

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Excerpt

[More information](#)

1

First Ideas: Complex Manifolds, Riemann Surfaces, and Projective Curves

This chapter presents some elementary (and not so elementary) ideas in continual use throughout the book. For more details and further information see, for example, Ahlfors [1979], Bliss [1933], Clemens [1980], Farkas and Kra [1992], Hurwitz and Courant [1964], Kirwan [1992], Reyssat [1989], Springer [1981], and/or Weyl [1955]. These are all perfectly accessible to beginners; further references will be given as we go along.

1.1 The Riemann Sphere

Let \mathbb{R}^3 be the 3-dimensional (real) space of points $x = (x_1, x_2, x_3)$ and let $|x| = \sqrt{x_1^2 + x_2^2 + x_3^2}$ be the distance from x to the origin $o = (0, 0, 0)$. \mathcal{M} is the unit sphere $|x| = 1$ and \mathbb{C} is its equatorial plane $x_3 = 0$, identified as the complex numbers via the map $(x_1, x_2, 0) \mapsto x_1 + \sqrt{-1}x_2$. \mathcal{M} is temporarily punctured at the north pole $n = (0, 0, 1)$ and the rest ($x_3 < 1$) is mapped 1:1 onto \mathbb{C} by the projection p depicted in profile in Fig. 1.1. The rule is: Sight from n through the point $x \in \mathcal{M}$, the projection $p(x)$ being the intersection of this line of sight with \mathbb{C} . Obviously, $p(x)$ and $x_1 + \sqrt{-1}x_2$ lie on the same ray of \mathbb{C} ; also the triangles $n, o, p(x)$ and $n, q = (0, 0, x_3), x$ are similar, so

$$|p(x)| = \frac{\text{distance}[o, p(x)]}{\text{distance}[o, n]} = \frac{\text{distance}[q, x]}{\text{distance}[q, n]} = \frac{\sqrt{x_1^2 + x_2^2}}{1 - x_3}.$$

In short,

$$p(x) = \frac{x_1 + \sqrt{-1}x_2}{1 - x_3}.$$

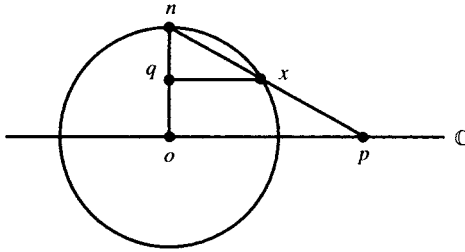


Figure 1.1. The Riemann sphere.

This is the **stereographic projection** of the cartographers. Denote it by p_+ to distinguish it from the analogous projection

$$p_-(x) = \frac{x_1 + \sqrt{-1}x_2}{1 + x_3}$$

of $\mathcal{M} \cap (x_3 > -1)$ produced by sighting from the south pole $(0, 0, -1)$. Now, for $-1 < x_3 < 1$, both maps are available and

$$\begin{aligned} [p_-(x)]^{-1} &= \frac{1 + x_3}{x_1 + \sqrt{-1}x_2} = \frac{1 + x_3}{x_1^2 + x_2^2 (= 1 - x_3^2)} \times (x_1 - \sqrt{-1}x_2) \\ &= \frac{x_1 - \sqrt{-1}x_2}{1 - x_3} = [p_+(x)]^*, \end{aligned}$$

the star being complex conjugation, so the two images are anticonformally related. Replacing $p_-(x)$ by $[p_-(x)]^*$ produces the following situation: \mathcal{M} is covered by two open patches $U_+ = \mathcal{M} \cap (x_3 < 1)$ and $U_- = \mathcal{M} \cap (x_3 > -1)$, each provided with a **local coordinate**: $z_+ = p_+(x)$ for U_+ and $z_- = [p_-(x)]^*$ for U_- . Most points of \mathcal{M} lie in the overlap $U_- \cap U_+$, and for them the two competing coordinates are conformally related: $z_- = 1/z_+$. This object [\mathcal{M} + patches + projections] is the **Riemann sphere**, alias the extended plane $\mathbb{C} + \infty$, the so-called **point at infinity** being identified with the north pole $n = (0, 0, 1)$.

