14. Divisors on Curves

In its version for curves, Bézout's Theorem determines the number of zeroes of a homogeneous polynomial on a projective curve (see Corollaries 12.20 and 12.26). For example, if $X \subset \mathbb{P}^2$ is a cubic curve then the zero locus of a homogeneous linear polynomial f on X consists of three points, counted with multiplicities. But of course not every collection of three points on X can arise in this way, as three points will in general not lie on a line, and thus cannot be in the zero locus of f. So by reducing the question of the zeroes of polynomials to just their number we are losing information about their possible positions. To avoid this, we will now present a theory that is able to keep track of the actual configurations of points on curves.

It turns out that these configurations, called *divisors* below, are parametrized by a group that is naturally associated to the curve X. This will allow us to study and classify curves with methods from group theory, very much in the same way as in topology the fundamental group or the homology groups can be used to study and distinguish topological spaces. For example, using divisors we will be able to prove in Proposition 14.19 and Remark 14.20 that a smooth plane cubic curve as above is never isomorphic to $\mathbb{P}^1$. Note that for the ground field $\mathbb{C}$ we have already seen this topologically in Remark 13.19 since a smooth plane cubic is a torus whereas $\mathbb{P}^1_{\mathbb{C}}$ is a sphere — but of course this was using techniques from topology that would certainly require some work to make them rigorous. In contrast, our new proof here will be entirely self-contained and algebraic, so in particular applicable to any ground field.

The concept of divisors can be defined for arbitrary curves. For example, in the smooth affine case this leads to the notion of Dedekind domains studied in commutative algebra [G5, Chapter 13], and for singular curves one needs two different concepts of divisors, called *Weil divisors* and *Cartier divisors*. However, in our applications we will only need irreducible smooth projective curves. So for simplicity of notation we will restrict ourselves to this case from the very beginning, even if many of our constructions and results do not need all these assumptions.

Let us start by giving the definition of divisors. It should be noted that the name "divisor" in this context has historical reasons; it is completely unrelated to the notion of divisors in an integral domain.

Definition 14.1 (Divisors)**.** Let X be an irreducible smooth projective curve.

(a) A **divisor** on X is a formal finite linear combination $k_1a_1 + \cdots + k_na_n$ of distinct points $a_1,\dots,a_n \in X$ with integer coefficients $k_1,\dots,k_n \in \mathbb{Z}$ for some $n \in \mathbb{N}$. Obviously, the divisors on X form an Abelian group under pointwise addition of the coefficients. We will denote it by $\operatorname{Div} X$.

Equivalently, in algebraic terms $\operatorname{Div} X$ is just the *free Abelian group* generated by the points of X (i. e. the group of maps $X \to \mathbb{Z}$ being non-zero at only finitely many points; with a point mapping to its coefficient in the sense above).

(b) A divisor $D = k_1a_1 + \cdots + k_na_n$ as above is called **effective**, written $D \geq 0$, if $k_i \geq 0$ for all $i = 1,\dots,n$. If D_1, D_2 are two divisors with $D_2 - D_1$ effective, we also write this as $D_2 \geq D_1$ or $D_1 \leq D_2$. In other words, we have $D_2 \geq D_1$ if and only if the coefficient of any point in D_2 is greater than or equal to the coefficient of this point in D_1.

(c) The **degree** of a divisor $D = k_1a_1 + \cdots + k_na_n$ as above is the number $\deg D := k_1 + \cdots + k_n \in \mathbb{Z}$. Obviously, the degree is a group homomorphism $\deg : \operatorname{Div} X \to \mathbb{Z}$. Its kernel is denoted by

$$\operatorname{Div}^0 X = \{D \in \operatorname{Div} X : \deg D = 0\}.$$

Construction 14.2 (Divisors from polynomials and intersections)**.** Again, let $X \subset \mathbb{P}^n$ be an irreducible smooth curve. Our construction of multiplicities in Definition 12.23 (b) allows us to define divisors on X as follows.

