laborious procedure. On the other hand, the geometric method sketched above gives an elegant derivation of the auxiliary cubic which only involves evaluating a 3×3 determinant.

The above treatment is taken from [M.Berger, 16.4.10 and 16.4.11.1].

Exercises to Chapter 1

1.1 Parametrise the conic $C : (x^2+y^2 = 5)$ by considering a variable line through $(2,1)$ and hence find all rational solutions of $x^2 + y^2 = 5$.

1.2 Let p be a prime; by experimenting with various p, guess a necessary and sufficient condition for $x^2+y^2 = p$ to have rational solutions; prove your guess (a hint is given after Ex. 1.9 below – bet you can't do it for yourself!).

1.3 Prove the statement in (1.3), that an affine transformation can be used to put any conic of $\mathbb{R}^2$ into one of the standard forms (a–l). [Hint: use a linear transformation $\mathbf{x} \mapsto A\mathbf{x}$ to take the leading term $ax^2 + bxy + cy^2$ into one of $\pm x^2 \pm y^2$ or $\pm x^2$ or 0; then complete the square in x and y to get rid of as much of the linear part as possible.]

1.4 Make a detailed comparison of the affine conics in (1.3) with the projective conics in (1.6).

1.5 Let k be any field of characteristic $\neq 2$, and V a 3-dimensional k-vector space; let $Q \colon V \to k$ be a nondegenerate quadratic form on V. Show that if $0 \neq e_1 \in V$ satisfies $Q(e_1) = 0$ then V has a basis e_1, e_2, e_3 such that $Q(x_1e_1 + x_2e_2 + x_3e_3) = x_1x_3 + ax_2^2$. [Hint: work with the symmetric bilinear form φ associated to Q; since φ is nondegenerate, there is a vector e_3 such that $\varphi(e_1, e_3) = 1$. Now find a suitable e_2.]

Deduce that a nonempty, nondegenerate conic $C \subset \mathbb{P}^2_k$ is projectively equivalent to $(XZ = Y^2)$.

1.6 Let k be a field with at least 4 elements, and $C : (XZ = Y^2) \subset \mathbb{P}^2_k$; prove that if $Q(X,Y,Z)$ is a quadratic form which vanishes on C then $Q = \lambda(XZ - Y^2)$. [Hint: if you really can't do this for yourself, compare with the argument in the proof of Lemma 2.5.]

1.7 In $\mathbb{R}^3$, consider the two planes $A : (Z = 1)$ and $B : (X = 1)$; a line through 0 meeting A in $(x, y, 1)$ meets B in $(1, y/x, 1/x)$. Consider the map $\varphi \colon A \dashrightarrow B$ defined by $(x, y) \mapsto (y' = y/x, z' = 1/x)$; what is the image under φ of

(i) the line $ax = y + b$; the pencil of parallel lines $ax = y + b$ (fixed a and variable b);

(ii) circles $(x - 1)^2 + y^2 = c$ for variable c (distinguish the 3 cases $c > 1$, $c = 1$ and $c < 1$).

Try to imagine the above as a perspective drawing by an artist sitting at $0 \in \mathbb{R}^3$, on a plane $(X = 1)$, of figures from the plane $(Z = 1)$. Explain what happens to the points of the two planes where φ and φ^{-1} are undefined.

1.8 Let $P_1, \dots, P_4$ be distinct points of $\mathbb{P}^2$ with no 3 collinear. Prove that there is a unique coordinate system in which the 4 points are $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,1)$. Find all conics passing through $P_1, \dots, P_5$, where $P_5 = (a, b, c)$ is some other point, and use this to give another proof of Corollary 1.10 and Proposition 1.11.

1.9 In (1.12) there is a list of possible ways in which two conics can intersect. Write down equations showing that each possibility really occurs. Find all the singular conics in the corresponding pencils. [Hint: you will save yourself a lot of trouble by using symmetry and a well chosen coordinate system.]

