2

Roots

In the first chapter, the emphasis was on given numbers, and we were led to look at the equations of which they are solutions. In this chapter, we switch roles and look at polynomial equations and their eventual roots. Generalizing the construction of the field of complex numbers from the real numbers, we show how to create roots of a polynomial which does not have enough of them in a given field.

2.1 Ring of remainders

Let K be a field and let P be a nonconstant polynomial with coefficients in K. We denote its degree by d. Endow the vector space $E \subset K[X]$ of polynomials with degree $< d$ with a ring structure in the following way:

– addition, with its identity element 0, is given by the vector space structure;

– the identity element for the multiplication is the constant polynomial 1;

– if A and B are two polynomials in E, one defines the multiplication $A * B$ as the remainder in the Euclidean division of the polynomial AB by the polynomial P.

Let us show that this actually defines a ring. First of all, it is obvious that $(E, +, 0)$ is an abelian group. The internal law $*$ is obviously commutative; moreover, $1 * A = A * 1$ is the remainder in the Euclidean division of A by P, so is equal to A since $\deg A < d = \deg P$. This shows that 1 is the identity for the law $*$. To show associativity, consider the equations $AB = PQ_1 + A * B$ and $(A * B)C = PQ_2 + (A * B) * C$ obtained from Euclidean division, so that

$$\begin{aligned} ABC &= (PQ_1 + A * B)C = PQ_1C + PQ_2 + (A * B) * C \\ &= P(Q_1C + Q_2) + (A * B) * C. \end{aligned}$$

This shows that $(A*B)*C$ is the remainder in the Euclidean division of ABC by P. Similarly, $A*(B*C)$ is the remainder in the Euclidean division of ABC by P, so is equal to $(A*B)*C$. The law $*$ is thus associative. The distributivity is shown in the same way: considering the equations $AB = PQ_1 + A*B$ and $AC = PQ_2 + A*C$ obtained by Euclidean division, one deduces that

$$A(B+C) = AB + AC = P(Q_1+Q_2) + A*B + A*C.$$

Hence, the remainder in the Euclidean division of $A(B+C)$ by P is equal to $A*B + A*C$, which gives us the equality $A*(B+C) = A*B + A*C$.

Let us also remark that mapping the element $a \in K$ to the constant polynomial $a \in E$ defines a ring homomorphism $K \to E$.

Definition 2.1.1. *The ring that we just constructed is denoted* $K[X]/(P)$.

This is *the ring of remainders of Euclidean divisions* by P. As soon as we are familiar with this new ring, we will drop the symbol $*$ and just denote multiplication as usual.

Proposition 2.1.2. *Let P be a nonconstant polynomial in $K[X]$. The following properties are equivalent:*

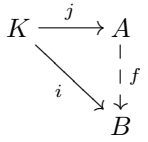
a) *the ring $K[X]/(P)$ is a field;*
b) *the ring $K[X]/(P)$ is an integral domain;*
c) *the polynomial P is irreducible in $K[X]$.*

Proof. Implication $a)\Rightarrow b)$ is obvious. Assume $b)$. If $P = QR$ in $K[X]$, for two polynomials Q and R with degrees $< \deg P$, one has $Q*R = 0$ in $K[X]/(P)$, which contradicts the hypothesis that $K[X]/(P)$ is an integral domain, so P is irreducible in $K[X]$, hence $c)$. Finally, assume $c)$. Let A be a nonzero element of $K[X]/(P)$, viewed as a polynomial of degree $< \deg P$; we have to show that A has an inverse in $K[X]/(P)$. Since P is irreducible and A is not a multiple of P, they are coprime and Bézout's relation (Corollary 2.4.2) gives us two polynomials U and V in $K[X]$ such that $UA + VP = 1$. If $U = PQ + U_1$ is the Euclidean division of U by P, then $U_1 * A = 1$, which shows that A is invertible in the ring $K[X]/(P)$. □

Let P be an irreducible polynomial in $K[X]$ and consider the field extension $j\colon K \to K[X]/(P)$ that we have just defined. Let x denote the polynomial X viewed as an element in $K[X]/(P)$. By construction, for every polynomial $A \in K[X]$, $A(x)$ is the remainder in the Euclidean division of the polynomial $A(X)$ by the polynomial P. In particular, $P(x) = 0$. In other words, *we just defined an extension of the field K in which the polynomial P has a root.* The next theorem claims that this is actually the "best" way of doing it. In fact, this ring $K[x]/(P)$ satisfies a *universal property*.