(a) For a non-zero homogeneous polynomial $f \in S(X)$ the *divisor of* f is defined to be
$$\operatorname{div} f := \sum_{a \in V_X(f)} \operatorname{mult}_a(f) \cdot a \quad \in \operatorname{Div} X,$$
where $V_X(f)$ denotes the zero locus of f on X as in Construction 6.18. In other words, the divisor $\operatorname{div} f$ contains the data of the zeroes of f together with their multiplicities. By Bézout's Theorem as in Corollary 12.26 (a), its degree is $\deg(\operatorname{div} f) = \deg X \cdot \deg f$.

(b) If $n = 2$ and $Y \subset \mathbb{P}^2$ is another curve not containing X, the *intersection divisor* of X and Y is
$$X \cdot Y := \sum_{a \in X \cap Y} \operatorname{mult}_a(X,Y) \cdot a \quad \in \operatorname{Div} X.$$
By definition, this divisor is just the same as $\operatorname{div} f$ for a generator f of $I(Y)$. Note that it is symmetric in X and Y, so in particular the result can be considered as an element of $\operatorname{Div} Y$ as well if Y is also smooth and irreducible. By Bézout's Theorem as in Corollary 12.26 (b), we have $\deg(X \cdot Y) = \deg X \cdot \deg Y$.

Example 14.3. Consider again the two projective curves $X = V(x_0x_2 - x_1^2)$ and $Y = V(x_2)$ in $\mathbb{P}^2$ of Example 12.28. We have seen in this example that X and Y intersect in a single point $a = (1:0:0)$ with multiplicity 2. Hence $X \cdot Y = 2a$ in $\operatorname{Div} X$ in the notation of Construction 14.2. Equivalently, we can write $\operatorname{div} x_2 = 2a$ on X, and $\operatorname{div}(x_0x_2 - x_1^2) = 2a$ on Y.

Note that so far all our multiplicities have been non-negative, and hence all the divisors in Construction 14.2 are effective. Let us now extend this construction to multiplicities and divisors of rational functions, which will lead to negative multiplicities at their poles, and thus to non-effective divisors. To do this, we need the following lemma first.

Lemma 14.4. *Let X be an irreducible smooth projective curve, and let $f, g \in S(X)$ be two non-zero polynomials. Then*
$$\operatorname{mult}_a(fg) = \operatorname{mult}_a(f) + \operatorname{mult}_a(g)$$
for all $a \in X$. In particular, we have $\operatorname{div}(fg) = \operatorname{div} f + \operatorname{div} g$ *in* $\operatorname{Div} X$.

Proof. By Remark 12.25 (a) we have to show that
$$\dim_K \mathscr{O}_{X,a}/(fg) = \dim_K \mathscr{O}_{X,a}/(f) + \dim_K \mathscr{O}_{X,a}/(g).$$
for all $a \in X$. But this follows immediately by Lemma 12.5 from the exact sequence
$$0 \longrightarrow \mathscr{O}_{X,a}/(f) \xrightarrow{\cdot g} \mathscr{O}_{X,a}/(fg) \longrightarrow \mathscr{O}_{X,a}/(g) \longrightarrow 0$$
(for the injectivity of the first map note that $\mathscr{O}_{X,a}$ is an integral domain since X is irreducible). Taking these results for all $a \in X$ together, we conclude that $\operatorname{div}(fg) = \operatorname{div} f + \operatorname{div} g$. $\square$

Construction 14.5 (Multiplicities and divisors of rational functions)**.** Let X be an irreducible smooth projective curve, and let $\varphi \in K(X)^*$ be a non-zero rational function (see Construction 9.6). By Definition 7.1 we can write $\varphi = \frac{g}{f}$ for two homogeneous polynomials f and g of the same degree.

(a) We define the *multiplicity* of φ at a point $a \in X$ to be
$$\operatorname{mult}_a(\varphi) := \operatorname{mult}_a(g) - \operatorname{mult}_a(f) \quad \in \mathbb{Z}.$$
Note that this is well-defined: if $\frac{g'}{f'} = \frac{g}{f}$ for two other homogeneous polynomials f' and g' of the same degree then $g'f - f'g = 0$ on a non-empty open subset, hence on all of X since X is irreducible, and consequently $g'f = f'g \in S(X)$. Lemma 14.4 thus implies that $\operatorname{mult}_a(g') + \operatorname{mult}_a(f) = \operatorname{mult}_a(f') + \operatorname{mult}_a(g)$, i. e. that $\operatorname{mult}_a(g') - \operatorname{mult}_a(f') = \operatorname{mult}_a(g) - \operatorname{mult}_a(f)$.

