Appendix A

Background Mathematics

For convenience, we summarise some notation, conventions, definitions and results that will be used in the book. This chapter is for reference only.

A.1 Basic Notation

We write $\mathbb{R}$ for the real numbers and define $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} : x \geq 0\}$ and similarly for $\mathbb{R}_{>0}$. We write $\mathbb{Z}$ for the integers and $\mathbb{N} = \mathbb{Z}_{>0} = \{n \in \mathbb{Z} : n > 0\} = \{1, 2, 3, \ldots\}$ for the natural numbers.

We write $\#S$ for the number of elements of a finite set S. If S, T are sets we write $S - T$ for the set difference $\{s \in S : s \notin T\}$. We denote the empty set by $\varnothing$.

We write $\mathbb{Z}/n\mathbb{Z}$ for the ring of integers modulo n (many authors write $\mathbb{Z}_n$). When n is a prime and we are using the field structure of $\mathbb{Z}/n\mathbb{Z}$ we prefer to write $\mathbb{F}_n$. The statement $a \equiv b \pmod{n}$ means that $n \mid (a - b)$. We follow a common mis-use of this notation by writing $b \pmod{n}$ for the integer $a \in \{0, 1, \ldots, n-1\}$ such that $a \equiv b \pmod{n}$. Hence, the statement $a = b \pmod{n}$ is an assignment of a to the value of the operator $b \pmod{n}$ and should not be confused with the predicate $a \equiv b \pmod{n}$.

The word **map** $f : X \to Y$ means a function on some subset of X. In other words a map is not necessarily defined everywhere. Usually the word **function** implicitly means "defined everywhere on X", though this usage does not apply in algebraic geometry where a rational function is actually a rational map. If $f : X \to Y$ is a map and $U \subset X$ then we write $f|_U$ for the restriction of f to U, which is a map $f|_U : U \to Y$.

If $P = (x_P, y_P)$ is a point and f is a function on points then we write $f(x_P, y_P)$ rather than $f((x_P, y_P))$ for $f(P)$. We write $f \circ g$ for composition of functions (i.e., $(f \circ g)(x) = f(g(x))$); the notation fg will always mean product (i.e., $fg(P) = f(P)g(P)$). The notation f^n usually means exponentiating the value of the function f to the power n, except when f is an endomorphism of an elliptic curve (or Abelian variety), in which

context it is standard to write f^n for n-fold composition. Hence, we prefer to write $f(P)^n$ than $f^n(P)$ when denoting powering (and so we write $\log(x)^n$ rather than $\log^n(x)$).

A.2 Groups

Let G be a group and $g \in G$. The **subgroup generated by** g is $\langle g \rangle = \{g^a : a \in \mathbb{Z}\}$. The **order** of the element g is the number of elements in the group $\langle g \rangle$. The **exponent** of a finite group is the smallest positive integer n such that $g^n = 1$ for all $g \in G$.

Let G be a finite Abelian group. The classification of finite Abelian groups (see Theorem II.2.1 of [301] or Section I.8 of [367]) states that G is isomorphic to a direct sum of cyclic groups of orders $m_1, m_2, \ldots, m_t$ such that $m_1 \mid m_2 \mid \cdots \mid m_t$.

A.3 Rings

All rings in this book have a multiplicative identity 1. For any ring R, the smallest positive integer n such that $n1 = 0$ is called the **characteristic** of the ring and is denoted $\mathrm{char}(R)$. If there is no such n then we define $\mathrm{char}(R) = 0$.

If R is a ring and $n \in \mathbb{N}$ then we write $M_n(R)$ for the ring of $n \times n$ matrices with entries in R.

If R is a ring then R^* is the multiplicative group of invertible elements of R. The **Euler phi function** $\varphi(n)$ is the order of $(\mathbb{Z}/n\mathbb{Z})^*$. One has

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Theorem A.3.1. *There exists $N \in \mathbb{N}$ such that $\varphi(n) > n/(3\log(\log(n)))$ for all $n \in \mathbb{N}_{>N}$.*

Proof: Theorem 328 of [276] states that

$$\liminf_{n \to \infty} \frac{\varphi(n)\log(\log(n))}{n} = e^{-\gamma}$$

where $\gamma \approx 0.57721566$ is the Euler-Mascheroni constant. Since $e^{-\gamma} \approx 0.56 > 1/3$ the result follows from the definition of $\liminf$. □

An element $a \in R$ is **irreducible** if $a \notin R^*$ and $a = bc$ for $b, c \in R$ implies $b \in R^*$ or $c \in R^*$. We write $a \mid b$ for $a, b \in R$ if there exists $c \in R$ such that $b = ac$. An element $a \in R$ is **prime** if $a \mid bc$ implies $a \mid b$ or $a \mid c$.

An integral domain R is a **unique factorisation domain** (UFD) if each $a \in R$ can be written uniquely (up to ordering and multiplication by units) as a product of irreducibles. In a UFD an element is prime if and only if it is irreducible.

A.4 Modules

Let R be a ring. An R-module M is an Abelian group, written additively, with an operation rm for $r \in R$ and $m \in M$, such that $(r_1 + r_2)m = r_1 m + r_2 m$ and $r(m_1 + m_2) = rm_1 + rm_2$. An R-module M is **finitely generated** if there is a set $\{m_1, \ldots, m_k\} \subset M$ such that $M = \{\sum_{i=1}^k r_i m_i : r_i \in R\}$.

A finitely generated R-module M is a **free module** if there is a set $\{m_1, \ldots, m_k\}$ that generates M and is such that $0 = \sum_{i=1}^k r_i m_i$ if and only if $r_i = 0$ for all $1 \leq i \leq k$. Such an R-module is said to have **rank** k.

Let R be a commutative ring, M an R-module and $\Bbbk$ a field containing R. Consider the set of all symbols of the form $m \otimes a$ where $m \in M$, $a \in \Bbbk$ under the equivalence relation $rm \otimes a \equiv m \otimes ra$ for $r \in R$, $(m_1 + m_2) \otimes a = (m_1 \otimes a) + (m_1 \otimes a)$ and $m \otimes (a_1 + a_2) = (m \otimes a_1) + (m \otimes a_2)$. The **tensor product** $M \otimes_R \Bbbk$ is the set of all equivalence classes of such symbols. If M is a finitely generated free R-module with generating set $\{m_1, \ldots, m_k\}$ then $M \otimes_R \Bbbk$ is a $\Bbbk$-vector space of dimension k with basis $\{m_1 \otimes 1, \ldots, m_k \otimes 1\}$.

A.5 Polynomials

Let R be a commutative ring. Denote by $R[\underline{x}] = R[x_1, \ldots, x_n]$ the set of polynomials over R in n variables. We write $\deg_{x_i}(F(x_1, \ldots, x_n))$ to be the degree as a polynomial in x_i with coefficients in $R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. For polynomials $F(x) \in R[x]$ we write $\deg(F(x))$ for $\deg_x(F(x))$. The **total degree** of a polynomial $F(\underline{x}) = \sum_{i=1}^l F_i x_1^{m_{i,1}} \cdots x_n^{m_{i,n}}$ (with $F_i \neq 0$) is $\deg(F) = \max_{1 \leq i \leq l} \sum_{j=1}^n m_{i,j}$.

Let R be a commutative ring with a unit 1. A degree d polynomial in $R[x]$ is **monic** if the coefficient of x^d is 1.

