Universitext

Daniel Coray

Notes on Geometry and Arithmetic

Translated by
John Steinig and Constantin Manoil

Springer

Universitext

Universitext

Universitext is a series of textbooks that presents material from a wide variety of mathematical disciplines at master's level and beyond. The books, often well class-tested by their author, may have an informal, personal even experimental approach to their subject matter. Some of the most successful and established books in the series have evolved through several editions, always following the evolution of teaching curricula, into very polished texts.

Thus as research topics trickle down into graduate-level teaching, first textbooks written for new, cutting-edge courses may make their way into *Universitext.*

More information about this series at http://www.springer.com/series/223

Daniel Coray

Notes on Geometry and Arithmetic

Springer

Daniel Coray
L'Enseignement Mathématique
Université de Genève
Genève, Switzerland

Translated by
John Steinig
Genève, Switzerland

Constantin Manoil
Le Grand-Saconnex, Switzerland

ISSN 0172-5939 ISSN 2191-6675 (electronic)
Universitext
ISBN 978-3-030-43780-0 ISBN 978-3-030-43781-7 (eBook)
https://doi.org/10.1007/978-3-030-43781-7

Mathematics Subject Classification: 14AXX, 14Gxx, 14Jxx, 14Mxx, 13F07

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Daniel François Coray was born in Geneva, Switzerland, in 1947. He passed away unexpectedly in 2015.

Professor Coray was a person of great culture but, above all, a mathematician passionate about his research and teaching during his entire career. As an invited researcher and speaker, he worked with and attended the most prestigious universities and institutes of mathematics in Europe, North America, Latin America, and the Russian Federation.

As a young mathematician Professor Coray was inspired by Professor André Haefliger in Geneva and by Professor J.W.S. Cassels in Cambridge, where Daniel Coray obtained his PhD in 1974 at Trinity College. During his professional life he specialized in algebraic number theory, the arithmetic of algebraic varieties, enumerative geometry, theoretical applications of computer methods, and the mathematical modeling of spatial concepts. He produced a substantial number of publications.

This book is the result of a recent series of dynamic lectures that Professor Daniel Coray delivered to his Geneva graduate students, as well as to researchers and teachers working in the same mathematical fields.

In his preface to the manuscript Professor Coray underlines that, in this creative process, he was strongly motivated by his students and that he wanted the book to be a concrete sign of their genuine exchanges.

When Professor Coray passed away in June 2015 in Geneva, only 2 months after he had completed his manuscript, a small group of his colleagues and his wife Lorenza Coray joined forces to translate and publish the manuscript. The publisher Springer Verlag, with which Professor Coray had already held consultations prior to his passing merits sincere gratitude for their professional and fruitful support.

Preface

The study of arithmetical problems using geometrical methods goes back to the Greek mathematicians, starting with Thales and Pythagoras, in the sixth century B.C.E., followed by Eudoxus, Euclid, and Nicomedes in the following centuries, and finally by Diophantus of Alexandria, who lived around 250 C.E. These questions are often referred to as *Diophantine geometry*, even if the subjects gathered under this name differ markedly from one author to another.

Beyond the elementary stage, the methods become very specialized and require a considerable knowledge of algebraic geometry and number theory. The solutions of famous problems such as the Mordell conjecture or Fermat's last theorem lead to numerous additional results, but open questions remain.

We shall make a choice among many possible directions, in an effort to introduce the reader to various themes. We aim to provide readers with a language that would allow them to read specialized papers, even if these are sometimes written from slightly different points of view. For this reason, one will find few hints at the arithmetic of elliptic curves, which constitutes an immense field, but limited and exclusive enough, to which much work has already been devoted.

In fact, this book arose out of several master's degree courses given at the University of Geneva. This means that it addresses students with a good background in algebra (groups, rings, fields, determinants), who wish to acquire solid knowledge in arithmetic or geometry when starting to work for their PhD thesis. It is of course also intended for researchers and teachers, because all chapters enclose original research, some of which has never been published.

The difficulty, when one is based on algebraic geometry, is that one has to start with a long series of preliminaries of commutative algebra, which may discourage more than one student. In this book, this knowledge is reduced to an essential minimum and is most often illustrated by applications to arithmetic.

Also, it must be said that common presentations of algebraic geometry are almost exclusively developed over an algebraically closed field; it is not always easy to guess which results are valid over any field. The classical example is the Nullstellensatz, which so many mathematicians are convinced is valid only over an algebraically closed field. One of the goals of this work is to show that this is not the case, if one

takes the trouble to write the foundations properly; in fact it is an essential theorem over any field, for it seals the unity between algebra, arithmetic, and geometry.

The language chosen is essentially that of classical geometry (i.e., without sheaves or schemes), completed by an indispensable minimum of Galois theory. Actually, the field extensions that occur in arithmetic are seldom Galois. Therefore, the Galois homomorphisms play an important role, but no results on Galois groups are needed.

We work most frequently over a perfect field, since the analysis of the non-perfect case would have forced us toward technical considerations (associated with the definition of *rational k-cycles*) which, in our opinion, would not be suitable in an introductory book. However, in view of the applications in Chapter 10, we have to define the norm in the general case. We also make the effort not to exclude the characteristic 2 case when it does not represent a particular difficulty, as was the case for Brumer's theorem.

For clarity of presentation, we include numerous cross-references between chapters. Probably too many, but they allow one to read the chapters almost independently. In this way, it is possible to teach the content of Chapters 8 and 9 in a one-semester course provided we add, as required, the missing topics to be found in some paragraphs of the first chapters. Exercises are there for the reader to gain familiarity with the subject; most are treated, at least partially, in the solutions to the exercises, which often give additional information.

The list of chapters shows a historical introduction, which devotes a significant amount of space to Diophantus and Fermat (Chapter 1); the foundations of algebraic geometry in language suited to an arithmetic context (Chapter 2); Galois actions with, in particular, norm forms and the arithmetic of finite fields (Chapter 3); and an introduction to projective varieties with some arithmetic applications (conics and quadrics: Chapter 4). The development of the functorial relation between arithmetic, algebra, and geometry is described in the chapter on the Nullstellensatz (Chapter 5).

There follows a digression on Euclidean rings, which can be read independently (Chapter 6), then a chapter on the geometry of cubic surfaces over an arbitrary base field (Chapter 7), which also mentions blow-ups and the Néron–Severi group. In Chapter 8, one finds the definition of p-adic fields and their properties, which are essential for the following chapters; this is why we limit ourselves to $\mathbf{Q}_p$, without attempting to treat the algebraic extensions of that field, although their study does not lack interest. Chapter 9 is devoted to the Hasse principle, with many counter-examples from the literature, but also with a certain number of affirmative results. Here, the presentation requires some knowledge of algebraic number theory, as special emphasis is given to presenting a great number of diverse methods. Of course, the reader will learn from this chapter even without attempting to master its entire content. The last chapter is devoted to Artin's conjecture on the Diophantine dimension of p-adic fields. The reader will find general results on the Diophantine dimension of fields, and then a brief outline, which we hope is nonetheless comprehensible, of the theorems of Ax & Kochen and especially of Arkhipov & Karatsuba.

The influence of my masters will be apparent: André Haefliger, John W. S. Cassels, Peter Swinnerton-Dyer, Oscar Zariski, Jacob Murre and Yuri Manin, as well as that

of several colleagues, in particular Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. I am happy to take this opportunity to thank all my students, who have greatly motivated me to write this book. My thoughts were with them throughout the writing.

Geneva, Switzerland Daniel Coray
April 2015

Contents

Chapter 1
Diophantus of Alexandria

Diophantus is like an island in the history of mathematics. He lived in Alexandria around 250 C.E. Nobody before him had ever tackled a study of arithmetic over the field of rational numbers. It was 1,300 years before Western[1] mathematicians to become interested in this type of problem (Bombelli, Viète, Bachet, Fermat), ... on reading Diophantus to be precise. He also introduced new methods and a special symbol to express an unknown, which makes him an essential precursor of algebraic notation.

1.1 Pythagorean Triangles

Columbia University in New York owns a cuneiform tablet (known as *Plimpton 322*), which dates back to the ancient Babylonian period (between 1900 and 1600 B.C.E.). This clay tablet contains a long list of *Pythagorean triangles*, that is, right-angled triangles whose sides have integer lengths, such as $\langle 3, 4, 5\rangle$, but also $\langle 65, 72, 97\rangle$, $\langle 4961, 6480, 8161\rangle$, etc. (Figures 1.1 and 1.2).

We do not know how these triangles were found, but Diophantus had complete mastery of the problem and was able to produce solutions *ad libitum.* This resolution of the problem is given at the beginning of his work ([Di], Problem II.8), so that throughout he could refer to it as something familiar.

For instance, for Problem 7.13 of the Arabic text (see [Ses]), he first splits 100 as $36 + 64$, which corresponds to the Pythagorean triangle $(6, 8, 10)$, then 64 in $\left(8 \cdot \frac{20}{29}\right)^2 + \left(8 \cdot \frac{21}{29}\right)^2$, only explaining that the reader has already seen (that is, in Problem II.8) "how to split any square number into two squares" (of rational numbers).

[1] But we know that in the tenth century Arab mathematicians (among others abu'l-Wafa and al-Karajī) were already studying and commenting on Diophantus.

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_1

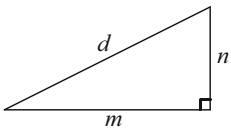


Fig. 1.1 A right-angled triangle

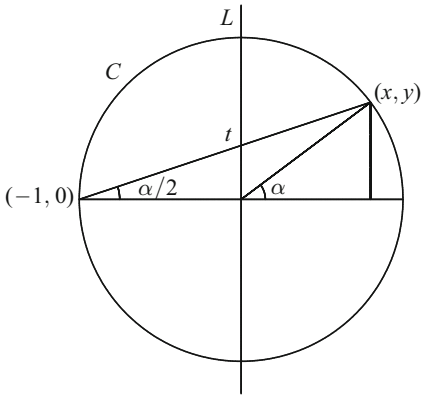


Fig. 1.2 A parametrization of the circle

The method presented in Problem II.8 is similar to the following geometrical construction. One observes that the condition

$$m^2 + n^2 = d^2 \quad (\text{with } m, n, d \in \mathbf{N}) \tag{1.1.1}$$

is a *homogenous* equation, equivalent (if $d \neq 0$) to the affine equation $(m/d)^2 + (n/d)^2 = 1$, i.e.,

$$x^2 + y^2 = 1 \quad (\text{with } x, y \in \mathbf{Q})\,. \tag{1.1.2}$$

This is obviously the equation of the circle C of radius 1 centered at the origin. In this Cartesian reference system, one can parametrize the points $(x, y) \in C$ with rational coordinates by drawing a line through the points $(-1, 0)$ and (x, y) and computing the intersection of this line with the vertical axis L, (Fig. 1.2). If we denote by t the ordinate of this intersection, we have:

$$t = \frac{y}{1+x}\,, \quad \text{and conversely} \quad (x, y) = \Big(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\Big)\,. \tag{1.1.3}$$

These formulas correspond to the classical expression of $x = \cos\alpha$ and $y = \sin\alpha$ as functions of $t = \mathrm{tg}(\alpha/2)$, but primarily they express a bijection between the rational points of the circle minus the point $(-1, 0)$ and those of the vertical line.

On giving rational values to t, one gets all the rational points of the circle, and therefore all the Pythagorean triangles. For instance, $t = \frac{1}{2}$ corresponds to $x = \frac{3}{5}$ and hence to the solution $(3, 4, 5)$ of (1.1.1). The solution $(65, 72, 97)$ corresponds

to $t = \frac{4}{9}$ and the solution $(20, 21, 29)$, which occurs in problem 7.13 of Diophantus, corresponds to $t = \frac{3}{7}$ (and also to $t = \frac{2}{5}$ by symmetry).

Remark 1.1.1. The point $(-1, 0)$ has no correspondence, but one can also view the relation (1.1.3) as a bijection between the rational points of the projective line and those of the projective curve given by $x^2 + y^2 = z^2$:

$$[t : u] \mapsto [x : y : z] = [u^2 - t^2 : 2tu : u^2 + t^2] \tag{1.1.4}$$

$$[x : y : z] \mapsto [t : u] = \begin{cases} [y : z + x] & \text{if } z + x \neq 0 \\ [z - x : y] & \text{if } z - x \neq 0 \end{cases} \tag{1.1.5}$$

Indeed, we have $[y : z + x] = [z - x : y]$ if $z + x \neq 0$ and $z - x \neq 0$.

Comment 1.1.2. This map is just the stereographic projection of the circle on its equator. It may be generalized for every smooth conic having at least one rational point: if S is a point with rational coordinates, any line passing through S meets the conic in one other point P; by elimination, the coordinates of this point are obtained by solving a linear equation with rational coefficients. This establishes, in the projective plane, a bijection $P \mapsto P'$ between the rational points of the conic and those of an arbitrarily fixed line.

We shall see later (Proposition 4.2.7) that this is in fact an isomorphism: on Figure 1.3, the point at infinity on the line corresponds to the intersection with the parallel line (horizontal) passing through S; the tangent at S is associated with S, a well-defined point on the projective line.

In a higher dimension, the same construction yields, for every smooth hypersurface of degree 2 with at least one rational point, a birational map of this quadric onto a hyperplane (see Example 5.5.6).

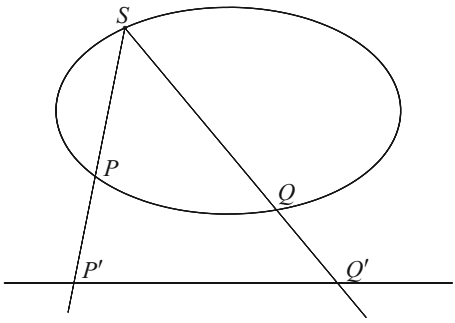


Fig. 1.3 Projection of a conic with a rational point onto a line

1.2 Cubics

Among curves of degree 3, a very simple instance is given by the *strophoid*, whose equation is $y^2 = x^3 + x^2$. The origin is a double point, through which one can draw all the lines $y = tx$, where t is a rational number (Figure 1.4).

On intersecting with the vertical line given by $x = 1$, we get the correspondence

$$t = \frac{y}{x}\,, \quad \text{and conversely} \quad (x, y) = (t^2 - 1, t^3 - t)\,. \tag{1.2.1}$$

This is not quite a bijection, since the two values $t = \pm 1$ have the same image $(x, y) = (0, 0)$.

Another cubic with a long history is related to the following statement, which appears in Diophantus' works, apparently[2] without proof:

Problem 1.2.1. *Every positive difference of two cubes is also a sum of two positive cubes.*

This amounts to studying the equation

$$x^3 + y^3 = a^3 - b^3\,, \tag{1.2.2}$$

where a and b are two given rational positive numbers. Supposing $a > b$, we look for solutions $x, y \in \mathbf{Q}_+^*$.

Viète ([Vi], IV.18–20) had noted that one can solve by setting:

$$x = \frac{3a^3b}{a^3 + b^3} - b\,, \quad y = a - \frac{3ab^3}{a^3 + b^3}\,, \tag{1.2.3}$$

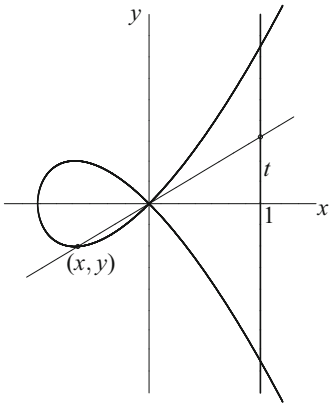


Fig. 1.4 The strophoid $y^2 = x^3 + x^2$

[2] ἔχομεν δὲ ἐν τοῖς Πορίσμασιν ὅτι... (in the resolution of Problem V.16: "*but we have in the Porisms that...*"), but nobody knows if the word "Porisms" refers to statements proved elsewhere, in Diophantus' books that have not survived, or if it is for instance the title of a book.

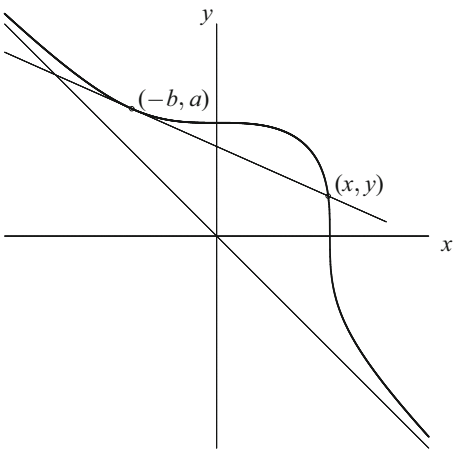


Fig. 1.5 Residual intersection of a cubic with the tangent at one of its points

but Bachet, in his Latin translation of Diophantus, pointed out that this solution is valid only if $a^3 > 2\,b^3$. Otherwise, y is still negative.

It was Fermat [Fe] who indicated the complete solution, which consists in iterating Viète's solution as many times as necessary ("*quod sane miraretur ipse Bachetus*").

Indeed, Equation (1.2.2) corresponds to a plane curve (Figure 1.5) and (1.2.3) amounts to calculating the residual intersection of this curve with the tangent at $(-b, a)$, having equation $b^2x + a^2y = a^3 - b^3$. If the solution (x, y) found is not positive, one can repeat this operation until one ends up in the first quadrant.

Scholion 1.2.2. Fermat even claims that one can continue *ad infinitum*, since one can start with positive solutions and iterate to obtain negative ones, "*quod nec Bachetus nec ipse Vieta expedire potuit*". Now we know, owing to the geometrical interpretation, that Fermat's statement was rather bold. One can repeat *ad infinitum* only if one starts from a point of infinite order in the Mordell–Weil group, and it was by no means obvious that there would be no rational point of finite order, for any difference $a^3 - b^3$. Actually, this is true, but it is a property of $\mathbf{Q}$, not of any field (theorem of Fueter–Billing; see [Cas], Th. V, p. 246).

1.3 Diophantus of Alexandria

Diophantus lived in Alexandria about 250 C.E. The dates are uncertain, but we know that he studied systems of equations, to be solved in **rational** positive numbers.

His works consisted of 13 books, six of which have reached us in Greek, from the Renaissance, and four others were discovered very recently (1972, Rashed [Ra]) in an Arabic translation that goes back to the tenth century.

For example, here are some of the problems he knew how to solve (Roman numerals refer to the numbering of the Greek text, Arabic numerals refer to problems included in the Arabic translation):

$$x^3 + y^3 = z^2 \tag{4.1}$$

$$x^9 + y^4 = z^2 \tag{4.29}$$

$$x^2y^2z^2 + (x^2 + y^2 + z^2) = u^2 \tag{6.18}$$

$$\begin{cases} t^2 = x + y + z \\ t^2 + x = u^2 \\ t^2 + y = v^2 \\ t^2 + z = w^2 \end{cases} \tag{7.13}$$

$$\begin{cases} x^3 + y^2 = u^2 \\ y^2 + z^2 = v^3 \end{cases} \tag{IV.7}$$

$$\begin{cases} (x + y + z)^3 - x = u^3 \\ (x + y + z)^3 - y = v^3 \\ (x + y + z)^3 - z = w^3 \end{cases} \tag{V.16}$$

$$x^4 + y^4 + z^4 = w^2 \tag{V.29}$$

We do not know which *methods* enabled Diophantus to tackle these difficult questions. Maybe they were geometric, as Bashmakova (see [Ba] and [BaSl]) suggests, that is, somewhat like the generation of Pythagorean triangles presented in Paragraph 1.1.

Quite remarkable is the special notation that Diophantus used for a variable (a symbol that might originally have been an abbreviation of the Greek word ἀριθμός, which means "number").

However, the *generality* of his results was often underestimated, because in the absence of a notation with several variables, he frequently uses specific numerical values, implying a wider generality. We shall illustrate Diophantus' approach by analyzing his solution to Problem IV.24. To avoid excessive interruption of the presentation, we put most of the comments in footnotes.

1.4 An Example from Diophantus

IV.24 *To split a given number into two numbers, whose product is a cube minus its root.*

Expressed in more familiar notation, the formulation is the following:

IV.24 *Given a rational positive number a, one looks for rational positive numbers X_1, X_2 such that $X_1 + X_2 = a$ and $X_1 X_2$ is of the form $y^3 - y$.*

Diophantus' Solution. Suppose[3] that $a = 6$ (sic!). We put[4] $X_1 = x$; hence, $X_2 = 6 - x$.

Let us try[5] to put $y = 2x - 1$ (sic!). We have to equate $(2x - 1)^3 - (2x - 1) = 8x^3 + 4x - 12x^2$ with $6x - x^2$. It would be easier[6] if $4 = 6$ (sic!). Now, $4x$ comes from $3 \cdot (2x) - (2x) = 2 \cdot (2x)$. We should have put $y = 3x - 1$ (sic!). Hence, the equation[7]

$$27x^3 - 27x^2 + 6x = 6x - x^2 \implies x^2(27x - 26) = 0 \implies x = \frac{26}{27}.$$

Hence: $X_1 = \frac{26}{27}$ and $X_2 = \frac{136}{27}$. □

We do not claim that this is the only solution!

Geometrical Interpretation. The equation $x\,(a - x) = y^3 - y$ corresponds to a cubic with no singular points. We know the point $(x, y) = (0, -1)$. We then pass a line ℓ having equation $y = mx - 1$ through this point (see Figure 1.6).

If $m = \frac{a}{2}$, the line ℓ is simply the tangent at $(0, -1)$; hence, only one residual intersection P; therefore, the problem is reduced to a linear question and one finds the point P with coordinates $(x, y) = (\frac{3m^2-1}{m^3}, 2 - \frac{1}{m^2})$.

---

[3] This approach led many commentators to say that Diophantus treated only particular cases. However, it is obvious that the method he developed is extremely general. Diophantus did not really claim that his method works without changes for all positive rational numbers, but the problem is formulated for a general enough number, not only for $a = 6$.

[4] A very original contribution of Diophantus is the introduction of a symbol for an unknown x. However, as he lacked a symbol for a second variable, he had to use circumlocutions to name the other unknowns. Here he says: "we put the first number to be x; the second is then $6 - x$".

[5] This method, called "of the false position", has been found in mathematical texts since the highest antiquity. It serves to address the lack of notation for a variable. Here we would write $y = mx - 1$ and would show that it would better to take $m = a/2$, but Diophantus lacked a second letter for the variable m. We do not keep $y = 2x - 1$ at the end of the solution. See the discussion that follows to understand the geometric meaning of this working hypothesis.

[6] We can solve the equation, but this introduces $\sqrt{185}$, which is not a rational number. Diophantus actually says "if the coefficients of x were the same on both sides of the equality. . . ", then he looks for where the 4 in $4x$ comes from.

[7] Diophantus worked very well with polynomials, even if he constantly wrote $(27x^3 + 6x) - (27x^2)$ rather than $27x^3 - 27x^2 + 6x$, which allowed him to always subtract a positive number from another greater positive number.

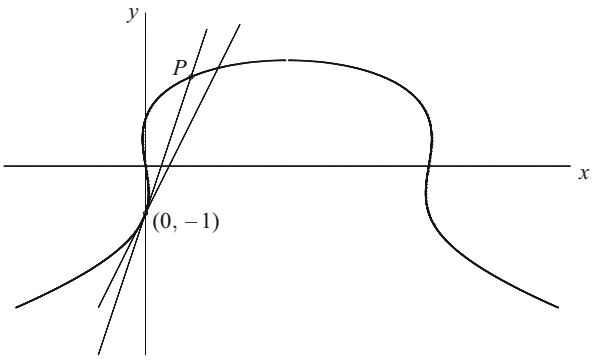


Fig. 1.6 The curve $x\,(a-x) = y^3 - y$ for $a = 6$

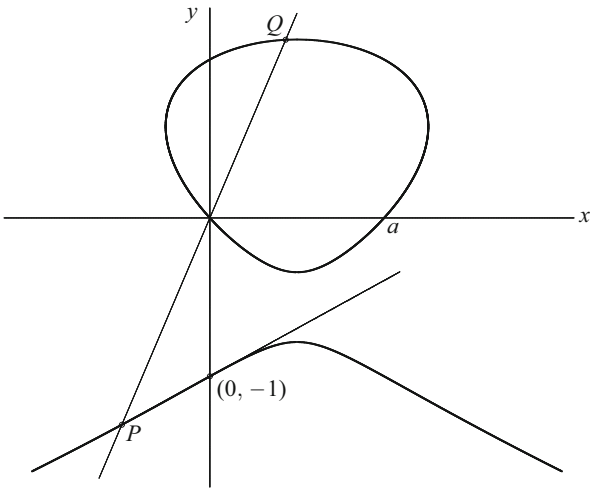


Fig. 1.7 The curve $x\,(a-x) = y^3 - y$ for $a = 11/10$

Solution 1.4.1. The problem is not entirely solved for all that. It happens that the new point does not have positive coordinates. This phenomenon occurs anyway when $m < 1/\sqrt{2}$, since then $y = 2 - \frac{1}{m^2} < 0$. Even more difficult: if $1/\sqrt{2} < m < 1$, we do indeed have $y > 0$, but $x > a$ and so $X_2 < 0$.

We also know that if $m^4 < 4/27$, the cubic has two connected components (proof by the Cardano formula). In this case, the construction with the tangent does not allow one to escape the odd component, as one is easily convinced by looking at Figure 1.7. The point P does indeed have rational coordinates, but $y = 2 - \frac{1}{m^2} < 0$.

Nonetheless, in this case, one can achieve this by drawing not only the tangent at $(0, -1)$ but also the chord passing through P and the origin. The new intersection point Q has rational coordinates and is located on the even component. Depending on the value of a, the point Q is not necessarily located in the first quadrant. It may also be that $x > a$, which does not correspond to a valid solution of the problem as posed by Diophantus, since then $X_2 < 0$. The argument must therefore be completed and the discussion of all the cases would be quite cumbersome.

Exercises

1.1. For which values of a and b can one solve the system

$$X_1^3 + X_2^3 = 2a\,, \quad X_1 + X_2 = 2b$$

in rational numbers?
(*Hint:* Diophantus (IV.1) does not use Viète's formula, but he cleverly puts $X_1 = b+x$ and $X_2 = b - x$, which is much simpler!)

1.2. Use the stereographic projection from the point $(-1, 0)$ to write down all the rational solutions of the equation $x^2 + 3y^2 = 1$.

1.3. Describe all rational solutions of the equation $y^2 = x^3$.

1.4. Consider the curve with equation $x^3 + y^3 = a^3 - b^3$, where $a, b \in \mathbf{Q}_+^*$ and $a > b$. Write the equation of the tangent to this curve at the point $(-b, a)$ and calculate the coordinates (x, y) of the other point of intersection of this tangent with the curve. Show that we have the formulas (1.2.3):

$$x = \frac{3a^3b}{a^3 + b^3} - b \qquad \text{and} \qquad y = a - \frac{3ab^3}{a^3 + b^3}\,.$$

1.5. Use the stereographic projection from the point $S = (-1, 0, 0)$ to describe all the rational points of the quadric Q with equation $x^2+3y^2-3z^2 = 1$. What happens with the solutions in the plane given by $x + 1 = 0$, tangent at S?

Chapter 2
Algebraic Closure; Affine Space

In general, Diophantus' methods do not use any specific property of rational numbers. They are therefore applicable independently of the base field. This is why they can quite easily be interpreted in terms of algebraic geometry, by adding if necessary rudiments of Galois theory. In this chapter, we introduce the algebraic and geometric concepts that seem best adapted to the arithmetic context.

2.1 Algebraic Extensions

Consider the circle $x^2 + y^2 = 1$, intersected by a horizontal line. The intersection points involve various quadratic irrationalities: $y = \frac{1}{2} \implies x = \pm\frac{1}{2}\sqrt{3}$; $y = 2 \implies x = \pm\sqrt{-3}$. There are always algebraic solutions and the intersection is never empty.

More generally, we shall suppose that a commutative field k is given. An *extension* K/k is a commutative field K containing k.

Definition 2.1.1. Given an extension K/k, we say that a number $\alpha \in K$ is *algebraic* over k if there is a non-zero polynomial $f \in k[X]$ such that $f(\alpha) = 0$. (Otherwise we say that α is *transcendental* over k.)

Definition 2.1.2. An extension K/k is an *algebraic extension* if every number $\alpha \in K$ is algebraic over k.

Examples. k/k (where k is any field); $\mathbf{C}/\mathbf{R}$; $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$, where $\sqrt[3]{2} \in \mathbf{R}$ is the real cubic root of 2.

Reminder 2.1.3. If K/k is an arbitrary extension, then K is a k-vector space. We say that the extension is *finite* if the dimension of this vector space is finite; in this case, we denote this dimension, also called the *degree* of the extension, by $[K : k]$

Lemma 2.1.4. *Any finite extension K/k is algebraic.*

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_2

Proof. If $[K : k] = d$, the numbers $1, \alpha, \ldots, \alpha^d$ are linearly dependent over k, for any $\alpha \in K$. On writing a relation of linear dependence, we obtain a non-zero polynomial $f \in k[X]$, which vanishes at α. □

Lemma 2.1.5. *If L/K and K/k are finite extensions, then L/k is also finite, and $[L : k] = [L : K] \cdot [K : k]$.*

Proof. One easily shows that, if $\{u_i\}$ and $\{v_j\}$ are bases, respectively of L/K and of K/k, then $\{u_i v_j\}$ is a basis of L/k. □

Definition 2.1.6. We say that K/k is a *simple* extension if $K = k(\alpha)$, where $k(\alpha)$ is the smallest subfield of K containing k and α.

Lemma 2.1.7. *Let K/k be a simple extension. If $K = k(\alpha)$ with α algebraic over k, then $K \cong k[X]/(f)$, where f is the* minimal polynomial *of α. The class of X by this isomorphism corresponds to α.*

Proof. Let $\psi : k[X] \to K$ be the map giving the value of a polynomial at α: if $g \in k[X]$, then $\psi(g) = g(\alpha)$. It is a ring homomorphism and $\ker \psi \neq (0)$, since α is algebraic. Hence, $\mathfrak{p} = \ker \psi$ is a non-zero prime ideal and, since $k[X]$ is a principal domain, also a maximal ideal. Consequently, $k[X]/\mathfrak{p}$ is a field. There is a commutative diagram

$$\begin{array}{ccc} k[X] & \xrightarrow{\psi} & K \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\varphi} & \\ & k[X]/\mathfrak{p}\,. & \end{array}$$

The homomorphism φ is injective, because $\mathfrak{p} = \ker \psi$. It is also surjective, since the image of $\pi(X)$ by φ is $\psi(X) = X(\alpha) = \alpha$ and $\operatorname{Im}\varphi \supset \psi(k) = k$, which generates $K = k(\alpha)$. Consequently, $K \cong k[X]/(f)$, where f is a generator of the principal ideal $\mathfrak{p}$. □

Comment 2.1.8. Since the polynomial f generates the ideal $\mathfrak{p} = \ker \psi$, it obviously vanishes at α: $f(\alpha) = \psi(f) = 0$. It is often normalized, requiring its dominant coefficient to be 1. In this case, it follows from Euclid's algorithm that it may also be defined as the monic polynomial of smallest degree among non-zero polynomials, which vanish at α. Note the relation: $g(\alpha) = 0 \implies g \in \ker \psi = (f) \implies f \mid g$ ("f *divides* g").

Examples. One may write $\mathbf{Q}(\sqrt[3]{2}) \cong \mathbf{Q}[X]/(X^3 - 2)$; this is also a $\mathbf{Q}$-vector space with basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. A more geometrical example is $\mathbf{C}(t)(\sqrt{t^3 - t + 9}) \cong \mathbf{C}(t)[X]/(X^2 - t^3 + t - 9)$: this is simply the function field of the elliptic curve illustrated in Figure 1.6, if one sets $X = x - 3$ and $t = -y$. This field is important in analysis because of its relationship with the theory of elliptic functions.

Comment 2.1.9. On writing $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ one can view $\mathbf{Q}(\sqrt[3]{2})$ as a subfield of $\mathbf{R}$, whereas the representation $\mathbf{Q}[X]/(X^3 - 2)$ describes this field only up to

isomorphism: if one takes $\alpha = \sqrt[3]{2}\, e^{2\pi i/3}$, one also has $\mathbf{Q}(\alpha) \cong \mathbf{Q}[X]/(X^3 - 2)$, even if $\mathbf{Q}(\sqrt[3]{2})$ and $\mathbf{Q}(\alpha)$ are two distinct subfields of $\mathbf{C}$. This remark underlies Galois theory (see Example 3.1.6 below).

Definition 2.1.10. A *number field* is a finite extension of $\mathbf{Q}$.

Corollary 2.1.11. *Let K/k be a simple extension. If $K = k(\alpha)$, with α algebraic over k, then K/k is a finite extension, of a degree equal to the degree of the minimal polynomial of α.*

Proof. By Lemma 2.1.7, we know that $K \cong k[X]/(f)$, where f is the minimal polynomial of α. It follows that K is generated as a k-vector space by the classes of powers of X, and hence by the classes $1, \alpha, \ldots, \alpha^{d-1}$, where d is the degree of f. Indeed, modulo f one can express the class α^d, and by induction all greater powers of α in terms of $1, \alpha, \ldots, \alpha^{d-1}$. Furthermore, these classes are linearly independent over k. Otherwise, there would be a non-trivial linear combination of $1, \alpha, \ldots, \alpha^{d-1}$ over k, which would vanish and f would not be the minimal polynomial of α. □

Corollary 2.1.12. *If $\alpha, \beta \in K$ are algebraic over k, then $\alpha + \beta$, $\alpha \cdot \beta$ and $1/\alpha$ are also algebraic over k (if $\alpha \neq 0$).*

Proof. Set $L = k(\alpha) \subset K$ and $M = L(\beta) \subset K$; then β is also algebraic over L, and hence $[M : L] < \infty$ (Corollary 2.1.11); likewise, $[L : k] < \infty$, so $[M : k] < \infty$ (Lemma 2.1.5), thus M/k is algebraic (by Lemma 2.1.4). The elements $\alpha + \beta$, $\alpha \cdot \beta$ and $1/\alpha$, which belong to M, are therefore all algebraic over k. □

Corollary 2.1.13. *The set $\overline{\mathbf{Q}} = \{\alpha \in \mathbf{C} \mid \alpha$ algebraic over $\mathbf{Q}\}$ is a field.* □

2.2 Algebraic Closure

Lemma 2.1.7 has a well-known converse:

Lemma 2.2.1. *If $f \in k[X]$ is irreducible of degree $d > 0$, there is an extension K/k of degree d in which f has a root α, and $K = k(\alpha)$.*

Proof. Define $K = k[X]/(f)$; since $k[X]$ is a principal ring and $f = X^d + a_1 X^{d-1} + \cdots + a_d$ is irreducible, we know that the ideal (f) is maximal. Hence, K is a field and the composed homomorphism $k \hookrightarrow k[X] \xrightarrow{\pi} K$ is injective (since k is a field!). Consequently, we are dealing with an extension K/k in which $\alpha = \pi(X)$ verifies $f(\alpha) = f(\pi(X)) = \pi(X)^d + a_1 \pi(X)^{d-1} + \cdots + a_d = \pi(X^d + a_1 X^{d-1} + \cdots + a_d) = \pi(f) = 0$. □

Definition 2.2.2. A field k is *algebraically closed* if it verifies the following equivalent conditions:

(i) k has no proper algebraic extension;
(ii) Every irreducible polynomial of $k[X]$ has degree 1;

(iii) Every non-constant polynomial of $k[X]$ factors completely in linear factors;
(iv) Every non-constant polynomial of $k[X]$ has at least one root in k.

The equivalence of these conditions is easily proved using Lemmas 2.1.7 and 2.2.1.

Definition 2.2.3. If $k \subset K$, we say that K is an *algebraic closure* of k if (i) K/k is an algebraic extension and (ii) K is algebraically closed.

Example. $\mathbf{Q} \subset \mathbf{C}$ does not fulfill condition (i), since $\mathbf{C}$ contains transcendental elements. But $\mathbf{Q} \subset \overline{\mathbf{Q}}$ satisfies both conditions (use Exercise 2.1).

Lemma 2.2.4. *If K and $\bar{k}$ are two algebraic closures of k such that $K \subset \bar{k}$, then $K = \bar{k}$.* □

Theorem 2.2.5. *Any field k has an algebraic closure $\bar{k}$, which is unique up to k-isomorphism.*

Proof. By transfinite induction; we first prove the existence.

The family $\mathcal{Z}$ of all algebraic extensions of k is ordered inductively: it is non-empty, since it contains k as an element; and every chain of algebraic extensions of k (every subset totally ordered by inclusion) has an upper bound, namely the union of all the elements of the chain.

By Zorn's Lemma, we deduce the existence of a maximal element in $\mathcal{Z}$, which is therefore an algebraic extension of k and is also algebraically closed; otherwise, it would contradict its maximality (by virtue of Exercise 2.1).

The concern about this argument is that *the family $\mathcal{Z}$ under question is not a set* (one can construct with it all the paradoxes of set theory, exactly as for the set of all sets). To get around this difficulty, we observe that the algebraic closure of k must be countable if k is a finite field and must have the same cardinality as k if k is infinite (one counts, for each degree, the set of all polynomials). Consequently, it is enough to introduce a set $\mathcal{B} \supset k$ of cardinality strictly greater than $\max(|k|, \aleph_0)$, and then to restrict the search for an algebraic closure inside the box $\mathcal{B}$ by defining $\mathcal{Z}$ as the set of all algebraic extensions of k contained in $\mathcal{B}$. We are then in the set theory context and the above argument is correct.

To prove uniqueness, we proceed in the same way starting with Zorn's Lemma, using Lemma 2.1.7 and ordering the *k-embeddings* (Definition 3.1.1) rather than the extensions. This is Corollary 3.1.12, applied to an algebraic closure K of k. We obtain a k-embedding $\sigma : K \hookrightarrow \bar{k}$ and it suffices to notice that $\sigma(K)$ is also algebraically closed; hence, the equality $\sigma(K) = \bar{k}$, by Lemma 2.2.4. □

Notation. In the sequel, we denote as usual by $\bar{k}$ a fixed algebraic closure of k. By abuse of language, one often speaks of *the* algebraic closure of k, even if it is unique only up to isomorphism. In fact, we notice, as specified by Galois theory (Lemma 3.1.9), that the k-isomorphism $\sigma : K \xrightarrow{\approx} \bar{k}$ obtained at the end of the preceding proof is almost never unique.

2.3 Affine Space

Definition 2.3.1. We call *affine space of dimension n (over k)* a topological space $\mathbf{A}_k^n$, whose structure depends on k and which is described as follows:

Its underlying set is $\bar{k}^n$, that is,

$$\mathbf{A}_k^n = \left\{(x_1, \ldots, x_n) \mid x_i \in \bar{k} \text{ for every } i = 1, \ldots, n\right\}.$$

The closed subsets of $\mathbf{A}_k^n$ are the *algebraic subsets*, that is, subsets of the form

$$V(f_1, \ldots, f_r) = \left\{P \in \mathbf{A}_k^n \mid f_i(P) = 0 \text{ for every } i = 1, \ldots, r\right\},$$

where the f_i are polynomials with coefficients in k (finite in number), in other words

$$f_i \in k[X_1, \ldots, X_n] \text{ for every } i = 1, \ldots, r\,.$$

This topology is called the *Zariski topology*.

Comment 2.3.2. One can identify $\mathbf{A}_k^{n-1}$ to the subset of the form $(x_1, \ldots, x_{n-1}, 0)$ in $\mathbf{A}_k^n$. Iterating this reasoning, we see that $\mathbf{A}_k^0$ must be defined as the space $\{(0, \ldots, 0)\}$, which is the topological space consisting of one point.

Definition 2.3.3. A *hypersurface* is any algebraic subset of $\mathbf{A}_k^n$ of the form $V(f)$, where $f \in k[X_1, \ldots, X_n]$ is a non-constant polynomial.

The algebraic subsets are therefore finite intersections of hypersurfaces. Because of the condition on f, $V(1) = \emptyset$ and $V(0) = \mathbf{A}_k^n$ are not considered hypersurfaces. This is obvious for the first case (since $\bar{k}$ is algebraically closed), and is Lemma 2.4.11 for the second.

Examples. Take $k = \mathbf{Q}$. We may consider $V(f)$, where $f = X_1^2 + X_2^2 - 1$ and $n = 2$: these are the points of the circle that have coordinates not only in $\mathbf{Q}$ (Pythagorean triangles!), but also in $\overline{\mathbf{Q}}$. For $f = X_1^2 + X_2^2 - 3$, the set of rational points on the circle of radius $\sqrt{3}$ is empty (3 is not the sum of the squares of two rational numbers), but $V(f) \neq \emptyset$, since there are points with coordinates in $\overline{\mathbf{Q}}$. Also, for $f = X_1^2 + X_2^2$ there is only one real point, but there are two lines consisting of complex points contained in $V(f) = V\big((X_1 - iX_2)(X_1 + iX_2)\big) \subset \mathbf{A}_{\mathbf{R}}^2$ (see also Exercise 2.4).

Remark 2.3.4. Consider the ideal $\mathfrak{a} = (f_1, \ldots, f_r) \subset k[X_1, \ldots, X_n]$. Then,

$$V(f_1, \ldots, f_r) = V(\mathfrak{a}) := \left\{P \in \mathbf{A}_k^n \mid f(P) = 0 \ \forall f \in \mathfrak{a}\right\}.$$

Notice that $\mathfrak{a} \subset \mathfrak{b} \implies V(\mathfrak{a}) \supset V(\mathfrak{b})$.

Since any ideal of $k[X_1, \ldots, X_n]$ is finitely generated (the ring $k[X_1, \ldots, X_n]$ is Nœtherian, by *Hilbert's basis theorem*), finiteness is not a restriction and one can define more simply algebraic subsets as subsets of $\mathbf{A}_k^n$ of the form

$$V(\mathfrak{a}) = \left\{P \in \mathbf{A}_k^n \mid f(P) = 0 \ \forall f \in \mathfrak{a}\right\},$$

where $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ is an arbitrary ideal.

If $1 \in \mathfrak{a}$, we have $V(\mathfrak{a}) = \emptyset$. But if $1 \notin \mathfrak{a}$, the ideal $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{m}$ and $V(\mathfrak{a}) \supset V(\mathfrak{m})$. We shall later prove the *Weak Nullstellensatz* (Theorem 5.2.1), which states that $V(\mathfrak{m}) \neq \emptyset$. (This is a non-trivial result.)

It remains to verify the axioms of a topological space.

Proposition 2.3.5. *The algebraic subsets are the closed sets of a topology on* $\mathbf{A}_k^n$.

Proof. First of all, $\emptyset = V(1)$ and $\mathbf{A}_k^n = V(0)$. Let us show that the union of two closed sets is closed: $V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1\,\mathfrak{a}_2)$, where $\mathfrak{a}_1\,\mathfrak{a}_2$ denotes the ideal generated by all products $f\,g$, where $f \in \mathfrak{a}_1$ and $g \in \mathfrak{a}_2$. This is the set of finite sums $\left\{\sum f_i\, g_i \mid f_i \in \mathfrak{a}_1 \text{ and } g_i \in \mathfrak{a}_2 \text{ for every } i\right\}$.

Indeed, we trivially have $\mathfrak{a}_1 \supset \mathfrak{a}_1\,\mathfrak{a}_2$ ö hence, $V(\mathfrak{a}_1) \subset V(\mathfrak{a}_1\,\mathfrak{a}_2)$. Similarly for $V(\mathfrak{a}_2)$. It is therefore enough to prove that $V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) \supset V(\mathfrak{a}_1\,\mathfrak{a}_2)$. Now, if $P \notin V(\mathfrak{a}_1)$, there exists $f \in \mathfrak{a}_1$ such that $f(P) \neq 0$. And if $P \notin V(\mathfrak{a}_2)$, there exists $g \in \mathfrak{a}_2$ such that $g(P) \neq 0$. Then, $fg(P) \neq 0$ and $fg \in \mathfrak{a}_1\,\mathfrak{a}_2$; hence, $P \notin V(\mathfrak{a}_1\,\mathfrak{a}_2)$.

It remains to show that any intersection of closed sets is closed. Now, obviously $\bigcap_{i\in I} V(\mathfrak{a}_i) = V\left(\sum_{i\in I} \mathfrak{a}_i\right)$, where $\sum_{i\in I} \mathfrak{a}_i$ is the ideal generated by all the $\mathfrak{a}_i$. □

Comment 2.3.6. One may conceptualize the affine space as a *contravariant functor* $\mathbf{A}^n$ from the category of commutative fields having a fixed algebraic closure $\bar{k}$ to the category of topological spaces: with any field k with algebraic closure $\bar{k}$, one associates the affine space $\mathbf{A}_k^n$ (endowed with the Zariski topology described above), and to $K \hookrightarrow L$ one associates the map $id : \mathbf{A}_L^n \to \mathbf{A}_K^n$, which is obviously continuous. This is why we shall always write $\mathbf{A}_k^n$ for this topological space, rather than $\mathbf{A}^n$, a notation that is apparently simpler, but which denotes the *functor* just described.

Definition 2.3.7. Let $Y \subset \mathbf{A}_k^n$ be any subset. The *ideal of* Y is defined as

$$I(Y) = \{\, f \in k[X_1, \ldots, X_n] \mid f(Y) = 0\} \ .$$

Remark 2.3.8. We clearly have: $Y_1 \subset Y_2 \implies I(Y_1) \supset I(Y_2)$; $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$; $V(I(Y)) \supset Y$ and $I(V(\mathfrak{a})) \supset \mathfrak{a}$.

Lemma 2.3.9. *The set* $V(I(Y))$ *is the closure of* Y *(in the Zariski topology).*

Proof. If a closed set $V(\mathfrak{a})$ contains Y, then $\mathfrak{a}(Y) = 0$; hence, $\mathfrak{a} \subset I(Y)$. It follows that $V(\mathfrak{a}) \supset V(I(Y))$, which shows that $V(I(Y))$ is the smallest closed set containing Y. □

The ideal $I(V(\mathfrak{a}))$ also has an interesting characterization, which we see in Theorem 5.3.3.

Remark 2.3.10. Points are not closed in general. For instance, if $P \in \mathbf{A}^1_{\mathbf{R}}$ is the point $P = i$, its closure is $V(I(\{P\})) = \{+i, -i\}$. Indeed, any polynomial with real coefficients that vanishes at i also vanishes at $-i$.

2.4 Irreducible Components

Definition 2.4.1. A topological space $X \neq \emptyset$ is *irreducible* if it is not the union of two proper closed subsets.

Do not confuse this property with connexity: we do not require the two closed sets to be disjoint.

Example 2.4.2. $\mathbf{A}^1_k$ is irreducible: the only proper closed sets are finite, whereas $\bar{k}$ is infinite.

Lemma 2.4.3. $\mathbf{A}^n_k$ *is a* Nœtherian *topological space: any descending chain of closed sets is stationary.*

Proof. If $Y_1 \supset Y_2 \supset \ldots$ is a descending chain of closed sets, the corresponding ideals form an ascending chain $I(Y_1) \subset I(Y_2) \subset \ldots$. Now, the ring $k[X_1, \ldots, X_n]$ is Nœtherian. Therefore, there is an index r such that $I(Y_r) = I(Y_i)$ for all $i > r$. Then, $Y_i = \overline{Y}_i = V(I(Y_i)) = V(I(Y_r))$ for all $i \geq r$. □

The Nœtherian condition is also expressed in another way, because of a well-known result:

Proposition 2.4.4. *Let* $(\Sigma, \leq)$ *be an ordered set. The following statements are equivalent:*

(i) *Any ascending chain* $x_1 \leq x_2 \leq \ldots$ *of elements of* Σ *is stationary;*
(ii) *Any non-empty subset of* Σ *has a maximal element.*

Proof. It suffices to show that (i) $\Rightarrow$ (ii). Let T be a non-empty subset of Σ that has no maximal element. Then, with any $x \in T$, we can associate $\tau(x)$ chosen in the non-empty set of those $y \in T$ such that $y > x$. This defines a map $\tau : T \to T$ (*choice function*). Starting from $x_1 \in T$, we can define successively $x_2 = \tau(x_1)$, $x_3 = \tau(x_2)$, etc. We form in this manner an infinite strictly increasing sequence $x_1 < x_2 < \ldots$, which contradicts (i). □

Comment 2.4.5. This proof is often presented as a (*reduction ad absurdum*, in such a way that one does not see that it actually uses the axiom of choice. However, this is really necessary in order to make an infinity of choices in subsets defined recursively.

Corollary 2.4.6. *Any non-empty family of closed sets of* $\mathbf{A}^n_k$ *has a minimal element.*
Proof. This follows from Lemma 2.4.3 and Proposition 2.4.4. □

Proposition 2.4.7. *Any non-empty algebraic subset of* $\mathbf{A}_k^n$ *can be expressed in a unique way as a finite union of irreducible algebraic subsets* without embedded components: $Y = Y_1 \cup \cdots \cup Y_r$ *with* $Y_i \not\subset Y_j$ *if* $i \neq j$.

Proof. Let Σ be the family of non-empty closed subsets of $\mathbf{A}_k^n$, which *cannot* be expressed as a finite union of irreducible algebraic subsets. If $\Sigma \neq \emptyset$, Corollary 2.4.6 entails that Σ contains a minimal element $Y \neq \emptyset$. This set Y is not irreducible (or else it would trivially be a union of irreducible sets!). We can therefore write $Y = Y_1 \cup Y_2$, where Y_1 and Y_2 are non-empty closed sets strictly smaller than Y. Taking into account the minimality of $Y \in \Sigma$, we know that $Y_1 \notin \Sigma$ and $Y_2 \notin \Sigma$. Given the definition of Σ, this means that Y_1 and Y_2 are finite unions of irreducible sets; consequently, so is $Y = Y_1 \cup Y_2$. This contradicts the fact that $Y \in \Sigma$.

Thus, $\Sigma = \emptyset$ and, if there are embedded components, we can simply eliminate them. This establishes the existence statement. To prove unicity, we must obviously suppose that there are no embedded components, and then normalize the decompositions. So, let $Y_1 \cup \cdots \cup Y_r = Y_1' \cup \cdots \cup Y_s'$ be two decompositions into irreducible sets, where we suppose that, if $i \neq j$, then $Y_i \not\subset Y_j$ and also $Y_i' \not\subset Y_j'$. Under this hypothesis, we write: $Y_1' = \bigcup (Y_1' \cap Y_i)$. Since the Y_i are closed and Y_1' is irreducible, there is an index i such that $Y_1' \subset Y_i$. Renumbering the components, we may take $i = 1$. Therefore, $Y_1' \subset Y_1$. Similarly, we find $Y_1 \subset Y_j'$ for an index j. It follows that $Y_1' \subset Y_j'$; hence, $j = 1$, since there are no embedded components. Thus, $Y_1' = Y_1$.

We start again with Y_2. We show in this way that $Y_2 \subset Y_j'$, with $j \neq 1$ since $Y_1' = Y_1$, etc. We finally find that $r = s$ and the two decompositions are identical. □

Definition 2.4.8. These irreducible subsets Y_i are called the *irreducible components* of $Y = Y_1 \cup \cdots \cup Y_r$.

Examples. $V(X_1^2 + X_2^2)$ is irreducible as an algebraic subset of $\mathbf{A}_{\mathbf{R}}^2$, but reducible in $\mathbf{A}_{\mathbf{C}}^2$, with irreducible components $V(X_1 - i\,X_2)$ and $V(X_1 + i\,X_2)$: two complex lines.

The curve $V(X_1\,(a - X_1) - X_2^3 + X_2) \subset \mathbf{A}_{\mathbf{Q}}^2$ is irreducible for any $a \in \mathbf{Q}$. The fact that for some values of a its set of real points might be disconnected, as shown in Figure 1.7, does not change anything regarding irreducibility.

The curve $\Gamma = V(X_2^2 - X_1^3 + X_1^2) \subset \mathbf{A}_{\mathbf{R}}^2$ shown in Figure 2.1 is also irreducible. Its real locus $\Gamma(\mathbf{R})$ has two connected components, one of them reduced to a point. However, this point is not an irreducible component of the curve.

This situation naturally occurs when, for a surface like $y^2 = x^3 - x^2 + (x - 2)\,z$, we examine the intersections with tangent planes, such as the horizontal plane $z = 0$ at $(0, 0, 0)$. The level curve for $z = 0$ corresponds to Figure 2.1. Figure 2.2 displays some others. This surface also contains lines, such as $x = y = 2$ and $x = -y = 2$. It has many other properties, of which Figure 2.3 shows only a part.[1]

[1] For instance, it has a unique double point P at infinity, with a pair of planes as a tangent cone. In the Bruce & Wall [BW] classification, this is a point of type A_5. The cubic surface carries only

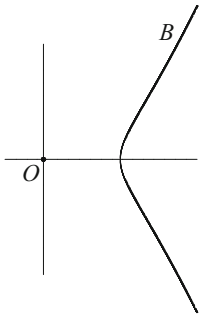


Fig. 2.1 An irreducible curve with two real connected components: $\{O\}$ and B

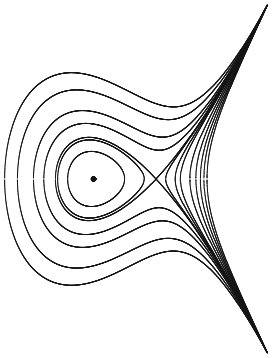


Fig. 2.2 Level curves on the surface $y^2 = x^3 - x^2 + (x-2)\,z$

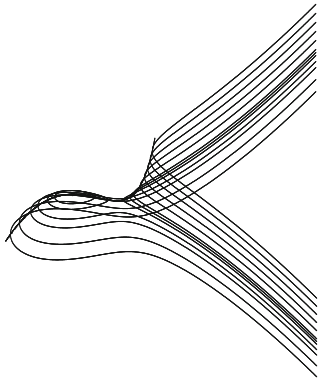


Fig. 2.3 A picture of the surface $y^2 = x^3 - x^2 + (x-2)\,z$

To understand all these examples, we need the following result.

Proposition 2.4.9. *An arbitrary non-empty subset Y of $\mathbf{A}_k^n$ is irreducible if and only if its ideal $I(Y) \subset k[X_1, \ldots, X_n]$ is prime.*

three lines: the two just indicated and a line at infinity. These lines all lie in the plane $\{x = 2\}$ and they meet at P (see Definition 7.2.2).

Reminder 2.4.10. An ideal $\mathfrak{p} \subset A$ in a commutative ring A is called *prime* if (i) $\mathfrak{p} \neq A$ and (ii) for any $f, g \in A$, we have: $fg \in \mathfrak{p} \Longrightarrow f \in \mathfrak{p}$ or $g \in \mathfrak{p}$. (This is the same as saying that $A/\mathfrak{p}$ is an integral ring, i.e., non-zero and without zero divisors.)

A prime ideal also has the property that $\mathfrak{p} \supset \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \supset \mathfrak{a}$ or $\mathfrak{p} \supset \mathfrak{b}$. (Otherwise, there would exist $x \in \mathfrak{a} \setminus \mathfrak{p}$ and $y \in \mathfrak{b} \setminus \mathfrak{p}$, and we would have $xy \in \mathfrak{a}\mathfrak{b} \setminus \mathfrak{p}$.) The relation $\supset$ between ideals may therefore be read as "divides" for integers.

Proof of Proposition 2.4.9. Let $Y \subset \mathbf{A}_k^n$ with $I(Y)$ be not prime. Since $Y \neq \emptyset$, we know that $I(Y) \neq (1)$; hence, condition (ii) is not satisfied. Therefore, there are $f, g \notin I(Y)$ such that $fg \in I(Y)$. Set $Y_1 = Y \cap V(f)$ and $Y_2 = Y \cap V(g)$. Then, $Y_1 \cup Y_2 = Y \cap V(fg) = Y$; and $Y_1 \neq Y$, since $f(Y) \neq 0$, whereas $f(Y_1) = 0$. Similarly, $Y_2 \neq Y$; hence, Y is reducible.

Conversely, if $Y = Y_1 \cup Y_2 = \big(Y \cap V(\mathfrak{a})\big) \cup \big(Y \cap V(\mathfrak{b})\big)$ is a proper decomposition, then $\mathfrak{a} \not\subset I(Y)$; hence, $\exists\, f \in \mathfrak{a} \setminus I(Y)$; likewise, $\exists\, g \in \mathfrak{b} \setminus I(Y)$. Then, $fg \in \mathfrak{a}\mathfrak{b} \subset I(Y)$ and $I(Y)$ is not prime. □

Lemma 2.4.11. $I(\mathbf{A}_k^n) = (0)$.

Proof. We proceed by induction on n, starting with $n = 0$ (see Comment 2.3.2). It suffices to show that, if $f \in k[X_1, \ldots, X_n]$ is a non-zero polynomial, there is a point $P = (\alpha_1, \ldots, \alpha_n) \in \mathbf{A}_k^n$ such that $P \notin V(f)$. Now, we can write $f(X_1, \ldots, X_n) = \sum_j f_j(X_1, \ldots, X_{n-1})\, X_n^j$, where the $f_j \in k[X_1, \ldots, X_{n-1}]$ are polynomials, not all zero. By the induction hypothesis, if $f_j \neq 0$, there are $(\alpha_1, \ldots, \alpha_{n-1})$ such that $f_j(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Since $\bar{k}$ is an infinite field, then there exists $\alpha_n \in \bar{k}$ such that $f(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \neq 0$. □

Corollary 2.4.12. $\mathbf{A}_k^n$ *is irreducible for all* n.

Proof. $I(\mathbf{A}_k^n) = (0)$ is a prime ideal in the integral ring $k[X_1, \ldots, X_n]$. □

Example 2.4.13. Non-trivial irreducible subsets of $\mathbf{A}_k^1$ are in one-to-one correspondence with monic non-constant irreducible polynomials of $k[X]$; hence, with algebraic extensions of k. In this aspect, arithmetic merges with geometry in dimension 1.

Generally speaking, the question of deciding whether a variety is irreducible can be difficult, and obtaining good criteria for irreducibility was a leading concern of algebraic geometers. For hypersurfaces, the following result is an often used corollary of Hilbert's Nullstellensatz (theorem of zeros, which we prove in Chapter 5):

Lemma 2.4.14. *If* $f \in k[X_1, \ldots, X_n]$ *is a non-constant irreducible polynomial, the algebraic subset* $V(f) \subset \mathbf{A}_k^n$ *is non-empty and irreducible.*

Proof. Since the ring $k[X_1, \ldots, X_n]$ is factorial, the ideal (f) is prime. Then, $V(f) \neq \emptyset$ (since $\bar{k}$ is algebraically closed) and $I(V(f)) = (f)$ because of Corollary 5.3.4. The ideal $I(V(f))$ is therefore prime and we apply Proposition 2.4.9. □

This result applies, for instance, to the curve Γ in Figure 2.1: to see that Γ is irreducible, it suffices to show that the polynomial $X_2^2 - X_1^3 + X_1^2$ is irreducible, which is not difficult, because the degrees are rather low.

Corollary 2.4.15. *Let $f \in k[X_1, \ldots, X_n]$ be a non-constant polynomial. The hypersurface $Y = V(f)$ is irreducible if and only if the polynomial f is of the form $f = c \cdot f_1^m$, where $c \in k^*$ and f_1 is an irreducible polynomial.*

Proof. If $f = c \cdot f_1^m$ with f_1 irreducible, then $V(f) = V(f_1)$ and we apply the lemma.

Conversely, since the ring $k[X_1, \ldots, X_n]$ is factorial, $f \neq 0$ factors uniquely as a finite product $f = c \cdot f_1^{m_1} \cdot \ldots \cdot f_r^{m_r}$ of irreducible factors. Then, $Y = V(f) = V(f_1) \cup \ldots \cup V(f_r)$ and, by Lemma 2.4.14, the $V(f_i)$ are irreducible. If we assume that Y is irreducible, it follows from Proposition 2.4.7 that $Y = V(f_1)$ and that the other components are embedded. But we cannot have $V(f_2) \subset V(f_1)$, since this would imply, by Corollary 5.3.4, that $(f_2) = I(V(f_2)) \supset I(V(f_1)) = (f_1)$, whereas we know that f_2 does not divide f_1. □

Exercises

2.1. Show that if L/K and K/k are algebraic extensions, then the extension L/k is algebraic.

2.2. Consider $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2})(\sqrt{3})$. Show that this is a simple extension of $\mathbf{Q}$, by verifying that $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$. Also, find the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$.

2.3. Let K/k be a field extension. Show that K/k is an algebraic extension if and only if every ring A such that $k \subset A \subset K$ is actually a field.

2.4. Let $f(X_1, X_2, X_3) = X_1^2 + X_2^2 + X_3^2 - 1 \in \mathbf{R}[X_1, X_2, X_3]$. Let $S = V(f) \subset \mathbf{A}^3_{\mathbf{R}}$. Find the tangent plane to S at $(0, 0, 1)$ and study its intersection with S in $\mathbf{A}^3_{\mathbf{R}}$.

2.5. Let $\mathfrak{a} \subset \mathbf{Q}[X, Y]$ be the ideal generated by $Y + X^2$ and $X + Y^2$. Is it prime? Study the set of zeros of this ideal. How many irreducible components does $V(\mathfrak{a}) \subset \mathbf{A}^2_{\mathbf{Q}}$ have?

2.6. Show that in $\mathbf{A}^2_{\mathbf{Q}}$

$$V(X^2 - 2,\ Y^2 - 2) = V(X^2 + Y^2 - 4,\ X - Y) \cup V(X^2 + Y^2 - 4,\ X + Y)\,.$$

Deduce that the product of two irreducible sets is not necessarily irreducible.

2.7. Describe the irreducible components of $Y = V(X^2 - YZ,\ XZ - X) \subset \mathbf{A}^3_{\mathbf{C}}$.

2.8. What are $V(I(V(\mathfrak{a})))$ and $I(V(I(Y)))$?

2.9. Let $Y \subset \mathbf{A}_k^n$ be any subset. Show that $I(Y) = I(\overline{Y})$.

2.10. Let X be an irreducible topological space and let $f : X \to Y$ be a continuous map. Show that its image $f(X)$ is irreducible.

2.11. Let X be a Nœtherian topological space. Show that every subspace of X is also Nœtherian and that X is quasi-compact.

2.12. Any non-empty open subset of an irreducible topological space is irreducible and dense.

2.13. If $Y \subset X$ is irreducible (for the induced topology), its closure $\overline{Y}$ is also irreducible.

2.14. Compare the Zariski topology on $\mathbf{A}_k^2$ with the product topology on $\mathbf{A}_k^1 \times \mathbf{A}_k^1$.

2.15. Find the 27 lines on the cubic surface $Y \subset \mathbf{A}_{\mathbf{C}}^3$ with equation $x^3 + y^3 = z^3 + 1$.

Chapter 3
Rational Points; Finite Fields

Finite fields play an essential role in the study of rational solutions of equations. In this chapter we study Galois actions, in order to define correctly the arithmetic notions of *point* and *k-rational variety*, which we illustrate in the case of finite fields in particular. We also prove the Chevalley–Warning Theorem on the *diophantine dimension* of finite fields.

3.1 Galois Homomorphisms

We start with a field k. This is often $\mathbf{Q}$ or another number field (Definition 2.1.10), but sometimes a finite field, the real numbers, a p-adic field (see Chapter 8), or any other field. In each case, we fix an algebraic closure, which we denote by $\bar{k}$.

Definition 3.1.1. If K/k and L/k are two field extensions of k, a *Galois homomorphism*, or *k-embedding*, is any field homomorphism $\sigma : K \to L$ (necessarily injective) such that $\sigma|_k = id$.

Remark 3.1.2. If $\alpha \in K$ is a root of a polynomial $f \in k[X]$, then $\sigma(\alpha)$ is a root of the same polynomial. Indeed, σ fixes coefficients, sums, and products; therefore, $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$.

Example 3.1.3. The most familiar example is perhaps complex conjugation : $K/k = \mathbf{C}/\mathbf{R}$, $\sigma(z) = \bar{z} \in \mathbf{C}$:

$$\begin{array}{ccc} \mathbf{C} & \xrightarrow{\sigma} & \mathbf{C} \\ & \nwarrow \quad \nearrow & \\ & \mathbf{R} & \end{array}$$

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_3

Example 3.1.4. Similarly, for $K/k = \mathbf{Q}(\sqrt{2})/\mathbf{Q}$, one can consider $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2} \in \mathbf{R}$ $(\forall\, a, b \in \mathbf{Q})$:

$$\begin{array}{ccc} \mathbf{Q}(\sqrt{2}) & \xrightarrow{\sigma} & \mathbf{R} \\ & \nwarrow \quad \nearrow & \\ & \mathbf{Q} & \end{array}$$

Application: *the equation* $g = (1 + x_1^2 + x_2^2 + x_3^2 + x_4^2) - \sqrt{2}\,(x_5^2 + x_6^2 + x_7^2) = 0$ *has no solutions in* $K = \mathbf{Q}(\sqrt{2})$.

Indeed, if there were a solution with $x_j \in K$ $(j = 1, \ldots, 7)$, we could write $x_j = a_j + \sqrt{2}\,b_j$ with $a_j,\ b_j \in \mathbf{Q}$. Then, writing $y_j = \sigma(x_j) = a_j - \sqrt{2}\,b_j$, we would also have: $\sigma(g) = (1 + y_1^2 + y_2^2 + y_3^2 + y_4^2) + \sqrt{2}\,(y_5^2 + y_6^2 + y_7^2) = 0$, which is impossible, since in $\mathbf{R}$ all squares are positive.

Definition 3.1.5. Let $\alpha \in \bar{k}$; the set of roots of its minimal polynomial $f \in k[X]$ that lie in $\bar{k}$ are called the *conjugates* of α (with respect to the field k).

The set of conjugates of α is the closure of $P = \{\alpha\}$ in $\mathbf{A}^1_k$. Indeed, $I(P) = (f) \subset k[X]$; hence, $\overline{P} = V(I(P)) = V(f)$ (see also Remark 2.3.10 and Example 2.4.13).

Example 3.1.6. Consider $f(X) = X^3 - 2 \in \mathbf{Q}[X]$, $\sqrt[3]{2} \in \mathbf{R}$, $\rho = e^{2\pi i/3}$ (see Comment 2.1.9):

$$\begin{array}{ccccc} & & \mathbf{C} & & \\ & \swarrow & | & \searrow & \\ \mathbf{Q}(\sqrt[3]{2}) & \cong & \mathbf{Q}(\rho\sqrt[3]{2}) & \cong & \mathbf{Q}(\bar{\rho}\sqrt[3]{2}) \\ & \searrow & | & \swarrow & \\ & & \mathbf{Q} & & \end{array}$$

The three fields in the middle row are distinct, but by Lemma 2.1.7, they are all isomorphic to $\mathbf{Q}[X]/(f)$. It follows from Remark 3.1.2 that they are not isomorphic to any other subfield of $\overline{\mathbf{Q}}$ or $\mathbf{C}$.