Geometrically, we can think of this multiplicity as the order of the zero (if $\operatorname{mult}_a(\varphi) > 0$) resp. pole (if $\operatorname{mult}_a(\varphi) < 0$) of φ at a.

(b) Analogously to Construction 14.2, we define the *divisor* of φ to be

$$\operatorname{div}\varphi := \sum_{a \in V_X(f) \cup V_X(g)} \operatorname{mult}_a(\varphi) \cdot a = \operatorname{div} g - \operatorname{div} f.$$

23

Example 14.6. The rational function $\varphi = \frac{x_0 x_1}{(x_0 - x_1)^2}$ on $\mathbb{P}^1$ has divisor

$$\operatorname{div}\varphi = (1:0) + (0:1) - 2\,(1:1).$$

Remark 14.7 (Multiplicities of local functions)**.** By Exercise 9.8 (b) every local function $\varphi \in \mathscr{O}_{X,a}$ at a point a of an irreducible smooth projective curve X can be considered as a rational function on X. Hence Construction 14.5 also defines a multiplicity $\operatorname{mult}_a(\varphi)$ for any non-zero $\varphi \in \mathscr{O}_{X,a}$.

Moreover, note that φ then has a representation of the form $\varphi = \frac{g}{f}$ with $f, g \in S(X)$ and $f(a) \neq 0$. By Remark 12.24, this means that $\operatorname{mult}_a(f) = 0$, and thus $\operatorname{mult}_a(\varphi) = \operatorname{mult}_a(g) \in \mathbb{N}$. By the same remark, we have $\operatorname{mult}_a(\varphi) = 0$ if and only if $g(a) \neq 0$ as well, i. e. if and only if $\varphi(a) \neq 0$.

Remark 14.8. As above, let X be an irreducible smooth projective curve.

(a) Lemma 14.4 implies that $\operatorname{mult}_a(\varphi_1\varphi_2) = \operatorname{mult}_a \varphi_1 + \operatorname{mult}_a \varphi_2$ for any $a \in X$ and any two non-zero rational functions $\varphi_1, \varphi_2 \in K(X)^*$. We therefore also have $\operatorname{div}(\varphi_1\varphi_2) = \operatorname{div}\varphi_1 + \operatorname{div}\varphi_2$, i. e. the map $\operatorname{div} : K(X)^* \to \operatorname{Div} X$ is a homomorphism of groups.

(b) As any non-zero rational function on X has the form $\varphi = \frac{g}{f}$ for two homogeneous polynomials of the same degree, we see by Construction 14.2 (a) that its divisor always has degree 0:

$$\deg\operatorname{div}\varphi = \deg(\operatorname{div} g - \operatorname{div} f) = \deg\operatorname{div} g - \deg\operatorname{div} f = \deg X \cdot \deg g - \deg X \cdot \deg f = 0.$$

Hence the homomorphism of (a) can also be viewed as a morphism $\operatorname{div} : K(X)^* \to \operatorname{Div}^0 X$.

This observation leads to the idea that we should give special attention to the divisors of rational functions, i. e. to the image subgroup of the above divisor homomorphism.

Definition 14.9 (Principal divisors and the Picard group)**.** Let X be an irreducible smooth projective curve.

(a) A divisor on X is called **principal** if it is the divisor of a (non-zero) rational function. We denote the set of all principal divisors by $\operatorname{Prin} X$. Note that $\operatorname{Prin} X$ is just the image of the divisor homomorphism $\operatorname{div} : K(X)^* \to \operatorname{Div}^0 X$ of Remark 14.8 (b), and hence a subgroup of both $\operatorname{Div}^0 X$ and $\operatorname{Div} X$.

(b) The quotient

$$\operatorname{Pic} X := \operatorname{Div} X / \operatorname{Prin} X$$

is called the **Picard group** or **group of divisor classes** on X. Restricting to degree zero, we also define $\operatorname{Pic}^0 X := \operatorname{Div}^0 X / \operatorname{Prin} X$. By abuse of notation, a divisor and its class in $\operatorname{Pic} X$ will usually be denoted by the same symbol.

