Chapter 4

Preliminary Remarks on Algebraic Groups

For efficient public key cryptography based on discrete logarithms one would like to have groups for which computing g^n is as fast as possible, the representation of group elements is as small as possible, and for which the DLP (see Definition 2.1.1 or 13.0.1) is (at least conjecturally) as hard as possible.

If g is a group element of order r then one needs at least $\log_2(r)$ bits to represent an arbitrary element of $\langle g \rangle$. This optimal size can be achieved by using the **exponent representation**, i.e., represent g^a as $a \in \mathbb{Z}/r\mathbb{Z}$. However, the DLP is not hard when this representation is used.

Ideally, for any cyclic group G of order r, one would like to be able to represent arbitrary group elements (in a manner which does not then render the DLP trivial) using roughly $\log_2(r)$ bits. This can be done in some cases (e.g., elliptic curves over finite fields with a prime number of points) but it is unlikely that it can always be done. Using algebraic groups over finite fields is a good way to achieve these conflicting objectives.

4.1 Informal Definition of an Algebraic Group

The subject of algebraic groups is large and has an extensive literature. Instead of presenting the full theory, in this book we present only the algebraic groups that are currently believed to be useful in public key cryptography. Informally[1], an **algebraic group** over a field $\Bbbk$ is a group such that:

- Group elements are specified as n-tuples of elements in a field $\Bbbk$;

[1] We refrain from giving a formal definition of algebraic groups; mainly as it requires defining products of projective varieties.

- The group operations (multiplication and inversion) can be performed using only polynomial equations (or ratios of polynomials) defined over $\Bbbk$. In other words, we have polynomial or rational maps mult : $\Bbbk^{2n} \to \Bbbk^n$ and inverse : $\Bbbk^n \to \Bbbk^n$. There is not necessarily a single n-tuple of polynomial equations that defines mult for all possible pairs of group elements.

An algebraic group quotient is the set of equivalence classes of an algebraic group under some equivalence relation (see Section 4.3 for an example). Note that, in general, an algebraic group quotient is not a group.

We stress that being an algebraic group is not a group-theoretic property; it is a property of a particular description of the group. Perhaps it helps to give an example of a group whose usual representation is not an algebraic group.

Example 4.1.1. Let $n \in \mathbb{N}$ and let S_n be the group of permutations on n symbols. Permutations can be represented as an n-tuple of distinct integers from the set $\{1, 2, \dots, n\}$. The composition $(x_1, \dots, x_n) \circ (y_1, \dots, y_n)$ of two permutations is $(x_{y_1}, x_{y_2}, \dots, x_{y_n})$. Since x_{y_1} is not a polynomial, the usual representation of S_n is not an algebraic group. However, S_n can be represented as a subgroup of the matrix group $GL_n(\Bbbk)$ (for any field $\Bbbk$), which is an algebraic group.

Our main interest is algebraic groups over finite fields $\mathbb{F}_q$. For each example of an algebraic group (or quotient) G we will explain how to achieve the following basic functionalities:

- Efficient group operations in G (typically requiring $O(\log(q)^2)$ bit operations);
- Compact representation of elements of G (typically $O(\log(q))$ bits);
- Generating cryptographically suitable G in polynomial-time (i.e., $O(\log(q)^c)$ for some (small) $c \in \mathbb{N}$);
- Generating random elements in G in polynomial-time;
- Hashing from $\{0, 1\}^l$ to G or from G to $\{0, 1\}^l$ in polynomial-time.

In order to be able to use an algebraic group (or quotient) G for cryptographic applications we need some or all of these functionalities, as well as requiring the discrete logarithm problem (and possibly other computational problems) to be hard.

We sometimes use the notation AG to mean "algebraic group in the context of this book"; similarly AGQ means "algebraic group quotient in the context of this book". The aim of this part of the book is to describe the algebraic groups of relevance for public key cryptography (namely, multiplicative groups, algebraic tori, elliptic curves and divisor class groups). As is traditional, we will use multiplicative notation for the group operation in multiplicative groups and tori, and additive notation for the group operation on elliptic curves and divisor class groups of hyperelliptic curves. In Parts III and V, when we discuss cryptographic applications, we will always use multiplicative notation for algebraic groups.