Exercise 1. Prove that p_+ maps spherical circles into plane circles or lines and vice versa. *Hints:* $x \cdot e = \cos \theta$ marks off a spherical circle for any unit vector e and any angle $0 < \theta \leq \pi/2$. Check that $p_+(x) = a + \sqrt{-1}b$ satisfies $(1 - x_3)(ae_1 + be_2) + x_3e_3 = \cos \theta$ and $a^2 + b^2 = (1 - x_3)^{-1}(1 + x_3)$. Then eliminate x_3 .

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic
Henry McKean and Victor Moll

Excerpt

[More information](#)

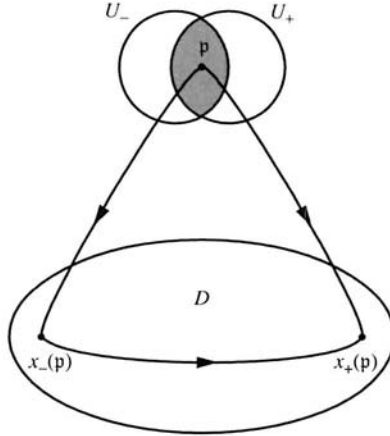
1.2 Complex Manifolds

3

Exercise 2. Prove that the map $p_+ : \mathcal{M} \rightarrow \mathbb{C}$ is conformal, that is, angle preserving, spherical angles being measured in the natural way.

1.2 Complex Manifolds

A **2-dimensional manifold** or **surface** \mathcal{M} is a geometrical figure that looks in the small like an (open) disk. To be precise, this means three things: (1) \mathcal{M} is a topological space covered by a countable number of open **patches** U . (2) The typical patch U is equipped with a **patch map** $p \rightarrow x(p)$ of points $p \in U$ to the open unit disk $D = \{(x_1, x_2) : x_1^2 + x_2^2 < 1\} \subset \mathbb{R}^2$. This map is 1:1, continuous, and onto; it provides U with **local coordinates** $x = x(p)$. (3) An ambiguity arises if the point $p \in \mathcal{M}$ lies in the overlap $U_- \cap U_+$ of two patches so that two competing coordinates $x_-(p)$ and $x_+(p)$ are available; in this case, the composite map $x_-(p) \rightarrow p \rightarrow x_+(p)$, and likewise its inverse, is required to be continuous; see Fig. 1.2.

Figure 1.2. Local coordinates on \mathcal{M} .

Examples. The plane; the (open) half-plane, disk, or annulus; the sphere or the cylinder; the surface of a doughnut (torus) or a pretzel; the Möbius strip.

- \mathcal{M} is **connected** if it comes in one piece, that is, if any two of its points can be joined by a nice curve; this feature is assumed from now on without further comment.

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Excerpt

[More information](#)

