercise 6.3.9. Prove Lemma 6.3.8.

Alert readers will notice that the maps comp_2 and decomp_2 are between $G_{q,2}$ and $\mathbb{A}^1$, rather than between $\mathbb{T}_2$ and $\mathbb{A}^1$. For completeness we now give a map from $G_{q,2}$ to $\mathbb{T}_2 \subset \mathbb{A}^2$. From this one can deduce birational maps between $\mathbb{T}_2$ and $\mathbb{A}^1$, which prove that $\mathbb{T}_2$ is indeed rational.

Lemma 6.3.10. *An element of the form $(a+\theta)/(a+\overline{\theta}) \in G_{q,2}$ corresponds to the element*

$$\left(\frac{a^2 - B}{a^2 - aA + B}, \frac{2a - A}{a^2 - aA + B}\right)$$

of $\mathbb{T}_2$.

Proof: Let (x, y) be the image point in $\mathbb{T}_2$. In other words

$$(a + \theta)/(a + \overline{\theta}) = x + y\theta$$

and so $a + \theta = (x + y\theta)(a + \overline{\theta}) = (ax + By - Ax) + \theta(ay - x)$. Equating coefficients gives the result. □

Exercise 6.3.11. Prove that $\mathbb{T}_2$ is rational.

We now present the partial group operations on $\mathbb{A}^1$ induced by the map from $\mathbb{A}^1$ to $G_{q,2}$. We stress that $\mathbb{A}^1$ is not a group with respect to these operations, since the identity element of $G_{q,2}$ is not represented as an element of $\mathbb{A}^1$.

Lemma 6.3.12. *Let the notation be as above. For $a, b \in \mathbb{A}^1$ define $a \star b = (ab - B)/(a + b - A)$ and $a' = A - a$. Then $a \star b$ is the product and a' is the inverse for the partial group law.*

Proof: The partial group law on $\mathbb{A}^1$ is defined by $\text{comp}_2(\text{decomp}_2(a)\text{decomp}_2(b))$. Now,

$$\text{decomp}_2(a)\text{decomp}_2(b) = \left(\frac{a + \theta}{a + \overline{\theta}}\right)\left(\frac{b + \theta}{b + \overline{\theta}}\right) = \frac{ab - B + (a + b - A)\theta}{ab - B + (a + b - A)\overline{\theta}}.$$

The formula for $a \star b$ follows.

Similarly,

$$\text{decomp}_2(a)^{-1} = \frac{a + \overline{\theta}}{a + \theta} = \frac{a + (-A - \theta)}{a + (-A - \overline{\theta})},$$

which gives the formula for a'. □

It follows that one can compute directly with the compressed representation of elements of $\mathbb{T}_2(\mathbb{F}_q)$. Note that computing the partial group law on $\mathbb{A}^1$ requires an inversion, so is not very efficient. For cryptographic applications one is usually computing $\text{comp}_2(g^n)$ from $\text{comp}_2(g)$; to do this one decompresses to obtain $g \in G_{q,2}$, then computes g^n using any one of a number of techniques, and finally applies comp_2 to obtain a compact representation.[3]

6.3.2 Lucas Sequences

Lucas[4] sequences can be used for efficient computation in quadratic fields. We give the details for $G_{q,2} \subset \mathbb{F}_{q^2}^*$. The name LUC cryptosystem is applied to any cryptosystem using Lucas sequences to represent elements in an algebraic group quotient of $G_{q,2}$. Recall the **trace** $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = g + g^q$ for $g \in \mathbb{F}_{q^2}$.

[3] This is analgous to using projective coordinates for efficient elliptic curve arithmetic; see Exercise 9.1.5.

[4] They are named after Edouard Lucas (1842-1891); who apparently died due to a freak accident involving broken crockery. Lucas sequences were used for primality testing and factorisation before their cryptographic application was recognised.

Definition 6.3.13. Let $g \in \mathbb{F}_{q^2}^*$ satisfy $g^{q+1} = 1$. For $i \in \mathbb{Z}$ define $V_i = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g^i)$.