Theorem 2.1.3. *Let K be a field and let P be a polynomial in $K[X]$. Let us denote the ring $K[X]/(P)$ by A and let $j\colon K \to A$ be the canonical ring homomorphism. Now let $i\colon K \to B$ be a ring homomorphism and y an element in B such that $P(y) = 0$. Then there exists a* unique *ring homomorphism $f\colon A \to B$ such that $f \circ j = i$ and $f(x) = y$.*

This is sometimes represented by a diagram



where the dotted arrow $f\colon A \to B$ is the one whose existence is claimed by the theorem.

The idea of the proof is not complicated, yet requires understanding of what we did during the construction of $K[X]/(P)$. We started with the ring $K[X]$ in which we have a new element $x = X$, but this satisfies no relation at all and it is not a root of P. Then we changed the rules in a clever way by imposing $P(x) = 0$. Some of the consequences of $P(x)$ vanishing come from Euclidean division: if $A = QP + B$, then the relation $P(x) = 0$ forces $A(x) = B(x)$. A posteriori, the validity of the given construction actually means that all consequences are obtained from Euclidean divisions.

Proof. If $f(x) = y$, one must have $f(Q(x)) = Q(y)$ for any polynomial $Q \in K[X]$, and in particular for any polynomial with degree $< \deg P$. That shows that there exists at most one homomorphism f satisfying $f \circ j = i$, and that if it actually exists, it has to be given by the map

$$f\colon K[X]/(P) \to B, \quad Q(X) \mapsto Q(y).$$

(Recall that an element of $K[X]/(P)$ *is* really a polynomial with degree $<$ $\deg P$.) Let us define f in this way. We now have to prove that f is a ring homomorphism. It is obviously a morphism of vector spaces and it satisfies $f \circ j = i$. Moreover, if Q and R are two polynomials in $K[X]$ with degrees $< \deg P$, let us write the Euclidean division of QR by P, say, $QR = PS + Q*R$. Then, since $P(y) = 0$ in B,

$$\begin{aligned} f(Q*R) = (Q*R)(y) &= (Q*R)(y) + P(y)S(y) \\ &= (QR)(y) = Q(y)R(y) = f(Q)f(R), \end{aligned}$$

which shows that f is a ring homomorphism. □

To sum up the construction of this section, let us introduce a definition.

Definition 2.1.4. *If $i\colon E \to F$ and $j\colon E \to F'$ are two extensions of a field E, a* homomorphism of extensions *from F' to F is a field homomorphism $f\colon F' \to F$ such that $f \circ j = i$.*

A bijective homomorphism of extensions is called an *isomorphism*.

Theorem 2.1.5. *Let K be a field and let P be a irreducible polynomial with coefficients in K. There exists a finite field extension $K \to K_1$ and a root x of P in K_1 such that*

a) *$K_1 = K[x]$;*

b) *If $K \to L$ is a field extension, the set of morphisms of extensions from K_1 to L is in bijection with the set of roots of P in L, this bijection being given by $f \mapsto f(x)$.*

2.2 Splitting extensions

Definition 2.2.1. *Let K be a field and let P be a nonconstant polynomial in $K[X]$. A* splitting extension *of P is a field extension $j\colon K \to E$ such that:*

a) *over E, P can be decomposed as a product of linear factors; explicitely, if d is the degree of P and if c denotes its leading coefficient, then there exist $x_1, \ldots, x_d$ in E such that $P = c\prod_{i=1}^{d}(X - x_i)$;*

b) *as a field, E is generated by the x_i, that is, $E = K(x_1, \ldots, x_d)$.*

In other words, a splitting extension of an irreducible polynomial P is an extension which contains all of "the" roots of P (this is condition a) and which is "minimal" for that property (this is condition b).