4

1 First Ideas

- \mathcal{M} is **simply connected** if it has no punctures, holes, or handles, that is, if every closed curve (**loop**) can be shrunk to a point in \mathcal{M} . This is so for the disk, half-plane, and sphere, but not for the annulus, cylinder, torus, or pretzel.
- \mathcal{M} is **compact** if every cover of it by open sets admits a finite subcover. In this case it is possible to pick a number $0 < r < 1$ so that the images of the closed disk of radius r under a finite number of the patch maps already cover \mathcal{M} . This is so for the sphere, torus, and pretzel, but not for the disk, plane, or cylinder.
- \mathcal{M} is **orientable** if the relation between patch maps preserves the sense of (say, counterclockwise) rotation. This is so for the Riemann sphere of Section 1, but is not possible on a Möbius band.
- \mathcal{M} is **smooth** if competing local coordinates x_- and x_+ on overlaps $U_- \cap U_+$ are smoothly related, that is, if $x_-(\mathbf{p})$ is an infinitely differentiable function of $x_+(\mathbf{p})$ and vice versa. Then you may speak of smooth functions $f: \mathcal{M} \rightarrow \mathbb{R}$, of which you ask that $f(\mathbf{p})$ be a smooth function of the local coordinate $x(\mathbf{p})$ on any patch. Plainly, there can be no competition in this regard: On overlaps, $f(\mathbf{p})$ is a smooth function of both $x_-(\mathbf{p})$ and $x_+(\mathbf{p})$ or of neither.
- \mathcal{M} acquires the more subtle structure of a **complex manifold** or **Riemann surface** if the complex local coordinates or **parameters** $z(\mathbf{p}) = x_1(\mathbf{p}) + \sqrt{-1}x_2(\mathbf{p})$ are conformally related on overlaps; orientability is necessary for this. Then it makes sense to speak of the class $\mathbf{K}(\mathcal{M})$ of functions $f: \mathcal{M} \rightarrow \mathbb{C} + \infty$ of **rational character** defined by the requirement that in the vicinity of any point \mathbf{p}_0 , $f(\mathbf{p})$ have an expansion $w^d[c_0 + c_1w + c_2w^2 + \dots]$ ($d > -\infty$, $c_0 \neq 0$) in powers of $w = z(\mathbf{p}) - z(\mathbf{p}_0)$. Naturally the expansion changes if the local parameter is changed, but the number d does not, so it is permissible to speak of a **root** of multiplicity d if $d > 0$ and of a **pole** of multiplicity $-d$ if $d < 0$; d is the **degree** of f at \mathbf{p}_0 .

Exercise 1. $\mathbf{K}(\mathcal{M})$ is a field.

Exercise 2. Check the statement that the degree d is independent of the local parameter.

Now for some easy examples.

Example 1. It is needless to pause over the complex structure of the plane \mathbb{C} except to note that it has a *global parameter* $z(\mathbf{p}) = x_1 + \sqrt{-1}x_2$. This example is too simple, as is the disk, half-plane, or annulus, or any other open part of \mathbb{C} which obtains a complex structure by mere inheritance.

1.2 Complex Manifolds

Example 2. The cylinder is the quotient of \mathbb{C} by its (arithmetic) subgroup \mathbb{Z} , so it, too, obtains a complex structure by inheritance, and likewise the (square) torus, which is the quotient of \mathbb{C} by the lattice $\mathbb{Z} \oplus \sqrt{-1}\mathbb{Z}$; see Fig. 1.3.

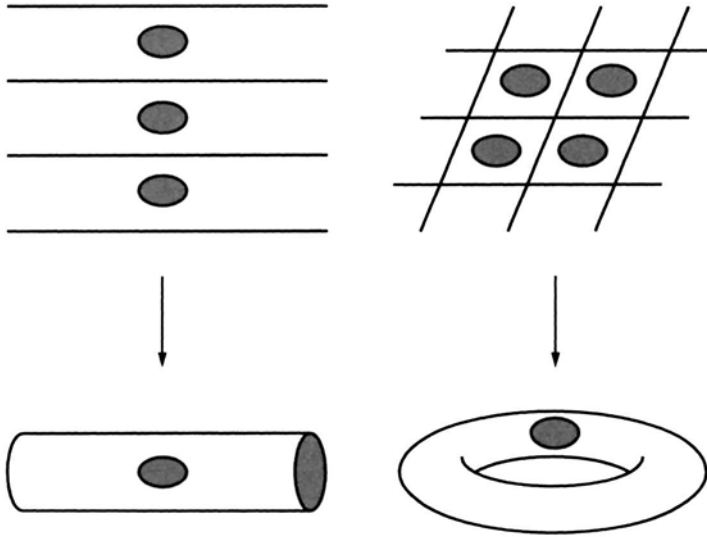


Figure 1.3. Complex structures on the cylinder and the torus.

Example 3. The sphere is more interesting. The stereographic projections of Section 1 provide it with a complex structure after self-evident adjustments; for instance, $z_+(U_+) = \mathbb{C}$ is not the unit disk, but no matter.