Remark 14.10. The groups $\operatorname{Pic} X$ and $\operatorname{Pic}^0 X$ carry essentially the same information on X, since we always have

$$\operatorname{Pic} X / \operatorname{Pic}^0 X \cong \operatorname{Div} X / \operatorname{Div}^0 X \cong \mathbb{Z}.$$

It just depends on the specific application in mind whether it is more convenient to work with $\operatorname{Pic} X$ or with $\operatorname{Pic}^0 X$.

By construction, the group $\operatorname{Div} X$ of divisors on an irreducible smooth projective curve X is a free Abelian group with an infinite number of generators, and hence not very interesting from a group-theoretic point of view. In contrast, the Picard group is rather "small" and has quite a rich structure that we want to study now in some examples.

Example 14.11 (The Picard group of $\mathbb{P}^1$ is trivial)**.** On $\mathbb{P}^1$, every degree-0 divisor is principal: if $D = k_1\,(a_{1,0}:a_{1,1}) + \cdots + k_n\,(a_{n,0}:a_{n,1})$ for some points $(a_{i,0}:a_{i,1}) \in \mathbb{P}^1$ and integers k_i for $i = 1,\dots,n$ with $k_1 + \cdots + k_n = 0$, the rational function given by

$$\varphi(x_0:x_1) = \prod_{i=1}^{n} (a_{i,1}x_0 - a_{i,0}x_1)^{k_i}$$

has divisor $\operatorname{div}\varphi = D$. Hence the divisor map $\operatorname{div} : K(\mathbb{P}^1)^* \to \operatorname{Div}^0 \mathbb{P}^1$ is surjective, so that we have $\operatorname{Prin}\mathbb{P}^1 = \operatorname{Div}^0\mathbb{P}^1$, and consequently

$$\operatorname{Pic}^0\mathbb{P}^1 = \{0\} \quad \text{and} \quad \operatorname{Pic}\mathbb{P}^1 = \operatorname{Div}\mathbb{P}^1 / \operatorname{Div}^0\mathbb{P}^1 \cong \mathbb{Z},$$

with the isomorphism $\deg : \operatorname{Pic}\mathbb{P}^1 \to \mathbb{Z}$.

Let us now move on to more complicated curves. We know already from Example 7.6 (d) that a smooth conic $X \subset \mathbb{P}^2$ (which is irreducible by Exercise 10.22 (a)) is isomorphic to $\mathbb{P}^1$. As the Picard group is clearly invariant under isomorphisms, this means that $\operatorname{Pic}^0 X$ will then be the trivial group again. So the next case to consider is a smooth cubic curve $X \subset \mathbb{P}^2$. Our main goal in this chapter is to prove that $\operatorname{Pic}^0 X$ is not trivial in this case, so that X cannot be isomorphic to $\mathbb{P}^1$. In fact, in the next chapter in Proposition 15.2 we will even be able to compute $\operatorname{Pic}^0 X$ for a plane cubic explicitly.

However, even for the special case of plane cubics the computation of $\operatorname{Pic}^0 X$ is not easy, and so we will need some preliminaries first. The following lemma will be well-known to you if you have attended the Commutative Algebra class already, since it essentially states in algebraic terms that the local rings of X are discrete valuation rings [G5, Lemma 12.1]. It is the first time in this chapter that the smoothness assumption on X is essential.

Lemma 14.12 (Local coordinates on a smooth plane curve)**.** *Let $X \subset \mathbb{P}^2$ be a smooth curve, and let $I_a \trianglelefteq \mathscr{O}_{X,a}$ be the maximal ideal in the local ring of a point $a \in X$ as in Definition 3.22.*

(a) *The ideal I_a is principal, with $I_a = (\varphi_a)$ for a suitable $\varphi_a \in \mathscr{O}_{X,a}$ with $\operatorname{mult}_a(\varphi_a) = 1$.*

(b) *Any non-zero $\varphi \in \mathscr{O}_{X,a}$ can be written as $\varphi = c \cdot \varphi_a^m$, where $c \in \mathscr{O}_{X,a} \backslash I_a$ and $m = \operatorname{mult}_a(\varphi)$.*

Proof.