Lemma 6.3.14. *Let $g = v_1 + w_1\theta$ with $v_1, w_1 \in \mathbb{F}_q$ and θ as in equation (6.1). Suppose $g^{q+1} = 1$ and let V_i be as in Definition 6.3.13. Then, for $i, j \in \mathbb{Z}$,*

1. $V_0 = 2$ *and* $V_1 = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = 2v_1 - Aw_1$.
2. $V_{-i} = V_i$.
3. $V_{i+1} = V_1V_i - V_{i-1}$.
4. $V_{2i} = V_i^2 - 2$.
5. $V_{2i-1} = V_iV_{i-1} - V_1$.
6. $V_{2i+1} = V_iV_{i+1} - V_1$.
7. $V_{2i+1} = V_1V_i^2 - V_iV_{i-1} - V_1$.
8. $V_{i+j} = V_iV_j - V_{i-j}$.

Proof: Let $\overline{g} = g^q = v_1 + w_1\overline{\theta}$. Then $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = g + \overline{g} = (v_1 + w_1\theta) + (v_1 + w_1(-\theta - A)) = 2v_1 - Aw_1$. Similarly, $g^0 = 1$ and the first statement is proven. The second statement follows from $g^{-1} = \overline{g}$. Statements 3 to 6 are all special cases of statement 8, which follows from the equation

$$V_{i+j} = g^{i+j} + \overline{g}^{i+j} = (g^i + \overline{g}^i)(g^j + \overline{g}^j) - g^j\overline{g}^j(g^{i-j} + \overline{g}^{i-j}).$$

(An alternative proof of Statement 3 is to use the fact that g satisfies $g^2 = V_1g - 1$.) Statement 7 then follows from 3 and 6. □

Exercise 6.3.15. Define $U_i = (g^i - \overline{g}^i)/(g - \overline{g})$. Prove that $U_{i+1} = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)U_i - U_{i-1}$, $U_{2i} = V_iU_i$, $U_{i+j} = U_iU_{j+1} - U_{i-1}U_j$.

Definition 6.3.16. Denote by $G_{q,2}/\langle\sigma\rangle$ the set of equivalence classes of $G_{q,2}$ under the equivalence relation $g \equiv \sigma(g) = g^q = g^{-1}$. Denote the class of $g \in G_{q,2}$ by $[g] = \{g, g^q\}$.

The main observation is that $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g^q)$ and so a class $[g]$ can be identified with the value $V = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)$. This motivates Definition 6.3.18. When q is odd, the classes $[1]$ and $[-1]$ correspond to $V = 2$ and $V = -2$ respectively; apart from these cases, the other possible values for V are those for which the polynomial $x^2 - Vx + 1$ is irreducible over $\mathbb{F}_q$.

Exercise 6.3.17. Prove that if $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g')$ for $g, g' \in G_{q,2}$ then $g' \in \{g, g^q\}$. Hence, show that when q is odd there are $2 + (q-1)/2$ values for $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)$ over $g \in G_{q,2}$.

The set $G_{q,2}/\langle\sigma\rangle$ is not a group, however for a class $[g] \in G_{q,2}/\langle\sigma\rangle$ and $n \in \mathbb{N}$ one can define $[g]^n$ to be $[g^n]$.

Definition 6.3.18. Let $G'_{q,2} = \{\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g) : g \in G_{q,2}\}$. For $V \in G'_{q,2}$ and $n \in \mathbb{N}$ define $[n]V = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g^n)$ for any $g \in G_{q,2}$ such that $V = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g)$.

It follows that we may treat the set $G'_{q,2}$ as an algebraic group quotient. One method to efficiently compute $[n]V$ for $n \in \mathbb{N}$ is to take a root $g \in \mathbb{F}_{q^2}$ of $x^2 - Vx + 1 = 0$, compute g^n in $\mathbb{F}_{q^2}$ using the square-and-multiply method, and then compute $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(g^n)$. However, we want to be able to compute $[n]V$ directly using an analogue of the square-and-multiply

method.[5] Lemma 6.3.14 shows that, although V_{2n} is determined by V_n and n, V_{n+1} is not determined by V_n alone. Hence it is necessary to develop an algorithm that works on a pair (V_n, V_{n-1}) of consecutive values. Such algorithms are known as **ladder methods**. One starts the ladder computation with $(V_1, V_0) = (V, 2)$.

Lemma 6.3.19. *Given (V_i, V_{i-1}) and V one can compute (V_{2i}, V_{2i-1}) (i.e., "squaring") or (V_{2i+1}, V_{2i}) (i.e., "square-and-multiply") in one multiplication, one squaring and two or three additions in $\mathbb{F}_q$.*

Proof: One must compute V_i^2 and $V_i V_{i-1}$ and then apply part 4 and either part 5 or 7 of Lemma 6.3.14. □

Exercise 6.3.20. Write the ladder algorithm for computing $[n]V$ using Lucas sequences in detail.