Example 4. The **projective line** \mathbb{P}^1 is the family of all complex lines in the 2-dimensional complex space \mathbb{C}^2 : In detail, \mathbb{C}^2 is punctured at the origin and two of its points are identified if they lie on the same (complex) line, that is, (a, b) is identified with (a', b') if $a' = ca$ and $b' = cb$ for some nonvanishing complex number c . \mathbb{P}^1 is covered by two patches $U_+ = \mathbb{C} \times 1$ and $U_- = 1 \times \mathbb{C}$, provided with self-evident local parameters: $z_+(\mathbf{p}) = z$ for $\mathbf{p} = (z, 1) \in U_+$ and $z_-(\mathbf{p}) = z$ for $\mathbf{p} = (1, z) \in U_-$; on the overlap $U_- \cap U_+ = \{(a, b) \in \mathbb{C}^2: ab \neq 0\}$, you have the identifications $(a/b, 1) \equiv (a, b) \equiv (1, b/a)$ and so also the relation of local parameters: $z_+(\mathbf{p}) = [z_-(\mathbf{p})]^{-1}$. This is the *same rule* as for the Riemann sphere of Section 1. In short, the projective line and the Riemann sphere are identical (as complex manifolds).

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Excerpt

[More information](#)

6

1 First Ideas

Exercise 3. \mathbb{P}^1 is compact. That is obvious from its identification with the sphere, but do it from scratch, from the original definition of compactness.

A Little Topology. Let \mathcal{M} be any compact surface, with complex structure or not, and let it be **triangulated** by cutting it up into little (topological) triangles having (in sum) c corners, e edges, and f faces (triangles). Reyssat [1989] has a nice proof that this is always possible. Then (remarkable fact!) the Euler number $\chi = c - e + f$ is always the same: 2 for the sphere, 0 for the torus, -2 for the pretzel, and so forth, that is, it depends only upon the surface and not upon the particular triangulation in hand. This number determines the topology of \mathcal{M} completely. In fact, \mathcal{M} is necessarily a **handlebody**, that is, a (topological) sphere with $g = 1 - (1/2)\chi(\mathcal{M})$ handles attached: 0 for the sphere, 1 for the torus, 2 for the pretzel, and so on; this number is the **genus** of \mathcal{M} . Hurwitz and Courant [1964: 497–534] present an elementary proof; see also Coxeter [1980] for more information and Euler [1752] who started it all. The next items are illustrative.

Example. The spherical triangulation seen in Fig. 1.4 has 6 corners (the black spots), 12 edges, and 8 faces for an Euler number of $6 - 12 + 8 = 2$.

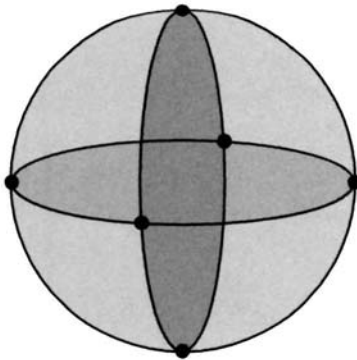


Figure 1.4. Triangulation of the sphere: $c = 6$, $e = 12$, $f = 8$.

Exercise 4. Check by hand that the Euler number and so also the genus of the sphere does not depend upon the triangulation. *Hint:* The sphere can be laid out flat on the plane by cutting all edges that meet at some particular corner. Now count.

Exercise 5. Repeat for higher handlebodies: torus, pretzel, and so on; especially, check that the genus $1 - (1/2)\chi(\mathcal{M})$ really is the handle number.

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic
Henry McKean and Victor Moll

Excerpt

[More information](#)

1.3 Rational Functions

7

Preview. It is a fact that any handlebody can be provided with a complex structure, as was already seen for sphere and torus and will appear for the pretzel in Section 12. This can be done in one and only one way for the sphere, but already the torus admits infinitely many (conformally) distinct complex structures; see Section 2.6. It is this unobvious fact that prompted the adjective *subtle* in first speaking of complex manifolds.

1.3 Rational Functions

The function field $\mathbf{K} = \mathbf{K}(\mathbb{P}^1)$ of the projective line is easy to compute: It is just the field $\mathbb{C}(z)$ of rational functions of $z = p_+(x)$.

