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

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

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

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

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 $S_d(P_1, \ldots, P_n)$ is a vector space of dimension $\geq \binom{d+2}{2} - n$.

Lemma 2.5 *Suppose that k is an infinite field, and let $F \in S_d$.*

(i) Let $L \subset \mathbb{P}^2_k$ be a line; if $F \equiv 0$ on L, then F is divisible in $k[X,Y,Z]$ by the equation of L. That is, $F = H \cdot F'$ where H is the equation of L and $F' \in S_{d-1}$.

(ii) Let $C \subset \mathbb{P}^2_k$ be a nonempty nondegenerate conic; if $F \equiv 0$ on C, then F is divisible in $k[X,Y,Z]$ by the equation of C. That is, $F = Q \cdot F'$ where Q is the equation of C and $F' \in S_{d-2}$.

If you think this statement is obvious, congratulations on your intuition: you have just guessed a particular case of the Nullstellensatz. Now find your own proof (GOTO 2.6).

Proof (i) By a change of coordinates, I can assume $H = X$. Then for any $F \in S_d$, there exists a unique expression $F = X \cdot F'_{d-1} + G(Y,Z)$: just gather together all the monomials involving X into the first summand, and what's left must be a polynomial in Y, Z only. Now

$$F \equiv 0 \text{ on } L \iff G \equiv 0 \text{ on } L \iff G(Y,Z) = 0.$$

The last step holds because of (1.8): if $G(Y,Z) \neq 0$ then it has at most d zeros on $\mathbb{P}^1_k$, whereas if k is infinite, then so is $\mathbb{P}^1_k$.

(ii) By a change of coordinates, $Q = XZ - Y^2$. Now let me prove that for any $F \in S_d$, there exists a unique expression

$$F = Q \cdot F'_{d-2} + A(X,Z) + YB(X,Z):$$

if I just substitute $XZ - Q$ for Y^2 wherever it occurs in F, what's left has degree ≤ 1 in Y, and is therefore of the form $A(X,Z) + YB(X,Z)$. Now as in (1.7), C is the parametrised conic given by $X = U^2, Y = UV, Z = V^2$, so that

$$\begin{aligned} F \equiv 0 \text{ on } C &\iff A(U^2,V^2) + UVB(U^2,V^2) \equiv 0 \text{ on } C \\ &\iff A(U^2,V^2) + UVB(U^2,V^2) = 0 \in k[U,V] \\ &\iff A(X,Z) = B(X,Z) = 0. \end{aligned}$$

Here the last equality comes by considering separately the terms of even and odd degrees in the form $A(U^2,V^2) + UVB(U^2,V^2)$. Q.E.D.

Ex. 2.2 gives similar cases of 'explicit' Nullstellensatz.

Corollary *Let $L : (H = 0) \subset \mathbb{P}^2_k$ be a line (or $C : (Q = 0) \subset \mathbb{P}^2_k$ a nondegenerate conic); suppose that points $P_1, \dots, P_n \in \mathbb{P}^2_k$ are given, and consider $S_d(P_1, \dots, P_n)$ for some fixed d. Then*

(i) If $P_1, \dots, P_a \in L, P_{a+1}, \dots, P_n \notin L$ and $a > d$, then

$$S_d(P_1, \dots, P_n) = H \cdot S_{d-1}(P_{a+1}, \dots, P_n).$$

(ii) If $P_1, \dots, P_a \in C, P_{a+1}, \dots, P_n \notin C$ and $a > 2d$, then

$$S_d(P_1, \dots, P_n) = Q \cdot S_{d-2}(P_{a+1}, \dots, P_n).$$