CHAPTER 2

Algebraic Curves

In this chapter, we introduce the theory of algebraic geometry used for our construction of balanced arrays in Chapters 3 and balanced n-ary designs in Chapter 4. We assumed that the reader is familiar with some basic concepts and properties of groups, rings, and fields. The interested reader is referred to, for example, [CLO98, Mor91] and [Uen97] for covering more precisely this chapter and the above algebraic systems.

2.1. Projective curves and affine curves

Let K be a field. $\mathbb{A}^2(K)$ is the cartesian product of K with itself, that is, $\mathbb{A}^2(K)$ is the set of ordered two tuples of elements of K. $\mathbb{A}^2(K)$ is called the *affine plane* over K, and its elements are called *points*. We often write it briefly as $\mathbb{A}^2$. In general, we can extend the notion to the n-dimensional affine space, denoted by $\mathbb{A}^n$, by a similar definition as above: $\mathbb{A}^n$ is the set of ordered n-tuples and its elements are also called points.

The *projective plane* over K, denoted by $\mathbb{P}^2(K)$ or simply $\mathbb{P}^2$, is defined to be the set of all 1-dimensional subspaces through the origin $(0,0,0)$ in the 3-dimensional affine space $\mathbb{A}^3$, and the elements of $\mathbb{P}^2$ are also called *points*. Any point $P = (a_1, a_2, a_3)$ in $\mathbb{A}^3 \setminus \{(0,0,0)\}$ uniquely determines such a 1-dimensional subspace, namely $\{(\lambda a_1, \lambda a_2, \lambda a_3) | \lambda \in K\}$. This implies that $\mathbb{P}^2$ consists of all equivalence classes of triples

(a_1, a_2, a_3) of elements of K, not all zero, under the equivalence relation given by $(a_1, a_2, a_3) \sim (\lambda a_1, \lambda a_2, \lambda a_3)$ for all $\lambda \in K, \lambda \neq 0$. Therefore a point $P \in \mathbb{P}^2$ is often denoted by a representative element. To distinguish a point P on a projective plane from that in an affine space, we use the notation $P = (a_1 : a_2 : a_3)$, which is called the *homogeneous coordinates* for P.

An *algebraically closed field* $\bar{K}$ is a field in which the roots of any polynomial with one variable defined over this field $\bar{K}$ always lie. The complex number field is algebraically closed, while the real number field and finite fields are not. The union of all finite dimensional extensions of a finite field $\mathbb{F}_q$ is an algebraically closed field containing $\mathbb{F}_q$.

Assume here that K is an algebraically closed field. Let $F(x_1, x_2, x_3)$ be a polynomial of $K[x_1, x_2, x_3]$. If all its monomials have the same degree, then $F(x_1, x_2, x_3)$ is said to be *homogeneous*. For example $x^3 + xyz + zx^2$ is homogeneous, while $x^3 + xy + x^2$ is not.

Let F be a homogeneous polynomial of $K[x_1, x_2, x_3]$. A point $P = (a_1 : a_2 : a_3) \in \mathbb{P}^2$ is called a *zero* of the polynomial F if $F(a_1, a_2, a_3) = 0$. We often write $F(a_1, a_2, a_3) = F(P) = 0$ for simplicity.

Definition 2.1.1 (projective curve). A *projective curve* C over a field K is the set of zeroes of a homogeneous polynomial in $K[x_1, x_2, x_3]$.

Let C be a projective curve defined by a polynomial F. If the polynomial F is irreducible, then the curve C is also said to be *irreducible*.

Definition 2.1.2 (degree of curve). The *degree* of a projective curve C defined by an equation $F = 0$ is the degree of the polynomial F.