The storage requirement of the ladder algorithm is the same as when working in $\mathbb{F}_{q^2}$, although the output value is compressed to a single element of $\mathbb{F}_q$. Note however that computing a squaring alone in $\mathbb{F}_{q^2}$ already requires more computation (at least when q is not a power of 2) than Lemma 6.3.19.

We have shown that for $V \in G'_{q,2}$ one can compute $[n]V$ using polynomial operations starting with the pair $(V, 2)$. Since $G'_{q,2}$ is in one-to-one correspondence with $G_{q,2}/\langle\sigma\rangle$, it is natural to consider $G'_{q,2}$ as being an algebraic group quotient.

Performing discrete logarithm based cryptography in $G'_{q,2}$ is sometimes called the LUC cryptosystem.[6] To solve the discrete logarithm problem in $G'_{q,2}$ one usually lifts the problem to the **covering group** $G_{q,2} \subset \mathbb{F}_{q^2}^*$ by taking one of the roots in $\mathbb{F}_{q^2}$ of the polynomial $x^2 - Vx + 1$.

Example 6.3.21. Define $\mathbb{F}_{37^2} = \mathbb{F}_{37}(\theta)$ where $\theta^2 - 3\theta + 1 = 0$. The element $g = -1 + 3\theta$ has order 19 and lies in $G_{37,2}$. Write $V = \mathrm{Tr}_{\mathbb{F}_{37^2}/\mathbb{F}_{37}}(g) = 7$. To compute $[6]V$ one uses the addition chain $(V_1, V_0) = (7, 2) \to (V_3, V_2) = (26, 10) \to (V_6, V_5) = (8, 31)$; this is because $6 = (110)_2$ in binary so the intermediate values for i are $(1)_2 = 1$ and $(11)_2 = 3$.

Exercise 6.3.22. Using the same values as Example 6.3.21 compute $[10]V$.

Exercise 6.3.23.★ Compare the number of $\mathbb{F}_q$ multiplications and squarings to compute a squaring or a squaring-and-multiplication in the quotient $G'_{q,2}$ using Lucas sequences with the cost for general arithmetic in $G_{q,2} \subset \mathbb{F}_{q^2}$.

6.4 The Group $G_{q,6}$

The group $G_{q,6}$ is the subgroup of $\mathbb{F}_{q^6}^*$ of order $\Phi_6(q) = q^2 - q + 1$. The natural representation of elements of $G_{q,6}$ requires 6 elements of $\mathbb{F}_q$.

Assume (without loss of generality) that $\mathbb{F}_{q^6} = \mathbb{F}_{q^3}(\theta)$ where $\theta \in \mathbb{F}_{q^2}$ and $\theta^2 + A\theta + B = 0$ for some $A, B \in \mathbb{F}_q$.

[5] In practice it is often more efficient to use other processes instead of the traditional square-and-multiply method. We refer to Chapter 3 of [579] for more details.

[6] The original LUC cryptosystem due to Smith and Lennon [574] was using Lucas sequences modulo a composite integer N; we refer to Section 6.6 for further discussion. The finite field version is only very briefly mentioned in [574], but is further developed in [575].

6.4.1 The Torus $\mathbb{T}_6$

Recall that $\mathbb{T}_6$ is a two dimensional algebraic set in $\mathbb{A}^6$ defined by the intersection of the kernels of the norm maps $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}$ and $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$. It is known that $\mathbb{T}_6$ is rational, so the goal is to represent elements of $G_{q,6}$ using only two elements of $\mathbb{F}_q$.

The kernel of the norm map $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}$ is identified with $\mathbb{T}_2(\mathbb{F}_{q^3}) \subset \mathbb{A}^2(\mathbb{F}_{q^3})$. As in Section 6.3.1, $\mathbb{T}_2$ is birational to $\mathbb{A}^1(\mathbb{F}_{q^3})$ (which can then be identified with $\mathbb{A}^3(\mathbb{F}_q)$) via the map $\mathrm{decomp}_2(a) = (a+\theta)/(a+\overline{\theta})$ where $\mathbb{F}_{q^6} = \mathbb{F}_{q^3}(\theta)$. The next step is to compute the kernel of the norm map with respect to $\mathbb{F}_{q^6}/\mathbb{F}_{q^2}$.