A polynomial $F(\underline{x}) \in R[\underline{x}]$ is divisible by $G(\underline{x}) \in R[\underline{x}]$ if there exists a polynomial $H(\underline{x}) \in R[\underline{x}]$ such that $F(\underline{x}) = G(\underline{x})H(\underline{x})$. A polynomial $F(\underline{x}) \in R[\underline{x}]$ is **irreducible** over R (also called R-irreducible) if whenever $F(\underline{x}) = G(\underline{x})H(\underline{x})$ with $G(\underline{x}), H(\underline{x}) \in R[\underline{x}]$ then either G or H is a constant polynomial.

There are various ways to show that a polynomial is irreducible. **Eisenstein's criteria** states that $F(x) = \sum_{i=0}^n F_i x^i \in R[x]$, where R is a UFD, is irreducible if there is a prime p in R such that $p \nmid F_n$, $p \mid F_i$ for $0 \leq i < n$, and $p^2 \nmid F_0$. We refer to Proposition III.1.14 of [589], Theorem IV.3.1 of [367] or Theorem III.6.15 of [301] for proofs.

If $\Bbbk$ is a field then the polynomial ring $\Bbbk[x_1, \ldots, x_n]$ is a UFD (Theorem III.6.14 of [301]). Let $F(x) \in \Bbbk[x]$ be a polynomial in one variable of degree d. Then either $F = 0$ or else $F(x)$ has at most d roots in $\Bbbk$.

Lemma A.5.1. *Let $N_{d,q}$ be the number of monic irreducible polynomials of degree d in $\mathbb{F}_q[x]$. Then $q^d/2d \leq N_{d,q} \leq q^d/d$.*

Proof: See Theorem 20.11 of [556] or Exercise 3.27 of [388]. A more precise result is given in Theorem 15.5.12. □

Let $F(x) \in \Bbbk[x]$. One can define the **derivative** $F'(x)$ by using the rule $(F_n x^n)' = nF_n x^{n-1}$ for $n \geq 0$ for each monomial. This is a formal algebraic operation and does not require an interpretation in terms of calculus.

Lemma A.5.2. *Let $F_1(x), F_2(x) \in \Bbbk[x]$. Then*

1. $(F_1(x) + F_2(x))' = F_1'(x) + F_2'(x)$.
2. $(F_1(x)F_2(x))' = F_1(x)F_2'(x) + F_2(x)F_1'(x)$.
3. $(F_1(F_2(x))' = F_1'(F_2(x))F_2'(x)$
4. *If* $\mathrm{char}(\Bbbk) = p$ *then* $F'(x) = 0$ *if and only* $F(x) = G(x)^p$ *for some* $G(x) \in \Bbbk[x]$.

Similarly, the notation $\partial F/\partial x_i$ is used for polynomials $F(\underline{x}) \in \Bbbk[\underline{x}]$ and an analogue of Lemma A.5.2 holds.

A.5.1 Homogeneous Polynomials

Definition A.5.3. A non-zero polynomial $F(\underline{x}) \in \Bbbk[\underline{x}]$ is **homogeneous** of degree d if all its monomials have degree d, i.e.,

$$F(x_0, \ldots, x_n) = \sum_{\substack{i_0, i_1, \ldots, i_n \in \mathbb{Z}_{\geq 0} \\ i_0 + i_1 + \cdots i_n = d}} F_{i_0, i_1, \ldots, i_n} x_0^{i_0} x_1^{i_1} \cdots x_n^{i_n}.$$

Any polynomial $F(\underline{x}) \in \Bbbk[x_0, \ldots, x_n]$ can be written as a **homogeneous decomposition** $\sum_{i=0}^{m} F_i(\underline{x})$ for some $m \in \mathbb{N}$ where $F_i(\underline{x})$ is a homogeneous polynomial of degree i; see Section II.3 of [367].

Lemma A.5.4. *Let R be an integral domain.*

1. *If $F(x) \in R[x_0, \ldots, x_n]$ is homogeneous and $\lambda \in R$ then $F(\lambda x_0, \ldots, \lambda x_n) = \lambda^d F(x_0, \ldots, x_n)$.*
2. *If $F_1, F_2 \in R[x_0, \ldots, x_n]$ are non-zero and homogeneous of degrees r and s respectively then $F_1(\underline{x})F_2(\underline{x})$ is homogeneous of degree $r + s$.*
3. *Let $F_1, F_2 \in R[x_0, \ldots, x_n]$ be non-zero. If $F_1(\underline{x})F_2(\underline{x})$ is homogeneous then $F_1(\underline{x})$ and $F_2(\underline{x})$ are both homogeneous.*

Proof: See Exercise 1-1 (page 6) of Fulton [216]. □

A.5.2 Resultants

Let R be a commutative integral domain. Let $F(x) = F_n x^n + F_{n-1} x^{n-1} + \cdots + F_0$ and $G(x) = G_m x^m + G_{n-1} x^{n-1} + \cdots + G_0$ be two polynomials over R with $F_0, F_n, G_0, G_m \neq 0$. The polynomials $F, xF, \ldots, x^{m-1}F, G, xG, \ldots, x^{n-1}G$ can be written as $n+m$ linear combinations of the $n+m$ variables $1, x, \ldots, x^{n+m-1}$ and so the variable x may be eliminated to compute the **resultant** (there should be no confusion between the use of the symbol R for both the ring and the resultant)

$$R(F, G) = R_x(F, G) = \det \begin{pmatrix} F_0 & F_1 & \cdots & F_n & 0 & 0 & \cdots & 0 \\ 0 & F_0 & \cdots & F_{n-1} & F_n & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & F_0 & F_1 & \cdots & F_n \\ G_0 & \cdots & G_m & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & G_0 & \cdots & G_m & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & G_0 & \cdots & G_m \end{pmatrix}.$$

Theorem A.5.5. *Let $\Bbbk$ be a field and $F(x), G(x) \in \Bbbk[x]$. Write $F(x) = \sum_{i=0}^{n} F_i x^i$ and $G(x) = \sum_{i=0}^{m} G_i x^i$. Suppose $F_0 G_0 \neq 0$. Then $R(F(x), G(x)) = 0$ if and only if $F(x)$ and $G(x)$ have a common root in $\overline{\Bbbk}$.*

Proof: See Proposition IV.8.1 and Corollary IV.8.4 of Lang [367] or Proposition 3.5.8 of Cox, Little and O'Shea [158]. □

Theorem A.5.5 is generalised to polynomials in $R[x]$ where R is a UFD in Lemma 2.6 on page 41 of Lorenzini [394]. Section IV.2.7 of [394] also describes the relation between $R(F, G)$ and the norm of $G(\alpha)$ in the number ring generated by a root α of $F(x)$.

If $F(x, y), G(x, y) \in \mathbb{Z}[x, y]$ then write $R_x(F, G) \in \mathbb{Z}[y]$ for the resultant, which is a polynomial in y, obtained by treating F and G as polynomials in x over the ring $R = \mathbb{Z}[y]$. If F and G have total degree d in x and y then the degree in y of $R_x(F, G)$ is $O(d^2)$.

A.6 Field Extensions

General references for fields and their extensions are Chapter II of Artin [14], Chapter V of Hungerford [301] or Chapter V of Lang [367].

Let $\Bbbk$ be a field. An **extension** of $\Bbbk$ is any field $\Bbbk'$ such that $\Bbbk \subseteq \Bbbk'$, in which case we write $\Bbbk'/\Bbbk$. Then $\Bbbk'$ is a vector space over $\Bbbk$. If this vector space has finite dimension then the **degree** of $\Bbbk'/\Bbbk$, denoted $[\Bbbk' : \Bbbk]$, is the vector space dimension of $\Bbbk'$ over $\Bbbk$.

