

The standard open sets  $V_f$  are important because they form a basis for the Zariski topology of  $V$ : every open set  $U \subset V$  is a union of  $V_f$  (since every closed subset is of the form  $V(I) = \bigcap_{f \in I} V(f)$  for some ideal). Thus the point of the result just proved is that every open set  $U \subset V$  is a union of open sets  $V_f$  which are affine varieties.

## 4.14 Worked example

In §2 I discussed the addition law  $(A, B) \mapsto A + B$  on a plane nonsingular (projective) cubic  $C \subset \mathbb{P}^2$ . Let  $C_0 : (y^2 = x^3 + ax + b)$  be a nonsingular affine cubic:

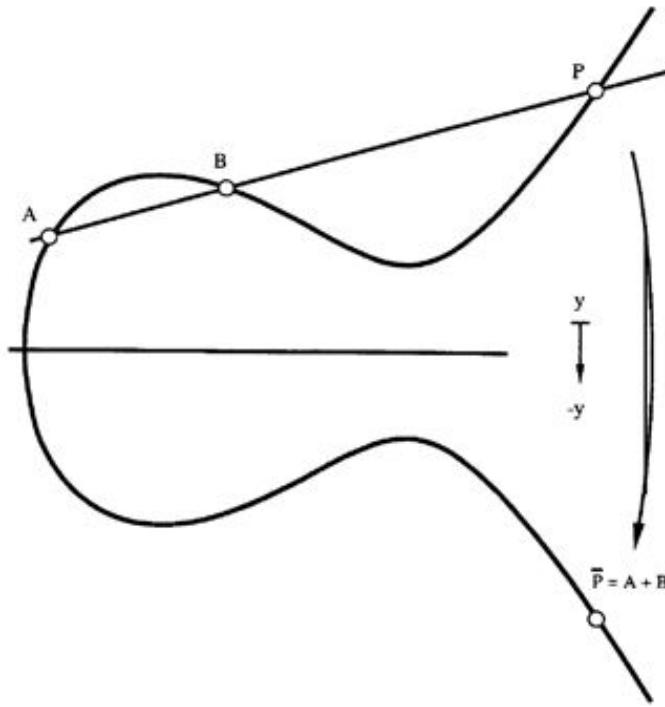


Figure 4.2: Group law on cubic as a morphism

I show here that the addition law defines a rational map  $\varphi: C_0 \times C_0 \dashrightarrow C_0$ , and that  $\varphi$  is a morphism wherever it should be. Although I will not labour the point, this argument can be used to give another proof ‘by continuity’ of the associativity of the group law valid for any field (see the discussion in (2.10)).

It is not difficult to see (compare Ex. 2.7) that if  $A = (x, y)$ ,  $B = (x', y')$ , and  $x \neq x'$  then setting  $u = (y - y')/(x - x')$ , the third point of intersection is  $P = (x'', y'')$ , where

$$\begin{aligned} x'' &= f(x, y, x', y') = u^2 - (x + x'), \\ y'' &= g(x, y, x', y') = u^3 + xu + y'. \end{aligned}$$

Since  $x''$  and  $y''$  are rational functions in the coordinates  $(x, y), (x', y')$ , this shows that  $\varphi: C_0 \times C_0 \dashrightarrow C_0$  is a rational map. From the given formula,  $\varphi$  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  $\varphi: C_0 \times C_0 \dashrightarrow C_0$  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  $\varphi: \mathbb{A}^1 \rightarrow \mathbb{A}^3$  is the polynomial map given by  $X \mapsto (X, X^2, X^3)$ ; prove that the image of  $\varphi$  is an algebraic subset  $C \subset \mathbb{A}^3$  and that  $\varphi: \mathbb{A}^1 \rightarrow C$  is an isomorphism. Try to generalise.
- 4.3  $\varphi_n: \mathbb{A}^1 \rightarrow \mathbb{A}^2$  is the polynomial map given by  $X \mapsto (X^2, X^n)$ ; show that if  $n$  is even, the image of  $\varphi_n$  is isomorphic to  $\mathbb{A}^1$ , and  $\varphi_n$  is two-to-one outside 0. And if  $n$  is odd, show that  $\varphi_n$  is bijective, and give a rational inverse of  $\varphi_n$ .
- 4.4 Prove that a morphism  $\varphi: X \rightarrow Y$  between two affine varieties is an isomorphism of  $X$  with a subvariety  $\varphi(X) \subset Y$  if and only if the induced map  $\Phi: k[Y] \rightarrow k[X]$  is surjective.
- 4.5 Let  $C : (Y^2 = X^3) \subset \mathbb{A}^2$ ; then
  - (a) the parametrisation  $f: \mathbb{A}^1 \rightarrow C$  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)  $\text{dom } g = C \setminus \{(0, 0)\}$ ;
  - (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  $\text{dom } f \cap f^{-1}(\text{dom } g)$ . [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  $C^\infty$  when restricted to any smooth curve through  $(0, 0)$ , but is not even continuous as a function of 2 variables.