(a) Choose a linear function φ_a vanishing at a such that the line $V(\varphi_a)$ is not the tangent line to X at a. Then φ_a vanishes on X with multiplicity 1 at a by Exercise 12.27. Hence $\varphi_a \in I_a$, and

$$1 = \dim_K \mathscr{O}_{X,a}/(\varphi_a) \geq \dim_K \mathscr{O}_{X,a}/I_a > 0.$$

It follows that we must have equality, so in particular that $I_a = (\varphi_a)$.

(b) Note that $\varphi \notin I_a^{m+1}$, since by (a) the elements of I_a^{m+1} are multiples of φ_a^{m+1}, and thus have multiplicity at least $m+1$ at a. Hence there is a maximal $n \in \mathbb{N}$ with $\varphi \in I_a^n$. By (a) this means $\varphi = c \cdot \varphi_a^n$ for some $c \in \mathscr{O}_{X,a}$. But we must have $c \notin I_a$ since n is maximal. Hence $m = \operatorname{mult}_a(\varphi) = \operatorname{mult}_a(c \cdot \varphi_a^n) = n$, and the result follows. □

Remark 14.13. Thinking of a smooth curve $X \subset \mathbb{P}^2_{\mathbb{C}}$ as a 1-dimensional complex manifold, we can interpret the function φ_a of Lemma 14.12 as a *local coordinate* on X at a, i. e. as a function that gives an isomorphism of a neighborhood of a with a neighborhood of the origin in $\mathbb{C}$ in the classical topology. By standard complex analysis, any local holomorphic function on X at a can then be written as a non-vanishing holomorphic function times a power of the local coordinate [G4, Lemma 10.4]. Lemma 14.12 (b) is just the corresponding algebraic statement. Note however that this is only a statement about the local ring — in contrast to the analytic setting it does not imply that X has a Zariski-open neighborhood of a isomorphic to an open subset of $\mathbb{A}^1_{\mathbb{C}}$!

Remark 14.14 (Infinite multiplicity)**.** Let $X \subset \mathbb{P}^2$ be a smooth curve. For the following lemma, it is convenient to set formally $\operatorname{mult}_a(X, f) = \infty$ for all $a \in X$ if f is a homogeneous polynomial that vanishes identically on X. Note that by Lemma 14.12 (b) we then have for an arbitrary homogeneous polynomial f that $\operatorname{mult}_a(X, f) \geq m$ if and only if f is a multiple of φ_a^m in $\mathscr{O}_{X,a}$, where we interpret f as an element in $\mathscr{O}_{X,a}$ as in Remark 12.25, and φ_a is a local coordinate as in Lemma 14.12.

Lemma 14.15. *Let $X \subset \mathbb{P}^2$ be a smooth curve, and let $a \in X$ be a point.*

(a) *Let $f, g \in K[x_0, x_1, x_2]$ be homogeneous polynomials of the same degree with $\operatorname{mult}_a(X, f) \geq m$ and $\operatorname{mult}_a(X, g) \geq m$ for some $m \in \mathbb{N}$. Then:*
   - *$\operatorname{mult}_a(X, \lambda f + \mu g) \geq m$ for all $\lambda, \mu \in K$;*
   - *there are $\lambda, \mu \in K$, not both zero, such that $\operatorname{mult}_a(X, \lambda f + \mu g) \geq m+1$.*

(b) *Let $Y \subset \mathbb{P}^2$ be another curve, and set $m = \operatorname{mult}_a(X, Y)$. If $f \in K[x_0, x_1, x_2]$ is a homogeneous polynomial with $\operatorname{mult}_a(X, f) \geq m$, then we also have $\operatorname{mult}_a(Y, f) \geq m$.*

Proof. As in Remark 12.25, we will consider f and g as elements in the local ring $\mathscr{O}_{X,a}$.