An element $\theta \in \Bbbk'$ is **algebraic** over $\Bbbk$ if there is some polynomial $F(x) \in \Bbbk[x]$ such that $F(\theta) = 0$. An extension $\Bbbk'$ of $\Bbbk$ is **algebraic** if every $\theta \in \Bbbk'$ is algebraic over $\Bbbk$. If $\Bbbk'/\Bbbk$ is algebraic and $\Bbbk \subseteq \Bbbk'' \subseteq \Bbbk'$ then $\Bbbk''/\Bbbk$ and $\Bbbk'/\Bbbk''$ are algebraic. Similarly, if $\Bbbk'/\Bbbk$ is finite then $[\Bbbk' : \Bbbk] = [\Bbbk' : \Bbbk''][\Bbbk'' : \Bbbk]$.

Lemma A.6.1. *Let $\Bbbk$ be a field. Every finite extension of $\Bbbk$ is algebraic.*

Proof: See Theorem 4 of Section II.3 of [640], Proposition V.1.1 of [367], or Theorem V.1.11 of [301]. □

The **compositum** of two fields $\Bbbk$ and $\Bbbk'$ is the smallest field that contains both of them. We define $\Bbbk(\theta) = \{a(\theta)/b(\theta) : a(x), b(x) \in \Bbbk[x], b(\theta) \neq 0\}$ for any element θ. This is the smallest field that contains $\Bbbk$ and θ. For example, θ may be algebraic over $\Bbbk$ (e.g., $\Bbbk(\sqrt{-1})$) or transcendental (e.g., $\Bbbk(x)$). More generally, $\Bbbk(\theta_1, \ldots, \theta_n) = \Bbbk(\theta_1)(\theta_2)\cdots(\theta_n)$ is the field generated over $\Bbbk$ by $\theta_1, \ldots, \theta_n$. A field extension $\Bbbk'/\Bbbk$ is **finitely generated** if $\Bbbk' = \Bbbk(\theta_1, \ldots, \theta_n)$ for some $\theta_1, \ldots, \theta_n \in \Bbbk'$.

Theorem A.6.2. *Let $\Bbbk$ be a field. Suppose K is field that is finitely generated as a ring over $\Bbbk$. Then K is an algebraic extension of $\Bbbk$.*

Proof: See pages 31-33 of Fulton [216]. □

An **algebraic closure** of a field $\Bbbk$ is a field $\overline{\Bbbk}$ such that every non-constant polynomial in $\overline{\Bbbk}[x]$ has a root in $\overline{\Bbbk}$. For details see Section V.2 of [367]. We always assume that there is a fixed algebraic closure of $\Bbbk$ and we assume that every algebraic extension $\Bbbk'/\Bbbk$ is chosen such that $\Bbbk' \subset \overline{\Bbbk}$ and that $\overline{\Bbbk'} = \overline{\Bbbk}$. Since the main case of interest is $\Bbbk = \mathbb{F}_q$ this assumption is quite natural.

We recall the notions of separable and purely inseparable extensions (see Sections V.4 and V.6 of Lang [367], Section V.6 of Hungerford [301] or Sections A.7 and A.8 of Stichtenoth [589]). An element α, algebraic over a field $\Bbbk$, is **separable** (respectively, **purely inseparable**) if the minimal polynomial of α over $\Bbbk$ has distinct roots (respectively, one root) in $\overline{\Bbbk}$. Hence, α is separable over $\Bbbk$ if its minimal polynomial has non-zero derivative. If $\mathrm{char}(\Bbbk) = p$ then α is purely inseparable if the minimal polynomial of α is of the form $x^{p^m} - a$ for some $a \in \Bbbk$.

Let $\Bbbk'/\Bbbk$ be a finite extension of fields and let $\alpha \in \Bbbk'$. One can define the **norm** and **trace** of α in terms of the matrix representation of multiplication by α as a linear map on the vector space $\Bbbk'/\Bbbk$ (see Section A.14 of [589] or Section IV.2 of [394]). When $\Bbbk'/\Bbbk$ is separable then an equivalent definition is to let $\sigma_i : \Bbbk' \to \overline{\Bbbk}$ be the $n = [\Bbbk' : \Bbbk]$ distinct embeddings (i.e., injective field homomorphisms), then the norm of $\alpha \in \Bbbk'$ is $N_{\Bbbk'/\Bbbk}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ and the **trace** is $\mathrm{Tr}_{\Bbbk'/\Bbbk}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$.

An element $x \in K$ is **transcendental** over $\Bbbk$ if x is not algebraic over $\Bbbk$. Unless there is an implicit algebraic relation between $x_1, \ldots, x_n$ we write $\Bbbk(x_1, \ldots, x_n)$ to mean the field $\Bbbk(x_1)(x_2)\cdots(x_n)$ where each x_i is transcendental over $\Bbbk(x_1, \ldots, x_{i-1})$.

Definition A.6.3. Let K be a finitely generated field extension of $\Bbbk$. The **transcendence degree** of $K/\Bbbk$, denoted $\mathrm{trdeg}(K/\Bbbk)$, is the smallest integer n such that there are $x_1, \ldots, x_n \in K$ with K algebraic over $\Bbbk(x_1, \ldots, x_n)$ (by definition x_i is transcendental over $\Bbbk(x_1, \ldots, x_{i-1})$). Such a set $\{x_1, \ldots, x_n\}$ is called a **transcendence basis** for $K/\Bbbk$.

Theorem A.6.4. *Let $K/\Bbbk$ be a finitely generated field extension. Then the transcendence degree is well-defined (i.e., all transcendence bases have the same number of elements).*

Proof: See Theorem 25 of Section II.12 of [640], Theorem VI.1.8 of [301] or Theorem 1.6.13 of [635]. □

Theorem A.6.5. *Let $K/\Bbbk$ and F/K be finitely generated field extensions. Then* $\mathrm{trdeg}(F/\Bbbk) = \mathrm{trdeg}(F/K) + \mathrm{trdeg}(K/\Bbbk)$.

Proof: See Theorem 26 of Section II.12 of [640]. □

Corollary A.6.6. *Let $K/\Bbbk$ be finitely generated with transcendence degree 1 and let $x \in K$ be transcendental over $\Bbbk$. Then K is a finite algebraic extension of $\Bbbk(x)$.*

A **perfect field** is one for which every algebraic extension is separable. A convenient equivalent definition is that a field $\Bbbk$ of characteristic p is perfect if $\{x^p : x \in \Bbbk\} = \Bbbk$ (see Section V.6 of Lang [367]). We restrict to perfect fields for a number of reasons, one of which is that the primitive element theorem does not hold for non-perfect fields, and another is due to issues with fields of definition (see Remark 5.3.7). Finite fields, fields of characteristic 0, and algebraic closures of finite fields are perfect (see Exercise V.7.13 of [301] or Section V.6 of [367]).