The purpose of this chapter is to give the simplest examples of algebraic groups and quotients. The later chapters introduce enough algebraic geometry to be able to define the algebraic groups of interest in this book and prove some important facts about them.

4.2 Examples of Algebraic Groups

The simplest examples of algebraic groups are the **additive group** G_a and **multiplicative group** G_m of a field $\Bbbk$. For $G_a(\Bbbk)$ the set of points is $\Bbbk$ and the group operation is given by the polynomial $\mathrm{mult}(x, y) = x + y$ (for computing the group operation) and $\mathrm{inverse}(x) = -x$ (for computing inverses). For $G_m(\Bbbk)$ the set of points is $\Bbbk^* = \Bbbk - \{0\}$ and the group operation is given by the polynomial $\mathrm{mult}(x, y) = xy$ and the rational function $\mathrm{inverse}(x) = 1/x$ (Example 5.1.5 shows how to express $G_m(\Bbbk)$ as an algebraic set).

The additive group is useless for cryptography since the discrete logarithm problem is easy. The discrete logarithm problem is also easy for the multiplicative group over certain fields (e.g., if $g \in \mathbb{R}^*$ then the discrete logarithm problem in $\langle g \rangle \subseteq \mathbb{R}^*$ is easy due to algorithms that compute approximations to the natural logarithm function). However, $G_m(\mathbb{F}_q)$ is useful for cryptography and will be one of the main examples used in this book.

The other main examples of algebraic groups in public key cryptography are algebraic tori (see Chapter 6), elliptic curves and divisor class groups of hyperelliptic curves.

4.3 Algebraic Group Quotients

Quotients of algebraic groups are used to reduce the storage and communication requirements of public key cryptosystems. Let G be a group with an automorphism ψ such that $\psi^n = 1$ (where $1 : G \to G$ is the identity map and ψ^n is the n-fold composition $\psi \circ \cdots \circ \psi$). We define $\psi^0 = 1$. Define the **orbit** or **equivalence class** of $g \in G$ under ψ to be $[g] = \{\psi^i(g) : 0 \le i < n\}$. Define the **quotient** as the set of orbits under ψ. In other words

$$G/\psi = \{[g] : g \in G\}.$$

We call G the **covering group** of a quotient G/ψ. In general, the group structure of G does not induce a group structure on the quotient G/ψ. Nevertheless, we can define exponentiation on the quotient by $[g]^n = [g^n]$ for $n \in \mathbb{Z}$. Since exponentiation is the fundamental operation for many cryptographic applications it follows that quotients of algebraic groups are sufficient for many cryptographic applications.

Lemma 4.3.1. *Let $n \in \mathbb{Z}$ and $[g] \in G/\psi$, then $[g]^n$ is well-defined.*

Proof: Since ψ is a group homomorphism we have $\psi^i(g)^n = \psi^i(g^n)$ and so for each $g_1 \in [g]$ we have $g_1^n \in [g^n]$. □

The advantage of algebraic group quotients G/ψ is that they can require less storage than the original algebraic group G. We now give an example of this.

Example 4.3.2. Let p be an odd prime. Consider the subgroup $G \subset \mathbb{F}_{p^2}^*$ of order $p + 1$. Note that $\gcd(p - 1, p + 1) = 2$ so $G \cap \mathbb{F}_p^* = \{1, -1\}$. If $g \in G$ then we have $g^{p+1} = 1$, which is equivalent to $g^p = g^{-1}$. Let ψ be the automorphism $\psi(g) = g^p$. Then $\psi^2 = 1$ in $\mathbb{F}_{p^2}$ and the orbits $[g]$ in G/ψ all have size 2 except for $[1]$ and $[-1]$.

