Chapter 2

Cubics and the group law

2.1 Examples of parametrised cubics

Some plane cubic curves can be parametrised, just as the conics:

Nodal cubic $C : (y^2 = x^3 + x^2) \subset \mathbb{R}^2$ is the image of the map $\varphi \colon \mathbb{R}^1 \to \mathbb{R}^2$ given by $t \mapsto (t^2 - 1, t^3 - t)$ (check it and see);

Cuspidal cubic $C : (y^2 = x^3) \subset \mathbb{R}^2$ is the image of $\varphi \colon \mathbb{R}^1 \to \mathbb{R}^2$ given by $t \mapsto (t^2, t^3)$:

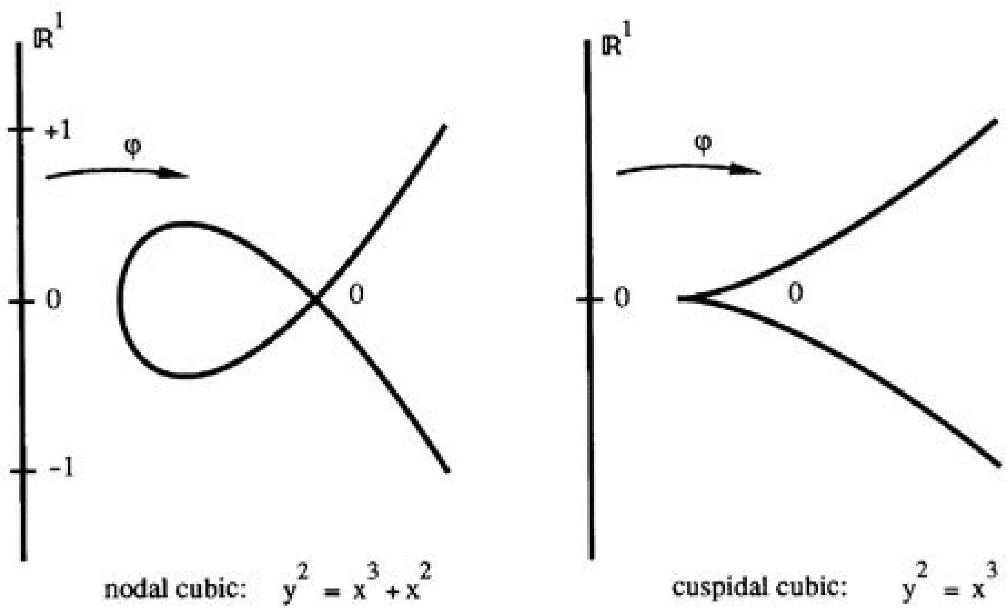

Figure 2.1: Parametrised cubic curves

Think about the singularities of the image curve, and of the map φ. These examples will occur throughout the course, so spend some time playing with the equations; see Ex. 2.1–2.

2.2 The curve $(y^2 = x(x-1)(x-\lambda))$ has no rational parametrisation

Parametrised curves are nice; for example, if you're interested in Diophantine problems, you could hope for a rule giving all $\mathbb{Q}$-valued points, as in (1.1). The parametrisation of (1.1) was of the form $x = f(t), y = g(t)$, where f and g were *rational functions*, that is, quotients of two polynomials.

Theorem *Let k be a field of characteristic $\neq 2$, and let $\lambda \in k$ with $\lambda \neq 0, 1$; let $f, g \in k(t)$ be rational functions such that*

$$f^2 = g(g-1)(g-\lambda). \tag{$*$}$$

Then $f, g \in k$.

This is equivalent to saying that there does not exist any nonconstant map $\mathbb{R}^1 \dashrightarrow C : (y^2 = x(x-1)(x-\lambda))$ given by rational functions. This reflects a very strong 'rigidity' property of varieties.

The proof of the theorem is arithmetic in the field $k(t)$ using the fact that $k(t)$ is the field of fractions of the UFD $k[t]$. It's quite a long proof, so either be prepared to study it in detail, or skip it for now (GOTO 2.4). In Ex. 2.12, there is a very similar example of a nonexistence proof by arithmetic in $\mathbb{Q}$.

Proof Using the fact that $k[t]$ is a UFD, I write

$$f = r/s \quad \text{with } r, s \in k[t] \text{ and coprime,}$$
$$g = p/q \quad \text{with } p, q \in k[t] \text{ and coprime.}$$

Clearing denominators, $(*)$ becomes

$$r^2 q^3 = s^2 p(p-q)(p-\lambda q).$$

Then since r and s are coprime, the factor s^2 on the right-hand side must divide q^3, and in the same way, since p and q are coprime, the left-hand factor q^3 must divide s^2. Therefore,

$$s^2 \mid q^3 \text{ and } q^3 \mid s^2, \quad \text{so that } s^2 = aq^3 \quad \text{with } a \in k$$

(a is a unit of $k[t]$, therefore in k).

Then

$$aq = (s/q)^2 \quad \text{is a square in } k[t].$$

Also,

$$r^2 = ap(p-q)(p-\lambda q),$$

so that by considering factorisation into primes, there exist nonzero constants $b, c, d \in k$ such that

$$bp, \quad c(p-q), \quad d(p-\lambda q)$$

are all squares in $k[t]$. If I can prove that p, q are constants, then it follows from what's already been said that r, s are also, proving the theorem. To prove that p, q are constants, set K for the algebraic closure of k; then $p, q \in K[t]$ satisfy the conditions of the next lemma.