Since x'' and y'' are rational functions in the coordinates $(x,y),(x',y')$, this shows that $\varphi\colon C_0 \times C_0 \dashrightarrow C_0$ is a rational map. From the given formula, φ is a morphism wherever $x \neq x'$, since then the denominator of u is nonzero. Now if $x = x'$ and $y = -y'$, then x'' and y'' should be infinity, corresponding to the fact that the line AB meets the projective curve C at the point at infinity $O = (0,1,0)$. However, if $x = x'$ and $y = y' \neq 0$ then the point $P = (x'', y'')$ should be well defined. I claim that f, g are regular functions on $C_0 \times C_0$ at such points: to see this, note that

$$y^2 = x^3 + ax + b \quad \text{and} \quad y'^2 = x'^3 + ax' + b,$$

giving

$$y^2 - y'^2 = x^3 - x'^3 + a(x - x');$$

therefore as rational functions on $C_0 \times C_0$, there is an equality

$$u = (y - y')/(x - x') = (x^2 + xx' + x'^2 + a)/(y + y').$$

Looking at the denominator, it follows that u (hence also f and g) is regular whenever $y \neq -y'$.

The conclusion of the calculation is the following proposition: the addition law $\varphi\colon C_0 \times C_0 \dashrightarrow C_0$ is a morphism at $(A,B) \in C_0 \times C_0$ provided that $A + B \neq O$.

Exercises to Chapter 4

4.1 Check that the statements of §4 up to and including (4.8, I) are valid for any field k; discover in particular what they mean for a finite field. Give a counterexample to (4.8, II) if k is not algebraically closed.

4.2 $\varphi\colon \mathbb{A}^1 \to \mathbb{A}^3$ is the polynomial map given by $X \mapsto (X, X^2, X^3)$; prove that the image of φ is an algebraic subset $C \subset \mathbb{A}^3$ and that $\varphi\colon \mathbb{A}^1 \to C$ is an isomorphism. Try to generalise.

4.3 $\varphi_n\colon \mathbb{A}^1 \to \mathbb{A}^2$ is the polynomial map given by $X \mapsto (X^2, X^n)$; show that if n is even, the image of φ_n is isomorphic to $\mathbb{A}^1$, and φ_n is two-to-one outside 0. And if n is odd, show that φ_n is bijective, and give a rational inverse of φ_n.

4.4 Prove that a morphism $\varphi\colon X \to Y$ between two affine varieties is an isomorphism of X with a subvariety $\varphi(X) \subset Y$ if and only if the induced map $\Phi\colon k[Y] \to k[X]$ is surjective.

4.5 Let $C : (Y^2 = X^3) \subset \mathbb{A}^2$; then

(a) the parametrisation $f\colon \mathbb{A}^1 \to C$ given by (T^2, T^3) is a polynomial map;

(b) f has a rational inverse $g : C \dashrightarrow \mathbb{A}^1$ defined by $(X,Y) \mapsto Y/X$;

(c) $\operatorname{dom} g = C \setminus \{(0,0)\}$;

(d) f and g give inverse isomorphisms $\mathbb{A}^1 \setminus \{0\} \cong C \setminus \{(0,0)\}$.

4.6 (i) Show that the domain of $g \circ f$ may be strictly larger than $\operatorname{dom} f \cap f^{-1}(\operatorname{dom} g)$. [Hint: this may happen if g and f are inverse rational maps; try f and g as in Ex. 4.5.]

(ii) Most courses on calculus of several variables contain examples such as the function $f(x,y) = xy/(x^2+y^2)$. Explain how come f is C^∞ when restricted to any smooth curve through $(0,0)$, but is not even continuous as a function of 2 variables.

4.7 Let $C : (Y^2 = X^3 + X^2) \subset \mathbb{A}^2$; the familiar parametrisation $\varphi\colon \mathbb{A}^1 \to C$ given by $(T^2 - 1, T^3 - T)$ is a polynomial map, but is not an isomorphism (why not?). Find out whether the restriction $\varphi'\colon \mathbb{A}^1 \setminus \{1\} \to C$ is an isomorphism:

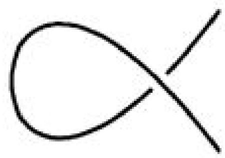

Figure 4.3: Nodal curve with gap

4.8 Let $C : (Y^3 = X^4 + X^3) \subset \mathbb{A}^2$; show that $(X, Y) \mapsto X/Y$ defines a rational map $\psi\colon C \dashrightarrow \mathbb{A}^1$, and that its inverse is a polynomial map $\varphi\colon \mathbb{A}^1 \to C$ parametrising C. Prove that φ restricts to an isomorphism

$$\mathbb{A}^1 \setminus \{3 \text{ pts.}\} \cong C \setminus \{(0,0)\}.$$

4.9 Let $V : (XT = YZ) \subset \mathbb{A}^4$; explain why $k[V]$ is not a UFD. (It's not hard to get the idea, but rather harder to give a rigorous proof.) If $f = X/Y \in k(V)$, find $\operatorname{dom} f$, and prove that it is strictly bigger than the locus $(Y = 0) \subset V$.

4.10 Let $f\colon \mathbb{A}^1 \to \mathbb{A}^2$ be given by $X \mapsto (X, 0)$, and let $g\colon \mathbb{A}^2 \dashrightarrow \mathbb{A}^1$ be the rational map given by $(X, Y) \mapsto X/Y$; show that the composite $g \circ f$ is not defined anywhere. Determine what is the largest subset of the function field $k(\mathbb{A}^1)$ on which g^* is defined.

4.11 Define and study the notion of product of two algebraic sets. More precisely,

(i) if $V \subset \mathbb{A}^n_k$ and $W \subset \mathbb{A}^m_k$ are algebraic sets, prove that $V \times W \subset \mathbb{A}^{n+m}_k$ is also;

(ii) give examples to show that the Zariski topology on $V \times W$ is not the product topology of those on V and on W;

(iii) prove that V, W irreducible $\implies V \times W$ irreducible;

(iv) prove that if $V \cong V'$ and $W \cong W'$ then $V \times W \cong V' \times W'$.

4.12 (a) Prove that any $f \in k(\mathbb{A}^2)$ which is not regular at the origin $(0,0)$ also fails to be regular at points of a curve passing through $(0,0)$.

(b) Deduce that $\mathbb{A}^2 \setminus (0,0)$ is not affine. [Hints: For (a), use the fact that $k(\mathbb{A}^2) = k(X, Y)$ is the field of fractions of the UFD $k[X, Y]$, together with the result of Ex. 3.13, (b). For (b), assume that $\mathbb{A}^2 \setminus (0,0)$ is affine, and determine its coordinate ring; then get a contradiction using Corollary 4.5.]

Part III

Applications