The natural representation for elements of $G \subseteq \mathbb{F}_{p^2}$ is a pair of elements of $\mathbb{F}_p$. However, since $\#(G/\psi) = 2 + (p - 1)/2$ one might expect to be able to represent elements of G/ψ using just one element of $\mathbb{F}_p$.

Let $g \in G$. Then the elements of $[g] = \{g, g^p\}$ are the roots of the equation $x^2 - tx + 1$ in $\mathbb{F}_{p^2}$ where $t = g + g^p \in \mathbb{F}_p$. Conversely, each $t \in \mathbb{F}_p$ such that the roots of $x^2 - tx + 1$ are Galois conjugates corresponds to a class $[g]$ (the values $t = \pm 2$ correspond to $[1]$ and $[-1]$). Hence, one can represent an element of G/ψ by the trace t. We therefore require half the storage compared with the standard representation of $G \subset \mathbb{F}_{p^2}$.

In Section 6.3.2 we show that, given the trace t of g, one can compute the trace t_n of g^n efficiently using Lucas sequences (though there is a slight catch, namely that we have to work with a pair (t_n, t_{n-1}) of traces).

Another important example of an algebraic group quotient is elliptic curve arithmetic using x-coordinates only. This is the quotient of an elliptic curve by the equivalence relation $P \equiv -P$.

4.4 Algebraic Groups over Rings

Algebraic geometry is traditionally studied over fields. However, several applications (both algorithmic and cryptographic) will exploit algebraic groups or algebraic group quotients over $\mathbb{Z}/N\mathbb{Z}$ (we do not consider general rings).

Let $N = \prod_{i=1}^k p_i$ be square-free (the non-square-free case is often more subtle). By the Chinese remainder theorem, $\mathbb{Z}/N\mathbb{Z}$ is isomorphic as a ring to $\oplus_{i=1}^k \mathbb{F}_{p_i}$ (where $\oplus$ denotes the direct sum of rings). Hence, if G is an algebraic group then it is natural to define

$$G(\mathbb{Z}/N\mathbb{Z}) = \bigoplus_{i=1}^{k} G(\mathbb{F}_{p_i}) \tag{4.1}$$

(where $\oplus$ now denotes the direct sum of groups). A problem is that this representation for $G(\mathbb{Z}/N\mathbb{Z})$ does not satisfy the natural generalisation to rings of our informal definition of an algebraic group. For example, group elements are not n-tuples over the ring, but over a collection of different fields. Also the value n is no longer bounded.

The challenge is to find a representation for $G(\mathbb{Z}/N\mathbb{Z})$ that uses n-tuples over $\mathbb{Z}/N\mathbb{Z}$ and satisfies the other properties of the informal definition. Example 4.4.1 shows that this holds for the additive and multiplicative groups.

Example 4.4.1. Let $N = \prod_i p_i$ where the p_i are distinct primes. Then, using the definition in equation (4.1),

$$G_a(\mathbb{Z}/N\mathbb{Z}) \cong \bigoplus_i G_a(\mathbb{F}_{p_i}) \cong \bigoplus_i \mathbb{F}_{p_i} \cong \mathbb{Z}/N\mathbb{Z}.$$

Similarly,

$$G_m(\mathbb{Z}/N\mathbb{Z}) \cong \bigoplus_i G_m(\mathbb{F}_{p_i}) \cong \bigoplus_i \mathbb{F}_{p_i}^* \cong (\mathbb{Z}/N\mathbb{Z})^*.$$

Hence, both groups can naturally be considered as algebraic groups over $\mathbb{Z}/N\mathbb{Z}$.

Note that $G_m(\mathbb{Z}/N\mathbb{Z})$ is not cyclic when N is square-free but not prime.

To deal with non-square-free N it is necessary to define $G(\mathbb{Z}/p^n\mathbb{Z})$. The details of this depend on the algebraic group. For G_a and G_m it is straightforward and we still have $G_a(\mathbb{Z}/N\mathbb{Z}) = \mathbb{Z}/N\mathbb{Z}$ and $G_m(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^*$. For other groups it can be more complicated.