Hint for 1.2: it is known from elementary number theory that -1 is a quadratic residue modulo p if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

1.10 (Sylvester's determinant). Let k be an algebraically closed field, and suppose given a quadratic and cubic form in U, V as in (1.8):

$$\begin{aligned} q(U,V) &= a_0U^2 + a_1UV + a_2V^2, \\ c(U,V) &= b_0U^3 + b_1U^2V + b_2UV^2 + b_3V^3. \end{aligned}$$

Prove that q and c have a common zero $(\eta : \tau) \in \mathbb{P}^1$ if and only if

$$\det \begin{vmatrix} a_0 & a_1 & a_2 & & \\ & a_0 & a_1 & a_2 & \\ & & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & \\ & b_0 & b_1 & b_2 & b_3 \end{vmatrix} = 0$$

[Hint: Show that if q and c have a common root then the 5 elements

$$U^2q, \quad UVq, \quad V^2q, \quad Uc \quad \text{and} \quad Vc$$

do not span the 5-dimensional vector space of forms of degree 4, and are therefore linearly dependent. Conversely, use unique factorisation in the polynomial ring $k[U, V]$ to say something about relations of the form $Aq = Bc$ with A and B forms in U, V, $\deg A = 2$, $\deg B = 1$.]

1.11 Generalise the result of Ex. 1.10 to two forms in U, V of any degrees n and m.

Chapter 2

Cubics and the group law

2.1 Examples of parametrised cubics

Some plane cubic curves can be parametrised, just as the conics:

Nodal cubic $C : (y^2 = x^3 + x^2) \subset \mathbb{R}^2$ is the image of the map $\varphi\colon \mathbb{R}^1 \to \mathbb{R}^2$ given by $t \mapsto (t^2 - 1, t^3 - t)$ (check it and see);

Cuspidal cubic $C : (y^2 = x^3) \subset \mathbb{R}^2$ is the image of $\varphi\colon \mathbb{R}^1 \to \mathbb{R}^2$ given by $t \mapsto (t^2, t^3)$:

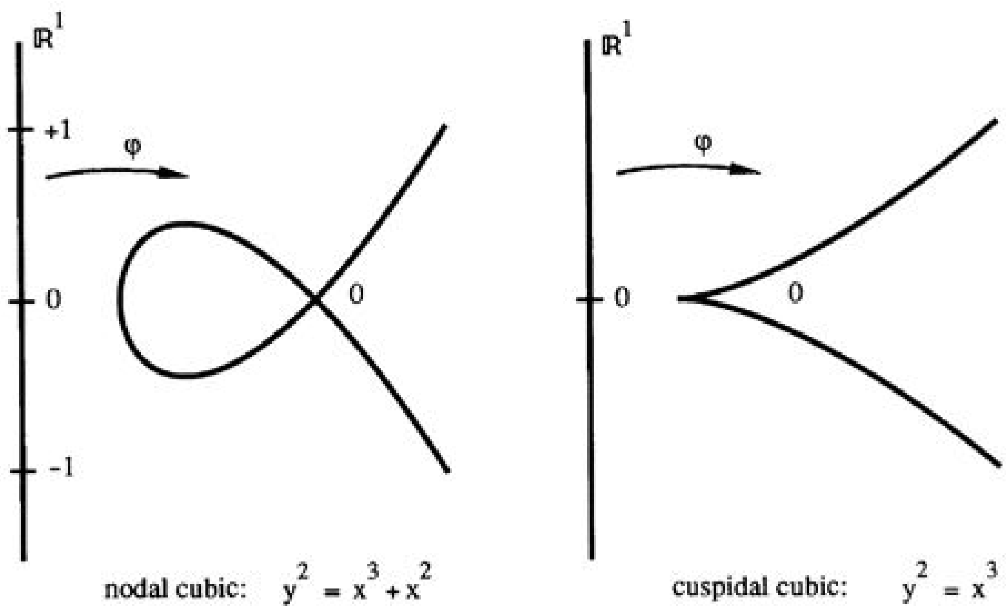

Figure 2.1: Parametrised cubic curves