We now consider relations between $\mathbb{P}^2$ and $\mathbb{A}^2$. Let $C \subseteq \mathbb{P}^2$ be a projective curve defined by $F(x_1, x_2, x_3) = 0$. The set of points in $\mathbb{P}^2$ can be partitioned into the two subsets $U_1 = \{(a_1 : a_2 : 1)\} \subset \mathbb{P}^2$ and $U_0 = \{(a_1 : a_2 : 0)\} \subset \mathbb{P}^2$. We can denote a point $P = (a_1 : a_2 : a_3) \in C \cap U_1$ by $P = (a_1, a_2)$. In fact, the point $P = (a_1 : a_2 : a_3)$ satisfying

$a_3 \neq 0$ can be rewritten as $P = (a_1/a_3, a_2/a_3)$. The set $C \cap \mathbb{A}^2$ can be defined by $F' = F(x_1, x_2, 1) = 0$. The points of U_0, the *points at infinity*, play an important role in connecting affine geometry with projective geometry. For example, any elliptic curve $y^2 = x^3 + ax + b$ has a unique point at infinity since the projective point $(0 : 1 : 0)$ is on the corresponding projective curve $y^2z = x^3 + axz^2 + bz^3$.

For any polynomial $F \in K[x, y]$, a point $P = (a_1, a_2) \in \mathbb{A}^2$ is called, similarly to the homogeneous case, a *zero* of F if $F(a_1, a_2) = 0$.

Definition 2.1.3 (affine curve). An *affine curve* over a field K is the set of zeroes of a polynomial in $K[x, y]$.

We can establish the correspondence between a projective curve and an affine curve. By the above observations on the relation between $\mathbb{P}^2$ and $\mathbb{A}^2$, the points $P = (a_1 : a_2 : a_3)$, $a_3 \neq 0$, on a projective curve C defined by a homogeneous polynomial F can be regarded as the affine curve $C \cap \mathbb{A}^2$ defined by the polynomial $F(x, y, 1)$. On the other hand, an affine curve defined by a polynomial G corresponds to the projective curve defined by the polynomial $G(x/z, y/z)$.

Example 2.1.4. Let C be a projective curve defined by the equation $F = x^3 + xyz + zx^2 = 0$. Any point $P = (a_1 : a_2 : a_3)$, $a_3 \neq 0$, on C satisfies the equation $F(x, y, 1) = x^3 + xy + x^2 = 0$. This implies that $(a_1/a_3, a_2/a_3) \in \mathbb{A}^2$ is a point on the corresponding affine curve defined by $F(x, y, 1) = 0$.

For an affine curve C, a point $P = (a_1, a_2) \in C$ is called a *point at infinity* if the point $(a_1 : a_2 : 0)$ is on the corresponding projective curve.

Now we consider the singularity of points and curves.

Definition 2.1.5 (nonsingular affine curve). Let C be an affine curve defined by a polynomial F. A point $P = (a_1, a_2) \in C$ is said to be

nonsingular if

$$(\frac{\partial F}{\partial x_1}(P), \frac{\partial F}{\partial x_2}(P)) \neq (0,0).$$

If all points on an affine curve C are nonsingular, then the curve C is said to be *nonsingular*.

For projective curves, we define the singularity similarly to the case of affine curves.

Definition 2.1.6 (nonsingular projective curve). Let C be a projective curve defined by a homogeneous polynomial F. A point $P = (a_1 : a_2 : a_3) \in C$ is called *nonsingular* if

$$(\frac{\partial F}{\partial x_1}(P), \frac{\partial F}{\partial x_2}(P), \frac{\partial F}{\partial x_3}(P)) \neq (0,0,0).$$

If all points on a projective curve C are nonsingular, then the curve C is said to be *nonsingular*.

2.2. Curves over finite fields

Keeping the definitions of previous sections in mind, we consider the case when K is a finite field. Let q be a prime power and $\mathbb{F}_q$ a finite field of order q. In Section 2.1, we assumed that the field is algebraically closed. For the finite case, we consider curves over the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$.

Let C be a curve defined over $\mathbb{F}_q$. Then the curve C is also defined over any extension $\mathbb{F}_{q^m}$ of the field $\mathbb{F}_q$, that is, the coordinates of the points on C also lie in $\mathbb{F}_{q^m}$. We usually regard a curve defined over $\mathbb{F}_q$ as a curve defined over its closure $\bar{\mathbb{F}}_q$. Thus we can consider curves over finite fields in a similar way as in the case of the complex number field.