Notation 3.1.7. If K/k is an algebraic extension, we denote by $\mathrm{Plong}(K/k)$ the set of k-embeddings of K into $\bar{k}$.

The set $\mathrm{Plong}(K/k)$ is not a group in general, since one cannot compose embeddings whose images are contained in different fields.

Remark 3.1.8. If $K = k(\alpha)$, we know (Remark 3.1.2) that any element $\sigma \in \mathrm{Plong}(K/k)$ sends α onto a root of the minimal polynomial of α, which completely determines σ. Hence, the number of k-embeddings does not exceed the degree of the extension K/k.

If K/k is an arbitrary finite extension, we can describe it as a succession of simple extensions and it is easy[1] to show that in this case we also have $|\mathrm{Plong}(K/k)| \leq [K:k]$.

We make this result more precise in the following lemma, which is fundamental for extending Galois homomorphisms by successive simple extensions.

Lemma 3.1.9 (Key Lemma of Galois Theory). *Let $\sigma : k \to k'$ be a field homomorphism, $f \in k[X]$ an irreducible polynomial, and $f^\sigma \in k'[X]$ its image by σ. Let $K = k(\alpha)$ and $K' = k'(\beta)$, where α is a root of f and β a root of f^σ. There is then a homomorphism $\tau : K \to K'$ such that $\tau|_k = \sigma$ and $\tau(\alpha) = \beta$.*

Proof. Let $k^\sigma = \sigma(k) \subset k'$. The homomorphism $\sigma : k \to k'$ induces a natural isomorphism $\overline{\sigma} : k[X] \to k^\sigma[X]$; hence, an isomorphism $\widetilde{\sigma} : k[X]/(f) \to k^\sigma[X]/(f^\sigma)$. It then suffices to apply 2.1.7: the isomorphism $k[X]/(f) \xrightarrow[\varphi]{\approx} K$ sends the class of X onto α, and the morphism $k^\sigma[X]/(f^\sigma) \xrightarrow[\varphi']{\approx} k^\sigma(\beta) \subset K'$ sends it onto β. The composed morphism $\tau = \varphi' \circ \widetilde{\sigma} \circ \varphi^{-1}$ has the required properties. □

Corollary 3.1.10. *If $K = k(\alpha)$, the k-embeddings of K in $\bar{k}$ are in one-to-one correspondence with the distinct roots of the minimal polynomial of α.*

Proof. We already know (Remark 3.1.2) that, if f is the minimal polynomial of α, any k-embedding sends α onto one of its roots. Lemma 3.1.9 allows us to assert (starting from $\sigma = id : k \to k$) that any other root β of f is the image of α by a k-embedding $\tau : K \to K' \subset \bar{k}$. On the other hand, the condition $\tau(\alpha) = \beta$ determines τ uniquely. □

Corollary 3.1.11. *If two elements α andβ of a field K are such that $K = k(\alpha) = k(\beta)$, the minimal polynomial of α has the same number of distinct roots as the minimal polynomial of β.*

Proof. This follows from Corollary 3.1.10, since the set $\mathrm{Plong}(K/k)$ is an intrinsic object to the extension, independent of the specific generators α and β. □

Corollary 3.1.12. *Let K/k be an algebraic extension. There is a k-embedding $\sigma : K \hookrightarrow \bar{k}$.*

Proof. If K/k is a finite extension, it can be described as a finite succession of simple extensions and it is enough to apply Lemma 3.1.9 recursively. Since we do not assume in this statement that K/k is finite, we shall need Zorn's Lemma. Let $\mathcal{Z}$ be the set of k-embeddings $\tau : L \hookrightarrow \bar{k}$, where $k \subset L \subset K$. This non-empty set is ordered by restriction: τ *precedes* $\tau' : L' \hookrightarrow \bar{k}$ if $L \subset L'$ and $\tau = \tau'|_L$.

[1] In Galois theory, the cardinal number of $|\mathrm{Plong}(K/k)|$ is termed *degree of separability* and denoted by $[K:k]_s$. One also shows that it divides the degree $[K:k]$ (see Proposition 3.2.5), but this result is of little interest for us, since arithmetic often forces us to assume that the base field is perfect, so that all extensions become separable. This is why we mention separability only marginally.

One easily verifies that $\mathcal{Z}$ is ordered inductively; it therefore possesses a maximal element $\sigma : M \hookrightarrow \bar{k}$. Obviously, M is equal to K; otherwise, by Lemma 3.1.9 we could extend σ and σ would not be maximal. □

Corollary 3.1.13. *Let K/k be an algebraic extension. Every k-embedding $\sigma : K \hookrightarrow \bar{k}$ can be extended to (at least) a k-isomorphism $\overline{\sigma} : \bar{k} \to \bar{k}$.*

Proof. In this statement, we suppose as usual that $K \subset \bar{k}$, which is allowed by the preceding corollary, but the given k-embedding $\sigma : K \hookrightarrow \bar{k}$ is arbitrary. We even have in general $\sigma(K) \neq K$ (if the extension is not *Galois*). Let $\mathcal{Z}$ be the set of k-embeddings $\tau : L \hookrightarrow \bar{k}$, where $K \subset L \subset \bar{k}$ and $\tau|_K = \sigma$. This set is also ordered inductively by restriction. Then Zorn's Lemma implies that it has a maximal element $\overline{\sigma} : M \hookrightarrow \bar{k}$. If M were not algebraically closed, we could extend $\overline{\sigma}$, by appealing to Lemma 3.1.9 and $\overline{\sigma}$ would not be maximal. Hence, $M = \bar{k}$, as Lemma 2.2.4 shows. Likewise, since $\overline{\sigma}(\bar{k})$ is algebraically closed, the inclusion $\overline{\sigma}(\bar{k}) \subset \bar{k}$ is an equality and $\overline{\sigma}$ is an isomorphism. □

Notation 3.1.14. As we have seen, the set $\mathrm{Plong}(\bar{k}/k)$ consists of isomorphisms. It is therefore a group, called the *Galois group of $\bar{k}$ over k*, usually denoted by $\mathrm{Gal}(\bar{k}/k)$.

Definition 3.1.15. A field k is called *perfect* if every irreducible polynomial $f \in k[X]$ has $n = \deg f$ distinct roots (in $\bar{k}$).

Another way of saying this is that, over a perfect field, irreducible polynomials have only simple roots (in $\bar{k}$). All fields of characteristic zero are perfect (see Exercise 3.1). The classical example of a *non-perfect* field is the field $k = \mathbf{F}_p(t)$ of rational fractions over the finite field $\mathbf{F}_p$. In this case, $f = X^p - t = (X - t^{1/p})^p$ is irreducible over $k[X]$.

Proposition 3.1.16. *If k is perfect and K/k is a finite extension, the number of k-embeddings of K into $\bar{k}$ equals the degree $[K : k]$.*

Proof. If K/k is a simple extension, this follows from Corollary 3.1.10. The general case is proved in the same way, by composing simple extensions and using Lemma 3.1.9. □

One can further simplify this proof (and others in fact), by using a well-known result:

Lemma 3.1.17 (Theorem of the Primitive Element). *Every finite extension K/k of a perfect field is simple.*

Proof. If k is a finite field, we can write $K = k(\theta)$, where θ is a generator of the multiplicative group of K, which is cyclic (see Reminder 3.4.6). We therefore assume that k is infinite.

By induction it is enough to see that, if K is generated by two elements α and β, there exists $\theta \in K$ such that $K = k(\theta)$. Let $f \in k[X]$ be the minimal polynomial of α and $\{\alpha_i\}_{i=1,\ldots,r}$ the set of its roots in $\bar{k}$. Also, let $g \in k[X]$ be the minimal

polynomial of β and $\{\beta_j\}_{j=1,\dots,s}$ the set of its roots in $\bar{k}$. We set $\beta_1 = \beta$, so that $\beta_j \neq \beta \ \forall\, j > 1$.

Observe that for $j > 1$, the set of x-s, which are solutions of a linear equation of the form $\alpha_i + x\beta_j = \alpha + x\beta$, is finite. Now, since the field is infinite, there is a $c \in k$ not in this set. *We define* $\theta = \alpha + c\,\beta$.

θ obviously belongs to the field K and it suffices to see that we also have $\beta \in k(\theta)$. Since $f(\theta - c\beta) = f(\alpha) = 0$, we set $F(X) = f(\theta - cX)$, a polynomial whose coefficients are in $k(\theta)$. The polynomials F and g both vanish at β; consequently, they have $(X - \beta)$ as a common factor in $\bar{k}[X]$.

In fact, $(X - \beta)$ *is their gcd*, for F and g cannot have another common factor. First, since g has distinct roots in $\bar{k}$, the factor $(X - \beta)$ can only occur with exponent one. Then, $g(X) = \prod_{j=1}^{s}(X - \beta_j)$, but F does not vanish at β_j if $j > 1$, because we have chosen c such that $F(\beta_j) = f(\theta - c\beta_j) \neq 0$, since $\theta - c\beta_j = \alpha + c\beta - c\beta_j$ equals none of the α_i.

Finally, notice that F and g are both polynomials with coefficients in $k(\theta)$ and that we can compute their gcd (which is $X - \beta$) by *Euclid's algorithm* within this field. It follows that $\beta \in k(\theta)$. □

Comment 3.1.18. The proof only uses the fact that β is *k-separable*, which means that its minimal polynomial in $k[X]$ has no multiple roots in $\bar{k}$.

Proposition 3.1.19. *If k is perfect, the set of fixed points of $\bar{k}$ under the action of $\mathcal{G} = \mathrm{Gal}(\bar{k}/k)$ is k:*

$$\bar{k}^{\mathcal{G}} = k\,. \tag{3.1.1}$$

Proof. Let $\alpha \in \bar{k}^{\mathcal{G}}$; if the minimal polynomial of α had degree ≥ 2, it would have at least another root β, since all roots are distinct. By Lemma 3.1.9, there would exist a k-embedding $\sigma : k(\alpha) \hookrightarrow \bar{k}$ sending α onto β. Hence, this k-embedding would not fix α and could be extended to an element of $\mathrm{Gal}(\bar{k}/k)$, by Corollary 3.1.13. □

Comment 3.1.20. In almost all applications, we can reduce our considerations to a finite extension K/k, since varieties are given by a finite number of polynomials, whose coefficients are in a finite extension of k. From a strictly logical point of view, we could then do without Corollary 3.1.13 and Zorn's Lemma, referring instead to Proposition 3.1.16 or to Lemma 3.1.9; but it is rather nice to use (3.1.1).

3.2 Norm Forms

Definition 3.2.1. Let k be a perfect field. If K/k is a finite extension and $\alpha \in K$, the *norm* of α (relatively to K/k) is the element of k defined by

$$N_{K/k}(\alpha) = \prod_{\sigma \in \mathrm{Plong}(K/k)} \sigma(\alpha)\,. \tag{3.2.1}$$

By Proposition 3.1.16, this is a product of $[K : k]$ factors in $\bar{k}$. It is an element of k, by (3.1.1), since $\mathrm{Gal}(\bar{k}/k)$ acts on the set $\mathrm{Plong}(K/k)$ like a permutation group: $\sigma \in \mathrm{Plong}(K/k)$ and $\tau \in \mathrm{Gal}(\bar{k}/k) \implies \tau \circ \sigma \in \mathrm{Plong}(K/k)$; and $\tau \circ \sigma_1 = \tau \circ \sigma_2 \implies \sigma_1 = \sigma_2$.

Notation 3.2.2. One usually writes α^σ for $\sigma(\alpha)$. The set of α^σ is the set of conjugates of α, in the sense of Definition 3.1.5.

In Chapter 10, we shall need the norm for extensions of non-perfect fields. This is one reason for including the following more general definition.

Definition 3.2.3. Let K/k be a finite extension. The *norm* of $\alpha \in K$ (relatively to K/k) is the determinant of the k-vector spaces endomorphism $\ell_\alpha : K \to K$ defined by $\ell_\alpha(\xi) = \alpha\,\xi$ (multiplication by α endomorphism). It is an element of k, which is non-zero if $\alpha \neq 0$, since in this case ℓ_α has $\ell_{\alpha^{-1}}$ as inverse.

This element is also denoted by $N_{K/k}(\alpha)$, as we shall see that, when k is perfect, it coincides with the one defined previously (Proposition 3.2.5 with $m = 1$). We first treat the case when the extension K/k is generated by α:

Lemma 3.2.4. *If $K = k(\alpha)$, we have:* $\det \ell_\alpha = \left(\prod_{\sigma \in \mathrm{Plong}(K/k)} \alpha^\sigma\right)^m$, *where* $m = \frac{[K:k]}{|\mathrm{Plong}(K/k)|}$ *is* the index of inseparability *of K/k.*

Proof. Let $f(X) = X^d - a_1 X^{d-1} - \cdots - a_d \in k[X]$ be the minimal polynomial of α. We know that $f(X) = \prod_{\sigma \in \mathrm{Plong}(K/k)} (X - \alpha^\sigma)^{m_\sigma}$, where m_σ is the multiplicity of each root α^σ. By Lemma 3.1.9, $\mathrm{Gal}(\bar{k}/k)$ acts transitively on the set $\mathrm{Plong}(K/k)$ and on the roots of the polynomial f, which remains fixed, since its coefficients are in k. It follows that the m_σ are all equal. The integer $m = m_\sigma$ is usually called the *index of inseparability* of K/k. One immediately sees that it divides the degree $d = [K : k]$, and even that $d = m \cdot |\mathrm{Plong}(K/k)|$; on considering the derivative of the polynomial f, we also see that in characteristic $p > 0$ the index m is a power of p (see Exercise 3.1).

Thus, the constant term of f is $-a_d = (-1)^d \left(\prod_{\sigma \in \mathrm{Plong}(K/k)} \alpha^\sigma\right)^m$. On the other hand, the endomorphism ℓ_α is represented with respect to the basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$ by the matrix

$$M = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_d \\ 1 & 0 & \ldots & 0 & a_{d-1} \\ 0 & 1 & \ldots & 0 & a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_1 \end{pmatrix},$$

whose determinant is $(-1)^{d-1} a_d$; hence, the desired equality. □

Proposition 3.2.5. *If K/k is a finite extension and $\alpha \in K$, one can write:*

$$N_{K/k}(\alpha) = \det \ell_\alpha = \Big(\prod_{\sigma \in \mathrm{Plong}(K/k)} \alpha^\sigma \Big)^m ,$$

where $m = \frac{[K:k]}{|\mathrm{Plong}(K/k)|}$ is the index of inseparability of K/k.

Proof. Set $L = k(\alpha) \subset K$; let $r = [K : L]$ and let $\{\beta_1, \ldots, \beta_r\}$ be a basis of K/L; we choose the basis of K/k given by

$$\left\{ \beta_1, \beta_1\alpha, \ldots, \beta_1\alpha^{d-1}, \beta_2, \beta_2\alpha, \ldots, \beta_2\alpha^{d-1}, \ldots, \beta_r, \beta_r\alpha, \ldots, \beta_r\alpha^{d-1} \right\} .$$

On this basis, ℓ_α is represented by a diagonal matrix consisting of blocks containing r times the matrix M along the diagonal. Lemma 3.2.4 states that

$$\det \ell_\alpha = (\det \ell_\alpha|_L)^r = \Big(\prod_{\sigma \in \mathrm{Plong}(L/k)} \alpha^\sigma \Big)^{\frac{[L:k]}{|\mathrm{Plong}(L/k)|} \cdot r} .$$

By Lemma 3.1.9, $|\mathrm{Plong}(K/k)| = s \cdot |\mathrm{Plong}(L/k)|$, where $s = |\mathrm{Plong}(K/L)|$. Since $\alpha \in L$, if we sum up over $\mathrm{Plong}(K/k)$ instead of $\mathrm{Plong}(L/k)$, each factor is repeated s times. The exponent in the above formulation is thus

$$m = \frac{[L:k]}{|\mathrm{Plong}(L/k)|} \cdot \frac{r}{s} = \frac{[K:k]}{|\mathrm{Plong}(K/k)|} .$$

□

Let us now show how to obtain a homogenous polynomial of degree d, in d variables, without non-trivial zeros in k^d, starting from an even more general, though very simple definition:

Construction 3.2.6. Let K/k be an algebraic extension of degree d. If $\{\omega_1, \ldots, \omega_d\}$ is a basis for K as a vector space over k, we define a *norm form*

$$F(X_1, \ldots, X_d) = N_{K/k}(\omega_1 X_1 + \cdots + \omega_d X_d) = \det \ell_\varphi ,$$

where ℓ_φ is the endomorphism determined by multiplication by

$$\varphi(X_1, \ldots, X_d) = \omega_1 X_1 + \cdots + \omega_d X_d$$

in $K[X_1, \ldots, X_d]$, which is a free module over $k[X_1, \ldots, X_d]$, with the basis $\{\omega_1, \ldots, \omega_d\}$.

It is clear that $F(X_1, \ldots, X_d)$ is a homogenous polynomial of degree d belonging to $k[X_1, \ldots, X_d]$. If we specialize the X_j by substituting values $a_j \in k$, we obtain the norm in the preceding sense (Definition 3.2.3), that is:

$$F(a_1, \ldots, a_d) = N_{K/k}(\omega_1 a_1 + \cdots + \omega_d a_d) = \det \ell_\alpha ,$$

where $\alpha = \varphi(a_1, \ldots, a_d) \in K$. For $\det \ell_\alpha$ to be zero, α must be 0, which is possible only if all a_j are zero, since the ω_j are linearly independent over k. Hence, the following very important proposition.

Proposition 3.2.7. *If a field k has an algebraic extension K/k of degree d, there is a homogenous polynomial of degree d in d variables, with coefficients in k, without non-trivial zeros in k^d.*

Proof. It is enough to choose a basis for K/k and to take the norm form, as defined above. □

Remark 3.2.8. One may also write:

$$F(X_1, \ldots, X_d) = \prod_{\sigma \in \mathrm{Plong}(K/k)} \sigma(\omega_1 X_1 + \cdots + \omega_d X_d)^m , \tag{3.2.2}$$

where $m = \frac{[K:k]}{|\mathrm{Plong}(K/k)|}$. Indeed, $\{\omega_1, \ldots, \omega_d\}$ is also a basis for the field extension $K(X_1, \ldots, X_d)/k(X_1, \ldots, X_d)$ and we can apply Proposition 3.2.5, in which $\sigma \in \mathrm{Plong}(K/k)$, since the k-embeddings σ act trivially on the X_j.

Since the product is invariant under the action of $\mathrm{Gal}(\bar{k}/k)$, which only interchanges factors, it follows from this expression that, if k is perfect, $F \in k[X_1, \ldots, X_d]$ is a homogenous polynomial of degree d without non-trivial zeros in k^d.

Definition 3.2.9. A *form* of degree d is a homogenous polynomial $F \in k[X_1, \ldots, X_n]$ of degree d (all monomials have the same degree). If this polynomial has a zero in k^n, other than $(0, \ldots, 0)$, we say that the form F *represents zero (non-trivially) in* k.

More generally, we say that F *represents* an element $c \in k$ if there are $a_1, \ldots, a_n \in k$ such that $F(a_1, \ldots, a_n) = c$.

Example 3.2.10. Let $k = \mathbf{F}_7$, the finite field with seven elements. Let α be a cubic root of 2 in $\bar{k}$. (The polynomial $X^3 - 2 \in \mathbf{F}_7[X]$ is irreducible, since it has no roots in $\mathbf{F}_7$. The conjugates of α are $\alpha,\ 2\alpha,\ 4\alpha$.) We then obtain, for the basis $\{1, \alpha, \alpha^2\}$:

$$F(X_1, X_2, X_3) = N_{k(\alpha)/k}(X_1 + \alpha X_2 + \alpha^2 X_3) = X_1^3 + 2X_2^3 + 4X_3^3 + X_1 X_2 X_3$$

(see also Exercise 3.7).

This form does not represent zero (non-trivially) in $\mathbf{F}_7$. We infer that the form

$$F(X_1, X_2, X_3) = X_1^3 + 2X_2^3 + 4X_3^3 + X_1 X_2 X_3$$

does not represent zero in $\mathbf{Q}$. Indeed, since the polynomial is homogenous, we would obtain from a non-trivial solution in $\mathbf{Q}^3$ a *primitive* solution $(a_1, a_2, a_3) \in \mathbf{Z}^3$ (that is, with a_j-s without a common factor, and in particular not all divisible by 7); hence, also a non-trivial solution modulo 7.

We also see that no homogenous polynomial of the form

$$F(X_1, X_2, X_3) = X_1^3 + 2X_2^3 + 4X_3^3 + X_1X_2X_3 + 7\,G(X_1, X_2, X_3)\,,$$

where $G \in \mathbf{Z}[X_1, X_2, X_3]$ is an arbitrary cubic form, represents zero in $\mathbf{Q}$.

Comment 3.2.11. Geometrically, if F is a norm form, Formula (3.2.2) shows that the subset $V(F) \subset \mathbf{A}_k^d$ is a union of hyperplanes (defined over $\bar{k}$). This observation allows one to see that the norm forms are not the only *complete* ($n = d$) forms that do not represent zero in a finite field. For example, if $k = \mathbf{F}_5$, the form $F = X_1^4 + X_2^4 + X_3^4 + X_4^4$ does not represent zero in k (the only fourth powers are 0 and $+1$), but $V(F) \subset \mathbf{A}_k^4$ is *absolutely irreducible* (i.e., irreducible over $\bar{k}$), as the variety $V(F) \subset \mathbf{A}_{\bar{k}}^4$ is a cone over a smooth surface.

3.3 Field of Definition

Let k be a perfect field; we shall denote by $\mathcal{G}$ the Galois group $\mathrm{Gal}(\bar{k}/k)$. This group acts in an obvious manner on the points $P = (\alpha_1, \ldots, \alpha_n) \in \mathbf{A}_k^n$.

Notation 3.3.1. One often writes P^σ for $\sigma(P) = (\alpha_1^\sigma, \ldots, \alpha_n^\sigma)$. This creates some confusion, as we shall continue to think of this action as a left action; thus, $P^{\sigma\tau} = \sigma(P^\tau) = (P^\tau)^\sigma$. But this is a more comprehensible notation that avoids the use of many parentheses.

Definition 3.3.2. Let $P = (\alpha_1, \ldots, \alpha_n) \in \mathbf{A}_k^n$. The *conjugates* of P (over the field k) are the points of the orbit of P under the action of $\mathcal{G}$ on $\mathbf{A}_k^n$.

Proposition 3.3.3. *If K/k designates the finite extension generated by the α_j, the point P has exactly $[K : k]$ distinct conjugates.*

Proof. Set $\mathcal{H} = \mathrm{Gal}(\bar{k}/K)$. This group coincides with the isotropy group $\mathcal{G}_P$ of the point P. Indeed, we obviously have $\mathcal{H} \subset \mathcal{G}_P$ and, if $\sigma(\alpha_j) = \alpha_j \;\; \forall\, j = 1, \ldots, n$, then $\sigma(\alpha) = \alpha \;\; \forall\, \alpha \in K$, since the elements of K can be written as polynomial expressions in the α_j with coefficients in k (see Corollary 2.1.12). Besides, there are natural bijections

$$\mathcal{G}\,.\,P \xleftarrow{\approx} \mathcal{G}/\mathcal{G}_P = \mathcal{G}/\mathcal{H} \xrightarrow{\approx} \mathrm{Plong}(K/k).$$

The first is a classical relation between the orbit of a point and the set of left classes of the corresponding isotropy group. The other is the restriction $\sigma \mapsto \sigma|_K$. Notice that the surjectivity of this last map follows from Corollary 3.1.13. It then follows from Proposition 3.1.16 that $|\mathcal{G}\,.\,P| = [K : k]$. □

Now let $Y \subset \mathbf{A}_{\bar{k}}^n$ be a closed subset (we shall also say a *variety*), defined by $Y = V(\mathfrak{b})$, where $\mathfrak{b}$ is an ideal $\mathfrak{b} \subset \bar{k}[X_1, \ldots, X_n]$. We also have *conjugates*

$\mathfrak{b}^\sigma = \left\{ f^\sigma \in \bar{k}[X_1, \ldots, X_n] \mid f \in \mathfrak{b} \right\}$ and $Y^\sigma = V(\mathfrak{b}^\sigma)$, for all $\sigma \in \mathcal{G}$. Since the σ are isomorphisms, we easily see that $Y^\sigma = \{P^\sigma \mid P \in Y\}$ and that, if $\mathfrak{a} = I(Y)$, then $\mathfrak{a}^\sigma = I(Y^\sigma)$.

We have in fact already met an example with norm forms: $\mathfrak{b} = (g)$ with $g = \omega_1 X_1 + \cdots + \omega_d X_d$. In this case, $Y = V(g)$ was a linear subspace of $\mathbf{A}^d_{\bar{k}}$ and we considered the union of its conjugates $Y^\sigma = V(g^\sigma)$.

Definition 3.3.4. Given a closed subset $Y = V(\mathfrak{b}) \subset \mathbf{A}^n_{\bar{k}}$ and a field $K \subset \bar{k}$, we say that K is a *field of definition* for Y if the ideal $I(Y) \subset \bar{k}[X_1, \ldots, X_n]$ is generated by polynomials with coefficients in K. In this case, Y is also a closed set in the Zariski topology on $\mathbf{A}^n_K$.

Comment 3.3.5. If $k = \mathbf{F}_p(t)$ and $Y \subset \mathbf{A}^1_{\bar{k}}$ is the point $(t^{1/p})$, we have $Y = V(X^p - t) \subset \mathbf{A}^1_{\bar{k}}$. But k is not a field of definition for Y, since the ideal of Y in $\bar{k}[X]$ is $(X - t^{1/p})$. This situation does not occur if k is perfect, as the following proposition shows.

Proposition 3.3.6. *We assume k to be perfect and set $\mathcal{G} = \mathrm{Gal}(\bar{k}/k)$. Let $Y \subset \mathbf{A}^n_{\bar{k}}$ be a closed subset and $\mathfrak{b} \subset \bar{k}[X_1, \ldots, X_n]$ its ideal. The following conditions are equivalent:*

(a) *Y is defined over k (that is, $\mathfrak{b}$ is generated by polynomials with coefficients in k);*
(b) *Y is closed in the Zariski topology on $\mathbf{A}^n_k$;*
(c) *$Y = Y^\sigma$ for all $\sigma \in \mathcal{G}$;*
(d) *$\mathfrak{b} = \mathfrak{b}^\sigma$ for all $\sigma \in \mathcal{G}$.*

Proof. (a) $\Rightarrow$ (b): let $\mathfrak{b} = (f_1, \ldots, f_s) \subset \bar{k}[X_1, \ldots, X_n]$, with polynomials f_i that have coefficients in k. Defining the ideal $\mathfrak{a} = (f_1, \ldots, f_s) \subset k[X_1, \ldots, X_n]$, we have $Y = V(\mathfrak{b}) = V(\mathfrak{a})$.

(b) $\Rightarrow$ (c): if $Y = V(\mathfrak{a})$ with $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ then, for all $\sigma \in \mathcal{G}$, we have $\mathfrak{a}^\sigma = \mathfrak{a}$; hence, $Y^\sigma = V(\mathfrak{a}^\sigma) = V(\mathfrak{a}) = Y$.

(c) $\Rightarrow$ (d): $\mathfrak{b} = I(Y) \Rightarrow \mathfrak{b}^\sigma = I(Y^\sigma) = I(Y) = \mathfrak{b}$.

(d) $\Rightarrow$ (a): since $\bar{k}[X_1, \ldots, X_n]$ is a Nœtherian ring, the ideal $\mathfrak{b} \subset \bar{k}[X_1, \ldots, X_n]$ is generated by a finite number of polynomials $f_1, \ldots, f_s$, whose coefficients belong to a finite extension K/k. Let d be the degree of this extension, which is of the form $K = k(\theta)$, by Lemma 3.1.17. We thus obtain a basis $\{\omega_1, \ldots, \omega_d\}$ of K over k by setting $\omega_j = \theta^{j-1}$. We can write:

$$f_i = \varphi_1^{(i)} \omega_1 + \cdots + \varphi_d^{(i)} \omega_d \qquad (i = 1, \ldots, s)\,,$$

where the $\varphi_j^{(i)}$ are polynomials with coefficients in k. Since $\mathfrak{b} = \mathfrak{b}^\sigma \ \forall \sigma \in \mathcal{G}$, the ideal $\mathfrak{b}$ contains all conjugates $f_i^\sigma = \varphi_1^{(i)} \omega_1^\sigma + \cdots + \varphi_d^{(i)} \omega_d^\sigma$, where σ runs through the distinct k-embeddings of K in $\bar{k}$, which are also d in number, by Proposition 3.1.16. Now the square matrix $\Omega = (\omega_j^\sigma)_{j,\sigma}$, whose coefficients are in $\bar{k}$, is invertible, since it is a Vandermonde matrix. This allows us to express the $\varphi_j^{(i)}$, over $\bar{k}$, as functions of

f_i^σ, which belong to the ideal $\mathfrak{b}$, as we have seen. Consequently, for each index i we have $\varphi_1^{(i)}, \ldots, \varphi_d^{(i)} \in \mathfrak{b}$. It follows that $\mathfrak{b} = (\varphi_1^{(i)}, \ldots, \varphi_d^{(i)})_{1 \le i \le s} \subset \bar{k}[X_1, \ldots, X_n]$. □

Definition 3.3.7. A variety Y, which satisfies the equivalent conditions in Proposition 3.3.6, is also called[2] *k-rational*.

Corollary 3.3.8. *The orbit of a point $P \in \mathbf{A}_k^n$ under the action of $\mathcal{G}$ on $\mathbf{A}_k^n$ is the closure of $Y = \{P\}$ in $\mathbf{A}_k^n$.*

Proof. By (c) $\Rightarrow$ (b), this is a closed set in $\mathbf{A}_k^n$ and by (b) $\Rightarrow$ (c), it is the smallest one containing P. □

Notation 3.3.9. Given a closed subset $Y \subset \mathbf{A}_k^n$, whose ideal is $\mathfrak{a} = I(Y) \subset k[X_1, \ldots, X_n]$, we may assign to it a *functor* in the category of sets, such that to any extension K/k there corresponds the set

$$Y(K) = \left\{ P = (x_1, \ldots, x_n) \in K^n \mid f(P) = 0 \quad \forall f \in \mathfrak{a} \right\} .$$

This is the set of *K-rational points* of Y. To say that this is a functor amounts to saying that $K \subset L \implies Y(K) \subset Y(L)$. If $K \subset \bar{k}$, we also have

$$Y(K) = \left\{ P \in Y \mid P^\sigma = P \quad \forall \sigma \in \mathrm{Gal}(\bar{k}/K) \right\} .$$

Examples. If $Y = V(2X_1^2 + 5X_2^2 + 1) \subset \mathbf{A}_{\mathbf{Q}}^2$, we have: $Y(\mathbf{Q}) \subset Y(\mathbf{R}) = \emptyset$ and $(\sqrt{-3}, 1) \in Y(\mathbf{Q}(\sqrt{-3}))$. One can also show that $Y(\mathbf{Q}(i)) = \emptyset$.

If, moreover, $Y = V(f) \subset \mathbf{A}_{\mathbf{Q}}^2$ with $f = X_1^3 + X_2^3 - 1$, we can assert with Fermat that $Y(\mathbf{Q}) = \{(1, 0)\} \cup \{(0, 1)\}$.

Example 3.3.10. Let $\Gamma \subset \mathbf{A}_k^2$ be a k-rational cubic[3] and $\ell \subset \mathbf{A}_k^2$ a k-rational line, as in Figure 3.1.

The intersection $\Gamma \cap \ell$ consists of three points and is clearly invariant under the action of $\mathcal{G}$. If one of these points, say P, is not k-rational, but defined over an extension K/k of degree 2, then its orbit consists of two points (Proposition 3.3.3). One of the three points is thus the conjugate P^σ, the third one is a point Q, invariant under the action of $\mathcal{G}$, and hence k-rational.

Remark 3.3.11. The curve $\Gamma = V(X_2^2 - X_1^3 + 392) \subset \mathbf{A}_{\mathbf{Q}}^2$, which also appears in the proof of Proposition 9.2.7, has points in different quadratic extensions

[2] We often use the name *k-rational* in this sense. In the literature, a variety birationally equivalent (over k or over $\bar{k}$) to a linear space is also called a *rational variety* (see Definition 5.5.11). The meaning is usually clear from the context; otherwise, it is preferable to use "defined over k" for the first meaning.

[3] A non-singular projective plane curve Γ of degree 3 has *genus* 1 (if it has rational points, it is also called an *elliptic curve*). This is precisely an example of a curve that is not birationally equivalent to a line, and hence not rational in the second sense of the term (see Exercise 5.8).

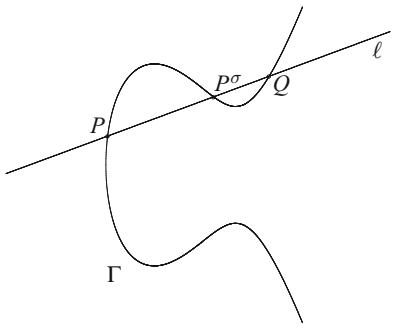


Fig. 3.1 A k-rational cubic cut by a k-rational line

of $\mathbf{Q}$. However, $\Gamma(\mathbf{Q}) = \emptyset$. In fact, it has an unique rational point Q, located at infinity in the plane. The above argument shows that, for this curve, all lines joining two conjugate quadratic points pass through Q (in Figure 3.1, these are vertical lines). This points to the fact that, in order to state a general result, we would be better off in the projective context. We shall see this in Chapter 4.

3.4 Finite Fields

Let us first recall some known facts about finite fields (see also Remark 3.4.15).

Lemma 3.4.1. *Let k be a finite field with q elements. Then, q is of the form p^s, with p prime. Moreover, k contains a subfield isomorphic to $\mathbf{F}_p = \mathbf{Z}/(p)$; hence, $s = [k : \mathbf{F}_p]$.*

Proof. There is a unique ring homomorphism $h : \mathbf{Z} \to k$ that sends $1 \in \mathbf{Z}$ onto $1 \in k$. Its kernel is a non-zero prime ideal $(p) \subset \mathbf{Z}$, since k is integral and finite. We deduce that h factors through an embedding of $\mathbf{Z}/(p)$ into k, which is therefore a vector space of finite dimension s over $\mathbf{F}_p$. □

Thus, k is a finite and hence algebraic extension of the field $\mathbf{F}_p$. As usual, we denote an algebraic closure of $\mathbf{F}_p$ by $\overline{\mathbf{F}}_p$.

Proposition 3.4.2. *Let k be a field with q elements, with $\mathbf{F}_p \subset k \subset \overline{\mathbf{F}}_p$. Then, k is the set of roots in $\overline{\mathbf{F}}_p$ of the polynomial $X^q - X \in \mathbf{F}_p[X]$.*

Proof. Let $S = \left\{\alpha \in \overline{\mathbf{F}}_p \mid \alpha^q - \alpha = 0\right\}$. Since k^* is a group of order $q - 1$, we have: $\alpha^{q-1} = 1 \ \forall \alpha \in k^*$, so $\alpha^q = \alpha \ \forall \alpha \in k$; hence, $k \subset S$. Now, the polynomial $X^q - X$ has at most q roots, since k is commutative.[4] Thus, $|S| \leq q = |k|$; hence, the equality $k = S$. □

[4] As is well known, the polynomial $X^2 + 1$ has an infinity of roots in the field $\mathbf{H}$ of quaternions!

Corollary 3.4.3. *Every finite field is perfect.*

Proof. Let k be a finite field and $f \in k[X]$ an irreducible polynomial. If $\alpha \in \bar{k}$ is a root of f, the field $K = k(\alpha)$ is also finite; set $q = |K|$. By Proposition 3.4.2, K is the set of roots of $X^q - X$; thus, all roots are simple. This polynomial vanishes at α; it is therefore a multiple of f, which consequently can have only simple roots. □

Proposition 3.4.2 entails that $\overline{\mathbf{F}}_p$ contains at most one field with $q = p^s$ elements. The existence is stated in the following theorem:

Theorem 3.4.4. *For every prime p and every integer $s \geq 1$, there is a field $\mathbf{F}_q$ with $q = p^s$ elements. It is unique up to isomorphism, and even unique as a subfield of a fixed algebraic closure $\overline{\mathbf{F}}_p$. Moreover, $\mathbf{F}_q$ has a subfield with p^t elements if and only if t divides s, in which case this subfield is the unique subfield of $\mathbf{F}_q$ having p^t elements.*

Proof. Let $k = \left\{\alpha \in \overline{\mathbf{F}}_p \mid \alpha^q = \alpha\right\}$. This is a field! Indeed, the binomial formula shows that in characteristic p we have $(\alpha + \beta)^p = \alpha^p + \beta^p$, and hence also $(\alpha+\beta)^q = \alpha^q + \beta^q$ (by induction on s). We infer that, if α and β are elements of k, their sum, product, and inverses are also elements of k. Moreover, $|k| = q$, for the polynomial $f(X) = X^q - X$ has q distinct roots in $\overline{\mathbf{F}}_p$, since its derivative is the constant polynomial -1 (see Exercise 3.1).

Unicity follows from the previous proposition. Moreover, s is the degree of $\mathbf{F}_q$ over $\mathbf{F}_p$, and t the degree of $\mathbf{F}_{p^t}$ over $\mathbf{F}_p$. The multiplicative property of degrees (Lemma 2.1.5) implies that t divides s. Conversely, if $\alpha \in \mathbf{F}_{p^t}$ and if $s = tm$, we have: $\alpha^{p^t} = \alpha$, and hence $\alpha \in \mathbf{F}_q$; indeed, $\alpha^q = \alpha^{p^{tm}} = \alpha^{p^t \cdot p^{t(m-1)}} = \alpha^{p^{t(m-1)}} = \cdots = \alpha^{p^t} = \alpha$. □

For $q = p^s$, the lattice of subfields of $\mathbf{F}_q$ is thus isomorphic to the lattice of divisors of s (for every p).

Example 3.4.5. $\mathbf{F}_4 \cong \mathbf{F}_2(\rho)$, where ρ is a root of the irreducible polynomial $X^2 + X + 1$. Warning: $\mathbf{F}_4$ is not isomorphic to $\mathbf{Z}/(4)$, which has zero divisors!

Reminder 3.4.6. $\mathbf{F}_q^*$ is a cyclic group, like any finite subgroup G of the multiplicative group of a commutative field. (This result is not valid for the subgroups of non-commutative fields, as shown by the example of the *Hamiltonian group H* of order 8, generated multiplicatively by i and j in the field $\mathbf{H}$ of quaternions.)

Proof. If G has m elements, then $x^m = 1 \ \forall x \in G$. We can factor m into prime factors: $m = \prod p_i^{s_i} = \prod q_i$. Then, the polynomial $X^{m/p_i} - 1$ has at most $m/p_i < m$ distinct roots; consequently, there exists $a_i \in G$ such that $a_i^{m/p_i} \neq 1$. We define $b_i = a_i^{m/q_i}$, which has order q_i; indeed, $b_i^{q_i/p_i} = a_i^{m/p_i} \neq 1$. Then the product $b = \prod b_i$ has order $\prod q_i = m$, for the q_i are relatively prime. □

Given that $k = \mathbf{F}_q$ and $K = \mathbf{F}_{q^n}$, we can give explicitly all k-embeddings of K into $\bar{k}$. These are the powers of the *Frobenius automorphism*

$$\sigma = \mathrm{Frob}_{\mathbf{F}_q} : K \to K\,, \quad \text{defined by } \xi \mapsto \xi^q\,. \tag{3.4.1}$$

Indeed, with the binomial formula in characteristic p, we see that σ is a field homomorphism, and $\sigma|_k = id$, since $\xi^q = \xi \ \forall \xi \in \mathbf{F}_q$ (Proposition 3.4.2). Moreover, $\sigma(K) \subset K$; hence, $\sigma(K) = K$ since σ is injective and K finite. Thus, this is indeed an automorphism of K and we can study the powers $\sigma^i : \xi \mapsto \xi^{q^i}$.

Proposition 3.4.7. *If k is a finite field with q elements and K/k is the extension of degree n, then* $\mathrm{Plong}(K/k)$ *is a cyclic group* $\mathrm{Gal}(K/k) \cong \mathbf{Z}/(n)$, *generated by the Frobenius automorphism $\sigma : \xi \mapsto \xi^q$.*

Proof. One verifies that $\sigma^i \circ \sigma^j = \sigma^{i+j}$ if $i,\ j \geq 0$ and that $\sigma^n = id$. On the other hand, the σ^i are distinct, for $1 \leq i \leq n$. Indeed, $\sigma^i = \sigma^j$ with $i > j$ would imply that $\sigma^\ell = id\ \ell = i - j$. But, since $1 \leq \ell \leq n - 1$, there exists $\xi \in K$ such that $\sigma^\ell(\xi) = \xi^{q^\ell} \neq \xi$, because the polynomial $X^{q^\ell} - X$ has no more than q^ℓ roots in K.

We have thus found n distinct embeddings. There are no others, for the number of k-embeddings cannot exceed the degree $[K : k] = n$ (see Remark 3.1.8; K/k is a simple extension, by Lemma 3.1.17). Hence, the set $\mathrm{Plong}(K/k)$ coincides with the cyclic group of order n generated by the Frobenius automorphism. In this case, we say that the extension is *Galois* and write $\mathrm{Gal}(K/k)$, rather than $\mathrm{Plong}(K/k)$. □

Lemma 3.4.8. *Let k be a finite field. Then, for every positive integer d, there exists a form of degree d in $n = d$ variables, defined over k, that does not represent zero (non-trivially) in k.*

Proof. By Theorem 3.4.4, k has an extension of degree d. We then apply Proposition 3.2.7. □

In 1935, Emil Artin asked whether in a finite field, any form of degree d in $n > d$ variables possesses a non-trivial zero. In other words, are the finite fields C_1 where, more generally, the C_i property is defined as follows:

Definition 3.4.9. A field k is called *a C_i field* if (for every d) any form of degree d in $n > d^i$ variables, defined over k, has a non-trivial zero in k^n.

Examples. Algebraically closed fields are C_0. The field $\mathbf{R}$ is not C_i, for any i, since the quadratic form $\sum_{j=1}^n X_j^2$ does not represent zero, for any n.

Claude Chevalley solved Artin's conjecture almost instantly, by showing that the finite fields are C_1. In the same volume, Ewald Warning gave a more precise result.

Theorem 3.4.10 (Chevalley–Warning Theorem). *A family of polynomials $F_1, \ldots, F_s \in \mathbf{F}_q[X_1, \ldots, X_n]$ is given, of respective degrees $d_1, \ldots, d_s$, set $d = d_1 + \cdots + d_s$. Let $Y = V(F_1, \ldots, F_s) \subset \mathbf{A}^n_{\mathbf{F}_q}$ and let $N = \left|Y(\mathbf{F}_q)\right|$ be the number of points of Y with coordinates in $\mathbf{F}_q$. Then, $n > d \implies N \equiv 0 \pmod{p}$, where p is the characteristic of $\mathbf{F}_q$.*

Corollary 3.4.11. *If the F_i have no constant term (for instance, if they are forms), the system $F_1 = \cdots = F_s = 0$ admits a non-trivial solution in $\mathbf{F}_q^n$.*

Proof. The trivial solution $(0, \ldots, 0)$ accounts for 1; hence, $N \neq 0$. But, since N is divisible by p, we have $N \geq 2$ and there is at least one other solution. □

Corollary 3.4.12. $\mathbf{F}_q$ *is a* C_1 *field.*

Proof. This is the case $s = 1$ in the preceding corollary. □

Proof of the Theorem *3.1.* We obtain a *characteristic function* for the set $Y(\mathbf{F}_q)$ on putting $G = (1 - F_1^{q-1}) \dots (1 - F_s^{q-1})$. Indeed, for $x \in \mathbf{F}_q^n$, we have: $G(x) = 1$ if $x \in Y(\mathbf{F}_q)$ and $G(x) = 0$ if $x \notin Y(\mathbf{F}_q)$. Then,

$$\sum_{x \in \mathbf{F}_q^n} G(x) = N \,.\, 1 \text{ in } \mathbf{F}_q \,.$$

N is a multiple of the characteristic p of $\mathbf{F}_q$ if and only if this number is zero. Moreover, $\deg G = d(q-1) < n(q-1)$. It then suffices to show:

Lemma 3.4.13. *If* $G \in \mathbf{F}_q[X_1, \dots, X_n]$ *is a polynomial of degree* $\delta < n(q-1)$, *then* $\sum_{x \in \mathbf{F}_q^n} G(x) = 0$.

Proof. If this is true, it is true in particular for monomials; and it suffices to prove the lemma for this case! So, let $G(X) = X_1^{u_1} \dots X_n^{u_n}$, with $\sum u_i \leq \delta < n(q-1)$. There is an i such that $u_i < q - 1$; say, $u_1 < q - 1$. Since

$$\sum_{x \in \mathbf{F}_q^n} G(x) = \sum_{(x_1, \dots, x_n) \in \mathbf{F}_q^n} \Big(\prod_{i=1}^{n} x_i^{u_i}\Big) = \prod_{i=1}^{n} \Big(\sum_{x_i \in \mathbf{F}_q} x_i^{u_i}\Big),$$

it is enough to see that $\sum_{x \in \mathbf{F}_q} x^{u_1} = 0$.

We treat the case $u_1 = 0$ separately. The above expression is simply a manner of writing for $X_1^{u_1} = 1$; hence, $\sum_{x \in \mathbf{F}_q} x^{u_1} = q.1 = 0$. This case being dealt with, we may assume that $0 < u_1 < q - 1$; we choose a generator g of the cyclic group $\mathbf{F}_q^*$. It then remains to add up a geometric series:

$$\sum_{x \in \mathbf{F}_q} x^{u_1} = 0 + \sum_{x \in \mathbf{F}_q^*} x^{u_1} = \sum_{0 \leq v \leq q-2} g^{v u_1} = \frac{1 - g^{(q-1)u_1}}{1 - g^{u_1}} = 0,$$

since $g^{q-1} = 1$ and that $g^{u_1} \neq 1$. This concludes the proof of the lemma and of Theorem 3.4.10. □

Remark 3.4.14. One does not necessarily have $N \equiv 0 \pmod{q}$. However, one can prove (Warning) that $N > 0 \implies N \geq q^{n-d}$ (see [Jo], Chap. 3).

Remark 3.4.15. From this result, one can deduce that every finite field is commutative (Wedderburn's Theorem). Indeed, we can show that, if H is a skew field with **center** R, the vector space H has dimension $n = d^2$ over R. (And there is at least one maximal commutative subfield C, which is an extension of R of degree d; a situation quite similar to that of ordinary quaternions $\mathbf{H} \supset \mathbf{C} \supset \mathbf{R}$). Moreover, there is a form, called the *reduced norm*, of degree d in n variables, that does not

represent zero in R (just like the form $X_1^2 + X_2^2 + X_3^2 + X_4^2$ over $\mathbf{H}$). If $d > 1$, such a form cannot exist if R is a C_1 field, since then $n = d^2 > d$.

Comment 3.4.16. The abelian closure of the field of rational numbers, which can also be described as the extension $\mathbf{Q}^{ab}$ of $\mathbf{Q}$ generated by all roots of unity, is not the center of any skew field of finite dimension, but it is still unknown whether it has the C_1 property, even for very small degrees.

Exercises

3.1. Given a field k, let $f \in k[X]$ be a non-zero polynomial and f' its derivative. Show that the following two statements are equivalent:

(i) The polynomial f has $n = \deg f$ distinct roots (in an algebraic closure $\bar{k}$);
(ii) The gcd of f and f' is 1.

If f is irreducible, show that (ii) is also equivalent to

(iii) $f' \neq 0$.

3.2. Let k be a field of characteristic $p > 0$. Then, k is perfect if and only if $k^p = k$, that is: $\forall\, a \in k,\ \exists\, b \in k$ such that $a = b^p$.

3.3. Use Exercise 3.2, to give another proof that a finite field is perfect.

3.4. Let K/k be an algebraic extension. Show that if k is perfect, then so is K. What can be said about the converse?

3.5. Let $Y = V(f) \subset \mathbf{A}^2_{\mathbf{F}_q}$, where $f = a_1 X_1^2 + a_2 X_2^2 + a_3 \in \mathbf{F}_q[X_1, X_2]$. Show (by counting squares in $\mathbf{F}_q$) that, if $a_1 \neq 0$ and $a_2 \neq 0$, then $Y(\mathbf{F}_q) \neq \emptyset$.

3.6. Find the number of irreducible polynomials of degree n over $\mathbf{F}_p$ in the following cases:

a) $p = 2, n = 6$;
b) $p = 3, n = 2$;
c) $p = 5, n = 4$.

3.7. Let k be a perfect field of characteristic different from 3 and α a root of the polynomial $X^3 - m \in k[X]$, which we assume to be irreducible. Compute $N_{k(\alpha)/k}(X_1 + \alpha X_2 + \alpha^2 X_3)$.

3.8. Describe the $\mathbf{Q}$-embeddings of $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$ in $\overline{\mathbf{Q}}$ (see Exercise 2.2). Is $\mathrm{Plong}(K/\mathbf{Q})$ a group?

3.9. Let p be a prime and $F(i) = \mathbf{F}_{p^{3^i}}$; then, $F(i) \subset F(i+1)$ and we can define $F_\infty = \bigcup_{i=0}^{\infty} F(i) \subset \overline{\mathbf{F}}_p$. Show that F_∞ is a perfect field of characteristic $p > 0$, which is not algebraically closed. What can be said about its cubic extensions?

3.10. Let $K = \mathbf{F}_p(t_1, t_2)$ and $k = \mathbf{F}_p(t_1^p, t_2^p)$, where p is a prime and t_1, t_2 are indeterminates. Show that $[K : k] = p^2$ and that K is not a simple extension of k. Also, find an infinity of fields between k and K.

3.11. Let $k = \mathbf{F}_3(t)$ and $P = (t^{1/3}, t^{2/3}) \in \mathbf{A}_k^2$. Show that P does not belong to any line $\ell \subset \mathbf{A}_k^2$ defined over k.

3.12. Show that the form $F(X_1, X_2, X_3) = X_1^4 - 3X_2^4 + 2X_3^4 - 3X_2^2X_3^2$ does not represent zero trivially in $\mathbf{F}_5$. Also, show that it has a solution $(1, \theta, \theta^2)$ in $\mathbf{F}_5(\theta)$, where $\theta^3 - \theta^2 - 1 = 0$.

3.13. Let k be a C_i field, with $i < 1$. Show that k is C_0.

Chapter 4
Projective Varieties; Conics and Quadrics

The arithmetic study of varieties defined by homogenous polynomials leads to the identification of proportional solutions, which means that we are working in a projective setting. Arithmetic properties of projective varieties are strongly dependent on their geometry. The case of conics serves as a first illustration. Then we shall prove Springer's and Brumer's theorems on algebraic points on quadrics and intersections of quadrics.

4.1 Projective Space

Definition 4.1.1. We call *projective space of dimension n* (over k) the topological space $\mathbf{P}_k^n$, which is described as follows:

$$\mathbf{P}_k^n = \left(\left\{(x_0, \ldots, x_n) \mid x_i \in \bar{k}\right\} \setminus \{(0, \ldots, 0)\}\right)/\sim \; = \left(\mathbf{A}_k^{n+1} \setminus \{0\}\right)/\sim,$$

where the equivalence relation $\sim$ is given by:

$$\mathbf{x} \sim \mathbf{y} \Leftrightarrow \exists\, \lambda \neq 0 \in \bar{k} \;\text{ such that } \mathbf{x} = \lambda\, \mathbf{y}\,.$$

Thus, we may also consider $\mathbf{P}_k^n$ as *the space of lines in* $\mathbf{A}_k^{n+1}$ *passing through the origin* (Figure 4.1).

Definition 4.1.2. A point of $\mathbf{P}_k^n$, which is the equivalence class of a point $(x_0, \ldots, x_n) \in \mathbf{A}_k^{n+1} \setminus \{0\}$, is denoted by its *homogenous coordinates* $[x_0 : \cdots : x_n]$.

We endow $\mathbf{P}_k^n$ with the *quotient topology*. Thus, if π denotes the canonical projection of $\mathbf{A}_k^{n+1} \setminus \{0\}$ on $\mathbf{P}_k^n$, the closed sets Y of $\mathbf{P}_k^n$ are characterized by the fact that $\pi^{-1}(Y)$ is closed in $\mathbf{A}_k^{n+1} \setminus \{0\}$. Since $\{0\}$ is closed in $\mathbf{A}_k^{n+1}$, this is the same as saying that $\pi^{-1}(Y) \cup \{0\}$ is closed in $\mathbf{A}_k^{n+1}$.

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_4

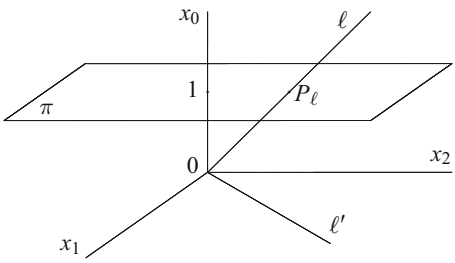


Fig. 4.1 A line ℓ passing through the origin intersects the hyperplane $\pi = \{x_0 = 1\}$ in a point P_ℓ, except if, like ℓ', it is entirely contained in the hyperplane $x_0 = 0$, these lines ℓ' are in bijection with the *points at infinity* in the hyperplane $\pi \cong \mathbf{A}^n_k$.

Remark 4.1.3. Every polynomial $g \in k[X_0, \ldots, X_n]$ can be uniquely written as a sum $g = \sum_{i=0}^{d} g_i$, where the g_i are forms of degree i, called *homogenous components* of g. Since $\bar{k}$ is infinite, it is easy to see that, if $g(\lambda x_0, \ldots, \lambda x_n) = 0$ for all $\lambda \in \bar{k} \setminus \{0\}$, then $g_i(x_0, \ldots, x_n) = 0$ for all $i = 0, \ldots, d$ also.

The *closed sets* of the projective space are therefore defined by the vanishing of homogenous polynomials. For such a polynomial f, we write $f(P) = 0$, if $f(x_0, \ldots, x_n) = 0$ for an element in the class of P (hence for all elements in that class). We also define

$$V(f_1, \ldots, f_r) = \big\{P \in \mathbf{P}^n_k \mid f_i(P) = 0 \text{ for all } i = 1, \ldots, r\big\},$$

where the $f_i \in k[X_0, \ldots, X_n]$ are homogenous polynomials (finite in number). This topology is also called the *Zariski topology*.

Remark 4.1.4. We obtain a covering of $\mathbf{P}^n_k$ by open affine sets $U_i = \mathbf{P}^n_k \setminus H_i$ on setting $H_i = V(X_i)$ and defining[1] a bijection $\varphi_i : U_i \to \mathbf{A}^n_k$ by $(a_0, \ldots, a_n) \mapsto (a_0/a_i, \ldots, \widehat{a_i/a_i}, \ldots, a_n/a_i)$.

Example 4.1.5. The *hyperbola* with equation $x_1^2 - x_2^2 = 1$ in the affine plane $U_0 \cong \mathbf{A}^2_{\mathbf{R}}$ with coordinates x_1 and x_2, is a subset of the projective curve $C \subset \mathbf{P}^2_{\mathbf{R}}$ with equation $X_1^2 - X_2^2 = X_0^2$ (where $x_i = X_i/X_0$). But if we consider the plane at infinity given by $X_1 = 0$, it is better to write $X_0^2 + X_2^2 = X_1^2$. The curve C is then seen as a *circle* with equation $y_0^2 + y_2^2 = 1$ in the affine plane $U_1 \cong \mathbf{A}^2_{\mathbf{R}}$ with coordinates $y_i = X_i/X_1$. Hence, from a projective point of view, there is no distinction between this hyperbola and a circle (see also Exercises 4.2 and 4.5).

Example 4.1.6. The circle $C \subset \mathbf{A}^2_{\mathbf{R}}$ with equation $x_1^2 + x_2^2 = 1$ has two points at infinity, namely $[X_0 : X_1 : X_2] = [0 : 1 : \pm i]$; (see also Exercise 4.3). The cissoid with equation $x_2^2 = x_1^3$, with a cusp at the origin, has the homogenous equation $X_0 X_2^2 = X_1^3$. If we take the line $X_2 = 0$ as the line at infinity, we find the equation $y_0 = y_1^3$, which represents a smooth curve with the line $y_0 = 0$ as inflection tangent at the origin.

[1] Georges de Rham's notation: the hat is placed above the deleted coordinate.

Definition 4.1.7. An ideal $\mathfrak{a} \subset k[X_0, \ldots, X_n]$ is called *homogenous* if it is generated by homogenous elements.

Lemma 4.1.8. *$\mathfrak{a}$ is homogenous if and only if*

$$f = \sum_{i=0}^{d} f_i \in \mathfrak{a} \implies f_i \in \mathfrak{a} \quad \forall\, i = 0, \ldots, d,$$

where f_i is the homogenous component of degree i.

Proof. $\Leftarrow$) If the ideal $\mathfrak{a}$ is generated by elements $f^{(1)}, \ldots, f^{(r)}$, it is also generated by the homogenous components of the $f^{(j)}$, since by hypothesis these also belong to $\mathfrak{a}$.

$\Rightarrow$) If $\mathfrak{a}$ is generated by homogenous polynomials $h^{(j)}$ with $\deg h^{(j)} = d_j$, we can write every $f \in \mathfrak{a}$ as $f = \sum g^{(j)} h^{(j)}$. Then, for all $i = 0, \ldots, d$, we have: $f_i = \sum_{d_j \leq i} g^{(j)}_{i-d_j} h^{(j)} \in \mathfrak{a}$. □

Remark 4.1.9. Consider the ideal $\mathfrak{a} = (f_1, \ldots, f_r) \subset k[X_0, \ldots, X_n]$, where the f_i are homogenous polynomials. Obviously,

$$V(f_1, \ldots, f_r) = V(\mathfrak{a}) := \left\{ P \in \mathbf{P}^n_k \mid f(P) = 0 \ \forall\, f \in \mathfrak{a} \right\}.$$

Since every ideal of $k[X_0, \ldots, X_n]$ is finitely generated, the closed sets in $\mathbf{P}^n_k$ can be described as subsets of the form

$$V(\mathfrak{a}) = \left\{ P \in \mathbf{P}^n_k \mid f(P) = 0 \ \forall\, f \in \mathfrak{a} \right\},$$

where $\mathfrak{a} \subset k[X_0, \ldots, X_n]$ is a *homogenous* ideal.

In contrast to what happens in the affine case (see Remark 2.3.4), we have $V(\mathfrak{m}) = \emptyset$ if $\mathfrak{m}$ is the maximal homogenous ideal $(X_0, \ldots, X_n)$. This is called the *maximal irrelevant ideal* (for more details see Corollary 5.3.6).

Notation 4.1.10. Given a closed subset $Y \subset \mathbf{P}^n_k$, we can also define the set $Y(k)$ of its *k-rational points*. These are the points that have *at least* one representation in homogenous coordinates $[x_0 : \cdots : x_n]$ with all x_i in k.

4.2 Morphisms

We have not yet defined morphisms. This is a rather complicated theory in algebraic geometry and we shall confine ourselves to sketching some basics.

4.2.1 The Affine Case

The definition we shall give is natural enough, but apparently depends on the choice of coordinates. Only with the Nullstellensatz can we improve the description (see §4.2).

Definition 4.2.1. If $Y \subset \mathbf{A}_k^n$ is a closed subset (an *affine variety*), a *morphism* from Y into $\mathbf{A}_k^1$ is a *polynomial function* on Y, i.e., an element of the *coordinate ring* $k[Y] = k[X_1, \ldots, X_n]/I(Y)$, where $I(Y)$ denotes the ideal of Y as in Definition 2.3.7.

Based on this definition, one easily sees how to define a morphism from Y into $Z \subset \mathbf{A}_k^m$. If Y is irreducible, we can also give a "local" definition:

Definition 4.2.2. Assume that the coordinate ring $k[Y]$ is an integral domain; let $k(Y)$ be its field of fractions. We say that $\varphi \in k(Y)$ is a *regular function at* $y \in Y$ if there are $f,\ g \in k[Y]$ such that $\varphi = f/g$ and $g(y) \neq 0$.

Example 4.2.3. If $Y \subset \mathbf{A}_k^2$ is the circle $V(x_1^2 + x_2^2 - 1)$, the function $\varphi = (1 - x_1)/x_2 \in k(Y)$ is regular at $(1, 0)$, where it takes the value 0, since it can also be written as $\varphi = x_2/(1 + x_1)$. But it is easy to see that $\varphi \notin k[Y]$ (Exercise 4.8); therefore, this function cannot be regular at $(-1, 0)$, because of the following proposition.

Proposition 4.2.4. *If $\varphi \in k(Y)$ is regular at every point $y \in Y$ of an irreducible affine variety Y, then $\varphi \in k[Y]$.*

Proof. For every point $y \in Y$, we choose an expression $\varphi = f_y/g_y$ with $g_y(y) \neq 0$. Let $\mathfrak{a} \subset k[Y]$ be the ideal generated by all denominators g_y chosen in this manner $(\forall\, y \in Y)$. Let $\mathfrak{b} = \pi^{-1}(\mathfrak{a}) \subset k[X_1, \ldots, X_n]$ be the inverse image of $\mathfrak{a}$ by the canonical projection $\pi : k[X_1, \ldots, X_n] \to k[Y]$. Then, $Z = V(\mathfrak{b}) = \emptyset$, since, on the one hand, $\mathfrak{b} \supset \pi^{-1}(0) = I(Y)$, hence $Z \subset V(I(Y)) = \overline{Y} = Y$, and on the other hand, $y \in Y \implies y \notin V(\mathfrak{b})$, as $\mathfrak{b}$ contains elements $G \in \pi^{-1}(g_y)$ corresponding to generators g_y of $\mathfrak{a}$, which do not vanish at y, and hence not on all Y.

Therefore, $1 \in \mathfrak{b} \subset k[X_1, \ldots, X_n]$ by the Weak Nullstellensatz (Theorem 5.2.1); hence, $1 = \pi(1) \in \mathfrak{a} \subset k[Y]$. There then exists a decomposition (a *partition of unity*) $1 = \sum_{i=1}^{N} u_i\, g_{y_i}$, with $u_i \in k[Y]$; hence,

$$\varphi = \sum_{i=1}^{N} u_i\, g_{y_i}\, \varphi = \sum_{i=1}^{N} u_i\, f_{y_i} \in k[Y]\,. \qquad \square$$

4.2.2 The Projective Case

We have just seen there are two equivalent definitions in the affine case. To pass to the projective case, the local definition should be used.

Definition 4.2.5. Let $Y \subset \mathbf{P}^n_k$ and $Z \subset \mathbf{P}^m_k$ be two projective varieties, with Y irreducible. A *morphism* $\varphi : Y \to Z$ is given *at every point* $y \in Y$, by a system of forms $[F_0 : \cdots : F_m]$ of the same degree, such that there is at least one index i with $F_i(y) \neq 0$. If we have several expressions at different points, we want them to be compatible. The *compatibility condition* of two expressions $[F_0 : \cdots : F_m]$ and $[G_0 : \cdots : G_m]$ is:

$$F_i G_j = F_j G_i \quad \text{on } Y, \quad \forall\, 0 \leq i < j \leq m\,. \tag{4.2.1}$$

Example 4.2.6. Let $Y = V(g) \subset \mathbf{P}^2_k$ be a *smooth conic*, with $Y(k) \neq \emptyset$. This means that g is a quadratic form and that, for all $P \in Y$, there is at least one index i such that $\frac{\partial g}{\partial X_i}(P) \neq 0$.

By a k-linear change of variables, we may assume without loss of generality that $Y(k)$ contains the point $Q = [1 : 0 : 0]$, so that g has no term in X_0^2. Thus, we may write $g(X_0, X_1, X_2) = X_1\, g_1 + X_2\, g_2$, where g_1 and g_2 are linear forms.

We define $\varphi : Y \to \mathbf{P}^1_k$ as follows:

$$y = [X_0 : X_1 : X_2] \mapsto \begin{cases} [X_1 : X_2] & \text{if } y \neq Q \\ [-g_2(X_0, X_1, X_2) : g_1(X_0, X_1, X_2)] & \text{if } y = Q \end{cases}$$

The compatibility condition of these two expressions is ensured, since $g = X_1\, g_1 + X_2\, g_2 = 0$ on Y. Moreover, φ is a morphism, for $X_1 = X_2 = 0$ occurs only at Q, and then

$$[-g_2(Q) : g_1(Q)] = [-\frac{\partial g}{\partial X_2}(Q) : \frac{\partial g}{\partial X_1}(Q)] \neq [0 : 0]\,,$$

since $\frac{\partial g}{\partial X_0}(Q) = 0$ and since the conic is smooth.

In fact, *φ has an inverse and hence is an isomorphism.* Indeed, write $g = X_0\, \ell + q$, where $\ell(X_1, X_2)$ is a linear form and $q(X_1, X_2)$ a binary quadratic form. Then, if $g = 0$, we have $X_0\, \ell = -q$. Define $\psi : \mathbf{P}^1_k \to Y$ by the formula

$$[X_1 : X_2] \mapsto [-q : X_1\, \ell : X_2\, \ell]\,.$$

The map ψ is defined everywhere, since we cannot have $\ell = q = 0$ at any point of $\mathbf{P}^1_k$. Indeed, ℓ is not identically zero, or else $Y = V(g)$ would not be smooth. Therefore, by a linear transformation we can reduce our considerations to the case $\ell = X_1$. We would then have $q(0, 1) = 0$ and the coefficient of X_2^2 in q would be zero. But then $X_1 = \ell$ would divide q, and we could write $g = X_1\, h$, which is not smooth. The fact that φ and ψ are inverse to one another is then obvious.

We have thus proved an important result:

Proposition 4.2.7 (Hilbert & Hurwitz, 1891). *If $Y \subset \mathbf{P}^2_k$ is a smooth conic with $Y(k) \neq \emptyset$, then Y is isomorphic to $\mathbf{P}^1_k$.*

Notice that the isomorphism is defined over the field k. Consequently, the images of rational points are rational points. This proposition applies in particular to finite fields:

Corollary 4.2.8. *If $Y \subset \mathbf{P}^2_k$ is a smooth conic over $k = \mathbf{F}_q$, then $|Y(k)| = q + 1$.*

Proof. By the Chevalley–Warning Theorem (Theorem 3.4.10), we know that $Y(k) \neq \emptyset$. By Proposition 4.2.7, Y and $\mathbf{P}^1_k$ have the same number of points in k, and in fact in every finite extension K/k. □

Example 4.2.9. Let $C \subset \mathbf{A}^2_k$ be the *affine* circle with equation $x_1^2 + x_2^2 = 1$ over $k = \mathbf{F}_p$, where p is an odd prime. Then

$$|C(k)| = \begin{cases} p - 1 & \text{if } p \equiv +1 \pmod 4 \\ p + 1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Indeed, consider the closure $Y = \overline{C} \subset \mathbf{P}^2_k$. This is a smooth conic that has $p + 1$ k-rational points, by Corollary 4.2.8. Now, two of these points are at infinity if $p \equiv +1 \pmod 4$, since in this case -1 is a quadratic residue modulo p. However, if $p \equiv -1 \pmod 4$, the congruence $X_1^2 + X_2^2 \equiv 0 \pmod p$ has no non-trivial solutions and all k-rational points of Y lie on C.