Theorem A.6.7. ***(Primitive element theorem)*** *Let $\Bbbk$ be a perfect field. If $\Bbbk'/\Bbbk$ is a finite, separable extension then there is some $\alpha \in \Bbbk'$ such that $\Bbbk' = \Bbbk(\alpha)$.*

Proof: Theorem V.6.15 of [301], Theorem 27 of [14], Theorem V.4.6 of [367]. □

A.7 Galois Theory

For an introduction to Galois theory see Chapter V of Hungerford [301], Chapter 6 of Lang [367] or Stewart [585]. An algebraic extension $\Bbbk'/\Bbbk$ is Galois if it is normal (i.e., every irreducible polynomial $F(x) \in \Bbbk[x]$ with a root in $\Bbbk'$ splits completely over $\Bbbk'$) and separable. The Galois group of $\Bbbk'/\Bbbk$ is

$$\mathrm{Gal}(\Bbbk'/\Bbbk) = \{\sigma : \Bbbk' \to \Bbbk' : \sigma \text{ is a field automorphism, and } \sigma(x) = x \text{ for all } x \in \Bbbk\}.$$

Theorem A.7.1. *Let $\Bbbk'/\Bbbk$ be a finite Galois extension. Then there is a one-to-one correspondence between the set of subfields $\{\Bbbk'' : \Bbbk \subseteq \Bbbk'' \subseteq \Bbbk'\}$ and the set of normal subgroups H of* $\mathrm{Gal}(\Bbbk'/\Bbbk)$*, via*

$$\Bbbk'' = \{x \in \Bbbk' : \sigma(x) = x \text{ for all } \sigma \in H\}.$$

Proof: See Theorem V.2.5 of [301]. □

If $\Bbbk$ is a perfect field then $\overline{\Bbbk}$ is a separable extension and hence a Galois extension of $\Bbbk$. If $\Bbbk'$ is any algebraic extension of $\Bbbk$ (not necessarily Galois) then $\overline{\Bbbk}/\Bbbk'$ is Galois. The Galois group $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ can be defined using the notion of an inverse limit (see Chapter 5 of [124]). Topological aspects of $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ are important, but we do not discuss them.

A.7.1 Galois Cohomology

One finds brief summaries of **Galois cohomology** in Appendix B of Silverman [564] and Chapter 19 of Cassels [122]. More detailed references are Serre [542] and Cassels and Frölich [124].

Let $K/\Bbbk$ be Galois (we include $K = \overline{\Bbbk}$). Let $G = \mathrm{Gal}(K/\Bbbk)$. Unlike most references we write our Galois groups acting on the left (i.e., as $\sigma(f)$ rather than f^σ). A 1-cocyle in the additive group K is a function[1] $\xi : G \to K$ such that $\xi(\sigma\tau) = \sigma(\xi(\tau)) + \xi(\sigma)$. A 1-coboundary in K is the function $\xi(\sigma) = \sigma(\gamma) - \gamma$ for some $\gamma \in K$. The group of 1-cocycles modulo 1-coboundaries (the group operation is addition $(\xi_1 + \xi_2)(\tau) = \xi_1(\tau) + \xi_2(\tau)$) is denoted $H^1(G, K)$. Similarly, for the multiplicative group K^*, a 1-cocyle satisfies $\xi(\sigma\tau) = \sigma(\xi(\tau))\xi(\sigma)$, a 1-coboundary is $\sigma(\gamma)/\gamma$ and the quotient group is denoted $H^1(G, K^*)$.

Theorem A.7.2. *Let $K/\Bbbk$ be Galois. Then $H^1(\mathrm{Gal}(K/\Bbbk), K) = \{0\}$ and (**Hilbert 90**) $H^1(\mathrm{Gal}(K/\Bbbk), K^*) = \{1\}$ (i.e., both groups are trivial).*

Proof: The case of finite extensions $K/\Bbbk$ is given in Exercise 20.5 of Cassels [122] or Propositions 1 and 2 of Chapter 10 of [542]. For a proof in the infinite case see Propositions 2 and 3 (Sections 2.6 and 2.7) of Chapter 5 of [124]. □

A.8 Finite Fields

Let p be a prime. Denote by $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the finite field of p elements. The multiplicative group of non-zero elements is $\mathbb{F}_p^*$. Recall that $\mathbb{F}_p^*$ is a cyclic group. A generator for $\mathbb{F}_q^*$ is called a **primitive root**. The number of primitive roots in $\mathbb{F}_q^*$ is $\varphi(q-1)$.

Theorem A.8.1. *Let p be a prime and $m \in \mathbb{N}$. Then there exists a field $\mathbb{F}_{p^m}$ having p^m elements. All such fields are isomorphic. Every finite field can be represented as $\mathbb{F}_p[x]/(F(x))$ where $F(x) \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree m; the corresponding vector space basis $\{1, x, \ldots, x^{m-1}\}$ for $\mathbb{F}_{p^m}/\mathbb{F}_p$ is called a **polynomial basis**.*

Proof: See Corollary V.5.7 of [301] or Section 20.2 of [556]. □

If p is a prime and $q = p^m$ then $\mathbb{F}_{p^{nm}}$ may be viewed as a degree n algebraic extension of $\mathbb{F}_q$.

Theorem A.8.2. *Every finite field $\mathbb{F}_{p^m}$ has a vector space basis over $\mathbb{F}_p$ of the form $\{\theta, \theta^p, \ldots, \theta^{p^{m-1}}\}$; this is called a **normal basis**.*

Proof: See Theorem 2.35 or Theorem 3.73 of [388, 389] or Exercise 20.14 of [556] (the latter proof works for extensions of $\mathbb{F}_p$, but not for all fields). □

We discuss methods to construct a normal basis in Section 2.14.1.

Theorem A.8.3. *Let q be a prime power and $m \in \mathbb{N}$. Then $\mathbb{F}_{q^m}$ is an algebraic extension of $\mathbb{F}_q$ that is Galois. The Galois group is cyclic of order m and generated by the q-power Frobenius automorphism $\pi : x \mapsto x^q$.*

Let $\alpha \in \mathbb{F}_{q^m}$. The **trace** and **norm** with respect to $\mathbb{F}_{q^m}/\mathbb{F}_q$ are

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i} \quad \text{and} \quad \mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \prod_{i=0}^{m-1} \alpha^{q^i}.$$

The **characteristic polynomial** over $\mathbb{F}_q$ of $\alpha \in \mathbb{F}_{q^m}$ is $F(x) = \prod_{i=0}^{m-1}(x - \alpha^{q^i}) \in \mathbb{F}_q[x]$. The trace and norm of $\alpha \in \mathbb{F}_{q^m}$ are (up to sign) the coefficients of x^{m-1} and x^0 in the characteristic polynomial.

An element $\alpha \in \mathbb{F}_q$ is a **square** or **quadratic residue** if the equation $x^2 = \alpha$ has a solution $x \in \mathbb{F}_q$. If g is a primitive root for $\mathbb{F}_q$ then g^a is a square if and only if a is even. Hence α is a square in $\mathbb{F}_q^*$ if and only if $\alpha^{(q-1)/2} = 1$.

[1] It is also necessary that ξ satisfy some topological requirements, but we do not explain these here.