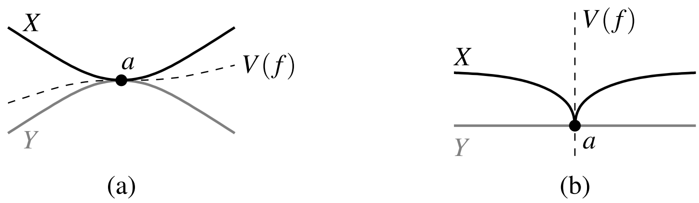
(a) We may assume that f and g do not vanish identically on X, since otherwise the statement is trivial. By Remark 14.14 there are then $u, v \in \mathscr{O}_{X,a}$ such that $f = u\,\varphi_a^m$ and $g = v\,\varphi_a^m$ in $\mathscr{O}_{X,a}$. So for any $\lambda, \mu \in K$, we have $\lambda f + \mu g = (\lambda u + \mu v)\,\varphi_a^m$, and thus $\operatorname{mult}_a(\lambda u + \mu v) \geq m$. Moreover, we can pick λ and μ not both zero such that $\lambda u(a) + \mu v(a) = 0 \in K$. Then $\operatorname{mult}_a(\lambda u + \mu v) \geq 1$, and hence $\operatorname{mult}_a(\lambda f + \mu g) \geq m+1$.

(b) As above we can assume that f does not vanish identically on X or Y. Let g and h be polynomials such that $I(X) = (g)$ and $I(Y) = (h)$. The assumption then means that $k := \operatorname{mult}_a(X, f) \geq m = \operatorname{mult}_a(X, h)$. Hence $f = u\,\varphi_a^k$ and $h = v\,\varphi_a^m$ for suitable units $u, v \in \mathscr{O}_{X,a}$ by Lemma 14.12 (b). This implies that $(f) \subset (h)$ in $\mathscr{O}_{X,a}$, so that $(f, g) \subset (g, h)$ in $\mathscr{O}_{\mathbb{A}^2,a}$. But then $(f, h) \subset (g, h)$ in $\mathscr{O}_{\mathbb{A}^2,a}$ as well, hence $\operatorname{mult}_a(f, h) \geq \operatorname{mult}_a(g, h)$, and thus $\operatorname{mult}_a(Y, f) \geq \operatorname{mult}_a(X, Y) = m$. □

Example 14.16. The following examples show that the smoothness assumption in Lemma 14.15 (b) is crucial.

(a) Let X and Y be two smooth plane curves such that $\operatorname{mult}_a(X, Y) = 2$. By Exercise 12.27 this means that X and Y are tangent at a, as in the picture below on the left. Lemma 14.15 (b) then states that any polynomial vanishing on X to order at least 2 at a also vanishes on Y to order at least 2 at a. In terms of the corresponding curve $V(f)$, this means using Exercise 12.27 again that any other curve that is (singular or) tangent to X at a is also (singular or) tangent to Y at a — which is obvious.

(b) In contrast to (a), in the picture on the right we have $X = V_p(x_2^3 - x_1^2 x_0)$, $Y = V_p(x_2)$, $f = x_1$, and thus at the origin $m = \operatorname{mult}_a(X, Y) = 2$, $\operatorname{mult}_a(X, f) = 3$, but $\operatorname{mult}_a(Y, f) = 1$. This fits well with the geometric interpretation of Remark 14.13: the curve X is singular at the origin, so locally not a 1-dimensional complex manifold. Hence there is no local coordinate on X around a, and the argument of Lemma 14.12 resp. Lemma 14.15 breaks down.



Lemma 14.17. *Let $X \subset \mathbb{P}^2$ be a smooth curve, and let $g, h \in S(X)$ be two non-zero homogeneous polynomials.*

(a) *If $\operatorname{div} g = \operatorname{div} h$ then g and h are linearly dependent in $S(X)$.*

(b) *If h is linear and $\operatorname{div} g \geq \operatorname{div} h$ then $h \mid g$ in $S(X)$.*

Proof. Let $f \in K[x_0, x_1, x_2]$ be a homogeneous polynomial with $I(X) = (f)$.

(a) By assumption we have $m_a := \operatorname{mult}_a(g) = \operatorname{mult}_a(h)$ for all $a \in X$. Moreover, Bézout's Theorem as in Corollary 12.26 (a) implies that $\sum_{a \in X} m_a = \deg X \cdot \deg g = \deg X \cdot \deg h$, so in particular we see already that $d := \deg g = \deg h$.