Lemma 6.4.1. *The Weil restriction of the kernel of* $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}$ *on* $\mathbb{T}_2(\mathbb{F}_{q^3})$ *is birational with a quadratic hypersurface* U *in* $\mathbb{A}^3(\mathbb{F}_q)$.

Proof: First, we represent an element of $\mathbb{T}_2(\mathbb{F}_{q^3}) - \{1\}$ as a single value $a \in \mathbb{F}_{q^3}$. Now impose the norm equation on the image of $\mathrm{decomp}_2(a)$

$$\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\mathrm{decomp}_2(a)) = \left(\frac{a+\theta}{a+\overline{\theta}}\right)\left(\frac{a+\theta}{a+\overline{\theta}}\right)^{q^2}\left(\frac{a+\theta}{a+\overline{\theta}}\right)^{q^4} = \left(\frac{a+\theta}{a+\overline{\theta}}\right)\left(\frac{a^{q^2}+\theta}{a^{q^2}+\overline{\theta}}\right)\left(\frac{a^{q^4}+\theta}{a^{q^4}+\overline{\theta}}\right).$$

To solve $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\mathrm{decomp}_2(a)) = 1$ one clears the denominator and equates coefficients of θ, giving

$$\begin{aligned} & a^{1+q^2+q^4} + \theta(a^{1+q^2} + a^{1+q^4} + a^{q^2+q^4}) + \theta^2(a + a^{q^2} + a^{q^4}) + \theta^3 \\ = \;& a^{1+q^2+q^4} + \overline{\theta}(a^{1+q^2} + a^{1+q^4} + a^{q^2+q^4}) + \overline{\theta}^2(a + a^{q^2} + a^{q^4}) + \overline{\theta}^3. \end{aligned}$$

The crucial observations are that the cubic terms in a cancel and that $\theta^2 - \overline{\theta}^2 = -A(\theta - \overline{\theta})$ and $\theta^3 - \overline{\theta}^3 = (A^2 - B)(\theta - \overline{\theta})$. Hence we obtain a single equation in a.

Now, we identify $a \in \mathbb{A}^1(\mathbb{F}_{q^3})$ with a 3-tuple $(a_0, a_1, a_2) \in \mathbb{A}^3(\mathbb{F}_q)$. Using the fact that $a \mapsto a^q$ corresponds to an $\mathbb{F}_q$-linear map on $\mathbb{A}^3(\mathbb{F}_q)$, it follows that the single equation given above is actually a quadratic polynomial in (a_0, a_1, a_2). In other words, the values (a_0, a_1, a_2) corresponding to solutions of the norm equation are points on a quadratic hypersurface in $\mathbb{A}^3(\mathbb{F}_q)$, which we call U. □

The general theory (see Rubin and Silverberg [504]) implies that U is irreducible, but we do not prove this. It remains to give a rational parameterisation $p_U : U \to \mathbb{A}^2$ of the hypersurface. This is done using essentially the same method as Example 5.5.14.

Lemma 6.4.2. *An irreducible quadratic hypersurface* $U \subset \mathbb{A}^3$ *over a field* $\Bbbk$ *is birational over* $\Bbbk$ *to* $\mathbb{A}^2$.

Proof: (Sketch) Let $P = (x_P, y_P, z_P)$ be a point on U and change variables so that the tangent plane T to U at P is $x = x_P$. We have not discussed T in this book; the only property we need is that T contains every line through P that is not contained in U and that intersects U at P with multiplicity 2.

Let $Q \in U(\Bbbk)$ be such that $Q \neq P$ and such that the line between P and Q is not contained in U (this is generically the case for an irreducible quadratic hypersurface). Then the line between P and Q does not lie in T and so is given by an equation of the form[7]

$$(x, y, z) = P + t(1, a, b) \tag{6.3}$$

for some $a, b \in \Bbbk$ (in other words, the equations $x = x_P + t, y = y_P + at$, etc). Such a line hits U at precisely one point $Q \in U(\Bbbk)$ with $Q \neq P$. Writing $U = V(F(x, y, z))$ it

[7]Here, and below, $P + Q$ denotes the usual coordinate-wise addition of 3-tuples over a field.

