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:

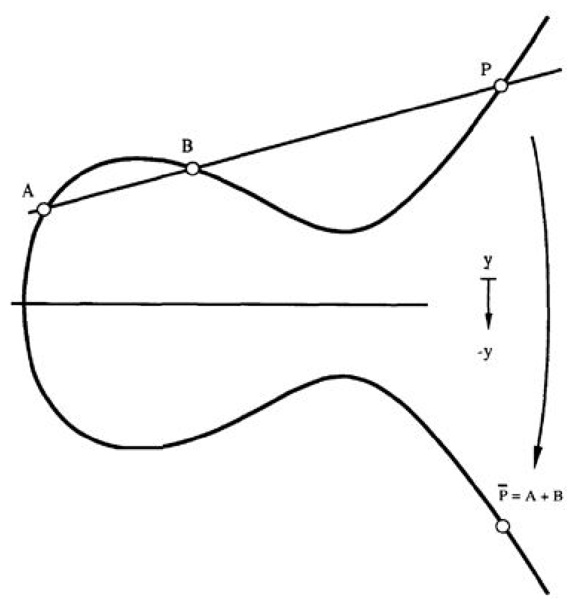

Figure 2.6: Minus as reflexion in the x-axis

(c) The inverse of the group law (2.8, IV) is described in terms of $\overline{O}$, the point constructed as the 3rd point of intersection of the unique line L such that $F|L$ has O as a repeated zero; however, in our case, this line is the line at infinity $L : (Z = 0)$, and $L \cap C = 3O$, so that $\overline{O} = O$, and the inverse of the group law then simplifies to $-P = \overline{P}$.

I can now restate the group law as a much simplified version of Theorem 2.8:

Theorem *Let C be a cubic in the normal form $(**)$; then there is a unique group law on C such that $O = (0, 1, 0)$ is the neutral element, the inverse is given by $(x, y) \mapsto (x, -y)$, and for all $P, Q, R \in C$,*

$$P + Q + R = O \iff P, Q, R \text{ are collinear.}$$

Exercises to Chapter 2

2.1 Let $C : (y^2 = x^3 + x^2) \subset \mathbb{R}^2$. Show that a variable line through $(0, 0)$ meets C at one further point, and hence deduce the parametrisation of C given in (2.1). Do the same for $(y^2 = x^3)$ and $(x^3 = y^3 - y^4)$.

2.2 Let $\varphi\colon \mathbb{R}^1 \to \mathbb{R}^2$ be the map given by $t \mapsto (t^2, t^3)$; prove directly that any polynomial $f \in \mathbb{R}[X, Y]$ vanishing on the image $C = \varphi(\mathbb{R}^1)$ is divisible by $Y^2 - X^3$. [Hint: use the method of Lemma 2.5.] Determine what property of a field k will ensure that the result holds for $\varphi\colon k \to k^2$ given by the same formula.

Do the same for $t \mapsto (t^2 - 1, t^3 - t)$.

2.3 Let $C : (f = 0) \subset k^2$, and let $P = (a, b) \in C$; assume that $\partial f/\partial x(P) \neq 0$. Prove that the line

$$L : \frac{\partial f}{\partial x}(P) \cdot (x - a) + \frac{\partial f}{\partial y}(P) \cdot (y - b) = 0)$$

is the tangent line to C at P, that is, the unique line L of k^2 for which $f|L$ has a multiple root at P (this is worked out in detail in (6.1)).

2.4 Let $C : (y^2 = x^3 + 4x)$, with the simplified group law (2.13). Show that the tangent line to C at $P = (2, 4)$ passes through $(0, 0)$, and deduce that P is a point of order 4 in the group law.

2.5 Let $C : (y^2 = x^3 + ax + b) \subset \mathbb{R}^2$ be nonsingular; find all points of order 2 in the group law, and understand what group they form (there are two cases to consider).

Now explain geometrically how you would set about finding all points of order 4 on C.

2.6 Let $C : (y^2 = x^3 + ax + b) \subset \mathbb{R}^2$; write a computer program to sketch part of C, and to calculate the group law. That is, it prompts you for the coordinates of 2 points A and B, then draws the lines and tells you the coordinates of $A + B$. (Use real variables.)

2.7 Let $C : (y^2 = x^3 + ax + b) \subset k^2$; if $A = (x_1, y_1)$ and $B = (x_2, y_2)$, show how to give the coordinates of $A + B$ as rational functions of x_1, y_1, x_2, y_2. [Hint: if $F(X)$ is a polynomial of degree 3 and you know 2 of the roots, you can find the 3rd by looking at just one coefficient of F. This is a question with a nonunique answer, since there are many correct expressions for the rational functions. One solution is given in (4.14).]