Proof. $f \in \mathbf{K}$ is a function of rational character of $z_+ = p_+(x)$ on the patch $x_3 < 1$, and likewise of $z_- = [p_-(x)]^*$ on $x_3 > -1$. It follows that f has, in the first patch, a finite number of poles $p_i (1 \leq i \leq m)$, repeated according to their multiplicity, and the possibility of an extra pole of multiplicity n at $\infty =$ the north pole for a total count of $n + m = d$. View $f(p)$ as a function of $z = p_+(x)$ and let z_1, \dots, z_m be the projections of p_1, \dots, p_m . Then the product $Q(z)$ of $f(p)$ and $P(z) = (z - z_1) \times \dots \times (z - z_m)$ is pole-free in \mathbb{C} and of limited growth at ∞ : $|Q(z)| \leq$ a constant multiple of $|z|^d$ far out. Now use Cauchy's formula for a big circle of radius R :

$$\frac{D^p Q(0)}{p!} = \frac{1}{2\pi\sqrt{-1}} \oint \frac{Q(z)dz}{z^{p+1}}$$

to check that

$$|D^p Q(0)| \leq \text{a constant multiple of } R^d \times R^{-p-1} \times 2\pi R = o(1)$$

for $R \rightarrow \infty$ if $p > d$. The upshot is that Q is a polynomial of degree $\leq d$ and f is a ratio Q/P , as advertised.

Exercise 1. Check the estimate of Q at ∞ .

The **degree** of $f \in \mathbf{K}$ is the total number of its poles, counted according to multiplicity, ∞ included, that is, $\deg f = d = n + m$, and it is plain from its representation as rational function that f has the same number of roots, counted likewise, according to multiplicity. But also $f - c \in \mathbf{K}$ has the same number of poles as f for any complex number c , so f takes on every complex value, ∞ included, d times. In short, d is also the **topological degree** of f as a map of \mathbb{P}^1 to itself, taking $f(p) = \infty$ at poles. This is a general principle for functions

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic
Henry McKean and Victor Moll

Excerpt

[More information](#)

8

1 First Ideas

of rational character on compact Riemann surfaces \mathcal{M} : As maps of \mathcal{M} to \mathbb{P}^1 , they take on every value the same number of times; see Section 16.

Exercise 2. Clarify the statement: $f \in \mathbf{K}(\mathbb{P}^1)$ is an analytic map of \mathbb{P}^1 to itself.

Exercise 3. Check that the roots and poles of $f \in \mathbf{K}(\mathbb{P}^1)$ can be placed any way you like, provided only that they are the same in number. This is not the case for any other compact Riemann surface: It is already false for the torus; see Section 2.7, item 4.

Exercise 4. Let p_1, \dots, p_n be any collection of points on \mathbb{P}^1 , repetition permitted, and let \mathcal{L} be the space of functions $f \in \mathbf{K}(\mathbb{P}^1)$ having these poles or softer; for example, f is permitted a pole at p_1 , of degree no more than the number of its repetitions. \mathcal{L} is a vector space over \mathbb{C} . Prove that its (complex) dimension is $n + 1$.

Besides its functions of rational character, \mathbb{P}^1 also carries **differentials of rational character**. These are the objects ω expressible patchwise as $c(z)dz$ with coefficients c of rational character in the local parameter $z = z(p)$. If the parameter is changed from $z_+ = z$ to $z_- = w$ on the overlap $U_- \cap U_+$, then the coefficient changes in the natural way, from c to $c \times (dz/dw)$. The differential ω has a root or pole of degree d at the point p_0 if its coefficient does so. The residue of ω at p_0 is the integral $(2\pi\sqrt{-1})^{-1} \oint \omega$ taken about a small circle enclosing p_0 . ω is a **differential of the first kind** if it is pole-free, of the **second kind** if it has poles but only vanishing residues, and of the **third kind** otherwise.

Exercise 5. dz is a differential of the second kind on \mathbb{P}^1 : It has 2 poles at ∞ . $df = f'(z)dz$ is likewise of the second kind for any $f \in \mathbf{K}(\mathbb{P}^1)$. $z^{-1}dz$ is different, being of the third kind, in agreement with the fact that the logarithm is not single-valued. Check all that.

Exercise 6. \mathbb{P}^1 has no differentials of the first kind besides $\omega = 0$.