Theorem 2.2.2. *Let K be a field and let P be a nonconstant polynomial in $K[X]$.*

a) *There is a splitting extension for P.*

b) *Any two such extensions are isomorphic: if $j\colon K \to E$ and $j'\colon K \to E'$ are two splitting extensions of P, there exists an isomorphism of fields $f\colon E \to E'$ such that $f \circ j = j'$.*

Proof. Let us begin with a very simple remark: let $K \to E$ be a splitting extension of P and let α be a root of P in E. This allows us to write $P = (X - \alpha)Q$, where Q is a polynomial with coefficients in $K[\alpha]$. It is then clear that E is a splitting extension of the polynomial Q over the field $K[\alpha]$. This remark gives the idea of the proof of the theorem: if we know how to construct $K[\alpha]$, we will obtain a splitting extension E by induction. And we know precisely how to define a field $K[\alpha]$; that was the main result of the last section.

Let us now show *a*) and *b*) by induction on the degree of P. If $\deg P = 1$, it suffices to let $E = K$. Let $Q \in K[X]$ be an irreducible factor of P. By Theorem 2.1.5, there exists an extension $K \to K_1$ and an element $x_1 \in K_1$ such that *a*) $Q(x_1) = 0$; *b*) $K_1 = K[x_1]$. Then let P_1 be the quotient of P by $X - x_1$ in the ring $K_1[X]$. By induction, the polynomial P_1 admits a splitting extension over K_1, say $K_1 \to E$. The composed extension $K \to E$ is a field extension in which P is a product of factors of degree 1. Moreover, if $x_2, \ldots, x_d$ are the roots of P_1 in E (set $d = \deg P$),

$$E = K_1(x_2, \ldots, x_d) = K(x_1)(x_2, \ldots, x_d) = K(x_1, \ldots, x_d),$$

so that E is generated by the x_i over K. Hence E is a splitting extension of P over K.

Let $K \to E'$ be another splitting extension of P and let us define an isomorphism of extensions from E to E'. By hypothesis, the chosen irreducible factor Q of P has a root x_1' in E'. By Theorem 2.1.5, there exists a homomorphism of extensions $f_1 \colon K_1 \to K_1'$, where $K_1' = K[x_1']$ is the subfield of E' generated by x_1'. As f_1 is surjective, it has to be an isomorphism and this isomorphism maps the polynomial P_1 to the polynomial $P_1' = P/(X - x_1')$. The composite extension $K_1 \xrightarrow{\sim} K_1' \to E'$ is therefore a splitting extension of the polynomial $P/(X - x_1)$. By induction, the two extensions $K_1 \to E$ and $K_1 \to E'$ are isomorphic and there exists an isomorphism $f \colon E \to E'$ extending the isomorphism $f_1 \colon K_1 \to K_1'$. □

2.3 Algebraically closed fields; algebraic closure

Definition 2.3.1. *One says that a field K is* algebraically closed *if any nonconstant polynomial of $K[X]$ has a root in K.*

By induction on the degree, we see that this statement is equivalent to saying that *any polynomial is split in K*. The constructions of this chapter also show that a field is algebraically closed if and only if *it has no nontrivial algebraic extensions* (that is, if $j \colon K \to E$ is an algebraic extension, j is a isomorphism). One direction is clear. If K is algebraically closed and if $j \colon K \to E$ is an algebraic extension, let x be an element of E, P its minimal polynomial. By hypothesis, P is split in K: there exist elements $x_1, \ldots, x_n$ in K such that $P = (X - x_1) \ldots (X - x_n)$. Since $P(x) = 0$, x is one of the x_i (more precisely one of the $j(x_i)$). This shows that j is surjective and hence an isomorphism. For the other direction, let P be a nonconstant polynomial in $K[X]$ and let Q be an irreducible factor of P. We showed that the ring $K[X]/(Q)$ is an algebraic extension of K with degree $\deg Q$. Since K has no

nontrivial algebraic extensions, $\deg Q = 1$, so that Q has a root in K, and so does P.