This example illustrates the fact that, even if one is interested in affine varieties, it is often easier to study first the corresponding projective varieties. There is in this case a fundamental result, which we do not prove here (see [Sh], Chap. I, §5, Theorem 2):

Theorem 4.2.10. *The image of a projective variety by a morphism is always closed.*

Therefore, in Definition 4.2.5, the image of Y in Z is closed. From this one easily deduces:

Corollary 4.2.11. *Let Y be a projective absolutely irreducible variety and φ a morphism such that $\varphi(Y) \subset \mathbf{A}^1_k$. Then, φ is a constant map.*

This is an essentially projective property, as the example of the hyperbola $Y = V(x_1x_2 - 1) \subset \mathbf{A}^2_k$ and its projection on $\mathbf{A}^1_k \setminus \{0\}$ shows.

From an arithmetic point of view, we must mention the next important theorem:

Theorem 4.2.12 (Weil's Theorem, 1948). *Let Y be a smooth projective, absolutely irreducible curve of genus g, defined over $k = \mathbf{F}_q$. Then,*

$$\big||Y(k)| - (q + 1)\big| \leq 2\, g\, q^{1/2}\,.$$

For plane curves, it is known that a smooth curve $Y \subset \mathbf{P}^2_k$ of degree d has genus $g = \frac{1}{2}(d - 1)(d - 2)$. Thus, conics ($d = 2$) have genus 0 and Theorem 4.2.12

includes Corollary 4.2.8 as a particular case. It also includes the following very deep result:

Corollary 4.2.13 (F. K. Schmidt, 1929). *If Y is a curve of genus 1 (projective, absolutely irreducible and smooth, defined over $k = \mathbf{F}_q$), then $|Y(k)| \neq \emptyset$.* □

Schmidt's proof required a study of the *zeta function* of the function field $K = k(Y)$ of the curve and also made use of the *Riemann–Roch Theorem*, for which it also provided a proof, valid over any perfect field. In 1936, Schmidt extended this result to an arbitrary field, giving a proof that highly motivated André Weil.

Theorem 4.2.12 has a long and complicated proof. André Weil had to write three books in order to formulate it completely. This theorem on finite fields (and the conjectures generalizing it) played a fundamental role in the development of algebraic geometry in the second half of the twentieth century.

4.3 Springer's Theorem

This theorem is stated for an arbitrary quadratic form over any field. The proof has a very nice geometric interpretation. To keep things simple, we give this interpretation, referring mainly to the case of an absolutely irreducible quadric defined over a perfect field.

Theorem 4.3.1 (Springer, 1952). *Let $Y = V(f) \subset \mathbf{P}^n_k$ be an arbitrary quadric; let K/k be an algebraic extension of* odd *degree d. Then, $Y(K) \neq \emptyset \implies Y(k) \neq \emptyset$.*

Proof. In this statement, $f(X_0, \ldots, X_n)$ is a quadratic form with coefficients in k. Since the result is obviously true for $d = 1$, we proceed by induction, assuming that the theorem is proved for odd degrees $\delta < d$, *over any field*.

We may also assume, without loss of generality, that K is a simple extension $K = k(\theta)$. Otherwise, there would be an intermediate field $K \supsetneq k(\theta) \supsetneq k$ and the result would be immediate by induction [2].

Let $P \in Y(K)$; we may assume its coordinate x_0 is not zero and write $P = [1 : p_1(\theta) : \cdots : p_n(\theta)]$, where the $p_i \in k[t]$ are polynomials of degree $\leq d - 1$. Also, let $h(t)$ be the minimal polynomial of θ, which is therefore of degree d.

We define $F(t) = f(1, p_1(t), \ldots, p_n(t)) \in k[t]$. Then, $F(\theta) = f(P) = 0$, which implies that F is divisible by h. (Geometrically, this means that we have found a rational curve Γ passing through P and all its conjugates. This is the image of a projective morphism $\varphi : \mathbf{P}^1_k \to \mathbf{P}^n_k$, whose restriction to $\mathbf{A}^1_k$ is defined parametrically by $t \mapsto [1 : p_1(t) : \cdots : p_n(t)]$.)

[2] If k is perfect, we may also use Lemma 3.1.17. Note that an intermediate field does not necessarily exist, even if the degree $[K : k]$ is not prime; for instance, Galois theory shows the existence of degree 4 extensions of the field of rational numbers which contain no quadratic extension of $\mathbf{Q}$.

We may also assume that $F(t)$ is not the zero polynomial. Otherwise, we would have $F(a) = 0$ for all $a \in k$; hence, $[1 : p_1(a) : \cdots : p_n(a)] \in Y(k)$.

Let m be the highest of the degrees of the $p_i(t)$. It is clear that $\deg F \leq 2m \leq 2d-2$, but we may even assume that $\deg F = 2m$. Otherwise, the coefficient of t^{2m} is zero, whence a non-trivial solution, formed by the coefficients of the degree m of the polynomials p_i. (This solution is at infinity, since $x_0 = 0$, and it would correspond to $t = \infty$ in the parametrization of Γ.)

We thus have $\frac{F(t)}{h(t)} = g(t)$, where $\deg g = 2m - d \leq d - 2$ is odd. Let η be a root of g of odd degree δ; then, since $F(\eta) = h(\eta)g(\eta) = 0$, we have: $[1 : p_1(\eta) : \cdots : p_n(\eta)] \in Y(k(\eta))$, where $k(\eta)/k$ is of odd degree $\delta \leq d - 2 < d$. □

Scholion 4.3.2. Bézout's Theorem states that in the projective space the curve Γ, which is of degree m, cuts the quadric Y in $2m$ points. These points include the d conjugates of P, and there are $2m - d$ others, which form a *k-rational cycle*.

4.4 Brumer's Theorem

Notation 4.4.1. If $Q(x)$ is a quadratic form over a field k (or more generally, over a commutative ring), we denote by $B(x, y)$ the bilinear form defined by the relation

$$B(x, y) = Q(x + y) - Q(x) - Q(y)\,. \tag{4.4.1}$$

Notice that $B(x, x) = 2\,Q(x)$. To verify that $B(x, y)$ is indeed a bilinear form, it is enough to observe that the terms in x_i^2 are changed into $2\,x_i\,y_i$, and that the terms $x_i\,x_j$ give $x_i\,y_j + x_j\,y_i$. In characteristic 2, we always have $B(x, x) = 0$ and the theory of quadratic forms is no longer the same as that of bilinear forms.

Theorem 4.4.2 (Brumer, 1978). *Let Q_1, Q_2 be two quadratic forms with coefficients in k; let Y_1, $Y_2 \subset \mathbf{P}_k^n$ be the associated quadrics. Also, let $Y \subset \mathbf{P}_{k(t)}^n$ be the quadric associated with the quadratic form $Q = Q_1 + t\,Q_2$, where t is an indeterminate. Then*

$$(Y_1 \cap Y_2)(k) \neq \emptyset \Longleftrightarrow Y(k(t)) \neq \emptyset\,.$$

Proof. It is enough to show sufficiency. Consider a point $W \in Y(k(t))$. We may assume that its coordinates are polynomials, and write $W = \sum_{i=0}^{d} t^i\,V_i$, where the V_i are vectors with coordinates in k, with $V_d \neq 0$ (and also $V_0 \neq 0$, on dividing if necessary by a power of t in order to normalize the expression). The V_i may be zero; hence, not all of them correspond to points in the projective space. But since $V_d \neq 0$, we say that W has *degree d*. In this case, we may consider the point $V_d \in \mathbf{P}_k^n(k)$. If $Q(V_d) = 0$, obviously also $Q_1(V_d) = Q_2(V_d) = 0$; therefore, $(Y_1 \cap Y_2)(k) \neq \emptyset$.

Thus, we may assume that $V_d \notin Y$ and that $d > 0$. We proceed by induction on d. Indeed, if $d = 0$, the result is at hand.

Since $V_d \notin Y$, the line connecting V_d to W meets Y in a second intersection point $W' = W + \lambda V_d$ ($\lambda = 0$ corresponds to W, $\lambda = \infty$ to V_d). It suffices to see that $\deg W' < \deg W$ (which also implies that the line is not tangent to Y at W; otherwise, we would have $W' = W$). Now, W' is defined by the equation $Q(W') = Q(W + \lambda V_d) = Q(W) + \lambda^2 Q(V_d) + \lambda\, B(W, V_d) = 0$. Since $Q(W) = 0$, we find that $\lambda = -\frac{B(W,V_d)}{Q(V_d)}$.

On the other hand, on applying Formula (4.4.1), we see that the terms of highest degree in $Q(W)$ are

$$Q_2(V_d)\, t^{2d+1} + [Q_1(V_d) + B_2(V_{d-1}, V_d)]\, t^{2d} + \dots$$

Therefore, $Q_2(V_d) = 0$; hence, $Q(V_d) = Q_1(V_d) \in k$, so that λ is a polynomial in t. This polynomial has degree at most d, for $B_2(V_d, V_d) = 2\, Q_2(V_d) = 0$. Consequently, $W' = W + \lambda\, V_d$ has degree at most d.

Moreover, $Q_1(V_d) + B_2(V_{d-1}, V_d) = 0$ implies that the coefficient of t^d in W' is also zero, since it is:

$$V_d - \frac{V_d}{Q_1(V_d)} \{B_1(V_d, V_d) + B_2(V_{d-1}, V_d)\}$$
$$= V_d - \frac{V_d}{Q_1(V_d)} \{2\, Q_1(V_d) + B_2(V_{d-1}, V_d)\} = V_d - V_d = 0\,.$$

This shows that W' has a smaller degree than W, which concludes the proof. □

Corollary 4.4.3. *Let K/k be an algebraic extension of odd degree; then*

$$(Y_1 \cap Y_2)(K) \neq \emptyset \implies (Y_1 \cap Y_2)(k) \neq \emptyset\,.$$

Proof. $(Y_1 \cap Y_2)(K) \neq \emptyset \implies Y(K(t)) \neq \emptyset$, and Springer's Theorem entails that $Y(k(t)) \neq \emptyset$; hence, $(Y_1 \cap Y_2)(k) \neq \emptyset$. □

Comment 4.4.4. Counter-examples show that this result does not extend to intersections of three or more quadrics. This indicates that the proof must include more than elementary computations with the degrees of algebraic extensions.

4.5 Choudhry's Lemma

Let Q be an arbitrary quadratic form in n variables over a field k. For a fixed n-uple $u = (u_1, \dots, u_n) \in k^n$, we are concerned with the quadric $V(R) \subset \mathbf{A}_k^n$, where $R(x) = Q(x) - Q(u)$. We already know a rational point on this variety, namely $x = u$, and we can look for others, by stereographic projection from this point.

We thus take any vector $v \neq 0$ in k^n, and then look for the intersection of the quadric $R(x) = 0$ with the line $\{x = u + \lambda v \mid \lambda \in k\}$, which passes through u (for $\lambda = 0$). The computation is done by means of Formula (4.4.1):

$$0 = R(x) = R(u + \lambda v) = Q(u + \lambda v) - Q(u) = Q(\lambda v) + B(u, \lambda v)\,.$$

As in the proof of Brumer's Theorem, we find the condition

$$0 = Q(\lambda v) + B(u, \lambda v) = \lambda^2 Q(v) + \lambda B(u, v)\,,$$

that is $\lambda = -\frac{B(u,v)}{Q(v)}$, provided that $Q(v) \neq 0$.

On substituting this value of λ in the preceding equations, we find:

$$Q(u - \frac{B(u, v)}{Q(v)}v) = Q(u)\,.$$

Multiplying in the parenthesis by $Q(v)$ we get:

$$Q(uQ(v) - B(u, v)v) = Q(u)Q(v)^2\,,$$

a formula that is valid (trivially) even if $Q(v) = 0$. Hence, the lemma:

Lemma 4.5.1 (Choudhry, 2010). *Let Q be an arbitrary quadratic form in n variables over a field k. There is a composition law $\tau : k^n \times k^n \to k^n$, defined by*

$$\tau : (u, v) \mapsto w = uQ(v) - B(u, v)v \tag{4.5.1}$$

for which the following formula holds:

$$Q(w) = Q(u)Q(v)^2\,. \tag{4.5.2}$$

Proof. This statement is deduced directly from Formula (4.4.1), without going through the above heuristic argument. Indeed,

$$\begin{aligned} Q(w) &= Q\big(uQ(v) - B(u, v)v\big) \\ &= Q\big(uQ(v)\big) + Q\big(-B(u, v)v\big) + B\big(uQ(v), -B(u, v)v\big) \\ &= Q(u)Q(v)^2 + B(u, v)^2 Q(v) - Q(v)B(u, v)B(u, v) \\ &= Q(u)Q(v)^2\,. \end{aligned}$$

□

This lemma has various arithmetic applications, in particular because it is valid not only over a field, like $k = \mathbf{Q}$ but also over a ring, like $A = \mathbf{Z}$. For example, if $Q(x) = x_1^2 + x_2^2 + x_3^2$, we may start from $1^2 + 4^2 + 8^2 = 9^2$ and find other sums

of three squares by simply composing $u = (1, 0, 0)$ and $v = (1, 4, 8)$ by means of Formula (4.5.1); we find in this way $8^2 + 16^2 + 79^2 = 81^2$, and so on.

Property (4.5.2) also shows that we can define algebraic functors $S \times S \to S$ and $T \times T \to T$ respectively on $S = \{x \mid Q(x) = 1\}$ and on $T = \{x \mid Q(x) = -1\}$, by means of the composition Formula (4.5.1). Such a law exists for any quadratic form in any dimension.

Exercises

4.1. Let $\mathfrak{p} \subsetneq k[X_0, \ldots, X_n]$ be a homogenous ideal. Show that $\mathfrak{p}$ is prime if and only if it satisfies the following condition: if f and g are two homogenous polynomials, then: $fg \in \mathfrak{p} \Rightarrow f \in \mathfrak{p}$ or $g \in \mathfrak{p}$.

4.2. If $F \in k[X_0, \ldots, X_n]$ is a form, one defines its *dehomogenization* $F_* = F(1, X_1, \ldots, X_n)$. Conversely, let $f \in k[X_1, \ldots, X_n]$ be a polynomial of degree d. One defines its *homogenization* $f^* = X_0^d\, f(X_1/X_0, \ldots, X_n/X_0)$. Then, f^* is a form of degree d. Show that:

(a) $(FG)_* = F_* G_*$;
(b) $(fg)^* = f^* g^*$;
(c) $X_0^r (F_*)^* = F$, where r is the highest power of X_0, which divides F;
(d) $(f^*)_* = f$;
(e) $(F + G)_* = F_* + G_*$;
(f) $X_0^t (f + g)^* = X_0^r f^* + X_0^s g^*$, where $r = \deg g$, $s = \deg f$ and $t = r + s - \deg(f + g)$.

4.3. Let $F(X_0, X_1, X_2) \in \mathbf{R}[X_0, X_1, X_2]$ be a real quadratic form such that $F(0, 1, \pm i) = 0$. Let $Y = V(F_*) \subset \mathbf{A}^2_{\mathbf{R}}$; show that in general, $Y(\mathbf{R})$ is a circle, provided that $Y(\mathbf{R}) \neq \emptyset$. Study degenerate cases.

4.4. Find the points at infinity of the plane quartic $V(x_1^4 + x_1 x_2 - x_2^4) \subset \mathbf{A}^2_k$ illustrated in Figure 4.2.

4.5. Let $Y \subset \mathbf{A}^n_k$ be an affine variety. We identify $\mathbf{A}^n_k$ with $\mathbf{P}^n_k \setminus V(X_0)$ via the map $j : \mathbf{A}^n_k \to \mathbf{P}^n_k$, which sends $(x_1, \ldots, x_n)$ onto $[1 : x_1 : \cdots : x_n]$. Show that if $F \in k[X_0, \ldots, X_n]$ is a form, we have $F \circ j = F_*$. We define $\overline{Y}$ as the closure of $j(Y)$ in $\mathbf{P}^n_k$. Show that $I(\overline{Y})$ is the ideal generated by $\{f^* \mid f \in I(Y)\}$.

4.6. Let $Y \subset \mathbf{A}^3_{\mathbf{C}}$ be the image of the morphism $\varphi : \mathbf{A}^1_{\mathbf{C}} \to \mathbf{A}^3_{\mathbf{C}}$, defined by $t \mapsto (t, t^2, t^3)$. Find generators f_1 and f_2 for $I(Y)$ such that $I(\overline{Y}) \neq (f_1^*, f_2^*)$.

4.7. Find the points at infinity on the cubic surface $Y = V(x_1 x_2 x_3 - 1) \subset \mathbf{A}^3_k$. How many distinct lines does the projective surface $\overline{Y} \subset \mathbf{P}^3_k$ contain?

4.8. Prove the assertion in Example 4.2.3: $\varphi \notin k[Y]$.

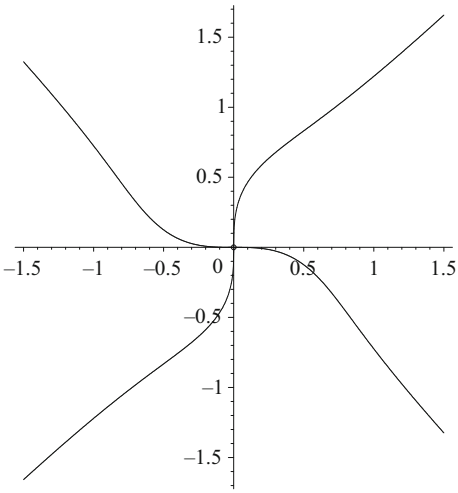


Fig. 4.2 The plane quartic $V(x_1^4 + x_1x_2 - x_2^4) \subset \mathbf{A}_k^2$

4.9. Let $Y = V(X_0X_3 - X_1X_2) \subset \mathbf{P}_k^3$. Study the fibers of the morphism $\varphi : Y \to \mathbf{P}_k^1$, defined on an open set in Y by $\varphi([X_0 : \cdots : X_3]) = [X_0 : X_2]$.

4.10. Consider the projective curve $\Gamma = V(X_1X_2 - X_3^2,\ X_1^2 - 17X_2^2 - 2X_0^2) \subset \mathbf{P}_k^3$. Show that $\varphi : \Gamma \to \mathbf{P}_k^2$ given by $\varphi([X_0 : X_1 : X_2 : X_3]) = [X_0 : X_1 : X_3]$ is a morphism. What is the image of φ? Study the inverse image of points of the image of φ.

4.11. Let $\Gamma \subset \mathbf{P}_k^2$ be a plane cubic: $\Gamma = V(f)$, where $f(X_0, X_1, X_2)$ is a homogenous polynomial of degree 3. Let K/k be a quadratic extension. Show that $\Gamma(K) \neq \emptyset \implies \Gamma(k) \neq \emptyset$.

4.12. (Aubry, *Sphinx-Œdipe*, 1912) If $m \in \mathbf{N}$ is a sum of three squares of rational numbers $m = x_1^2 + x_2^2 + x_3^2$ ($x_i \in \mathbf{Q}$), then m is also the sum of three integer squares: $m = m_1^2 + m_2^2 + m_3^2$ ($m_i \in \mathbf{N}$).
(*Hint:* Geometric proof, analogous to that of Brumer's Theorem: if P is a rational point on the sphere $V(x_1^2 + x_2^2 + x_3^2 - m) \subset \mathbf{A}_{\mathbf{Q}}^3$, choose in $\mathbf{A}_{\mathbf{Q}}^3$ a point N with integer coordinates whose distance to P is as small as possible; draw the line NP, show that it is not tangent to the sphere and examine the common denominator of its residual intersection with this surface.)

Chapter 5
The Nullstellensatz

Hilbert's *Zeros Theorem* plays an essential role in algebraic geometry. It allows one to better define morphisms, as the Nullstellensatz implies that the affine algebraic k-varieties form a category equivalent to that of reduced k-algebras of finite type. The most important consequence is the *unity of algebra and geometry*. Since the field k is arbitrary, this leads to numerous arithmetic applications.

5.1 Integral Extensions

We shall prove the Nullstellensatz here. Most presentations in the literature assume the base field to be algebraically closed. This hypothesis is unnecessary and even deleterious for applications to arithmetic.

We begin with some preliminaries that we need concerning integral extensions.

Definition 5.1.1. Let $A \subset B$ be two rings. We say that $\xi \in B$ is *integral* over A if there is a **monic** polynomial $f \in A[X]$ such that $f(\xi) = 0$.

It is an essential requirement that f should be monic, that is, with leading coefficient 1. When A is a field, this is obviously not a restriction and we retrieve the definition of an algebraic number (Definition 2.1.1).

Definition 5.1.2. B is *integral* over A if all its elements are.

Definition 5.1.3. Let A be an integral domain with field of fractions K. We say that A is *integrally closed* if every element of K that is integral over A belongs to A. (In other words, $f \in A[X]$ monic, $\xi \in K$ and $f(\xi) = 0$ imply $\xi \in A$.)

Lemma 5.1.4. *A factorial ring is integrally closed.*

Proof. If A is factorial with field of fractions K, we can write every $\xi \in K$ as $\xi = \alpha/\beta$ with $\alpha,\ \beta \in A$ relatively prime. If $\xi^n + a_1\,\xi^{n-1} + \cdots + a_n = 0$, where the

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_5

a_i are in A, we also have $\alpha^n + \beta(a_1\alpha^{n-1} + \cdots + a_n\beta^{n-1}) = 0$. Consequently, each irreducible factor of β divides α^n; hence, α, which is impossible, since α and β are relatively prime. We deduce that β is a unit and that $\xi \in A$. □

Examples. $\mathbf{Z}$, $K[X]$, $K[X_1, \ldots, X_n]$, etc., are factorial, and hence integrally closed.

$\mathbf{Z}[i]$ is Euclidean, and hence principal, hence factorial, and hence integrally closed.

$\mathbf{Z}[\sqrt{5}] = \left\{m + n\sqrt{5} \mid m, n \in \mathbf{Z}\right\}$ is not integrally closed. Indeed, the golden ratio $\xi = \frac{1+\sqrt{5}}{2}$ is not in this ring. However, it is a root of the polynomial $f(X) = X^2 - X - 1$.

$\mathbf{Z}[\sqrt{-5}] = \left\{m + n\sqrt{-5} \mid m, n \in \mathbf{Z}\right\}$ is not factorial, but is integrally closed (see Exercises 5.9 and 5.1).

$\mathbf{Q}[X_1, X_2]/(X_2^2 - X_1^3)$, the coordinate ring of the *cissoid* (see Example 5.1.15), is not integrally closed: if x denotes the class of X_1, and y the class of X_2, the ratio $\xi = y/x$ is a square root of x;

$\mathbf{Q}[X_1, X_2]/(X_1^2 + X_2^2 - 1)$ is not factorial, but is integrally closed (see Exercises 5.11 and 5.2).

Notation 5.1.5. In the sequel, the notation $A[\xi]$ denotes the ring of all polynomial expressions $\sum_{i=0}^{n} a_i \xi^i$, where ξ is an element of a ring $B \supset A$. This amounts to substituting $X = \xi$ in the polynomials with coefficients in A; the computations take place in B, since $\xi \in B$. The ring $A[\xi]$ contains A as a subring; it is therefore *algebra of finite type over* A, generated by ξ. It is also a module over the ring A, but in general it is *not of finite type as an* A*-module*.

Proposition 5.1.6. *Let $A \subset B$ be two rings, and let $\xi \in B$. The following properties are equivalent:*

(a) *ξ is integral over A;*
(b) *The ring $A[\xi]$ is an A-module of finite type;*
(c) *$A[\xi]$ is contained in a ring C, which is an A-module of finite type.*

Proof. (a) $\Longrightarrow$ (b): If $\xi^n + a_1\xi^{n-1} + \cdots + a_n = 0$, then $A[\xi]$ is generated as an A-module by $1, \xi, \ldots, \xi^{n-1}$. Indeed, we can write ξ^n as a linear expression in $1, \xi, \ldots, \xi^{n-1}$, but also ξ^{n+1}, and so on inductively.

(b) $\Longrightarrow$ (c): it suffices to take $C = A[\xi]$.

(c) $\Longrightarrow$ (a): we shall give two proofs: the first one is very quick, but valid only if A is a Nœtherian ring (this condition is often fulfilled in applications); the second one is valid in all generality, but is based on a version of the Cayley–Hamilton Theorem.

I. (van der Waerden [vdW], §135) We assume A to be Nœtherian. In this case, C is a Nœtherian A-module (as it is the quotient of a free A-module of finite type, which is also Nœtherian, since it is a finite direct sum of Nœtherian modules). Hence, the sub-A-modules generated by $1, \xi, \ldots, \xi^r$ ($r \to \infty$) form a stationary chain, hence the result. (We have not used the fact that C is a ring!)

II. Without a hypothesis on the ring A, let $\{\gamma_1, \ldots, \gamma_n\}$ be a system of generators of the A-module C. We consider multiplication by ξ:

$$\xi\, \gamma_i = \sum_{j=1}^{n} a_{ij}\, \gamma_j .$$

(The $a_{ij} \in A$ are not uniquely determined, but this is not important for this argument.) Introducing the Kronecker symbol ($\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ii} = 1$), this can also be written:

$$\sum_{j=1}^{n} (\delta_{ij}\, \xi - a_{ij})\, \gamma_j = 0 \qquad (i = 1, \ldots, n).$$

In matrix notation, these n relations are written $M\, \boldsymbol{\gamma} = 0$, where M is the matrix $(\delta_{ij}\, \xi - a_{ij})$, and $\boldsymbol{\gamma}$ the column vector (γ_j). We can then multiply the matrix M, with determinant $d \in A[\xi] \subset C$, by its *adjoint* M^*; hence (denoting by $\mathbf{I}$ the identity matrix),

$$d\, \boldsymbol{\gamma} = d\, \mathbf{I}\, \boldsymbol{\gamma} = M^* M\, \boldsymbol{\gamma} = \mathbf{0}.$$

Consequently, $d\gamma_j = 0 \ \forall\, j$ and, hence $d \,.\, 1 = 0$, since the γ_j generate C as an A-module and $1 \in C$. It is then enough to expand the determinant, to find a relation of integral dependence for ξ. □

Corollary 5.1.7. *Let $\xi_1, \ldots, \xi_n \in B$ be integral elements over A. Then the ring $A[\xi_1, \ldots, \xi_n]$ is an A-module of finite type.*

Proof. By induction on n: for $n = 1$, this is (a) $\Longrightarrow$ (b) from Proposition 5.1.6. If $n > 1$, we set $C = A[\xi_1, \ldots, \xi_{n-1}]$ and find that $A[\xi_1, \ldots, \xi_n] = C[\xi_n]$ is of finite type over C, which by induction is of finite type over A. If $\{\delta_1, \ldots, \delta_m\}$ is a system of generators of $C[\xi_n]$ over C, and if $\{\gamma_1, \ldots, \gamma_\ell\}$ is a system of generators of C over A, it is immediate that the products $\gamma_i\, \delta_j$ generate $C[\xi_n]$ over A. □

Corollary 5.1.8. *If $\alpha, \beta \in B$ are integral over A, then so are $\alpha + \beta$ and $\alpha \cdot \beta$.*

Proof. $A[\alpha + \beta]$ and $A[\alpha \cdot \beta]$ belong to the ring $C = A[\alpha, \beta]$, which is also an A-module of finite type, by Corollary 5.1.7. The assertion then follows from (c) $\Longrightarrow$ (a) in Proposition 5.1.6. □

Corollary 5.1.9. *The ring $A[\alpha] \subset B$ is integral over A if and only if $\alpha \in B$ is integral over A.* □

Corollary 5.1.10. *The set of the elements of B, which are integral over A, form a ring.* □

Definition 5.1.11. This ring is called the *integral closure* of A in B. In the particular case when B is the field of fractions of A, the ring is denoted by $\widetilde{A}$ and called the *integral closure* of A.

$\widetilde{A}$ is integrally closed, as easily results from the following corollary.

Corollary 5.1.12. *If $A \subset B \subset C$, with C integral over B and B integral over A, then C is integral over A.*

Proof. Let $\xi \in C$ satisfy a relation of integral dependence $\xi^n + b_1 \xi^{n-1} + \cdots + b_n = 0$, with $b_i \in B$. Corollary 5.1.7 entails that the ring $B' = A[b_1, \ldots, b_n] \subset B$ is an A-module of finite type. On the other hand, the integral dependence relation shows that ξ is also integral over B'. Therefore, the ring $C' = B'[\xi] \subset C$ is a B'-module of finite type (Proposition 5.1.6). The argument in Corollary 5.1.7 then shows that C' is an A-module of finite type. Since $A[\xi] \subset C'$, we find that ξ is integral over A, by virtue of (c) $\Longrightarrow$ (a) in Proposition 5.1.6. □

Definition 5.1.13. We say that $Y \subset \mathbf{A}_k^n$ is a *normal variety* if its coordinate ring is integrally closed.

Comment 5.1.14. The integral closure plays a major role in algebraic number theory and algebraic geometry. In number theory, it allows one to define the ring of integers of a number field: the *ring of integers* $\mathcal{O}_K$ of a finite extension $K/\mathbf{Q}$ is defined as the integral closure of $\mathbf{Z}$ in K. In algebraic geometry, if $A = k[Y]$ is the coordinate ring of an affine irreducible variety, one shows ([ZS], Chap. V, §4, thm. 9) that the integral closure $\widetilde{A}$ of A is also the coordinate ring of an affine variety $\widetilde{Y}$: the *normalization* of Y. This *normalization* process, discovered by Zariski in 1937, is extremely powerful. For example, if Y is a curve, one shows that $\widetilde{Y}$ is a non-singular curve, and that the inclusion $A \hookrightarrow \widetilde{A}$ induces a surjective morphism $\widetilde{Y} \to Y$, which is an isomorphism over a non-empty open subset of Y. This entirely algebraic method gives an immediate answer to the problem of *resolution of singularities* for a curve. It has many other applications and normal varieties have many good properties (Figure 5.1).

Example 5.1.15. Let $\Gamma \subset \mathbf{A}_k^2$ be the plane curve with equation $y^2 = x^3$. Its coordinate ring is $A = k[X_1, X_2]/(X_2^2 - X_1^3)$, where x and y are the classes of X_1 and X_2 respectively. This ring is integral, but not integrally closed, since its field of fractions contains the ratio $z = y/x$, which is a square root of x but is not in A. By adjoining z to the ring A, we obtain the ring $\widetilde{A} = A[z] \cong k[X_1, X_2, X_3]/(X_2^2 - X_1^3, X_2 - X_1X_3, X_1 - X_3^2)$, which has the same field of fractions and is integrally closed, for one easily sees that $\widetilde{A} \cong k[X_1, X_2, X_3]/(X_1 - X_3^2, X_2 - X_3^3) \cong k[X_3]$.

The normalization of Γ may therefore be viewed either as the skew cubic $\widetilde{\Gamma}$, image of the morphism $t \mapsto (t^2, t^3, t) \in \mathbf{A}_k^3$, or as the line $\mathbf{A}_k^1$. The inclusion $A \hookrightarrow \widetilde{A}$ corresponds to the projection $(x, y, z) \mapsto (x, y)$ in the first case, and to the parametrization $t \mapsto (t^2, t^3)$ in the second (see Theorem 5.4.7).

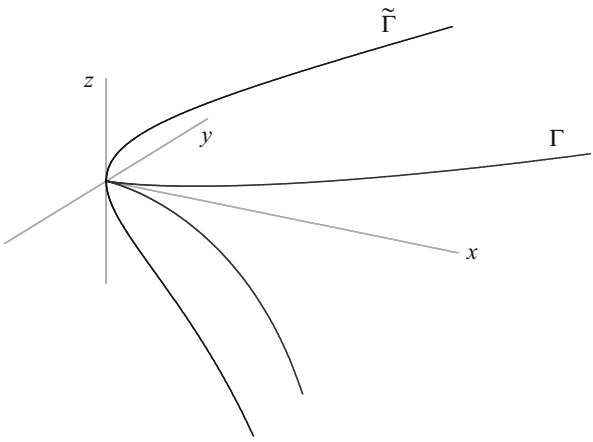


Fig. 5.1 The cissoid Γ and its normalization, viewed as a skew cubic $\widetilde{\Gamma}$ in $\mathbf{A}_k^3$

Let us point out one more result, often quoted in explicit computations.

Proposition 5.1.16. *Let $A \subset B$ be integral rings; let $\xi \in B$ be an element integral over A. In particular, ξ is algebraic over the field of fractions K of A. Assume that A is integrally closed. Then, the minimal polynomial (monic) of ξ over K has all its coefficients in the ring A.*

Proof. Let $q \in K[X]$ be the minimal polynomial of ξ. Let L/K be an extension containing all the roots of q (for example, $L = \overline{K}$). Let $p(\xi) = 0$ be a relation of integral dependence. Then, all the roots ξ_i of q satisfy this same relation (as q divides p). Now, the coefficients of q are polynomials in the ξ_i (the elementary symmetric functions, whose coefficients are all equal to ± 1). They are therefore integral over A. But they also belong to K, the field of fractions of A, which is integrally closed by hypothesis. □

5.2 The Weak Nullstellensatz

In its weak version, the statement of Hilbert's Nullstellensatz is very simple: $V(\mathfrak{m}) \neq \emptyset$. This is more precisely shown in the following.

Theorem 5.2.1 (Weak Nullstellensatz). *Let k be a field, with a fixed algebraic closure $\bar{k}$. Let $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ be a maximal ideal; we define $Y = V(\mathfrak{m}) \subset \mathbf{A}_k^n$. Then, $Y(\bar{k}) \neq \emptyset$.*

The proof is analogous to that of Lemma 2.2.1: since $\mathfrak{m}$ is a maximal ideal, the quotient $K = k[X_1, \ldots, X_n]/\mathfrak{m}$ is a field, and an extension of k. Consider the classes $\alpha_i = \pi(X_i)$; then the n-uple $P = (\alpha_1, \ldots, \alpha_n)$ is canceled by every $f \in \mathfrak{m}$. Indeed, $f(\alpha_1, \ldots, \alpha_n)$ is the class of $f(X_1, \ldots, X_n) \in \mathfrak{m}$.

The proof would be finished (and very easy!) if we knew that P is a point of $\mathbf{A}_k^n$. In fact, we do not even know whether the α_i are algebraic. This is the content of the next proposition ([ZS], Chap. VII, §3, p. 165).

Proposition 5.2.2. *If an algebra of finite type $K = k[\alpha_1, \ldots, \alpha_n]$ is a field, then K/k is an algebraic extension.*

Proof. If $n = 1$, it is clear that α_1 is algebraic. Indeed, $\alpha_1 \neq 0$ has an inverse $\alpha_1^{-1} = a_0\,\alpha_1^m + \cdots + a_m$ (where $a_0 \neq 0$) and $a_0\,\alpha_1^{m+1} + \cdots + a_m\,\alpha_1 - 1 = 0$ is a relation of algebraic dependence.

The proof is then done by induction on n. The field K contains $k' = k(\alpha_1)$. Hence, $K = k'[\alpha_2, \ldots, \alpha_n]$ and by induction we can assume that K is algebraic over k'. By Exercise 2.1, it is enough to see that α_1 is algebraic over k.

Since the α_i are algebraic over k', there is a non-zero polynomial $g \in k[X]$ such that $g(\alpha_1) \neq 0$ and such that the products $g(\alpha_1)\,\alpha_i$ $(i = 2, \ldots, n)$ are integral over the ring $k[\alpha_1]$. Hence,

$$\forall\, \xi \in K,\ \exists\, \rho = \rho(\xi) \text{ such that } g(\alpha_1)^\rho\, \xi \text{ is integral over } k[\alpha_1]. \tag{5.2.1}$$

Indeed, each element $\xi \in K$ can be written as a polynomial expression $\xi = f(\alpha_1, \ldots, \alpha_n)$ with coefficients in k, and multiplying by a large enough power of $g(\alpha_1)$, we reduce considerations to sums and products of elements integral over $k[\alpha_1]$.

This assertion is valid in particular for every element $\xi \in k'$. But if α_1 were transcendental over k, we would have $k[\alpha_1] \cong k[X]$, which is integrally closed. So we would have:

$$\forall\, \xi \in k' = k(\alpha_1),\ \exists\, \rho = \rho(\xi) \text{ such that } g(\alpha_1)^\rho\, \xi \in k[\alpha_1]. \tag{5.2.2}$$

This is absurd; to see this, it suffices to consider $\xi = \frac{1}{p(\alpha_1)}$, where p is an irreducible polynomial not dividing g. (Such a polynomial exists, because if there were only a finite number of irreducible polynomials $p_1, \ldots, p_M$, it would suffice to consider the irreducible factors of $1 + p_1 \cdot \cdots \cdot p_M$ to find one more.) □

It follows from this proposition that the field $K = k[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite algebraic extension of k. By Corollary 3.1.12, there is a k-embedding $\varphi : K \hookrightarrow \bar{k}$. We set $\alpha_i = \varphi(\pi(X_i))$; then, $P = (\alpha_1, \ldots, \alpha_n)$ belongs to $\mathbf{A}_k^n$ and is a point of $Y(\bar{k})$. Indeed, we have: $f(\alpha_1, \ldots, \alpha_n) = f\big(\varphi \circ \pi(X_1), \ldots, \varphi \circ \pi(X_n)\big) = \varphi \circ \pi(f) = 0$ for all $f \in \mathfrak{m}$. □

5.3 Hilbert's Nullstellensatz

Let us recall a well-known notion of commutative algebra.

Definition 5.3.1. The *radical* of an ideal $\mathfrak{a} \subset A$ is the ideal

$$\mathrm{rad}(\mathfrak{a}) = \big\{\, f \in A \mid \exists\, m > 0 \text{ such that } f^m \in \mathfrak{a} \big\}.$$

One easily verifies that $\mathrm{rad}(\mathfrak{a})$ is an ideal; in particular, if $f_1^\ell \in \mathfrak{a}$ and $f_2^m \in \mathfrak{a}$, on expanding the expression we see that $(f_1 + f_2)^{\ell+m-1} \in \mathfrak{a}$. We always have $\mathfrak{a} \subset \mathrm{rad}(\mathfrak{a})$ and, if $\mathfrak{p}$ is prime, $\mathrm{rad}(\mathfrak{p}) = \mathfrak{p}$. For ideals $\mathfrak{a}$ in the ring $A = k[X_1, \ldots, X_n]$, we obviously have $V(\mathfrak{a}) = V(\mathrm{rad}(\mathfrak{a})) \subset \mathbf{A}_k^n$.

Proposition 5.3.2. $\mathrm{rad}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$, *where* $\mathfrak{p}$ *runs through the prime ideals containing* $\mathfrak{a}$.

Proof. If $f \in \mathrm{rad}(\mathfrak{a})$, there is an integer $m > 0$ such that $f^m \in \mathfrak{a}$. Hence, $f^m \in \mathfrak{p}$ for every prime ideal $\mathfrak{p} \supset \mathfrak{a}$, which implies that $f \in \mathfrak{p}$ for all $\mathfrak{p} \supset \mathfrak{a}$.

If $f \notin \mathrm{rad}(\mathfrak{a})$, we have $f^m \notin \mathfrak{a}$ for all $m > 0$. Consider the set $\Sigma = \{\mathfrak{b} \subset A \mid \mathfrak{b} \supset \mathfrak{a} \text{ and } \forall\, m > 0,\ f^m \notin \mathfrak{b}\}$. We have $\Sigma \neq \emptyset$, since $\mathfrak{a} \in \Sigma$; this set is ordered inductively. By Zorn's Lemma, Σ has a maximal element $\mathfrak{p}$. Since $\mathfrak{p} \in \Sigma$, we have $f = f^1 \notin \mathfrak{p}$. Moreover, the ideal $\mathfrak{p}$ is necessarily prime, because if $x, y \notin \mathfrak{p}$, the maximality of $\mathfrak{p}$ in Σ implies that $\exists\, \ell > 0$ such that $f^\ell \in \mathfrak{p} + (x)$ and $\exists\, m > 0$ such that $f^m \in \mathfrak{p} + (y)$. In this case, $xy \in \mathfrak{p} \implies f^{\ell+m} \in \mathfrak{p}$, which would contradict the fact that $\mathfrak{p}$ belongs to Σ. □

A particular case frequently encountered is the *nilradical* of A: this is the ideal $\mathfrak{N} = \mathrm{rad}(0)$, which is therefore at the same time the set of nilpotent elements and the intersection of all prime ideals of the ring A.

Theorem 5.3.3 (Nullstellensatz). *Let* $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ *be an ideal. Then,* $I(V(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$.

Proof. Hilbert proved this result in a 60-page paper: *Math. Ann. 42* (1893), 313–373. Later, Rabinowitsch showed in a one-page paper (*Math. Ann. 102* (1929), 520) that this theorem is an immediate consequence of the weak theorem! The argument[1] is the following.

The inclusion $\mathrm{rad}(\mathfrak{a}) \subset I(V(\mathfrak{a}))$ being obvious, let $f \in k[X_1, \ldots, X_n]$ be a non-zero element such that $f(V(\mathfrak{a})) = 0$. We shall show that $f \in \mathrm{rad}(\mathfrak{a})$. Let us write $\mathfrak{a} = (f_1, \ldots, f_r)$ and introduce a new indeterminate X_0. If we consider the ideal $\mathfrak{I} = (f_1, \ldots, f_r, 1 - X_0 f) \subset k[X_0, X_1, \ldots, X_n]$, we trivially observe that $V(\mathfrak{I}) \subset \mathbf{A}_k^{n+1}$ is the empty set!

Hence, $\mathfrak{I} = (1)$; otherwise, the ideal $\mathfrak{I}$ would be contained in a maximal ideal $\mathfrak{m} \subset k[X_0, X_1, \ldots, X_n]$ and, by Theorem 5.2.1, we would have $V(\mathfrak{I}) \supset V(\mathfrak{m}) \neq \emptyset$. Consequently, there exist polynomials $b_i \in k[X_0, X_1, \ldots, X_n]$ such that

$$1 = b_1(X_0, \ldots, X_n)\, f_1(X_1, \ldots, X_n) + \cdots + b_r(X_0, \ldots, X_n)\, f_r(X_1, \ldots, X_n) + b_0(X_0, \ldots, X_n)\big(1 - X_0\, f(X_1, \ldots, X_n)\big).$$

[1] This is often called *Rabinowitsch's trick.*

This polynomial identity remains valid, in the field of fractions of $k[X_1, \ldots, X_n]$, when we replace X_0 by $\frac{1}{f(X_1, \ldots, X_n)}$. On multiplying by a suitable power of f, we eliminate denominators and obtain a relation of the form

$$f^m = a_1 f_1 + \cdots + a_r f_r \quad \text{in } k[X_1, \ldots, X_n].$$

Hence, $f \in \mathrm{rad}(\mathfrak{a})$. □

Corollary 5.3.4. *Let $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ be a prime ideal. Then, $I(V(\mathfrak{p})) = \mathfrak{p}$. In particular, $V(\mathfrak{p}) \neq \emptyset$ and $V(\mathfrak{p})$ is irreducible.*

Proof. Irreducibility follows from Proposition 2.4.9. □

Corollary 5.3.5. *There is a one-to-one correspondence between the algebraic subsets of $\mathbf{A}_k^n$ and the ideals of $k[X_1, \ldots, X_n]$, which coincide with their radical. This correspondence is given by: $Y \mapsto I(Y)$ and $\mathfrak{a} \mapsto V(\mathfrak{a})$. It reverses inclusions.*

Proof. If $\mathfrak{a} = I(Y)$, we trivially have $\mathfrak{a} = \mathrm{rad}(\mathfrak{a})$. On the other hand, these maps are the inverse of one another, for $V(I(Y)) = \overline{Y} = Y$ (Lemma 2.3.9) and $I(V(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a}) = \mathfrak{a}$, by the theorem. □

There are obvious enough versions of the Nullstellensatz for subvarieties of a given affine variety (see Proposition 5.4.2). As for the projective version, it is rarely used; we recall it here.

Corollary 5.3.6 (Projective Nullstellensatz). *Let $\mathfrak{a} \subset k[X_0, \ldots, X_n]$ be a homogenous ideal; let $\mathfrak{m} = (X_0, \ldots, X_n)$ be the irrelevant maximal ideal. Then:*

(i) $V(\mathfrak{a}) = \emptyset \iff \exists\, N > 0$ *such that* $\mathfrak{a} \supset \mathfrak{m}^N$;
(ii) *If* $V(\mathfrak{a}) \neq \emptyset$, *then* $I(V(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$.

Proof. If $V(\mathfrak{a}) \subset \mathbf{P}_k^n$ is empty, the affine algebraic subset $V^{\mathrm{aff}}(\mathfrak{a}) \subset \mathbf{A}_k^{n+1}$ defined by the same ideal is contained in $Y_0 = \{(0, \ldots, 0)\}$. Theorem 5.3.3 then implies that $\mathrm{rad}(\mathfrak{a}) = I(V^{\mathrm{aff}}(\mathfrak{a})) \supset I(Y_0) = \mathfrak{m}$. Consequently, all X_i have a power X_i^M contained in the ideal $\mathfrak{a}$, and it suffices to take $N = (n+1)M$ to obtain the result.

If $V(\mathfrak{a}) \neq \emptyset$, the affine cone $V^{\mathrm{aff}}(\mathfrak{a})$ is not contained in Y_0, and since $\mathfrak{a}$ is a homogenous ideal, one verifies that $I(V(\mathfrak{a})) = I(V^{\mathrm{aff}}(\mathfrak{a}))$, hence the result. □

5.4 Equivalence of Categories

If $Y \subset \mathbf{A}_k^n$ is an affine variety, we recall (Definition 4.2.1) that its *coordinate ring* is the ring $k[Y] = k[X_1, \ldots, X_n]/I(Y)$. This is a Nœtherian ring, but more importantly a *reduced* (i.e., without nilpotent elements) k-algebra of finite type.

Example 5.4.1. If $Y = \{+i, -i\} \subset \mathbf{A}_{\mathbf{R}}^1$, we have $\mathbf{R}[Y] = \mathbf{R}[X]/(X^2 + 1) \cong \mathbf{C}$.

If $Y = V(X_1X_2 - 1) \subset \mathbf{A}_k^2$, we have $k[Y] = k[X_1, X_2]/(X_1X_2 - 1) \cong k[X_1, X_1^{-1}]$; these are the Laurent polynomials.

The next result seals the unity of algebra and arithmetic with geometry.

Proposition 5.4.2.

(a) *$k[Y]$ is a reduced k-algebra of finite type. It is integral if and only if Y is irreducible. There is a one-to-one correspondence between the subvarieties of Y and the ideals of $k[Y]$, which coincide with their radical.*
(b) *Conversely, every reduced k-algebra A of finite type is the coordinate ring of a variety Y.*

Proof.

(a) Let $\pi : k[X_1, \ldots, X_n] \to k[Y]$ be the canonical projection. The correspondence is defined by $\varphi : Z \mapsto I(Z)/I(Y)$ and $\psi : \mathfrak{b} \mapsto V(\pi^{-1}(\mathfrak{b}))$. Since π is surjective, the map φ associates with each subvariety Z of Y an ideal of $k[Y]$, and this ideal is trivially equal to its radical. As for ψ, this map associates with each ideal $\mathfrak{b}$ of $k[Y]$, which coincides with its radical a closed subset of Y, since $V(\pi^{-1}(\mathfrak{b})) \subset V(\pi^{-1}(0)) = V(I(Y)) = Y$. These two maps are the inverse of one another, for $\varphi \circ \psi(\mathfrak{b}) = \pi(I(V(\pi^{-1}(\mathfrak{b})))) = \pi(\mathrm{rad}(\pi^{-1}(\mathfrak{b}))) = \pi(\pi^{-1}(\mathrm{rad}(\mathfrak{b}))) = \mathrm{rad}(\mathfrak{b}) = \mathfrak{b}$ (since π is surjective) and $\psi \circ \varphi(Z) = V(\pi^{-1}(I(Z)/I(Y))) = V(I(Z)) = \overline{Z} = Z$ (car $I(Y) \subset I(Z) \implies \pi^{-1}(I(Z)/I(Y)) = I(Z)$).
(b) A k-algebra of finite type, generated by elements $\alpha_1, \ldots, \alpha_n$, can be written $k \hookrightarrow A = k[\alpha_1, \ldots, \alpha_n]$. There is then a commutative diagram

$$\begin{array}{ccc} & k & \\ & \swarrow \quad \searrow & \\ k[X_1, \ldots, X_n] & \xrightarrow{\varphi} & \!\!\!\!\longrightarrow\!\!\!\!\!\rightarrow A\,, \end{array}$$

where φ is a surjective k-homomorphism defined by $\varphi : X_i \mapsto \alpha_i$. Consequently, $A \cong k[X_1, \ldots, X_n]/\ker\varphi$. We set $Y = V(\ker\varphi) \subset \mathbf{A}_k^n$, and it suffices to verify that $k[Y] = A$. But this follows immediately from $\ker\varphi = I(Y)$. Indeed, $I(Y) = I(V(\ker\varphi)) = \mathrm{rad}(\ker\varphi) = \ker\varphi$, since by hypothesis A has no nilpotent elements. □

As seen in Definition 4.2.1, an element of $k[Y]$ may be conceived as a polynomial function $f : Y \to \mathbf{A}_k^1$. In fact, affine varieties form a category if one defines morphisms more generally as follows.

Definition 5.4.3. Let $Y \subset \mathbf{A}_k^n$ and $Z \subset \mathbf{A}_k^m$ be two affine algebraic varieties. A *morphism* of Y into Z is a polynomial map $f : Y \to Z$, which means that there are polynomials $F_1, \ldots, F_m$ in $k[X_1, \ldots, X_n]$ such that

$$\forall\, P \in Y, \quad f(P) = (F_1(P), \ldots, F_m(P)) \in Z. \tag{5.4.1}$$

Example 5.4.4. If $Y = \mathbf{A}_k^1$ and $Z = V(X_1^3 + X_1^2 - X_2^2) \subset \mathbf{A}_k^2$ (the strophoid in Figure 1.4), there is a morphism of Y into Z given by the parametrization (1.2.1), $f : t \mapsto (t^2 - 1, t^3 - t)$.

If $k = \mathbf{F}_p$ and $Y = Z = \mathbf{A}_k^n$, there is a *Frobenius morphism*

$$f : (X_1, \ldots, X_n) \mapsto (X_1^p, \ldots, X_n^p).$$

This is a bijection, and even a homeomorphism in the Zariski topology, but f is obviously not an isomorphism, since its differential is identically zero. The fixed points of f are the points of $\mathbf{A}_k^n$ with coordinates in k.

Remark 5.4.5. The morphisms $f : Y \to Z$ are continuous maps in the Zariski topology: the inverse image of a closed set $V(\mathfrak{b}) \subset Z$ is of the form $f^{-1}(V(\mathfrak{b})) = \{P \in Y \mid g \circ f(P) = 0 \ \forall\, g \in \mathfrak{b}\} = V(\mathfrak{b} \circ f)$.

The morphisms of Y into $\mathbf{A}_k^1$ are all elements of $k[Y]$. A morphism $f : Y \to Z$ therefore induces a k-homomorphism

$$f^* : k[Z] \to k[Y],$$

defined by $f^*(g) = g \circ f$. One easily verifies that f^* is a homomorphism of k-algebras. This correspondence is functorial, for

$$f_1^*(\, f_2^*(g)) = (g \circ f_2) \circ f_1 = g \circ (\, f_2 \circ f_1) = (\, f_2 \circ f_1)^*(g).$$

Example 5.4.6. If $Y = V(X_1X_2 - 1) \subset \mathbf{A}_k^2$, the morphism $f : Y \to \mathbf{A}_k^1$ given by the vertical projection $f : (X_1, X_2) \mapsto X_1$ corresponds to the embedding $f^* : k[X_1] \hookrightarrow k[X_1, X_1^{-1}]$ of polynomials into Laurent polynomials.[2]

See also Example 5.1.15 of the cissoid Γ and its normalization $\widetilde{\Gamma}$.

Theorem 5.4.7.

(a) *Let $Y \subset \mathbf{A}_k^n$ and $Z \subset \mathbf{A}_k^m$ be two affine algebraic varieties. There is a one-to-one correspondence between morphisms $f : Y \to Z$ and k-homomorphisms $f^* : k[Z] \to k[Y]$.*

(b) *The functor $f \rightsquigarrow f^*$, from the category of affine algebraic k-varieties into the category of reduced k-algebras of finite type, is an equivalence of categories.*

(c) *f^* is injective if and only if f is* dominant *(that is, if* Im$(\, f)$ *is dense in Z in the Zariski topology).*

(d) *If f^* is surjective, then f is injective, but not conversely.*

[2] We see that this morphism (which reminds us of *Rabinowitsch's trick*) allows us to define a structure of algebraic variety on the line minus one point, by isomorphism with the hyperbola.

Proof.

(a) Given a k-homomorphism $\varphi : k[Z] \to k[Y]$, we can construct a morphism $f : Y \to Z$ such that $f^* = \varphi$ in the following manner. We write $k[Z] = k[T_1, \ldots, T_m]/I(Z)$ and observe that the class $[T_i]$ of T_i is the i-th coordinate function $\kappa_i : Z \to \mathbf{A}^1_k$ $(i = 1, \ldots, m)$. We want to ensure that $\kappa_i \circ f = f^*(\kappa_i) = \varphi(\kappa_i)$, a condition that characterizes f completely.

Since by hypothesis the $\varphi(\kappa_i)$ are known, we construct the morphism f by choosing, for all $i = 1, \ldots, m$, a polynomial $F_i \in k[X_1, \ldots, X_n]$, which is a representative of $\varphi(\kappa_i)$ modulo $I(Y)$. We then set

$$f : P \mapsto \big(F_1(P), \ldots, F_m(P)\big),$$

which is of the form (5.4.1). Indeed, the image of f is contained in Z, because if $G \in k[T_1, \ldots, T_m]$ belongs to $I(Z)$, we have for all $P \in Y$:

$$G(f(P)) = G(F_1(P), \ldots, F_m(P)) = G(\varphi(\kappa_1), \ldots, \varphi(\kappa_m))(P)$$

and

$$\begin{aligned} G(\varphi(\kappa_1), \ldots, \varphi(\kappa_m)) &= \varphi(G(\kappa_1, \ldots, \kappa_m)) = \varphi(G([T_1], \ldots, [T_m])) \\ &= \varphi([G(T_1, \ldots, T_m)]) = \varphi(0) = 0 \end{aligned}$$

To see that $f^* = \varphi$, it suffices to verify that $f^*([T_i]) = \varphi([T_i])$, since f^* and φ are both k-algebra homomorphisms. Indeed, $f^*(\kappa_i) = \kappa_i \circ f = [F_i]_Y = \varphi(\kappa_i)$, où $[\ ]_Y$ denotes the class modulo $I(Y)$. The correspondence is one-to-one, because f (and also f^*) is characterized by the condition $\kappa_i \circ f = f^*(\kappa_i)$.

(b) Starting with $f : Y \to Z$, we obtain $\varphi = f^* : B \to A$, where $A = k[Y]$ and $B = k[Z]$. However, Y and Z are given as subvarieties of an affine space, whereas the algebras A and B are defined only up to isomorphism.

We also know (Proposition 5.4.2) that given two reduced k-algebras of finite type A and B, one can find two affine varieties Y_1 and Z_1, such that $A = k[Y_1]$ and $B = k[Z_1]$. If, moreover, we know a morphism of k-algebras $\varphi : B \to A$, there exists by (a) a morphism $f_1 : Y_1 \to Z_1$ satisfying ${f_1}^* = \varphi$.

Let Φ be the functor that associates f^* with f, and let Ψ be the functor that associates f_1 with φ. These two functors are not the inverse of one another, but they still define an equivalence of categories. In fact, $\Phi \circ \Psi = id$ and $\Psi \circ \Phi$ is *naturally isomorphic* to the identity.

(c) Let $g \in k[Z]$; then $f^*(g) = 0 \iff g \circ f(Y) = 0$, and this condition is equivalent to $g \in I(f(Y))/I(Z) = I(\overline{f(Y)})/I(Z)$, by Exercise 2.9. Hence, $\ker f^* = I(\overline{f(Y)})/I(Z)$, which is zero if and only if $\overline{f(Y)} = Z$.

(d) If $P \neq Q$ differ at their i-th coordinate $\kappa_i : Y \to \mathbf{A}^1_k$, let g be such that $f^*(g) = \kappa_i$. Then,

$$\kappa_i(P) \neq \kappa_i(Q) \implies g \circ f(P) \neq g \circ f(Q) \implies f(P) \neq f(Q).$$

Concerning the converse, a counter-example is given by the cissoid in Example 5.1.15, where the parametrization $f : \mathbf{A}^1_k \to \Gamma$ defined by $t \mapsto (t^2, t^3)$ is a bijection, whereas the morphism f^* is clearly injective, but not surjective (see Exercise 5.3). □

5.5 Local Properties

In arithmetic as well as in geometry, rational maps play a greater role than morphisms. These are maps defined only on a Zariski open set, but recall that non-empty open sets are dense in an irreducible space (Exercise 2.12).

Recall (Definition 4.2.2) that a function φ belonging to the function field $k(X)$ of an irreducible variety is called regular at $x \in X$ if there is a representation $\varphi = f/g$ with $f,\ g \in k[X]$ and $g(x) \neq 0$.

Since $V(g)$ is a closed subset of X, the function φ is regular on a whole neighborhood of x. There is therefore a non-empty open set $U \subset X$ on which φ is regular. Since X is irreducible, U is dense in X. Consequently, a definition that seems to be local at a point of a variety may also be read: "for almost all $x \in X$."

Definition 5.5.1. Let X and Y be two algebraic varieties. We assume that X is irreducible. *Rational map* $f : X \dashrightarrow Y$ is a morphism from a non-empty Zariski open set $U \subset X$ into Y.

In this definition, by *morphism* we mean a map that is regular at all points of the open set U. We can also define a rational map $f : X \dashrightarrow Y$ as an equivalence class of pairs (f_U, U), where $U \subset X$ is a non-empty open set and f_U a morphism from U into Y: two such pairs (f_U, U) and (f_V, V) are considered equivalents if f_U and f_V coincide on the intersection $U \cap V$. (Since X is assumed irreducible, this intersection is never empty and we do indeed obtain an equivalence relation.)

However, one must be aware that it is not always possible to compose two rational maps, so that these maps do not form a category. If, for instance Y has a greater dimension than X, the image of f is too small; a rational map $g : Y \to Z$ may very well be defined only on the complement of this image and then $g \circ f$ is not defined at any point of X.

Nevertheless, one obtains a category when restricting to *dominant* rational maps between irreducible varieties. The approach is quite simple: if X and Y are two affine varieties and if $f : X \to Y$ is a dominant morphism, Theorem 5.4.7 states that f^* is an injective morphism of k-algebras. In the more general case, when the varieties are not algebraic subsets of an affine space, or if f is only a rational map, definitions are local and involve the fields of fractions of the corresponding coordinate rings. One then obtains the following statement.

Proposition 5.5.2. *A rational dominant map $f : X \dashrightarrow Y$ between two irreducible varieties induces an embedding $f^* : k(Y) \hookrightarrow k(X)$.* □

Definition 5.5.3. Let X and Y be two irreducible algebraic varieties, and $f : X \dashrightarrow Y$ a rational map. We say that f is *birational* if it has an inverse $g : Y \dashrightarrow X$ in the same category. We also say that the varieties are *birationally equivalent* (over the field k).

This amounts to saying that there exist two non-empty Zariski open sets $U \subset X$ and $V \subset Y$, which are isomorphic. In this case, $k(X) \cong k(Y)$. We see that the central role belongs to the function fields of the varieties. The analogy with Theorem 5.4.7 is complete and one proves the following statement.

Proposition 5.5.4. *There is a functor $f \rightsquigarrow f^*$ from the category of projective irreducible k-varieties with rational dominant maps as morphisms, into the dual of the category of finitely generated extensions of the field k. This functor associates with each variety its function field and is an equivalence of categories.*

Example 5.5.5. If a smooth quadric $Q \subset \mathbf{P}^3_k$ has a k-rational line $L = \{X_2 = X_3 = 0\}$, we can consider the family of planes passing through L. A general plane π_λ in this family has equation $\lambda_0 X_3 = \lambda_1 X_2$, where $[\lambda_0 : \lambda_1] \in \mathbf{P}^1_k$. We shall write more simply $X_3 = \lambda X_2$ with $\lambda \in \mathbf{P}^1_k$. This amounts to setting $\lambda = \lambda_1/\lambda_0$ if $\lambda_0 \neq 0$ and to agree to write $\lambda = \infty$ for $\lambda_0 = 0$.

The intersection of Q with π_λ is the union of L and of a variable line D_λ defined in the plane π_λ by an equation whose coefficients are in the field $K = k(\lambda)$. This residual intersection D_λ is therefore isomorphic to $\mathbf{P}^1_K$.

This construction defines a *fibering* $f : Q \to \mathbf{P}^1_k$, which associates with each point $P \in D_\lambda$ the parameter $\lambda \in \mathbf{P}^1_k$. This map is well defined, even at the points of the line L, as in this case π_λ is the tangent plane to the quadric at P. Therefore, this map is a morphism from Q to $\mathbf{P}^1_k$.

However, one cannot describe f^* in terms of coordinate rings, since all the varieties involved are projective. The local definition of morphisms naturally leads us to using function fields. In fact, f is also a rational dominant map and Proposition 5.5.2 allows us to write an embedding $f^* : K = k(\lambda) = k(\mathbf{P}^1_k) \hookrightarrow k(Q)$. The *fiber* of f over $\lambda \in \mathbf{P}^1_k$ is the line D_λ. On the other hand, on substituting $\lambda = X_3/X_2$, the equation of Q over k is the same as that of D_λ over K. The field $k(Q)$ therefore coincides with $K(D_\lambda) = K(u)$, where u is transcendental over K. Hence, an isomorphism $k(Q) \cong K(u) = k(\lambda, u)$.

This shows that Q is birationally equivalent to $\mathbf{P}^2_k$, but this variety is not isomorphic to the projective plane, as we know that Q is isomorphic to the product $\mathbf{P}^1_k \times \mathbf{P}^1_k$ (see Exercise 4.9) and the two varieties $\mathbf{P}^1_k \times \mathbf{P}^1_k$ and $\mathbf{P}^2_k$ do not have the same Néron–Severi group (see §7.7): on $\mathbf{P}^1_k \times \mathbf{P}^1_k$ there are two infinite families of mutually skew lines; these lines should correspond to smooth curves of genus 0 in $\mathbf{P}^2_k$, but two such curves always have a non-empty intersection.

Example 5.5.6. Let $Y = V(g) \subset \mathbf{P}^n_k$ be an irreducible quadric such that $Y(k) \neq \emptyset$. By a k-linear change of variables, we may suppose without loss of generality that $Y(k)$ contains the point $P = [1 : 0 : \cdots : 0]$, so that g has no term in X_0^2. We can thus write $g = X_0\,\ell + q$, where $\ell(X_1, \ldots, X_n)$ is a linear form, and $q(X_1, \ldots, X_n)$

a quadratic form that is not a multiple of ℓ. We assume moreover that ℓ is not identically zero, which has the geometrical meaning that P is a non-singular point of the variety.

Making the stereographic projection from the point P on the hyperplane $\{X_0 = 0\}$, we obtain a rational map $\varphi : Y \dashrightarrow \mathbf{P}_k^{n-1}$

$$\varphi : y = [X_0 : \cdots : X_n] \mapsto x = [X_1 : \cdots : X_n].$$

In contrast to Example 4.2.6, if $n > 2$, this map is not defined at every point of Y. However, it is defined on the open complement to P; this is why it is a rational map. If $g = 0$, we can write $X_0\,\ell = -q$, which suggests defining $\psi : \mathbf{P}_k^{n-1} \dashrightarrow Y$ by the formula

$$x = [X_1 : \cdots : X_n] \mapsto y = [-q : X_1\,\ell : \cdots : X_n\,\ell].$$

One easily verifies that φ and ψ are inverses of another. This shows that *all irreducible hypersurfaces of degree* 2 *in* $\mathbf{P}_k^n$ *are birationally equivalent to* $\mathbf{P}_k^{n-1}$ *if they have at least a* k*-rational non-singular point.* The condition of having a rational point is obviously necessary (see in particular Lemma 5.5.12 below).

Another important local definition is the following.

Definition 5.5.7. Let $f \in k[X_1, \ldots, X_n]$, where k is a field. A point $(x_1, \ldots, x_n) \in \mathbf{A}_k^n$ is a *simple* zero of f if $f(x_1, \ldots, x_n) = 0$ and if there exists an index j such that $\frac{\partial f}{\partial X_j}(x_1, \ldots, x_n) \neq 0$. We also say that $P = (x_1, \ldots, x_n)$ is a *non-singular* point of the hypersurface $V(f) \subset \mathbf{A}_k^n$. In this case, the variety $V(f)$ has a *tangent hyperplane* at P, with equation $\sum_{j=1}^{n} \frac{\partial f}{\partial X_j}(x_1, \ldots, x_n)(X_j - x_j) = 0$.

There are of course definitions for more general varieties (regularity and the Jacobian criterion of singularity). We do not go into detail here.

Definition 5.5.8. A variety is *smooth* if all its points are non-singular.

Remark 5.5.9. One proves in algebraic geometry that the notion of a non-singular point is intrinsic. To illustrate this, we show that it is independent of the choice of a chart: if $P = (x_1, \ldots, x_n)$ is an affine chart of $\mathbf{P}_k^n$, we define $F = f^* = X_0^d\, f(X_1/X_0, \ldots, X_n/X_0)$ as in Exercise 4.2. Suppose for instance that $\frac{\partial F}{\partial X_1}(1, x_1, \ldots, x_n) = \frac{\partial f}{\partial X_1}(x_1, \ldots, x_n) \neq 0$, since in the chart $\{X_0 \neq 0\}$, the point P is non-singular. It is obvious that P remains non-singular in all the charts for which we can differentiate with respect to X_1. Finally, if $x_1 \neq 0$, the point P is also visible in the chart $\{X_1 \neq 0\}$, for which we cannot differentiate with respect to X_1, but for which P is still non-singular. Indeed, since F is homogenous of degree d, we have Euler's relation:

$$0 = d \cdot F(1, x_1, \ldots, x_n) = \frac{\partial F}{\partial X_0}(1, x_1, \ldots, x_n) + \sum_{i \geq 1} x_i \frac{\partial F}{\partial X_i}(1, x_1, \ldots, x_n).$$

This implies that there is an index $j \neq 1$ such that $\frac{\partial F}{\partial X_j}(1, x_1, \ldots, x_n) \neq 0$.

