(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).]

2.8 By writing down the equation of the tangent line to C at A, find a formula for $2A$ in the group law on C, and verify that it is the limit of a suitable formula for $A+B$ as B tends to A. [Hint: use Ex. 2.7, and if necessary refer to (4.14).]

2.9 Let x, z be coordinates on k^2, and let $f \in k[x,z]$; write f as

$$f = a + bx + cz + dx^2 + exz + fz^2 + \cdots.$$

Write down the conditions in terms of $a, b, c, \dots$ that must hold in order that

(i) $P = (0,0) \in C : (f = 0)$;

(ii) the tangent line to C at P is $(z = 0)$;

(iii) P is an inflexion point of C with $(z = 0)$ as the tangent line.

(Recall from (2.12) that $P \in C$ is an inflexion point if the tangent line L is defined, and $f|L$ has at least a 3-fold zero at P.)

2.10 Let $C \subset \mathbb{P}^2_k$ be a plane cubic, and suppose that $P \in C$ is an inflexion point; prove that a change of coordinates in $\mathbb{P}^2_k$ can be used to bring C into the normal form

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

[Hint: take coordinates such that $P = (0,1,0)$ and the inflexion tangent is $(Z = 0)$; then using the previous question, in local coordinates (x,z), Y will appear in a quadratic term Y^2Z, and otherwise only linearly. Show then that you can get rid of the linear term in Y by completing the square.]

2.11 (Group law on a cuspidal cubic.) Consider the curve

$$C : (z = x^3) \subset k^2;$$

C is the image of the bijective map $\varphi\colon k \to C$ by $t \mapsto (t, t^3)$, so it inherits a group law from the additive group k. Prove that this is the unique group law on C such that $(0,0)$ is the neutral element and

$$P + Q + R = 0 \iff P, Q, R \text{ are collinear}$$

for $P, Q, R \in C$. [Hint: you might find useful the identity

$$\det \begin{vmatrix} 1 & a & a^3 \\ 1 & b & b^3 \\ 1 & c & c^3 \end{vmatrix} = (a-b)(b-c)(c-a)(a+b+c).]$$

In projective terms, C is the curve $(Y^2Z = X^3)$, our old friend with a cusp at the origin and an inflexion point at $(0,1,0)$, and the point of the question is that the usual construction gives a group law on the complement of the singular point.

2.12 (Due to Leonardo Pisano, known as Fibonacci, A.D.1220.) Prove that for $u, v \in \mathbb{Z}$,

$$u^2 + v^2 \text{ and } u^2 - v^2 \text{ both squares} \implies v = 0.$$

Hints (due to Pierre de Fermat, see J.W.S.Cassels, Journal of London Math Soc. **41** (1966), p. 207):

Step 1 Reduce to solving

$$x^2 = u^2 + v^2, \quad y^2 = u^2 - v^2 \tag{$*$}$$

with $x, y, u, v \in \mathbb{Z}$ pairwise coprime.

Step 2 Considerations mod 4 show that x, y, u are odd and v even.

Step 3 The 4 pairs of factors on the l.-h.s. of the factorisations

$$\begin{aligned} (x-u)(x+u) &= v^2 \\ (u-y)(u+y) &= v^2 \\ (x-y)(x+y) &= 2v^2 \\ (2u-x-y)(2u+x+y) &= (x-y)^2 \end{aligned} \tag{$**$}$$

have no common factors other than powers of 2.

Step 4 Replacing y by $-y$ if necessary, we can assume that $4 \nmid x - y$. Now by considering the parity of factors on l.-h.s. of $(**)$, prove that

$$x - u = 2v_1^2, \quad u - y = 2u_1^2, \quad x - y = 2x_1^2$$
$$\text{and} \quad 2u - x - y = 2y_1^2$$

with $u_1, v_1, x_1, y_1 \in \mathbb{Z}$.

Step 5 Show that u_1, v_1, x_1, y_1 is another solution of $(*)$ with $v_1 < v$, and deduce a contradiction by 'infinite descent'.

Compare this argument with the proof of (2.2), which was easier only in that I didn't have to mess about with 2s.

Appendix to Part I: Curves and their genus

2.14 Topology of a nonsingular cubic

It is easy to see that a nonsingular plane cubic $C : (y^2 = x^3 + ax + b) \subset \mathbb{P}^2_{\mathbb{R}}$ has one of the two shapes

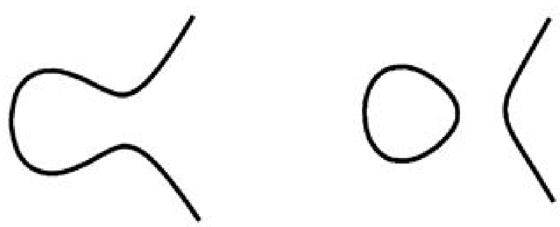

Figure 2.7: Real cubics

That is, topologically, C is either one or two circles (including the single point at infinity, of course). To look at the same question over $\mathbb{C}$, take the alternative normal form

$$C : (y^2 = x(x-1)(x-\lambda)) \cup \{\infty\};$$

what is the topology of $C \subset \mathbb{P}^2_{\mathbb{C}}$? The answer is a torus:

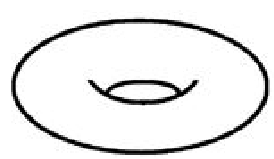

Figure 2.8: Torus

The idea of the proof is to consider the map

$$\pi \colon C \to \mathbb{P}^1_{\mathbb{C}} \text{ by } (X,Y,Z) \mapsto (X,Z) \quad \text{and } \infty \mapsto (1,0);$$