Definition 2.2.1 ($\mathbb{F}_{q^m}$-rational point). Let $P = (a_1, a_2, a_3)$ be a point of C. If $a_i \in \mathbb{F}_{q^m}$ for all i then P is called a $\mathbb{F}_{q^m}$-*rational point* of C. The set of all $\mathbb{F}_{q^m}$-rational points of C is denoted by $C(\mathbb{F}_{q^m})$.

2.3. Rational functions

In this section, we will mainly consider rational functions on affine curves.

Definition 2.3.1 (rational function). Let K be a field. A *rational function* is a quotient F/G of two polynomials $F, G \in K[x_1, x_2]$, where G is not the zero polynomial. The set of rational functions is denoted by $K(x_1, x_2)$.

In the above definition, if F and G are homogeneous polynomial of same degree and if the denominator G does not vanish at some point P on a projective curve C, then the ratio F/G is called a *rational function on* C. Similarly, if the denominator $G(P) \neq 0$ for some point P on an affine curve C' then F/G is a *rational function on* C'.

The following considerations hold for the rational functions on projective curves as well as affine curves. Note that for the projective case polynomials must be homogeneous.

Two distinct ratio F/G and F'/G' on a curve C define the same function if and only if $F' \cdot G - F \cdot G'$ vanishes on C. The set of rational functions on C, denoted by $K(C)$, forms a field under the usual addition and multiplication:

$$\begin{aligned} \frac{F}{G} + \frac{F'}{G'} &= \frac{F \cdot G' + F' \cdot G}{G \cdot G'}, \\ \frac{F}{G} \cdot \frac{F'}{G'} &= \frac{F \cdot F'}{G \cdot G'}. \end{aligned}$$

This field is called the *field of rational functions* on C, and its multiplicative group is denoted by $K^*(C)$. A rational function $f \in K(C)$ is *regular* at a point P on a curve C if there exists a representation

$f = F/G$ with $G(P) \neq 0$. $f(P) = F(P)/G(P)$ is called the *value* of f at P.

In the remainder of this section, we focus our attention on affine curves, since we can regard a projective curve as an affine one.

Definition 2.3.2 (ideal). A non-empty subset I of a ring R is an *ideal* if

- $F + G \in I$ whenever $F \in I$ and $G \in I$, and
- $HF \in I$ whenever $F \in I$ and $H \in R$.

Since $K[x_1, x_2]$ is a ring, we can define an ideal of $K[x_1, x_2]$. For $F_1, \ldots, F_s \in K[x_1, x_2]$ let $\langle F_1, \ldots, F_s \rangle = \{H_1F_1 + \cdots + H_sF_s : H_i \in K[x_1, x_2] \text{ for } i = 1, \ldots, s\}$. Then the set $\langle F_1, \ldots, F_s \rangle$ is an ideal in $K[x_1, x_2]$.

Let P be a point in $\mathbb{A}^2$. We next consider the set of rational functions which are regular at P.

Definition 2.3.3 (local ring). The *local ring* $\mathcal{O}_P$ with respect to a point P is the set of rational functions which are regular at P.

In general, a ring is called a *local ring* if it has exactly one *maximal ideal*, which is an ideal I of a ring R such that there is no ideal J satisfying $I \subsetneq J \subsetneq R$ other than $J = I$ or $J = R$. It is known (see for example, Section 4.1 in [CLO98]) that for a point $P = (a_1, a_2)$ the ring $\mathcal{O}_P$ in Definition 2.3.3 has the unique maximal ideal $\langle x_1 - a_1, x_2 - a_2 \rangle$. Since we will only use this special local ring $\mathcal{O}_P$ throughout this thesis, Definition 2.3.3 is enough for our discussion.