Definition 5.5.10. A variety X is a *model* of a variety Y if X and Y are birationally equivalent (over their field of definition). We say that X is a *smooth model* if all its points are non-singular.

Definition 5.5.11. An irreducible variety Y defined over k is *k-rational* if it is birationally equivalent (over the field k) to a projective space $\mathbf{P}_k^d$, that is, if its function field $k(Y)$ is isomorphic to $k(u_1, \ldots, u_d)$. This is the same as saying that $\mathbf{P}_k^d$ is a model of Y in the sense of the above definition.

If an arbitrary smooth model of Y has a k-rational point, so does every projective model of Y, as follows from Nishimura's Lemma.

Lemma 5.5.12 (Nishimura). *Let k be a field, X an irreducible k-variety, Y a projective k-variety, and $f : X \dashrightarrow Y$ a rational map defined over k. If $X(k)$ contains a non-singular point, then $Y(k) \neq \emptyset$.*

Proof. We may assume X to be embedded in an affine space. Let $P \in X(k)$ be the given non-singular point. There is a linear subspace H (an intersection of hyperplanes) that cuts X transversely at P, such that $X \cap H$ is a curve C non-singular at P. The map f may not be defined globally, but its restriction g to the curve C is a morphism (see [Sh], Chap. II, §3, Cor. 1 to Theorem 3) and the image of P is a point $g(P) \in Y(k)$. To ensure the existence of this image, an essential requirement is that Y should be a complete variety. □

Corollary 5.5.13. *The condition $X(k) \neq \emptyset$ is a k-birational invariant of smooth projective varieties.* □

Exercises

5.1. Let $K/\mathbf{Q}$ be an extension of degree 2. There exists $d \in \mathbf{Z}$ square-free, such that $K = \mathbf{Q}(\sqrt{d})$. Let $\mathcal{O}_K \subset K$ be the integral closure of $\mathbf{Z}$ in K. Show that

$$\mathcal{O}_K = \begin{cases} \mathbf{Z} \oplus \mathbf{Z}\sqrt{d} & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \\ \mathbf{Z} \oplus \mathbf{Z}\frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

5.2. Let k be a field of characteristic $\neq 2$. Show that the coordinate ring of a curve with equation $y^2 = f(x)$, where $f \in k[x]$ has distinct roots, is integrally closed.

5.3. Let $Y = V(y^2 - x^3) \subset \mathbf{A}^2_k$. Show that the cissoid Y is irreducible and that its coordinate ring is not factorial. Deduce that Y is not isomorphic to $\mathbf{A}^1_k$, although their topological spaces are homeomorphic (see Exercise 1.3).

5.4. Let A be a factorial ring and let $\mathfrak{p} \subset A$ be a prime ideal, which is minimal in the family of non-zero prime ideals. Show that $\mathfrak{p}$ is principal.

5.5. Let $Y \subsetneq \mathbf{A}^n_k$ be an algebraic subset. Show that Y is a maximal irreducible subvariety of $\mathbf{A}^n_k$ (among irreducible subvarieties different from $\mathbf{A}^n_k$) if and only if there is an irreducible polynomial $f \in k[X_1, \ldots, X_n]$ such that $Y = V(f)$.

5.6. (Euler) Let $Y \subset \mathbf{A}^3_{\mathbf{Q}}$ be the cubic surface with equation

$$x_1^3 + x_2^3 + x_3^3 = 1. \qquad (*)$$

Also, let $Q \subset \mathbf{A}^3_{\mathbf{Q}}$ be the quadric with equation $(x_1 + x_2)x_3 - x_1 + 2x_2 = 0$. Finally, consider the two conjugate lines $L_i = \{x_3 = \rho^i\,;\ x_2 = -\rho^i x_1\}$ $(i = 1, 2)$, where ρ is a primitive cubic root of unity. Show that the intersection $Y \cap Q$ contains L_1, L_2 and the curve, which is the image of the morphism $\varphi : \mathbf{A}^1_{\mathbf{Q}} \to \mathbf{A}^3_{\mathbf{Q}}$ defined by

$$t \mapsto (-9t^4 - 3t,\ 9t^4,\ 9t^3 + 1).$$

(This parametrization proves the existence of an infinity of integer solutions for the equation $(*)$, such as $(-12)^3 + 9^3 + 10^3 = 1$, etc.)

5.7. (Carmichael, 1915) Find a parametric solution over $\mathbf{Q}$ for the equation $x^4 + y^4 + z^4 = 2$.
(*Hint:* cut the surface $V(x^4 + y^4 + z^4 - 2) \subset \mathbf{A}^3_{\mathbf{Q}}$ by the plane $V(x + y - z)$. Show that the intersection is a reducible curve. Parametrize the component that has $\mathbf{Q}$-rational points.)

5.8. (Fermat's curve) Show that if $n \geq 3$, one cannot find two *non-constant* rational fractions $\varphi(t),\ \psi(t) \in \mathbf{C}(t)$ such that $\varphi(t)^n + \psi(t)^n = 1$ identically.
(*Hint:* one can reduce to the case of polynomials $p, q, r \in \mathbf{C}[t]$ satisfying $p(t)^n + q(t)^n - r(t)^n = 0$ identically. Calculate the derivative of this expression, interpret the result as a system of linear equations in the variables p^{n-1}, q^{n-1}, and r^{n-1}, and then proceed by elimination.)

5.9. Show that in the ring $A = \mathbf{Z}[\sqrt{-5}] = \mathbf{Z}[X]/(X^2 + 5)$, the number 2 divides the product $(1 + \sqrt{-5})(1 - \sqrt{-5})$, but none of the factors. Deduce that (2) is not a prime ideal in this ring. Is the ideal $(1 + \sqrt{-5}) \subset A$ prime? Is the ring A factorial?

5.10. Let $A = \mathbf{C}[X_1, X_2]/(X_1^2 + X_2^2 - 1)$ and let x_1 and x_2 be the classes of X_1 and X_2 respectively. Show that the ideal $\mathfrak{m} = (x_2, 1 - x_1) \subset A$ is principal, generated by $(x_1 + i\,x_2 - 1)$.

5.11. Let $A = \mathbf{Q}[X_1, X_2]/(X_1^2 + X_2^2 - 1)$ and let x_1 and x_2 be the classes of X_1 and X_2 respectively. Show that $x_2^2 = (1 - x_1)(1 + x_1)$ and that the ideal $(x_2) \subset A$ is therefore not prime. Show also that the ideal $\mathfrak{m} = (x_2, 1 - x_1) \subset A$ is not principal.

Chapter 6
Euclidean Rings

We have seen the important role that factorial rings play in algebraic geometry (see in particular the exercises in the previous chapter). It is natural to be interested in Euclid's division algorithm too, which has given rise to some impressive works. On formalizing the notion of the *Euclidean ring*, unexpected algorithms, revealed by new methods, have recently been discovered. There are also connections to several old unsolved conjectures.

6.1 Euclidean Norms

Definition 6.1.1. An integral domain A is called *Euclidean* if it possesses a *Euclidean division algorithm*, that is, if there is a function $\varphi : A \to \mathbf{N}$ (called a *Euclidean norm*) such that

$$\forall\, a,\ b \in A,\ a \neq 0,\ \exists\, q,\ r \in A \text{ with } b = a\,q + r \text{ and } \varphi(r) < \varphi(a).$$

Example 6.1.2. $A = \mathbf{Z}$ is Euclidean for the norm $\varphi(a) = |a|$. Indeed, if a if b are positive, we can subtract a from b repeatedly and find an integer $q \in \mathbf{N}$ such that $0 \leq b - aq < a$. From this we easily deduce the other cases, when a or b is negative.

Note that the numbers q and r are not unique; for instance, if $a = 3$ and $b = 7$, we can equally take $q = 2$ with $r = 1$ or $q = 3$ with $r = -2$. In each case, $b \equiv r \mod a$.

Lemma 6.1.3. *$\varphi(0) < \varphi(a)$ for all $a \neq 0$.*

Proof. For $a \neq 0$, there exist q and a_1 in A such that $0 = a\,q + a_1$ and $\varphi(a_1) < \varphi(a)$. If $a_1 \neq 0$ we can write $0 = a_1\,q_1 + a_2$ with $\varphi(a_2) < \varphi(a_1)$, and so on, $0 = a_{n-1}\,q_{n-1} + a_n$ with $\varphi(a_n) < \varphi(a_{n-1})$. But a decreasing sequence of positive

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_6

integers cannot be infinite; therefore, there is an integer $n \geq 1$ such that $a_n = 0$. Then, $\varphi(0) = \varphi(a_n) < \cdots < \varphi(a)$. □

We denote by A^* the group of invertible elements of the ring A (the *units*).

Lemma 6.1.4. *If $a \in A \setminus \{0\}$ is such that $\varphi(a)$ is the smallest element of $\varphi(A \setminus \{0\})$, then $a \in A^*$.*

Proof. Dividing 1 by a, we find $1 = a\,q + r$ with $\varphi(r) < \varphi(a)$. This implies that $r = 0$ and that a is invertible. □

The converse is obviously false: for instance, a field A is a Euclidean ring for any map $\varphi : A \to \mathbf{N}$ such that $\varphi(a) > 0 \iff a \neq 0$, whereas the elements of $A \setminus \{0\}$ are all units.

Proposition 6.1.5. *A Euclidean ring is principal.*

Proof. Let $\mathfrak{a} \neq (0)$ be an ideal of the ring A; let $S = \{\varphi(x) \mid x \in \mathfrak{a},\ x \neq 0\} \subset \mathbf{N}$. Let $a \in \mathfrak{a}$ be a non-zero element such that $\varphi(a)$ is the smallest element of S. We show that $\mathfrak{a} = (a)$. Let $b \in \mathfrak{a}$; it can be written as $b = a\,q + r$ with $\varphi(r) < \varphi(a)$; hence, $\varphi(r) \notin S$. But then $r = 0$, for $r = b - a\,q \in \mathfrak{a}$. Therefore, $b \in (a)$. □

Example 6.1.6. The polynomial ring $A = k[X]$ over a field k is Euclidean for the norm $\varphi(a) = 1 + \deg a$ for $a \neq 0$, if we agree that $\varphi(0) = 0$. Indeed, one can perform reminder division over any ring k, when the divisor a has leading coefficient 1. If k is a field, we reduce to that case by multiplying a by the inverse of its leading coefficient. If k is not a field, for example, if $k = \mathbf{Z}$, this method does not work; in fact, $k[X]$ is Euclidean only if k is a field. Indeed, if $k[X]$ is Euclidean, it is also principal (Proposition 6.1.5); then, since $k \subset k[X]$ is an integral domain, the ideal $(X) \subset k[X]$ is prime, and hence maximal; therefore, $k \approx k[X]/(X)$ is a field.

Proposition 6.1.7. *Given a Euclidean division algorithm φ on A, one can define a new algorithm $\widetilde{\varphi}$ by the property*

$$\widetilde{\varphi}(a) = \min\{\varphi(ac) \mid c \in A \setminus \{0\}\}\,.$$

We then have $\widetilde{\varphi}(b) \geq \widetilde{\varphi}(a)$ if $b \neq 0$ is a multiple of a.

Proof. Let us first show that $\widetilde{\varphi}$ is indeed a Euclidean division algorithm on A. Let $a,\ b \in A$, $a \neq 0$; then there exists $c \in A \setminus \{0\}$ such that $\widetilde{\varphi}(a) = \varphi(ac)$. Since A is Euclidean for the norm φ, there exist q and r in A such that $b = (ac)\,q + r$ with $\varphi(r) < \varphi(ac)$. Hence, $b = a(cq) + r$ with $\widetilde{\varphi}(r) \leq \varphi(r) < \varphi(ac) = \widetilde{\varphi}(a)$.

It is also clear that if $b = ad \neq 0$, we have: $\widetilde{\varphi}(b) = \widetilde{\varphi}(ad) = \min\{\varphi(c) \mid c \in (ad),\ c \neq 0\} \geq \min\{\varphi(c) \mid c \in (a),\ c \neq 0\} = \widetilde{\varphi}(a)$. □

Corollary 6.1.8. *The function $\widetilde{\varphi}$ also satisfies: $\widetilde{\varphi}(a) < \widetilde{\varphi}(b)$ if a divides $b \neq 0$, without b dividing a.*

Proof. Given $b = ac$, we can write $a = bq + r$ with $\widetilde{\varphi}(r) < \widetilde{\varphi}(b)$. If $r = 0$, then b divides a. We may thus assume that $r = a(1 - cq) \neq 0$; then, $\widetilde{\varphi}(a) \leq \widetilde{\varphi}(r) < \widetilde{\varphi}(b)$. □

Remark 6.1.9. It follows from Lemma 6.1.3 that one can replace φ by $\varphi_0 = \varphi - \varphi(0)$, which satisfies $\varphi_0(0) = 0$. Applying Proposition 6.1.7 and Corollary 6.1.8 to $\widetilde{\varphi_0}$, one can even find a Euclidean division algorithm $\psi : A \to \mathbf{N}$ with the following properties:

1. $\psi(0) = 0$;
2. $\psi(A^*) = 1$;
3. $\psi(b) \geq \psi(a)$ if $b \neq 0$ is a multiple of a.

For all $a \neq 0$, $\psi(a) > 0$ (Lemma 6.1.3). The value 1 is taken by ψ precisely on the units of A (Lemma 6.1.4). Property 3 obviously entails that if a and b define the same ideal, then $\psi(a) = \psi(b)$.

Definition 6.1.10. A Euclidean division algorithm having the three properties above is called a *normalized Euclidean algorithm*.

Definition 6.1.11. A Euclidean division algorithm is called *multiplicative* if $\psi(ab) = \psi(a)\,\psi(b)$ for all $a,\ b \in A$.

Such an algorithm is always normalized.

Example 6.1.12. For the polynomial ring $A = k[X]$ (Example 6.1.6), one can define $\psi(a) = 2^{\deg a}$ for $a \neq 0$ and $\psi(0) = 0$. Then, ψ is a multiplicative algorithm.

Classically, one denotes by $\mathcal{O}_K$ *ring of integers* of a number field (Definition 2.1.10), that is the integral closure of $\mathbf{Z}$ in K, where K is a finite extension of $\mathbf{Q}$ (see Comment 5.1.14). We know that $\mathcal{O}_K$ is an integrally closed ring (actually a *Dedekind ring*) and we consider the function $\psi : \mathcal{O}_K \to \mathbf{N}$ given by the absolute value of the Galois norm (relatively to $K/\mathbf{Q}$): $\psi = \left|N_{K/\mathbf{Q}}\right|$ (Definition 3.2.1). This function is multiplicative, but cannot be a Euclidean norm, unless $\mathcal{O}_K$ is principal (Proposition 6.1.5).

Of course, this condition is not a priori sufficient and there are rings $\mathcal{O}_K$ that are principal but for which ψ is not a Euclidean norm (see Exercise 6.1).

6.2 Imaginary Quadratic Fields

For $d \in \mathbf{Z}$ square-free, define

$$\delta = \begin{cases} \sqrt{d} & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

We have seen (Exercise 5.1) that the set $\mathcal{O}_d = \{\alpha = m + n\delta \mid m, n \in \mathbf{Z}\}$ is the integral closure of $\mathbf{Z}$ in $K = \mathbf{Q}(\sqrt{d})$.

For $d < 0$, one can view $\mathcal{O}_d$ as a *lattice* $\Lambda \subset \mathbf{C}$, that is, a discrete subgroup of $\mathbf{C}$ that generates $\mathbf{C}$ as a $\mathbf{R}$-vector space.

Lemma 6.2.1. *If $d < 0$, the ring $\mathcal{O}_d$ is Euclidean, with a Euclidean norm $\psi = \left|N_{K/\mathbf{Q}}\right| : \alpha \mapsto |\alpha|^2$ if and only if the translates of the open unit disc by vectors of Λ cover all points of $K \subset \mathbf{C}$.*

Proof. Let $\alpha, \beta \in \mathcal{O}_d$ with $\alpha \neq 0$; then, $z = \beta/\alpha \in K$. If there is an element $q \in \Lambda = \mathcal{O}_d$ such that the unit disk centered at q contains z, that is $|z - q| < 1$, then $\gamma = (z - q)\,\alpha$ verifies $\gamma = \beta - \alpha\, q \in \mathcal{O}_d$ and $\psi(\gamma) = |z - q|^2 \cdot |\alpha|^2 < \psi(\alpha)$. Consequently, $\mathcal{O}_d$ is Euclidean for this norm.

Conversely, if $\mathcal{O}_d$ is Euclidean for the norm ψ and if $z = \beta/\alpha \in K$, one can divide, with remainder, $\beta = \alpha\, q + \gamma$, and $\psi(\gamma) < \psi(\alpha)$ implies that $|\beta - \alpha\, q| < |\alpha|$; hence, $|z - q| < 1$. □

Corollary 6.2.2. *If $d < 0$, the ring $\mathcal{O}_d$ is Euclidean with Euclidean norm $\psi = \left|N_{K/\mathbf{Q}}\right| : \alpha \mapsto |\alpha|^2$ if and only if $d = -1,\ -2,\ -3,\ -7$ or -11.*

Proof. Consider the parallelogram $\Delta \subset \mathbf{C}$ with vertices 0, 1, δ, and $1 + \delta$. This is a *fundamental domain* for the action of Λ by translation on $\mathbf{C}$: each element of the plane has a representative in this parallelogram (and this representative is even unique for the interior points). Its height is $h = \operatorname{Im}\delta = \sqrt{|d|}/\mu$, where $\mu = 1$ if $d \equiv 2$ or $3 \pmod 4$ (first case) and $\mu = 2$ if $d \equiv 1 \pmod 4$ (second case). If $h \geq 2$, the open unit disks centered at the vertices of Δ cannot cover the points on the vertical axis, comprised between i and $(h - 1)\, i$. Lemma 6.2.1 then shows that $\mathcal{O}_d$ is not Euclidean for the norm. This covers the cases $|d| \geq 4$ if $\mu = 1$ and $|d| \geq 16$ if $\mu = 2$.

Therefore, the ring $\mathcal{O}_d$ can be Euclidean for the norm only if $d = -1,\ -2,\ -3,\ -7,\ -11$, or -15. But $d = -15$ is excluded, because in that case the points having the abscissa $\frac{1}{2}$ and the ordinate between $\frac{1}{2}\sqrt{3}$ and $h - 1 = \frac{1}{2}\sqrt{15} - 1$ are not covered by the unit disks centered at the vertices of the parallelogram (Figure 6.1).

In fact, the half-disks centered at real integer points cover the entire space between the horizontal axis and the line with equation $y = \frac{1}{2}\sqrt{3}$. Now, the center of Δ has ordinate $y = \frac{h}{2}$. If $\sqrt{3} > h$, the lower half of the parallelogram is entirely covered, that is, if $3 > |d|$ in the first case and $12 > |d|$ in the second. This deals with the cases $d = -1,\ -2$ and $d = -3,\ -7$, and -11. The other points of Δ are in the interior of the unit disks centered at δ and $1 + \delta$ respectively. The condition of Lemma 6.2.1 is satisfied. □

Lemma 6.2.3. *If $\alpha \in \mathcal{O}_d$ is non-zero, the quotient $\mathcal{O}_d/(\alpha)$ is finite, of order $|\mathcal{O}_d/(\alpha)| = N_{K/\mathbf{Q}}(\alpha)$.*

Proof. This concerns the computation of the *index* of $\alpha\Lambda$ as submodule of the free $\mathbf{Z}$-module $\Lambda = \mathcal{O}_d$. Now, it is obvious that the quotients $\Lambda/\alpha\Lambda$ and $\Lambda/\bar{\alpha}\Lambda$ are

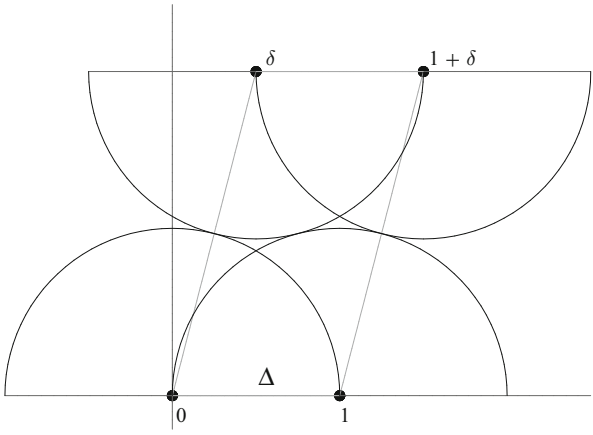


Fig. 6.1 The fundamental domain Δ for $d = -15$

isomorphic, for the map $\xi \mapsto \bar{\xi}$ is an involution. We thus have

$$[\Lambda : \alpha\Lambda] = [\Lambda : \bar{\alpha}\Lambda] = [\alpha\Lambda : \alpha\bar{\alpha}\Lambda].$$

Let $N = N_{K/\mathbf{Q}}(\alpha) \neq 0$. Since $\alpha\bar{\alpha} = N \in \mathbf{Z}$, we have:

$$N^2 = [\Lambda : \alpha\bar{\alpha}\Lambda] = [\Lambda : \alpha\Lambda] \cdot [\alpha\Lambda : \alpha\bar{\alpha}\Lambda].$$

Consequently, the index is finite and $|\mathcal{O}_d/(\alpha)| = [\Lambda : \alpha\Lambda] = N$. □

Comment 6.2.4. Formula $|\mathcal{O}_K/(\alpha)| = \left|N_{K/\mathbf{Q}}(\alpha)\right|$ is more generally valid for the ring of integers $\mathcal{O}_K$ of any number field K. It is usually proved using Proposition 3.2.5, as one can see, by a triangulation argument, that the index of $\alpha\mathcal{O}_K$ in $\mathcal{O}_K$ is equal to the absolute value of the determinant of the change-of-basis matrix ℓ_α between two bases.

Lemma 6.2.5. *If $d \neq -1, -2, -3, -7, -11$ and $\alpha \neq 0, \pm 1$, the number of elements of $\mathcal{O}_d/(\alpha)$ is greater than* 3.

Proof. Set $N = |\mathcal{O}_d/(\alpha)|$ and $\alpha = m + n\delta$. It follows from Lemma 6.2.3 that $N = |\alpha|^2 = m^2 + n^2\,|d|$ if $d \equiv 2$ or $3 \pmod 4$ and that $4N = (2m + n)^2 + n^2\,|d|$ if $d \equiv 1 \pmod 4$.

We see that N can be 1 with $\alpha \neq \pm 1$, only if $d = -1$ or $d = -3$. We also see that there is no solution with m and n integers for $N = 2$ or 3 if $|d| > 2$ in the first case and if $|d| > 11$ in the second. □

Theorem 6.2.6. *If $d < 0$, the ring $\mathcal{O}_d$ is Euclidean only if $d = -1, -2, -3, -7$, or -11.*

Proof. If $d \neq -1, -2, -3, -7, -11$, we first have $\mathcal{O}_d^* = \{\pm 1\}$, because Lemma 6.2.5 entails that there are no other units. If $\mathcal{O}_d$ had a Euclidean division algorithm φ, we could choose an element $\alpha \in \mathcal{O}_d$, which achieves the minimum

of φ on $\mathcal{O}_d \setminus \{0, \pm 1\}$. Then, for all $\beta \in \mathcal{O}_d$, there would exist $q,\ \gamma \in \mathcal{O}_d$ such that $\beta = \alpha q + \gamma$ with $\varphi(\gamma) < \varphi(\alpha)$. Consequently, every $\beta \in \mathcal{O}_d$ would be congruent to 0 or to ± 1 modulo α. This contradicts Lemma 6.2.5, which states that there are at least four classes modulo (α). □

Corollary 6.2.7. *If $d < 0$, the ring $\mathcal{O}_d$ is Euclidean if and only if it is for the usual norm $\psi = \left|N_{K/\mathbf{Q}}\right| : \alpha \mapsto |\alpha|^2$.*

Proof. This follows immediately from Corollary 6.2.2 and Theorem 6.2.6. □

Corollary 6.2.8. *If $d = -19,\ -43,\ -67$, or -163, the ring $\mathcal{O}_d$ is principal, but not Euclidean.*

Proof. One shows, in algebraic number theory, that these rings are principal, and Theorem 6.2.6 states that they have no Euclidean division algorithm. □

Remark 6.2.9. It has been known since 1966 that these nine rings $\mathcal{O}_d$ are the only ones that are principal, for $d < 0$. Before, it was only known that there were at most ten (see [CF], page 296).

6.3 Motzkin's Construction

The proof of Theorem 6.2.6 raises two interesting points. First, instead of writing $\beta = \alpha q + \gamma$ (with $\varphi(\gamma) < \varphi(\alpha)$), it is simpler to write $\beta \equiv \gamma \pmod{\alpha}$ or $\beta - \gamma = 0$ in $\mathcal{O}_d/(\alpha)$.

Then, for $d < 0$, there are not enough units to cover the entire quotient $\mathcal{O}_d/(\alpha)$. This situation is specific to quadratic imaginary fields, because in all other number fields the units form an infinite group, whereas $\mathcal{O}_K/(\alpha)$ remains finite (see Comment 6.2.4). Nevertheless, it is not always possible to obtain the whole of $\mathcal{O}_K/(\alpha)$ with units, if only because the ring is not always principal.

Motzkin's construction allows one to examine the existence of more general Euclidean division algorithms for arbitrary rings A.

Construction 6.3.1 (Motzkin). We set $A_0 = \{0\}$ and define recursively (for each integer $i > 0$):

$$A_i = \{0\} \cup \{\alpha \in A \mid \text{the canonical map } A_{i-1} \to A/(\alpha) \text{ is surjective}\}.$$

For instance,

$$A_1 = \{0\} \cup A^* \text{ and}$$

$$A_2 = \{0\} \cup \big\{\alpha \in A \mid \text{every element of } A/(\alpha) \text{ is the class of 0 or of a unit}\big\}.$$

Lemma 6.3.2. *For all $i \geq 0$, we have: $A_i \subset A_{i+1}$; and if there is an index i_0 such that $A_{i_0+1} = A_{i_0}$, then the sequence is stationary: $A_i = A_{i_0}\ \forall\, i \geq i_0$. If $A = \bigcup_{i\geq 0} A_i$, then A is Euclidean.*

Proof. The first assertion is proved by induction: it is obviously true if $i = 0$; then, if the canonical map $A_{i-1} \to A/(\alpha)$ is surjective, so is a fortiori the map $A_i \to A/(\alpha)$. Moreover, if $\alpha \in A_{i_0+2}$, the canonical map $A_{i_0+1} \to A/(\alpha)$ is surjective and, assuming that $A_{i_0+1} = A_{i_0}$, so is the map $A_{i_0} \to A/(\alpha)$; hence, $\alpha \in A_{i_0+1}$, etc.

Finally, if $A = \bigcup_{i\geq 0} A_i$, we can define an Euclidean division algorithm in an obvious manner: it suffices to set $\psi(\alpha) = i$ if $\alpha \in A_i \setminus A_{i-1}$. Indeed, given $\alpha \in A \setminus \{0\}$ with $\psi(\alpha) = i$, every $\beta \in A$ is, by the definition of A_i, in the same class modulo α as an element $\gamma \in A_{i-1}$; hence, $\psi(\gamma) \leq i - 1 < \psi(\alpha)$. Since $\beta \equiv \gamma \pmod{\alpha}$, this tells us that there exists $q \in A$ such that $\beta = \alpha\, q + \gamma$. □

□

Remark 6.3.3. ψ is a normalized Euclidean algorithm in the sense of Definition 6.1.10. Indeed, if $\gamma \neq 0$ is a multiple of α, the canonical map $A_{i-2} \to A/(\alpha)$ factors through $A_{i-2} \to A/(\gamma)$, and $A/(\gamma) \to A/(\alpha)$ is surjective. Consequently, $i = \psi(\alpha) \implies \alpha \notin A_{i-1} \implies \gamma \notin A_{i-1} \implies \psi(\gamma) \geq i = \psi(\alpha)$.

Example 6.3.4. For $A = \mathbf{Z}$, we see that $A_1 = \{0, \pm 1\}$ has three elements, which represent all remainder classes modulo 2 and 3. Therefore, $A_2 = \{0, \pm 1, \pm 2, \pm 3\}$, whose seven elements represent all remainder classes up to $7 = 2^3 - 1$. It follows that $A_3 = \{0, \pm 1, \ldots, \pm 7\}$. More generally, one finds that $A_i = \left\{m \in \mathbf{Z} \;\middle|\; |m| < 2^i\right\}$, which has $2^{i+1} - 1$ elements.

Notice that $\mathbf{Z} = \bigcup_{i\geq 0} A_i$. Hence, $\mathbf{Z}$ is also Euclidean for the Euclidean norm of Lemma 6.3.2, which can be put (if $m \neq 0$) in the form

$$\psi(m) = 1 + \left[\log_2 |m|\right],$$

where $[.]$ denotes the integer part. This is also the number of digits in the base 2 expansion of $|m|$. This norm is quite different from the one in Example 6.1.2.

Remark 6.3.5. The elements $\alpha \in A_2 \setminus A_1$ are necessarily prime. Indeed, it follows from the definition of A_2 that every non-zero element of $A/(\alpha)$ is of the form $\pi(u)$, where π is the canonical map $A_1 \to A/(\alpha)$ and $u \in A^*$. Such an element is therefore invertible, so that $k = A/(\alpha)$ is a field and (α) is a maximal ideal. For $\alpha \in A_2 \setminus A_1$, the restriction of π to the group of units is therefore a homomorphism of A^* onto the multiplicative group of the field k.

Of course, there are also rings for which $A_2 \setminus A_1$ is empty (see Lemma 6.2.5). If $A = \mathcal{O}_K$ is the ring of integers of a number field, k is a finite field (Comment 6.2.4). For such a ring, a generalization of the famous Artin's conjecture concerning *primitive roots* asks, under the hypothesis that $\mathcal{O}_K^*$ is infinite, if there exists an

infinity of primes α for which $\pi(\mathcal{O}_K^*) = k^*$. This raises the question of the size of A_2; see Ram Murty & Petersen [RMP].

Remark 6.3.6. A_1 is certainly not an additive group, but number fields are known, whose rings of integers have the property that many differences of units are still units. This led to the discovery of several unusual rings, which are Euclidean for the usual norm (Lenstra [Le]).

Theorem 6.3.7. *If A is Euclidean, then $A = \bigcup_{i\geq 0} A_i$ and the algorithm ψ described in Lemma 6.3.2 is the smallest Euclidean algorithm on A.*

Proof. Let $\varphi : A \to \mathbf{N}$ be a Euclidean division algorithm. According to Lemma 6.1.3, $\varphi(\alpha) > 0$ for all $\alpha \neq 0$. For $i \in \mathbf{N}$, we define subsets of A as follows:

$$B_i = \{\alpha \in A \mid \varphi(\alpha) \leq i\}.$$

One shows by induction that $B_i \subset A_i$ for all $i \in \mathbf{N}$. Indeed, this is obviously true for $i = 0$. For $i > 0$, let $\alpha \in A \setminus \{0\}$ be such that $\varphi(\alpha) \leq i$. Then

$$\forall\, \beta \in A,\ \exists q,\ \gamma \in A \text{ with } \beta = \alpha q + \gamma \text{ and } \varphi(\gamma) < \varphi(\alpha) \leq i.$$

Hence, $\beta \equiv \gamma \pmod{\alpha}$, and $\varphi(\gamma) < i \implies \gamma \in B_{i-1} \subset A_{i-1}$, because of the induction hypothesis. Therefore, $\alpha \in A_i$.

Hence, $A = \bigcup_{i\geq 0} B_i \subset \bigcup_{i\geq 0} A_i$. Moreover, if $\varphi(\alpha) = i$ we find $\alpha \in B_i \subset A_i$; hence, $\psi(\alpha) \leq i$, where ψ denotes the algorithm described in Lemma 6.3.2. This implies that $\psi(\alpha) \leq \varphi(\alpha)$ for all $\alpha \in A$. Hence, ψ is smaller than any other Euclidean division algorithm on A. □

6.4 Real Quadratic Fields

For $d > 0$, the ring $\mathcal{O}_d$ is Euclidean for the usual norm if and only if $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57$, or 73. The proof is analogous to that of Corollary 6.2.2, but considerably more difficult: unit disks are replaced by areas delimited by branches of hyperbolas and it is better to use a computer to deal with the numerous cases of superposition. A very old conjecture of Gauss predicts the existence of an infinity of real quadratic fields whose rings of integers $\mathcal{O}_d$ are principal. This conjecture is still open, but we know many rings $\mathcal{O}_d$ that are principal. The first non-Euclidean one, for the usual norm is $\mathcal{O}_{14} = \mathbf{Z}[\sqrt{14}]$. Until 2004, it was not known whether it was Euclidean after all (for another algorithm).

However, a result of Weinberger indicates that, under a very strong hypothesis – also unproved to this day – all number rings that are principal should be

Euclidean, except if there is only a finite number of units available. The four rings in Corollary 6.2.8 would thus be the only exceptions.

The following criterion uses only the irreducible elements of the ring.

Proposition 6.4.1 (Weinberger). *Let $\mathcal{O}_K$ be the ring of integers of a number field; consider Motzkin's subsets A_i (Construction 6.3.1 for $A = \mathcal{O}_K$). Assume that $\mathcal{O}_K$ is a principal ring, all of whose irreducible elements belong to A_3. Then, $\mathcal{O}_K$ is Euclidean.*

Proof. According to Lemma 6.3.2, it suffices to see that every non-zero $\alpha \in \mathcal{O}_K$ belongs to one of the subsets A_i. Now, α factors in the factorial ring $\mathcal{O}_K$ as a product of units and irreducible elements, in an essentially unique manner. Write:

$$\alpha = u \cdot \prod_{i=1}^{n_2} p_i \cdot \prod_{j=1}^{n_3} q_j,$$

where u is a unit (and hence belongs to A_1) and where the p_i are in $A_2 \setminus A_1$ and the q_j in $A_3 \setminus A_2$. We define a *height* map $\chi : \mathcal{O}_K \to \mathbf{N} \cup \{-\infty\}$ by $\chi(\alpha) = 2n_2 + 3n_3$ if $\alpha \neq 0$ and $\chi(0) = -\infty$. Thus, we always have $\chi(\alpha_1\alpha_2) = \chi(\alpha_1) + \chi(\alpha_2)$.

We shall show by induction that if $h = \chi(\alpha) \geq 2$, then $\alpha \in A_h$. This is clearly true for $h = 2$, since $p_1 \in A_2$ implies that $u \cdot p_1 \in A_2$ for every unit $u \in \mathcal{O}_K^*$. We may therefore assume that $h \geq 3$. We must show that the canonical map $A_{h-1} \to \mathcal{O}_K/(\alpha)$ is surjective. We shall prove that every $\beta \in \mathcal{O}_K$ is in the same class modulo α as an element γ such that $\chi(\gamma) < h$. By induction, we then have $\gamma \in A_{h-1}$, hence the required surjectivity.

Let a be gcd of α and β; then,

$$\alpha = am\,, \quad \beta = ab \quad \text{and} \quad \gcd(m, b) = 1.$$

We distinguish several cases, according to the value of $\chi(m)$: if $\chi(m) = 0$, then $m \in \mathcal{O}_K^*$; so, $\alpha \mid \beta$ and we can take $\gamma = 0$.

If $\chi(m) = 2$, then $m \in A_2 \setminus A_1$ and there exists $c \in A_1$ such that $b \equiv c \pmod{m}$. Moreover, $c \neq 0$, since $\gcd(m, b) = 1$; we define $\gamma = ac$. Then, $\alpha = am \mid a(b - c) = \beta - \gamma$. We thus have $\beta \equiv \gamma \pmod{\alpha}$ and $\chi(\gamma) = \chi(a) = \chi(\alpha) - \chi(m) < \chi(\alpha)$.

If $\chi(m) = 3$, then $m \in A_3 \setminus A_2$ and there exists $c \in A_2$ such that $b \equiv c \pmod{m}$. Here, also, $c \neq 0$ and we define $\gamma = ac$. Then, $\alpha = am \mid a(b-c) = \beta - \gamma$. Indeed, we have $\beta \equiv \gamma \pmod{\alpha}$ and $\chi(c) \leq 2$. Hence, $\chi(\gamma) = \chi(a) + \chi(c) \leq \chi(a) + 2 = \chi(\alpha) - \chi(m) + 2 = \chi(\alpha) - 1$; thus, $\chi(\gamma) < \chi(\alpha)$.

The case $\chi(m) > 3$ makes use of a well-known extension of Dirichlet's Theorem on prime numbers in an arithmetic progression.

Notation 6.4.2. Let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{m} \subset \mathcal{O}_K$ be non-zero ideals. The notation $\mathfrak{a} \equiv \mathfrak{b} \mod \mathfrak{m}$ means that there exists a principal fractional ideal (c) such that $\mathfrak{a}\mathfrak{b}^{-1} = (c)$, with $v(c - 1) \geq v(\mathfrak{m})$ for every place v of K.

Lemma 6.4.3 (Dirichlet). *Let $\mathfrak{m} \subset \mathcal{O}_K$ be a non-zero ideal. For every ideal $\mathfrak{b}$ prime to $\mathfrak{m}$, there is an infinity of prime ideals $\mathfrak{p}$ of degree 1 such that $\mathfrak{p} \equiv \mathfrak{b} \mod \mathfrak{m}$.*

Corollary 6.4.4 (Dirichlet). *Suppose that $\mathcal{O}_K$ is principal; let $m \in \mathcal{O}_K$ be a non-zero element. Then, for every element $b \in \mathcal{O}_K$ prime to m, there is an infinity of prime ideals $\mathfrak{p} = (\pi)$ of degree 1 such that $\pi/b - 1 \in (m)$, and hence $m \mid (\pi - b)$.*

Let us resume the proof of Proposition 6.4.1: if $\chi(m) > 3$, Corollary 6.4.4 implies that there exists an irreducible element $\pi \in \mathcal{O}_K$ such that $b \equiv \pi \pmod{m}$. By hypothesis, $\chi(\pi) = 2$ or 3; we define $\gamma = a\pi$. Then, $\alpha = am \mid a(b - \pi) = \beta - \gamma$. We thus have $\beta \equiv \gamma \pmod{\alpha}$ and $\chi(\pi) \leq 3$; hence, $\chi(\gamma) = \chi(a) + \chi(\pi) \leq \chi(a) + 3 = \chi(\alpha) - \chi(m) + 3 < \chi(\alpha)$. □

Weinberger also showed that, under a very strong hypothesis (*the generalized Riemann hypothesis*), the condition that all irreducible elements belong to A_3 is satisfied as soon as $\mathcal{O}_K$ has an infinity of units.

Corollary 6.4.5 (Weinberger). *Let $\mathcal{O}_K$ be the ring of integers of a number field, having an infinity of units. Assume that the generalized Riemann hypothesis holds. Then the ring $\mathcal{O}_K$ is Euclidean if and only if it is principal.*

Most recently, Malcolm Harper has succeeded in showing, without conditions, that $\mathbf{Z}[\sqrt{14}]$ is Euclidean. In his paper from 2004 [Ha], he even showed that all rings of integers of real quadratic fields are Euclidean if they are principal, depending on a condition to be verified in each case, yet apparently always satisfied. He proved at the same time that the statement is also valid for cyclotomic extensions of $\mathbf{Q}$, which incidentally represents only 29 cases, from which at least 12 are also Euclidean for the norm. Since then, the result has been extended to Galois extensions whose group of units have rank greater than 3, but the general case, which would include Weinberger's result without assuming the generalized Riemann hypothesis, is still missing.

Exercises

6.1. One shows, in algebraic number theory, that the ring $\mathcal{O}_{14} = \mathbf{Z}[\sqrt{14}]$ is principal. However, it is not Euclidean for the norm $\varphi(m + n\sqrt{14}) = \left|m^2 - 14n^2\right|$. Indeed, show that one cannot divide $1 + \delta$ by 2 with a remainder having norm strictly smaller than 4.

6.2. Show that in fact 2 must be divided by $1 + \delta$ in the ring $A = \mathcal{O}_{14}$, since for the minimal algorithm described in Lemma 6.3.2 we have $\psi(2) > \psi(1 + \delta)$. More precisely, show that $1 + \delta \in A_2$ and $2 \in A_3$, so that $\psi(1 + \delta) = 2$ and $\psi(2) = 3$.

6.3. Establish the Euclidean minimal algorithm for the ring $A = k[X]$.

6.4. If $S \neq \emptyset$ is a multiplicative subset ($0 \notin S$; $x, y \in S \implies xy \in S$) of a Euclidean ring A, show that the ring of fractions $S^{-1}A$ is also Euclidean.

Chapter 7
Cubic Surfaces

Projective varieties of degree 3 are an important topic in arithmetic. This includes genus 1 plane curves, which continue to generate research (theory of *elliptic curves*: computation of the rank of the Mordell–Weil group, the study of the Tate–Shafarevich group, and the Birch and Swinnerton-Dyer conjecture). For smooth cubic hypersurfaces of dimension 3, a difficult theorem (Clemens & Griffiths, 1972) states that they are never k-rational (in the sense of definition 5.5.11), even if k is algebraically closed. They are nevertheless *k-unirational*, which means that one can parametrize their points, even if the base field is not algebraically closed, but not in an injective manner.

Dimension 2 is very different: at the same time simpler than curves and richer in geometrical structure. In this chapter, we focus on this case, which is of great interest. In fact, the study of cubic surfaces played a fundamental role in the development of both algebraic geometry and arithmetic.

7.1 The Space of Cubics

A *cubic surface* is a projective irreducible variety of the form $Y = V(F) \subset \mathbf{P}^3_k$, where F is a non-zero homogenous polynomial of degree 3, in four variables. One can write

$$F = \sum_{0 \le i \le j \le k \le 3} a_{ijk}\, X_i\, X_j\, X_k\,, \qquad \text{with } a_{ijk} \in k.$$

There are 20 coefficients, defined up to multiplication by a non-zero constant. Cubic surfaces are therefore parametrized by the points of a projective space $\mathbf{P}^{19}_k = \mathrm{Proj}\, S^3(k^4)$, where $S^3(k^4)$ classically denotes the vector space of homogenous

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_7

polynomials of degree 3, in four variables (it is also the vector space of all polynomials of degree 3, in three variables).

Of course, this space also parametrizes reducible polynomials, such as $F = X_1 X_2 X_3$, or even non-reduced ones, such as $F = X_1^2 X_2$ or $F = X_1^3$. From an arithmetic point of view, one is interested mainly in irreducible polynomials, but it must be noted that even with this restriction, there are a certain number of particular cases to consider.

The most obvious is that of *cones*, where F depends (up to a projective transformation) on three variables only. For instance, $F = 3X_1^3 + 4X_2^3 + 5X_3^3$ defines a curve in $\mathbf{P}^2_{\mathbf{Q}}$ with no rational point (Proposition 9.2.2), but one may also consider the surface $Y = V(F) \subset \mathbf{P}^3_{\mathbf{Q}}$. This is a cone whose vertex $[1 : 0 : 0 : 0]$ is the unique rational point. Such a point is clearly singular; actually, it is a triple point of the variety Y and Theorem 7.2.1 below does not apply.

The different types of singularities of cubic surfaces were first described over the field of real numbers by Schläfli in 1863, and the classification was completed and presented over the complex field by Cayley in 1868. Cones excluded, 23 main types are distinguished, which include the surfaces with at most four double isolated points (see Exercises 4.7 and 7.4) and two types of *ruled surfaces*, having a double line and an infinite family of other lines (see §7.4). Yet most cubic surfaces are clearly smooth, that is, all their points are non-singular (Definition 5.5.7).

7.2 Unirationality

The study of cubic surfaces over an algebraically closed field owes much to Beniamino Segre. One of the first results was the following.

Theorem 7.2.1 (B. Segre, 1943). *Let $Y \subset \mathbf{P}^3_k$ be a smooth cubic surface defined over a perfect infinite field k. Then the set $Y(k)$ is empty or infinite.*

Proof. The idea of the proof is very simple: if $Y(k) \neq \emptyset$, let $P \in Y(k)$ and $\pi = T_P Y$ be the tangent plane to Y at this point; the intersection $\Gamma = \pi \cap Y$ is considered.

Γ is a curve on which the point P is singular. This follows from general arguments, but here is an *ad hoc* proof: the equation of the tangent plane is $\sum_{j=0}^{3} \frac{\partial F}{\partial X_j}(P)\, X_j = 0$ (see Definition 5.5.7). By a projective change of variables we may suppose that π has equation $X_3 = 0$. Then, only $\frac{\partial F}{\partial X_3}(P)$ is non-zero, the three other partial derivatives vanishing at P. Now, Γ is a hypersurface in the plane π, defined by the equation $F(X_0, X_1, X_2, 0) = 0$; therefore, it is a curve and all partial derivatives are zero at P.

If we could assume that Γ is irreducible, we would have finished. Indeed, Γ is a curve of degree 3 and, as shown in Figure 1.4 of §1.2, its trace on a line ℓ passing through P is the union of P, which counts twice, and of a single other point (see also Exercise 1.3). If we choose ℓ among the infinity of k-rational lines passing

Fig. 7.1 A plaster model of a cubic surface with 27 real lines.
(Plaster model by Alexander Crum Brown c. 1900; photograph courtesy of the Science Museum / Science and Society Picture Library)

through P, we get an infinity of residual points, which are also k-rational, since they are invariant under the action of the Galois group $\mathrm{Gal}(\bar{k}/k)$. All these points thus belong to $Y(k)$ (Figure 7.1).

We are dealing here with a typical situation in algebraic geometry: after having solved the so-called "general case", we are brought back to the study of a multitude of particular cases, which we hope are simpler. In fact, the situation is complicated enough.

First, since Γ has degree 3, it is clear that, if it is reducible, one of its components is a line. If this line is defined over k, it has an infinity of k-rational points and we are done. Because of the action of the Galois group, such a situation arises in particular if Γ is the union of a line and an irreducible conic. In that case, the two components necessarily meet at P, because it is a double point on Γ. By reasoning out the various possibilities, we are left with considering only the case when Γ is the union of three distinct lines, constituting a single orbit under the action of Galois. Moreover, these lines must all pass through P, since this point is k-rational.

At first sight, this case is impossible. Indeed, one pictures that, if a cubic surface carries three lines that meet in one point, this point should be singular. This argument would be correct "in general", but it fails if the three lines belong to the same plane.

Definition 7.2.2. An *Eckardt point* on a smooth cubic surface is a point through which pass three (necessarily coplanar) lines on the surface.

In fact, we have already seen an example in Exercise 2.15: the diagonal surface $X_0^3 + X_1^3 + X_2^3 + X_3^3 = 0$ has 18 Eckardt points, $[1 : -\rho^j : 0 : 0]$ ($j = 0, 1, 2$), and permutations of these coordinates ($\rho = e^{2\pi i/3}$). Segre studied the possible different configurations of the Eckardt points. The line joining two Eckardt points may be

contained in the cubic surface; otherwise, it intersects the surface in a third point, which is also an Eckardt point. Most cubic surfaces have no Eckardt points and one can show that there are never more than 18 such points. All we need to know is that a smooth cubic surface has only a finite number of Eckardt points, which clearly follows from the finiteness of the number of lines, which we see in §7.5 (Theorem 7.5.1).

Comment 7.2.3. The Eckardt points may also be described as singularities of the *hessian* H, whose equation is $\left|\partial^2 F/\partial X_i \partial X_j\right| = 0$. There is an analogy with the inflexion points of plane curves. As a matter of fact, it is easy to see that cutting Y with a transverse plane in an Eckardt point P, one obtains a curve of degree 3 on which P is an inflexion point.

To complete the proof of the theorem, we make use of an argument attributed to Skolem. The point is to show that the surface Y also has k-rational points that are not Eckardt points. Given $P \in Y(k)$, we first consider the family of k-rational lines passing through P. Since we know that there are only a finite number of lines on a smooth cubic surface, we can find a k-rational line L passing through P and that does not meet any line contained in Y.

Then, L intersects Y in two other points, P_1 and P_2. If $P_1 \in Y(k)$, we are finished. If not, P_1 and P_2 are two conjugate points in a quadratic extension K/k. The preceding argument works well over K: if $\pi_i = T_{P_i} Y$ denotes the tangent plane to Y at P_i, the intersection $\Gamma_i = \pi_i \cap Y$ is an irreducible curve on which P_i is a double point ($i = 1, 2$). We have $\pi_2 = \sigma(\pi_1)$, where σ is the generator of the group $\mathrm{Gal}(K/k)$.

Let π be a plane containing the line L, and suppose that this plane is defined over K, *but not over* k. Its intersection with Γ_1 is the union of P_1 (which counts double) and of a further point $Q_1 \in Y(K)$. The conjugate of Q_1 is a point Q_2 on $\pi_2 \cap \sigma(\pi)$. The line joining Q_1 to Q_2 is k-rational and does not meet the line L. Indeed, L and Q_1 generate the plane π, and Q_2 cannot belong to that plane, since it belongs to $\sigma(\pi)$, but not to $\pi \cap \sigma(\pi) = L$.

The line joining Q_1 to Q_2 meets Y in a new point $Q \in Y(k)$ (see Example 3.3.10), and $Q \neq P$ since $Q \notin L$. It still might be the case that Q is an Eckardt point, but we show that the construction yields an infinity of points $Q \in Y(k)$, whereas there are only a finite number of Eckardt points.

Since $Q_1 \in \Gamma_1$, the point Q_2 belongs to the cubic cone C_Q with vertex Q and base curve Γ_1. This cone has a generating double line passing through P_1 and cannot contain the curve Γ_2. Otherwise, the double point P_2 of Γ_2 would be on the same generator, and this would imply that the two double points P_1 and P_2 are aligned with the vertex Q. This is impossible, because $Q \notin L$. Hence, Γ_2 intersects C_Q in a finite number of points (at most 9).

Starting from a point Q obtained by the above construction, we can retrieve the point Q_2 in the *finite* intersection of Γ_2 with the cone C_Q. Now, letting the plane π vary, we have found an infinity of possibilities for Q_2. Hence, there are also an infinite number of points Q. □

Corollary 7.2.4. *Every smooth cubic surface $Y \subset \mathbf{P}^3_k$, defined over a perfect infinite field k is k-unirational if $Y(k) \neq \emptyset$.*

Unirationality is defined as follows.

Definition 7.2.5. An irreducible variety $Y \subset \mathbf{P}^n_k$ is called *k-unirational* if there is a rational dominant map $f : \mathbf{P}^N_k \dashrightarrow Y$ (where $N \geq \dim Y$).

By virtue of Proposition 5.5.2, the algebraic expression of unirationality is the following.

Proposition 7.2.6. *An irreducible variety $Y \subset \mathbf{P}^n_k$ is k-unirational if and only if the function field $k(Y)$ has an extension of the form $k(u_1, \dots, u_N)$, purely transcendental over k.*

Moreover, one easily shows that in this case, $k(Y)$ also has a *finite* extension of the form $k(u_1, \dots, u_d)$, where $d = \dim Y$, but this is not necessarily useful in applications.

Proof of Corollary 7.2.4. Since by hypothesis $Y(k) \neq \emptyset$, Theorem 7.2.1 entails that $Y(k)$ is infinite. In particular, there exists $P_1 \in Y(k)$, which is not an Eckardt point. Let $\pi_1 = T_{P_1} Y$ be the tangent plane to Y at this point and let $\Gamma_1 = \pi_1 \cap Y$. If Γ_1 is irreducible, it is a curve with a double point at P_1. In this case, the argument in §1.2, illustrated by Figure 1.4, shows that Γ_1 is k-unirational: there is a dominant rational map $f_1 : \mathbf{P}^1_k \dashrightarrow \Gamma_1$. If Γ_1 is reducible, it contains a k-rational line L_1 and the following reasoning applies, replacing Γ_1 by L_1.

Since $\Gamma_1(k)$ is infinite, we can choose another point $Q \in \Gamma_1(k)$ and consider the tangent plane $\pi = T_Q Y$ to Y at Q. The intersection $\Gamma = \pi \cap Y$ is a curve on which we may choose another point $P_2 \in \Gamma(k)$. Let $\pi_2 = T_{P_2} Y$ be the tangent plane to Y at this point and let $\Gamma_2 = \pi_2 \cap Y$. As previously, Γ_2 is k-unirational: there is a dominant rational map $f_2 : \mathbf{P}^1_k \dashrightarrow \Gamma_2$.

Given two distinct points $Q_1,\ Q_2 \in Y(k)$ such that the line through Q_1 and Q_2 is not entirely contained in Y, we denote by $Q_1 \circ Q_2$ the third point of intersection of Y with that line. (It may coincide with Q_1 or Q_2 if the line is tangent to Y at that point). We obtain a dominant rational map $f : \mathbf{P}^2_k \dashrightarrow Y$ by composing $f_1 \circ f_2 : \mathbf{P}^1_k \times \mathbf{P}^1_k \dashrightarrow Y$ with a birational map $g : \mathbf{P}^2_k \dashrightarrow \mathbf{P}^1_k \times \mathbf{P}^1_k$.

There are some details to check. Manin gave a more refined argument for which the *degree of unirationality* $[k(u_1, u_2) : k(Y)]$ equals 6. □

Remark 7.2.7. k-rational varieties are clearly k-unirational. A classical theorem of Lüroth states that the converse is true for *curves*, over an arbitrary field. The converse is valid also for *surfaces* (Theorem of Castelnuovo), but only over an algebraically closed field of characteristic 0.

If k is not algebraically closed, there are smooth cubic surfaces $Y \subset \mathbf{P}^3_k$ that are not k-rational. In dimension 3, smooth cubic hypersurfaces $Y \subset \mathbf{P}^4_k$ are all unirational, but even if $k = \bar{k}$, none is rational (Theorem of Clemens and Griffiths).

7.3 Grassmannian of Lines

Given two distinct points $x = [x_0 : x_1 : x_2 : x_3]$ and $y = [y_0 : y_1 : y_2 : y_3]$ in $\mathbf{P}^3_k$, defining a space line L, the six determinants

$$p_{ij} = x_i\, y_j - x_j\, y_i \tag{7.3.1}$$

are the coordinates of a point $p = [\, p_1 : p_2 : p_3 : p_4 : p_5 : p_6] \in \mathbf{P}^5_k$, where:

$$p_1 = p_{01}\,, \quad p_2 = p_{02}\,, \quad p_3 = p_{03}\,, \quad p_4 = p_{23}\,, \quad p_5 = p_{31}\,, \quad p_6 = p_{12}. \tag{7.3.2}$$

This point depends solely on the line L. Indeed, if we replace y by any linear combination of x and y in $\bar{k}^4$, we get the same point of the projective space $\mathbf{P}^5_k$. This follows from standard properties of determinants.

Definition 7.3.1. The point $p = [\, p_1 : p_2 : p_3 : p_4 : p_5 : p_6] \in \mathbf{P}^5_k$ defined above constitutes the *Plücker coordinates* of L. It belongs to the *Klein quadric* $\Omega \subset \mathbf{P}^5_k$ having equation $p_1\, p_4 + p_2\, p_5 + p_3\, p_6 = 0$.

This 4-dimensional variety precisely parametrizes the family of lines in $\mathbf{P}^3_k$, which is easily verified to be 4-dimensional, because we can fix two planes π_1, π_2 in $\mathbf{P}^4_k$ and identify any line not intersecting $\pi_1 \cap \pi_2$ by an uniquely determined point in each of these planes. It is also referred to as the *Grassmannian* of lines in $\mathbf{P}^3_k$. It is classically denoted by $\mathcal{G}_{1,3}$ or $\mathcal{G}_{2,4}$, according to different authors, since it also parametrizes the 2-dimensional vector subspaces of $\bar{k}^4$.

The fundamental relation

$$p_1\, p_4 + p_2\, p_5 + p_3\, p_6 = 0 \tag{7.3.3}$$

is easily obtained by expanding, using the minors of the first two rows, the determinant

$$\begin{vmatrix} x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \end{vmatrix},$$

which is clearly zero. To see that every point $p \in \mathbf{P}^5_k$ that verifies this relation corresponds to a line of $\mathbf{P}^3_k$ (Exercise 7.3), it is useful to observe that a line with Plücker coordinates p meets the planes $\{X_i = 0\}$ at the following points:

$$\begin{aligned} z_0 &= [0 : p_1 : p_2 : p_3] \\ z_1 &= [\, p_1 : 0 : -p_6 : p_5] \\ z_2 &= [\, p_2 : p_6 : 0 : -p_4] \\ z_3 &= [\, p_3 : -p_5 : p_4 : 0] \end{aligned} \tag{7.3.4}$$

One must be aware that these expressions do not always represent four distinct points. For instance, if $p_1 = p_2 = p_3 = 0$, the line is contained in the plane $\{X_0 = 0\}$ and the expression $[0 : p_1 : p_2 : p_3]$ does not correspond to a point of the projective space. If $p_3 = p_6 = 0$, only two points are obtained.

Lemma 7.3.2. *The family of lines that meet a given line is in bijection with the points of* Ω *situated in its tangent space at the corresponding point.*

Proof. The equation of the tangent space $T_q\Omega$ to Ω at q is obtained by deriving equation (7.3.3):

$$q_4\, p_1 + q_5\, p_2 + q_6\, p_3 + q_1\, p_4 + q_2\, p_5 + q_3\, p_6 = 0. \tag{7.3.5}$$

If x is a common point of two lines with Plücker coordinates p and q, one can write the p_{ij} as in (7.3.1), and also $q_{ij} = x_i\, z_j - x_j\, z_i$. On expanding the determinant

$$\begin{vmatrix} x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ x_0 & x_1 & x_2 & x_3 \\ z_0 & z_1 & z_2 & z_3 \end{vmatrix},$$

which is clearly zero, with respect to the minors of the first two rows, one gets the same relation (7.3.5). The family of lines meeting the line with Plücker coordinates q is therefore represented by points of $T_q\Omega$ and it is of dimension 3. Since the intersection of Ω with the tangent hyperplane is irreducible of dimension 3, the two families coincide. □

Definition 7.3.3. A *line complex* in $\mathbf{P}^3_k$ is a family of lines that corresponds to a section of Ω by a hypersurface. Thus, it is represented in Plücker coordinates by the points of $\Omega \cap V(G)$, where $G \in k[\, p_1, \ldots, p_6]$ is a homogenous polynomial. Its *order* is the degree of G.

According to Lemma 7.3.2, the family of lines that meets a given line is an order 1 complex. In this case, $V(G) \subset \mathbf{P}^5_k$ is a hyperplane tangent to Ω, but there are other line complexes of a different nature.

Corollary 7.3.4. *The only codimension* 1 *subvarieties of* Ω *are the complete intersections of the form* $\Omega \cap V(G)$*, where* $G \in k[\, p_1, \ldots, p_6]$.

(There are direct proofs, but this also follows from a general theorem of Severi and Grothendieck, which applies to every smooth hypersurface of dimension at least 3.)

One shows that, if $\Gamma \subset \mathbf{P}^3_k$ is a curve of degree d, the family of lines that meet Γ is a complex of order d. We may thus associate with it a form of degree d, well-defined modulo Equation (7.3.3) of Ω. This idea, which goes back to Cayley, allows us to parametrize the set of all curves of a given degree by the points of an algebraic variety. Indeed, the coefficients of the associated form determine a point in a certain

projective space $\mathbf{P}_k^N$, and there is one such point for every curve. This is the origin of the notions of *Chow point* and *Chow variety.*

7.4 Ruled Cubic Surfaces

These are cubic surfaces, necessarily singular, which carry an infinity of lines, but are not cones over a plane curve. The classification attributed to Schläfli and Cayley indicates that they resolve into two distinct types:

$$\text{I.} \qquad X_0 X_1^2 - X_2^2 X_3 = 0;$$

$$\text{II.} \qquad X_1(X_0 X_1 - X_2 X_3) + X_2^3 = 0.$$

They all have a line consisting of double points. Over an algebraically closed field, all the surfaces of the first type are projectively equivalent; they form a 13-dimensional family. Those of type II are also mutually projectively equivalent; they form a family of dimension 12. The group $\mathbf{P}\mathrm{GL}_4$ is of dimension 15, but these surfaces admit inner automorphisms: a 2-dimensional group for type I, and 3-dimensional for type II.

Type I Surfaces. The line $D = \{X_1 = X_2 = 0\}$ obviously consists of double points. Using the equation of the surface Y, one recognizes another line $E = \{X_0 = X_3 = 0\}$, termed *ruling*, with the property that $D \cap E = \emptyset$. The general equation of a plane π containing D takes the form $\mu X_2 = \lambda X_1$. If $\mu \neq 0$, the computation of the intersection $\pi \cap Y$ leads to the product $X_1^2\,(\mu^2 X_0 - \lambda^2 X_3) = 0$, which represents, in the plane π, the union of the line D taken twice and of another line L_1, which varies with the plane. If $\mu = 0$, we directly obtain the equation $X_2^2 X_3 = 0$ in the plane $\{X_1 = 0\}$ and the conclusion is the same. This line L_1 cuts D in $[\lambda^2 : 0 : 0 : \mu^2]$. It also cuts E in a point $L_1 \cap E = (L_1 \cup D) \cap E = \pi \cap E = [0 : \mu : \lambda : 0]$. This last point is obtained in a unique way, whereas the point $[\lambda^2 : 0 : 0 : \mu^2]$ belongs to a second line L_2, lying in the plane $\mu X_2 = -\lambda X_1$. Each point of D therefore belongs to two other lines on the surface (except if $\lambda\mu = 0$, in which case L_1 and L_2 coincide), whereas each point of E belongs to a single other line of Y.

We may also view all this in a synthetic manner, by considering a pencil of planes all containing E: the residual intersection with Y is a curve of degree 2, with a double point on D; hence, it is the union of two lines. This establishes a correspondance which to each point of D associates two points of E.

To describe the whole family of lines on the surface, we can make use of Plücker coordinates.

Proposition 7.4.1. *The family of lines contained in the surface Y of type I, is represented on the Klein quadric by the union of a twisted cubic curve and of two points not belonging to the space generated by this curve.*

Proof. For the line D, on referring to (7.3.2), one checks that $p_i = 0$ if $i \neq 3$. For the line E, we have $p_i = 0$ if $i \neq 6$. Thus, the double line and the ruling are represented on the Klein quadric by the points

$$p_D = [0:0:1:0:0:0]\,, \quad p_E = [0:0:0:0:0:1]. \tag{7.4.1}$$

If L is another line contained in Y, with Plücker coordinates $\{p_i\}$, we know that the surface must contain all the points given by (7.3.4). On replacing in Equation I we find the following necessary conditions:

$$-p_2^2\, p_3 = 0\,, \quad -p_6^2\, p_5 = 0\,, \quad p_2\, p_6^2 = 0\,, \quad p_3\, p_5^2 = 0.$$

If $p_3 \neq 0$ or $p_6 \neq 0$, we have necessarily $p_2 = p_5 = 0$. In this case, the only possibility is D or E.

Indeed, if $p_1 = p_{01} \neq 0$, we do not have $X_0 = 0$ identically on L; and nor do we have $X_1 = 0$ identically on L. The relation $p_2 = x_0y_2 - x_2y_0 = 0$ then implies that the ratio $x_2/x_0 = y_2/y_0$ is a constant $\lambda \in \bar{k}$ for all points of the line L, which is therefore contained in the plane $X_2 - \lambda X_0 = 0$. Similarly, the relation $p_5 = x_3y_1 - x_1y_3 = 0$ implies that $x_3/x_1 = y_3/y_1$ is a constant $\mu \in \bar{k}$ for all the points of the line, which therefore lies in the plane $X_3 - \mu X_1 = 0$. On substituting in Equation I, we then find that L also lies in the plane $X_1 - \lambda^2\mu X_0 = 0$, which is impossible, since these conditions define only one point in $\mathbf{P}^3_k$.

The same reasoning shows that we cannot have $p_4 \neq 0$ when $p_2 = p_5 = 0$. Hence, we must have simultaneously $p_1 = p_2 = p_4 = p_5 = 0$, and hence also $p_3\, p_6 = 0$ in view of (7.3.3). One is left with the only solutions p_D and p_E according to whether p_3 or p_6 is non-zero.

This shows that if L is different from D and from E, we must have $p_3 = p_6 = 0$, which means that L meets D and E. Indeed, we have seen (Lemma 7.3.2) that the lines meeting D are in bijection with the points of Ω situated in its tangent space at the point p_D, associated with this line. They are therefore given by the equation $p_6 = 0$. Those meeting E are given by $p_3 = 0$.

Yet we will specify further; thus, let us assume that $p_3 = p_6 = 0$. From $p_6 = p_{12} = x_1y_2 - x_2y_1 = 0$ we deduce that the ratio $x_2/x_1 = y_2/y_1$ is a constant $\mu \in \mathbf{P}^1_k$ for all points of the line L. It could be that L lies in the plane $X_1 = 0$, from which the projective nature of the ratio μ, but we do not have identically $X_1 = X_2 = 0$. Indeed, this would imply that $p_1 = p_2 = p_4 = p_5 = p_6 = 0$, which is not possible, since we have also supposed that $p_3 = 0$. From this, we infer that $p_2/p_1 = \mu$ and also, according to (7.3.3), that

$$p_4/p_5 = -p_2/p_1 = -\mu.$$

The same reasoning, applied to the condition $p_3 = x_0y_3 - x_3y_0 = 0$ allows us to assert that $x_3/x_0 = y_3/y_0$ is a constant ratio $\lambda \in \mathbf{P}^1_k$, for every point on the line L. We do not have at the same time identically $X_0 = 0$ and $X_3 = 0$, since the intersection

of these two planes is just the line E, for which $p_6 \neq 0$. We deduce from these considerations that

$$p_4/p_2 = p_{23}/p_{02} = \frac{x_2y_3 - x_3y_2}{x_0y_2 - x_2y_0} = -\lambda\,,$$

hence also:

$$p_4/p_1 = p_4/p_2 \cdot p_2/p_1 = -\lambda \cdot \mu.$$

Now, if we set

$$X_2 = \mu X_1 \quad \text{and} \quad X_3 = \lambda X_0 \tag{7.4.2}$$

in Equation I, we find $X_0X_1^2(1 - \lambda\mu^2) = 0$, which shows that the intersection of these two planes is indeed a line lying on Y, provided that $\lambda\mu^2 = 1$. On combining the relations we have obtained for this line L_μ, we see that it is given in Plücker coordinates by

$$p_{L_\mu} = [\,\mu^2 : \mu^3 : 0 : -\mu : 1 : 0\,]. \tag{7.4.3}$$

This is the parametric representation of a twisted cubic Γ, drawn on the Klein quadric. It has a point at infinity (corresponding to $\lambda = 0$), namely $p_{L_\infty} = [0 : 1 : 0 : 0 : 0 : 0]$, associated with the line $L_\infty = \{X_1 = X_3 = 0\}$.

