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 $\geq \binom{d+2}{2} - n$.