Lemma A.8.4. *Let $g \in \mathbb{F}_{q^m}$, where $m > 1$, be chosen uniformly at random. The probability that g lies in a proper subfield $K \subset \mathbb{F}_{q^m}$ such that $\mathbb{F}_q \subseteq K$ is at most $1/q$.*

Proof: If $m = 2$ then the probability is $q/q^2 = 1/q$ so the result is tight in this case. When $m = l^i$ is a power of a prime $l \geq 2$ then all proper subfields of $\mathbb{F}_{q^m}$ that contain $\mathbb{F}_q$ are contained in $\mathbb{F}_{q^{l^{i-1}}}$ so the probability is $q^{l^{i-1}}/q^{l^i} = 1/q^{l^{i-1}(l-1)} \leq 1/q$. Finally, write $m = nl^i$ where $l \geq 2$ is prime, $i \geq 1$, $n \geq 2$ and $\gcd(n, l) = 1$. Then every proper subfield containing $\mathbb{F}_q$ lies in $\mathbb{F}_{q^{l^i}}$ or $\mathbb{F}_{q^{nl^{i-1}}}$. The probability that a random element lies in either of these fields is

$$\leq q^{l^i}/q^{nl^i} + q^{nl^{i-1}}/q^{nl^i} = 1/q^{l^i(n-1)} + 1/q^{nl^{i-1}(l-1)} \leq 1/q^2 + 1/q^2 \leq 1/q.$$

□

A.9 Ideals

If R is a commutative ring then an R-**ideal** is a subset $I \subset R$ that is an additive group and is such that for all $a \in I$ and $r \in R$ then $ar \in I$. An R-ideal I is proper if $I \neq R$ and is non-trivial if $I \neq \{0\}$. A **principal ideal** is $(a) = \{ar : r \in R\}$ for some $a \in R$. If $S \subset R$ then (S) is the R-ideal $\{\sum_{i=1}^{n} s_i r_i : n \in \mathbb{N}, s_i \in S, r_i \in R\}$. An ideal I is **finitely generated** if $I = (S)$ for a finite subset $S \subset R$. The **radical** of an ideal I in a ring R is $\mathrm{rad}_R(I) = \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}$ (see Definition VIII.2.5 and Theorem VIII.2.6 of Hungerford [301]). If I_1 and I_2 are ideals of R then

$$I_1 I_2 = \left\{ \sum_{i=1}^{n} a_i b_i : n \in \mathbb{N}, a_i \in I_1, b_i \in I_2 \right\}.$$

Note that $I_1 I_2 \subseteq I_1 \cap I_2$. For $a, b \in R$ one has $(ab) = (a)(b)$.

Let $I_1, \ldots, I_n$ be ideals in a ring R such that the ideal $(I_i \cup I_j) = R$ for all $1 \leq i < j \leq n$ (we call such ideals pairwise-coprime). If $a_1, \ldots, a_n \in R$ then there exists an element $a \in R$ such that $a \equiv a_i \pmod{I_i}$ (in other words, $a - a_i \in I_i$) for all $1 \leq i \leq n$. This is the **Chinese remainder theorem** for rings; see Theorem III.2.25 of [301] or Theorem II.2.1 of [367].

The following result gives three equivalent conditions for an ideal to be prime.

Lemma A.9.1. *Let I be an ideal of R. The following conditions are equivalent and, if they hold, I is called a* ***prime ideal****.*

1. *If $a, b \in R$ are such that $ab \in I$ then $a \in I$ or $b \in I$.*
2. *R/I is an integral domain (i.e., has no zero divisors).*
3. *If I_1 and I_2 are ideals of R such that $I_1 I_2 \subseteq I$ then $I_1 \subseteq I$ or $I_2 \subseteq I$.*

If $F(\underline{x}) \in \Bbbk[\underline{x}]$ is irreducible then the $\Bbbk[\underline{x}]$-ideal $(F(\underline{x})) = \{F(\underline{x})G(\underline{x}) : G(\underline{x}) \in \Bbbk[\underline{x}]\}$ is a prime ideal.

An R-ideal I is **maximal** if every R-ideal J such that $I \subseteq J \subseteq R$ is such that either $J = I$ or $J = R$.

Lemma A.9.2. *An R-ideal I is maximal if and only if R/I is a field (hence, a maximal R-ideal is prime). If I is a maximal R-ideal and $S \subset R$ is a subring then $I \cap S$ is a prime S-ideal.*

Proof: For the first statement see Theorem III.2.20 of [301] or Section II.2 of [367]. The second statement is proved as follows: Let I be maximal and consider the injection $S \to R$ inducing $S \to R/I$ with kernel $J = S \cap I$. Then $S/J \to R/I$ is is an injective ring homomorphism into a field, so J is a prime S-ideal. □

Let R be a commutative ring. A sequence $I_1 \subset I_2 \subset \cdots$ of R-ideals is called an **ascending chain**. A commutative ring R is **Noetherian** if every ascending chain of R-ideals is finite. Equivalently, a ring is Noetherian if every ideal is finitely generated. For more details see Section VIII.1 of [301] or Section X.1 of [367].

Theorem A.9.3. *(Hilbert basis theorem) If R is a Noetherian ring then $R[x]$ is a Noetherian ring.*

Proof: See Theorem 1 page 13 of [216], Theorem VIII.4.9 of [301] Section IV.4 of [367], or Theorem 7.5 of [15]. □

Corollary A.9.4. *$\Bbbk[x_1, \ldots, x_n]$ is Noetherian.*

A **multiplicative subset** of a ring R is a set S such that $1 \in S$, $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$. The **localisation** of a ring R with respect to a multiplicative subset S is the set

$$S^{-1}R = \{r/s : r \in R, s \in S\}$$

with the equivalence relation $r_1/s_1 \equiv r_2/s_2$ if $r_1 s_2 - r_2 s_1 = 0$. For more details see Chapter 3 of [15], Section 1.3 of [542], Section I.1 of [365], Section II.4 of [367] or Section III.4 of [301]. In the case $S = R^*$ we call $S^{-1}R$ the **field of fractions** of R. If $\mathfrak{p}$ is a prime ideal of R then $S = R - \mathfrak{p}$ is a multiplicative subset and the localisation $S^{-1}R$ is denote $R_{\mathfrak{p}}$.

Lemma A.9.5. *If R is Noetherian and S is a multiplicative subset of R then the localisation $S^{-1}R$ is Noetherian.*

Proof: See Proposition 7.3 of [15] or Proposition 1.6 of Section X.1 of [367]. □

A ring R is **local** if it has a unique maximal ideal. If $\mathfrak{m}$ is a maximal idea of a ring R then the localisation $R_{\mathfrak{m}}$ is a local ring. It follows that $R_{\mathfrak{m}}$ is Noetherian.

A.10 Vector Spaces and Linear Algebra

The results of this section are mainly used when we discuss lattices in Chapter 16. A good basic reference is Curtis [163].

Let $\Bbbk$ be a field. We write vectors in $\Bbbk^n$ as row vectors. We interchangeably use the words **points** and **vectors** for elements of $\Bbbk^n$. The zero vector is $\underline{0} = (0, \ldots, 0)$. For $1 \leq i \leq n$ the i-th unit vector is $\underline{e}_i = (e_{i,1}, \ldots, e_{i,n})$ such that $e_{i,i} = 1$ and $e_{i,j} = 0$ for $1 \leq j \leq n$ and $j \neq i$.

A **linear map** is a function $A : \Bbbk^n \to \Bbbk^m$ such that $A(\lambda \underline{x} + \mu \underline{y}) = \lambda A(\underline{x}) + \mu A(\underline{y})$ for all $\lambda, \mu \in \Bbbk$ and $\underline{x}, \underline{y} \in \Bbbk^n$. Given a basis for $\Bbbk^n$ any linear map can be represented as an $n \times m$ matrix A, such that $A(\underline{x}) = \underline{x}A$. We denote the entries of A by $A_{i,j}$ for $1 \leq i \leq n, 1 \leq j \leq m$. Denote by I_n the $n \times n$ **identity matrix**. We denote by A^T the **transpose**, which is an $m \times n$ matrix such that $(A^T)_{i,j} = A_{j,i}$. We have $(AB)^T = B^T A^T$.