Now pick an arbitrary point $b \in X$. By Lemma 14.15 (a) there are $\lambda, \mu \in K$, not both zero, such that $\operatorname{mult}_a(\lambda g + \mu h) \geq m_a$ for all $a \in X$, and $\operatorname{mult}_b(\lambda g + \mu h) \geq m_b + 1$. Summing up, this means that $\sum_{a \in X} \operatorname{mult}_a(\lambda g + \mu h) \geq d \cdot \deg X + 1$. But $\lambda g + \mu h$ also has degree d, hence by Bézout again it follows that $\lambda f + \mu g$ must vanish identically on X, i. e. $\lambda g + \mu h = 0 \in S(X)$.

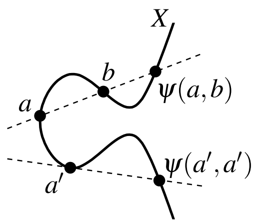
(b) Let $L = V(h)$, and choose a representative $\tilde{g} \in K[x_0, x_1, x_2]$ of $g \in S(X)$. We may assume that $\tilde{g}$ does not vanish identically on L, as otherwise $h \,|\, \tilde{g}$ in $K[x_0, x_1, x_2]$, and we are done.

By assumption, we have $\operatorname{mult}_a(X, \tilde{g}) \geq \operatorname{mult}_a(X, L)$ for all $a \in X \cap L$. As X is smooth, Lemma 14.15 (b) shows that then $\operatorname{mult}_a(L, \tilde{g}) \geq \operatorname{mult}_a(X, L)$, and thus that $\operatorname{div} \tilde{g} \geq \operatorname{div} f$ on L. As $L \cong \mathbb{P}^1$, we can find a homogeneous polynomial $f' \in K[x_0, x_1, x_2]$ of degree $\deg g - \deg f$ with $\operatorname{div} f' = \operatorname{div} \tilde{g} - \operatorname{div} f$ on L as in Example 14.11. Then $\operatorname{div}(f f') = \operatorname{div} \tilde{g}$ on L, which means by (a) that $f f'$ and $\tilde{g}$ are linearly dependent in $S(L)$. But then $\tilde{g} = f f' + ph$ for some homogeneous polynomial p and after possibly multiplying f' with a non-zero scalar, which means that $g = ph$ in $K[x_0, x_1, x_2]/(f) = S(X)$. □

24

We are now finally ready to prove that the Picard group of a smooth cubic curve in $\mathbb{P}^2$ is not trivial.

Notation 14.18. Let a and b be two points on a smooth cubic curve $X \subset \mathbb{P}^2$, not necessarily distinct. By Exercise 12.27 there is then a unique line $L \subset \mathbb{P}^2$ such that $a + b \leq L \cdot X$ as divisors on X (in the sense of Definition 14.1 (b)), namely the line through a and b if these points are distinct, and the tangent line to X at $a = b$ otherwise. But $L \cdot X$ is an effective divisor of degree 3 on X, and hence there is a unique point $c \in X$ (which need not be distinct from a and b) with $L \cdot X = a + b + c$. In the following, we will denote this point c by $\psi(a, b)$.



In geometric terms, for general $a, b \in X$ (i. e. such that none of the above points coincide) the point $\psi(a, b)$ is just the third point of intersection of X with the line through a and b. Hence the above definition is a generalization of our construction in Exercise 7.15. In fact, one can show that the map $\psi : X \times X \to X, (a, b) \mapsto \psi(a, b)$ is a morphism, but we will not need this result here.

Proposition 14.19. *Let $X \subset \mathbb{P}^2$ be a smooth cubic curve. Then for all distinct $a, b \in X$ we have $a - b \neq 0$ in $\operatorname{Pic}^0 X$, i. e. there is no non-zero rational function φ on X with $\operatorname{div} \varphi = a - b$.*

Proof. Assume for a contradiction that the statement of the proposition is false. Then there are a positive integer d and homogeneous polynomials $f, g \in S(X)$ of degree d such that the following conditions hold:

(a) There are points $a_1, \dots, a_{3d-1}$ and $a \neq b$ on X such that

$$\operatorname{div} g = a_1 + \cdots + a_{3d-1} + a \quad \text{and} \quad \operatorname{div} f = a_1 + \cdots + a_{3d-1} + b$$

(hence $\operatorname{div} \varphi = a - b$ for $\varphi = \frac{g}{f}$).