The curve Γ is contained in the 3-dimensional space defined by $p_3 = p_6 = 0$ and, in that space, it lies on the smooth quadric $p_1\,p_4 + p_2\,p_5 = 0$ and also on the quadratic cones $p_1\,p_5 - p_4^2 = 0$ and $p_1^2 + p_2\,p_4 = 0$ (on this subject, see Exercise 4.6). We may note that the vertexes of these cones are just the points associated with L_∞ and $L_0 = \{X_0 = X_2 = 0\}$ respectively. □

Type II Surfaces. Here, also, the double line is $D = \{X_1 = X_2 = 0\}$, with Plücker coordinates $p_D = [0 : 0 : 1 : 0 : 0 : 0]$, but this type is very different from the previous one, since there is no disjoint line, such as the line E. In fact, we have the following description.

Proposition 7.4.2. *The family of lines contained in the surface Y of type II is represented on the Klein quadric by a twisted cubic curve. The point associated with the double line belongs to this curve.*

Proof. If L is a line with Plücker coordinates $\{p_i\}$ lying on Y, the surface must contain the points given by (7.3.4), in particular $[\,p_1 : 0 : -p_6 : p_5]$. On substituting in Equation II, we find the necessary condition $p_6 = 0$. This already shows, by virtue of Lemma 7.3.2, that $L \cap D \neq \emptyset$.

And, since $p_6 = x_1\,y_2 - x_2\,y_1$, we obtain as above that $x_2/x_1 = y_2/y_1$ is a constant ratio $\mu \in \mathbf{P}^1_k$ for all points of the line L, provided that we do not have $X_1 = X_2 = 0$ identically, which amounts to saying that $L \neq D$.

The line L is thus contained in the plane $X_2 = \mu X_1$ and we can substitute this expression in Equation 7.4.2. We obtain in this way

$$X_1^2(X_0 - \mu X_3 + \mu^3 X_1) = 0\,,$$

which implies, for $L \neq D$:

$$X_2 = \mu X_1 \quad \text{and} \quad X_0 = \mu X_3 - \mu^3 X_1. \tag{7.4.4}$$

This line contains the points $[\,\mu : 0 : 0 : 1]$ and $[-\mu^3 : 1 : \mu : 0]$. Its Plücker coordinates are therefore

$$p_{L_\mu} = [\,\mu : \mu^2 : \mu^3 : -\mu : 1 : 0\,]. \tag{7.4.5}$$

As previously, this is the parametric representation of a twisted cubic Γ, drawn on the Klein quadric. It has a point at infinity, namely $p_{L_\infty} = [0 : 0 : 1 : 0 : 0 : 0] = p_D$. Thus, we see that L_∞ is just the double line D. In other words, for type II, the double line also belongs to the family of generating lines of the surface.

The curve Γ belongs to the 3-dimensional space defined by $p_1 + p_4 = p_6 = 0$. In particular, it is contained in the quadratic cone $p_2\, p_5 - p_4^2 = 0$, whose vertex is just the point associated with $L_\infty = D$. □

7.5 The 27 Lines

The following theorem has strongly inspired the development of algebraic geometry.

Theorem 7.5.1. *Over an algebraically closed field k, every smooth cubic surface in $\mathbf{P}_k^3$ has exactly 27 distinct lines.*

This striking result was discovered in 1849 in correspondence between Cayley and Salmon: Cayley noted that, for a surface $Y = V(F)$ of degree 3 to contain a given line, it suffices that it contain four points of the line and that this condition may be expressed by four linear conditions on the coefficients of F. By introducing the Grasmannian of lines in $\mathbf{P}_k^3$, which is precisely of dimension 4, he concluded that a general cubic surface had to possess a finite number of lines. Now, Salmon knew how to find a formula giving the number of bitangent planes passing through an point exterior to a surface. Applying this formula, he then showed that the desired number equals 27.

This theorem immediately prompted great interest among geometers; in particular, Steiner communicated the result to Schläfli and both discovered numerous other results concerning lines on a cubic surface. The understanding of the theory of blowing up and minimal surfaces also started from this description. These developments were taken over and used in the twentieth century in order to elaborate

a general classification of surfaces over an algebraically closed field, as well as for the arithmetic study (over an arbitrary field k) of $\bar{k}$-rational surfaces.

Sketch of Proof. We indicate the main points of the proof. The beginning is more or less the same in all approaches. In contrast, the number 27 may be computed in different ways, according to different geometrical arguments ($27 = 3+3\cdot 2\cdot(5-1) = 28-1 = \binom{6}{1}+\binom{6}{2}+\binom{6}{5}$, etc.). Ultimately, the most difficult point is to show that the number of lines equals 27, not only for a cubic surface "in general", but for every smooth cubic surface.

(a) As above, we denote by $\mathbf{P}_k^{19}$ the linear space, which parametrizes all cubic surfaces, and by Ω the Grasmannian of lines in $\mathbf{P}_k^3$. We denote by $\mathcal{I}$ the *incidence variety*, defined as the subset $\mathcal{I} \subset \Omega \times \mathbf{P}_k^{19}$ of couples (p_L, F) such that $L \subset V(F)$:

$$\begin{array}{ccc} & \mathcal{I} \subset \Omega \times \mathbf{P}_k^{19} & \\ {\scriptstyle\varphi}\swarrow & & \searrow{\scriptstyle\psi} \\ \Omega & & \mathbf{P}_k^{19} \end{array}$$

As in Proposition 7.4.1, we can establish whether $L \subset V(F)$ by using the Plücker coordinates p_L of L. However, it is not enough to examine if the polynomial F vanishes at the points z_j of (7.3.4), which could possibly yield four equations and prove easily the existence of at least one line.

In fact, we have seen in §7.4 that there are quite a few degenerate cases, leading to false solutions that we must eliminate by additional reasoning. Nevertheless, we can note that the points on the line L are all of the form

$$z = \alpha_0 z_0 + \alpha_1 z_1 + \alpha_2 z_2 + \alpha_3 z_3,$$

where $\alpha_j \in \bar{k} = k$ (see [Sh], Chap. I, §6, no. 4).

Hence, we may express the fact that $L \subset V(F)$ by writing $F(z) = 0$ for all the $\alpha_j \in k$. This means identifying to zero all the coefficients of the monomials $\alpha_i\alpha_j\alpha_k$ (since F is of degree 3). This leads to 20 homogenous equations of degree 3 in the six variables p_i ($i = 1, \ldots, 6$), together with the relation (7.3.3).

This is not an easy game, but this argument shows that $\mathcal{I}$ is a closed subset of the product $\Omega \times \mathbf{P}_k^{19}$. We examine the two projections φ and ψ of $\mathcal{I}$ on the factors of this product.

(b) It is crucial to show that $\mathcal{I}$ is irreducible. Given a line $L \subset \mathbf{P}_k^3$, associated with the point $p_L \in \Omega$, the surfaces of degree 3, which contain L, form a linear subspace of codimension 4 in $\mathbf{P}_k^{19}$. Indeed, one expresses the fact that a surface $V(F)$ contains L by forcing F to vanish at four of its points, which represents four linear conditions on the coefficients of F. These conditions are independent, because three points do not suffice; indeed, a line in $\mathbf{P}_k^3$ always cuts $V(F)$ at three points. Consequently, the fiber of φ over p_L is a linear variety of dimension 15. This

conclusion holds for all lines equally. Actually, the group $\mathbf{P}\mathrm{GL}_4$ operates on the lines and interchanges the fibers, which therefore are all equivalent.

Since Ω is irreducible and all the fibers are irreducible and of the same dimension, an easy argument[1] shows that $\mathcal{I}$ is an irreducible variety of dimension 19.

(c) To prove that every cubic surface contains at least one line, it suffices to show that the morphism ψ is surjective.

Now, the image of ψ is closed (Theorem 4.2.10). Thus, if ψ were not surjective, its image $\psi(\mathcal{I})$ would be an irreducible algebraic set of smaller dimension than that of $\mathbf{P}^{19}_k$. In this case, a theorem in algebraic geometry states that all non-empty fibers (i.e., the fibers over points in the image) would be of dimension ≥ 1.

However, we already know by examples that this is not the case, since there are cubic surfaces with a finite, non-zero number of lines (Exercise 4.7). Thus, ψ is surjective.

(d) For the same reason, the fibers of ψ cannot be of dimension ≥ 1 on an open set of $\mathbf{P}^{19}_k$. In particular, on smooth cubic surfaces there lie, *in general*, only a finite number of lines. We want to check that this number is finite and equal to 27 for *all* smooth cubics. To that end, we may suppose that $Y = V(F)$ contains the line $L = \{X_2 = X_3 = 0\}$ and we examine the pencil of planes passing through this line, namely $\pi_\lambda = \{X_3 = \lambda X_2\}$, where $\lambda \in \mathbf{P}^1_k$. We may then write $\pi_\lambda \cap Y$ in the plane π_λ as the set of zeros of

$$F_\lambda = X_2\,(a_1X_0^2 + 2b_1X_0X_1 + 2c_2X_0X_2 + d_1X_1^2 + 2e_2X_1X_2 + f_3X_2^2), \quad (7.5.1)$$

whose coefficients[2] are polynomials in λ, of degrees indicated by subscripts.

The set of zeros of F_λ is the union of the line L and of a conic, which decomposes into a pair of lines if and only if the determinant

$$\begin{vmatrix} a & b & c \\ b & d & e \\ c & e & f \end{vmatrix}$$

vanishes. It is a polynomial of degree 5 in λ. Under the hypothesis that Y is smooth, one can show that this polynomial is non-zero and without multiple roots; the details are outlined in [vdW2] (§35). Hence, there are exactly five planes through L, on which one gets in total ten additional lines, because the smoothness makes it possible to show that in each of these planes there are indeed three distinct lines.

If we start with a triangle made of three coplanar lines L_1, L_2, L_3, we thus obtain eight other lines intersecting L_1, eight others intersecting L_2, and eight others intersecting L_3, that is 27 lines in total. It is indeed easy to see that any line

[1] We have not dealt with dimension theory in this book. It is a difficult enough topic in algebra to which several quite different approaches exist (see for instance [Sh], Chap. I). Thus, we are content merely with an intuitive perception.

[2] For simplicity, we may suppose here that k does not have characteristic 2.

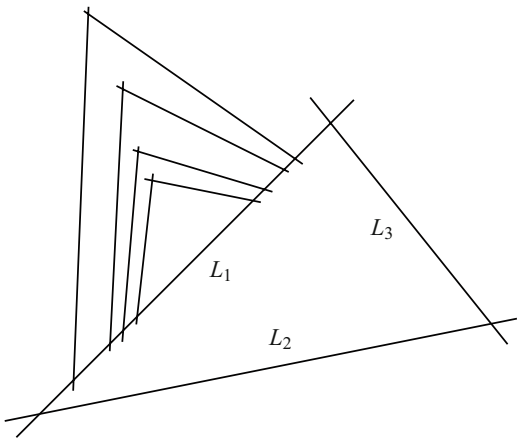


Fig. 7.2 The 27 lines on a cubic surface

contained in Y must intersect the plane generated by L_1, L_2, and L_3, which means that it necessarily meets one of those three lines. □

Remark 7.5.2. In any of these planes, the three lines may possibly meet in one point (an Eckardt point), which slightly complicates the proof. In this case, Figure 7.2 is obviously quite wrong.

The above proof shows that any line on a smooth cubic surface meets exactly 10 other such lines. There are therefore 16 lines on the surface that it does not meet. If we consider two skew lines on the surface, they intersect 20 lines, but there are still five that they do not intersect. Hence, every smooth cubic surface has *triplets* of mutually skew lines.

Lemma 7.5.3. *Given three mutually skew lines on a smooth cubic surface, there exists an unique complementary triplet consisting of three lines that meet the given three lines.*

Proof. We choose three points on each of these lines. There is a surface Q of degree 2 that contains these nine points, since the surfaces of degree 2 in $\mathbf{P}^3_k$ are parametrized by the points of a projective space $\mathbf{P}^9_k = \operatorname{Proj} S^2(k^4)$, where $S^2(k^4)$ denotes the vector space of polynomials of degree 2 in four variables. Since the three lines are mutually skew, one easily sees that Q is not a cone; this quadric is therefore smooth and isomorphic to $\mathbf{P}^1_k \times \mathbf{P}^1_k$ (see Exercise 4.9). One also sees that the conditions are independent, so that Q is uniquely determined. The intersection $Q \cap Y$ is of degree 6 and contains the three lines; the residual component consists of three further lines, transversal to the first three. The unicity follows from the fact that any system of six lines having this configuration is contained in the unique quadric defined by the nine points of intersection of these lines. □

Corollary 7.5.4. *Every smooth cubic surface $Y \subset \mathbf{P}^3_{\mathbf{R}}$ defined over the field of real numbers contains at least three real lines.*

Proof. The set of 27 lines is left invariant by complex conjugation. Since 27 is odd, at least one of the lines is real, say L_1 on Figure 7.2, and it is enough to see that there is another one. Moreover, there are five planes passing through L_1, which contain lines of Y. At least one is defined over $\mathbf{R}$; let L_2 and L_3 be the other two lines contained in this plane. If one of these lines is real, so is the other and we are done. Otherwise, they are conjugated; any other line L_4 that meets L_2 has its conjugate L_5, which meets L_3. We note that these two lines do not meet L_1; otherwise, Y would be singular. If L_4 and L_5 belong to a same plane, this plane contains a real line, which is not L_1 and we have finished. If not, L_4 and L_5 are skew, so that L_1, L_4, and L_5 form a triplet defined over $\mathbf{R}$. The complementary triplet being unique, it is also defined over $\mathbf{R}$ and at least one of the lines that it consists of is real. □

We have given these two results as an illustration. In fact, there are many other properties. Perhaps the most important is the following.

Proposition 7.5.5. *Over an algebraically closed field k, every smooth cubic surface $Y \subset \mathbf{P}^3_k$ has at least one sextuplet of mutually skew lines.*

Proof. To exhibit a sextuplet, let us start by taking two skew lines L_1 and L'_1 on Y. In a plane passing through L_1 in which the residual conic degenerates in a union of two lines $L'_2 \cup L''_2$, the line L'_1 cannot meet both L'_2 and L''_2, since it is not contained in this plane and since Y is non-singular. We take L'_2 to be the line which does not meet L'_1. We obtain in this way a line $L'_2, \ldots, L'_6$ in each of these five planes passing through L_1. These lines do not meet L'_1 and they do not intersect mutually; indeed, L'_3 meets the plane generated by L_1 and L'_2 in only one point, which is located on L_1 but not on L'_2. The six lines $L'_1, \ldots, L'_6$ are therefore mutually skew. □

On interchanging the roles of L_1 and L'_1 in this construction, we obtain a second sextuplet. The union of these two sextuplets forms a *double-six*, a structure discovered by Schläfli in 1858. On every smooth cubic surface, there are 72 sextuplets of mutually skew lines, distributed into 36 double-sixes.

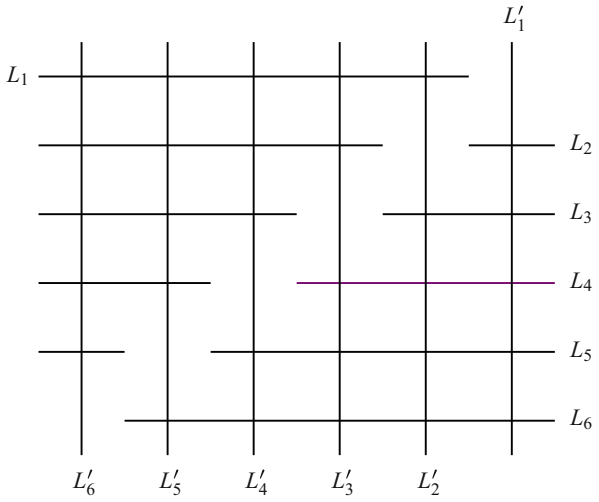
Figure 7.3 exhibits an additional property of this concept: just like L_1, the line L_2 meets all the lines L'_i except one, which we designate by L'_2 in order to highlight symmetry.

Proposition 7.5.6. *Given a sextuplet of mutually skew lines on a smooth cubic surface, there is a unique complementary sextuplet such that the union of the two forms a double-six.*

Proof. Unicity is obvious, according to Lemma 7.5.3, because the complementary sextuplet to $\{L_1, \ldots, L_6\}$ is also the union of the triplets complementary to $\{L_1, L_2, L_3\}$ and to $\{L_4, L_5, L_6\}$.

This argument also gives the existence; it suffices to verify that the union of the two complementary triplets has the desired properties. Recall that $L_1 \cup L_2 \cup L_3 \cup L'_4 \cup L'_5 \cup L'_6$ is the intersection of Y with a quadric $Q \subset \mathbf{P}^3_k$. Since L_4 is not one of these six lines, its intersection with Q consists of two points. Consequently, L_4 cannot cut all the lines L'_4, L'_5, L'_6. By choosing convenient numbering, we may

Fig. 7.3 A double-six



agree that $L_4 \cap L_4' = \emptyset$ and that L_4 has a non-empty intersection with the two other lines. By continuing this argument, we find the configuration in Figure 7.3. □

This statement has an arithmetic corollary.

Corollary 7.5.7. *If a cubic surface $Y \subset \mathbf{P}_k^3$ has a double-six defined over a field k, it also has a sextuplet defined over k or over a quadratic extension of k.*

Proof. The double-six contains exactly two sextuplets, which are either k-rational or interchanged under the action of the Galois group $\mathrm{Gal}(\bar{k}/k)$. □

Remark 7.5.8. The group of permutations of the 27 lines has a subgroup with 51,840 elements, which correspond to those permutations that preserve the intersections of lines on a cubic surface. This concerns only mutually incidence relations. *This group does not take into account the Eckardt points.*

Proposition 7.5.9. *Over an algebraically closed field k, every smooth cubic surface $Y \subset \mathbf{P}_k^3$ is k-rational.*

Proof. Applying Theorem 7.5.1, we may assume that Y contains the line $L = \{X_2 = X_3 = 0\}$. We may also consider the family of planes passing through L. A general plane π_λ in this family has equation $X_3 = \lambda X_2$, with $\lambda \in \mathbf{P}_k^1$.

The intersection of Y with π_λ is the union of L and of a variable smooth conic C_λ defined over the field $K = k(\lambda)$. As in (7.5.1), the equation of C_λ in π_λ may be written in the form

$$a_1 X_0^2 + 2b_1 X_0 X_1 + 2c_2 X_0 X_2 + d_1 X_1^2 + 2e_2 X_1 X_2 + f_3 X_2^2 = 0,$$

whose coefficients are polynomials in λ of degrees specified by subscripts. We can apply Tsen's Theorem (see Theorem 10.1.4): $K = k(\lambda)$ is a C_1 field. Therefore, $C_\lambda(K) \neq \emptyset$ and Proposition 4.2.7 implies that $C_\lambda \cong \mathbf{P}^1_K$.

This construction defines a *fibering* $f : Y \to \mathbf{P}^1_k$, which to each point $P \in C_\lambda$ associates the parameter $\lambda \in \mathbf{P}^1_k$. This map is well-defined, even at the points of the line L, as π_λ is in this case the tangent plane to the cubic surface at the point P. Therefore, this map is a morphism from Y to $\mathbf{P}^1_k$.

As in Example 5.5.5, f is also a dominant rational map and Proposition 5.5.2 yields an embedding $f^* : K = k(\lambda) = k(\mathbf{P}^1_k) \hookrightarrow k(Y)$. The *fiber* of f over $\lambda \in \mathbf{P}^1_k$ is the conic C_λ. Moreover, on substituting $\lambda = X_3/X_2$, the equation of Y over k is the same as that of C_λ over K. The field $k(Y)$ therefore coincides with $K(C_\lambda) = K(u)$, where u is transcendental over K. Hence, an isomorphism $k(Y) \cong K(u) = k(\lambda, u)$. □

This reasoning by fibering is quite classical in numerous applications.

Remark 7.5.10. If the field k were not algebraically closed, the field $k(\lambda)$ would not be C_1, and C_λ would not be isomorphic to $\mathbf{P}^1_K$, even if the curves C_λ had k-rational points for an infinity of values of λ, since we know that Y is k-unirational. Actually, it is shown that there exist smooth cubic surfaces, defined over $k = \mathbf{Q}$, with three rational lines (coplanar), which are not $\mathbf{Q}$-rational ([CTs], Ex. 4.4.2).

Notation 7.5.11. Given a smooth cubic surface $Y \subset \mathbf{P}^3_k$, we denote by S_n any subset of mutually skew lines, contained in Y and invariant under the action of the Galois group $\mathrm{Gal}(\bar{k}/k)$.

Thus, a S_3 is a triplet defined over k; a S_1 is a k-rational line. It is also known that $n \leq 6$.

Proposition 7.5.12. *If a smooth cubic surface $Y \subset \mathbf{P}^3_k$ contains a subset S_2, it is k-rational.*

Proof. We denote by L_1 and L_2 two skew lines forming a S_2 on Y. We also fix an arbitrary plane $\pi \subset \mathbf{P}^3_k$. Let $Q \in Y$ be in general position, that is, in an open subset of Y, so as to avoid undesirable situations such as $Q \in L_1$. For $i = 1, 2$, let π_i be the plane passing through Q and containing L_i. The intersection $\pi_1 \cap \pi_2$ is a line L that meets L_1 and L_2; it also meets the plane π in a point R. This construction defines a map that sends Q to R univocally and is defined over the base field, since S_2 is k-rational. The inverse map is defined in the same manner, starting from a point $R \in \pi$, with which the third intersection point of the line L determined by R and the L_i-s is associated. In this way, we have found a birational map between Y and $\pi \cong \mathbf{P}^2_k$. □

Theorem 7.5.13 (Criterion of Segre and Swinnerton-Dyer). *A smooth cubic surface $Y \subset \mathbf{P}^3_k$ such that $Y(k) \neq \emptyset$ is k-rational if and only if it contains a k-rational subset S_n with $n = 2$, 3, or 6.*

This criterion (which we do not prove) was discovered by B. Segre, but the case $n = 1$ was not treated. Swinnerton-Dyer gave the complete statement. Knowing that there are cubic surfaces with a rational line that are not rational, it is quite striking that this criterion states that *no* surface of this type can be k-rational if it does not also have a S_n for $n \geq 2$. On the other hand, the existence of a S_6 on Y does not imply that $Y(k) \neq \emptyset$ (see Corollary 9.3.5).

7.6 Blowing Up

Let $P \in \mathbf{P}^2_k$ be the point with coordinates $[X_0 : X_1 : X_2] = [1 : 0 : 0]$. The family of conics passing through P is a vector space of dimension 5. By choosing generators for this space, one defines a rational map

$$\Phi : \mathbf{P}^2_k \dashrightarrow \mathbf{P}^4_k$$
$$[X_0 : X_1 : X_2] \longmapsto [Y_0 : Y_1 : Y_2 : Y_3 : Y_4] = [X_1X_2 : X_0X_1 : X_0X_2 : X_1^2 : X_2^2].$$

This map is not defined at P, but it is for all other points in the plane and it is easy to see that it is an injective morphism of $\mathbf{P}^2_k \setminus \{P\}$ into $\mathbf{P}^4_k$. Its image $\Phi(\mathbf{P}^2_k \setminus \{P\})$ is a surface whose closure $\Sigma \subset \mathbf{P}^4_k$ verifies the following equations:

$$Y_0Y_1 = Y_2Y_3\,, \quad Y_0Y_2 = Y_1Y_4\,, \quad Y_0^2 = Y_3Y_4. \tag{7.6.1}$$

The first two equations define an intersection of two quadrics in $\mathbf{P}^4_k$, i.e., a surface of degree 4. But this surface is reducible: one of its components is the plane $\pi = \{Y_1 = Y_2 = 0\}$. The third equation causes the elimination of this irreducible component. Thus, Σ is a surface of degree 3.

Remark 7.6.1. To calculate the degree of Σ, one may also count the number of its intersections with a plane in general position in $\mathbf{P}^4_k$. Such a plane is the intersection of two hyperplanes of the form $\sum \lambda_i Y_i = 0$. The intersection with the image of Φ is therefore the image of the intersection of two conics $\sum \lambda_i \Phi(X)_i = 0$, belonging to the linear system of conics passing through P. Now, two general conics meet in four points, but the point P is fixed and does not contribute to $\mathrm{Im}(\Phi)$; in fact, it has no image by Φ. We must count only *variable points* and there are $2 \cdot 2 - 1 = 3$.

Σ has no singular point, but it is not a cubic surface in the sense of the definition in §7.1, since it is not a hypersurface. We shall see later (Corollary 7.6.8) that it is not isomorphic to a smooth cubic surface in $\mathbf{P}^3_k$. In fact, it looks more like one of the ruled surfaces in §7.4, because if we combine the first two equations of (7.6.1), we find that Σ also verifies the equation

$$Y_1^2Y_4 = Y_2^2Y_3. \tag{7.6.2}$$

This relation means that Σ is contained in the cone with vertex $[1:0:0:0]$ over the surface $S \subset \mathbf{P}^3_k$ defined by Equation (7.6.2). One recognizes a ruled surface of type I. Moreover, there is a morphism

$$\Psi : \Sigma \to S$$
$$[Y_0 : Y_1 : Y_2 : Y_3 : Y_4] \longmapsto [Y_1 : Y_2 : Y_3 : Y_4],$$

which realizes Σ as a smooth model of S, which means that Ψ is not only a morphism of Σ into S but it is also an isomorphism away from the plane $\pi = \{Y_1 = Y_2 = 0\}$. Indeed, the image of $\pi \cap \Sigma$ by Ψ is the singular locus of S, namely the line $D = \{Y_1 = Y_2 = 0\} \subset S$, and the inverse morphism $\tau : S \setminus D \to \Sigma$ has the following definition:

$$\tau : [Y_1 : Y_2 : Y_3 : Y_4] \mapsto \begin{cases} [Y_2Y_3 : Y_1^2 : Y_1Y_2 : Y_1Y_3 : Y_1Y_4] & \text{if } Y_1 \neq 0 \\ [Y_1Y_4 : Y_1Y_2 : Y_2^2 : Y_2Y_3 : Y_2Y_4] & \text{if } Y_2 \neq 0. \end{cases}$$

We also observe that $\Psi^{-1}(D)$ is the conic C with equation $Y_0^2 = Y_3Y_4$ in the plane π. The restriction of Ψ to the curve C is not injective, but sends two points on one point, which is consistent with the fact that D is a double line of S.

Remark 7.6.2. If $L \subset \mathbf{P}^2_k$ is a line that passes through the point P, its image by Φ is a line. Indeed, as in Remark 7.6.1, we can calculate the degree of this image by counting its number of intersections with a hyperplane $\sum \lambda_i Y_i = 0$ in general position in $\mathbf{P}^4_k$. The intersection with $\Phi(L \setminus \{P\})$ is therefore the image of the intersection of L with a conic $\sum \lambda_i \Phi(X)_i = 0$ belonging to the linear system of conics passing through P. Now, a general conic meets a line in two points, but the point P is fixed and has no image by Φ. Hence, there is only one variable point and the degree is 1. Thus, the surface Σ contains an infinity of lines, whose images by Ψ are nothing but the lines of the ruled surface S (except D, which is the image of the conic $\pi \cap \Sigma$). The same argument shows that the images of the other lines of the plane are conics drawn on Σ, since we cannot subtract 1, as for the lines passing through P.

In addition, the surface Σ contains the line $E = \{Y_0 = Y_3 = Y_4 = 0\}$, which lies entirely away from the image of Φ. Although there are an infinite number of lines on Σ, this one plays a very particular role. There is indeed a morphism $\sigma : \Sigma \to \mathbf{P}^2_k$, which is the inverse of Φ and which shrinks E in one point, namely P; everywhere else it is an isomorphism. This morphism has the following definition:

$$\sigma : [Y_0 : Y_1 : Y_2 : Y_3 : Y_4] \mapsto \begin{cases} [Y_1 : Y_3 : Y_0] & \text{if } [Y_1 : Y_3 : Y_0] \neq [0:0:0] \\ [Y_2 : Y_0 : Y_4] & \text{if } [Y_2 : Y_0 : Y_4] \neq [0:0:0]. \end{cases}$$

The consistency condition (4.2.1) between these two formulas is ensured, since we have the relations (7.6.1) on Σ. All points of E have the same image, namely the point P.

Remark 7.6.3. If $L \subset \mathbf{P}^2_k$ is a line that passes through the point P, having equation $X_2 = \lambda X_1$ (with $\lambda \in \mathbf{P}^1_k$), its image by Φ is the line whose equations are $\{Y_2 = \lambda Y_1,\ Y_4 = \lambda Y_0,\ Y_0 = \lambda Y_3\}$. This line cuts the line E at the point $[0 : 1 : \lambda : 0 : 0]$. Hence, there is a bijection between the points of E and the lines of the plane that pass through P, i.e., the tangent directions at P.

Definition 7.6.4. The surface Σ is called the *blowing up* of the plane at the point P. This surface differs from $\mathbf{P}^2_k$ inasmuch as the point P is replaced by the line E, which represents bijectively all tangent directions at P. We also say that E is the *blowing up* of the point P. The inverse morphism σ is called *blowing down*, or even *σ-process*.

It is by now understood that the notion of blowing up is one of the most fundamental of algebraic geometry. It is a basic operation, which generalizes to all varieties and several points can be blown up successively, in any order, as well as simultaneously. It is shown that, under certain natural conditions, the result is the same.

There is also an intersection theory on every smooth surface Y. Recall that a *divisor* on Y is an element of the free abelian group generated by irreducible curves. As long as the curves are distinct, the theory amounts to counting their intersection points, assigning to them the correct multiplicities. But it can happen that one has to intersect divisors having a common component. In this case, one shows that one can proceed algebraically, even if certain *self-intersection* numbers are negative. Moreover, the computation should depend only on the linear equivalence classes of the divisors.

Example 7.6.5. Consider the example of a smooth cubic surface $Y \subset \mathbf{P}^3_k$. Let L be a line contained in Y. Let π_1 and π_2 be two distinct planes containing L. The intersection of each of these planes with the surface is the union of L and of a conic. In the language of divisors, we may write $\pi_1 \cap Y = L + C_1$ and $\pi_2 \cap Y = L + C_2$, where C_1 and C_2 are conics. Since Y is smooth, it is easy to see that $C_1 \cap C_2 = \emptyset$. On the other hand, two planes in general position intersect along a line, which cuts Y again at three points. Consequently,

$$3 = (L+C_1)\,.\,(L+C_2) = (L\,.\,L)+(L\,.\,C_2)+(C_1\,.\,L)+(C_1\,.\,C_2) = (L^2)+2+2+0,$$

so $(L^2) = -1$.

We can make the same computation on Σ: two lines $L_1,\ L_2$ in $\mathbf{P}^2_k$ usually meet in one point; this property must be reflected on Σ, even if one of the lines passes through the point P; thus,[3] we have: $\sigma^{-1}(L_1)\,.\,\sigma^{-1}(L_2) = (L_1\,.\,L_2) = 1$. By extension, the same computation remains valid if the two lines pass through the point P. In this case, we can write $\sigma^{-1}(L_i) = E + \widetilde{L}_i$, where the $\widetilde{L}_i$ are – as we have seen – lines

[3]The first product is on Σ; the second on $\mathbf{P}^2_k$. As long as the intersections are a finite number of points, there is no difficulty.

on Σ (Remark 7.6.2). These lines do not meet, because L_1 and L_2 intersect only at P, and so $\widetilde{L}_1$ and $\widetilde{L}_2$ can intersect only on the line E. However, we have also seen (Remark 7.6.3) that each one of these lines meets E in a different point, which corresponds to the tangent direction it represents. Consequently, we have:

$$1 = (E + \widetilde{L}_1) \,.\, (E + \widetilde{L}_2) = (E^2) + 1 + 1 + 0,$$

and so $(E^2) = -1$.

Definition 7.6.6. We call *exceptional divisor of the first kind* on a smooth surface Y any curve $E \subset Y$ isomorphic to $\mathbf{P}^1_k$ and such that $(E^2) = -1$ on Y.

Remark 7.6.7. If $L \subset \mathbf{P}^2_k$ is a line passing through P, we have: $\sigma^{-1}(L) = E + \widetilde{L}$, and $(\sigma^{-1}(L)^2) = (L^2) = 1$, so that $1 = (E + \widetilde{L})^2 = (E^2) + 2\,(E \,.\, \widetilde{L}) + (\widetilde{L}^2) = -1 + 2 + (\widetilde{L}^2)$. Consequently, $(\widetilde{L}^2) = 0$ and the line $\widetilde{L} \subset \Sigma$ is not an exceptional divisor of the first kind!

Corollary 7.6.8. *The surface $\Sigma \subset \mathbf{P}^4_k$ is not isomorphic to any smooth cubic surface in $\mathbf{P}^3_k$.*

Proof. Σ possesses an unique exceptional divisor of the first kind, in contrast to cubic surfaces in $\mathbf{P}^3_k$, which have 27 lines (Example 7.6.5). □

It is not enough to notice that Σ has an infinity of lines, to conclude that Σ is not isomorphic to a smooth cubic in $\mathbf{P}^3_k$. Indeed, by an isomorphism, the lines on Σ might very well correspond to curves of higher degree on the other surface (conics, twisted cubics, etc.).

The following criterion is very famous and often useful. It states that the only curves that can be blown down are exceptional divisors of the first kind.

Proposition 7.6.9 (Castelnuovo's Criterion). *Let Y be a smooth surface and $E \subset Y$ a curve isomorphic to $\mathbf{P}^1_k$. Then, $(E^2) = -1$ if and only if there is a smooth surface Y_0, a point $P \in Y_0$ and a morphism $\sigma : Y \to Y_0$ with $\sigma^{-1}(P) = E$ such that the restriction of σ to $\sigma^{-1}(Y_0 \setminus \{P\})$ is an isomorphism on $Y_0 \setminus \{P\}$.*

We shall not prove this. Instead, we shall see how to obtain the cubic surfaces in $\mathbf{P}^3_k$ by blowing up six points in the plane. So, let us consider a set of six points $P_1, \ldots, P_6$ in general position in $\mathbf{P}^2_k$. This simply means that the points are distinct, that there are no three points on a line and that they are not all on the same conic. To blow them up simultaneously, it suffices to consider the linear system of cubics passing through the six points. This is a vector space of dimension 4, for the vector space of plane cubics is of dimension 10 and the six points impose six independent linear conditions. By choosing generators $\varphi_i(X)$ for this space, one defines a rational map

$$\begin{aligned} \Phi : \mathbf{P}^2_k &\dashrightarrow \mathbf{P}^3_k \\ [X_0 : X_1 : X_2] &\longmapsto [\varphi_0(X) : \cdots : \varphi_3(X)]. \end{aligned}$$

This map is not defined at the points P_i, but it is at all other points of the plane and one can see that it is an injective morphism of $\mathbf{P}^2_k \setminus \{P_i\}_{i=1}^6$ into $\mathbf{P}^3_k$.

Lemma 7.6.10. *The image $\Phi(\mathbf{P}^2_k \setminus \{P_i\})$ is a surface whose closure $Y \subset \mathbf{P}^3_k$ verifies an equation of degree* 3.

Proof. We can compute the degree of Y by counting its number of intersections with a line in a general position in $\mathbf{P}^3_k$. Such a line is the intersection of two hyperplanes of the form $\sum \lambda_i Y_i = 0$. The intersection with the image of Φ is then the image of the intersection of the two cubics $\sum \lambda_i \Phi(X)_i = 0$, belonging to the linear system of cubics passing through the P_i. Now, two general cubics meet in nine points, but P_i are fixed and do not contribute to $\mathrm{Im}(\Phi)$; in fact, they have no image by Φ. We must count only variable points, and there are $3 \cdot 3 - 6 = 3$ of them. □

These results are classical and we do not give all the details of the proofs. What should be remembered is that this construction, by blowing up six points of the plane, produces smooth cubic surfaces. If the field k is algebraically closed, all smooth cubic surfaces in $\mathbf{P}^3_k$ are obtained in this way; this is essentially a consequence of Castelnuovo's criterion (Proposition 7.6.9). If $k \neq \bar{k}$, a k-rational set of six points may also be blown up, but that does not cover all possible cases of smooth cubic surfaces defined over the field k. For instance, it is known that a smooth cubic surface does not always have a k-rational sextuplet. Moreover, it does not always have a rational point. Indeed, that is why the arithmetic study of these surfaces is of particular interest (see §9.3).

Let us say for the sake of brevity that the blowing down morphism $\sigma : Y \to \mathbf{P}^2_k$, inverse of Φ, contracts six lines $E_i \subset Y$ on the six points P_i. But there are other exceptional divisors, which are the 15 inverse images of the lines of the plane passing through two of the points P_i and the six inverse images of the conics that pass through five of the six points P_i. We recover 27 as the sum $6 + 15 + 6$.

In the next section, we return to this situation in more detail by introducing the *Néron–Severi group* of divisor classes on a smooth cubic surface.

7.7 The Néron–Severi Group

Among the different equivalence relations between divisors on a non-singular projective variety Y, one of the most interesting[4] is *algebraic equivalence*. We do not define it here, but one should keep in mind that the *Néron–Severi group* $\mathrm{NS}(Y)$ of divisors modulo algebraic equivalence on Y is always of finite type. For these questions, the base field is supposed to be algebraically closed; the picture over an arbitrary field follows by studying the action of Galois (Galois cohomology).

[4]Sometimes algebraic equivalence coincides with linear equivalence; this is the case for cubic surfaces and the Néron–Severi group is identical to the Picard group. In general, however, the two relations are very different; an example is the product of a line with an elliptic curve.

If Y is a surface, the intersection of divisors induces a quadratic form on the Néron–Severi group, with values in $\mathbf{Z}$. The Hodge Theorem specifies that this form is negative definite on the orthogonal space to any ample divisor (corresponding to a hyperplane section).

Besides, if $\widetilde{Y}$ is the blowing up of Y in one point, we have $\mathrm{NS}(\widetilde{Y}) = \mathrm{NS}(Y) \oplus \mathbf{Z}e$, so that e is the class of the exceptional divisor; moreover, $e^2 = -1$ and e is orthogonal to $\mathrm{NS}(Y)$.

Example 7.7.1. For $Y = \mathbf{P}^2_k$, the computation is simple: all divisors of the same degree are linearly equivalent and correspond to the same class in the Néron–Severi group. In this case, $\mathrm{NS}(\mathbf{P}^2_k) = \mathbf{Z}\lambda_0$, where λ_0 is the class of a line.

Example 7.7.2. If $Y \subset \mathbf{P}^3_k$ is a smooth quadric, we may write its equation in the form $Y_0Y_3 = Y_1Y_2$ (we recall that the field is supposed algebraically closed). This shows that Y is isomorphic to $\mathbf{P}^1_k \times \mathbf{P}^1_k$ (see Exercise 4.9). Actually, one sees directly that, for $\lambda, \mu \in \mathbf{P}^1_k$, the lines with equations $E_\lambda = \{Y_2 = \lambda\, Y_0\} \cap \{Y_3 = \lambda\, Y_1\}$ form one system of skew lines on Y, and the lines with equations $F_\mu = \{Y_1 = \mu\, Y_0\} \cap \{Y_3 = \mu\, Y_2\}$ constitute another one. On the other hand, the line E_λ meets the line F_μ at the point $[1 : \mu : \lambda : \lambda\mu]$. One easily deduces that $\mathrm{NS}(Y) = \mathbf{Z}e \oplus \mathbf{Z}f$, where e is the class of E_λ and f that of F_μ. We have the relations

$$(e^2) = (f^2) = 0\,, \qquad (e\,.\,f) = 1.$$

We may also consider blowing up two points of the plane by considering the linear system of conics that contain them. If $P_1 = [0 : 1 : 0]$ and $P_2 = [0 : 0 : 1]$, this four-dimensional vector space is generated by X_0^2, X_0X_1, X_0X_2, and X_1X_2. We obtain in this way a rational map

$$\Phi : \mathbf{P}^2_k \dashrightarrow \mathbf{P}^3_k$$
$$[X_0 : X_1 : X_2] \longmapsto [Y_0 : Y_1 : Y_2 : Y_3] = [X_0^2 : X_0X_1 : X_0X_2 : X_1X_2].$$

The image of Φ is a surface of degree 2, since the degree is computed by counting the number of intersections with a line in general position in $\mathbf{P}^3_k$: we are brought to the study of the intersection of two conics $\sum \lambda_i \Phi(X)_i = 0$. Now, two general conics meet in four points, but here there are two fixed points and two variable points left.

As a matter of fact, it is not so hard to find the equation of the image of Φ, as one sees at once that $Y_0Y_3 = Y_1Y_2$. However, the map Φ is not an injective morphism of $\mathbf{P}^2_k \setminus \{P_1, P_2\}$ into $\mathbf{P}^3_k$, because the line $L = \{X_0 = 0\}$ has a single point as image. The point P_1 is blown up into the line $F_\infty = \{Y_0 = Y_2 = 0\}$, and the point P_2 into $E_\infty = \{Y_0 = Y_1 = 0\}$, but the strict transform $\widetilde{L}$ of L, which verifies $(\widetilde{L}^2) = -1$, is then blown down on the intersection of E_∞ and F_∞. This is why we do not have $(e^2) = (f^2) = -1$.

Example 7.7.3. If $Y \subset \mathbf{P}^3_k$ is a smooth cubic surface, it contains a sextuplet of skew lines (Proposition 7.5.5), which, as seen above, have self-intersection -1 (Example 7.6.5). According to Castelnuovo's criterion (Proposition 7.6.9), we can

blow down the lines of this sextuplet simultaneously, and this yields a surface isomorphic to the plane. To study the divisors on Y over an algebraically closed field, we may then write Y as the blowing up of the plane at six points.

The Néron–Severi group of Y is free of rank 7, generated by the class λ_0 of a general line of the plane and by the classes λ_i $(i = 1, \ldots, 6)$ of the six exceptional divisors over the six blown-up points. Thus, $\mathrm{NS}(Y) = \mathbf{Z}\lambda_0 \oplus \bigoplus_{i=1}^{6} \mathbf{Z}\lambda_i$ and the intersection numbers are:

$$\lambda_0^2 = 1\,, \quad \lambda_i^2 = -1 \quad (i = 1, \ldots, 6)\,, \quad \lambda_i \,.\, \lambda_j = 0 \quad (i \neq j). \tag{7.7.1}$$

Notice that the transform of a general line of the plane is of degree 3; consequently, the class λ_0 is represented on Y by a twisted cubic, which intersects none of the six exceptional lines corresponding to the λ_i $(i = 1, \ldots, 6)$.

Another remarkable class is the "anticanonical class" π (the opposite of the class of differential forms on Y), which is the strict transform of a plane cubic passing through the six base points. It is also the class of a hyperplane section. One has:

$$\pi = 3\lambda_0 - \sum_{i=1}^{6} \lambda_i \,.$$

One verifies that the degrees are indeed $\pi \,.\, \lambda_0 = 3$ and $\pi \,.\, \lambda_i = 1$ $(i = 1, \ldots, 6)$.

As an application of this description, we have for instance the following preposition.

Proposition 7.7.4. *There are* 72 *classes of twisted cubics on a smooth cubic surface* $Y \subset \mathbf{P}_k^3$.

Proof. Let $\gamma = n_0\lambda_0 - \sum_{i=1}^{6} n_i\lambda_i$ be the class of a twisted cubic Γ in the Néron–Severi group of Y. On calculating the product of γ with the λ_i (which correspond to positive divisors), we see that the integers n_i are all non-negative. The degree of the curve is given by its intersection with a plane; hence, the condition $3 = \pi \,.\, \gamma = 3n_0 - \sum_{i=1}^{6} n_i$.

For the sequel of the computation, it is necessary to introduce another invariant, since curves are characterized not only by their degrees but also by their *genus*: twisted cubics have genus 0, whereas plane sections of Y have genus 1. The *adjunction formula* applied to the cubic surface gives the arithmetic genus $p_a(\Gamma)$ as:

$$p_a(\Gamma) = \frac{(\Gamma^2) - \deg \Gamma}{2} + 1.$$

If $p_a(\Gamma) = 0$ and $\deg \Gamma = 3$, we obtain in this way the condition $1 = \gamma^2 = n_0^2 - \sum_{i=1}^{6} n_i^2$. Putting together the two relations we obtained (one for the degree, the other for the genus), we may write:

$$\sum_{i=1}^{6} n_i = 3(n_0 - 1) \quad \text{and} \quad \sum_{i=1}^{6} n_i^2 = n_0^2 - 1.$$

Apply the Schwarz inequality $\sum_{i=1}^{6} n_i\, m_i \le (\sum_{i=1}^{6} n_i^2)^{1/2}\,(\sum_{i=1}^{6} m_i^2)^{1/2}$ to the vectors (n_i) and (m_i) with $m_i = 1$ for every i. This yields:

$$3(n_0 - 1) = \sum_{i=1}^{6} n_i \le \sqrt{6}\,\Big(\sum_{i=1}^{6} n_i^2\Big)^{1/2} = \sqrt{6}\,\sqrt{n_0^2 - 1}.$$

On solving this inequality, we find $(n_0 - 5)(n_0 - 1) \le 0$, and hence $1 \le n_0 \le 5$. Up to a permutation, the possible values are:

$$\begin{aligned}
&n_0 = 1: && n_1 = \cdots = n_6 = 0\\
&n_0 = 2: && n_1 = n_2 = n_3 = 1\,; \quad n_4 = n_5 = n_6 = 0\\
&n_0 = 3: && n_1 = 2\,; \quad n_2 = n_3 = n_4 = n_5 = 1\,; \quad n_6 = 0\\
&n_0 = 4: && n_1 = n_2 = n_3 = 2\,; \quad n_4 = n_5 = n_6 = 1\\
&n_0 = 5: && n_1 = \cdots = n_6 = 2,
\end{aligned}$$

that is, $1 + \binom{6}{3} + 6 \cdot 5 + \binom{6}{3} + 1 = 72$ different classes. □

Exercises

7.1. Show that the vector space $S^d(k^{n+1})$ of homogenous polynomials of degree d in $n+1$ variables is of dimension $\binom{d+n}{n}$.

7.2. Show that every rational number is a sum of three cubes (of rational numbers!). (*Hint:* apply Theorem 7.2.1.)

7.3. Show that every point $p \in \mathbf{P}_k^5$ verifying relation (7.3.3) corresponds to a line of $\mathbf{P}_k^3$.

7.4. Show that the *Cremona Transformation*

$$\Phi : [X_0 : X_1 : X_2 : X_3] \mapsto [X_1X_2X_3 : X_2X_3X_0 : X_3X_0X_1 : X_0X_1X_2]$$

is a birational map from $\mathbf{P}_k^3$ to $\mathbf{P}_k^3$. Show that the image of a plane in $\mathbf{P}_k^3$ in general position is a cubic surface with four double points. What is the image of a line in $\mathbf{P}_k^3$ in general position?

7.5. Show that, for $a, b \in k^*$, the cubic surfaces $X_0^3 + X_1^3 + X_2^3 + aX_3^3 = 0$ and $X_0^3 + X_1^3 + X_2^3 + bX_3^3 = 0$ are not projectively k-isomorphic if a/b is not a cube in the field k.
(*Hint:* examine the Eckardt points.)

Chapter 8
p-Adic Completions

The field of p-adic numbers was introduced by Hensel at the beginning of the twentieth century. This remarkable idea greatly simplifies computations involving congruences, and is also of considerable theoretical interest, preparing the way for powerful generalizations.

8.1 Valuations

Definition 8.1.1. Let $p \in \mathbf{Z}$ be a prime; if $m \in \mathbf{Z}$ is a non-zero integer, we denote by $v_p(m)$ the exponent of p in the decomposition of m as a product of powers of primes. If $\alpha = m/n \in \mathbf{Q}^*$, we call *$p$-adic valuation* of α the integer $v_p(\alpha) = v_p(m) - v_p(n)$. Moreover, we agree to set $v_p(0) = +\infty$.

Lemma 8.1.2. *v_p is a homomorphism of the multiplicative group $\mathbf{Q}^*$ onto the additive group $\mathbf{Z}$: $v_p(\alpha\beta) = v_p(\alpha) + v_p(\beta)$. Also, we have the* ultrametric inequality

$$v_p(\alpha + \beta) \geq \min(v_p(\alpha), v_p(\beta)).$$

If $v_p(\alpha) \neq v_p(\beta)$, we even have the equality $v_p(\alpha + \beta) = \min(v_p(\alpha), v_p(\beta))$. □

We say that v_p is an *additive valuation.* We consider it to be a logarithm of a *p-adic absolute value*

$$|\alpha|_p = p^{-v_p(\alpha)},$$

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_8

if we also define $|0|_p = 0$. We have: $|\alpha\beta|_p = |\alpha|_p \cdot |\beta|_p$ for all $\alpha, \beta \in \mathbf{Q}$. The ultrametric inequality reads:

$$|\alpha + \beta|_p \leq \max(|\alpha|_p, |\beta|_p).$$

If $|\alpha|_p \neq |\beta|_p$, we have in fact the equality $|\alpha + \beta|_p = \max(|\alpha|_p, |\beta|_p)$.

Definition 8.1.3. More generally, an *absolute value* defined on a field k is a map $\varphi : k \to \mathbf{R}_+$ such that $\varphi(0) = 0$, which is a homomorphism of k^* into $\mathbf{R}_+^*$ and verifies the triangle inequality

$$\varphi(a + b) \leq \varphi(a) + \varphi(b).$$

Two absolute values φ_1 and φ_2 are called *equivalent* if there is a real number $c > 0$ such that $\varphi_1(a) = \varphi_2(a)^c$ for all $a \in k$.

Every absolute value defines a metric space structure on the field k, with distance $\delta(a, b) = \varphi(a - b)$. Two equivalent absolute values induce the same topology.

In contrast to the ordinary absolute value, which satisfies Archimedes' axiom ($\forall\, \alpha,\ \exists\, N \in \mathbf{N}^*$ such that $|N\alpha| > 1$), the p-adic metric is *non-Archimedean* . The field of rational numbers has an infinity of metrics: the Archimedean metric, as a subset of $\mathbf{R}$ and the non-Archimedean metrics defined by $\delta_p(a, b) = |a - b|_p$, for very prime p. Ostrowski's Theorem states that these are the only metrics induced by an absolute value.

Theorem 8.1.4 (Ostrowski). *Every non-trivial absolute value defined on* $\mathbf{Q}$ *is equivalent either to the ordinary absolute value or to a* p*-adic absolute value.*

Proof. Assume that $\varphi(n) \leq 1$ for all $n \in \mathbf{N}$. If $\varphi(n) = 1$ for all $n \in \mathbf{N}^*$, then $\varphi|_{\mathbf{Q}^*}$ is the trivial homomorphism. Otherwise, there is a prime p such that $\varphi(\,p) < 1$. For any other prime q, we have $\varphi(q) = 1$. If not, by Bézout's Theorem, we could find an expression of the form $mp^k + nq^k = 1$ with $\varphi(\,p^k) < 1/2$ and $\varphi(q^k) < 1/2$. Then, $\varphi(1) \leq \varphi(m)\varphi(\,p^k) + \varphi(n)\varphi(q^k) < 1$, which is impossible, since $\varphi(1) = 1$. Finally, $\varphi(\,p) = p^{-c} = |p|_p^c$ for a real number $c > 0$, and then $\varphi(n) = |n|_p^c$ for all $n \in \mathbf{N}$; hence, $\varphi(\alpha) = |\alpha|_p^c$ for all $\alpha \in \mathbf{Q}$.

If on the contrary, there exists an integer $N \in \mathbf{N}$ such that $\varphi(N) > 1$, we see on factoring it that there is also a prime q such that $\varphi(q) > 1$ and a real number $c > 0$ such that $\varphi(q) = q^c$. Observe that $c \leq 1$, since for all $n \in \mathbf{N}$, $\varphi(n) = \varphi(1 + \cdots + 1) \leq \varphi(1) + \cdots + \varphi(1) = n$. Now, if p is another prime, there exists for every $\ell \in \mathbf{N}$ a p-adic expansion $q^\ell = m_0 + m_1\, p + \cdots + m_k\, p^k$, where the m_i are integers between 0 and $p - 1$, with $m_k \neq 0$. Moreover, $p^k \leq q^\ell$; hence, $k \leq \ell \log_p q$. Let $K = \max_{m=1}^{p-1} \varphi(m)$; then,

$$\varphi(q)^\ell \leq K \sum_{i=0}^{k} \varphi(\,p)^i \leq K\, (\ell \log_p q + 1)\, \max_{i=0}^{k} \varphi(\,p)^i,$$

which entails that $\varphi(p) > 1$, because ℓ may be arbitrarily large and $\varphi(q) > 1$. Thus, we may write $\varphi(p) = p^{c'}$ with $c' > 0$, and

$$q^{c\ell} = \varphi(q)^{\ell} \leq K\,(\ell \log_p q + 1)\,\varphi(p)^k$$
$$\leq K\,(\ell \log_p q + 1)\,p^{c'\ell \log_p q} = K\,(\ell \log_p q + 1)\,q^{c'\ell}.$$

On taking ℓ large enough, we see that $c \leq c'$. But we may also interchange the roles of p and q, from which $c' \leq c$. Ultimately, $c = c'$ and $\varphi(n) = n^c$ for all $n \in \mathbf{N}$; hence, $\varphi(\alpha) = |\alpha|^c$ for all $\alpha \in \mathbf{Q}$. □

Remark 8.1.5. The two metrics δ_p and δ_q associated with two distinct primes p and q are indeed different, because the sequence $\{p^n\}_{n=1}^{\infty}$ tends toward 0 for δ_p, but not for δ_q.

Comment 8.1.6. v_p is called a *discrete valuation*, since the induced topology on the image of $\mathbf{Q}^*$ by $|\ |_p$, in the set of real numbers is the discrete topology.

Definition 8.1.7. More generally, a *discrete valuation* on a field k is a surjective homomorphism from the multiplicative group k^* onto the additive group $\mathbf{Z}$: $v(ab) = v(a) + v(b)$, which verifies the ultrametric inequality

$$v(a + b) \geq \min(v(a), v(b)).$$

(We agree that $v(0) = +\infty$.) The set $\mathcal{O}_v = \{0\} \cup \{a \in k^* \mid v(a) \geq 0\}$ is a ring, called the *valuation ring* of v.

Example 8.1.8. Let $k = \mathbf{C}(T)$; there is a valuation v_α for every $\alpha \in \mathbf{C}$: any element of k^* can be written as a quotient of two polynomials; if $f \in \mathbf{C}[T]$, we factor it as a product of irreducible polynomials (hence of degree 1, since $\mathbf{C}$ is algebraically closed); $v_\alpha(f)$ is the exponent of $(T - \alpha)$ in this factorization. There is no Archimedean valuation, but there is a *valuation at infinity* v_∞, which comes from the fact that k is also the field of fractions of the ring $\mathbf{C}[\frac{1}{T}]$; on substituting $T = 1/U$ in the polynomials, one further valuation is obtained, associated with $U = 0$. It can easily be seen that, for $f/g \in k^*$ we have $v_\infty(f/g) = \deg g - \deg f$. This example is geometric in nature: the valuations correspond to the points of the line $\mathbf{A}^1_{\mathbf{C}} = \operatorname{Spec} \mathbf{C}[T]$, plus the point at infinity; this is the projective line $\mathbf{P}^1_{\mathbf{C}}$.

Example 8.1.9. Similarly, if $k = \mathbf{Q}(T)$, we define a discrete valuation v_π for every irreducible polynomial $\pi \in \mathbf{Q}[T$, by factoring any $f \in \mathbf{Q}[T]$ as a product of $\mathbf{Q}$-irreducible factors and defining $v_\pi(f)$ as the exponent of π in this factorization.

The valuation ring of v_π is the localization $A_{\mathfrak{p}} = S^{-1}A$, where $A = \mathbf{Q}[T]$, $\mathfrak{p} = (\pi)$ and $S = A \setminus \mathfrak{p}$. Here, also, there is a valuation at infinity. The discrete valuations are in one-to-one correspondence with the orbits of $\mathcal{G} = \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acting on the points of the projective line $\mathbf{P}^1_{\mathbf{Q}}$ (see Proposition 3.3.6).

Scholion 8.1.10. More generally, given an irreducible affine curve $\Gamma \subset \mathbf{A}_k^n$ with coordinate ring $A = k[\Gamma]$, the field of rational functions on the curve, which is simply the field of fractions of the ring A, has discrete valuations associated with the *closed points* of the normalization of Γ, that is, to the non-zero prime ideals of the integral closure $\widetilde{A}$ of the ring A (see Comment 5.1.14). In fact, $\widetilde{A}$ is a *Dedekind ring* (since it is Nœtherian, integrally closed, and has dimension 1); then, all its localizations at maximal ideals are discrete valuation rings. Moreover, there are discrete valuations associated with the points at infinity on the curve. In this case, the notion of discrete valuation is closely related to the resolution of singularities, but it has many other applications to algebraic geometry.

8.2 p-Adic Numbers

Let us begin with an example:

Example 8.2.1. We try to solve the equation $x^2 + 1 = 0$ by Newton's method, endowing $\mathbf{Q}$ *with the 5-adic metric.*

We proceed by successive approximations, computing each time the tangent to the graph of the function $x \mapsto x^2 + 1$. As first approximation we choose $x_0 = 2$, so that $\left|x_0^2 + 1\right|_5 = \frac{1}{5}$.

For $i \in \mathbf{N}$ and $x_i \in \mathbf{Q}$, we define $d_i = x_i^2 + 1$. We make the inductive hypothesis $|d_i|_5 < 1$ and $|x_i|_5 = 1$, which is verified for $i = 0$. We then set $x_{i+1} = x_i + h_i$, where the increment h_i must be suitably chosen.

We thus have $d_{i+1} = x_{i+1}^2 + 1 = d_i + 2x_i h_i + h_i^2$ and observe that we can eliminate the linear term in h_i by defining $h_i = -\frac{d_i}{2x_i}$. We then have $|h_i|_5 = \frac{|d_i|_5}{|2|_5 |x_i|_5} = |d_i|_5$, and $d_{i+1} = h_i^2 \implies |d_{i+1}|_5 = |h_i|_5^2 = |d_i|_5^2$. The ultrametric inequality implies that $|x_{i+1}|_5 = \max(|x_i|_5, |h_i|_5) = 1$, since $|x_i|_5 = 1$ and $|h_i|_5 = |d_i|_5 < 1$.

The inductive hypothesis, therefore, holds true for all $i \in \mathbf{N}$; observe that the numbers $|d_i|_5 = \left|x_i^2 + 1\right|_5$ (and also the $|h_i|_5$) even tend quadratically toward 0. In this way, we obtain a sequence of *rational numbers* $x_0 = 2$, $x_1 = \frac{3}{4}$, $x_2 = -\frac{7}{24}$, ... such that $\left|x_i^2 + 1\right|_5 \to 0$ when i tends toward infinity. Moreover, if $m > n$, we have: $|x_m - x_n|_5 = |h_n + h_{n+1} + \ldots|_5 = |h_n|_5 = |d_n|_5 \to 0$ when $n \to \infty$.

The x_n therefore form a Cauchy sequence, but of course $\mathbf{Q}$ is not complete for this metric. Otherwise, -1 would be a rational square!

However, there exists a field $\mathbf{Q}_p$ endowed with an absolute value that extends the p-adic absolute value, contains the field of rational numbers as a dense subset, and in which all Cauchy sequences are convergent. This field is obtained from $\mathbf{Q}$ in the same way as the field of real numbers, but with the p-adic metric instead of the ordinary absolute value.

Definition 8.2.2. The *field* $\mathbf{Q}_p$ *of p-adic numbers* is the *completion* of $\mathbf{Q}$ with respect to the p-adic absolute value $|\ |_p$.

The existence of this field comes from the following very general construction.

Construction 8.2.3. We define $\mathfrak{F}$ as the set of *fundamental sequences* $(a_n)_{n=0}^{\infty}$, where $a_n \in \mathbf{Q}$, that is (a_n) verifies the *Cauchy condition*: $|a_m - a_n|_p \to 0$ if $m, n \to \infty$. The set $\mathfrak{F}$ contains the subset $\mathfrak{N}$ consisting of all sequences "equivalent to zero," i.e., such that $|a_n|_p \to 0$ when $n \to \infty$. $\mathfrak{F}$ becomes a ring if one defines $(a_n) + (b_n) = (a_n + b_n)$ and $(a_n) \cdot (b_n) = (a_n\, b_n)$. It is clear that $(a_n + b_n)$ is a fundamental sequence since, by the triangle inequality $|(a_m + b_m) - (a_n + b_n)|_p \leq |a_m - a_n|_p + |b_m - b_n|_p \to 0$. The Cauchy condition is also satisfied for $(a_n\, b_n)$, since on the one hand the relation $a_m = (a_m - a_n) + a_n$ implies that $|a_m|_p \leq |a_m - a_n|_p + |a_n|_p$ is bounded: there is a number $T_a \in \mathbf{N}$ such that $|a_m|_p \leq T_a$ for all $m \in \mathbf{N}$. On the other hand, we can write $|a_m b_m - a_n b_n|_p = |a_m(b_m - b_n) + (a_m - a_n)b_n|_p \leq |a_m|_p |b_m - b_n|_p + |a_m - a_n|_p |b_n|_p \leq T_a \cdot |b_m - b_n|_p + T_b \cdot |a_m - a_n|_p \to 0$.

Also, $\mathfrak{N}$ is an ideal in the ring $\mathfrak{F}$: if $(c_n) \in \mathfrak{N}$ and $(a_n) \in \mathfrak{F}$, then $(a_n)(c_n) = (a_n \cdot c_n) \in \mathfrak{N}$, since $|a_n c_n|_p \leq T_a \cdot |c_n|_p \to 0$ when $n \to \infty$.

Finally, the sequences $(a_n) \in \mathfrak{F} \setminus \mathfrak{N}$ are invertible in the quotient $\mathfrak{F}/\mathfrak{N}$, because of the following lemma.

Lemma 8.2.4. *For a fundamental sequence $(a_n) \in \mathfrak{F} \setminus \mathfrak{N}$, the absolute value becomes constant on the end of the sequence: $\exists\, m_0$ such that $|a_m|_p = \left|a_{m_0}\right|_p$ for all $m \geq m_0$.*

Proof. $(a_n) \notin \mathfrak{N}$ entails

$$\exists\, \epsilon > 0 : \forall\, n_0,\ \exists\, m_0 > n_0 : \left|a_{m_0}\right|_p \geq \epsilon, \tag{$*$}$$

and $(a_n) \in \mathfrak{F}$ implies

$$\forall\, \epsilon > 0,\ \exists\, n_0 : m, n \geq n_0 \implies |a_m - a_n|_p < \epsilon. \tag{$**$}$$

Then, first choosing ϵ as in $(*)$, then n_0 by $(**)$, and finally m_0 by $(*)$, we find $a_m = (a_m - a_{m_0}) + a_{m_0} \implies |a_m|_p = \left|a_{m_0}\right|_p \quad \forall\, m \geq m_0$. □

In particular, the a_m are never zero for $m \geq m_0$ and we can find the inverse of the sequence (a_n), modulo $\mathfrak{N}$, defining (b_n) by $b_n = 1$ if $n < m_0$ and $b_n = 1/a_n$ if $n \geq m_0$. The sequence (b_n) is still a Cauchy sequence, for $|b_m - b_n|_p = \left|a_m^{-1} - a_n^{-1}\right|_p = \left|\frac{a_n - a_m}{a_m a_n}\right|_p = \frac{|a_n - a_m|_p}{|a_{m_0}|_p^2} \to 0$ if $m, n \geq m_0$. One verifies that the product $(a_n) \cdot (b_n)$ is equal to 1 modulo $\mathfrak{N}$, since $(a_n\, b_n - 1) \in \mathfrak{N}$. Thus, the quotient $\mathfrak{F}/\mathfrak{N}$ is a field; we denote it by $\mathbf{Q}_p$.

Remark 8.2.5. The above construction can be carried out for any field endowed with an absolute value. It does not use any specific property of the field of rationals. Lemma 8.2.4 must just be replaced by another argument, if the absolute value is Archimedean (see Exercise 8.5).

Proposition 8.2.6.

(a) *The field* $\mathbf{Q}_p$ *contains* $\mathbf{Q}$ *as a subfield.*
(b) *The* p*-adic absolute value* $|\ |_p$ *extends naturally from* $\mathbf{Q}$ *to* $\mathbf{Q}_p$.
(c) $|\ |_p$ *takes the same values on* $\mathbf{Q}$ *and on* $\mathbf{Q}_p$.
(d) $\mathbf{Q}$ *is dense in* $\mathbf{Q}_p$ *endowed with the metric induced by* $|\ |_p$.
(e) $\mathbf{Q}_p$ *is complete for this metric.*

Proof.

(a) The embedding $\mathbf{Q} \hookrightarrow \mathbf{Q}_p$ comes from the fact that any $\alpha \in \mathbf{Q}$ defines a fundamental sequence (a_n), where $a_n = \alpha$ for all n. One easily verifies that this is an injection and a field homomorphism.
(b) If α is the class modulo $\mathfrak{N}$ of a sequence $(a_n) \in \mathfrak{F} \setminus \mathfrak{N}$, we define $|\alpha|_p = \left|a_{m_0}\right|_p$, where m_0 is given by Lemma 8.2.4. If α is also the class of another sequence $(b_n) \in \mathfrak{F}$, we have $|b_n - a_n|_p \to 0$, and since $b_n = (b_n - a_n) + a_n$, we have: $|b_n|_p = |a_n|_p$ as soon as n is large enough. Consequently, the definition of $|\alpha|_p$ is independent of the choice of the sequence (a_n) in the class of α. From this we easily see that $|\ |_p$ is a non-Archimedean absolute value on the field $\mathbf{Q}_p$, whose restriction to $\mathbf{Q}$ coincides with the p-adic absolute value on this field.
(c) The definition $|\alpha|_p = \left|a_{m_0}\right|_p$ shows that all real numbers of the form $|\alpha|_p$ are already of the form $\left|a_{m_0}\right|_p$ with $a_{m_0} \in \mathbf{Q}$.
(d) If $\alpha \in \mathbf{Q}_p$ is the class modulo $\mathfrak{N}$ of a sequence $(a_n) \in \mathfrak{F} \setminus \mathfrak{N}$, then by $(**)$ there exists for all $\epsilon > 0$ a rational number a_{n_0} such that $\left|a_m - a_{n_0}\right|_p < \epsilon$ for all $m \geq n_0$. Then, $\left|\alpha - a_{n_0}\right|_p < \epsilon$.
(e) Let (α_n) be a Cauchy sequence in $\mathbf{Q}_p$. Since $\mathbf{Q}$ is dense in $\mathbf{Q}_p$, there exists for all n a number $a_n \in \mathbf{Q}$ such that $|\alpha_n - a_n|_p < 1/n$. Therefore, $|a_m - a_n|_p \leq |a_m - \alpha_m|_p + |\alpha_m - \alpha_n|_p + |\alpha_n - a_n|_p \to 0$ if $m, n \to \infty$. Then, $(a_n) \in \mathfrak{F}$, and the class α of (a_n) is also the limit of the sequence (α_n). □

Property (c) guarantees that we can write $|\alpha|_p = p^{-v_p(\alpha)}$ for all $\alpha \in \mathbf{Q}_p^*$, where v_p is a discrete valuation on $\mathbf{Q}_p$ (Definition 8.1.7).