A fundamental computational problem is to solve the linear system of equations $\underline{x}A = \underline{y}$ and it is well known that this can be done using Gaussian elimination (see Section 6 of Curtis [163] or Chapter 3 of Schrijver [531]).

The **rank** of an $m \times n$ matrix A (denoted rank(A)) is the maximum number of linearly independent rows of A (equivalently, the maximum number of linearly independent

columns). If A is an $n \times n$ matrix then the **inverse** of A, if it exists, is the matrix such that $AA^{-1} = A^{-1}A = I_n$. If A and B are invertible then $(AB)^{-1} = B^{-1}A^{-1}$. One can compute A^{-1} using Gaussian elimination.

A.10.1 Inner Products and Norms

Definition A.10.1. The **inner product** of two vectors $\underline{v} = (v_1, \ldots, v_n)$ and $\underline{w} = (w_1, \ldots, w_n) \in \Bbbk^n$ is

$$\langle \underline{v}, \underline{w} \rangle = \sum_{i=1}^{n} v_i w_i.$$

The **Euclidean norm** or ℓ_2**-norm** of a vector $\underline{v} \in \mathbb{R}^n$ is

$$\|\underline{v}\| = \sqrt{\langle \underline{v}, \underline{v} \rangle}.$$

More generally for $\mathbb{R}^n$ one can define the ℓ_a**-norm** of a vector $\underline{v}$ for any $a \in \mathbb{N}$ as $\|\underline{v}\|_a = (\sum_{i=1}^n |v_i|^a)^{1/a}$. Important special cases are the ℓ_1-norm $\|\underline{v}_i\| = \sum_{i=1}^n |\underline{v}_i|$ and the ℓ_∞-norm $\|\underline{v}\|_\infty = \max\{|v_1|, \ldots, |v_n|\}$. (The reader should not confuse the notion of norm in Galois theory with the notion of norm on vector spaces.)

Lemma A.10.2. *Let $\underline{v} \in \mathbb{R}^n$. Then*

$$\|\underline{v}\|_\infty \leq \|\underline{v}\|_2 \leq \sqrt{n}\|\underline{v}\|_\infty \quad \text{and} \quad \|\underline{v}\|_\infty \leq \|\underline{v}\|_1 \leq n\|\underline{v}\|_\infty.$$

Lemma A.10.3. *Let $\underline{v}, \underline{w} \in \mathbb{R}^n$ and let $\|\underline{v}\|$ be the Euclidean norm.*

1. $\|\underline{v} + \underline{w}\| \leq \|\underline{v}\| + \|\underline{w}\|$.
2. $\langle \underline{v}, \underline{w} \rangle = \langle \underline{w}, \underline{v} \rangle$.
3. $\|\underline{v}\| = 0$ *implies* $\underline{v} = \underline{0}$.
4. $|\langle \underline{v}, \underline{w} \rangle| \leq \|\underline{v}\|\|\underline{w}\|$.
5. *Let A be an $n \times n$ matrix over $\mathbb{R}$. The following are equivalent:*
   (a) $\|\underline{x}A\| = \|\underline{x}\|$ *for all* $\underline{x} \in \mathbb{R}^n$;
   (b) $\langle \underline{x}A, \underline{y}A \rangle = \langle \underline{x}, \underline{y} \rangle$ *for all* $\underline{x}, \underline{y} \in \mathbb{R}^n$;
   (c) $AA^T = I_n$ *(which implies* $\det(A)^2 = 1$*).*

   Such a matrix is called an ***orthogonal matrix****.*

Definition A.10.4. A basis $\{v_1, \ldots, v_n\}$ for a vector space is **orthogonal** if

$$\langle v_i, v_j \rangle = 0$$

for all $1 \leq i < j \leq n$. If we also have the condition $\langle v_i, v_i \rangle = 1$ then the basis is called **orthonormal**.

Lemma A.10.5. *Let $\{\underline{v}_1, \ldots, \underline{v}_n\}$ be an orthogonal basis for $\mathbb{R}^n$. If $\underline{v} = \sum_{j=1}^n \lambda_j \underline{v}_j$ then $\|\underline{v}\|^2 = \sum_{j=1}^n \lambda_j^2 \|\underline{v}_j\|^2$.*

If one has an orthogonal basis $\{\underline{v}_1, \ldots, \underline{v}_n\}$ then it is extremely easy to decompose an arbitrary vector $\underline{w}$ over the basis. The representation is

$$\underline{w} = \sum_{i=1}^{n} \frac{\langle \underline{w}, \underline{v}_i \rangle}{\langle \underline{v}_i, \underline{v}_i \rangle} \underline{v}_i.$$

This is simpler and faster than solving the linear system using Gaussian elimination.

If $V \subseteq \mathbb{R}^n$ is a subspace then the **orthogonal complement** is $V^\perp = \{\underline{w} \in \mathbb{R}^n : \langle \underline{w}, \underline{v} \rangle = 0 \text{ for all } \underline{v} \in V\}$. The dimension of $V^\perp$ is $n - \dim(V)$. Given a basis $\{\underline{v}_1, \ldots, \underline{v}_m\}$ for V (where $m = \dim(V) < n$) one can compute a basis $\{\underline{v}_{m+1}, \ldots, \underline{v}_n\}$ for $V^\perp$. The **orthogonal projection** of $\mathbb{R}^n$ to a subspace V is a linear map $P : \mathbb{R}^n \to V$ that is the identity on V and is such that $P(V^\perp) = \{0\}$. In other words, if $\underline{v} \in \mathbb{R}^n$ then $\underline{v} - P(\underline{v}) \in V^\perp$.

A.10.2 Gram-Schmidt Orthogonalisation

Given a basis $\underline{v}_1, \ldots, \underline{v}_n$ for a vector space, the Gram-Schmidt algorithm iteratively computes an orthogonal basis $\underline{v}_1^*, \ldots, \underline{v}_n^*$ (called the **Gram-Schmidt orthogonalisation** or **GSO**). The idea is to set $\underline{v}_1^* = \underline{v}_1$ and then, for $2 \leq i \leq n$, to compute

$$\underline{v}_i^* = \underline{v}_i - \sum_{j=1}^{i-1} \mu_{i,j} \underline{v}_j^* \quad \text{where} \quad \mu_{i,j} = \frac{\langle \underline{v}_i, \underline{v}_j^* \rangle}{\langle \underline{v}_j^*, \underline{v}_j^* \rangle}.$$

We discuss this algorithm further in Section 17.3.

A.10.3 Determinants

Let $\underline{b}_1, \ldots, \underline{b}_n$ be n vectors in $\Bbbk^n$. One can define the **determinant** of the sequence $\underline{b}_1, \ldots, \underline{b}_n$ (or of the matrix B whose rows are $\underline{b}_1, \ldots, \underline{b}_n$) in the usual way (see Chapter 5 of Curtis [163] or Section VII.3 of Hungerford [301]).