Let f be a rational function in a local ring $\mathcal{O}_P$ and I an ideal of $\mathcal{O}_P$. Set $[f] = f + I = \{f + h : h \in I\}$. The *quotient ring* $\mathcal{O}_P/I$ is a ring defined over the set $\{[f] : f \in \mathcal{O}_P\}$ with $[f] + [g] = [f + g]$ and $[f] \cdot [g] = [f \cdot g]$ for any $[f], [g] \in \mathcal{O}_P/I$. Since we can perform the scalar multiplication as $k[f] = [kf]$ for $k \in K$ and $[f] \in \mathcal{O}_P/I$, we know that $\mathcal{O}_P/I$ is also a linear space over K. Hence, we can define the dimension $\dim_K \mathcal{O}_P/I$ as the dimension of the linear space over K.

Now consider the intersection multiplicity of an intersection point of two curves. Let C_1 and C_2 be two affine curves defined by polynomials F_1 and F_2, respectively. An *intersection point* of the curves C_1 and C_2 is a common zero of the polynomials F_1 and F_2.

Definition 2.3.4 (intersection multiplicity). Let P be an intersection point of two curves C_1 and C_2 defined by relatively prime polynomials F_1 and F_2, respectively. The intersection multiplicity $I_P(C_1, C_2)$ of the point P is

$$I_P(C_1, C_2) = \dim_K \mathcal{O}_P/\langle F_1, F_2\rangle,$$

where $\mathcal{O}_P = \{F/G \in K(x_1, x_2) : G(P) \neq 0\}$ is the local ring with respect to P. Note that the ideal $\langle F_1, F_2\rangle$ is an ideal of $\mathcal{O}_P$ since $K[x_1, x_2] \subset \mathcal{O}_P$.

Next we consider the order of a rational function at a point. Let C be an affine curve defined by a polynomial $F \in K[x_1, x_2]$.

Definition 2.3.5 (order of f at P). Let $f = G_1/G_2$ be a rational function on C, where $G_1, G_2 \in K[x_1, x_2]$. Then the *order* $\mathrm{ord}_P(f)$ of f at P is

$$\mathrm{ord}_P(f) = I_P(C, C_1) - I_P(C, C_2),$$

where C_1 and C_2 are affine curves defined by the polynomials G_1 and G_2, respectively.

The following are two elementary properties on the orders of $f, g \in K(C)$ (see for example, Section 2.5 in [Ful69]):

$$\begin{aligned} \mathrm{ord}_P(f \cdot g) &= \mathrm{ord}_P(f) + \mathrm{ord}_P(g); \\ \mathrm{ord}_P(f + g) &\geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g)). \end{aligned}$$

2.4. Divisors

Let C be a nonsingular projective curve defined over a field K.

Definition 2.4.1 (divisor). A *divisor D on C* is a finite formal sum $D = \sum_P m_P \cdot P$ for a finite number of points $P \in C$ with m_P being integers. The set of divisors on C is denoted by $\mathrm{Div}(C)$.

The set $\mathrm{Div}(C)$ of divisors on a curve C forms an Abelian group under the addition

$$D \pm E = \sum_P (m_P \pm m'_P) \cdot P,$$

where $D = \sum_P m_P \cdot P$ and $E = \sum_P m'_P \cdot P$.

Let $D = \sum m_P P$ be a divisor on C. The *support* of D, denoted by $\mathrm{Supp}\, D$, is the set of points P with $m_P \neq 0$. The *degree* of D is $\sum m_P$, and is denoted by $\deg D$. If $m_P \geq 0$ for any $P \in C$ then the divisor D is said to be *effective* and is denoted by $D \geq 0$. Moreover if $D \neq 0$ we call it *positive*. For any two divisors $D, E \in \mathrm{Div}(C)$, we write $D \geq E$ if and only if $D - E \geq 0$.

Now we consider the divisor of a rational function.

Definition 2.4.2 (divisor of rational function). For a rational function $f \in K(C)$, $f \neq 0$, on a projective curve C over a field K,

$$\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f) \cdot P$$

is called the *divisor of f*.

Since a polynomial can be considered as a rational function with denominator 1, and since a curve can be represented by a polynomial, the divisors of curves can also be defined in the same manner as rational functions.