Definition 8.2.7. The ring of *p-adic integers* is the valuation ring $\mathbf{Z}_p = \left\{\alpha \in \mathbf{Q}_p \;\middle|\; |\alpha|_p \leq 1\right\} = \{0\} \cup \left\{\alpha \in \mathbf{Q}_p^* \mid v_p(\alpha) \geq 0\right\}$.

This is a discrete valuation ring (see Exercises 8.2 and 8.3), whose maximal ideal is $\mathfrak{p} = \left\{\alpha \in \mathbf{Q}_p \;\middle|\; |\alpha|_p < 1\right\} = \{0\} \cup \left\{\alpha \in \mathbf{Q}_p^* \mid v_p(\alpha) > 0\right\} = p\mathbf{Z}_p$.

8.3 Canonical Representation

Clearly, $\mathbf{Z} \subset \mathbf{Z}_p$ and $\mathfrak{p} \cap \mathbf{Z} = (p)$; consequently, there is a natural embedding $\mathbf{Z}/(p) \hookrightarrow \mathbf{Z}_p/\mathfrak{p}$. This is actually an isomorphism.

Lemma 8.3.1. $\mathbf{Z}_p/\mathfrak{p}$ *is naturally isomorphic to* $\mathbf{Z}/(p)$.

Proof. Let $\alpha \in \mathbf{Z}_p \setminus \mathfrak{p}$; we have $v_p(\alpha) = 0$ and we must see that the class of α has a representative b_0 in $\mathbf{Z}$. Now, $\mathbf{Q}$ is dense in $\mathbf{Q}_p$; thus, there exists $a \in \mathbf{Q}$ such that $v_p(\alpha - a) \geq 1$. We may write $a = \frac{c}{d}$, with $c, d \in \mathbf{Z}$ and $p \nmid d$, for $a = (a - \alpha) + \alpha \implies v_p(a) \geq \min(v_p(a - \alpha), v_p(\alpha)) = 0$.

Since the class of d is non-zero in the field $\mathbf{Z}/(p)$, there is an integer $d' \in \mathbf{Z}$ such that $dd' \equiv 1 \pmod{p}$. Then, $\alpha - cd' = (\alpha - \frac{c}{d}) + \frac{c}{d}(1 - dd') \implies v_p(\alpha - cd') \geq \min\big(v_p(\alpha - a), v_p(\frac{c}{d}) + v_p(1 - dd')\big) > 0$. From this, it follows that there exists $b_0 \in \mathbf{Z}$ such that $v_p(\alpha - b_0) > 0$; we can take $b_0 = cd'$, but we may still modify b_0 by an integer multiple of p to ensure that $0 < b_0 \leq p - 1$. (The integer b_0 is not zero, since $v_p(\alpha - b_0) > 0$, whereas $v_p(\alpha) = 0$.) □

On iterating this reasoning, we obtain the following proposition.

Proposition 8.3.2. *Every p-adic number $\alpha \neq 0$ can be written in a unique manner in the form $\alpha = \sum_{i=m}^{\infty} b_i\, p^i$, with $m = v_p(\alpha) \in \mathbf{Z}$, $0 \leq b_i \leq p - 1$ ($b_i \in \mathbf{Z}$) and $b_m \neq 0$.*

Proof. Unicity is obvious. To show existence, we first multiply α by p^{-m}, where $m = v_p(\alpha)$, to be in the case treated in Lemma 8.3.1, where $\alpha \in \mathbf{Z}_p \setminus \mathfrak{p}$. After determining b_0, we replace α by $\beta = (\alpha - b_0)/p$ and continue recursively. □

Example 8.3.3. In $\mathbf{Q}_3$, we have: $-1 = 2 + 2\cdot 3 + 2\cdot 3^2 + \cdots$ and $\frac{1}{2} = 2 + 3 + 3^2 + 3^3 + \cdots$. It is also useful to remember the geometric series $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \cdots$ in $\mathbf{Q}_p$.

Remark 8.3.4. In contrast to $\mathbf{Z}$ and $\mathbf{Q}$, the ring $\mathbf{Z}_p$ is not countable, as Proposition 8.3.2 clearly shows. And despite appearances, $\mathbf{Q}_p$ is a field of characteristic zero.

Proposition 8.3.5. *$\mathbf{Z}_p$ is a compact topological space.*

Proof. The topology is defined by the p-adic metric. Let $\mathbf{Z}_p = \bigcup_{i \in I} U_i$, where the U_i are open in $\mathbf{Z}_p$. *Suppose that there is no finite sub-cover.*

Since $\mathbf{Z}_p = \bigcup_{0 \leq b_0 < p} (b_0 + p\mathbf{Z}_p)$, at least one of the sets $b_0 + p\mathbf{Z}_p$ is not covered by a finite number of sets U_i. There then exists b_1 with $0 \leq b_1 < p$ such that $b_0 + b_1 p + p^2\mathbf{Z}_p$ is not covered by a finite number of open sets U_i. And so on; let $\alpha = b_0 + b_1 p + b_2 p^2 + \cdots$. Clearly, $\alpha \in U_{i_0}$ for at least one $i_0 \in I$. Since U_{i_0} is open, it contains a ball of the form $\alpha + p^k\mathbf{Z}_p = b_0 + b_1 p + \cdots + b_{k-1} p^{k-1} + p^k\mathbf{Z}_p$, which would therefore be covered by U_{i_0} alone, a contradiction. □

One can give another proof, based on the fact that, in a metric space, compactness is equivalent to the property that any sequence contains a convergent subsequence. If $(\alpha_n)_{n=0}^{\infty}$ is a sequence of p-adic integers, we represent them in canonical form and find an infinite subsequence on $(\alpha_n^{(0)})$ with the same b_0, then a subsequence $(\alpha_n^{(1)})$ of $(\alpha_n^{(0)})$ with the same b_1, etc. Finally, the sequence $(\alpha_0^{(0)}, \alpha_1^{(1)}, \dots)$ converges to $b_0 + b_1 p + \cdots$.

Corollary 8.3.6. *$\mathbf{Q}_p$ is locally compact.*

Proof. Every $\alpha \in \mathbf{Q}_p$ has a compact neighborhood, namely the closed ball $\alpha + \mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid |x - \alpha|_p \leq 1\}$. □

However, $\mathbf{Q}_p$ is not compact, because the sequence $(p^{-n})_{n=0}^{\infty}$ contains no convergent subsequence.

Corollary 8.3.7. *If $f \in \mathbf{Z}[X_1, \ldots, X_n]$, solving $f(x_1, \ldots, x_n) = 0$ in $\mathbf{Z}_p$ is equivalent to solving $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^k}$ for all $k \geq 1$.*

Proof. In one direction, this follows immediately from Proposition 8.3.2. Conversely, since $\mathbf{Z}_p$ is compact, so is $\mathbf{Z}_p^n$. Therefore, if $f(x_1^{(k)}, \ldots, x_n^{(k)}) \equiv 0 \pmod{p^k}$, there exists a convergent subsequence $(x_1^{(\ell)}, \ldots, x_n^{(\ell)})$ in $\mathbf{Z}_p^n$; let $(\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}_p^n$ be the limit of this sequence. Then, $f(\alpha_1, \ldots, \alpha_n) = 0$, since f is a continuous function and $\left| f(x_1^{(\ell)}, \ldots, x_n^{(\ell)}) \right|_p \to 0$ for $\ell \to \infty$. □

For homogenous polynomials, we are mainly interested in *non-trivial solutions*, that is, other than $(0, \ldots, 0)$ (see Definition 3.2.9).

Corollary 8.3.8. *If $F \in \mathbf{Z}[X_1, \ldots, X_n]$ is a homogenous polynomial, the equation $F(x_1, \ldots, x_n) = 0$ has a solution in $\mathbf{Z}_p^n$ other than $(0, \ldots, 0)$ if and only if, for all $k \geq 1$, the congruence $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k}$ has a solution whose coordinates x_i are not all multiples of p.*

Proof. In the preceding proof, we may assume that $x_1^{(\ell)}$ is not a multiple of p, for an infinity of values of ℓ. Then, $\alpha_1 \neq 0$. □

Comment 8.3.9. It is quite remarkable that congruence conditions, and hence equalities in the quotient rings of finite characteristic $\mathbf{Z}/(p^k)$, can be expressed as a single equality in a ring of characteristic zero. One also shows that the ring $\mathbf{Z}_p$ is (algebraically and topologically) the *projective limit* of the $\mathbf{Z}/(p^k)$; it is the *pro-finite group* $\mathbf{Z}_p = \varprojlim \mathbf{Z}/(p^k) \twoheadrightarrow \cdots \twoheadrightarrow \mathbf{Z}/(p^3) \twoheadrightarrow \mathbf{Z}/(p^2) \twoheadrightarrow \mathbf{Z}/(p)$.

Examples. p-adic numbers and the above corollaries are often used to provide *obstructions* to the existence of rational solutions, that is, conditions showing that there are no solutions. For instance, if the Pythagoreans wanted to show that 2 is not the square of a rational number, they could do so by a 2-adic argument: if $\alpha^2 = 2$ with $\alpha \in \mathbf{Q}$, then $2\, v_2(\alpha) = v_2(2) = 1$, which is impossible, for $v_2(\alpha)$ must be an integer. They could also do so by a 3-adic argument: if $\alpha^2 = 2$ with $\alpha \in \mathbf{Q}$, then $2\, v_3(\alpha) = v_3(2) = 0$; consequently, $v_3(\alpha) = 0$ and $\alpha \in \mathbf{Z}_3$. Corollary 8.3.7 then requires solving the congruence $x^2 \equiv 2 \pmod{3}$, which obviously has no solution. For homogenous equations, here are some examples among many:

(1) $x_1^2 + x_2^2 + x_3^2 = 0$ has no non-trivial solutions in $\mathbf{Q}_2$, for there is no primitive solution modulo 4 (Corollary 8.3.8).
(2) $x_1^2 + x_2^2 + 3x_3^2 + 21x_4^2 = 0$ has no non-trivial rational solutions, since $\mathbf{Q} \subset \mathbf{R}$ and a sum of squares can vanish in $\mathbf{R}$ only if all x_i are zero.
(3) In the equation $x_1^2 + x_2^2 - 3(x_3^2 + 7x_4^2) = 0$, the quadratic form is indefinite, yet this equation has no non-trivial rational solutions. To prove this, we use the

embedding $\mathbf{Q} \hookrightarrow \mathbf{Q}_3$: on multiplying or dividing by a power of $p = 3$, we could find a *primitive* integral solution, that is, with the $x_i \in \mathbf{Z}_3$ without a common factor. Since the congruence $x_1^2 + x_2^2 \equiv 0 \pmod 3$ has no non-trivial solution, we would find that x_1 and x_2 are multiples of 3. On writing $x_1 = 3y_1$ and $x_2 = 3y_2$, we could then divide the equation by 3 and repeat the same reasoning with $x_3^2 + 7x_4^2 \equiv 0 \pmod 3$; hence, x_3 and x_4 would also be multiples of 3, which contradicts the hypothesis.

(4) Similarly, $x_1^3 + 5x_2^3 + 25x_3^3 = 0$ has no non-trivial solutions in $\mathbf{Q}_5$.

(5) The equation $(x_1^3 + 2x_2^3) + 7\,(x_3^3 + 2x_4^3) + 49\,(x_5^3 + 2x_6^3) = 0$ has no non-trivial solutions in $\mathbf{Q}_7$, for the only cubes modulo 7 are $0, \pm 1$.

(6) Let $\varphi(x_1, x_2, x_3) = x_1^3 + 2x_2^3 + 4x_3^3 + x_1x_2x_3$. The equation $\varphi(x_1, x_2, x_3) + 7\,\varphi(x_4, x_5, x_6) + 49\,\varphi(x_7, x_8, x_9) = 0$ has no non-trivial solutions in $\mathbf{Q}_7$, as φ is the norm form

$$\varphi(x_1, x_2, x_3) = N_{k(\alpha)/k}(x_1 + \alpha x_2 + \alpha^2 x_3),$$

where $k = \mathbf{F}_7$ and α is a cubic root of 2 in $\bar{k}$. This form does not represent zero in $\mathbf{F}_7$ (see Example 3.2.10).

More generally, we have seen in Lemma 3.4.8 that $\mathbf{F}_p$ is indeed C_1 (Corollary 3.4.12), but not more: for any positive integer d, there is a form $\varphi(x_1, \ldots, x_d)$ of degree d in d variables, defined over $\mathbf{F}_p$, which does not represent zero (non-trivially) in $\mathbf{F}_p$. The above argument then shows that the equation

$$\varphi(x_1, \ldots, x_d) + p\,\varphi(x_{d+1}, \ldots, x_{2d}) + \cdots + p^{d-1}\,\varphi(x_{d^2-d+1}, \ldots, x_{d^2}) = 0$$

has no non-trivial solutions in $\mathbf{Q}_p$. In other words, $\mathbf{Q}_p$ is not more than C_2 (Definition 3.4.9).

Proposition 8.3.10. *For each p, there exists for every positive integer d a form of degree d in $n = d^2$ variables, defined over $\mathbf{Q}_p$, which does not represent zero (non-trivially) in $\mathbf{Q}_p$.* □

It was believed for a long time that p-adic fields are C_2, until in 1966 Terjanian obtained the first counter-example, in degree 4, over $\mathbf{Q}_2$ (Exercise 8.11). The episodes surrounding Artin's conjecture are fascinating. We examine this subject in detail in Chapter 10.

8.4 Hensel's Lemma

Corollaries 8.3.7 and 8.3.8 suggest that, in order to solve an equation in $\mathbf{Z}_p$, one should solve an infinity of congruences. Fortunately, everything reduces to a finite number of computations, and even a very small number, thanks to the following result, which extends and generalizes Newton's method presented in Example 8.2.1.

Proposition 8.4.1 (Hensel's Lemma). *Let $f \in \mathbf{Z}_p[X]$ be a polynomial and $x_0 \in \mathbf{Z}_p$ a p-adic integer such that*

$$v_p(f(x_0)) > 2\, v_p(f'(x_0)).$$

Then there exists $x \in \mathbf{Z}_p$ such that $f(x) = 0$, with, moreover, $v_p(x - x_0) > v_p(f'(x_0))$; and x is unique with this property.

Proof. We set $m_0 = v_p(f'(x_0)) \in \mathbf{N}$ (the « slope » at x_0) and, starting from x_0, define a sequence of numbers $x_i \in \mathbf{Z}_p$ such that

$$v_p(f(x_i)) > 2\, m_0 \quad \text{and} \quad v_p(f'(x_i)) = m_0,$$

by iterating $x_{i+1} = x_i + h_i$, where the increment h_i must be suitably chosen.

For this we write $x = x_i + y$, so $f(x) = f(x_i + y) = c_0 + y\, c_1 + y^2\, c_2(y)$ and $f'(x) = c_1 + y\, c_3(y)$, with $c_0 = f(x_i)$, $c_1 = f'(x_i)$ and $c_2,\ c_3 \in \mathbf{Z}_p[y]$. Then,

$$f(x_{i+1}) = f(x_i + h_i) = f(x_i) + h_i\, f'(x_i) + h_i^2\, c_2(h_i)$$

and observe that we can eliminate the linear term in h_i by defining $h_i = -\frac{f(x_i)}{f'(x_i)}$. We then have:

$$v_p(h_i) = v_p(f(x_i)) - m_0 > m_0 \geq 0.$$

In particular, h_i is a p-adic integer. From $f(x_{i+1}) = h_i^2\, c_2(h_i)$ we get:

$$v_p(f(x_{i+1})) \geq 2\, v_p(h_i) = 2\, v_p(f(x_i)) - 2\, m_0 > v_p(f(x_i)) > 2\, m_0.$$

This proves the first part of the inductive hypothesis. It also follows from this computation that the sequence $f(x_i)$ tends toward zero.

From $f'(x_{i+1}) = f'(x_i + h_i) = f'(x_i) + h_i\, c_3(h_i)$ we also obtain:

$$v_p(f'(x_{i+1}) - f'(x_i)) \geq v_p(h_i) > m_0 = v_p(f'(x_i)).$$

Therefore, the ultrametric inequality implies the inequality

$$v_p(f'(x_{i+1})) = v_p\big((f'(x_{i+1}) - f'(x_i)) + f'(x_i)\big) = v_p(f'(x_i)) = m_0,$$

which proves the second part of the inductive hypothesis.

Moreover, $v_p(h_{i+1}) = v_p(f(x_{i+1})) - m_0 > v_p(f(x_i)) - m_0 = v_p(h_i)$, so that the x_i form a convergent sequence, since $v_p(x_m - x_n) = v_p\big(\sum_{i=n}^{m-1} (x_{i+1} - x_i)\big) = v_p(h_n) \to \infty$, for every $m > n$. Besides, for all $i \geq 1$, $v_p(x_i - x_0) = v_p(h_0)$; hence, $v_p(x - x_0) = v_p(h_0) > m_0$.

As for unicity, let $z \in \mathbf{Z}_p$ be another solution of the equation $f(z) = 0$ with $v_p(z - x_0) > m_0$. Then, on setting $z = x + y$, Taylor's formula gives as above

$f(z) = f(x) + y\,f'(x) + y^2c_2(y)$, which implies that $y\,f'(x) + y^2c_2(y) = 0$. If $y \neq 0$, we would therefore have $f'(x) + yc_2(y) = 0$, which is impossible. Indeed, $v_p(f'(x)) = v_p(f'(x_0)) = m_0$, whereas $v_p(yc_2(y)) > m_0$, $y = z - x = (z - x_0) + (x_0 - x) \implies v_p(y) \geq \min(v_p(z - x_0), v_p(x_0 - x)) > m_0$. □

The convergence is quadratic, since $v_p(f(x_{i+1})) \geq 2\,v_p(f(x_i)) - 2m_0$ and also $v_p(h_{i+1}) = v_p(f(x_{i+1})) - m_0 \geq 2\,v_p(h_i) - m_0$.

Remark 8.4.2. The condition $v_p(f(x_0)) \geq 2\,v_p(f'(x_0))$ in the lemma is not sufficient: for example, the equation $x^2 + 3 = 0$ has no 2-adic solutions, whereas $x^2 + 7 = 0$ has.

Hensel's Lemma most frequently applies when x_0 is a *simple zero* of f modulo p (Definition 5.5.7), that is, when $f'(x_0) \not\equiv 0 \pmod{p}$. In this *elementary case*, the condition is $v_p(f(x_0)) > 0$ and in order to show that f has a root in $\mathbf{Z}_p$, it suffices to see that the congruence $f(x_0) \equiv 0 \pmod{p}$ is also satisfied.

Corollary 8.4.3. *Every simple zero of the reduction modulo p of a polynomial $f \in \mathbf{Z}_p[X_1, \ldots, X_n]$ lifts to a zero of f with coordinates in $\mathbf{Z}_p$.*

Proof. $(x_1, \ldots, x_n)$ is a simple zero of f modulo p if $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ and if there is a j such that $\frac{\partial f}{\partial X_j}(x_1, \ldots, x_n) \not\equiv 0 \pmod{p}$. For every coordinate with $i \neq j$, fix a representative $x_i \in \mathbf{Z}_p$ and consider the polynomial in one variable $g(X) = f(x_1, \ldots, x_{j-1}, X, x_{j+1}, \ldots, x_n) \in \mathbf{Z}_p[X]$. By hypothesis, $v_p(g(x_j)) \geq 1$ and $v_p(g'(x_j)) = 0$. Applying Proposition 8.4.1, we find $x \in \mathbf{Z}_p$ with $x \equiv x_j \pmod{p}$ and such that $g(x) = 0$. □

Corollary 8.4.4. *If $F \in \mathbf{Z}_p[X_0, \ldots, X_n]$ is a homogenous polynomial, every simple zero of its reduction modulo p lifts to a primitive zero of F with coordinates in $\mathbf{Z}_p$.*

Proof. The condition $\frac{\partial F}{\partial X_j}(x_0, \ldots, x_n) \not\equiv 0 \pmod{p}$ implies that the zero is non-trivial modulo p. Since the lifting is in the same class modulo p as the $(x_0, \ldots, x_n)$, its coordinates are obviously not all multiples of p. □

The next proposition is the exact analog of the implicit function theorem for real numbers. It is topological in nature, but also has important arithmetic applications (see Remark 9.1.7 or the note to Proposition 9.2.8).

Proposition 8.4.5 (Implicit Functions Theorem). *Given a hypersurface $Y = V(f) \subset \mathbf{A}^n_{\mathbf{Q}_p}$ defined by a polynomial $f \in \mathbf{Q}_p[X_1, \ldots, X_n]$, every non-singular point $P \in \mathcal{M} = Y(\mathbf{Q}_p)$ belongs to an open set $\mathcal{W} \subset \mathbf{Q}_p^n$ of the form $\mathcal{W} = \mathcal{V} \times \mathcal{U}$, where $\mathcal{U} \subset \mathbf{Q}_p^{n-1}$ and $\mathcal{V} \subset \mathbf{Q}_p$, in which there exists a continuous map $\varphi : \mathcal{U} \to \mathcal{V}$ with the property that $v = \varphi(u) \iff f(v, u) = 0$ for $(v, u) \in \mathcal{W}$.*

The projection $\pi : \mathcal{M} \cap \mathcal{W} \to \mathcal{U}$ has a section defined by $\sigma(u) = (\varphi(u), u)$; indeed, $\pi \circ \sigma = \mathbf{id}|_{\mathcal{U}}$. In particular, π is surjective and $\sigma : \mathcal{U} \to \mathcal{M}$ is a continuous map, injective and open; therefore, it is homeomorphism onto its image.

Proof. We may obviously assume that $f \in \mathbf{Z}_p[X_1, \ldots, X_n]$, but it is also permissible, thanks to Remark 5.5.9, to suppose that P has integer coordinates.

Indeed, in $\mathbf{P}^n_{\mathbf{Q}_p}$ the point P has primitive integer coordinates; we may assume that one of these coordinates is 1, which defines an affine space in which P has integer coordinates.

Let $P = (x_1, \dots, x_n)$. If $\frac{\partial f}{\partial X_1}(x_1, \dots, x_n) \not\equiv 0$, we do not necessarily have $\frac{\partial f}{\partial X_1}(x_1, \dots, x_n) \not\equiv 0 \pmod{p}$, but we can still define the "slope" $m_0 = v_p\big(\frac{\partial f}{\partial X_1}(x_1, \dots, x_n)\big) \in \mathbf{N}$. Let $\mathcal{U}$ be the open set defined by

$$\mathcal{U} = \Big\{(y_2, \dots, y_n) \in \mathbf{Z}_p^{n-1} \mid v_p(y_i - x_i) > N \quad \forall\, i \geq 2\Big\},$$

where $N > 2\,m_0$ is a sufficiently large integer, and let

$$\mathcal{V} = \big\{y_1 \in \mathbf{Z}_p \mid v_p(y_1 - x_1) > m_0\big\}.$$

Consider the polynomial in one variable $g(X) = f(X, y_2, \dots, y_n) \in \mathbf{Z}_p[X]$. One verifies that, if $(y_2, \dots, y_n) \in \mathcal{U}$, then $v_p(g(x_1)) = v_p(f(x_1, y_2, \dots, y_n)) > N$ and $v_p(g'(x_1)) = v_p\big(\frac{\partial f}{\partial X_1}(x_1, y_2, \dots, y_n)\big) = m_0$. Applying Proposition 8.4.1, we find $y_1 \in \mathbf{Z}_p$ with $g(y_1) = 0$ and $v_p(y_1 - x_1) > m_0$, so that $y_1 \in \mathcal{V}$.

Now, y_1 is unique with this property. The map $\varphi(y_2, \dots, y_n) = y_1$ is therefore well defined by this method and has all the stated properties. □

The following result is an interesting consequence (see Figure 2.1).

Corollary 8.4.6. *A non-singular point is never isolated.* □

The proposition is true not only for hypersurfaces, it even extends to all subvarieties of $\mathbf{A}^n_{\mathbf{Q}_p}$ and $\mathbf{P}^n_{\mathbf{Q}_p}$, on properly defining simple zeros (*Jacobian criterion of singularity*).

Example 8.4.7. The quartic $\Gamma \subset \mathbf{A}^2_{\mathbf{Q}_2}$ defined by the equation

$$(x_1^2 - x_2)^2 + (1 - x_1x_2)^2 + (x_2^2 - x_1)^2 = 0 \tag{8.4.1}$$

has only $(1, 1)$ and (ρ, ρ^2) has 2-adic points, where $\rho \in \mathbf{Q}_2$ is one of the two other cubic roots of unity. Since these three points are isolated, they are necessarily singular, as one easily verifies. (In fact, we have here the same situation as over $\mathbf{R}$, although there, two of the singular points are complex, whereas over $\mathbf{Q}_2$ all singular points have coordinates in the base field.)

One finds in the literature other statements relating the behavior over $\mathbf{Z}_p$ to the behavior under reduction. The following proposition is often called *Hensel's Lemma*.

Proposition 8.4.8. *Let $f \in \mathbf{Z}_p[X]$ be a polynomial, which factors modulo p as $\widetilde{f} = \tilde{g} \cdot \tilde{h}$, with $\tilde{g}$ and $\tilde{h}$ relatively prime. Then there exist lifts g, $h \in \mathbf{Z}_p[X]$ such that $f = g \cdot h$ and* $\deg g = \deg \tilde{g}$.

The particular case when $\deg \tilde{g} = 1$ corresponds to the elementary case of Hensel's Lemma, as seen above. (For the proof, see van der Waerden [vdW], §144).

Exercises

8.1. Let v be a discrete valuation on a field k. Show that if $v(a) \neq v(b)$, then $v(a+b) = \min(v(a), v(b))$.

8.2. Let $\mathcal{O}_v$ be the valuation ring of a discrete valuation v on a field k. Show that $\mathcal{O}_v$ is a principal local ring. What is its maximal ideal?

8.3. A *discrete valuation ring* is a principal local ring, which is not a field. Show that if A is a discrete valuation ring, its field of fractions is equipped with a discrete valuation, whose valuation ring is A.

8.4. Let $k = \mathbf{C}((X, Y))$, the field of fractions of the ring of formal series in two variables $A = \mathbf{C}[[X, Y]]$. Show that A is a local ring with maximal ideal $\mathfrak{m} = (X, Y)$, and that one can define a $\mathfrak{m}$-*adic* discrete valuation on k, by $v_{\mathfrak{m}}(f) = \max\{v \mid f \in \mathfrak{m}^v\}$.

8.5. What must be changed in Construction 8.2.3 in the case of an Archimedean absolute value?

8.6. Find the canonical representation of $\frac{1}{5}$ in $\mathbf{Q}_3$.

8.7. Let $\alpha \in \mathbf{Q}_p$ with canonical representation $\alpha = \sum_{i=m}^{\infty} b_i\, p^i$, with $m \in \mathbf{Z}$ and $0 \leq b_i \leq p-1$ ($b_i \in \mathbf{N}$). Show that this expansion is finite if and only if α is of the form $\frac{a}{p^n}$ with $a \in \mathbf{N}$. Show that it becomes periodic after a finite number of terms if and only if $\alpha \in \mathbf{Q}$.

8.8. Show that a series $\sum_{i=0}^{\infty} \alpha_i$ is convergent in $\mathbf{Q}_p$ if and only if the sequence $\alpha_n \to 0$ ($n \to \infty$).

8.9. If U and V are two open balls in $\mathbf{Q}_p$ such that $U \cap V \neq \emptyset$, then $U \subset V$ or $V \subset U$.

8.10. Does the equation $(x_1^4 + x_2^4 + x_3^4 + x_4^4) - 5(x_5^4 + x_6^4 + x_7^4 + x_8^4) = 0$ have non-trivial solutions in $\mathbf{Q}$?

8.11 (Terjanian, 1966). For $x = (x_1, x_2, x_3)$, we define:

$$f(x) = x_1^4 + x_2^4 + x_3^4 - x_1^2 x_2^2 - x_2^2 x_3^2 - x_3^2 x_1^2 - x_1 x_2 x_3 (x_1 + x_2 + x_3).$$

Show that if $x \not\equiv (0,0,0)$ modulo 2, then $f(x) \equiv +1 \pmod 4$. Since $f(x) \equiv 0 \pmod{16}$ if $x \equiv (0,0,0)$ modulo 2, deduce that $f(x) + f(y) + f(z) - 4(f(u) + f(v) + f(w))$ is a form in 18 variables with no non-trivial zero in $\mathbf{Q}_2$.

8.12. For which values of p does the equation $x^2 + 1 = 0$ have solutions in $\mathbf{Q}_p$?

8.13. Show that $\mathbf{Q}_p$ contains the group μ_{p-1} of $(p-1)$-th roots of unity.

8.14. Show that the equation $x_1^2 + x_2^2 + x_3^2 = 0$ has a non-trivial solution in $\mathbf{Q}_p$ for every $p \geq 3$.

Chapter 9
The Hasse Principle

The *Hasse principle* asks the natural question: if a polynomial equation has non-trivial solutions in $\mathbf{R}$ and in $\mathbf{Q}_p$ for every prime p, can one deduce that it also has solutions in $\mathbf{Q}$? For quadratic forms, the answer is encouraging, but for more general situations this is only a "principle", which may be verified or not.

9.1 The Hasse–Minkowski Theorem

The first result in this direction goes back to Legendre (for quadratic forms in three variables) and to Minkowski (who, however, was not speaking of p-adic fields). It was Hasse, a student of Hensel, who saw the advantage of rephrasing the statement in terms of *p-adic obstruction* and who generalized the result for number fields.

Theorem 9.1.1 (Hasse–Minkowski, 1920). *A quadratic form defined over a number field k represents zero (non-trivially) in k if and only if it represents zero in all completions k_v (Archimedean and non-Archimedean).*

In this statement, v denotes an equivalence class of absolute values (also called a *place* of k), as in Definition 8.1.3. The completion is obtained by the argument in Construction 8.2.3, and Hensel's Lemma applies in the non-Archimedean case.

In fact, there is a non-Archimedean valuation associated with each prime ideal of the ring of integers of the field k, since this ring $\mathcal{O}_k$ is a Dedekind ring. We conceive these places as being *local*, since the valuation ring $\mathcal{O}_v$ is a local principal ring (see Exercise 8.2).

Regarding the field k as a *global* field, the general question is: *how to pass from local to global?* For each Archimedean place, the completion is $\mathbf{R}$ or $\mathbf{C}$. We can also reason in terms of embeddings: if $k/\mathbf{Q}$ is an extension of degree d, the argument from Corollary 3.1.10 shows that there are $d = r_1 + 2r_2$ $\mathbf{Q}$-embeddings of k into $\mathbf{C}$, where r_1 is the number of real roots of a minimal polynomial, the $2r_2$ others being pairs of

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_9

complex conjugate roots. Then, the Archimedean places are $r_1 + r_2$ in number. (See also Example 3.1.4, where $k = \mathbf{Q}(\sqrt{2})$.)

We shall not prove the Hasse–Minkowski Theorem here (see Cassels & Fröhlich [CF], Exercise 4.8, p. 359). Let us only say that the proof is first done for three variables, then four, then five, and that it always uses versions of Dirichlet's Theorem about primes in arithmetic progressions (see Lemma 6.4.3), as well as the density of k in its completions. It also uses, by the way, a generalization of the quadratic reciprocity law, which highlights, for forms in three variables, a frequently used result.

Proposition 9.1.2. *The number of places where a form in three variables does not represent zero is even.*

In particular, in order to know whether a form in three variables represents zero, it suffices to verify this for all completions except one (see [CF], Exercise 4.5, p. 358). This property allows clever combinations with Dirichlet's Theorem, thanks to which we can make use of a prime about which we know almost nothing, with no need to control it further.

Since p-adic fields are C_2 for a quadratic form, we also have the following corollary, which was originally a theorem of Meyer.

Corollary 9.1.3. *Every indefinite quadratic form in at least five variables represents zero in k.*

We can also restate the theorem in geometric terms.

Theorem 9.1.4. *Let k be a number field and Ω the set of all places of k (Archimedean and non-Archimedean); then, if $Y = V(f) \subset \mathbf{P}_k^n$ is a quadric, we have:*

$$Y(k_v) \neq \emptyset \quad \forall\, v \in \Omega \implies Y(k) \neq \emptyset.$$

We say that *the Hasse principle holds for quadrics* $Y \subset \mathbf{P}_k^n$. We may ask if it also holds for other *classes* of varieties. Obviously, the answer is negative in general, but there are interesting families of varieties that verify or do not verify the Hasse principle.

Example 9.1.5 (W. Ellison, 1968). The Hasse principle does not hold for the surface $Y = V(f, g) \subset \mathbf{P}_{\mathbf{Q}}^4$ defined by the following system:

$$\begin{cases} f = x_0^2 - 17x_1^2 - x_2^2 \\ g = x_0^2 - 17x_1^2 + x_3^2 + x_4^2. \end{cases}$$

Indeed, using Corollary 3.4.11, we see that there are solutions in all p-adic fields. But $Y(\mathbf{Q}) = \emptyset$, for subtracting the two equations we find $x_2^2 + x_3^2 + x_4^2 = 0$, which has only the trivial solution in $\mathbf{Q}_2$ or in $\mathbf{R}$, and of course 17 is not a square in $\mathbf{Q}$.

Geometrically, Y is a projective surface with four double points, namely $[0:0:0:1:\pm i]$ and $[\pm\sqrt{17}:1:0:0:0]$. Since it has only two real points, it is quite easy to verify that $Y(\mathbf{Q}) = \emptyset$. This is why it is interesting to state the Hasse principle more precisely as follows.

Definition 9.1.6. We say that a class $\mathcal{V}$ of algebraic varieties, defined over a number field k, *verifies the fine Hasse principle* if the existence on $V \in \mathcal{V}$ of a **non-singular** point with coordinates in k_v, for all completions k_v of k, implies that **every projective model** of V has a k-rational point.

Thus, Ellison's example verifies the fine Hasse principle, since all its points with coordinates in $\mathbf{Q}_2$ or in $\mathbf{R}$ are singular.

Remark 9.1.7. The existence of a non-singular point, real or p-adic, on an arbitrary model of V, implies that there are such points on all models, as follows from the implicit functions theorem (Corollary 8.4.6). Moreover, if an arbitrary smooth model of V has a k-rational point, so does any projective model of V, as follows from Nishimura's Lemma (Lemma 5.5.12).

9.2 Counter-Examples

The most beautiful proof that the fine Hasse principle is not valid for curves of genus 1 is attributed to Lind. It makes use of the *quadratic reciprocity law*, which links the different primes and prevents them from behaving in a completely independent manner.

Proposition 9.2.1 (Reichardt–Lind, 1940). *The genus* 1 *curve* X *defined over* $\mathbf{Q}$ *by the equation*

$$2y^2 = x^4 - 17$$

is a counter-example to the fine Hasse principle.

Proof. The polynomial $x^4 - 17$ has a root in $\mathbf{Q}_2$ (take $x_0 = 3$ in Proposition 8.4.1), and 2 is a square modulo 17. These are the only explicit computations needed to show that there are solutions in every $\mathbf{Q}_p$, since for all other primes we can use Corollary 4.2.13.

As for solutions in $\mathbf{Q}$, we set $x = u/v$ with u and v relatively prime integers; then, since 2 is not a square, we can write $y = w/v^2$ with $w \in \mathbf{Z}$, so $2w^2 = u^4 - 17v^4$. Obviously, $w \neq 0$; let $p \neq 2$ be a prime factor of w; then, 17 is a square modulo p. Since $17 \equiv 1 \pmod 4$, we have: $\left(\frac{17}{p}\right) = 1 \implies \left(\frac{p}{17}\right) = 1$, by the quadratic reciprocity law; as 2 is also a square modulo 17, we find that w^2 is a *fourth-power* modulo 17. But then 2 should be a fourth-power modulo 17, which is not the case: $\mathbf{F}_{17}^*$ is cyclic of order 16; therefore, it has exactly four classes of non-zero fourth powers: these are ± 1 and ± 4.

The statement refers to the smooth compactification of the affine curve $2y^2 = x^4 - 17$ (see Corollary 5.5.13), but the closure of this curve in $\mathbf{P}^2_{\mathbf{Q}}$ is singular. It is thus better to consider its image by the morphism $(x, y) \mapsto (x, y, z = x^2)$ from $\mathbf{A}^2_{\mathbf{Q}}$ into $\mathbf{A}^3_{\mathbf{Q}}$. We find the curve $\Gamma \subset \mathbf{A}^3_{\mathbf{Q}}$ defined by the equations

$$z = x^2, \qquad 2y^2 = z^2 - 17.$$

The closure of Γ in $\mathbf{P}^3_{\mathbf{Q}}$ is a non-singular curve, defined by the equations

$$z\,t = x^2, \qquad 2y^2 = z^2 - 17t^2. \tag{9.2.1}$$

There are two points at infinity, (i.e., in the plane $t = 0$): these are $[x : y : z : t] = [0 : 1 : \pm\sqrt{2} : 0]$ and they are not rational. □

We can also desingularize by gluing two affine pieces, writing $x = 1/u$ and $y = v/u^2$; hence, $2v^2 = 1 - 17u^4$; for $u = 0$, we find $v = \pm 1/\sqrt{2}$.

The next example is just one of a great number exhibited by Selmer in a 160-page paper, but it has remained the most famous. The proof, typical in algebraic number theory, relies on a fine analysis of the field $\mathbf{Q}(\sqrt[3]{6})$.

Proposition 9.2.2 (Selmer, 1951). *The genus* 1 *curve* $X \subset \mathbf{P}^2_{\mathbf{Q}}$ *with equation*

$$3x^3 + 4y^3 + 5z^3 = 0,$$

is a counter-example to the fine Hasse principle.

Proof. For p-adic solutions, we can use Corollary 4.2.13, but an elementary argument is suggested in Exercise 9.3.

Let us show that $X(\mathbf{Q}) = \emptyset$. On multiplying the equation by 2 and making obvious changes of variables, we are reduced to showing that the equation

$$10Z^3 = X^3 - 6Y^3 \tag{9.2.2}$$

has no non-trivial integer solutions. Set $\theta = \sqrt[3]{6} \in \mathbf{R}$ and $K = \mathbf{Q}(\theta)$; then, $\mathcal{O}_K$ is a free $\mathbf{Z}$-module with basis $\{1, \theta, \theta^2\}$, since $6 \not\equiv \pm 1 \pmod 9$. (See Selmer's tables [Sel]; in particular, §1 of the introduction.) We also know that the group of positive units of $\mathcal{O}_K$ is cyclic, generated by the *fundamental unit*[1] $\eta = 1 - 6\theta + 3\theta^2$; its inverse is $\eta^{-1} = 109 + 60\theta + 33\theta^2$. Moreover, $\mathcal{O}_K$ *is principal*.

The primes 2 and 3 ramify totally in K: one checks directly that $2 = (2-\theta)^3\,\eta^{-1}$ and that $3 = (3 + 2\theta + \theta^2)^3\,\eta$. Moreover, $5 = N_{K/\mathbf{Q}}(-1+\theta) = (-1+\theta)(1+\theta+\theta^2) = \mathfrak{p}_1\mathfrak{p}_2$ is the product of an ideal of degree 1 and an ideal of degree 2.

[1] For the computations that follow, it suffices to know that η is not a cube. To see this, we may consider the ideal $\mathfrak{p} = (1+\theta)$, which has norm 7. In $\mathcal{O}_K/\mathfrak{p} = \mathbf{F}_7$, we have: $\eta \equiv 3$, which is neither a square nor a cube modulo 7.

Consider an integer solution (X, Y, Z) of the equation

$$10Z^3 = X^3 - 6Y^3 = N_{K/\mathbf{Q}}(X - \theta Y) = (X - \theta Y)(X^2 + \theta XY + \theta^2 Y^2), \qquad (9.2.3)$$

where we may assume that $Z \neq 0$ and that $\gcd(X, Y) = 1$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal dividing $X - \theta Y$. Then, if $\mathfrak{p} \nmid 6$, $\mathfrak{p}$ cannot divide $X^2 + \theta XY + \theta^2 Y^2 = (X - \theta Y)^2 + 3\theta XY$. Otherwise, it would divide XY; hence, X and Y. It follows from (9.2.3) that, if, moreover, $\mathfrak{p} \nmid 5$, we have $v_{\mathfrak{p}}(X - \theta Y) \equiv 0 \pmod 3$.

As for the ideal $\mathfrak{p}$ lying over 3, it cannot divide $X - \theta Y$. Indeed, $\mathfrak{p} \mid X - \theta Y \implies \mathfrak{p} \mid 10Z^3 \implies \mathfrak{p} \mid Z \implies 3 \mid Z$; hence, $3 \mid X$, then $3 \mid Y$, but $\gcd(X, Y) = 1$; a contradiction. We can thus write $(X - \theta Y) = \mathfrak{q}^{\alpha}\mathfrak{p}_1^{\beta}\mathfrak{p}_2^{\gamma}\mathfrak{a}^3$, with $\mathfrak{q}^3 = (2)$ and $\mathfrak{p}_1\mathfrak{p}_2 = (5)$, $\mathfrak{p}_2$ having degree 2.

Lemma 9.2.3. $\mathfrak{p}_2 \nmid X - \theta Y$.

Proof. Let $\nu = v_{\mathfrak{p}_2}(X - \theta Y)$. If $\nu \geq 1$, we have seen above that $\mathfrak{p}_2$ does not divide $X^2 + \theta XY + \theta^2 Y^2$. Therefore,

$$v_{\mathfrak{p}_2}(10Z^3) = v_{\mathfrak{p}_2}(X - \theta Y) + v_{\mathfrak{p}_2}(X^2 + \theta XY + \theta^2 Y^2) = \nu + 0 = \nu;$$

but, $N_{K/\mathbf{Q}}(\mathfrak{p}_2) = 5^2$; hence,

$$v_5(10Z^3) = v_5(N(X - \theta Y)) = 2\nu + v_{\mathfrak{p}_1}(X - \theta Y) \geq 2\nu.$$

Since $v_5(10Z^3) = v_{\mathfrak{p}_2}(10Z^3)$, we obtain: $2\nu \leq \nu$; thus, $\nu = 0$, a contradiction. □

We thus have: $(X - \theta Y) = \mathfrak{q}^{\alpha}\mathfrak{p}_1^{\beta}\mathfrak{a}^3$, with $\mathfrak{q} = (2 - \theta)$ and $\mathfrak{p}_1 = (-1 + \theta)$. Moreover, $\alpha \equiv \beta \equiv 1 \pmod 3$, since $N(\mathfrak{q}) = 2$ and $N(\mathfrak{p}_1) = 5$. Therefore, we can set $\alpha = \beta = 1$, absorbing the cubes into the ideal $\mathfrak{a}$. Since $\mathcal{O}_K$ is principal, we can write:

$$X - \theta Y = \eta^{\nu}(2 - \theta)(-1 + \theta)\,\xi^3, \qquad (9.2.4)$$

with $\nu = 0, \pm 1$, and $\xi = u + \theta v + \theta^2 w$ $(u, v, w \in \mathbf{Z})$. We shall consider, for each of these three values of ν, the coefficient of θ^2 on the right-hand side. It must be zero, because of the left-hand side. Its cancellation defines a plane cubic Y_ν with no rational points, as we show by a p-adic argument.

Lemma 9.2.4. *Let $\omega = (a + \theta b + \theta^2 c)(u + \theta v + \theta^2 w)^3$, with $a, b, c \in \mathbf{Z}$. Then, the cancellation of the coefficient of θ^2 in ω defines the curve Y with equation*

$$c(u^3 + 6v^3 + 36w^3 + 36uvw) + b(3u^2v + 18v^2w + 18uw^2) + a(3u^2w + 3uv^2 + 18vw^2) = 0.$$

If $c \not\equiv 0 \pmod 3$, this curve has no points with coordinates in $\mathbf{Q}_3$.

Proof. We calculate $(u+\theta v+\theta^2 w)^3 = (u^3+6v^3+36w^3+36uvw)+\theta(3u^2v+18v^2w+18uw^2)+\theta^2(3u^2w+3uv^2+18vw^2)$; hence, the first statement. As for the second one, we may assume that u, v, and w are relatively prime. If $c \not\equiv 0 \pmod 3$, we immediately see that $3 \mid u$. Then, 3^2 divides all the terms, except $6cv^3$. Hence, $3 \mid v$. Then, 3^3 divides all the terms, except for $36cw^3$. Thus, $3 \mid w$; contradiction. □

It now suffices to calculate $a+b\theta+\theta^2 c = \eta^\nu\,(2-\theta)(-1+\theta)$ and to check that $c \not\equiv 0 \pmod 3$. For $\nu = 0$, we find: $(2-\theta)(-1+\theta) = -2+3\theta-\theta^2$. For $\nu = 1$: $(1-6\theta+3\theta^2)(-2+3\theta-\theta^2) = \cdots - 25\theta^2$. For $\nu = -1$: $(109+60\theta+33\theta^2)(-2+3\theta-\theta^2) = \cdots + 5\theta^2$. In all three cases, the coefficient of θ^2 is not a multiple of 3, which finishes the proof. □

Comment 9.2.5. For each value of $\nu = 0, \pm 1$, we have obtained a curve Y_ν and we have shown that, if X had a rational point, then at least one of the curves Y_ν would also have one. Then, we showed that $Y_\nu(\mathbf{Q}_3) = \emptyset$ for all ν.

We have actually constructed morphisms $\varphi_\nu : Y_\nu \to X$ such that $X(\mathbf{Q}) = \bigcup \varphi_\nu(Y_\nu(\mathbf{Q}))$. If, for each ν, we could find a prime p such that $Y_\nu(\mathbf{Q}_p) = \emptyset$, we would have proved that $X(\mathbf{Q}) = \emptyset$. This is an illustration of the *descent method*, in the form developed by Colliot-Thélène and Sansuc, which allows many examples to be interpreted (see [CSS]).

With one more variable, there is another famous example.

Proposition 9.2.6 (Cassels & Guy, 1966). *The cubic surface $X \subset \mathbf{P}^3_{\mathbf{Q}}$, with equation*

$$5x^3+9y^3+10z^3+12w^3 = 0,$$

is a counter-example to the fine Hasse principle.

The proof is quite involved. It relies on a fine study (class number, units) of an extension of degree 9 of the rationals, which is the compositum of four purely cubic extensions of $\mathbf{Q}$. On intersecting with the plane with equation $x = z$, Selmer's example is retrieved in passing.

We must note that no counter-example of cubic of greater dimension is known. One can even conjecture that there are none, but the Hasse principle was proved for these varieties only if their dimension is very large (Heath-Brown), or if they have specific properties, like certain types of singularities.

For curves of genus greater than 1, we have the following nice example.

Proposition 9.2.7 (Coray & Manoil, 1996). *The hyperelliptic curve X of genus 2 defined over $\mathbf{Q}$ by*

$$s^2 = 2(t^3+7)(t^3-7)$$

is a counter-example to the fine Hasse principle.

Proof. For local solutions, it suffices, thanks to Weil's theorem (Theorem 4.2.12), to check that there are points in $\mathbf{Q}_p$ for $p \leq 13$. Now, there are solutions with $s = 0$ for $p = 2,\ 5$, and 11. Moreover, there is a solution with $t = 0$ for $p = 3$ and with $t = 2$ for $p = 7$ or 13.

Also, $X(\mathbf{Q}) = \emptyset$; indeed, there are no solutions at infinity, since 2 is not a square in $\mathbf{Q}$. Indeed, one can desingularize by gluing two affine pieces, writing $t = 1/u$ and $s = v/u^3$, Thus, $v^2 = 2(1 + 7u^3)(1 - 7u^3)$; for $u = 0$, we find $v = \pm\sqrt{2}$.

The image of X by the morphism $(t, s) \mapsto (2t^2, 2s) = (x, y)$ is the elliptic curve E with equation

$$y^2 = x^3 - 392$$

Now, E is one of the curves for which Birch and Swinnerton-Dyer already showed in 1962 that the Mordell–Weil group $E(\mathbf{Q})$ has rank 0 and no torsion. In fact, the only rational point of E is the point at infinity, over which lies no rational point on X. □

This example is of additional interest, because the curve X has smooth points in extensions of $\mathbf{Q}$ of degrees 2 and 3, but we see that this does not entail the existence of rational points, even if we assume, moreover, the existence of local solutions for every place.

Another historically important example concerns *rational surfaces having a fibering with conics* over $\mathbf{P}^1_{\mathbf{Q}}$: for the Châtelet surface below, we obtain the equation of a conic $y^2 + z^2 = (c - x_0^2)(x_0^2 - c + 1)\, t^2$ for each value of $x = x_0 \in \overline{\mathbf{Q}}$. We can also write

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1)\, t^2,$$

then make this subvariety of $\mathbf{P}^2_{\mathbf{Q}} \times \mathbf{A}^1_{\mathbf{Q}}$ compact, by gluing it to another subvariety

$$Y^2 + Z^2 = (cu^2 - 1)(1 - (c - 1)u^2)\, T^2,$$

obtained by the change of variables $y = x^2 Y$, $z = x^2 Z$, $t = T$, $x = 1/u$. These subvarieties coincide if $xu \neq 0$.

Proposition 9.2.8 (Iskovskikh, 1971). *The Châtelet surface with equation*

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1),$$

where $c \in \mathbf{N}$, $c \equiv 3 \pmod 4$, *is a counter-example to the fine Hasse principle.*

Proof. The fiber at infinity has equation $Y^2 + Z^2 = -T^2$, which has solutions in $\mathbf{F}_p$ (Corollary 4.2.8); hence,[2] in $\mathbf{Q}_p$ if $p \neq 2$ (Hensel). For $p = 2$, we find a solution with $x = 0$ if $c \equiv 3 \pmod 8$ and with $x = 1$ if $c \equiv -1 \pmod 8$.

On writing $x = u/v$, the equation becomes

$$y^2 + z^2 = (cv^2 - u^2)(u^2 - (c-1)v^2),$$

with $u,\ v \in \mathbf{Z}$, $\gcd(u, v) = 1$ and $y,\ z \in \mathbf{Q}$.

If a prime p divides both $cv^2 - u^2$ and $u^2 - (c-1)v^2$, by adding the two factors we see that $p \mid v$; hence, $p \mid u$, which is a contradiction. On the other hand, it is well-known that *if the product of two relatively prime positive integers is a sum of two squares, then each of its prime factors congruent to* 3 *modulo* 4 *appears with an even exponent*, so that each of the two numbers is a sum of two squares. Since $(cv^2 - u^2) + (u^2 - (c-1)v^2) = v^2 > 0$, we infer that both integers are positive and that there is a rational solution for the system

$$\begin{cases} u_1^2 + v_1^2 = cv^2 - u^2 \\ u_2^2 + v_2^2 = u^2 - (c-1)v^2. \end{cases} \qquad (*)$$

Now, there is no 2-adic solution, as one of the two members on the right-hand side is congruent to 3 modulo 4. □

Comment 9.2.9. As in Comment 9.2.5, the system $(*)$ defines a *descent variety* Y. In the present case, this is of greater dimension than the initial variety X, but there is nevertheless a morphism $\varphi : Y \to X$ such that $X(\mathbf{Q}) = \varphi(Y(\mathbf{Q}))$, whereas $Y(\mathbf{Q}_2) = \emptyset$.

9.3 Affirmative Results

Affirmative results are mostly characterized by geometric properties.

Definition 9.3.1. A *Severi–Brauer k-variety* is a projective k-variety K-isomorphic to $\mathbf{P}^n_K$, where K/k is an algebraic extension.

Example 9.3.2. Let $C \subset \mathbf{P}^2_k$ be a smooth conic. Let K/k be an algebraic extension such that $C(K) \neq \emptyset$. We know (Proposition 4.2.7) that C is K-isomorphic to $\mathbf{P}^1_K$.

Example 9.3.3. Let $V \subset \mathbf{P}^3_k$ be a smooth cubic surface having a rational sextuplet $\mathcal{S}_6$ (Notation 7.5.11). By Castelnuovo's criterion (Proposition 7.6.9), one can contract simultaneously the six lines of this sextuplet over k (see Example 7.7.3), and this

[2] The implicit functions theorem entails that there are also solutions other than at infinity, but we can dispense with looking for them explicitly!

shows that V is k-birationally equivalent to a k-variety, which is not $\mathbf{P}^2_k$ if $V(k) = \emptyset$, but which is isomorphic to the plane over an algebraic extension K/k such that $V(K) \neq \emptyset$. This is a Severi–Brauer k-variety of dimension 2.

Proposition 9.3.4 (F. Châtelet, 1944). *Severi–Brauer varieties defined over a number field verify the Hasse principle.*

The proof of this result would be far beyond the scope of this book. Let us note, however, that the Galois cohomology methods introduced in François Châtelet's thesis in order to study these varieties have become absolutely classic.

Corollary 9.3.5. *Over a number field conics, as well as the smooth cubic surfaces that possess a rational sextuplet, verify the Hasse principle.* □

The case of conics gives the Hasse–Minkowski statement (Theorem 9.1.1), for forms in three variables. A smooth cubic surface with a rational $\mathcal{S}_6$ is not in general isomorphic, but merely k-birationally equivalent to a Severi–Brauer variety. However, it follows from Corollary 5.5.13 that (by Proposition 9.3.4) this suffices to ensure the existence of a rational point, if there are points everywhere locally.

Corollary 9.3.6. *The smooth cubic surfaces defined over a number field that have a rational triplet verify the Hasse principle.*

Proof. The description of the lines on a smooth cubic surface, starting from the blowing-up of six points in the plane (see Example 7.7.3) clearly shows that any triplet is contained in exactly two sextuplets.[3] It then follows from Proposition 3.3.6 that V possesses a sextuplet rational over k or over a quadratic extension K/k. If $V(k_v) \neq \emptyset$ for all completions of k, we deduce from Corollary 9.3.5 that $V(K) \neq \emptyset$, and then, as in Example 3.3.10, that $V(k) \neq \emptyset$. □

Example 9.3.7. For diagonal cubics $ax^3 + by^3 + cz^3 + dw^3 = 0$, the existence of a rational triplet is equivalent to the statement (maybe after permutation of variables) that ab/cd is a cube in k^*. Therefore, such a surface verifies the Hasse principle.

Corollary 9.3.8. *The singular cubic surfaces defined over a number field that are not cones verify the fine Hasse principle.*

Proof. If $W \subset \mathbf{P}^3_k$ is a cone over a curve $X \subset \mathbf{P}^2_k$ of genus 1, as in Selmer's example, its vertex is k-rational, but it does not verify the fine Hasse principle, as it is birationally equivalent to the product $X \times \mathbf{P}^1_k$. This is why this case has been excluded from the statement.

If W is not a cone, the set $W(k)$ always contains an infinity of smooth points, except if this surface has exactly three double points on which the Galois group $\mathrm{Gal}(\bar{k}/k)$ acts transitively. In this latter case, one can show that W is k-birationally equivalent to a smooth cubic surface V having a rational triplet of lines,

[3] If the triplet is the blowing-up of three points P_1, P_2, and P_3, we can complete it either by the blowing-up of the three other points P_4, P_5, and P_6, or by the strict transforms of the three lines connecting P_4, P_5, and P_6 in pairs.

and we can apply the corollary below: if W has a non-singular point with coordinates in k_v, for all completions k_v of k, we also have $V(k_v) \neq \emptyset$ by Lemma 5.5.12; hence, $V(k) \neq \emptyset$ by Corollary 9.3.6. Then, every projective model of W also has a k-rational point (see Remark 9.1.7).

□

We can also give an interesting interpretation of Iskovskikh's counter-example, by showing that the proof we have given for Proposition 9.2.8 could work, because the associated descent variety verified the Hasse principle.

Theorem 9.3.9. *Let $c \in \mathbf{Z}$. The variety $Y \subset \mathbf{P}^5_{\mathbf{Q}}$ defined by the system*

$$\begin{cases} u_1^2 + v_1^2 = cv^2 - u^2 \\ u_2^2 + v_2^2 = u^2 - (c-1)v^2 \end{cases} \qquad (*)$$

verifies the fine Hasse principle.

If $c \leq 0$, we see that the only real points have $u_1 = v_1 = u = 0$ and are singular. If $c > 0$ is congruent to 3 modulo 4, we have seen in Proposition 9.2.8 that there is no 2-adic solution. There is another exception, since the integers congruent to 7 modulo 8 are not sums of three squares. Hence, the equivalent statement.

Theorem 9.3.10. *Let $c \in \mathbf{Z}$, $c > 0$, $c \not\equiv 3 \pmod 4$ and not of the form $4^\lambda(8\mu + 7)$. Then the system*

$$\begin{cases} u_1^2 + v_1^2 = cv^2 - u^2 \\ u_2^2 + v_2^2 = u^2 - (c-1)v^2 \end{cases} \qquad (*)$$

has a non-trivial rational solution.

Proof. The following proof dates back to 1979. It has never been published in this form, because more general statements were soon obtained. Although it is quite long, we give it in its entirety, because it makes use of several statements introduced before. In fact, it illustrates in a fairly elementary manner methods that appear under a more sophisticated form in general arguments.

(a) The first idea is to use Brumer's Theorem (Theorem 4.4.2). Thus, we only have to show that the equation

$$(u_1^2 + v_1^2) + t\,(u_2^2 + v_2^2) = (cv^2 - u^2) + t\,(u^2 - (c-1)v^2) \qquad (9.3.1)$$

has a non-trivial solution with coordinates in $\mathbf{Q}(t)$.

(b) The form

$$\varphi(u_1, v_1, u_2, v_2) = (u_1^2 + v_1^2) + t\,(u_2^2 + v_2^2)$$

is a *multiplicative Pfister form*. Therefore, the set of **non-zero** values it takes over $\mathbf{Q}(t)$ is a group. This result belongs to the general theory of Pfister forms, and this is all we need. It is however interesting to mention that, for four variables, there is a stronger statement expressed in terms of generalized quaternions (see [vdW], §93]).

Lemma 9.3.11. *Let k be a field and*

$$\varphi(u_1, u_2, u_3, u_4) = (u_1^2 + su_2^2) + t\,(u_3^2 + su_4^2), \tag{9.3.2}$$

with $s,\ t \in k$. There is a composition low in $\mathbf{A}_k^4$ such that the set of non-zero values taken by φ over k is a subgroup of k^*.

Proof. There is a composition law in $\mathbf{A}_k^4$ that associates with each couple $u = (u_1, u_2, u_3, u_4)$, $v = (v_1, v_2, v_3, v_4)$ the point

$$\begin{aligned} u*v = (&u_1v_1 - su_2v_2 - t\,(u_3v_3 + su_4v_4), u_1v_2 + u_2v_1 + t\,(u_3v_4 - u_4v_3),\\ &u_1v_3 - su_2v_4 + u_3v_1 + su_4v_2, u_1v_4 + u_2v_3 - u_3v_2 + u_4v_1). \end{aligned}$$

One verifies that $\varphi(u*v) = \varphi(u)\,\varphi(v)$. This law is associative, with neutral element $(1, 0, 0, 0)$. It is even a group law for each extension K/k if we restrict to the set $\Sigma = \left\{u \in K^4 \mid \varphi(u) \neq 0\right\}$: the inverse of $u \in \Sigma$ is $u^{-1} = \frac{1}{\varphi(u)}(u_1, -u_2, -u_3, -u_4)$. If we specialize for $s = t = 1$, we find of course the multiplication law of quaternions. (See Exercise 9.10.) □

(c) We shall look for a solution of (9.3.1) by taking u and v of the form

$$u = at + b, \qquad v = et + f, \tag{9.3.3}$$

where $a,\ b,\ e$, and f are suitably chosen integers. The right-hand side of (9.3.1) is then a polynomial

$$\begin{aligned} \pi(t) = &(a^2 - (c-1)e^2)\,t^3 + (ce^2 - a^2 + 2ab - 2(c-1)e\,f)\,t^2\\ &+ (2ce\,f - 2ab + b^2 - (c-1)\,f^2)\,t + (c\,f^2 - b^2), \end{aligned} \tag{9.3.4}$$

whose coefficients play an important role in the proof. Notice that we may assume, without loss of generality, that neither c nor $c-1$ are perfect squares, because in these cases the system $(*)$ has obvious rational solutions.

(d) Equation (9.3.1) can thus be written

$$(u_1^2 + v_1^2) + t\,(u_2^2 + v_2^2) = \pi(t) \tag{9.3.5}$$

and, since $\pi \in \mathbf{Q}[t]$ is a polynomial, we can study the *reduction modulo* π of this equation. This leads us to the following statement.

Proposition 9.3.12. *Under the hypothesis of Theorem 9.3.10, and provided that neither c nor $c-1$ are perfect squares, it is possible to choose integers a, b, e, and f such that $\pi(t)$ is $\mathbf{Z}$-irreducible of degree 3, with leading coefficient $+1$, and that the equation*

$$u^2 + v^2 + \tau w^2 = 0 \tag{9.3.6}$$

has non-trivial solutions in the field $\kappa_\pi = \mathbf{Q}[t]/(\pi) = \mathbf{Q}(\tau)$, where τ denotes the class of t in κ_π.

This proposition will be proved later. First, let us see how the main result follows, by a reasoning that goes back to Pfister.

(e) We must solve (9.3.5) with $u_1, v_1, u_2, v_2 \in \mathbf{Q}(t)$. Proposition 9.3.12 gives $u, v, w \in \kappa_\pi$ satisfying (9.3.6). Now, $w \neq 0$, since the cubic extension $\kappa_\pi/\mathbf{Q}$ cannot contain $\sqrt{-1}$. We can therefore find two numbers $x, y \in \kappa_\pi$ such that

$$x^2 + y^2 + \tau = 0. \tag{9.3.7}$$

Let $g(t)$ and $h(t)$ be two polynomials of degrees ≤ 2, which are lifts of x and y in $\mathbf{Q}[t]$. We thus have

$$g(t)^2 + h(t)^2 + t \equiv 0 \mod \pi(t),$$

that is

$$g(t)^2 + h(t)^2 + t = \pi(t)\rho(t), \tag{9.3.8}$$

where $\rho \in \mathbf{Q}[t]$ is a linear polynomial. Moreover, since the leading coefficient of π is 1, we observe that the leading coefficient of ρ is *the sum of the squares of the leading coefficients of g and h*.

Relation (9.3.8) indicates that the form φ of (9.3.2) represents the product $\pi(t)\rho(t)$ over the field $k = \mathbf{Q}(t)$, with $u_1 = g(t)$, $v_1 = h(t)$, $u_2 = 1$ and $v_2 = 0$. Hence, to solve (9.3.5) it suffices, by Lemma 9.3.11, to see that φ represents $\rho(t)$ over k.

Now, on considering (9.3.8) modulo $\rho(t)$, we also find that there are numbers $r, s \in \mathbf{Q}$ such that $r^2 + s^2 + \tau_1 = 0$ in the field $\kappa_\rho = \mathbf{Q}[t]/(\rho) = \mathbf{Q}(\tau_1) \cong \mathbf{Q}$, where τ_1 denotes the class of t in κ_ρ. Consequently, we can write $r^2 + s^2 + t = \frac{1}{d}\rho(t)$, where we find that d is nothing but the leading coefficient of ρ, already known to be a sum of two squares. Since $x^2 + y^2$ is a multiplicative $\mathbf{Q}$-form, it follows that $\rho(t) = d(r^2 + s^2) + td$ is indeed represented by φ over $\mathbf{Q}(t)$, which finishes the proof of Theorem 9.3.10. □

We still have to prove Proposition 9.3.12. As the proof is fairly technical, we shall start by studying a particular case, for which the proof is very short. Let us recall a well-known elementary result about *Pell–Fermat equations*.

Lemma 9.3.13. *Let $D \in \mathbf{N}^*$ be a positive integer that is not a perfect square. The equation $x^2 - Dy^2 = 1$ has an infinity of integer solutions.*

Proof. The set of numbers of norm 1 of the form $x + y\sqrt{D}$, with $x,\ y \in \mathbf{N}$, is a cyclic subgroup of the group of units of the field $\mathbf{Q}(\sqrt{D})$. The positive integer solutions of the equation are therefore given by all numbers of the form $(x_1 + y_1\sqrt{D})^m$, where (x_1, y_1) is the smallest[4] non-trivial solution of the equation. □

Remark 9.3.14. Equation $x^2 - Dy^2 = -1$ is very different, because the field $\mathbf{Q}(\sqrt{D})$ does not always have units with norm -1. For instance, if D has a prime factor $p \equiv 3 \pmod 4$ at an odd power, the Legendre symbol $\left(\frac{-1}{p}\right) = -1$ immediately shows that the equation has no rational solution. There are, however, cases in which the *false Pell equation* $Dy^2 - x^2 = 1$ has integer solutions, and then there is an infinity.

We turn to the proof of Proposition 9.3.12 *assuming that* $c = 13$. For the leading coefficient of $\pi(t)$ to be $+1$, we must, in view of (9.3.4), solve the Pell–Fermat equation $a^2 - 12e^2 = 1$, which has an infinity of integer solutions and in particular $a = 7$, $e = 2$.

If we also want to ensure that the constant term is $+1$, we are dealing with a false Pell equation $13\, f^2 - b^2 = 1$, which fortunately also has solutions in this case, for instance, $b = 18$, $f = 5$.

With these values we calculate $\pi(t) = t^3 + 15t^2 + 32t + 1$. This is an irreducible polynomial, because its reduction modulo 2 is a polynomial of degree 3 with no roots in the field $\mathbf{F}_2$. Hence, the quotient $\kappa_\pi = \mathbf{Q}[t]/(\pi)$ is indeed a field, in which the class τ of t is an algebraic integer with norm -1, and hence a unit.

Since all the coefficients of $\pi(t)$ are positive, all the real roots of this polynomial are negative. Consequently, τ is negative in all real embeddings of κ_π, so that the quadratic form (9.3.6) is indefinite at all real places.

Moreover, since the coefficients of this quadratic form are all units, we obtain, by the Chevalley–Warning Theorem (Corollary 3.4.12) and Hensel's Lemma that equation (9.3.6) has non-trivial solutions in all non-Archimedean completions of κ_π, except maybe at places over the ideal (2).

Now, there is only one prime ideal over (2), since $\pi(t)$ is irreducible modulo 2. It follows from Proposition 9.1.2 that the quadratic form (9.3.6) also represents zero at this unique remaining place.