Lemma A.10.6. *Let $\underline{b}_1, \ldots, \underline{b}_n \in \Bbbk^n$.*

1. *Let B be the matrix whose rows are $\underline{b}_1, \ldots, \underline{b}_n$. Then B is invertible if and only if $\det(\underline{b}_1, \ldots, \underline{b}_n) \neq 0$.*
2. *For $\lambda \in \Bbbk$, $\det(\underline{b}_1, \ldots, \underline{b}_{i-1}, \lambda \underline{b}_i, \underline{b}_{i+1}, \ldots, \underline{b}_n) = \lambda \det(\underline{b}_1, \ldots, \underline{b}_n)$.*
3. *$\det(\underline{b}_1, \ldots, \underline{b}_{i-1}, \underline{b}_i + \underline{b}_j, \underline{b}_{i+1}, \ldots, \underline{b}_n) = \det(\underline{b}_1, \ldots, \underline{b}_n)$ for $i \neq j$.*
4. *If $\{\underline{e}_1, \ldots, \underline{e}_n\}$ are the standard unit vectors in $\Bbbk^n$ then $\det(\underline{e}_1, \ldots, \underline{e}_n) = 1$.*
5. *If B_1, B_2 are square matrices then $\det(B_1 B_2) = \det(B_1) \det(B_2)$.*
6. *$\det(B) = \det(B^T)$.*
7. *(Hadamard inequality) $|\det(\underline{b}_1, \ldots, \underline{b}_n)| \leq \prod_{i=1}^{n} \|\underline{b}_i\|$ (where $\|\underline{b}\|$ is the Euclidean norm).*

Proof: See Theorems 16.6, 17.6, 17.15, 18.3 and 19.13 of Curtis [163]. □

Definition A.10.7. Let $\underline{b}_1, \ldots, \underline{b}_n$ be a set of vectors in $\mathbb{R}^n$. The **fundamental parallelepiped** of the set is

$$\left\{ \sum_{i=0}^{n} \lambda_i \underline{b}_i : 0 \leq \lambda_i < 1 \right\}.$$

Lemma A.10.8. *Let the notation be as above.*

1. *The volume of the fundamental parallelepiped of* $\{\underline{b}_1, \ldots, \underline{b}_n\}$ *is* $|\det(\underline{b}_1, \ldots, \underline{b}_n)|$.
2. $|\det(\underline{b}_1, \ldots, \underline{b}_n)| = \prod_{i=1}^{n} \|\underline{b}_i^*\|$ *where* $\underline{b}_i^*$ *are the Gram-Schmidt vectors.*

Proof: The first claim is Theorem 19.12 of Curtis [163]. The second claim is Exercise 19.11 (also see Theorem 19.13) of [163]. □

There are two methods to compute the determinant for vectors in $\mathbb{R}^n$. The first is to perform Gaussian elimination to diagonalise and then take the product of the diagonal elements. The second is to apply Gram-Schmidt (using floating point arithmetic) and then the determinant is just the product of the norms. Over $\mathbb{R}$ both methods only give an approximation to the determinant. To compute the determinant for vectors with entries in $\mathbb{Z}$ or $\mathbb{Q}$ one can use Gaussian elimination or Gram-Schmidt with exact arithmetic in $\mathbb{Q}$ (this gives an exact solution but suffers from coefficient explosion). Alternatively, one can compute the determinant modulo p_i for many small or medium sized primes p_i and use the Chinese remainder theorem.

A.11 Hermite Normal Form

Definition A.11.1. An $n \times m$ integer matrix $A = (A_{i,j})$ is in (row) **Hermite normal form** (**HNF**) if there is some integer $1 \leq r \leq n$ and a strictly increasing map $f : \{1, \ldots, n-r\} \to \{1, \ldots, m\}$ (i.e., $f(i+1) > f(i)$) such that

1. the last r rows of A are zero
2. $0 \leq A_{j,f(i)} < A_{i,f(i)}$ for $1 \leq j < i$ and $A_{j,f(i)} = 0$ for $i < j \leq n$.

In particular, an $n \times n$ matrix that is upper triangular and that satisfies the condition $0 \leq A_{j,i} < A_{i,i}$ for $1 \leq j < i \leq n$ is in Hermite normal form. The reader is warned that there are many variations on the definition of the Hermite normal form.

The HNF A' of an integer matrix A is unique and there is an $n \times n$ **unimodular matrix** U (i.e., U is a matrix with integer entries and determinant ± 1) such that $A' = UA$. For more details of the Hermite normal form see Section 2.4.2 of Cohen [136] or Section 4.1 of Schrijver [531] (though note that both books use columns rather than rows).

A.12 Orders in Quadratic Fields

A quadratic field is $\mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. If $d < 0$ then the field is called an **imaginary quadratic field**. The **discriminant** of $K = \mathbb{Q}(\sqrt{d})$ is $D = d$ if $d \equiv 1 \pmod 4$ or $D = 4d$ otherwise. The **ring of integers** of a quadratic field of discriminant D is is $\mathcal{O}_K = \mathbb{Z}[(D + \sqrt{D})/2]$.

An **order** in a field $\Bbbk$ containing $\mathbb{Q}$ is a subring R of $\Bbbk$ that is finitely generated as a $\mathbb{Z}$-module and is such that $R \otimes_{\mathbb{Z}} \mathbb{Q} = \Bbbk$. Every order in a quadratic field is of the form $\mathbb{Z}[c(D + \sqrt{D})/2]$ for some $c \in \mathbb{N}$. The integer c is called the **conductor** and the discriminant of the order is $c^2 D$.

A.13 Binary Strings

The binary representation of an integer $a = \sum_{i=0}^{l-1} a_i 2^i$ is written as

$$(a_{l-1} \ldots a_1 a_0)_2 \quad \text{or} \quad a_{l-1} \ldots a_1 a_0 \tag{A.1}$$

where $a_i \in \{0,1\}$ and $a_{l-1} = 1$. We say that the **bit-length** of a is l. An integer $a \in \mathbb{N}$ is represented by a binary string of bit-length $\lfloor \log_2(a) \rfloor + 1$. The **least significant bit** of a is $\mathrm{LSB}(a) = a_0 = a \pmod 2$. We call a_i the **i-th bit** or **bit** i of a. The "most significant bit" is trivially always one, but in certain contexts one uses different notions of MSB; for example see Definition 21.7.1.

Binary strings of length l are sequences $a_1 a_2 \ldots a_l$ with $a_i \in \{0,1\}$. Such a sequence is also called an **l-bit string**. The i-th bit is a_i. There is an ambiguity when one wants to interpret a binary string as an integer; our convention is that a_l is the least significant bit.[2]

We denote by $\{0,1\}^l$ the set of all length l binary strings and $\{0,1\}^*$ the set of all binary strings of arbitrary finite length. If a and b are binary strings then the exclusive-or (i.e., **XOR**) $a \oplus b$ is the binary string whose i-th bit is $a_i + b_i \pmod 2$ for $1 \leq i \leq l$.

A.14 Probability and Combinatorics

We briefly recall some ideas from probability. Good references are Ross [502], Woodroofe [636] and Chapter 6 of Shoup [556].

The number of ways to choose t items from n without replacement, and where the ordering matters, is $n(n-1)(n-2)\cdots(n-t+1) = n!/(n-t)!$. The number of ways to choose t items from n without replacement, and where the ordering does not matter, is $\binom{n}{t} = n!/(t!(n-t)!)$. The number of ways to choose t items from n with replacement and where the ordering doesn't matter is $\binom{n+t-1}{t-1}$. We have

$$\left(\frac{n}{m}\right)^m \leq \binom{n}{m} \leq \left(\frac{ne}{m}\right)^m$$

Stirling's approximation to the factorial is $n! \approx \sqrt{2\pi n} e^{-n} n^n$ or $\log(n!) \approx n(\log(n) - 1)$ (where log denotes the natural logarithm). For proof see Section 5.4.1 of [636].