follows that $F(x_P + t, y_P + at, z_P + bt) = 0$ has the form $t(h(a,b)t - g(a,b)) = 0$ for some quadratic polynomial $h(a,b) \in \Bbbk[a,b]$ and some linear polynomial $g(a,b) \in \Bbbk[a,b]$. Hence we have a rational map $\mathbb{A}^2 \to U$ given by

$$(a,b) \mapsto P + \tfrac{g(a,b)}{h(a,b)}(1,a,b).$$

The inverse is the rational map

$$p_U(x_Q, y_Q, z_Q) = ((y_Q - y_P)/(x_Q - x_P), (z_Q - z_P)/(x_Q - x_P))$$

such that $p_U : U \to \mathbb{A}^2$. □

Recall the map $\mathrm{comp}_2 : G_{q^3,2} \to \mathbb{A}^1(\mathbb{F}_{q^3})$ from the study of $\mathbb{T}_2$. We identify $\mathbb{A}^1(\mathbb{F}_{q^3})$ with $\mathbb{A}^3(\mathbb{F}_q)$. The image of comp_2 is U, which is birational via p_U to $\mathbb{A}^2$. This motivates the following definition.

Definition 6.4.3. The $\mathbb{T}_6$ **compression map** is $\mathrm{comp}_6 : G_{q,6} \to \mathbb{A}^2$ is given by $\mathrm{comp}_6 = p_U \mathrm{comp}_2$. The inverse of comp_6 is the $\mathbb{T}_6$ **decompression map** $\mathrm{decomp}_6 = \mathrm{decomp}_2\, p_U^{-1}$.

Example 6.4.4. Let $q \equiv 2, 5 \pmod 9$ be an odd prime power so that $\mathbb{F}_{q^6} = \mathbb{F}_q(\zeta_9)$ where ζ_9 is a primitive 9-th root of unity (see Exercise 6.4.5). Let $\theta = \zeta_9^3$ and $\alpha = \zeta_9 + \zeta_9^{-1}$. Then $\mathbb{F}_{q^2} = \mathbb{F}_q(\theta)$ and $\mathbb{F}_{q^3} = \mathbb{F}_q(\alpha)$. Note that $\alpha^3 - 3\alpha + 1 = 0$. Identify $\mathbb{A}^3(\mathbb{F}_q)$ with $\mathbb{A}^1(\mathbb{F}_{q^3})$ by $f : (x,y,z) \mapsto x + y\alpha + z(\alpha^2 - 2)$. As in the proof of Lemma 6.4.1 one can verify that the equation

$$\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}((f(x,y,z) + \theta)/(f(x,y,z) + \overline{\theta})) = 1$$

is equivalent to

$$F(x,y,z) = x^2 - x - y^2 + yz - z^2 = 0.$$

Denote by U the hyperplane $V(F(x,y,z))$ in $\mathbb{A}^3$. Let $P = (0,0,0)$. The tangent plane to U at P is given by the equation $x = 0$. Note that, since -3 is not a square in $\mathbb{F}_q$, the only solution to $F(0,y,z) = 0$ over $\mathbb{F}_q$ is $(y,z) = (0,0)$ (but this statement is not true over $\overline{\mathbb{F}}_q$; U contains, for example, the line $(0, -\zeta_3 t, t)$). Given $a, b \in \mathbb{F}_q$ the line (t, at, bt) hits U at $t = 0$ and

$$t = 1/(1 - a^2 + ab - b^2).$$

One therefore defines a birational map $g : \mathbb{A}^2 \to \mathbb{A}^3$ by

$$g : (a,b) \mapsto \left(\frac{1}{1 - a^2 + ab - b^2}, \frac{a}{1 - a^2 + ab - b^2}, \frac{b}{1 - a^2 + ab - b^2} \right).$$

Finally, the map decomp_6 from $\mathbb{A}^2$ to $G_{q,6}$ is $(f(g(a,b)) + \theta)/((f(g(a,b)) + \overline{\theta})$. It is then straightforward to compute comp_6.

Exercise 6.4.5. Let q be a prime power and ζ_9 a primitive 9-th root of unity in $\overline{\mathbb{F}}_q$. Show that $\mathbb{F}_q(\zeta_9) = \mathbb{F}_{q^6}$ if and only if $q \equiv 2, 5 \pmod 9$.