(b) Among the $a_1, \dots, a_{3d-1}$ there are at least $2d$ distinct points. (If this is not the case in the first place, we can replace f and g by $f \cdot l$ and $g \cdot l$, respectively, for some homogeneous linear polynomial l that vanishes on X at three distinct points that are not among the a_i. This raises the degree of the polynomials by 1 and the number of distinct points by 3, so by doing this often enough we can get at least $2d$ distinct points.)

Pick d minimal with these two properties.

If $d = 1$ then $\operatorname{div} g = a_1 + a_2 + a$ and $\operatorname{div} f = a_1 + a_2 + b$, so we must have $a = b = \psi(a_1, a_2)$ by Notation 14.18, in contradiction to our assumption. Hence we can assume that $d > 1$. Let us relabel the points $a_1, \dots, a_{3d-1}$ such that $a_2 \neq a_3$, and such that $a_1 = a_2$ if there are any equal points among the a_i.

Now consider linear combinations $\lambda f + \mu g$ for $\lambda, \mu \in K$, not both zero. As the polynomials f and g have different divisors they are linearly independent in $S(X)$, and hence $\lambda f + \mu g$ does not vanish identically on X. Moreover, by Lemma 14.15 (a) we have $a_1 + \dots + a_{3d-1} \leq \operatorname{div}(\lambda f + \mu g)$ for all λ and μ, and for any given $c \in X$ there are λ and μ with $a_1 + \dots + a_{3d-1} + c \leq \operatorname{div}(\lambda f + \mu g)$. Of course, by Bézout's Theorem we must then have $\operatorname{div}(\lambda f + \mu g) = a_1 + \dots + a_{3d-1} + c$.

In other words, by passing to linear combinations of f and g we can assume that the last points a and b in the divisors of f and g are any two points we like. Let us choose $a = \psi(a_1, a_2)$ and $b = \psi(a_1, a_3)$. Then

$$\begin{aligned} \operatorname{div} g &= (a_1 + a_2 + \psi(a_1, a_2)) + a_3 + a_4 + \dots + a_{3d-1} \\ \text{and} \quad \operatorname{div} f &= (a_1 + a_3 + \psi(a_1, a_3)) + a_2 + a_4 + \dots + a_{3d-1}. \end{aligned}$$

But $a_1 + a_2 + \psi(a_1, a_2)$ and $a_1 + a_3 + \psi(a_1, a_3)$ are divisors of homogeneous linear polynomials k and l in $S(X)$, respectively, and hence by Lemma 14.17 (b) there are homogeneous polynomials $f', g' \in S(X)$ of degree $d-1$ with $g = kg'$ and $f = lf'$, and thus with

$$\operatorname{div} g' = a_4 + \dots + a_{3d-1} + a_3 \quad \text{and} \quad \operatorname{div} f' = a_4 + \dots + a_{3d-1} + a_2.$$

Note that these new polynomials f' and g' satisfy (a) for d replaced by $d-1$, as $a_3 \neq a_2$ by assumption. Moreover, f' and g' satisfy (b) because, if there are any equal points among the a_i at all, then by our relabeling of these points there are only two distinct points among a_1, a_2, a_3, and so there must still be at least $2d-2$ distinct points among $a_4, \dots, a_{3d-1}$.

This contradicts the minimality of d, and therefore proves the proposition. □

Remark 14.20. In particular, Proposition 14.19 implies that $\operatorname{Pic}^0 X \neq \{0\}$ for any smooth cubic surface $X \subset \mathbb{P}^2$. So by Example 14.11 we can already see that X is not isomorphic to $\mathbb{P}^1$. In fact, we will see in the next chapter that Proposition 14.19 suffices to compute $\operatorname{Pic}^0 X$ explicitly.