Let $[0,1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. A **distribution** on a set S is a function Pr mapping "nice"[3] subsets of S to $[0,1]$, with the properties that $\Pr(\varnothing) = 0$, $\Pr(S) = 1$ and if $A, B \subseteq S$ are disjoint and "nice" then $\Pr(A \cup B) = \Pr(A) + \Pr(B)$. For $s \in S$ we define $\Pr(s) = \Pr(\{s\})$ if $\{s\}$ is "nice". The **uniform distribution** on a finite set S is given by $\Pr(s) = 1/\#S$.

An **event** is a "nice" subset $E \subseteq S$, and $\Pr(E)$ is called the probability of the event. We define $\neg E$ to be $S - E$, so that $\Pr(\neg E) = 1 - \Pr(E)$. We have $\Pr(E_1) \leq \Pr(E_1 \cup E_2) \leq \Pr(E_1) + \Pr(E_2)$. We define $\Pr(E_1 \text{ and } E_2) = \Pr(E_1 \cap E_2)$.

Let S be a finite set with an implicit distribution on it (usually the uniform distribution). In an algorithm we write $s \leftarrow S$ to mean that $s \in S$ is randomly selected from S according to the distribution, i.e., s is chosen with probability $\Pr(s)$.

If $A, E \subseteq S$ and $\Pr(E) > 0$ then the **conditional probability** is

$$\Pr(A \mid E) = \frac{\Pr(A \cap E)}{\Pr(E)}.$$

If $\Pr(A \cap E) = \Pr(A)\Pr(E)$ then A and E are **independent events** (equivalently, if $\Pr(E) > 0$ then $\Pr(A \mid E) = \Pr(A)$). If S is the disjoint union $E_1 \cup E_2 \cup \cdots \cup E_n$ then $\Pr(A) = \sum_{i=1}^n \Pr(A \mid E_i)\Pr(E_i)$.

[2] This means that the i-th bit of a binary string is not the i-th bit of the corresponding integer. This inconsistency will not cause confusion in the book.

[3] Technically, S must be a set with a measure and the "nice" subsets are the measurable ones. When S is finite or countable then every subset is "nice".

Let S be a set. A **random variable** is a function[4] $X : S \to \mathbb{R}$. Write $\mathcal{X} \subseteq \mathbb{R}$ for the image of X (our applications will always have $\mathcal{X}$ either finite or $\mathbb{N}$). Then X induces a distribution on $\mathcal{X}$, defined for $x \in \mathcal{X}$ by $\Pr(X = x)$ is the measure of $X^{-1}(\{x\})$ (in the case where S is finite or countable, $\Pr(X = x) = \sum_{s \in X^{-1}(x)} \Pr(s)$). Random variables X_1 and X_2 are **independent random variables** if $\Pr(X_1 = x_1 \text{ and } X_2 = x_2) = \Pr(X_1 = x_1) \Pr(X_2 = x_2)$ for all $x_1 \in \mathcal{X}_1$ and $x_2 \in \mathcal{X}_2$.

The **expectation** of a random variable X taking values in a finite or countable set $\mathcal{X} \subseteq \mathbb{R}$ is

$$E(X) = \sum_{x \in \mathcal{X}} x \Pr(X = x).$$

If $\mathcal{X} = \mathbb{N}$ then $E(X) = \sum_{n=0}^{\infty} \Pr(X > n)$ (this is shown in the proof of Theorem 14.1.1). Note that if $\mathcal{X}$ is finite then $E(X)$ exists, but for $\mathcal{X}$ countable then the expectation only exists if the sum is convergent. If X_1 and X_2 are random variables on S then $E(X_1 + X_2) = E(X_1) + E(X_2)$. If X_1 and X_2 are independent then $E(X_1 X_2) = E(X_1)E(X_2)$.

Example A.14.1. Consider flipping a coin, with probability p of "heads" and probability $1 - p$ of "tails" (where $0 < p < 1$). Assume the coin flips are independent events. What is the expected number of trials until the coin lands "heads"?

Let X be the random variable with values in $\mathbb{N}$ where $\Pr(X = n)$ is the probability that the first head is on the n-th throw. Then $\Pr(X > n) = (1 - p)^n$ and $\Pr(X = n) = (1 - p)^{n-1}p$. This gives the **geometric distribution** on $\mathbb{N}$. One can check that $\sum_{n=1}^{\infty} \Pr(X = n) = 1$.

The expectation of X is $E(X) = \sum_{n=1}^{\infty} n \Pr(X = n)$ (the ratio test shows that this sum is absolutely convergent). Write $T = \sum_{n=1}^{\infty} n(1 - p)^{n-1}$. Then

$$E(X) = pT = T - (1-p)T = \sum_{n=1}^{\infty} n(1-p)^{n-1} - \sum_{n=1}^{\infty} (n-1)(1-p)^{n-1} = 1 + \sum_{n=2}^{\infty} (1-p)^{n-1} = \frac{1}{p}.$$

To define this problem formally, one should define the geometric random variable $X : S \to \mathbb{N}$, where S is the (uncountable) set of countable length sequences of bits, such that $X(s_1 s_2 \dots) > n$ if and only if $s_1 = \cdots s_n =$ "tails". This leads to measure-theoretic technicalities that are beyond the scope of this book, but which are well understood in probability theory.

Example A.14.2. Suppose one has a set S of N items and one chooses elements of S (with replacement) uniformly and independently at random. Let X be a random variable taking values in $\mathbb{N}$ such that $\Pr(X = n)$ is the probability that, after sampling n elements from S, the first $n - 1$ elements are distinct and the n-th element is equal to one of the previously sampled elements. In other words, X is the number of samples from S until some element is sampled twice. A version of the **birthday paradox** states that the expected value of X is approximately $\sqrt{\pi N/2}$. We discuss this in detail in Section 14.1.

Example A.14.3. A version of the **coupon collector** problem is the following: Suppose S is a set of N items and one chooses elements of S (with replacement) uniformly at random.

Let X be a random variable taking values in $\mathbb{N}$ such that $\Pr(X \geq n)$ is the probability that after choosing $n - 1$ elements (sampled uniformly and independently at random from S) one has not yet chosen some element of S. In other words, X is the number of "coupons" to be collected until one has a full set of all N types. The expected value of X is $N(1 + 1/2 + \cdots + 1/(N - 1) + 1/N) \approx N \log(N)$ (see Example 7.2j of Ross [502]).

[4]Technically, a random variable is defined on a probability space, not an arbitrary set, and is a measurable function; we refer to Woodroofe [636] for the details.

The **statistical distance** (also called the **total variation**) of two distributions $\Pr_1$ and $\Pr_2$ on a finite or countable set S is $\Delta(\Pr_1, \Pr_2) = \frac{1}{2}\sum_{x \in S} |\Pr_1(s) - \Pr_2(s)|$. It is easy to see that $\Delta(\Pr_1, \Pr_1) = 0$ and $0 \leq \Delta(\Pr_1, \Pr_2) \leq 1$ (see Theorem 6.14 of Shoup [556]). Two distributions are **statistically close** if their statistical distance is "negligible" in some appropriate sense (typically, in cryptographic applications, this will mean "negligible in terms of the security parameter").

We end with a result that is often used in the analysis of algorithms.

Theorem A.14.4. *The probability that two uniformly and independently chosen integers* $1 \leq n_1, n_2 < N$ *satisfy* $\gcd(n_1, n_2) = 1$ *tends to* $1/\zeta(2) = 6/\pi^2 \approx 0.608$ *as* N *tends to infinity.*

Proof: See Theorem 332 of [276]. □