We now use the Hasse–Minkowski Theorem (Theorem 9.1.1) to conclude that equation (9.3.6) has non-trivial solutions in the number field κ_π. □

[4]This minimal solution may be extremely big, even for relatively small values of D; for instance, for $D = 991$, the smallest integer non-trivial solution of the equation $x^2 - Dy^2 = 1$ is given by $x_1 + y_1\sqrt{D} = 379516400906811930638014896080 + 12055735790331359447442538767\sqrt{D}$.

Comment 9.3.15. It might seem that this proof is pointless, since we were able to solve explicitly the two Pell equations contained in the polynomial $\pi(t)$ and the same binary forms appear in the system $(*)$. But if we try to set $u = 7$, $v = 2$ or $u = 18$, $v = 5$ in $(*)$, we obtain nothing. It is the transformation (9.3.3), which – together with Brumer's Theorem – has served to **separate variables**, in order to treat the two Pell equations independently.

What is more, with a bit of luck, one can discover that $(*)$ has a solution with $u = 32$ and $v = 9$, but it would be quite difficult to deduce this solution from the hardly constructive argument we have given, which shows the existence using the Hasse principle of a quadratic form defined over a cubic extension of the rational numbers.

The complete proof of Proposition 9.3.12 uses the same elements, but we already know (Remark 9.3.14) that we cannot always solve the false Pell equation. Nor can we replace it by the true Pell–Fermat equation, because Formula (9.3.5) shows that the constant term of $\pi(t)$ must be positive, since $\pi(0)$ must be a sum of two squares.

To overcome this difficulty, we shall need Dirichlet's Theorem concerning primes in arithmetic progressions. Another difficulty is that the ideal (2) is not always prime in the extension $\kappa_\pi/\mathbf{Q}$, which forces us to study its decomposition and to introduce an extra 2-adic argument.

The next lemma will be useful for irreducibility.

Lemma 9.3.16 (Perron's Irreducibility Criterion). *If a polynomial* $\pi(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbf{Z}[t]$ *is such that*

$$|a_1| > 1 + |a_2| + \cdots + |a_n| \quad \textit{and} \quad a_n \neq 0,$$

then $\pi(t)$ *is* $\mathbf{Z}$*-irreducible.*

Proof. The functions $f(z) = a_1 z^{n-1}$ and $g(z) = z^n + a_2 z^{n-2} + \cdots + a_n$ are defined and holomorphic on the closed disc $|z| \leq 1$. On the circle $|z| = 1$, they verify the inequalities $f(z) \neq 0$ and $|g(z)| < |f(z)|$. A classical theorem in analysis (Rouché) states then that f and $f + g = \pi$ have the same number of zeros in the open disk $|z| < 1$.

As a consequence, $\pi(t)$ has $n - 1$ roots in the interior of the disk with radius 1. If this polynomial were reducible over $\mathbf{Z}$, one of its factors would have all its complex or real roots in the interior of the open disk with radius 1, which is not possible with integer coefficients, since $a_n \neq 0$. □

Proof of Proposition 9.3.12. (a) We first look at the constant term of the polynomial $\pi(t)$, which means choosing b and f. Under the hypothesis of Theorem 9.3.10, the first equation of the system $(*)$ has non-trivial solutions in all completions of $\mathbf{Q}$. The Hasse–Minkowski Theorem (Theorem 9.1.1) then implies that there are two relatively prime positive integers b_0 and f_0, such that

$$m_0 = c\, f_0^2 - b_0^2 > 0 \tag{9.3.9}$$

is a sum of two squares of rational numbers. As we have already noted in the course of the proof of Proposition 9.2.8, this property translates very simply into the decomposition of m_0 as a product of irreducible factors: each prime factor of m_0, congruent to 3 modulo 4 appears at an even power in this decomposition. In this case, it is well-known that m_0 *is also a sum of two squares of integers.*

We also observe that f_0 *is necessarily odd*;[5] otherwise, m_0 would be congruent to 3 modulo 4. We may add that b_0 *is necessarily even if* $c \equiv 0 \pmod 4$ and that m_0 *can be chosen odd if* $c \not\equiv 0 \pmod 4$, for in the expression $u_1^2 + v_1^2 = c\, f_0^2 - b_0^2$, the three numbers u_1, v_1 and b_0 can be neither all even nor all odd; thus, in this case we can choose the parity of b_0.

(b) In order to control the coefficient of t in $\pi(t)$, we set

$$f = p\, f_0, \qquad b = p b_0, \tag{9.3.10}$$

where p is defined by the next lemma.

Lemma 9.3.17. *There is a prime number*[6] $p \equiv 1 \pmod 4$ *such that*

$$p\, f_0^2 \not\equiv \pm 2\, b_0 \pmod q \tag{9.3.11}$$

for every prime factor $q \neq 3$ *of* m_0 *such that* $q \equiv 3 \pmod 4$.

Proof of Proposition 9.3.12. By the Chinese Remainder Theorem, there is an integer $p \equiv 1 \pmod 4$ such that, for each factor $q \neq 3$ of m_0 with $q \equiv 3 \pmod 4$, we have $p \equiv 1 \pmod q$ if $2\, b_0 \not\equiv \pm f_0^2 \pmod q$ and $p \equiv 2 \pmod q$ otherwise. And p can be chosen to be prime, by Dirichlet's Theorem on primes in arithmetic progressions (Lemma 6.4.3). □

(c) To prove Proposition 9.3.12, we first fix f_0 and b_0 as indicated at point (a), then p as in Lemma 9.3.17. We also define

$$Q = \prod_{\substack{q \mid m_0 \\ q \equiv 3 \pmod 4}} q. \tag{9.3.12}$$

Then we choose a and e among the infinity of solutions of the Pell–Fermat equation

$$a^2 - (c-1)\, e^2 = 1, \tag{9.3.13}$$

requiring moreover that

$$e > 0 \qquad \text{and} \qquad e \equiv 0 \pmod{2\, Q}. \tag{9.3.14}$$

[5] A deep result of Gauss about integer quadratic forms even guarantees an integer solution with $f_0 = 1$ (see also Exercise 4.12), but the argument given here is more easily suitable for generalizations.

[6] If the relation is already verified for $p = 1$, we can also make this choice.

Indeed, by Lemma 9.3.13, we can solve the equation $a^2 - De_0^2 = 1$ with $D = (c-1)(2\,Q)^2$; we then define $e = 2\,Q\,e_0$.

The polynomial (9.3.4) then becomes:

$$\pi(t) = t^3 + (e^2 - 1 + 2ab - 2(c-1)e\,f)\,t^2 + p\,(2ce\,f_0 - 2ab_0 - p\,m_0 + p\,f_0^2)\,t + p^2 m_0. \tag{9.3.15}$$

We have $ce\,f_0 - |ab_0| > 0$, since by (9.3.13) and (9.3.9) we have:

$$c^2e^2\,f_0^2 - a^2b_0^2 = e^2(c^2\,f_0^2 - (c-1)\,b_0^2) - b_0^2 = e^2(c\,m_0 + b_0^2) - b_0^2 \geq c\,m_0\,e^2 > 0.$$

This relation shows more precisely that, if $e > 0$ is large enough,[7] the coefficient of t in the expression (9.3.15) is positive, *independently of the sign of* a, *which will be chosen later.* Since according to (9.3.13) we have the approximation $|a| \cong e\sqrt{c-1}$, we see that – for e large enough – the coefficient of t^2 is also positive and can even be chosen such that

$$\pi(t) = t^3 + m_2\,t^2 + pm_1\,t + p^2 m_0 \tag{9.3.16}$$

satisfies the criterion from Lemma 9.3.16: $m_2 > 1 + pm_1 + p^2 m_0$. Consequently, $\pi(t)$ *is* $\mathbf{Z}$*-irreducible and all its real roots are negative.*

(d) With these choices for a, b, e, and f, we know that the equation (9.3.6) has non-trivial solutions in all the real embeddings of the number field κ_π. It remains to examine the non-Archimedean places, but only those that correspond to prime ideals of κ_π, which divide 2τ. For the others, all coefficients of the quadratic form are units and we obtain solutions in the corresponding completions thanks to the Chevalley–Warning Theorem (Corollary 3.4.12) and to Hensel's Lemma.

On the other hand, relation (9.3.16) indicates that τ is an algebraic integer with norm

$$N_{\kappa_\pi/\mathbf{Q}}(\tau) = -p^2 m_0. \tag{9.3.17}$$

If $\mathfrak{q}$ is a prime ideal that divides 2τ, we can write $N_{\kappa_\pi/\mathbf{Q}}(\mathfrak{q}) = q^s$, where q is a prime factor of $2\,pm_0$.

If $q \equiv 1 \pmod 4$, which includes in particular the case $q = p$, the equation $u^2 + v^2 + \tau w^2 = 0$ already has a solution with $w = 0$ in the field $\mathbf{Q}_q$ and there is nothing more to prove. We may therefore assume without loss of generality that $q = 2$ or that q is a divisor of Q.

[7] If A, E, and ℓ are positive real numbers such that $E^2 - A^2 \geq \ell E^2 > 0$, we also have $E > A$, and hence $E + A < 2E$. Therefore, $E - A = \frac{E^2-A^2}{E+A} > \frac{E^2-A^2}{2E} \geq (\ell E^2)/2E = \frac{1}{2}\ell E$; here, $A = |ab_0|$ and $E = ce\,f_0$, which grows proportionally with e.

(e) If $q \mid Q$, we have $e \equiv 0 \pmod{q}$ by (9.3.14) and we see from (9.3.15) that the reduction of $\pi(t)$ modulo q is

$$\widetilde{\pi}(t) = t^3 + (2ab - 1)\, t^2 + p\,(\, p\, f_0^2 - 2ab_0)\, t \in \mathbf{F}_q[t], \tag{9.3.18}$$

with $a \equiv \pm 1 \pmod{q}$, according to (9.3.13).

If $q \neq 3$, the choice of p we made by Lemma 9.3.17 ensures then that $p\, f_0^2 - 2ab_0 \not\equiv 0$ modulo q.

For $q = 3$, we note that 3 does not divide f_0; otherwise, by (9.3.9) it would also divide b_0, which is impossible, as the two numbers are relatively prime. Hence, $p\, f_0^2 \not\equiv 0 \pmod{3}$ and we have seen at point (c) that we are still free to choose the sign of a. On choosing it properly, we also obtain $p\, f_0^2 - 2ab_0 \not\equiv 0 \pmod{3}$.

Thus, in any case, the coefficient of t in (9.3.18) is non-zero. Hence, we can write:

$$\widetilde{\pi}(t) = t\,.\,\rho(t), \quad \text{with } \rho \in \mathbf{F}_q[t] \text{ and } \rho(0) \neq 0. \tag{9.3.19}$$

Let $\mathfrak{q}$ be a prime ideal lying over q that divides τ, and let $v_\mathfrak{q}$ be the corresponding discrete valuation. Since pm_1 is a q-adic unit, relation (9.3.16) with $\pi(\tau) = 0$ yields:

$$v_\mathfrak{q}(\tau) = v_\mathfrak{q}(\tau^3 + m_2\,\tau^2 + pm_1\,\tau) = v_\mathfrak{q}(\,p^2 m_0) = v_\mathfrak{q}(m_0). \tag{9.3.20}$$

This equality implies that $\mathfrak{q}$ has degree 1, because of relation (9.3.17). Indeed, one sees very easily that

$$v_\mathfrak{q}(N\tau) = e_1 v_q(N\tau) \quad \text{and} \quad v_q(N\tau) \geq f_1 v_\mathfrak{q}(\tau), \tag{9.3.21}$$

where e_1 is the *ramification index* of $\mathfrak{q}$, and f_1 its *residual degree*.[8] Therefore, as a consequence of the equality $v_\mathfrak{q}(\tau) = v_\mathfrak{q}(m_0) = v_\mathfrak{q}(N\tau)$ we have $e_1\, f_1 = 1$; thus, $N_{\kappa_\pi/\mathbf{Q}}(\mathfrak{q}) = q$, the ideal $\mathfrak{q}$ is not ramified and it is even the unique ideal lying over q that divides τ.

On the other hand, we have seen at point (a) that m_0 is a sum of two squares; since $q \equiv 3 \pmod{4}$, this implies that the valuation $v_q(m_0)$ is even. Hence, $v_\mathfrak{q}(\tau) = v_\mathfrak{q}(m_0) = e_1 v_q(m_0)$ is even as well.

In the completion of κ_π with respect to the discrete valuation $v_\mathfrak{q}$ (which is actually isomorphic to $\mathbf{Q}_q$, since $\mathfrak{q}$ has degree 1), the ideal $\mathfrak{q}$ is principal (see Exercise 8.2). Write $\mathfrak{q} = (\vartheta)$. We have: $(\tau) = (\vartheta^{2r})$ in $\mathbf{Q}_q$, with $r \in \mathbf{N}^*$. The ratio $\frac{\tau}{\vartheta^{2r}}$ is therefore a $\mathfrak{q}$-adic unit and, by the Chevalley–Warning Theorem, we can solve the equation

$$u^2 + v^2 + \frac{\tau}{\vartheta^{2r}} w_1^2 = 0.$$

We then obtain a solution of Equation (9.3.6) on setting $w = \frac{w_1}{\vartheta^r}$.

[8] If $\mathfrak{q}^s$ divides τ, then $q^{\,f_1 s}$ divides $N\tau$, but there could be other prime ideals lying over q.

(f) To finish the proof of Proposition 9.3.12, it remains only to treat the case $q = 2$. If $c \not\equiv 0 \pmod 4$, we have chosen m_0 odd at point (a), as well as f_0. Since $e \equiv 0 \pmod 2$ according to (9.3.14), we see from (9.3.15) that the reduction of $\pi(t)$ modulo 2 is

$$\widetilde{\pi}(t) = t^3 + t^2 + 1 \in \mathbf{F}_2[t]. \tag{9.3.22}$$

Since this polynomial is irreducible, $\pi(t)$ is necessarily irreducible in $\mathbf{Z}_2[t]$. In this case, the ideal (2) remains prime in κ_π. It follows from Proposition 9.1.2 that the quadratic form (9.3.6) also represents zero at this unique remaining place. The Hasse–Minkowski Theorem (Theorem 9.1.1) allows us to conclude without further calculations that Equation (9.3.6) has non-trivial solutions in the number field κ_π, which concludes the proof.

If $c \equiv 0 \pmod 4$, the situation is more complicated, for m_0 being necessarily even, the reduction of $\pi(t)$ modulo 2 is

$$\widetilde{\pi}(t) = t \,.\, (t^2 + t + 1) \in \mathbf{F}_2[t], \tag{9.3.23}$$

so that the ideal (2) is the product of an ideal of degree 1 and of an ideal of degree 2 in κ_π. As above, it suffices to treat one of the two places, but we cannot avoid doing it; moreover, Hensel's Lemma for quadratic forms has a more complicated formulation for $\mathbf{Q}_2$ than for the other non-Archimedean valuations and it is not enough to study reductions modulo 2.

We shall treat the ideal $\mathfrak{q}$ of degree 1, the one that corresponds to the factor t in the decomposition (9.3.23). We can thus write $\tau = 2^\ell \eta$, where η is a 2-adic unit and $\ell \geq 0$. In fact $\ell \geq 1$, because (9.3.23) implies that $\mathfrak{q}$ divides τ. As seen at the end of point (a), we can write $m_0 = 2^n \mu$ with

$$\mu \equiv +1 \pmod 4 \quad \text{and} \quad n \geq 2. \tag{9.3.24}$$

Expression (9.3.15) reads over $\mathbf{Q}_2$:

$$\pi(\tau) = \tau^3 + m_2\,\tau^2 + p\,m_1\,\tau + 2^n\,p^2\mu = 0, \tag{9.3.25}$$

where the coefficient of τ is a 2-adic unit, since

$$m_1 = 2ce\,f_0 - 2ab_0 - p\,2^n\mu + p\,f_0^2 \equiv 1 \pmod 4.$$

Hence, we obtain

$$\ell = v_2(\tau) = v_2(\tau^3 + m_2\,\tau^2 + p\,m_1\,\tau) = v_2(2^n\,p^2\mu) = n,$$

that is,

$$\ell = n \geq 2.$$

If we divide (9.3.25) by 2^ℓ, we find:

$$2^{2\ell}\eta^3 + m_2\, 2^\ell \eta^2 + p\, m_1\, \eta + p^2\mu = 0, \tag{9.3.26}$$

from which

$$\eta + \mu \equiv 0 \pmod 4.$$

Therefore, $\eta \equiv -1 \pmod 4$; hence, $-\tau = -2^\ell\eta$ is a sum of two squares in $\mathbf{Q}_2$, which shows that Equation (9.3.6) has a non-trivial solution in this completion of κ_π. □

This result, proved in 1979, was considerably extended, in several steps. Here is one of the most general statements obtained at this time [CSS].

Theorem 9.3.18 (Colliot-Thélène, Sansuc, & Swinnerton-Dyer, 1987). *Let k be a number field and $Y \subset \mathbf{P}^n_k$ ($n \geq 4$) a pure, absolutely irreducible intersection of two quadrics, which is not a cone. Then, the fine Hasse principle is valid for Y in the following cases:*

(i) $n \geq 8$;
(ii) $n \geq 4$ *and Y contains a pair of conjugate skew lines (with an additional condition if $n = 5$);*
(iii) $n \geq 4$ *and Y contains a pair of conjugate double points (with an additional condition if $n = 4$ or 5).*

Exercises

9.1. Let p be a prime such that $p \equiv -1 \pmod 3$. Show that every integer is a cube modulo p.

9.2. If $p \equiv +1 \pmod 3$, show that the group $\mathbf{F}_p^*/(\mathbf{F}_p^*)^3$ is the cyclic group isomorphic to $\mathbf{Z}/(3)$. Deduce that, if 2 and 3 are not cubes modulo p, then 6 or 12 is a cube in $\mathbf{F}_p$.

9.3. Using the two preceding exercises, show that for any prime p the equation $3x^3 + 4y^3 + 5z^3 = 0$ has a non-trivial solution in $\mathbf{Q}_p$. (For instance, if 12 is a cube, one can set $z = -2y$, etc.)

9.4. Show that the Hasse principle is not valid for the equation in one variable $(X^2 - 2)(X^2 + 7)(X^2 + 14) = 0$, because the polynomial has a zero in $\mathbf{R}$ and in $\mathbf{Q}_p$ for every p, but not in $\mathbf{Q}$.

9.5. Using the Hasse–Minkowski Theorem, describe the integers N for which the equation $x^2 + y^2 + z^2 = N$ has rational solutions.

9.6. Combining the result of the previous exercise with that of Exercise 4.12, show that one can always take $f_0 = 1$ at point (a) in the proof of Proposition 9.3.12.

9.7. If a cubic surface has two singular points, show that it contains any line connecting these two points.

9.8. Show that the cubic surface with equation $x_1x_2x_3 = x_0^3$ has three singular points and determine all the lines on this surface (see Exercise 4.7).

9.9. Show that the surface with equation $x^3 + 2y^3 + 4z^3 - 6xyz - 929w^3 = 0$ verifies the fine Hasse principle. Does it have $\mathbf{Q}$-rational points? (See Exercise 3.7.)

9.10. Setting $\alpha = \begin{pmatrix} u_1 & u_2 \\ -su_2 & u_1 \end{pmatrix}$, $\beta = \begin{pmatrix} u_3 & u_4 \\ -su_4 & u_3 \end{pmatrix}$, $\bar{\alpha} = \begin{pmatrix} u_1 & -u_2 \\ su_2 & u_1 \end{pmatrix}$, $\bar{\beta} = \begin{pmatrix} u_3 & -u_4 \\ su_4 & u_3 \end{pmatrix}$ and similarly $\gamma = \begin{pmatrix} v_1 & v_2 \\ -sv_2 & v_1 \end{pmatrix}$, $\delta = \begin{pmatrix} v_3 & v_4 \\ -sv_4 & v_3 \end{pmatrix}$, etc., show that one finds the formulas in Lemma 9.3.11, based on the natural identification $u = \begin{pmatrix} \alpha & \beta \\ -t\bar{\beta} & \bar{\alpha} \end{pmatrix}$, $v = \begin{pmatrix} \gamma & \delta \\ -t\bar{\delta} & \bar{\gamma} \end{pmatrix}$.
(*Hint:* notice that $\det \alpha = u_1^2 + su_2^2$ naturally identifies with the diagonal matrix $\alpha\bar{\alpha}$ and that $u * v$ naturally identifies with the product of the matrices u and v. In fact, the matrices of the form $\begin{pmatrix} u_1 & u_2 \\ -su_2 & u_1 \end{pmatrix}$ form a commutative ring A that contains k as a subring; and $\varphi(u)$ equals the determinant of u, viewed as an endomorphism of A-modules.)

Chapter 10
Diophantine Dimension of Fields

Some Diophantine questions depend mainly on the geometry of the algebraic varieties involved, but others depend strongly on the *field* over which these varieties are defined. Diophantine dimension is a property of this nature.

10.1 The C_i Property

When Emil Artin, in 1934 or 1935, asked whether in a finite field, any form of degree d in $n > d$ variables had a non-trivial zero (property C_1), he was inspired by a theorem proven by Tsen in 1933. Tsen had proved that, if k is an algebraically closed field, the field $K = k(t)$ of rational fractions in one variable over this field has the property B_0 ("null Brauer group"). This amounts to saying that there is no non-commutative field that is a finite-dimensional K-algebra with center K.

Artin had noticed that Tsen actually proved that K is a C_1 field, before deducing directly B_0 from C_1, without using any particular property of the field. In passing, Artin was saying of a C_1 field that it was *quasi-algebraically closed*, because the proof of $C_1 \Rightarrow B_0$ we sketched in Remark 3.4.15 with the *reduced norm* resembles the proof – which uses the usual norm of algebraic extensions – that, for every $\epsilon > 0$, the fields $C_{1-\epsilon}$ are algebraically closed (see Exercise 3.13).

The solution given by Chevalley for finite fields (Corollary 3.4.12) was certainly complete, but did not diminish interest in the problem. On the contrary, it prompted new questions. Let us begin with precise definitions.

Definition 10.1.1. We say that k *is a* $C_i(d)$*field* if any form over k of degree d in $n > d^i$ variables has a non-trivial zero in k^n.

In this definition, d is clearly an integer, but i should be understood as belonging to $\overline{\mathbf{R}}_+ = \mathbf{R}_+ \cup \{+\infty\}$, agreeing to choose $i = +\infty$ if no $i \in \mathbf{R}$ satisfies the condition. For example, the field of real numbers is $C_0(d)$ for odd degrees, but $C_\infty(d)$ for even

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7_10

degrees. Recall that a field has the C_i property if it is $C_i(d)$ for every integer $d > 0$ (Definition 3.4.9).

On the other hand, it is clear that $C_i \Rightarrow C_{i'}$ for every $i' \geq i$. This justifies the following definition.

Definition 10.1.2. The *Diophantine dimension* $\alpha(k)$ of a field k is the smallest number $i \in \overline{\mathbf{R}}_+$ such that k is C_i. We also define, for each degree d, the number $\alpha_d(k)$ as the smallest $i \in \overline{\mathbf{R}}_+$ such that k is $C_i(d)$.

This is indeed a minimum, because if i denotes the infimum of the i' such that k is $C_{i'}$, it is clear that k also has the property C_i. Indeed, if F is a form of degree d in n variables with $n > d^i$, we have $n > d^{i+\epsilon}$ for every small enough $\epsilon > 0$ and then, on setting $i' = i + \epsilon$, we see that F has a non-trivial zero in k^n. We deduce from this a quite natural result.

Lemma 10.1.3. *A field whose Diophantine dimension $\alpha(k)$ is equal to i has the C_i property.* □

Finite fields have the C_1 property, by the Chevalley–Warning Theorem (Corollary 3.4.12), but Lemma 3.4.8 allows one to assert that $\alpha_d(\mathbf{F}_q) = 1$ for any degree d.

As a natural extension of this result, Artin conjectured that p-adic fields have Diophantine dimension 2 (see Chapter 8, in particular, Proposition 8.3.10). We shall return to this question in the following sections, but we already know the counter-example found by Terjanian in 1966 (Exercise 8.11), which proves that $\mathbf{Q}_2$ is not $C_2(4)$; in fact, $\alpha(\mathbf{Q}_2) \geq \alpha_4(\mathbf{Q}_2) \geq \log_4 18 > 2{,}08496$.

However, it was known for quite a while that $\alpha_2(\mathbf{Q}_p) = \alpha_3(\mathbf{Q}_p) = 2$ for every p. We shall first take an interest in general results, valid for any field, such as the following famous result, which generalizes Tsen's Theorem.

Theorem 10.1.4 (Lang's Thesis). *If k is a field C_i, the field of rational fractions in one variable $K = k(t)$ is C_{i+1}.*

This theorem, which dates back to 1951, was one of the main results of the thesis of Serge Lang, who was a student of Artin at Princeton. It was stated with a slightly restrictive condition, which M. Nagata managed to eliminate in 1957. All the proofs use the following construction.

Construction 10.1.5. Let Φ be a form of degree e in $N \geq r$ variables, and $F_1, \ldots, F_r$ forms in n variables, all having the same degree d. Starting from $\Phi^{(1)} = \Phi$ and $N_1 = N$, one defines recursively:

$$\Phi^{(\mu)}(X_1, \ldots, X_{N_\mu}) = \Phi^{(\mu-1)}(F_1, \ldots, F_r \mid \cdots \mid F_1, \ldots, F_r \mid 0, \ldots, 0),$$

which is a form of degree $D_\mu = e\, d^{\mu-1}$ in $N_\mu = n \left[\frac{N_{\mu-1}}{r} \right]$ variables.

The notation means that we distribute the variables so that $X_1, \ldots, X_n$ are associated with the first group of forms $F_1, \ldots, F_r$, then $X_{n+1}, \ldots, X_{2n}$ belong

to the second group, and so on. We complete by zeros, in numbers less than r. Writing explicitly, we would have:

$$\Phi^{(\mu-1)}(F_1(X_1,\dots,X_n),\dots,F_r(X_1,\dots,X_n),F_1(X_{n+1},\dots,X_{2n}),\dots,$$
$$\dots,F_1(X_{N_\mu-n+1},\dots,X_{N_\mu}),\dots,F_r(X_{N_\mu-n+1},\dots,X_{N_\mu}),0,\dots,0),$$

but the structured notation (which is attributed to Lang) allows one to discern better the properties of the $\Phi^{(\mu)}$.

This construction allows us to increase the number of variables of certain forms, while preserving some of their properties. For example (in the language of Definition 3.2.9), the following lemma.

Lemma 10.1.6. *If k is not C_0, there are forms in m variables of an arbitrarily large degree that do not represent zero (non-trivially) in k.*

Proof. Since k is not algebraically closed, it has at least one non-trivial extension K/k. The norm form $N_{K/k}$ (Proposition 3.2.7) is a form Φ of degree $e=[K:k]\geq 2$ in $N=e$ variables without non-trivial zero in k^N.

We set $r=1$ and $F_1=\Phi$; hence also $d=e$ and $n=N$. We then see by induction on μ that for any μ the form $\Phi^{(\mu)}$, which has degree $m=N^\mu$ and m variables, does not represent zero non-trivially in k. □

Another application of Construction 10.1.5 is that property C_i is preserved by algebraic extension. The example $\mathbf{C}/\mathbf{R}$ shows, however, that the Diophantine dimensions $\alpha(k)$ and $\alpha(K)$ are not equal in general, even if the extension is finite.

Proposition 10.1.7. *An algebraic extension K/k of a C_i field is also C_i.*

Proof. We may assume without loss of generality that K/k is a finite extension. Indeed, a given form $\Phi\in K[X_1,\dots,X_n]$ has only a finite number of coefficients, which belong to a finite extension contained in K/k.

So, let Φ be a form of degree d in n variables, defined over K, with $n>d^i$, and suppose that it does not represent zero in K. We set $r=1$ and $F_1=\Phi$; hence, also $N=n$ and $e=d$. Then, $\Phi^{(\mu)}$ is a form of degree $D_\mu=d^\mu$ in $N_\mu=n^\mu$ variables. If μ is large, it has many more variables than Φ, but as in Lemma 10.1.6, we observe that it does not represent zero non-trivially in K.

Let g be the degree of the extension K/k. We consider the *norm* (relatively to K/k): $F(X_1,\dots,X_{N_\mu})=N_{K/k}(\Phi^{(\mu)})$, i.e., as in Construction 3.2.6, the determinant $\det\ell_\varphi$ of the multiplication endomorphism by $\varphi=\Phi^{(\mu)}(X_1,\dots,X_{N_\mu})$ in $K[X_1,\dots,X_{N_\mu}]$.

This is a form $F\in k[X_1,\dots,X_{N_\mu}]$ of degree gD_μ. Since g and i are fixed, we also define the constant $\gamma=g^i$. Now, since $n>d^i$, we can choose μ large enough so that $n^\mu>\gamma(d^i)^\mu$; hence, $N_\mu=n^\mu>(gD_\mu)^i$. By hypothesis, k is a field C_i; therefore, the form F has a non-trivial zero in k^{N_μ}. Now, as we have seen in Chapter 3, if $\det\ell_\varphi$ vanishes at an element of k^{N_μ}, then φ has a non-trivial zero in K^{N_μ}, contradicting what precedes. □

Remark 10.1.8. It is apparently still unknown whether, for fixed d, any algebraic extension of a field $C_i(d)$ is also $C_i(d)$.

The next result reminds us of the complete statement of the Chevalley–Warning Theorem (Theorem 3.4.10).

Proposition 10.1.9 (Nagata). *Let k be a field C_i and let $F_1, \dots, F_r$ be forms in n variables, all of the same degree d. We suppose that $n > r\,d^i$. Then, these forms have a common non-trivial zero in k^n.*

Proof. For $i = 0$, this is a result in algebraic geometry: over an algebraically closed field, the intersection of r hypersurfaces in the projective space $\mathbf{P}^{n-1}$, with $n > r$, is not empty (see [Sh], Chap. I, §6, Cor. 5 of Theorem 4 and the remark that follows).

For $i > 0$ we first apply Lemma 10.1.6 in order to choose a form Φ in $N \geq r$ variables, of sufficiently large degree N, without a non-trivial zero in k^N. Construction 10.1.5 yields forms

$$\Phi^{(\mu)}(X_1, \dots, X_{N_\mu}) = \Phi^{(\mu-1)}(F_1, \dots, F_r \mid \cdots \mid F_1, \dots, F_r \mid 0, \dots, 0)$$

of degree $D_\mu = N\,d^{\mu-1}$ in $N_\mu = n\left[\frac{N_{\mu-1}}{r}\right]$ variables. It suffices to see that $N_\mu > (D_\mu)^i$ if N and μ are large enough.

Indeed, k is C_i, which ensures that the form $\Phi^{(\mu)}$ has a non-trivial zero $(a_1, \dots, a_{N_\mu}) \in k^{N_\mu}$. We may assume that μ is minimal with this property; hence, $\mu \geq 2$, since $\Phi^{(1)} = \Phi$ does not represent zero in k. There may be many zero coordinates, but there is at least a group, for instance the first one, such that $(a_1, \dots, a_n) \neq (0, \dots, 0)$. Since $\Phi^{(\mu-1)}$ does not represent zero non-trivially, we have $F_1(a_1, \dots, a_n) = \cdots = F_r(a_1, \dots, a_n) = 0$.

To see that $N_\mu > (D_\mu)^i$, it suffices to show that the sequence of ratios $\frac{N_\mu}{(D_\mu)^i}$ is increasing and tends to infinity (in fact, as quickly as a geometric progression) when μ tends to infinity. Indeed, the ratio

$$\frac{N_\mu}{(D_\mu)^i} \Big/ \frac{N_{\mu-1}}{(D_{\mu-1})^i} = \frac{n\left[\frac{N_{\mu-1}}{r}\right]}{(Nd^{\mu-1})^i} \cdot \frac{(Nd^{\mu-2})^i}{N_{\mu-1}} = \frac{n}{r\,d^i} \cdot \frac{r}{N_{\mu-1}} \cdot \left[\frac{N_{\mu-1}}{r}\right]$$

is of the form $\frac{n}{r\,d^i} \cdot \frac{[x]}{x}$, where $x = \frac{N_{\mu-1}}{r} \in \mathbf{R}$. By hypothesis, $\frac{n}{r\,d^i}$ is a constant > 1; and $1 - \frac{[x]}{x} = \frac{x-[x]}{x} < \frac{1}{x}$, which shows that the ratio $\frac{[x]}{x}$ tends toward 1 when x tends toward infinity. □

We are now in a position to prove Lang's thesis.

Proof of Theorem 10.1.4. Let F be a form of degree d in $n > d^{i+1}$ variables, defined over the field $K = k(t)$. We may assume from the outset that the coefficients are in the polynomial ring $k[t]$ and that their degrees are at most some integer M.

Let us apply the old method consisting of assuming the problem solved: the form F vanishes when we replace each variable X_j by a polynomial $\sum_{\ell=0}^{s} a_{j\ell}\,t^\ell$ with

coefficients in k, where the exponent s is chosen sufficiently large. On expanding, we find an expression of the form

$$F(X_1, \dots, X_n) = \sum_{\ell=0}^{ds+M} F_\ell(a_{10}, \dots, a_{ns})\, t^\ell,$$

where the F_ℓ are forms of degree d with coefficients in k. The number of variables is $n(s+1)$. The existence of numbers $a_{j\ell} \in k$, which are common zeros to all the F_ℓ, is guaranteed by Proposition 10.1.9, if $n(s+1) > (ds + M + 1)\, d^i$. Now, this condition is easy to satisfy by choosing s large enough, because it is equivalent to $s(n - d^{i+1}) > (M+1)\, d^i - n$ and by hypothesis $n - d^{i+1} > 0$. □

Scholion 10.1.10. If k is a field C_i, the field $k((t))$ of formal series in one indeterminate also has the C_{i+1} property. This result was first proved by Lang for a finite field $k = \mathbf{F}_q$. The argument in this case is very simple and resembles that in Corollary 8.3.7. Here, we use the fact that $k(t)$ is C_{i+1} to obtain a sequence of solutions modulo the powers of t, then the compactness of $k[[t]]$ to extract a convergent subsequence.

However, if k is infinite, the field $k((t))$ is not locally compact and another argument must be given. M. Greenberg discovered in 1967 a Henselian statement that allows one to assert that a form represents zero in $k((t))$ if and only if it represents zero non-trivially in $k[[t]]/(t^\nu)$ for every $\nu \geq 1$. This allows one to apply Theorem 10.1.4, since the quotients $k[t]/(t^\nu)$ are the same.

Unfortunately, these results do not extend well to a larger number of variables, for the field of fractions $k[[t_1, t_2]]$, usually denoted by $k((t_1, t_2))$, does not coincide with the iterated field $k((t_1))((t_2))$. Thus, the question of knowing whether $k((t_1, \dots, t_n))$ is C_{i+n} is still unsolved.

10.2 Diophantine Dimension of p-Adic Fields

Artin's conjecture was that $\alpha(\mathbf{Q}_p) = 2$ for every prime p. One motivation certainly was the Chevalley–Warning Theorem (Theorem 3.4.10), but there is also an old result of Meyer concerning quadratic forms.

Theorem 10.2.1 (Meyer, 1884). *Any indefinite quadratic form in five variables, with rational coefficients, represents zero in* $\mathbf{Q}$.

This result, re-interpreted in 1923 by Hasse in terms of p-adic numbers (see Corollary 9.1.3), strongly suggests the following statement.

Proposition 10.2.2. $\alpha_2(\mathbf{Q}_p) = 2$.

Proof. Since $\mathbf{Q}_p$ has characteristic zero, it is well-known that any quadratic form can be written in diagonal form. Hence, it suffices to see that any quadratic form in five variables

$$F(X_1, \dots, X_5) = \sum_{j=1}^{5} a_j X_j^2$$

represents zero non-trivially in $\mathbf{Q}_p$.

We may also assume that the a_j are in $\mathbf{Z}_p$ and are not all multiples of p. Moreover, if one of the a_j is a multiple of p^2, we can make a change of variables and replace X_j by $Y_j = pX_j$ and a_j by $\frac{1}{p^2} a_j$. By such homotheties we reduce to the case in which no a_j is a multiple of p^2. We then separate the a_j into two groups: those that are multiples of p at the first power and the others, which are prime to p. We can then rewrite F as

$$F(X_1, \dots, X_5) = \varphi_0(X_1, \dots, X_r) + p\,\varphi_1(X_{r+1}, \dots, X_5),$$

where φ_0 and φ_1 are primitive diagonal quadratic forms. One of them has at least three variables, for instance, $r \geq 3$.

For $p \neq 2$, it suffices to see that φ_0 represents zero in $\mathbf{Q}_p$, which follows immediately from the Chevalley–Warning Theorem and from Hensel's Lemma (Corollary 8.4.4).

This argument does not work if $p = 2$; for example, it is well-known that the form $X_1^2 + X_2^2 + X_3^2$ does not represent zero non-trivially modulo 4. One can prove the proposition for $\mathbf{Q}_2$, by foregoing the diagonal form and using linear transforms. If we set in the above example $X_1 = Y_1 + X_2 + X_3$, we obtain $Y_1^2 + 2\big((X_2^2 + X_2X_3 + X_3^2) + Y_1(X_2 + X_3)\big)$, which is no longer diagonal, but is approachable by arguments modulo 2 by the usual method (see Proposition 8.3.10). However, the details are quite tedious and a better approach is given by Theorem 10.2.7 (see Exercise 10.5). □

Another result tending to support Artin's conjecture is attributed to Brauer, who showed in 1945 that, for all p-adic fields and for any d we have $\alpha_d(\mathbf{Q}_p) < \infty$.

By 1950, several authors (Dem′yanov, Lewis, Davenport) independently extended Proposition 10.2.2 to forms of degree 3. We introduce first a very useful notation and lemma.

Notation 10.2.3. Let $F(X_1, \dots, X_n)$ be a form of degree 3 with coefficients in $\mathbf{Q}_p$. We denote by a_i the coefficient of X_i^3; we call this a *principal coefficient* of the form F. We denote by a_{ij} the coefficient of $X_i^2 X_j$ (to distinguish it from a_{ji}), and by a_{ijk} the coefficient of $X_i X_j X_k$.

Lemma 10.2.4. *Let $F(X_1, \dots, X_n)$ be a form of degree 3, with coefficients in $\mathbf{Z}_p$, which does not represent zero in $\mathbf{Q}_p$. Then, if p divides a principal coefficient a_i, it also divides a_{ij} for every j.*

Proof. If $p \mid a_1$ and $p \nmid a_{12}$, we choose $x_1 = 1$ and $x_i = 0$ for every $i > 1$. Then, $F(x) = a_1 \equiv 0 \pmod{p}$, whereas $\frac{\partial F}{\partial X_2}(x) = a_{12} \not\equiv 0 \pmod{p}$. This gives a non-trivial solution in $\mathbf{Q}_p^n$, by Hensel's Lemma (Proposition 8.4.1), in contradiction with the hypothesis. □

Corollary 10.2.5 (Springer, 1955). *Let $F(X_1, \ldots, X_n)$ be a form of degree 3 with coefficients in $\mathbf{Q}_p$, without non-trivial zero in $\mathbf{Q}_p^n$. If $x \in \mathbf{Q}_p^n$, we define $\|x\| = |F(x)|_p^{1/3}$. This function $\|\,.\,\|$ is a p-adic norm, i.e., $\|x\| = 0 \iff x = 0$, $\|\lambda\,.\,x\| = |\lambda|_p \cdot \|x\|$, and $\|x + y\| \leq \max\big(\|x\|, \|y\|\big)$ $(\forall\, \lambda \in \mathbf{Q}_p,\ \forall\, x, y \in \mathbf{Q}_p^n)$.*

Proof. It suffices to show that $\|x_1 + x_2\| \leq \max\big(\|x_1\|, \|x_2\|\big)$ for two linearly independent vectors x_1 and x_2. By a change of basis $X = \psi(Y)$ we replace them by $e_1 = (1, 0, \ldots, 0)$ and $e_2 = (0, 1, 0, \ldots, 0)$ respectively. Indeed, if we define $G = F \circ \psi$, the form G does not represent zero in $\mathbf{Q}_p$ and we have: $G(e_i) = F \circ \psi(e_i) = F(x_i)$, where $i = 1, 2$.

It is therefore enough to prove the corollary for $x_i = e_i$; in this case, $F(e_1) = a_1$, $F(e_2) = a_2$, and $F(e_1 + e_2) = a_1 + a_2 + a_{12} + a_{21}$. We may even assume that F has only two variables, since the others are zero. On multiplying by a power of p, we may also assume that the form has integer coprime coefficients. Now, Lemma 10.2.4 implies that if p divides a_1 and a_2, then p divides a_{12} and a_{21}, hence the result. □

Proposition 10.2.6. $\alpha_3(\mathbf{Q}_p) = 2$.

Proof. We give T. A. Springer's proof (1955), which is quite abstract, but is valid without restrictions on p and is also the most concise. We shall actually prove a more precise result, which provides an almost canonical expression for a cubic that does not represent zero in $\mathbf{Q}_p$.

Theorem 10.2.7. *Let $F(X_1, \ldots, X_n)$ be a form of degree 3 with coefficients in $\mathbf{Q}_p$, without non-trivial zero in $\mathbf{Q}_p^n$. Then F is equivalent to a form with coefficients in $\mathbf{Z}_p$:*

$$\varphi_0(X_1, \ldots, X_r) + p\varphi_1(X_1, \ldots, X_n) + p^2\varphi_2(X_1, \ldots, X_n),$$

where $p \nmid a_1, \ldots, a_r$, $p \parallel a_{r+1}, \ldots, a_s$, and $p^2 \parallel a_{s+1}, \ldots, a_n$, where moreover the forms

$$\varphi_0(X_1, \ldots, X_r), \qquad \sigma_1(X_{r+1}, \ldots, X_s) := \varphi_1(0, \ldots, 0, X_{r+1}, \ldots, X_s, 0, \ldots, 0)$$

and

$$\sigma_2(X_{s+1}, \ldots, X_n) := \varphi_2(0, \ldots, 0, X_{s+1}, \ldots, X_n)$$

do not represent zero modulo p.

The notation $p^m \parallel a$ means that $p^m \mid a$ and that $p^{m+1} \nmid a$ (that is: $v_p(a) = m$). This theorem immediately implies that $\mathbf{Q}_p$ is $C_2(3)$. Indeed, since finite fields are C_1, the forms φ_0, σ_1 and σ_2 each have at most three variables. □

Proof (Proof of Theorem 10.2.7). For every $i \in \mathbf{Z}$, we define

$$M_i = \left\{ x \in \mathbf{Q}_p^n \mid v_p\big(F(x)\big) \geq i \right\}.$$

By Corollary 10.2.5, these are $\mathbf{Z}_p$-modules, and of course $M_0 \supset M_1 \supset M_2 \supset M_3 = pM_0$. We set $E = M_0/M_3$ and $E_i = M_i/M_{i+1}$; these are vector spaces over $\mathbf{F}_p$.

Since $\mathbf{Q}_p$ is complete, $\dim_{\mathbf{F}_p} E = n$. This is a general result in commutative algebra (*Nakayama's Lemma*), in a version that is proved somewhat like Proposition 8.3.2: if $\left\{\tilde{b}_1, \ldots, \tilde{b}_m\right\}$ is a basis of E over $\mathbf{F}_p$, we choose representatives $b_i \in M_0$; then, if $x \in M_0$, we can write the class $\tilde{x}$ in E as $\tilde{x} = \sum \tilde{\lambda}_i \tilde{b}_i$ with $\lambda_i \in \mathbf{Z}_p$. Then, $x - \sum \lambda_i b_i \in M_3 = pM_0$; hence, $x - \sum \lambda_i b_i = py$ with $y \in M_0$, and so on, by induction (since Cauchy sequences are convergent). This shows that every element $x \in M_0$ is a linear combination with coefficients in $\mathbf{Z}_p$ of m elements; hence, $m \geq n$. On the other hand, it is clear that $m \leq n$. Moreover, it is easy to see that $\sum_{i=0}^{2} \dim_{\mathbf{F}_p} E_i = n$. Take a basis $\{\bar{e}_1, \ldots, \bar{e}_r\}$ of E_0, $\{\bar{e}_{r+1}, \ldots, \bar{e}_s\}$ of E_1, $\{\bar{e}_{s+1}, \ldots, \bar{e}_n\}$ of E_2, and choose representatives $\{e_1, \ldots, e_n\}$ such that

$$\{e_1, \ldots, e_r\} \subset M_0, \quad \{e_{r+1}, \ldots, e_s\} \subset M_1, \quad \{e_{s+1}, \ldots, e_n\} \subset M_2.$$

Obviously, $\{e_1, \ldots, e_n\}$ is a basis of $\mathbf{Q}_p^n$ and any vector $x \in \mathbf{Q}_p^n$ can be written as $x = \sum \xi_i e_i$ with $\xi_i \in \mathbf{Q}_p$. The form F estimated at x is therefore

$$F(x) = \sum_{i \leq j \leq k} \gamma_{ijk}\, \xi_i\, \xi_j\, \xi_k, \qquad \text{with} \qquad \gamma_{ijk} \in \mathbf{Q}_p.$$

Define

$$\sigma_0(x) = \varphi_0(x) = \sum_{i \leq j \leq k \leq r} \gamma_{ijk}\, \xi_i\, \xi_j\, \xi_k,$$

$$\sigma_1(x) = \frac{1}{p} \sum_{r < i \leq j \leq k \leq s} \gamma_{ijk}\, \xi_i\, \xi_j\, \xi_k \quad \text{and} \quad \sigma_2(x) = \frac{1}{p^2} \sum_{s < i \leq j \leq k} \gamma_{ijk}\, \xi_i\, \xi_j\, \xi_k.$$

Then, $F = \varphi_0 + p\sigma_1 + p^2\sigma_2 + \tau$, where τ contains only crossed terms, i.e., terms that mix the variables of the three groups.

The principal coefficients $a_j = \frac{\gamma_{jjj}}{p^i}$ of the σ_i are units, by definition of the M_i, since $a_j = \frac{1}{p^i} F(e_j)$. Then, the σ_i and F necessarily have integer coefficients (this is an easy consequence of Lemma 10.2.4 and of Exercise 10.4). We finally verify that the σ_i do not represent zero modulo p. Indeed, if $\sigma_i(x) \equiv 0 \pmod{p}$, where

$x = \sum \xi_j e_j$, we may clearly assume that $x \in M_i$. Hence, $F(x) = p^i \sigma_i(x) \equiv 0 \pmod{p^{i+1}}$. This implies that $x \in M_{i+1}$, and hence that all the ξ_j are congruent to zero modulo p, since the $\bar{e}_j$ form a basis of E_i.

Exercise 10.4 also shows that all the coefficients of τ are multiples of p. A good way of grouping terms consists in writing $\tau = p\,\tau_1 + p^2\,\tau_2$ and defining $\varphi_1 = \sigma_1 + \tau_1$ and $\varphi_2 = \sigma_2 + \tau_2$. □

Remark 10.2.8. This proof generalizes easily to algebraic extensions of $\mathbf{Q}_p$. It even applies to every field K, complete with respect to a discrete valuation v with residue field $k = \mathcal{O}_v/\mathfrak{p}_v$, where $\mathcal{O}_v$ is the valuation ring (see Definition 8.1.7) and $\mathfrak{p}_v$ its unique maximal ideal. It shows that if k is $C_i(3)$, then K is $C_{i+1}(3)$.

In 1956, Dem′yanov also showed that two quadratic forms in nine variables have a non-trivial common zero in $\mathbf{Q}_p^9$. But the most striking result was found in 1964 by J. Ax and S. Kochen.

Theorem 10.2.9 (Ax & Kochen, 1964). *For each degree $d \geq 2$, there is a* finite *set $\mathcal{S}_d$ of exceptional primes such that, for any $p \notin \mathcal{S}_d$, the field $\mathbf{Q}_p$ is $C_2(d)$; in other words, $\alpha_d(\mathbf{Q}_p) = 2$ $\forall\, p \notin \mathcal{S}_d$.*

This theorem had a great impact: even if it did not establish Artin's conjecture to any degree, it stated, however, that his conjecture is *almost true*; on the other hand, its proof used *methods of logic*, which were unfamiliar to arithmeticians. It is a non-constructive argument that tells nothing about these exceptional primes.

Scholion 10.2.10. It is not possible to present this proof here, as it is very long and uses concepts that we have not introduced. However, we shall try to give the reader an idea, because it also relies on results that we have mentioned or proved.

The first idea in the proof of Ax and Kochen was to reduce considerations to Lang's result, according to which the field of formal series $\mathbf{F}_p((t))$ has the property C_2 (see Solution 10.1.10). In fact, $\mathbf{Q}_p$ and $\mathbf{F}_p((t))$ are two complete fields with respect to a discrete valuation, and they have the same residue field $\mathbf{Z}_p/(p) = \mathbf{F}_p[[t]]/(t) = \mathbf{F}_p$. Lang had succeeded in proving that $\mathbf{F}_p((t))$ is C_2, but had failed for $\mathbf{Q}_p$.

As we cannot directly compare $\mathbf{Q}_p$ and $\mathbf{F}_p((t))$, since they do not have the same characteristic, we construct two fields, which are quotients of the product of *all* the $\mathbf{Q}_p$ respectively of all the $\mathbf{F}_p((t))$. Both of these fields have the characteristic zero, and one can hope to prove that they are isomorphic. We first explain the construction of these *ultrafields*.

Let $E = \{2, 3, 5, \ldots\}$ be the set of primes. Recall that a *filter* on E is a non-empty family $\mathfrak{F} \subset \mathcal{P}(E)$ of subsets of E,[1] which satisfies the two conditions:

(i) $X, Y \in \mathfrak{F} \implies X \cap Y \in \mathfrak{F}$,
(ii) $X \in \mathfrak{F}$ and $Y \supset X \implies Y \in \mathfrak{F}$.

[1] As for rings, where we accept (1) as an ideal, we accept the case when $\emptyset \in \mathfrak{F}$. In this case, $\mathfrak{F} = \mathcal{P}(E)$; we call it the *zero filter* and use $[\emptyset]$ to denote it.

An *ultrafilter* on E is a maximal filter in the set of filters different from the zero filter, ordered by inclusion. One easily shows, by Zorn's Lemma, that any filter different from $[\emptyset]$ is contained in at least one ultrafilter. Moreover, ultrafilters $\mathfrak{U}$ are characterized in the set of filters $\mathfrak{F} \neq [\emptyset]$ by the property that $X \notin \mathfrak{U} \implies E \setminus X \in \mathfrak{U}$. An important example is *Fréchet's filter* of *cofinite* subsets: $X \in \mathfrak{F} \iff |E \setminus X| < \infty$. The above characterization shows that this is not an ultrafilter (since E is infinite). Note that the only explicitly known ultrafilters are the *principal ultrafilters* $\mathfrak{U}_p = [\,p] = \{X \ni p\}$, where $p \in E$, and Fréchet's filter is not contained in any of them.

Now, if we have a family of fields K_p, indexed by $p \in E$, the Cartesian product $\prod_{p\in E} K_p$ has a natural ring structure, but is not a field, since there are zero divisors. However, if in addition we have an ultrafilter $\mathfrak{U}$ on $\mathcal{P}(E)$, we obtain a field by considering $\prod_{p\in E} K_p/\mathfrak{U}$, the quotient of $\prod_{p\in E} K_p$ by the equivalence relation defined by $(s_p) \sim (t_p) \iff \left\{\, p \in E \mid s_p = t_p \right\} \in \mathfrak{U}$. Indeed, if a class $s = [(s_p)]$ is not zero, it means that the set $S_0 = \left\{\, p \in E \mid s_p = 0 \right\} \notin \mathfrak{U}$. Since $\mathfrak{U}$ is an ultrafilter, this implies that $S_1 = \left\{\, p \in E \mid s_p \neq 0 \right\} = E \setminus S_0 \in \mathfrak{U}$. All elements of the form (t_p), where $t_p = s_p^{-1}$ if $s_p \neq 0$ and t_p is any element of K_p if $s_p = 0$, are equivalent, since the set of $p \in E$ on which they coincide contains $S_1 \in \mathfrak{U}$. Their class $t = [(t_p)]$ is the inverse of s, since $\left\{\, p \in E \mid s_p \,.\, t_p = 1 \right\}$ is equal to $S_1 \in \mathfrak{U}$.

Principal ultrafilters are of no interest (Exercise 10.6), we see that we have obtained – for each non-principal ultrafilter $\mathfrak{U}$ – two ultrafields: $\mathcal{Q}_\mathfrak{U} = \prod_{p\in E} \mathbf{Q}_p/\mathfrak{U}$ and $\mathcal{S}_\mathfrak{U} = \prod_{p\in E} \mathbf{F}_p((t))/\mathfrak{U}$. Both have characteristic zero, but more importantly, they are both complete with respect to a valuation (in a more general sense than in Definition 8.1.7) and they have the same residue field $\prod_{p\in E} \mathbf{F}_p/\mathfrak{U}$. They also have some additional properties in common, which allows one to show that they are actually isomorphic. This is a non-trivial algebraic result.

It is easy to see that $\mathcal{S}_\mathfrak{U}$ has the property C_2, since all $\mathbf{F}_p((t))$ are C_2. The field $\mathcal{Q}_\mathfrak{U}$ is therefore also C_2. To go back down to the fields $\mathbf{Q}_p$, one has to analyze the logical statements that express the property C_2 for a field. At this point, it is necessary to fix a degree d. Indeed, we cannot express the property C_2 in the language of first-order logic, but we can express the property $C_2(d)$ for each fixed d.

Since for every non-principal ultrafilter $\mathfrak{U}$, $\mathcal{Q}_\mathfrak{U}$ is $C_2(d)$, a *theorem of Łoś* allows one to deduce that

$$E \setminus \mathcal{S}_d = \left\{\, p \in E \mid \ \mathbf{Q}_p \text{ est } C_2(d) \right\} \in \mathfrak{U}.$$

It is then easy to see that $\mathcal{S}_d$ is finite.

Indeed, if the set $\mathcal{S}_d$ were infinite, it would have a non-empty intersection with each cofinite set. Hence, we could adjoin $\mathcal{S}_d$ to Fréchet's filter, to generate a filter $\mathfrak{G} \neq [\emptyset]$ finer than Fréchet's filter and such that $\mathcal{S}_d \in \mathfrak{G}$. Hence, there would also exist an ultrafilter $\mathfrak{U}$ containing $\mathfrak{G}$. Since Fréchet's filter is not contained in any principal ultrafilter, $\mathfrak{U}$ would be non-principal and, by Łoś's Theorem, it should contain $E \setminus \mathcal{S}_d$, which is impossible, since $\mathcal{S}_d \in \mathfrak{G} \subset \mathfrak{U}$. □

In 1969, Paul Cohen succeeded in completing the formulation of this theorem, specifying that the set $\mathcal{S}_d$ is given by a *primitive recursive* function. Unfortunately,

this statement still does not say anything that would permit the set of exceptional primes to be determined effectively.

At that time it was known that $\mathcal{S}_2 = \mathcal{S}_3 = \emptyset$ (Propositions 10.2.2 and 10.2.6) and that $\mathcal{S}_4 \supset \{2\}$, since Terjanian's example, mentioned above (Exercise 8.11), had been discovered in 1966. This example showed that $\mathbf{Q}_2$ is not C_2. It was immediately followed by other examples over $\mathbf{Q}_p$ for every prime p, in particular by Schanuel, then by Browkin, who even showed that $\alpha(\mathbf{Q}_p) \geq 3$, which means that $\mathbf{Q}_p$ is not more than C_3.

One could have conjectured that $\alpha(\mathbf{Q}_p) = 3$, but in 1981 Arkhipov and Karatsuba showed in a very unexpected manner that $\alpha(\mathbf{Q}_p) = +\infty$, which means that for any p, the field $\mathbf{Q}_p$ is not C_i for any integer i. We study this proof in the next section.

It is surprising to think that a statement could be *almost true* and also completely false at the same time! Yet it must be said that the first results were aimed rather at showing that the p-adic fields are C_2 for forms of low degree; principally for $d = 5$, 7 ou 11: Birch & Lewis (1962), then Laxton & Lewis (1965), whereas Arkhipov and Karatsuba let the degree be free to infinity.

Much later, Leep & Yeomans (1996) resumed the degree 5 case and showed that $\alpha_5(\mathbf{Q}_p) = 2$ for every $p \geq 47$. This result was recently improved by Heath-Brown (2010), who showed that $\alpha_5(\mathbf{Q}_p) = 2$ for all $p \geq 17$. In other words, we have: $\mathcal{S}_5 \subset \{2, 3, 5, 7, 11, 13\}$.

It must be added that, in all known counter-examples, the degree is not a prime number. Therefore, one can reasonably ask whether the set $\mathcal{S}_d$ is always empty when d is a prime number. More generally, is $\mathcal{S}_d = \emptyset$ for every odd degree d? Or else: does $p \in \mathcal{S}_d$ only if d is a multiple of $p - 1$? None of these questions has been solved so far.

10.3 The Result of Arkhipov and Karatsuba

The result obtained in 1981 by Arkhipov and Karatsuba, namely that the Diophantine dimension of p-adic fields is infinite, is astonishing in more than one aspect:

(1) Ax and Kochen had proved that Artin's conjecture is *almost true*.
(2) No example with $\alpha(\mathbf{Q}_p) > 3$ had ever been constructed.
(3) Arkhipov and Karatsuba's proof is extraordinarily simple.
(4) They prove an even stronger result, namely:

$$\sup \frac{\alpha_d(\mathbf{Q}_p)}{d/(\log d)^3} = +\infty. \tag{10.3.1}$$

(*sup*, not *lim*, because we could have, for example, $\alpha_d(\mathbf{Q}_p) = 2$ for all primes d.)

(5) This result was strengthened even more, from an asymptotic point of view.

The principal idea of Arkhipov and Karatsuba is very simple to present: instead of exhibiting a form in n variables with $n > d^2$, one assumes that $\mathbf{Q}_p$ is C_i and tries to contradict Nagata's statement (Proposition 10.1.9), for a well-chosen system of forms, which is simpler to study! In fact, these are simply symmetric functions, "sums of powers". Here is the statement for $p = 2$.

Lemma 10.3.1 (Arkhipov & Karatsuba). *For $r \geq \frac{d}{4}$, consider a set of positive integers $j_1, \dots, j_r$ such that*

$$0 < j_1 < j_2 < \cdots < j_r \leq \frac{d}{2} \tag{10.3.2}$$

and the system of equations (over $\mathbf{Q}_2$):

$$\begin{cases} S_{2j_1} = X_1^{2j_1} + \cdots + X_n^{2j_1} = 0 \\ \quad \vdots \\ S_{2j_r} = X_1^{2j_r} + \cdots + X_n^{2j_r} = 0. \end{cases} \tag{10.3.3}$$

If this system has a non-trivial zero in $\mathbf{Q}_2^n$, then

$$n \geq \exp_2\Big(\frac{3d}{8(\log_2 d + 2)}\Big). \tag{10.3.4}$$

Remark 10.3.2. To simplify the formulation, we denote by $\exp_b$ the exponential function inverse of $\log_b$, defined by $\exp_b(x) = b^x$. For $p \neq 2$, 2 has to be replaced by $p - 1$ almost everywhere in the statement and the final estimate becomes: $n \geq \exp_p\Big(\frac{d}{4p(\log_p d+1)}\Big)$.

We cannot apply Proposition 10.1.9 directly, because not all S_j have the same degree. However, a very simple trick allows one to consider only this situation, in order to show that $\mathbf{Q}_2$ is not C_i for any value of i.

Corollary 10.3.3 (Arkhipov & Karatsuba). $\alpha(\mathbf{Q}_2) = +\infty$.

Proof. For $d = 4r$, we consider the system of r equations (over $\mathbf{Q}_2$):

$$\begin{cases} F_1(X_1, \dots, X_n) = S_0 \cdot S_d = 0 \\ F_2(X_1, \dots, X_n) = S_2 \cdot S_{d-2} = 0 \\ \qquad\qquad \vdots \\ F_r(X_1, \dots, X_n) = S_{2r-2} \cdot S_{2r+2} = 0. \end{cases} \tag{10.3.5}$$

If we suppose that $\mathbf{Q}_2$ is C_i, Proposition 10.1.9 applies for all $n > r\,d^i = \frac{1}{4}\,d^{i+1}$. We deduce that there are positive integers[2] $j_1, \ldots, j_r$ verifying (10.3.2) and such that the equations of system (10.3.3) have a non-trivial common zero in $\mathbf{Q}_2^n$. Lemma 10.3.1 then entails that $\frac{1}{4}\,d^{i+1} + 1 \geq \exp_2\left(\frac{3d}{8(\log_2 d+2)}\right)$ and it suffices to choose d large enough to obtain a contradiction. □

Remark 10.3.4. We do not immediately obtain statement (10.3.1) with this reductio ad absurdum argument. Indeed, we have applied Proposition 10.1.9 assuming that $\mathbf{Q}_p$ is C_i for all degrees. But then we showed precisely that this hypothesis is not valid. To obtain formula (10.3.1), the proof is roughly the same, but slightly more technical, in order to better control the degrees. This is what Arkhipov and Karatsuba did.

Actually, many improvements of the asymptotic estimates have been suggested since the original paper by Arkhipov and Karatsuba, in particular by Lewis & Montgomery, by Brownawell, and by Browkin.

Lemma 10.3.5. *For every $m \in \mathbf{N}^*$, we have: $v_2(5^m - 1) = v_2(m) + 2$.*

Proof. Since $5^2 \equiv 1 \pmod 8$, if m is odd, $5^m \equiv 5 \pmod 8$; hence, $5^m = 5 + 8\lambda$ with $\lambda \in \mathbf{Z}$ and so $v_2(5^m - 1) = v_2(4 + 8\lambda) = 2$.

If $m = 2m'$ is even, then $v_2(5^{m'} + 1) = 1$ and we may assume by induction that $v_2(5^{m'} - 1) = v_2(m') + 2$. Hence: $v_2(5^m - 1) = v_2(5^{m'} + 1) + v_2(5^{m'} - 1) = 1 + v_2(m') + 2 = v_2(m) + 2$. □

Corollary 10.3.6. *The multiplicative group of units of the ring $\mathbf{Z}/(2^d)$ is generated by -1 and 5.*

Proof. The order of the group is 2^{d-1}; we may assume that $d \geq 3$. If $m = 2^{d-3}$, we have: $v_2(5^m - 1) = v_2(m) + 2 = d - 1$; hence, $5^m - 1 \not\equiv 0 \pmod{2^d}$, whereas $5^{2m} \equiv 1 \pmod{2^d}$. Therefore, 5 is an element of order 2^{d-2}. The subgroup it generates does not contain -1, since the powers of 5 are congruent to $+1$ modulo 4. □

Proof of Lemma 10.3.1. Rather than solving equations (10.3.3), we look for the primitive solutions of the system of congruences

$$\begin{cases} x_1^{2j_1} + \cdots + x_n^{2j_1} \equiv 0 \pmod{2^{2j_1}} \\ \vdots \\ x_1^{2j_r} + \cdots + x_n^{2j_r} \equiv 0 \pmod{2^{2j_r}}, \end{cases} \tag{10.3.6}$$

[2] $j_1 > 0$, for $S_0 = n$.

that is, with $x_\ell \in \mathbf{Z}$ and such that there exists ℓ with $x_\ell \not\equiv 0 \pmod 2$ (see Corollary 8.3.8). Now, even x_ℓ do not matter; thus, we can also ask for all x_ℓ to be odd.

With this condition, we immediately see that n cannot be odd. Therefore, we shall look for the largest power of 2 dividing n. Hence, in order to prove (10.3.4), we shall prove:

$$v_2(n) \geq \frac{3d}{8(\log_2 d + 2)}. \tag{10.3.7}$$

Corollary 10.3.6 allows us to write $x_\ell = \pm 5^{\lambda_\ell}$ with $\lambda_\ell \in \mathbf{N}$. Defining $f(t) = t^{\lambda_1} + \cdots + t^{\lambda_r}$, the system (10.3.6) can be written as

$$\begin{cases} f(5^{2j_1}) \equiv 0 \pmod{2^{2j_1}} \\ \vdots \\ f(5^{2j_r}) \equiv 0 \pmod{2^{2j_r}}. \end{cases} \tag{10.3.8}$$

Also, note that $f(1) = n$.

By Euclidean division, we find a decomposition

$$f(t) = g(t)(t-5^{2j_1})\ldots(t-5^{2j_r}) + a_{r-1}(t-5^{2j_2})\ldots(t-5^{2j_r}) + \cdots + a_1(t-5^{2j_r}) + a_0,$$

with $g(t) \in \mathbf{Z}[t]$ and $a_\ell \in \mathbf{Z}$. We shall show that each term has valuation $\geq \frac{3d}{8(\log_2 d+2)}$. For this, we set:

$$s_0 = \left[\frac{r}{2(\log_2 d + 2)}\right], \quad \text{then} \quad \ell = r - s_0 \geq \frac{3r}{4}.$$

We first calculate $v_2(a_s)$ for $0 \leq s \leq s_0$. In this case, we have:

$$j_{r-s} \geq r - s \geq r - s_0 = \ell;$$

hence, $a_0 = f(5^{2j_r}) \equiv 0 \pmod{2^{2\ell}}$ and so $v_2(a_0) \geq 2\ell$. Lemma 10.3.5 also shows that

$$v_2(5^{2j_{r-1}} - 5^{2j_r}) = v_2(1 - 5^{2j_r - 2j_{r-1}}) = v_2(2j_r - 2j_{r-1}) + 2 \leq \log_2 d + 2$$

and, since $f(5^{2j_{r-1}}) \equiv a_1(5^{2j_{r-1}} - 5^{2j_r}) \equiv 0 \pmod{2^{2\ell}}$, we have:

$$v_2(a_1) \geq 2\ell - (\log_2 d + 2).$$

We shall show by induction that

$$v_2(a_s) \geq 2\ell - s(\log_2 d + 2). \tag{10.3.9}$$

We assume that $v_2(a_\nu) \geq 2\ell - \nu(\log_2 d + 2)$ for all $\nu < s$. Then, the relation

$$f(5^{2j_{r-s}}) = \sum_{\nu=1}^{s} a_\nu (5^{2j_{r-s}} - 5^{2j_{r-\nu+1}}) \dots (5^{2j_{r-s}} - 5^{2j_r}) + a_0 \equiv 0 \pmod{2^{2\ell}}$$

entails:

$$\begin{aligned} &v_2\big(a_s(5^{2j_{r-s}} - 5^{2j_{r-s+1}}) \dots (5^{2j_{r-s}} - 5^{2j_r})\big) \\ &\quad \geq \min_{\nu=1}^{s-1} \big(v_2(f(5^{2j_{r-s}})), v_2(a_0), v_2(a_\nu(5^{2j_{r-s}} - 5^{2j_{r-\nu+1}}) \dots (5^{2j_{r-s}} - 5^{2j_r}))\big). \end{aligned}$$

Fix ν achieving the minimum. Then:

$$\begin{aligned} &v_2\big(a_s(5^{2j_{r-s}} - 5^{2j_{r-s+1}}) \dots (5^{2j_{r-s}} - 5^{2j_{r-\nu}})(5^{2j_{r-s}} - 5^{2j_{r-\nu+1}}) \dots (5^{2j_{r-s}} - 5^{2j_r})\big) \\ &\quad \geq \min\big(2\ell, 2\ell - \nu(\log_2 d + 2) + v_2\big((5^{2j_{r-s}} - 5^{2j_{r-\nu+1}}) \dots (5^{2j_{r-s}} - 5^{2j_r})\big)\big); \end{aligned}$$

hence,

$$v_2\big(a_s(5^{2j_{r-s}} - 5^{2j_{r-s+1}}) \dots (5^{2j_{r-s}} - 5^{2j_{r-\nu}})\big) \geq 2\ell - \nu(\log_2 d + 2)$$

and, applying again Lemma 10.3.5:

$$v_2\big(a_s\big) \geq 2\ell - s(\log_2 d + 2).$$

This is formula (10.3.9). From this we deduce:

$$v_2(a_s) \geq 2\ell - s_0(\log_2 d + 2) \geq \frac{3r}{2} - \frac{r}{2} = r.$$

Finally, if $s > s_0$, we have:

$$\begin{aligned} v_2\big((1 - 5^{2j_r}) \dots (1 - 5^{2j_{r-s+1}})\big) &= v_2(2j_r) + \dots + v_2(2j_{r-s+1}) + 2s \\ &\geq 3s \geq 3(s_0 + 1) > \frac{3r}{2(\log_2 d + 2)}. \end{aligned}$$

Consequently,

$$v_2(n) = v_2(f(1)) \geq \min(r, \frac{3r}{2(\log_2 d + 2)}) \geq \frac{3d}{8(\log_2 d + 2)}. \qquad \square$$

As indicated above, the result of Arkhipov and Karatsuba was refined by several authors. In his 2007 thesis, still unpublished, Nicolas Bartholdi was very interested in the degree of polynomials in a large number of variables that do not represent zero non-trivially in $\mathbf{Q}_p$. He examined in a very detailed manner the construction of examples, which led to substantial quantitative improvements. As an example, among his theorems, we point out the following.

