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.

Lemma 2.3 *Let K be an algebraically closed field, $p, q \in K[t]$ coprime elements, and assume that 4 distinct linear combinations (that is, $\lambda p + \mu q$ for 4 distinct ratios $(\lambda : \mu) \in \mathbb{P}^1 K$) are squares in $K[t]$; then $p, q \in K$.*

Proof *(Fermat's method of 'infinite descent')* Both the hypotheses and conclusion of the lemma are not affected by replacing p, q by

$$p' = ap + bq, \quad q' = cp + dq,$$

with $a, b, c, d \in K$ and $ad - bc \neq 0$. Hence I can assume that the 4 given squares are

$$p, \quad p - q, \quad p - \lambda q, \quad q.$$

Then $p = u^2$, $q = v^2$, and $u, v \in K[t]$ are coprime, with

$$\max(\deg u, \deg v) < \max(\deg p, \deg q).$$

Now by contradiction, suppose that $\max(\deg p, \deg q) > 0$ and is minimal among all p, q satisfying the condition of the lemma. Then both of

$$p - q = u^2 - v^2 = (u - v)(u + v)$$

and

$$p - \lambda q = u^2 - \lambda v^2 = (u - \mu v)(u + \mu v)$$

(where $\mu = \sqrt{\lambda}$) are squares in $K[t]$, so that by coprimeness of u, v, I conclude that each of $u - v$, $u + v$, $u - \mu v$, $u + \mu v$ are squares. This contradicts the minimality of $\max(\deg p, \deg q)$. Q.E.D.

2.4 Linear systems

Write $S_d = \{\text{forms of degree } d \text{ in } (X, Y, Z)\}$; (recall that a *form* is just a homogeneous polynomial). Any element $F \in S_d$ can be written in a unique way as

$$F = \sum a_{ijk} X^i Y^j Z^k$$

with $a_{ijk} \in k$, and the sum taken over all $i, j, k \geq 0$ with $i + j + k = d$; this means of course that S_d is a k-vector space with basis

$$\begin{array}{ccccc} & & Z^d & & \\ & XZ^{d-1} & & YZ^{d-1} & \\ & \dots & & \dots & \\ & X^{d-1}Z & X^{d-2}YZ \ \dots & XY^{d-2}Z & \\ X^d & X^{d-1}Y & X^{d-2}Y^2 & \dots & Y^d \end{array}$$

and in particular, $\dim S_d = \binom{d+2}{2}$. For $P_1, \dots, P_n \in \mathbb{P}^2$, let

$$S_d(P_1, \dots, P_n) = \left\{ F \in S_d \;\middle|\; F(P_i) = 0 \text{ for } i = 1, \dots, n \right\} \subset S_d.$$

Each of the conditions $F(P_i) = 0$ (more precisely, $F(X_i, Y_i, Z_i) = 0$, where $P_i = (X_i : Y_i : Z_i)$) is one linear condition on F, so that $S_d(P_1, \dots, P_n)$ is a vector space of dimension $\geq \binom{d+2}{2} - n$.