In principle one can write down the partial group operations on $\mathbb{A}^2$ induced from $G_{q,6}$, but this is not an efficient way to compute. Instead, to compute $\mathrm{comp}_6(g^n)$ from $\mathrm{comp}_6(g)$ one decompresses to obtain an element $g \in G_{q,6}$ (or $G_{q^3,2}$), computes g^n, and then compresses again.

6.4.2 XTR

An excellent survey of work in this area is the thesis of Stam [579].

The Galois group of $\mathbb{F}_{q^6}/\mathbb{F}_{q^2}$ is cyclic of order 3 and generated by the q^2-power Frobenius map σ. One can consider the set $G_{q,6}/\langle\sigma\rangle = G_{q,6}/\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ of equivalence classes under the relation $g \equiv \sigma^i(g)$ for $0 \leq i \leq 2$. This gives an algebraic group quotient. which was named **XTR**[8] by Lenstra and Verheul. The goal is to give a compressed representation for this quotient; this is achieved by using the trace with respect to $\mathbb{F}_{q^6}/\mathbb{F}_{q^2}$.

Lemma 6.4.6. *Let $g \in G_{q,6}$. Let $t = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g) \in \mathbb{F}_{q^2}$. Then $\mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g) = g^{1+q^2+q^4} = 1$ and the characteristic polynomial of g over $\mathbb{F}_{q^2}$ is $\chi_g(x) = x^3 - tx^2 + t^q x - 1$.*

Proof: The first claim follows since $g^{q^2-q+1} = 1$ and $(q^2-q+1)(q^2+q+1) = q^4+q^2+1$. Now, write $(x-g)(x-g^{q^2})(x-g^{q^4}) = x^3 - tx^2 + sx - 1$. Since this polynomial is fixed by $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ it follows that $s, t \in \mathbb{F}_{q^2}$. Indeed, $t = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g) = g + g^{q^2} + g^{q^4} = g + g^{q-1} + g^{-q}$. Also

$$s = g^{1+q^2} + g^{1+q^4} + g^{q^2+q^4} = g^q + g^{1-q} + g^{-1}.$$

Finally, $s^q = g^{q^2} + g^{q^2-q} + g^{-q} = t$, from which we have $s = t^q$. □

This result shows that one can represent an equivalence class of $g \in G_{q,6}/\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ using a single element $t \in \mathbb{F}_{q^2}$, as desired. It remains to explain how to perform exponentiation in the quotient (as usual, the quotient structure is not a group and so it makes no sense to try to compute a general group operation on it).

Exercise 6.4.7. Write $f(x) = x^3 - tx^2 + t^q x - 1$ for $t \in \mathbb{F}_{q^2}$. Prove that if $f(a) = 0$ for $a \in \overline{\mathbb{F}}_q$ then $f(a^{-q}) = 0$. Hence prove that either $f(x)$ is irreducible over $\mathbb{F}_{q^2}$ or splits completely over $\mathbb{F}_{q^2}$.

Definition 6.4.8. Fix $g \in G_{q,6}$. For $n \in \mathbb{Z}$ write $t_n = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g^n)$.

Lemma 6.4.9. *Let the notation be as above. Then, for $n, m \in \mathbb{Z}$,*

1. $t_{-n} = t_{nq} = t_n^q$.
2. $t_{n+m} = t_n t_m - t_m^q t_{n-m} + t_{n-2m}$.

Proof: We have $t_n = g^n + g^{n(q-1)} + g^{n(-q)}$ The first statement follows from the proof of Lemma 6.4.6, where it is proved that $t^q = g^q + g^{1-q} + g^{-1} = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g^{-1})$.

For the second statement, an elementary calculation verifies that

$$\begin{aligned} t_n t_m - t_{n+m} &= (g^n + g^{n(q-1)} + g^{-nq})(g^m + g^{m(q-1)} + g^{-mq}) - (g^{n+m} + g^{(n+m)(q-1)} + g^{-(n+m)q}) \\ &= g^{n+m(q-1)} + g^{n-mq} + g^{n(q-1)+m} + g^{n(q-1)-mq} + g^{-nq+m} + g^{-nq+m(q-1)}. \end{aligned}$$

This is equal to $t_m^q t_n - t_{n-2m}$. □

It remains to give a ladder algorithm to compute t_n. In this case one can work with triples (t_{n+1}, t_n, t_{n-1}) of 'adjacent' values centered at t_n. This is the **XTR representation** of Lenstra and Verheul. Note that, given $t_1 = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g)$ one can compute the triple $(t_1, t_0, t_{-1}) = (t_1, 3, t_1^q)$. Given a triple (t_{n+1}, t_n, t_{n-1}) and t_1 one can compute the triple centered at t_{2n} or t_{2n+1} using the following exercise.

