Proof In the diagram, consider the two triples of lines

$$L_1 : PAF, \quad L_2 : QDE, \quad L_3 : RBC,$$

and

$$M_1 : PCD, \quad M_2 : QAB, \quad M_3 : REF;$$

let $C_1 = L_1 + L_2 + L_3$ and $C_2 = M_1 + M_2 + M_3$. Now I'm all set to apply (2.7), since clearly C_1 and C_2 are two cubics such that

$$C_1 \cap C_2 = \{A, B, C, D, E, F, P, Q, R\}.$$

Suppose PQR are collinear, with $L = PQR$; let Γ be the conic through $ABCDE$ (the existence and unicity of which is provided by Proposition 1.11). Then by construction, $L+\Gamma$ is a cubic passing through the 8 points A, B, C, D, E, P, Q, R, and by (2.7), it must contain F; by assumption, $F \notin L$, so that necessarily $F \in \Gamma$, proving that the six points are conconic.

Now conversely, suppose that $ABCDEF$ are on a conic Γ, and let $L = PQ$; then $L + \Gamma$ is a cubic passing through A, B, C, D, E, F, P, Q, so by (2.7) it must pass through R. Now R can't be on the conic Γ (since otherwise Γ is a line pair, and some of the 6 lines of the diagram must coincide), so $R \in L$, that is, PQR are collinear. Q.E.D.

2.12 Inflexion, normal form

Every cubic in $\mathbb{P}^2_{\mathbb{R}}$ or $\mathbb{P}^2_{\mathbb{C}}$ can be put in the normal form

$$C : Y^2Z = X^3 + aXZ^2 + bZ^3, \qquad (**)$$

or in the affine form

$$y^2 = x^3 + ax + b.$$

Now consider the above curve C; where does it meet the line at infinity $L : (Z = 0)$? That's easy, just substitute $Z = 0$ in the defining polynomial $F = -Y^2Z + X^3 + aXZ^2 + bZ^3$ to get $F|L = X^3$; this means that $F|L$ has a triple zero at $P = (0, 1, 0)$. To see what this means geometrically, set $Y = 1$, to get the equation in affine coordinates (x, z) around $(0, 1, 0)$:

$$z = x^3 + axz^2 + bz^3.$$

This curve is approximated to a high degree of accuracy by $z = x^3$: the behaviour is described by

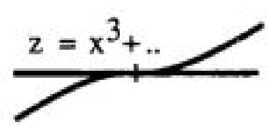

Figure 2.5: Inflexion point

saying that C has an *inflexion point* at $(0, 1, 0)$. More generally, an inflexion point P on a curve C is defined by the condition that there is a line $L \subset \mathbb{P}^2_k$ such that $F|L$ has a zero of multiplicity ≥ 3 at

P (see Ex. 2.9; in fact necessarily $L = T_P C$ by (2.8, b), and the multiplicity $= 3$ by (1.9)). It is not hard to interpret this in terms of the derivatives and second derivatives of the defining equations: for example, if the defining equation is $y = f(x)$, then the condition for an inflexion point is simply $\frac{d^2 f}{dx^2}(P) = 0$; this corresponds in the diagram to the curve passing through a transition from being 'concave downwards' to being 'concave upwards'. There is a general criterion for a plane curve to have an inflexion point in terms of the *Hessian*, see for example [Fulton, p. 116] or Ex. 7.3, (iii).

It can be shown (see Ex. 2.10) that conversely, if a plane cubic C has an inflexion point, then its equation can be put in normal form $(**)$ as above.

2.13 Simplified group law

The normal form $(**)$ is extremely convenient for the group law: take the inflexion point $O = (0, 1, 0)$ as the neutral element. Under these conditions, the group law becomes particularly nice, for the following reasons:

(a) $C = \{O\} \cup$affine curve $C_0 : (y^2 = x^3 + ax + b)$; so it is legitimate to treat C as an affine curve, with occasional references to the single point O at infinity, the zero of the group law.

(b) The lines through O, which are the main ingredient in part (i) of the construction of the group law in (2.8), are given projectively by $X = \lambda Z$, and affinely by $x = \lambda$; any such line meets C at points $(\lambda, \pm\sqrt{\lambda^3 + a\lambda + b})$, and at infinity. Hence if $P = (x, y)$, then the point $\overline{P}$ constructed in (2.8, i) is $(x, -y)$; thus $P \mapsto \overline{P}$ is the natural symmetry $(x, y) \mapsto (x, -y)$ of the curve C_0:

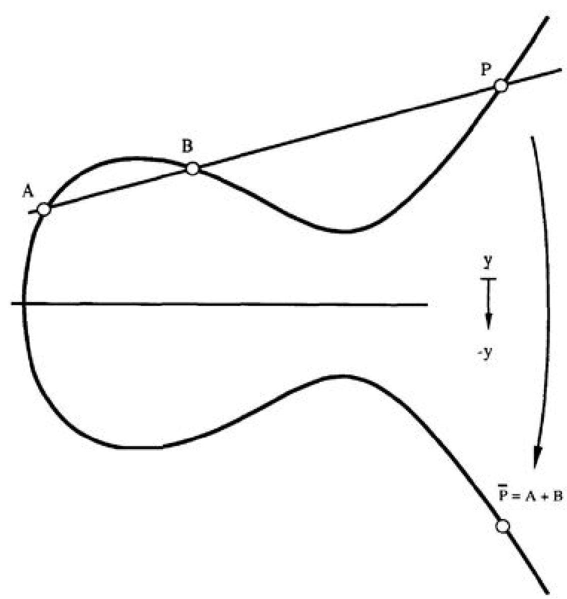

Figure 2.6: Minus as reflexion in the x-axis