Let C be a projective curve defined over a field K. For $f, g \in K(C)$ and $\alpha \in K$, $\alpha \neq 0$, the following properties hold (see for example, page

137 in [Uen97]):

$$\begin{aligned} \mathrm{div}(\alpha f) &= \mathrm{div}(f), \\ \mathrm{div}(fg) &= \mathrm{div}(f) + \mathrm{div}(g), \\ \mathrm{div}(f/g) &= \mathrm{div}(f) - \mathrm{div}(g). \end{aligned}$$

Moreover, if f is constant, i.e. $f = \alpha \in K$, then $\mathrm{div}(f) = \mathrm{div}(\alpha) = 0$. For the degree of the divisor of a rational function, the following lemma is well-known.

Lemma 2.4.3. *The degree of* $\mathrm{div}(f)$ *is equal to* 0 *for any rational function* $f \in K(C)$. *(See for example, Lemma 3.2 in* [**Uen97**].*)*

Let $D = m_1P_1 + \cdots m_sP_s$ be a divisor on a curve C defined over a finite field $\mathbb{F}_q$. In this case, each P_i is an $\bar{\mathbb{F}}_q$-rational point of C, that is, $P_i \in C(\bar{\mathbb{F}}_q)$. Let $\mathrm{Aut}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ be an automorphism group such that for any $\alpha \in \mathbb{F}_q$ and any $\sigma \in \mathrm{Aut}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, $\sigma(\alpha) = \alpha$ holds. For an $\bar{\mathbb{F}}_q$-rational point $P = (a_1 : a_2 : a_3)$, we define

$$P^\sigma = \big(\sigma(a_1), \sigma(a_2), \sigma(a_3)\big).$$

Then P^σ is also a $\bar{\mathbb{F}}_q$-rational point of C. This comes from the following reason. Since C is defined over $\mathbb{F}_q$, the curve C is defined by a homogeneous polynomial $F \in \mathbb{F}_q[x_1, x_2, x_3]$ with coefficients in $\mathbb{F}_q$. Therefore $F_i(P^\sigma) = F_i\big(\sigma(a_1), \sigma(a_2), \sigma(a_3)\big) = \sigma\big(F_i(a_1, a_2, a_3)\big) = \sigma(0) = 0$, which implies that P^σ is also a $\bar{\mathbb{F}}_q$-rational point of C.

For a divisor $D = m_1P_1 + \cdots + m_sP_s$ on a projective curve C we define D^σ by

$$D^\sigma = m_1P_1^\sigma + \cdots + m_sP_s^\sigma.$$

Definition 2.4.4 (rational divisor). A divisor $D = m_1P_1 + \cdots + m_sP_s$ on a projective curve C is called a *rational divisor over* $\mathbb{F}_q$ or an $\mathbb{F}_q$-*rational divisor* if it satisfies the following conditions:

1. Each P_i is a $\mathbb{F}_{q^m}$-rational point;
2. $D^\sigma = D$ for any $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

Definition 2.4.5 (prime rational divisor). Let D be a rational divisor over $\mathbb{F}_q$. D is called a *prime rational divisor over* $\mathbb{F}_q$ if it satisfies the following conditions:

1. $D = P_1 + \cdots + P_s$, where $P_i \neq P_j$ for any $i \neq j$;
2. There is an element σ in $\mathrm{Aut}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ such that $P_i^\sigma = P_j$ for any two distinct points $P_i, P_j \in \mathrm{Supp}\ D$.

Since a prime rational divisor is of form $D = \sum P^\sigma$ with $P \in C(\mathbb{F}_{q^m})$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, any rational divisor over $\mathbb{F}_q$ is a finite sum of prime rational divisors over $\mathbb{F}_q$.

We conclude this section by remarking that $\mathrm{Aut}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ can be represented by

$$\mathrm{Aut}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \{1, \varphi, \varphi^2, \cdots, \varphi^{m-1}\},$$

where $\varphi(\alpha) = \alpha^q$ for $\alpha \in \mathbb{F}_{q^m}$.