Exercise 6.4.10. Prove that

[8] XTR is an abbreviation for ECSTR, which stands for "Efficient and Compact Subgroup Trace Representation".

1. $t_{2n-1} = t_{n-1}t_n - t_1^q t_n^q + t_{n+1}^q$;
2. $t_{2n} = t_n^2 - 2t_n^q$;
3. $t_{2n+1} = t_{n+1}t_n - t_1 t_n^q + t_{n-1}^q$.

Exercise 6.4.11. If one uses triples (t_{n+1}, t_n, t_{n-1}) as above then what is the cost of a square or square-and-multiply in $G_{q,6}$?

Exercise 6.4.12.★ Give a more efficient ladder for XTR, for which the cost of squaring and square-and-multiply are the same.

In other words, one can compute $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g^n)$ from $t = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g)$ using polynomial arithmetic and so $G_{q,6}/\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ is an algebraic group quotient. Performing discrete logarithm based cryptography in this setting is called the **XTR cryptosystem**. To solve the discrete logarithm problem in $G_{q,6}/\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^2})$ one usually lifts the problem to the **covering group** $G_{q,6} \subset \mathbb{F}_{q^6}^*$ by taking any root of the polynomial $x^3 - tx^2 + t^q x - 1$. For further details about efficient arithmetic using XTR we refer to [579].

Exercise 6.4.13. Represent $\mathbb{F}_{67^2}$ as $\mathbb{F}_{67}(i)$ where $i^2 = -1$. Given that $t_1 = \mathrm{Tr}_{\mathbb{F}_{67^6}/\mathbb{F}_{67^2}}(g) = 48 + 63i$ for some $g \in G_{67,6}$ compute $t_7 = \mathrm{Tr}_{\mathbb{F}_{67^6}/\mathbb{F}_{67^2}}(g^7)$.

Exercise 6.4.14. (The Gong-Harn cryptosystem [259]) Consider the quotient $G'_{q,3} = G_{q,3}/\langle\sigma\rangle$ where σ is the q-power Frobenius in $\mathbb{F}_{q^3}$. Fix $g \in G_{q,3}$ and define $t_n = g^n + g^{nq} + g^{nq^2} \in \mathbb{F}_q$. Show that the characteristic polynomial for g is $x^3 - t_1 x^2 + t_{-1}x - 1$. Hence, show that an element of $G'_{q,3}$ can be represented using two elements of $\mathbb{F}_q$. Show that

$$t_{n+m} = t_n t_m - t_{n-m}t_{-m} + t_{n-2m}$$

Hence develop a ladder algorithm for exponentiation in $G'_{q,3}$.

Exercise 6.4.15. (Shirase, Han, Hibino, Kim and Takagi [551]) Let $q = 3^m$ with m odd. Show that $(q - \sqrt{3q} + 1)(q + \sqrt{3q} + 1) = q^2 - q + 1$. Let $g \in \mathbb{F}_{3^{6m}}^*$ have order dividing $q - \sqrt{3q} + 1$. Show that $g^{q+1} = g^{\sqrt{3q}}$ and $g^{q^3+1} = 1$. Let $t = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g)$ and $s = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_q}(g)$. Show that the roots of $x^2 - sx + s^{\sqrt{3q}}$ are t and t^q.

Hence, one can use s as a compressed representative for g; requiring only half the storage of XTR. To compute $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_q}(g^n)$ one solves the quadratic to obtain t, computes $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(g^n)$ using the XTR formulae, and then performs the further compression.

6.5 Further Remarks

Granger and Vercauteren [266] have proposed an index calculus algorithm for $\mathbb{T}_n(\mathbb{F}_{p^m})$ where $m > 1$. Kohel [351] has shown that one might map the discrete logarithm problem in an algebraic torus $\mathbb{T}_n(\mathbb{F}_q)$ to the discrete logarithm problem in the generalised Jacobian (which is a certain type of divisor class group) of a singular hyperelliptic curve over $\mathbb{F}_q$. This latter problem might be attacked using an index calculus method such as Gaudry's algorithm (see Section 15.6.3). It seems this approach will not be faster than performing index calculus methods in $\mathbb{F}_{p^n}^*$, but further investigation would be of interest.