Exercise 7. Check that the total degree (roots – poles) of a differential of rational character on \mathbb{P}^1 is necessarily -2 .

1.4 Luroth's Theorem*

The star means that you may skip this section, but *do* note the following fact which will be useful later: *Any subfield of $\mathbf{K} = \mathbf{K}(\mathbb{P}^1)$ containing more than the constant field \mathbb{C} is isomorphic to \mathbf{K} itself.* This is Luroth's theorem [1876].

1.4 Luroth's Theorem

9

Example. The subfield \mathbf{K}_0 of functions $f \in \mathbf{K}$ invariant under the involution $z \mapsto 1/z$ is the field $\mathbb{C}(w)$ of rational functions of $w = z + 1/z$. The latter is viewed as a map from one projective line (the cover) to a second projective line (the base); it is of degree 2. The field \mathbf{K} of the cover is likewise of degree 2 over the field \mathbf{K}_0 of the base in view of $z = [w \pm \sqrt{w^2 - 4}]/2$. It is this type of counting that is the key to the present proof. It is not the usual proof in that it mixes standard field theory with nonstandard geometric considerations. It is precisely this type of mixture that we want to emphasize in this book. Van der Waerden [1970] presents the standard proof; see also Hartshorne [1977].

A Little Algebra. Not much is needed. The letter \mathbf{K} denotes a field over the rational numbers \mathbb{Q} . The degree of a big field \mathbf{K} (the **extension**) over a smaller field \mathbf{K}_0 (the **ground field**) is the dimension of \mathbf{K} as a vector space over \mathbf{K}_0 , denoted by $[\mathbf{K} : \mathbf{K}_0] \leq \infty$. If the degree is not infinite, then the powers y^n , $n \geq 0$, of an element $y \in \mathbf{K}$ cannot be independent over \mathbf{K}_0 , so y is a root of some polynomial $P(x) = x^n + c_1x^{n-1} + \cdots + c_n$ with coefficients from \mathbf{K}_0 , and y is **algebraic** over \mathbf{K}_0 . $\mathbf{K}_0[x]$ is the ring of such polynomials. The **field polynomial** of y over \mathbf{K}_0 is the irreducible polynomial $P(x) = x^d + c_1x^{d-1} + \cdots$ of class $\mathbf{K}_0[x]$ that it satisfies. The extended field $\mathbf{K}_1 = \mathbf{K}_0(y)$ of rational functions of y with coefficients from \mathbf{K}_0 , obtained by adjunction of y to \mathbf{K}_0 , is spanned by the d powers $1, y, \dots, y^{d-1}$; in particular, $[\mathbf{K}_1 : \mathbf{K}_0] = d$. The roots $x_1 = y, x_2, \dots, x_d$ of $P(x) = 0$ are necessarily simple. They are adjoined to the ground field \mathbf{K}_0 to produce the **splitting field** $\mathbf{K}_2 = \mathbf{K}_0(x_1, \dots, x_d)$ of $P(x)$. This is the smallest extension of \mathbf{K}_0 in which $P(x)$ splits into factors of degree 1: $P(x) = (x - x_1) \cdots (x - x_d)$; it can be realized as the quotient field $\mathbf{K}_0[x]$ modulo $P(x)$. The simplicity of the roots implies that the **discriminant** $\Delta = \prod_{i < j} (x_i - x_j)^2$ does not vanish. This quantity, together with any other symmetric polynomial in the roots, belongs to the ground field \mathbf{K}_0 . The only other fact that will be needed is that if the extended field \mathbf{K} is obtained from the ground field by the adjunction of n such algebraic elements y_i ($1 \leq i \leq n$), then there is a single **primitive element** y_0 that does the job at one stroke: $\mathbf{K} = \mathbf{K}_0(y_0)$. Artin [1953], Lang [1984], Pollard [1950], and/or Stillwell [1994] are recommended as refreshers and for more information.

Exercise 1. Prove directly that the discriminant Δ is, itself, a polynomial in the so-called **elementary symmetric functions**

$$\sigma_1 = \sum x_i, \sigma_2 = \sum_{i < j} x_i x_j, \dots, \sigma_d = x_1 \cdots x_d.$$

Exercise 2. Deduce $\Delta \in \mathbf{K}_0$.