2.5. Vector space $L(D)$

Let C be a projective curve defined over a field K. For any divisor D in $\mathrm{Div}(C)$, we define $L^*(D)$ to be $L^*(D) = \{f \in K(C) \setminus \{0\} | \mathrm{div}(f) + D \geq 0\}$. Let $L(D) = L^*(D) \cup \{0\}$. Then $L(D)$ is a vector space over K, which is called the *space associated to* D. The dimension of $L(D)$ is denoted by $l(D)$. Let $D = m_1P_1 + \cdots + m_kP_k - m_{k+1}P_{k+1} - \cdots - m_lP_l$, where $m_j \geq 1, j = 1, 2, \ldots, l$. The condition $\mathrm{div}(f) + D \geq 0$ in the above definition of $L(D)$ can be rewritten as follows.

- $\mathrm{ord}_{P_j}(f) \leq m_j$ at $P_j, 1 \leq j \leq k$,
- $\mathrm{ord}_{P_j}(f) \geq m_j$ at $P_j, k+1 \leq j \leq l$, and
- f is regular at $P \notin \mathrm{Supp}\ D$.

It is clear that if $f, g \in L(D)$ then $f \pm g \in L(D)$, and that $\alpha f \in L(D)$ for $\alpha \in K$, $f \in L(D)$. Hence $L(D)$ is a vector space over K. The following lemma is a result on the dimension of the vector space.

Lemma 2.5.1. *$L(D)$ is finite-dimensional for any $D \in Div(C)$. In particular, if $D \geq 0$ then*

$$l(D) = \dim_K L(D) \leq \deg D + 1.$$

(See for example, Proposition 2 in Section 6.2 of [**Ful69**]*.)*

Lemma 2.5.2. *For divisors $D, E \in Div(C)$, if $D \geq E$ then*

$$L(D) \supseteq L(E).$$

(See for example, Proposition 2 in Section 6.2 of [**Ful69**]*.)*

The next lemma is an immediate consequence of Lemma 2.4.3. If $f \in L(D)$ and $f \neq 0$ then $\mathrm{div}(f)+D \geq 0$, that is, $\deg(\mathrm{div}(f)+D) \geq 0$. The degree of the divisor $\mathrm{div}(f)+D$ is $\deg(\mathrm{div}(f)+D) = \deg(\mathrm{div}(f))+\deg D = \deg D < 0$, which is impossible.

Lemma 2.5.3. *If $\deg D < 0$ then $L(D) = \{0\}$. (See for example, Corollary 3.1 in* [**Uen97**]*.)*

2.6. Riemann-Roch Theorem

In this section, we give an important theorem about the dimension $l(D)$ of $L(D)$. Let C be a projective curve over a field K and D a K-rational divisor on C.

Theorem 2.6.1 (Riemann's Inequality). *There is a non-negative integer g such that*

$$l(D) \geq \deg D + 1 - g \tag{2.6.1}$$

for any divisor $D \in Div(C)$. (See for example, Theorem 2.3 in [**Mor91**] *and Corollary 3.3 in* [**Uen97**]*.)*

The smallest integer of g is uniquely determined by the curve C. It is an important invariant for the curve C.

Definition 2.6.2. The smallest g satisfying the inequality (2.6.1) is called the *genus* of C.

When C is a nonsingular projective curve, the genus g of C can be calculated easily.

Lemma 2.6.3. *Let C be a nonsingular projective curve, g the genus of C and $d = \deg C$. Then*

$$g = \frac{1}{2}(d-1)(d-2).$$

(See for example, Lemma 3.6 in [Uen97].*)*

In the theory of algebraic geometry, there is a famous theorem called *Riemann-Roch Theorem*. The following is a special case of Riemann-Roch Theorem in finite fields, which plays a very important role in our applications.

Theorem 2.6.4 (Riemann-Roch Theorem). *Let $\mathbb{F}_q$ be a finite field of order q, C a nonsingular projective curve defined over $\mathbb{F}_q$ with genus g, and $D \in Div(C)$ an $\mathbb{F}_q$-rational divisor such that $\deg D > 2g - 2$. Then*

$$l(D) = \deg D + 1 - g,$$

where $l(D) = \dim L(D)$, $L(D) = \{f \in \mathbb{F}_q(C) | \mathrm{div}(f) + D \geq 0\} \cup \{0\}$. (See for example, Lemma 3.7 in [Uen97].*)*