6.6 Algebraic Tori over Rings

Applications in factoring and primality testing motivate the study of tori over $\mathbb{Z}/N\mathbb{Z}$. As mentioned in Section 4.4, the simplest approach is to restrict to N being square-free

and to use the Chinese remainder theorem to define the groups. First we explain how to construct rings isomorphic to the direct product of finite fields.

Example 6.6.1. Let $N = \prod_{i=1}^{k} p_i$ be square-free. Let $F(x) = x^2 + Ax + B \in \mathbb{Z}[x]$ be a quadratic polynomial such that $F(x)$ is irreducible modulo p_i for all $1 \leq i \leq k$. Define $R = (\mathbb{Z}/N\mathbb{Z})[x]/(F(x))$. By the Chinese remainder theorem, $R \cong \oplus \mathbb{F}_{p_i^2}$. We will usually write θ for the image of x in R and $\overline{\theta} = -A - x = Bx^{-1}$.

Define $G_{N,2}$ to be the subgroup of R^* of order $\prod_{i=1}^{k}(p_i + 1)$ isomorphic to the direct sum of the groups $G_{p_i,2}$. Note that $G_{N,2}$ is not usually cyclic.

We would like to represent a "general" element of $G_{N,2}$ using a single element of $\mathbb{Z}/N\mathbb{Z}$. In other words, we would like to have a map from $\mathbb{Z}/N\mathbb{Z}$ to $G_{N.2}$. One can immediately apply Definition 6.3.7 to obtain the map $a \mapsto (a+\theta)/(a+\overline{\theta})$. Since the reduction modulo p_i of this map correctly maps to $G_{p_i,2}$, for each prime p_i, it follows that it correctly maps to $G_{N,2}$. Hence, we can identify $\mathbb{T}_2(\mathbb{Z}/N\mathbb{Z})$ with $\mathbb{Z}/N\mathbb{Z}$. The group operation $\star$ from Lemma 6.3.12 can also be applied in $\mathbb{Z}/N\mathbb{Z}$ and its correctness follows from the Chinese remainder theorem.

Note that the image of $\mathbb{Z}/N\mathbb{Z}$ in $G_{N.2}$ under this map has size $N = \prod p_i$, whereas $G_{N,2}$ has order $\prod_i (p_i + 1)$. Hence, there are many elements of $G_{N,2}$ that are missed by the decompression map. Note that these "missed" elements are those which correspond to the identity element of $G_{p_i,2}$ for at least one prime p_i. In other words, they are of the form $g = u + v\theta$ where $\gcd(v, N) > 1$.

Similarly, Lucas sequences can be used modulo N when N is square-free, and their properties follow from the properties modulo p_i for all prime factors p_i of N. However, one should be careful when interpreting the Galois theory. In Section 6.3.2 the non-trivial element of $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ is written as $\sigma(g) = g^q$, but this formulation does not naturally generalise to the ring R of Example 6.6.1. Instead, define $\sigma(u + v\theta) = u + v\overline{\theta}$ so that $\sigma : R \to R$ is a ring homomorphism and $\sigma(g) \pmod{p_i} = \sigma(g \pmod{p_i})$. One can then define the trace map $\mathrm{Tr}_{R/(\mathbb{Z}/N\mathbb{Z})}(g) = g + \sigma(g)$. The theory of Section 6.3.2 can then immediately be adapted to give Lucas sequences modulo N.

Exercise 6.6.2. Let $N = \prod_{i=1}^{k} p_i$ be a square-free integer and let R be as in Example 6.6.1. Let $g \in G_{N,2}$. Determine how many elements $h \in G_{N,2}$, in general, satisfy $\mathrm{Tr}_{R/(\mathbb{Z}/N\mathbb{Z})}(h) = \mathrm{Tr}_{R/(\mathbb{Z}/N\mathbb{Z})}(g)$. Show that roughly $N/2^k$ of the values $V \in \mathbb{Z}/N\mathbb{Z}$ correspond to the trace of an element in $G_{N,2}$.

Using similar methods to the above it is straightforward to adapt the torus $\mathbb{T}_6$ and XTR to the ring $\mathbb{Z}/N\mathbb{Z}$ when N is square-free. We leave the details to the reader.