Exercise 3. What is the discriminant of the general cubic $x^3 + ax^2 + bx + c$?

Aside. Luroth’s theorem illustrates, in the simplest circumstances, an important theme of complex geometry: The *complex structure* of a compact Riemann surface \mathcal{M} is determined by the *algebraic structure* of its function field $\mathbf{K}(\mathcal{M})$; see Section 15 under **rational curves** for more information and also Section 2.13 for the case of the torus. The characteristic feature of the rational function field $\mathbf{K} = \mathbb{C}(z)$ is that it is of infinite degree over the ground field \mathbb{C} and isomorphic to any proper intermediate field. As to the geometry of \mathbb{P}^1 , if \mathcal{M} is a compact complex manifold and if $\mathbf{K} = \mathbf{K}(\mathcal{M})$ is a copy of $\mathbb{C}(z)$ then $\mathbf{K} = \mathbb{C}(f)$ for some distinguished $f \in \mathbf{K}$. Now view f as a map of \mathcal{M} to \mathbb{P}^1 : It has a degree d just like an ordinary rational function as expounded in Section 3. Besides, it is a fact that \mathbf{K} separates points of \mathcal{M} , so $d = 1$ and f maps \mathcal{M} 1:1 onto \mathbb{P}^1 . In short, as a complex manifold, \mathcal{M} is \mathbb{P}^1 .

Proof of Luroth’s theorem. The first item of business is to check that if f_0 is any nonconstant rational function, then the *algebraic degree* of $\mathbf{K} = \mathbb{C}(z)$ over $\mathbf{K}_0 = \mathbb{C}(f_0)$ is the same as the *topological degree* d_0 of f_0 . The first degree is finite because $f_0 = a_0/b_0$ with coprime $a_0, b_0 \in \mathbb{C}[z]$ and $P(x) = a_0(x) - f_0 b_0(x) \in \mathbf{K}_0[x]$ has $x = z$ as a root; moreover,

$$\begin{aligned} d = [\mathbf{K} : \mathbf{K}_0] &\leq \deg P = \text{the larger of the degrees of } a_0 \text{ and } b_0 \\ &= \deg f_0 = d_0. \end{aligned}$$

Now let $P_0 = x^d + s_1 x^{d-1} + \dots + s_d \in \mathbf{K}_0[x]$ be the field polynomial of z over \mathbf{K}_0 and observe that for most values c of f_0 three things happen: (1) c is not a pole of any coefficient s_n ($n \leq d$); (2) $f_0(z) = c$ has d_0 simple roots in \mathbb{C} ; (3) $z^d + s_1(c)z^{d-1} + \dots + s_d(c)$ vanishes at each of these. But that makes $d_0 \leq d$ and equality prevails: $d_0 = d$.

Now comes the proof of Luroth’s theorem itself; compare Fig. 1.5. Let the intermediate field \mathbf{K}_1 lie properly above the constant field \mathbb{C} so that $n = [\mathbf{K} : \mathbf{K}_1] \leq \min \{\deg f_0 : f_0 \in \mathbf{K}_1\} < \infty$ and let $P_1(x) = x^n + r_1 x^{n-1} + \dots + r_n \in \mathbf{K}_1[x]$ be the field polynomial of z over \mathbf{K}_1 . Then r_1 (or some other of its coefficients) is not constant, z being of infinite degree over \mathbb{C} . It is to be proved that $\mathbf{K}_1 = \mathbb{C}(r_1)$, producing the whole of that field by its adjunction to \mathbb{C} . Now write $r_1 = a_1/b_1$ with $a_1, b_1 \in \mathbb{C}[z]$, and so on, and clear denominators in $P_1(x)$ to produce $P_2(x) = c_0 x^n + c_1 x^{n-1} + \dots + c_n \in \mathbb{C}[z][x]$. This divides $P_3(x) = a_1(x)b_1(z) - a_1(z)b_1(x) \in \mathbb{C}[z][x]$ and comparison of degrees with