Theorem 10.3.7. *If $d = 8 \cdot (p-1)$ with $p \geq 47$, then $\alpha_d(\mathbf{Q}_p) > 2$.*

The interest of this result is that it provides counter-examples to Artin's conjecture, in fairly low degrees. Previously, no example in degree lower than $p(p-1)$ was known. Moreover, the constructions are very explicit. This thesis ([B]), also contains results of an asymptotic nature, such as the following one, which applies to *all* even degrees.

Theorem 10.3.8. *For every even degree, there is a form of degree d in n variables, without a non-trivial zero in $\mathbf{Q}_2^n$, with $n \geq \exp(\frac{1}{32} \cdot d^{2/3})$.*

This means in particular that – if we restrict to even degrees – the supremum in Relation (10.3.1) can be replaced by a limit:

$$\lim_{\substack{d \text{ pair} \\ d \to \infty}} \alpha_d(\mathbf{Q}_2) = +\infty.$$

This is only a selection of two results, as the thesis treats many other cases. The proofs combine the methods of Terjanian and those of Arkhipov and Karatsuba, introducing different subtle improvements.

Exercises

10.1. Show that one can also define the Diophantine dimension $\alpha_d(k)$ as the maximum of the i for which there is a form of degree d in $n = d^i$ variables without non-trivial zero in k^n.

10.2. Give another proof of Proposition 10.1.7, using the method in the proof of Theorem 10.1.4.

10.3. Show that the proof we have given for Proposition 10.1.9 is also valid if one replaces the word "form" by "polynomial without constant term".

Verify that the other results in that section are also valid for the *property* C_i', which is expressed like the property C_i, replacing forms by polynomials without constant term.

10.4. Let $F(X_1, \ldots, X_n)$ be a form of degree 3 with coefficients in $\mathbf{Z}_p$, which does not represent zero in $\mathbf{Q}_p$. Show that, if p divides a principal coefficient a_i, it divides not only a_{ij} (Lemma 10.2.4), but also a_{ji} and a_{ijk} for all j and all k.

10.5. Prove Proposition 10.2.2 for every characteristic, using T. A. Springer's method (Theorem 10.2.7).

10.6. Show that $\prod_{p\in E} K_p/\mathfrak{U}$ is isomorphic to K_p, if $\mathfrak{U}$ is the principal ultrafilter $\mathfrak{U}_p = [\,p]$.

Solutions to the Exercises

Only some of the exercises are completely solved, sometimes with additional comments. In general, we merely give hints, intended to simplify the resolution.

1.2. For $t \in \mathbf{Q}$, the line with equation $y = t\,(1+x)$ passes through the point $(-1, 0)$. Its intersection with the ellipse with equation $x^2 + 3y^2 = 1$ is computed as follows:

$$3t^2(1+x)^2 = 3y^2 = 1 - x^2 = (1-x)(1+x).$$

If $x \neq -1$, we can simplify to $3t^2(1+x) = 1 - x$, hence:

$$(x, y) = \Big(\frac{1-3t^2}{1+3t^2}, \frac{2t}{1+3t^2}\Big).$$

For instance, if $t = \frac{1}{2}$ we find $(x, y) = (\frac{1}{7}, \frac{4}{7})$.

1.4. The equation of the tangent is $b^2x + a^2y = a^3 - b^3$ (see Definition 5.5.7).

1.5. If $P = (x, y, z)$, the line through S and P meets the plane $x = 0$ at the point $\big(\frac{y}{1+x}, \frac{z}{1+x}\big)$. The stereographic projection on this plane can therefore be written in coordinates as $\varphi : (x, y, z) \mapsto (Y, Z) = \big(\frac{y}{1+x}, \frac{z}{1+x}\big)$. Conversely, we retrieve the corresponding point on the quadric Q by solving the equation $x^2 + 3(1+x)^2(Y^2 - Z^2) = 1$; hence, $x = \frac{1-3(Y^2-Z^2)}{1+3(Y^2-Z^2)}$, $y = \frac{2Y}{1+3(Y^2-Z^2)}$ and $z = \frac{2Z}{1+3(Y^2-Z^2)}$. For example, if $Y = \frac{1}{2}$ and $Z = \frac{1}{3}$, we obtain $(x, y, z) = (\frac{7}{17}, \frac{12}{17}, \frac{8}{17})$.

The map φ is not defined if $x = -1$. In fact, the intersection of the tangent plane at S with the quadric Q consists of two lines, namely $y = \pm z$. Of course, the lines have rational points, but these are not visible in the image of Q by the stereographic projection. Nor is the inverse map defined if $1 + 3(Y^2 - Z^2) = 0$, for instance, for $Y = \frac{1}{3}$ and $Z = \frac{2}{3}$. In a projective setting (see Example 5.5.6), these values correspond to points at infinity on the quadric Q.

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7

2.1. Let $\alpha \in L$ and $f \in K[X]$ be the minimal polynomial of α. Show first that the coefficients of f belong to a *finite* algebraic extension of k.

2.2. Calculate $1/\alpha$.

2.3. Introduce the ring $A = k[\alpha]$ of polynomial expressions of the form $a_0 + a_1\alpha + \cdots + a_m\alpha^m \in K$ with $m \in \mathbf{N}$ and, for all i, $a_i \in k$.

2.4. The equation of the tangent plane to the sphere S is $X_3 - 1 = 0$. Its intersection with S is the set of zeros of the polynomial $X_1^2 + X_2^2 = (X_1 - iX_2)(X_1 + iX_2)$, located in this plane. It therefore consists of two complex conjugate lines, meeting at a real point.

2.5. A simple diagram shows two irreducible components, $\{(0, 0)\}$ and $\{(-1, -1)\}$, and there is a third one consisting of two complex conjugate points. By Corollary 5.3.4, the ideal $\mathfrak{a}$ cannot be prime, since $V(\mathfrak{a})$ is reducible. But it is also easy to see that $X - Y$ and $X + Y - 1$ are not in $\mathfrak{a}$, whereas their product is.

2.6. A classical statement (over an algebraically closed field k) guarantees that the product of two irreducible subsets of $\mathbf{A}_k^n$ is still irreducible. The present example shows that this statement is not valid if k is not algebraically closed.

2.8. The relation $\mathfrak{a} \subset I(V(\mathfrak{a}))$ applied to $\mathfrak{a} = I(Y)$ gives $I(Y) \subset I(V(I(Y))) = I(\bar{Y}) \subset I(Y)$; hence, the functorial identity: $I \circ V \circ I = I$. Similarly, $V \circ I \circ V = V$.

2.11. If Y is a subspace of X, its closed sets are of the form $G = \overline{G} \cap Y$, where the closure is considered in X. To show quasi-compactness, one must show that, if a family of closed sets $\{G_i\}$ has empty intersection, it contains a finite sub-family having empty intersection. Take for Σ the set of all finite intersections of elements of the family $\{G_i\}$ and apply Proposition 2.4.4.

2.14. In $\mathbf{A}_k^1 \times \mathbf{A}_k^1$ endowed with the product topology, the only closed sets are finite unions of points and of vertical or horizontal lines.

2.15. Let $\rho = e^{2\pi i/3}$. We can write the equation as

$$(x + y)(x + \rho y)(x + \rho^2 y) = (z + 1)(z + \rho)(z + \rho^2).$$

We find in this way nine lines, each given as an intersection of two affine planes $x + \rho^i y = z + \rho^j = 0$ $(i, j = 0, 1, 2)$. By permuting variables, we can also write the equation as $x^3 - z^3 = 1 - y^3$, which reveals nine other lines, or as $x^3 - 1 = z^3 - y^3$, which identifies nine others. It is easy to prove that these are the only lines. A substantially deeper result (Cayley and Salmon, 1849) is that, in the projective space, *every* smooth cubic surface has exactly 27 lines. This result was one of the main sources of inspiration for the development of algebraic geometry (see Chapter 7).

3.1. Let $f(X) = (X - \alpha)\, g(X)$, where $\alpha \in \bar{k}$; then $f'(\alpha) = g(\alpha)$. Thus, α is a multiple root of $f \iff f(\alpha) = f'(\alpha) = 0 \iff$ *iff* $X - \alpha$ divides the gcd of f and f'. This shows the equivalence of (i) with (ii).

On the other hand, if f is not constant, it is clear that (ii) $\Longrightarrow$ (iii), since the gcd of f and 0 is f. If f is irreducible, we also have (iii) $\Longrightarrow$ (ii) since, if f' is

not identically zero, the gcd of f and f' is a polynomial of degree $\leq n-1$, which divides f.

In characteristic zero, f' cannot be identically zero, but this occurs in characteristic $p > 0$ for polynomials of the form $f(X) = h(X^p)$.

3.2. If $a \in k$, there exists $b \in \bar{k}$ such that $a = b^p$. Let $f \in k[X]$ be the minimal polynomial of b, which is therefore irreducible. The polynomial $X^p - a = (X-b)^p$ is a multiple of f. If k is perfect, f can have only simple roots; then $f(X) = X - b$, and $b \in k$.

Conversely, let $f \in k[X]$ be an irreducible polynomial of degree n. If it does not have n distinct roots in $\bar{k}$, we have $f' = 0$ (by Exercise 3.1). In this case, $f(X) = h(X^p)$; hence, $h(X) = a_0 X^m + \cdots + a_m \in k[X]$. If the coefficients have the form $a_i = b_i^p$ with $b_i \in k$, we can write $f(X) = (b_0 X^m + \cdots + b_m)^p$; hence, f would not be irreducible.

3.3. The map $\varphi : k \to k$, which sends x onto x^p, is injective, and hence also surjective.

3.4. Let $g \in K[X]$ be an irreducible polynomial. Let $\alpha \in \bar{k}$ be a root of g and $f \in k[X]$ the minimal polynomial of α over k. If we consider f as a polynomial in $K[X]$, it vanishes at α and is therefore a multiple of g. But f has only simple roots in $\bar{k}$, hence g also! The converse is trivially false, since the algebraic closure $K = \bar{k}$ is always a perfect field, for any field k.

3.5. If q is even, we have to treat a linear problem, by Exercises 3.3 and 3.2. Thus, we may assume that q is odd, and we must look for the solutions in $\mathbf{F}_q$ of the equation $-a_1 X_1^2 = a_2 X_2^2 + a_3$. When X_1 runs over all the elements of $\mathbf{F}_q$, the left-hand member takes on $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ distinct values. Similarly for the right-hand member, when X_2 runs through the elements of $\mathbf{F}_q$. We obtain in all $q+1$ values, whereas $\mathbf{F}_q$ has only q elements; thus, at least two of them must coincide.

3.6. The unique extension of degree 6 has 2^6 elements. It contains the extensions of degrees 2 and 3. The number of elements that really have degree 6 is therefore $2^6 - 2^2 - 2^3 + 2^1 = 54$ (for one must not subtract the elements of $\mathbf{F}_2$) twice. These 54 elements are distributed among $54/6 = 9$ polynomials of degree 6. Similarly, in the other cases, one finds $(3^2 - 3^1)/2 = 3$ irreducible polynomials of degree 2 and $(5^4 - 5^2)/4 = 150$ irreducible polynomials of degree 4.

3.7. The non-trivial k-embeddings are defined by $\sigma_1 : \alpha \mapsto \rho\alpha$ and $\sigma_2 : \alpha \mapsto \rho^2\alpha$, where $\rho^2 + \rho + 1 = 0$. The computation of $N_{k(\alpha)/k}(X_1 + \alpha X_2 + \alpha^2 X_3)$ is quite simple, since the norm is invariant by $\mathrm{Gal}(\bar{k}/k)$; thus, the terms that could a priori contain α are actually zero. Thus, it is pointless to calculate them. Finally: $N_{k(\alpha)/k}(X_1 + \alpha X_2 + \alpha^2 X_3) = X_1^3 + m X_2^3 + m^2 X_3^3 - 3m X_1 X_2 X_3$.

3.8. There are $[K : \mathbf{Q}] = 4$ embeddings, which send $\sqrt{2}$ onto $\pm\sqrt{2}$ and $\sqrt{3}$ onto $\pm\sqrt{3}$, independently. Hence, $\sigma(K) = K$ for all $\sigma \in \mathrm{Plong}(K/\mathbf{Q})$ and the extension is Galois. $\mathrm{Plong}(K/\mathbf{Q})$ is therefore the *Galois group* $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/2 \times \mathbf{Z}/2$.

3.9. If $a \in F_\infty$, there exists i such that $a \in F(i) = \mathbf{F}_{p^{3^i}}$. Since finite fields are perfect, there exists $b \in F(i)$ such that $a = b^p$. Since $b \in F_\infty$, this field is also perfect. It has extensions of degree 2, but none of degree 3.

3.10. One verifies that the field of fractions of $\mathbf{F}_p[t_1, t_2]$ coincides with the field of fractions of $\mathbf{F}_p(t_1)[t_2]$. Hence, $K = \mathbf{F}_p(t_1)(t_2)$ is an extension of $\mathbf{F}_p(t_1)$ of degree p; thus, $[K : k] = p^2$. On the other hand, every rational fraction $\alpha = \varphi(t_1, t_2) \in K$ (where $\varphi = f/g$, with $f, g \in \mathbf{F}_p[t_1, t_2]$) satisfies the equality $\alpha^p = \varphi(t_1, t_2)^p = \varphi(t_1^p, t_2^p) \in k$, so that α has degree at most p. Therefore, the field K contains no element of degree p^2 and the extension K/k cannot be simple. Finally, for $c \in k$, all the fields $K_c = k(t_1 + ct_2)$ are distinct. Indeed, if $t_1 + c't_2$ belonged to K_c for $c \neq c' \in k$, the field K_c would contain $(t_1 + ct_2) - (t_1 + c't_2) = (c - c')t_2$; hence, also t_2, and hence also t_1. Then we would have $K_c = K$, which is impossible, since K_c/k is a simple extension, whereas K/k is not.

3.12. Fourth powers are congruent to 0 or to 1 modulo 5.

3.13. Use Proposition 3.2.7.

4.1. If f and g are two polynomials in $k[X_0, \ldots, X_n]$ such that $f \notin \mathfrak{p}$ and $g \notin \mathfrak{p}$, we consider their homogenous components: there is a least index i such that $f_i \notin \mathfrak{p}$ and a least index j such that $g_j \notin \mathfrak{p}$. Then, the homogenous component of degree $k = i + j$ of fg is the sum of $f_i\, g_j \notin \mathfrak{p}$ and of other products, all belonging to $\mathfrak{p}$. Since by hypothesis $\mathfrak{p}$ is a homogenous ideal, Lemma 4.1.8 implies that $fg \notin \mathfrak{p}$.

4.3. The condition allows one to write $F = \epsilon(X_1^2 + X_2^2) + X_0\,(a_0X_0 + 2a_1X_1 + 2a_2X_2)$. If $\epsilon = 0$, $V(F)$ is the union of two lines, which may coincide, and $V(F_*)$ is a line in the affine plane, or empty (if $a_1 = a_2 = 0$). If $\epsilon \neq 0$, we can set $\epsilon = 1$ and then $F_* = (X_1 + a_1)^2 + (X_2 + a_2)^2 + (a_0 - a_1^2 - a_2^2)$. If $a_1^2 + a_2^2 > a_0$, $V(F_*)$ is a circle; otherwise, it is the union of two complex conjugate lines (with a single real point), or a complex variety without real points.

4.4. Writing the equation in homogenous form, we find $x_1^4 + x_0^2x_1x_2 - x_2^4 = 0$. The points at infinity are on the line $x_0 = 0$, where they are determined by the zeros of the polynomial $x_1^4 - x_2^4 = (x_1 - x_2)(x_1 + x_2)(x_1^2 + x_2^2)$. These are the points $[0 : 1 : 1]$, $[0 : 1 : -1]$ (corresponding to the two asymptotes at $\pm 45°$ of the curve pictured in Figure 4.2), and $[0 : 1 : \pm i]$.

4.5. We have seen (Remark 4.1.9) that, even in the projective case, closed sets are defined by zeros of polynomials. If a polynomial vanishes on a set, it also vanishes on its closure.

For $f \in I(Y)$ and $y \in Y$, we have: $f^*(\,j(y)) = (\,f^*)_*(y) = f(y) = 0$, using Exercise 4.2(d). Consequently, f^* vanishes on $j(Y)$, and hence also on its closure $\overline{Y}$. This shows that the ideal generated by $\{\,f^* \mid f \in I(Y)\}$ is contained in $I(\overline{Y})$.

Conversely, since $\overline{Y} \supset j(Y)$, we have: $g \in I(\overline{Y}) \implies g(\,j(Y)) = 0 \implies g_* = g \circ j \in I(Y)$ and, by Exercise 4.2(c), $g = X_0^r(g_*)^*$ is the ideal generated by $\{\,f^* \mid f \in I(Y)\}$ (with $f = g_*$).

4.6. We may take $f_1 = X_2 - X_1^2$ and $f_2 = X_3 - X_1^3$. Indeed, the ideal $\mathfrak{a} = (\,f_1, f_2)$ is clearly contained in $I(Y)$, and $Y = V(\mathfrak{a})$. Since the quotient $k[X_1, X_2, X_3]/\mathfrak{a}$

is isomorphic to the integral domain $k[X_1]$, we see that $\mathfrak{a}$ is a prime ideal. Hence, $I(Y) = I(V(\mathfrak{a})) = \mathfrak{a}$ (this follows from Corollary 5.3.4).

But also $X_1X_3 - X_2^2$ is in $I(Y)$, and in fact one verifies that $X_1X_3 - X_2^2 = X_1\, f_2 - (X_2 + X_1^2)\, f_1$. However, f_1^* and f_2^* cannot generate $X_1X_3 - X_2^2$, by simply considering degrees.

Kneser proved in 1960 that every irreducible curve in $\mathbf{P}^3$ has the form $V(\mathfrak{b})$, where the ideal $\mathfrak{b}$ is generated by at most three polynomials. How to know when two polynomials suffice prompted many efforts. (When this is the case, the curve is called a *set-theoretic complete intersection.*)

4.7. The homogenous equation is $X_1X_2X_3 - X_0^3 = 0$; thus, there are three lines in the plane at infinity: $X_0 = X_i = 0$ $(i = 1, 2, 3)$. There are no others, because a line in $\mathbf{A}_k^3$ would have a parametric expression $x_i = a_i + b_i\, t$; hence, $(a_1 + b_1\, t)(a_2 + b_2\, t)(a_3 + b_3\, t) = 1$, to be satisfied identically for all $t \in \bar{k}$. The a_i are not zero, since $a_1a_2a_3 = 1$. Examining the coefficients of highest degree, we then see that the b_i are all zero; thus, the parametrization does not represent a line.

4.8. For clarity, we shall denote by x_i the class of X_i modulo $I(Y)$. If $\frac{1-x_1}{x_2} \in k[Y]$, there exists a polynomial $\alpha \in k[X_1, X_2]$ such that $(1 - x_1)/x_2 = \alpha(x_1, x_2)/1$, i.e., such that $1-x_1 = x_2\alpha(x_1, x_2)$ in $k[Y]$. There then exists a polynomial $\beta \in k[X_1, X_2]$ such that $1-X_1-X_2\alpha(X_1, X_2) = (X_1^2+X_2^2-1)\,\beta(X_1, X_2)$. On substituting $X_2 = 0$ in this polynomial identity, we find $1 - X_1 = (X_1^2 - 1)\,\beta(X_1, 0)$ in $k[X_1]$. And since $k[X_1]$ is an integral domain, we obtain $-1 = (X_1+1)\,\beta(X_1, 0)$; impossible, because $X_1 + 1$ is not a unit.

4.9. The morphism $\varphi : Y \to \mathbf{P}_k^1$ is defined as follows:

$$y = [X_0 : X_1 : X_2 : X_3] \mapsto \begin{cases} [X_0 : X_2] & \text{if } [X_0 : X_2] \neq [0 : 0] \\ [X_1 : X_3] & \text{if } [X_1 : X_3] \neq [0 : 0]. \end{cases}$$

The compatibility condition of these two expressions is satisfied, since $X_0X_3 = X_1X_2$ on Y. Let L_1 be the line $\{X_0 = X_2 = 0\} \subset Y$ and let $U_1 = V \setminus L_1$. If $y \in U_1$ has image $[\lambda_0 : \lambda_1]$, we have: $[X_0 : X_2] = [\lambda_0 : \lambda_1]$ and $\lambda_0X_3 = \lambda_1X_1$. Therefore, the point y lies on the line

$$\ell = \{\lambda_0\, X_2 = \lambda_1\, X_0\} \cap \{\lambda_0\, X_3 = \lambda_1\, X_1\}\,.$$

If $y \in L_1$, it lies in the open set $U_2 = V \setminus L_2$, where L_2 denotes the line $\{X_1 = X_3 = 0\} \subset Y$. Computations are symmetric and we see that ℓ is the fiber of φ over $[\lambda_0 : \lambda_1]$.

The quadric $Y \subset \mathbf{P}_k^3$ therefore contains an infinity of lines: the fibers of the morphism φ. In fact, it contains another infinite family of lines: the fibers of the morphism $\psi : Y \to \mathbf{P}_k^1$ defined as follows:

$$y = [X_0 : X_1 : X_2 : X_3] \mapsto \begin{cases} [X_0 : X_1] & \text{if } [X_0 : X_1] \neq [0 : 0] \\ [X_2 : X_3] & \text{if } [X_2 : X_3] \neq [0 : 0]. \end{cases}$$

The fibers of φ (respectively ψ) are disjoint lines, whereas the lines of the first family meet each line of the second family at one point. We may add that there is a morphism $\mathbf{P}^1_k \times \mathbf{P}^1_k \to Y \subset \mathbf{P}^3_k$ defined by

$$[\lambda_0 : \lambda_1] \times [\mu_0 : \mu_1] \mapsto [X_0 : X_1 : X_2 : X_3] = [\lambda_0\,\mu_0 : \lambda_0\,\mu_1 : \lambda_1\,\mu_0 : \lambda_1\,\mu_1],$$

whose inverse is given by $\varphi \times \psi$. (Checks are local.)

4.10. We must assume that the field k has characteristic neither 2 nor 17. Then φ is defined everywhere on Γ, for $X_0 = X_1 = X_3 = 0 \implies X_2 = 0$. If $X_1 \neq 0$, we have: $X_2 = X_3^2/X_1$ and the map is injective. The image $\varphi(\Gamma)$ is therefore given by the equation $X_1^4 - 17X_3^4 - 2X_0^2X_1^2 = 0$, and all points on this curve have a unique pre-image, except $[X_0 : X_1 : X_3] = [1 : 0 : 0]$, which is the image of two points $[1 : 0 : \pm\sqrt{-2/17} : 0]$. The curve Γ, given by the Equations (9.2.1), appears in Chapter 9 in an arithmetical context (Proposition 9.2.1).

4.11. See Example 3.3.10. This Galois-type argument is very natural. One can also give a purely algebraic proof, which is less intuitive, but has the advantage of working over an arbitrary field and of automatically taking into account all degenerate cases.

4.12. We shall use the formalism in Choudhry's Lemma (Lemma 4.5.1), introducing the quadratic form $Q(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ over $k = \mathbf{Q}$. Given a point P with rational coordinates $x = (x_1, x_2, x_3)$ such that $Q(x) = m \in \mathbf{N}^*$, we choose a point N with integer coordinates $n = (n_1, n_2, n_3)$ as close as possible to P. If we consider the vector $v = x - n$, the distance from N to P is the square root of $Q(v)$, and $Q(v) \leq 3/4$. Since we can assume that P does not already have integer coordinates, we have $0 < Q(v) < 1$.

The residual point of intersection of the line joining N to P with the sphere with equation $Q(x) = m$ is given, on setting $u = x$ in Formula (4.5.1), by $x' = w/Q(v) = x - \frac{B(x,v)}{Q(v)}v$. By (4.5.2), we have $Q(x') = Q(x) = m$ and we have to show, on the one hand, that the line is not tangent, which means that $x' \neq x$, or that $B(x, v) \neq 0$; and on the other hand, that the coordinates of x' have a smaller common denominator than those of x.

For the first point, it suffices to see that $B(x, v) = 0 \implies Q(n) = Q(x) + Q(v)$, which would imply that $Q(v) = Q(n) - m \in \mathbf{Z}$, whereas $0 < Q(v) < 1$.

For the second point, we write $x = y/d$, where $d \in \mathbf{N}^*$ and y is a vector with integer coordinates. Then we can write x' as

$$x' = \frac{Q(v)y - B(y, v)v}{dQ(v)} = \frac{y'}{d'}.$$

Obviously, $d' = dQ(v) < d$; what is less obvious, is that $d' \in \mathbf{Z}$ and that y' is a vector with integer coordinates.

In fact, $d' = dQ(v) = dQ(x - n) = d\big(Q(x) + Q(n)\big) - B(dx, n) = d\big(m + Q(n)\big) - B(y, n) \in \mathbf{Z}$. As for the numerator, we can write $y' = \big(Q(v)y + B(x, n)y\big) - \big(B(y, v)v + B(x, n)y\big)$. The first term has the form cy, where $c = Q(v) + B(x, n) =$

$Q(x-n)+B(x,n)=Q(x)+Q(n)=m+Q(n)\in\mathbf{Z}$. The second term is $B(y,v)v+B(x,n)y=B(y,x-n)v+B(y,n)x=2dQ(x)v+B(y,n)(-v+x)=2md(x-n)+B(y,n)n=2m(y-dn)+B(y,n)n$. This vector also has integer coordinates.

5.1. $\alpha=\frac{1+\sqrt{d}}{2}$ is a root of the polynomial $X^2-X+\frac{1-d}{4}$. Hence, $\alpha\in\mathcal{O}_K$ if $d\equiv 1 \pmod 4$. It suffices to see that there are no other elements in $\mathcal{O}_K$. If $\xi=a+b\sqrt{d}\in K$ is integral over $\mathbf{Z}$ ($a,\ b\in\mathbf{Q}$), it is also algebraic over $\mathbf{Q}$. Since $\mathbf{Z}$ is integrally closed, Proposition 5.1.16 implies that the minimal polynomial of ξ (of degree 1 or 2) has all its coefficients in $\mathbf{Z}$. There remains an easy computation.

5.2. Let $A=k[x,y]/(y^2-f(x))$ be the coordinate ring of the curve. This is a domain, by Lemma 2.4.14 (it follows from the hypothesis that $f(x)$ is not the square of another polynomial). Denote by B its field of fractions. This is a quadratic extension of $K=k(x)$, generated by 1 and $\delta=\sqrt{f}$. If $\xi\in B$ is integral over A, it is also algebraic over K and there is a quadratic relation $\xi^2+c_1(x)\,\xi+c_2(x)=0$, where the $c_i(x)$ are in $k(x)$. As in Proposition 5.1.16, the coefficients of this polynomial are integral over A.

Lemma. *If $c(x)\in k(x)$ is integral over A, then $c(x)\in k[x]$.*

Proof. We can write a relation of integral dependence for $c(x)$ as $c(x)^m+(a_1(x)+\delta b_1(x))\,c(x)^{m-1}+\cdots+(a_m(x)+\delta b_m(x))=0$, where the a_i and the b_i are in $k[x]$. After expansion, the coefficient of δ does not matter. The other term gives a relation $c(x)^m+a_1(x)c(x)^{m-1}+\cdots+a_m(x)=0$, which shows that $c(x)$ is integral over $k[x]$. Since this ring is integrally closed, we deduce that $c(x)\in k[x]$. □

Therefore, in the relation $\xi^2+c_1(x)\,\xi+c_2(x)=0$, the c_i belong to $k[x]$ and, (since k has characteristic $\neq 2$) we can make a change of variables $\xi=\eta-\frac{1}{2}c_1(x)$; hence, a relation of the type $\eta^2=c(x)$ with $c(x)\in k[x]$ and $\eta\in B$. It remains to show that $\eta\in A$.

We can write $\eta=\frac{a(x)+\delta b(x)}{d(x)}$, where a, b, and d are elements of $k[x]$. Squaring, we obtain$(a+\delta b)^2=cd^2$; hence, $a^2+b^2\,f=cd^2$ and $ab=0$. The case $b=0$ corresponds to $\eta=a/d\in k(x)$; hence, $\eta\in k[x]$. And if $a=0$, we find $b^2\,f=cd^2$. Now, $k[x]$ is factorial and by hypothesis f has no multiple roots; hence, d divides b and $\eta=\delta b/d\in A$.

We have given here an *ad hoc* proof for a particular case of a much more general result of commutative algebra: *the coordinate ring of a non-singular curve is integrally closed.* Even more generally: *every smooth variety is normal.*

5.4. Let $b\in\mathfrak{p}$ be a non-zero element; b factors as a product of irreducible elements. Since the ideal $\mathfrak{p}$ is prime, at least one of these elements also belongs to $\mathfrak{p}$. We could have taken $b\in\mathfrak{p}$ as irreducible. In this case, (b) is a prime ideal, because the ring A is factorial. The minimality of $\mathfrak{p}$ implies that $\mathfrak{p}=(b)$.

One shows that the converse is also true: *a Nœtherian integral ring is factorial if and only if every prime ideal of height* 1 *is principal.*

5.5. This follows directly from Exercise 5.4, referring to Proposition 2.4.9 (see Lemma 2.4.14).

5.6. On the quadric $Q \subset \mathbf{P}^3_{\mathbf{Q}}$ with equation $(X_1 + X_2)X_3 - X_0X_1 + 2X_0X_2 = 0$, the projective cubic surface cuts, besides the two conjugate skew lines L_1 and L_2, a curve of degree 4. In the Néron–Severi group of the quadric (see Example 7.7.2), the complete intersection with the cubic surface is a divisor with class $3e + 3f$. If the two given lines are of type e, the residual intersection is a curve Γ of type $e + 3f$. Since the intersection number of this curve with the class f is 1, it follows that Γ is a rational curve (i.e., of genus 0). One verifies that the presented parametrization is correct.

5.7. $0 = x^4 + y^4 + (x + y)^4 - 2 = 2[(x^2 + xy + y^2)^2 - 1]$. The component $V(x^2 + xy + y^2 - 1)$ has a $\mathbf{Q}$-rational point $P = (0, 1)$. The lines passing through this point give the projection of this conic onto a line (see Proposition 4.2.7). On writing $y = 1 - \lambda x$, we find the parametric solution

$$x = \frac{2\lambda - 1}{\lambda^2 - \lambda + 1}, \quad y = 1 - \lambda x, \quad z = x + y.$$

5.8. If $p, q, r \in \mathbf{C}[t]$ are polynomials without common factors, which satisfy the relation

$$p(t)^n + q(t)^n - r(t)^n = 0$$

identically, there is also an identity of derivatives:

$$p(t)^{n-1} \cdot p'(t) + q(t)^{n-1} \cdot q'(t) - r(t)^{n-1} \cdot r'(t) = 0.$$

We can view these two relations as equations in the variables $X = p(t)^{n-1}$, $Y = q(t)^{n-1}$, $Z = -r(t)^{n-1}$ and write them as a system:

$$\begin{cases} pX + qY + rZ = 0 \\ p'X + q'Y + r'Z = 0. \end{cases}$$

Multiplying the first equation by r', the second by r, and subtracting the two expressions, we obtain: $(pr' - rp')X + (qr' - rq')Y = 0$. Similarly, $(pq' - qp')X - (qr' - rq')Z = 0$. If we define $\alpha = qr' - rq'$, we see that X divides αY and αZ. This implies that X divides α, since p, q, and r have no common factor, and this also implies that $\alpha \neq 0$.

We may assume without loss of generality that $d = \deg p$ is the largest of the degrees of p, q, and r. Then, comparing the degrees of X and of α, we find: $(n - 1)\, d \leq \deg q + \deg r - 1 \leq 2d - 1$, a contradiction if $n \geq 3$.

5.10. $2ix_2 = (x_1 + ix_2 - 1)(x_1 - ix_2 + 1)$. The line L with equation $X_1 + i\,X_2 - X_0 = 0$ meets the projective curve at the points $[1 : 1 : 0]$ and $[0 : -i : 1]$. Since the second

point is at infinity, it does not correspond to any maximal ideal of the coordinate ring of the affine curve, which is cut transversely by L at the point $P = (1, 0)$.

This remark applies to any point on the circle. This implies (since $\mathbf{C}$ is algebraically closed) that any prime ideal of height 1 is principal. As we have seen in the solution to Exercise 5.4, this implies that the ring $A = \mathbf{C}[X_1, X_2]/(X_1^2 + X_2^2 - 1)$ is factorial, and even principal (since it is a Dedekind ring).

5.11. $x_2^2 = (1-x_1)(1+x_1)$ implies that $(1-x_1)(1+x_1) \in (x_2)$, but one verifies that $1 - x_1 \notin (x_2)$ and that $1 + x_1 \notin (x_2)$. Indeed, $(1 - x_1) \subset (x_2) \implies V(1 - x_1) \supset V(x_2)$, which is not the case, since $V(1 - x_1)$ is the point $(1, 0)$, whereas $V(x_2)$ is the union of the two points $(1, 0)$ and $(-1, 0)$. (We can also give another argument, using Exercise 4.8.)

The ideal $\mathfrak{m} = (x_2, 1 - x_1) \subset A$ is the maximal ideal of the point $P = (1, 0)$. Assume that it is generated by the class of a polynomial $f \in \mathbf{Q}[X_1, X_2]$. We know (Exercise 5.10), that in the extension $B = \mathbf{C}[X_1, X_2]/(X_1^2 + X_2^2 - 1)$ $\mathfrak{m}$ becomes principal, generated by $x_1 + ix_2 - 1$. Thus, we must have $f(x_1, x_2) = (x_1 + ix_2 - 1)\,\epsilon(x_1, x_2)$, where ϵ is a unit of B, which implies that

$$N_{K/k}(\epsilon) = s \in \mathbf{C}^*,$$

where $k = \mathbf{Q}(x_1)$ and $K = Q(A)$.

On writing $f = a(x_1) + b(x_1)\,x_2$ with $a,\ b \in \mathbf{Q}[x_1]$, we find:

$$N_{K/k}(f) = a^2 - b^2 x_2^2 = a^2 - b^2(1 - x_1^2) \in \mathbf{Q}[x_1].$$

But we also have

$$N_{K/k}(f) = ((x_1 - 1)^2 + x_2^2)\, N_{K/k}(\epsilon) = 2(1 - x_1)\, s;$$

hence, $s \in \mathbf{Q}^*$.

Comparing the two expressions for the norm of f, we obtain: $2(1 - x_1)\, s = a^2 - b^2(1 - x_1^2)$; hence, $1 - x_1 \mid a$. Set $a = (1 - x_1)\, c(x_1)$; then:

$$2s = (1 - x_1)\, c^2 - b^2(1 + x_1).$$

For $x_1 = 1$, we find $2s = -2b(1)^2$; hence, $s < 0$, and for $x_1 = -1$ we find $2s = 2c(-1)^2$, so $s > 0$. But s cannot be both positive and negative at the same time! □

The geometric meaning of this computation is that the two points at infinity on the circle $V(X_1^2 + X_2^2 - 1)$ are not defined separately over $\mathbf{Q}$. The $\mathbf{Q}$-rational functions, which vanish at P, must vanish at least once more at a point on the affine circle. This makes the difference between this ring and the ring in Exercise 5.10.

Therefore, the ring A is not factorial, since, as we have seen in Exercise 5.4, *if the coordinate ring of a variety $V \subset \mathbf{A}_k^n$ is factorial, any codimension 1 subvariety is a complete intersection, which means that its ideal is generated by a single equation.*

Another reason is that the ideal (x_2) is not prime, whereas one can show that the element x_2 is irreducible.

A quite striking example of the behavior of unique factorization under field extensions is the coordinate ring of the circle C with equation $x_1^2 + x_2^2 = 3$. Since $C(\mathbf{Q}) = \emptyset$ and the points at infinity are defined over $\mathbf{Q}(i)$, the coordinate ring $k[X_1, X_2]/(X_1^2 + X_2^2 - 3)$ is factorial for $k = \mathbf{Q}$, not factorial for $k = \mathbf{Q}(\sqrt{3})$, and factorial again for $k = \mathbf{Q}(i, \sqrt{3})$. These examples were found by Samuel.

6.1. $\varphi(1 + \delta) = 13$ and $\varphi(2) = 4$; however, we cannot perform a division with remainder of $1 + \delta$ by 2. Otherwise, we would have $1 + \delta = 2(a + b\delta) + (c + d\delta)$ with $a, b, c, d \in \mathbf{Z}$ and $\varphi(c+d\delta) \leq 3$. In this expression, $1 = 2a+c$ and $1 = 2b+d$ imply that c and d are odd; hence, $c^2 \equiv d^2 \equiv 1 \pmod 8$. Then, $c^2 - 14d^2 \equiv 1 - 14 \equiv 3 \pmod 8$, so $c^2 - 14d^2 = 3$, since $\left|c^2 - 14d^2\right| = \varphi(c+d\delta) \leq 3$. This is impossible, because 3 is not a square modulo 7. (There is also a 3-adic obstruction: see Proposition 9.1.2.)

6.2. The group of units of $\mathcal{O}_K$ is generated by the *fundamental unit* $\epsilon = 15 + 4\delta$. But $\mathcal{O}_K/(2)$ has four elements (Lemma 6.2.3) and this ring contains the classes of 0, 1, δ, and $1 + \delta$, which are distinct. The map $A_1 \to \mathcal{O}_K/(2)$ sends ϵ onto 1 and is multiplicative on $\mathcal{O}_K^*$. Hence, it is not surjective, since its image does not contain the class of δ. Consequently, $2 \notin A_2$; hence, $\psi(2) \geq 3$.

On the other hand, $\mathcal{O}_K/(1+\delta) \cong \mathbf{Z}/(13)$, since $-13 = (1+\delta)(1-\delta)$. The map $A_1 \to \mathcal{O}_K/(1 + \delta)$, identifies δ to -1 and sends ϵ onto $15 - 4 = 11$. One verifies that the class of $11 \equiv -2$ is a primitive root modulo 13. From this, we see that the map is surjective; thus, $1 + \delta \in A_2$. Hence, $\psi(1 + \delta) = 2 < \psi(2)$.

In fact, $2 \in A_3$, since $\epsilon \mapsto 1 \in \mathcal{O}_K/(\delta)$; hence, $\delta \in A_2$. Therefore, the classes of δ and of $1 + \delta$ in $\mathcal{O}_K/(2)$ are in the image of A_2, so that $\psi(2) = 3$. A Euclidean division of 2 by $1 + \delta$ is: $2 = (1 + \delta)(3 + \delta) - \epsilon$, with $1 = \psi(\epsilon) < \psi(1 + \delta) = 2$.

6.3. $1 + \deg$ (Example 6.1.6).

6.4. If φ is an algorithm of Euclidean division in A, set

$$\psi(a/s) = \min\left\{\varphi(a') \mid a/s = a'/s' \text{ with } a' \in A \text{ and } s' \in S\right\}.$$

In order to divide b/t by a/s, first choose a representation a/s, which achieves the minimum: $\psi(a/s) = \varphi(a)$.

7.1. Any homogenous polynomial F of degree d in $n + 1$ variables $X_0, \ldots, X_n$ can be written as $F = F_0 + X_0\, G$, where F_0 is a homogenous polynomial of degree d in $X_1, \ldots, X_n$ and G is a homogenous polynomial of degree $d - 1$ in $n + 1$ variables. By induction on $d + n$, we see in this way that the desired dimension is equal to $\binom{d+n-1}{n-1} + \binom{d-1+n}{n} = \binom{d+n}{n}$.

7.3. Given a point p on the Klein quadric Ω, assume that $p_1 \neq 0$. Then, the first two points of (7.3.4) are well-defined. The line $L \subset \mathbf{P}_k^3$, which they define, has Plücker coordinates p, taking into account the relation (7.3.3).

7.4. The map can also be written as

$$\Phi : [X_0 : X_1 : X_2 : X_3] \mapsto \left[\frac{1}{X_0} : \frac{1}{X_1} : \frac{1}{X_2} : \frac{1}{X_3}\right].$$

From this, we see immediately that Φ is an involution. It is a degree 3 transformation, which is undefined only on the lines on which two of the X_i vanish. A surface whose image is a plane $\sum \lambda_i Y_i = 0$ has an equation $\sum \lambda_i \Phi(X)_i = 0$. These surfaces have four double points $P_0 = [1 : 0 : 0 : 0]$, $P_1 = [0 : 1 : 0 : 0]$, $P_2 = [0 : 0 : 1 : 0]$, $P_3 = [0 : 0 : 0 : 1] \in \mathbf{P}^3_k$, which are the vertices of a tetrahedron, called *fundamental*. (A cubic surface has a double point at P_0 if and only if any monomial in its equation contains X_0 at most in the first power.) The plane $\{X_i = 0\}$ contracts onto the opposite vertex of the fundamental tetrahedron, which is blown up. The number 3 is at the same time the intersection number of a general line with one of these cubic surfaces having four double points, and the intersection number of a plane with the image of a line in general position, which is therefore a skew cubic, passing through the four singular points P_i ($i = 0, \ldots, 3$), as one can verify.

We can also express this map as a *correspondence* in $\mathbf{P}^3_k \times \mathbf{P}^3_k$ defined by the equations $X_0Y_0 = X_1Y_1 = X_2Y_2 = X_3Y_3$ (the equations of the *graph*), which allows one to state many additional properties of this transformation.

7.5. A projective transformation must send lines onto lines, and hence also projective Eckardt points onto Eckardt points. But one cannot send, by a k-linear map, the cubic roots of a onto those of b if a/b is not a cube. A general theorem of algebraic geometry states that a k-birational map between two surfaces should send the anticanonical class of one surface onto the anticanonical class of the other, which implies that this map would be a projective isomorphism. From this, we deduce that the two surfaces are not k-birationally equivalent.

8.1. If $v(a) > v(b)$, then $v(b) \geq \min(v(a+b), v(-a)) = v(a+b)$, since $v(-a) = v(a) > v(b)$, but we also have $v(a+b) \geq \min(v(a), v(b)) = v(b)$; hence, $v(a+b) = v(b)$.

8.2. $\mathcal{O}_v$ is a local ring, since the set of its non-units is an ideal. Indeed, $\mathcal{O}_v^* = \{a \in k^* \mid v(a) = 0\}$ and its complement $\mathcal{O}_v \setminus \mathcal{O}_v^* = \{0\} \cup \{a \in k^* \mid v(a) > 0\} = \mathfrak{m}_v$ is an ideal. $\mathcal{O}_v$ is also principal, since it is even Euclidean for the norm $v : \mathcal{O}_v \setminus \{0\} \to \mathbf{N}$. Indeed, if $a \neq 0$ and $v(b) \geq v(a)$, the ratio b/a belongs to $\mathcal{O}_v$. We then apply Proposition 6.1.5.

8.3. Let $\mathfrak{m}$ be the unique maximal ideal of A. Since A is principal, we can write $\mathfrak{m} = (\pi)$, with $\pi \neq 0$ since A is not a field. (π is called a *uniformizing parameter*.) Moreover, any element $a \in A \setminus \{0\}$ can be uniquely written as $a = \epsilon \pi^\nu$ with $\epsilon \in A^*$ and $\nu \in \mathbf{N}$. On setting $v(a) = \nu$ and extending in an obvious manner, we obtain a discrete valuation on the field of fractions $k = Q(A)$. And $\mathcal{O}_v = \{0\} \cup \{a \in k^* \mid v(a) \geq 0\} = A$.

8.4. A formal series $f \in A$ is invertible if and only if its constant term is non-zero. Therefore, the non-units form an ideal $\mathfrak{m} = (X, Y)$. On the other hand, if

$f \in A$, the integer $v_{\mathfrak{m}}(f) = \max\{v \mid f \in \mathfrak{m}^v\}$ is just the degree of its initial form. One then easily verifies that $\forall f, g \in k^*$, $v_{\mathfrak{m}}(fg) = v_{\mathfrak{m}}(f) + v_{\mathfrak{m}}(g)$ and $v_{\mathfrak{m}}(f+g) \geq \min(v_{\mathfrak{m}}(f), v_{\mathfrak{m}}(g))$.

8.5. Lemma 8.2.4: the absolute value is not constant on the end of the sequence, but is bounded from below.

8.6. $\overline{20121} = 2 + \sum_{i=0}^{\infty} 3^{4i}(3^2 + 2 \cdot 3^3 + 3^4)$; one can also verify that $(3^2 + 2 \cdot 3^3 + 3^4) \sum_{i=0}^{\infty} 3^{4i} = \frac{144}{1-3^4} = -\frac{9}{5}$.

8.7. If $\alpha = \beta + p^{\ell}\overline{\gamma}$ with $\beta \in \mathbf{Q}_+$ and $\gamma \in \mathbf{N}$, that is, if $\alpha - \beta = p^{\ell}\gamma(1 + p^n + p^{2n} + \ldots) = p^{\ell}\gamma\frac{1}{1-p^n}$ (where $0 \leq \gamma < p^n$, but this is not important), we have $\alpha = \beta + \frac{p^{\ell}\gamma}{1-p^n} \in \mathbf{Q}$. Conversely, if $\alpha = a/b$ with $a \in \mathbf{Z}$ and $b \in \mathbf{N}^*$, on subtracting a suitable integer, we may assume that $\alpha < 0$. We then easily reduce considerations to the case when $p \nmid b$; there then exist $\lambda,\ \mu \in \mathbf{Z}$ such that $\lambda p + \mu b = 1$. Consequently, p is in the group of units of the ring $\mathbf{Z}/(b)$, which has order $n = \varphi(b)$, Euler's function (we set $\varphi(1) = 1$). We thus have $p^n \equiv 1 \pmod{b}$ and there exists $c \in \mathbf{N}$ such that $cb = p^n - 1$. Hence, $a/b = \frac{-ac}{1-p^n} = -ac(1 + p^n + p^{2n} + \ldots)$. We then use the fact that the positive integer $-ac$ has a finite expansion.

8.8. If $\alpha_n \to 0$ $(n \to \infty)$, the sums $s_N = \sum_{i=0}^{N} \alpha_i$ form a Cauchy sequence, because of the ultrametric inequality.

8.9. If $U = B_{\epsilon}(a)$ and $V = B_{\eta}(b)$ with $\epsilon \leq \eta$ and if $x \in U \cap V$, we have: $|a-b|_p = |(a-x)+(x-b)|_p < \max(\epsilon, \eta) = \eta$; hence, $y \in U \iff |y-a|_p < \epsilon \implies |y-b|_p = |(y-a)+(a-b)|_p < \max(\epsilon, \eta) = \eta \iff y \in V$.

8.10. The fourth powers modulo 5 are 0 and +1. A non-trivial solution in $\mathbf{Q}$ would imply a solution in $\mathbf{Z}$, with the x_i not all multiples of 5. Now, we find that $x_1^4 + x_2^4 + x_3^4 + x_4^4 \equiv 0 \pmod{5} \implies x_i \equiv 0 \pmod{5}\ \forall i = 1, \ldots, 4$. On writing $x_i = 5y_i\ \forall i = 1, \ldots, 4$ and dividing the equation by 5, we would then find that $x_5^4 + x_6^4 + x_7^4 + x_8^4 \equiv 0 \pmod{5}$; hence, $x_i \equiv 0 \pmod{5}$ for all $i = 1, \ldots, 8$; contradiction.

8.11. If $x_2 \equiv x_3 \equiv 0 \pmod{2}$, we immediately see that $f(x) \equiv x_1^4 \pmod{4}$. If $x_2 \equiv x_3 \equiv 1 \pmod{2}$ and $x_1 \equiv 0 \pmod{2}$, the term $x_1 x_2 x_3 (x_1 + x_2 + x_3)$ is a product of two even numbers; then, $f(x) \equiv x_2^4 + x_3^4 - x_2^2 x_3^2 \equiv 1 \pmod{4}$. Finally, if the x_i are all odd, we have $f(x) \equiv -x_1 x_2 x_3 (x_1 + x_2 + x_3) \pmod{4}$, but there are only two more cases to consider, for $f(x) = f(-x)$. If $x_1 \equiv x_2 \equiv x_3 \equiv 1 \pmod{4}$, we find $f(x) \equiv -1 \cdot 3 \pmod{4}$, and if $x_1 \equiv 1 \pmod{4}$ and $x_2 \equiv x_3 \equiv -1 \pmod{4}$, we find $f(x) \equiv -1 \cdot -1 \pmod{4}$. A non-trivial solution in $\mathbf{Q}_2$ implies the existence of a primitive solution in $\mathbf{Z}_2$. But on looking modulo 4, we see that $x,\ y$ and z should also be zero modulo 2; hence, $f(x) \equiv f(y) \equiv f(z) \equiv 0 \pmod{16}$; then, dividing by 4, $u,\ v$, and w should also be zero modulo 2; contradiction.

8.12. The p-adic solutions are in $\mathbf{Z}_p$, since $x^2 = -1 \implies 2v_p(x) = 0$. There is no solution for $p = 2$, since $x^2 \equiv 0,\ \text{where} 1 \pmod{4}$. If $p > 2$, a necessary condition

is that -1 is a square modulo p, which means that $p \equiv 1 \pmod 4$. By Hensel's Lemma (Proposition 8.4.1), this condition is also sufficient, since for any solution $x_0 \bmod p$, the derivative of x^2+1 is $2x_0 \not\equiv 0 \pmod p$.

8.13. The polynomial $f(x) = x^{p-1} - 1$ has $p-1$ distinct roots in the finite field $\mathbf{F}_p$. Each of these roots lifts to an element $x_0 \in \mathbf{Z}_p$ such that $f(x_0) \equiv 0 \pmod p$ and $f'(x_0) = (p-1)\,x_0^{p-2} \not\equiv 0 \pmod p$. Hensel's Lemma then states that there exists $x \in \mathbf{Z}_p$ such that $f(x) = 0$, with, moreover, $v_p(x - x_0) > v_p(f'(x_0)) = 0$. Thus, we do indeed obtain $p-1$ distinct roots in $\mathbf{Z}_p$, and these are all the roots of the polynomial f in $\overline{\mathbf{Q}}_p$.

8.14. If $(y_1, y_2, y_3) \in \mathbf{Z}_p$ is a non-trivial solution modulo p (see Exercise 3.5), we may assume that $y_1 \not\equiv 0 \pmod p$. We then fix $x_2 = y_2$ and $x_3 = y_3$ and set $f(x) = x^2 + x_2^2 + x_3^2$. Since $f(y_1) \equiv 0 \pmod p$ and $f'(y_1) = 2y_1 \not\equiv 0 \pmod p$, by Hensel's Lemma there exists a solution $(x_1, x_2, x_3) \in \mathbf{Z}_p$.

9.1. We consider the homomorphism $\lambda : \mathbf{F}_p^* \to \mathbf{F}_p^*$ defined by $x \mapsto x^3$. Then, $\ker\lambda$ has order 1 or 3, since the polynomial $x^3 - 1$ has 1 or 3 roots in $\mathbf{F}_p$. On the other hand, $|\ker\lambda|$ divides $p-1$, since $\ker\lambda$ is also a subgroup of $\mathbf{F}_p^*$. We deduce that $|\ker\lambda| = 1$ if $p \equiv -1 \pmod 3$; in this case, λ is injective, and hence also surjective.

9.2. If $p \equiv +1 \pmod 3$, we have necessarily $|\ker\lambda| = 3$, since the polynomial $x^{(p-1)/3} - 1$ has no more than $(p-1)/3$ roots, and hence there exists $\gamma \in \mathbf{F}_p^*$ such that $\alpha = \gamma^{(p-1)/3} \neq 1$. Then, $\alpha^3 = 1$, but $\alpha \neq 1$. Then, $\mathbf{F}_p^*/\ker\lambda \cong \mathrm{Im}\,\lambda = (\mathbf{F}_p^*)^3$; consequently, $\left|\mathbf{F}_p^*/(\mathbf{F}_p^*)^3\right| = |\ker\lambda| = 3$.

If 2 and 3 are not cubes modulo p, each one belongs by this isomorphism to a non-trivial class of cubes. But they can belong to distinct classes (in $\mathbf{Z}/3$) and then $2 \cdot 3$ is a cube, or they belong to the same class and then 2^2 and 3 are in two distinct classes and $2^2 \cdot 3$ is a cube.

(More generally, for $n \geq 2$, we consider the homomorphism $\lambda : \mathbf{F}_q^* \to \mathbf{F}_q^*$ defined by $x \mapsto x^n$. Then, $\mathbf{F}_q^*/\ker\lambda \cong \mathrm{Im}\,\lambda = (\mathbf{F}_q^*)^n$; consequently, $\left|\mathbf{F}_q^*/(\mathbf{F}_q^*)^n\right| = |\ker\lambda| = \mathrm{pgcd}(n, q-1)$.

Indeed, $\ker\lambda$ is a subgroup of $\mathbf{F}_q^*$, and also a subgroup of the group $\mu_n(\overline{\mathbf{F}_q})$ of n-th roots of 1, which has order n/p^i, where p^i is an inseparability index. Therefore, the order of $\ker\lambda$ divides $d = \mathrm{pgcd}(n, q-1)$. Finally, if γ is a generator of the cyclic group $\mathbf{F}_q^*$ (Reminder 3.4.6), $\gamma^{(q-1)/d}$ is an element of order d in $\ker\lambda$).

9.3. For $p = 3$, we set $x = 0$ and $y = -2$, since the polynomial $f(z) = 5z^3 - 32$ verifies $v_3(f(1)) = 3$ and $v_3(f'(1)) = 1$, and we apply Hensel's Lemma. Similarly, the curve has a smooth point $(1, 0, 1)$ modulo 2 and $(1, 2, 0)$ modulo 5. Finally, for primes $p > 5$, we can take $z = x$ if 2 is a cube, $z = y$ if 3 is a cube, $z = 0$ if 6 is a cube, and $z = -2y$ if 12 is a cube.

9.4. If $p \neq 2, 7$, there are solutions modulo p, since

$$\left(\frac{2}{p}\right) = -1 \quad \text{and} \quad \left(\frac{-7}{p}\right) = -1 \implies \left(\frac{-14}{p}\right) = +1.$$

If $m = 2, -7$ or -14 is a square modulo p, we can solve the equation $X^2 - m = 0$ as a congruence modulo p and lift the solution to $\mathbf{Z}_p$, by Hensel's Lemma. Since $2 \equiv 3^2 \pmod 7$, we can also solve $X^2 - 2 = 0$ in $\mathbf{Z}_7$. For $p = 2$, we can solve the equation $f(X) = X^2 + 7 = 0$ in $\mathbf{Z}_2$, since $v_2(f(1)) = 3$ and $v_2(f'(1)) = 1$. So, there are solutions in all p-adic fields and in $\mathbf{R}$, but clearly there is no solution $X \in \mathbf{Q}$.

9.5. Since there is no non-trivial solution in $\mathbf{Q}$ with $w = 0$, we can study the homogenous equation $x^2 + y^2 + z^2 - Nw^2 = 0$. For this equation, there is no p-adic obstruction for $p \geq 3$, because we have seen in Exercise 8.14 that there are even solutions in $\mathbf{Q}_p$ with $w = 0$, and hence also many others, by the implicit functions theorem (Proposition 8.4.5). For $p = 2$, we know that the squares modulo 8 are 0, 1, and 4. We easily deduce that there is no 2-adic solution if $N \equiv 7 \pmod 8$, and more generally if N has the form $N = 4^\lambda(8\mu + 7)$, with $\lambda \in \mathbf{N}$ and $\mu \in \mathbf{Z}$. In all other cases, we can solve modulo 8 and lift the solution by Hensel's Lemma (if N is a multiple of 4, we must start with a change of variables of the type $w' = 2^\lambda w$). There remains the Archimedean place, for which one must require that $N \geq 0$. Thus, the Hasse–Minkowski Theorem (Theorem 9.1.1) allows one to deduce that the quadratic form $x^2 + y^2 + z^2 - Nw^2$ represents zero in $\mathbf{Q}$ if and only if $N \geq 0$ with $N \neq 4^\lambda(8\mu + 7)$. It is also true that these integers are sums of three squares of integers, but to prove this, one needs an extra argument (see Exercise 4.12).

9.7. If $f \in k[X]$ is a polynomial in one variable and if $\alpha \in \bar{k}$, we know (Exercise 3.1) that $f(\alpha) = f'(\alpha) = 0$ if and only if f is a multiple of $(X - \alpha)^2$. If f has degree 3, this condition cannot be satisfied for two distinct values α and β, unless the polynomial is identically zero. Since the singularity condition is invariant under linear transformation, we can assume that the cubic surface is the set of zeros (in the affine space $\mathbf{A}^3_k$) of a polynomial $g \in k[X, Y, Z]$ of degree 3, and that the two points are on the line ℓ with equation $Y = Z = 0$. On setting $f(X) = g(X, 0, 0)$, we reduce the question to the case of one variable and $f = 0$: the polynomial g vanishes along the line ℓ, which is therefore contained in the surface.

9.8. There is no singular point in the affine space $x_0 \neq 0$, for if we set $x_0 = 1$, we obtain the affine equation $x_1x_2x_3 = 1$. A singular point should satisfy $\frac{\partial}{\partial x_1}(x_1x_2x_3 - 1) = 0$, and hence $x_2x_3 = 0$, which is not compatible with the equation of the surface. In the plane at infinity $\{x_0 = 0\}$, we find the equation $x_1x_2x_3 = 0$, which describes a union of three projective lines; their mutual intersections are singular points of the surface: $\frac{\partial}{\partial x_i}(x_1x_2x_3 - x_0^3) = 0 \ \forall i = 0, \ldots, 3$ at the points $[0 : 1 : 0 : 0]$, $[0 : 0 : 1 : 0]$ et $[0 : 0 : 0 : 1]$. Moreover, the surface does not contain any affine line (see Exercise 4.7).

9.9. We recognize the norm form associated with $\alpha = \sqrt[3]{2}$ (see Exercise 3.7): $N_{k(\alpha)/k}(x + \alpha y + \alpha^2 z) = x^3 + 2y^3 + 4z^3 - 6xyz$. By definition, this form is the product of three linear factors, and over $\bar{k}$ we can re-write the equation as $x_1x_2x_3 - 929w^3 = 0$. We have seen in Exercise 9.8 that this cubic surface has three double points. This entails that it verifies the fine Hasse principle (Corollary 9.3.8). Hence, to see if it has rational points, it suffices to show that it has points in all p-adic fields and in $\mathbf{R}$. For $\mathbf{R}$ this is obvious, and for $p \neq 2, 3$ or 929, we can apply the Chevalley–Warning Theorem (Theorem 3.4.10) and lift a non-singular solution by Hensel's Lemma (Corollary 8.4.4). One must only beware of the fact that some solutions modulo p are singular. This is not a serious problem, for if a cubic surface (over $k = \mathbf{F}_p$) has a double k-rational point, it also has non-singular points in k (a line defined over k and passing through a double point cuts the cubic surface only at one other point, which is invariant under the action of the Galois group $\mathrm{Gal}(\bar{k}/k)$, and hence has its coordinates in k). Then, for $p = 2$ we can take $x = w = 1$, $y = z = 0$. For $p = 3$, we observe that 929 is congruent to -16 modulo 27; thus, we can take $(x, y, z, w) = (0, -2, 0, 1)$ and apply Hensel's Lemma. Finally, 929 is a prime and 2 is a cube modulo 929, since $929 \equiv -1 \pmod 3$ (see Exercise 9.1). Therefore, the surface has $\mathbf{Q}$-rational points, even if this argument tells nothing about their location. (One can show that there is in fact an infinity of rational points; see §7.2.)

10.1. Let $\alpha_d(k) = i$; by Lemma 10.1.3, it suffices to see that d^i is an integer. And this is equivalent to asking that $n > d^i$ or that $n > [d^i]$.

10.2. Replace the powers of t by the elements of a basis of the algebraic extension K/k.

10.4. If $p \nmid a_{21}$, we choose $x_1 = -a_2/a_{21}$, $x_2 = 1$, $x_i = 0$ for all $i > 2$. Then, using Lemma 10.2.4, $F(x) \equiv a_{21}x_1x_2^2 + a_2x_2^3 \equiv 0 \pmod p$ and $\frac{\partial F}{\partial X_1}(x) \equiv a_{21}x_2^2 \not\equiv 0 \pmod p$. If $p \nmid a_{123}$, we can choose $x_1 = -\frac{a_2+a_3+a_{23}+a_{32}}{a_{123}}$, $x_2 = x_3 = 1$, $x_i = 0$ for all $i > 3$.

Bibliography

[B] Bartholdi, N.: La dimension diophantienne des corps p-adiques. Univ. de Genève, Genève (2007, unpublished)

[Ba] Bashmakova, I.G.: Diophantus and Diophantine Equations. Trans. from Russian (Nauka, Moscow, 1972). The Dolciani Mathematical Expositions, vol. 20. Math. Assoc. America, Washington, DC (1997)

[BaSl] Bashmakova, I.G., Slavutin, E.I.: La méthode des approximations successives dans l'Arithmétique de Diophante. Istor. Metodol. Estestv. Nauk **16**, 25–35 (1974, in Russian)

[BW] Bruce, J.W., Wall, C.T.C.: On the classification of cubic surfaces. J. Lond. Math. Soc. (2) **19**, 245–256 (1979)

[Ca] Cajori, F.: A History of Mathematics, 3rd edn. Chelsea, New York (1980)

[Cas] Cassels, J.W.S.: The rational solutions of the diophantine equation $Y^2 = X^3 - D$. Acta Math. **82**, 243–273 (1950)

[CF] Cassels, J.W.S., Fröhlich, A.: Algebraic Number Theory. Academic Press, London (1967)

[Cay] Cayley, A.: A memoir on cubic surfaces. Philos. Trans. R. Soc. **159**, 231–326 (1869)

[CSS] Colliot-Thélène, J.-L., Sansuc, J.-J., Swinnerton-Dyer, P.: Intersections of two quadrics and Châtelet surfaces. J. Reine Angew. Math. **373**, 37–107 (1987); **374**, 72–168 (1987)

[CTs] Coray, D.F., Tsfasman, M.A.: Arithmetic on singular Del Pezzo surfaces. Proc. Lond. Math. Soc. (3) **57**, 25–87 (1988)

[Di] Diophantus Alexandrinus: Opera Omnia, edition P. Tannery. Teubner, Stuttgart (1893)

[Fe] Fermat, P.: Œuvres, edition P. Tannery. Gauthier-Villars, Paris (1892–1922)

[Ha] Harper, M.: $\mathbf{Z}[\sqrt{14}]$ is Euclidean. Can. J. Math. **56**, 55–70 (2004)

[He] Heath, Sir Th.: A History of Greek Mathematics, vol. I. Dover, New York (1981)

[HCV] Hilbert, D., Cohn-Vossen, S.: Anschauliche Geometrie. Springer, Berlin (1932)

[Jo] Joly, J.-R.: Équations et variétés algébriques sur un corps fini. L'Enseignement Math. (2) **19**, 1–117 (1973)

[Le] Lenstra Jr., H.W.: Euclidean number fields of large degree. Invent. Math. **38**, 237–254 (1976/1977)

[RMP] Ram Murty, M., Petersen, K.L.: The generalized Artin conjecture and arithmetic orbifolds. In: Groups and Symmetries. CRM Proc. Lecture Notes, vol. 47, pp. 259–265. Amer. Math. Soc., Providence, RI (2009)

[Ra] Rashed, R.: Les travaux perdus de Diophante. I, II. Rev. Hist. Sci. **27**, 97–122 (1974); **28**, 3–30 (1975)

[Sch] Schläfli, L.: On the distribution of surfaces of the third order into species. Philos. Trans. R. Soc. **153**, 193–247 (1864)

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7

[Sel] Selmer, E.S.: Tables for the Purely Cubic Field $K(\sqrt[3]{m})$. Avh. Norske Vid. Adak. Oslo (1955)

[Ses] Sesiano, J.: Books IV to VII of Diophantus' Arithmetica: in the Arabic Translation Attributed to Qusṭā ibn Lūqā. Springer, New York (1982)

[Sh] Shafarevich, I.R.: Basic Algebraic Geometry. Springer, New York–Heidelberg (1974)

[Vi] Viète, F.: Zeteticorum Libri Quinque (publié en 1591). In: Opera Mathematica, pp. 42–81. G. Olms Verlag, Hildesheim (1970)

[vdW2] van der Waerden, B.L.: Einführung in die algebraische Geometrie. Springer, Heidelberg (1939)

[vdW] van der Waerden, B.L.: Algebra, 7th edn. Springer, Heidelberg (1966)

[ZS] Zariski, O., Samuel, P.: Commutative Algebra. Springer, Heidelberg (1960)

Index

D. Coray, *Notes on Geometry and Arithmetic*, Universitext,
https://doi.org/10.1007/978-3-030-43781-7