Definition 2.3.2. *An* algebraic closure *of a field K is an algebraic extension $j\colon K \to \Omega$, where Ω is an algebraically closed field.*

Theorem 2.3.3 (Steinitz, 1910). *Every field has an algebraic closure; two algebraic closures of a field are isomorphic.*

There are two types of algebraic closures: those that one can see, like the algebraic closure of the field of real numbers (which is the field of complex numbers), and those which are constructed by a transfinite procedure, as in the general proof of the existence of an algebraic closure.

Theorem 2.3.4. *The field $\mathbf{C}$ of complex numbers is algebraically closed.*

Despite its famous name, "the fundamental theorem of algebra," this is really a theorem from analysis. Let me offer you three proofs. The first one is short and frankly analytic. The second one looks as if it were algebraic, but analysis is hidden in the use of the "intermediate value theorem." The third one comes from topology.

First proof. Let $P \in \mathbf{C}[X]$ be a nonconstant polynomial with no root in $\mathbf{C}$. Let us write it $P = a_n X^n + \cdots + a_0$, with $a_n \neq 0$ and $n \geqslant 1$. Then, for any $z \in \mathbf{C}$ such that $|z| > 1$, one has

$$\begin{aligned} |P(z)| &\geqslant |a_n|\,|z|^n - (|a_0| + \cdots + |a_{n-1}|)\,|z|^{n-1} \\ &\geqslant |z^n| \left(|a_n| - \frac{1}{|z|}(|a_0| + \cdots + |a_{n-1}|) \right). \end{aligned}$$

In particular, $|P(z)|$ goes to $+\infty$ when $|z| \to \infty$. It follows that the function $1/P$ is bounded on $\mathbf{C}$ and holomorphic everywhere (P does not vanish). By Liouville's theorem, it is constant, hence we have a contradiction. □

Second proof. Let $P \in \mathbf{C}[X]$ be a nonconstant polynomial. Observe that the polynomial $Q(X) = P(X)\overline{P}(X)$ has real coefficients. If we show that it has a complex root z, then either $P(z) = 0$, or $P(\overline{z}) = \overline{\overline{P}(z)} = 0$, so that P also has a complex root. Therefore it suffices to show that every nonconstant polynomial $P \in \mathbf{R}[X]$ has a complex root, which we will prove by induction on the greatest power of 2, $\nu_2(P)$, which divides the degree of P.

If this power is 0, that is, if $\deg P$ is odd, the limits of $P(x)$ when $x \to \pm\infty$ are $+\infty$ and $-\infty$ (depending on the sign of the leading coefficient of P). It follows from the intermediate value theorem that P has a real root.

Assume the result is established for polynomials P such that $\nu_2(P) < n$ and let P be a polynomial in $\mathbf{R}[X]$ with $\nu_2(P) = n$. Let Ω be an extension

of $\mathbf{C}$ in which P is split and let us denote its roots by $(\xi_i)_{1\leqslant i\leqslant \deg P}$. Let c be a real number. For $1 \leqslant i < j \leqslant \deg P$, set $z_{i,j;c} = \xi_i + \xi_j + c\xi_i\xi_j$ and let us introduce the monic polynomial $Q \in \Omega[X]$ whose roots are the $z_{i,j;c}$. First of all, one has $\deg Q = \deg P(\deg P - 1)/2$, hence $\nu_2(Q) = \nu_2(P) - 1$. Moreover, Q has *real coefficients.* Indeed, these coefficients are given by polynomials with integer coefficients in the ξ_i, and these polynomials are invariant under every permutation of the variables. It follows from Theorem 1.5.3 on symmetric polynomials that the coefficients of Q can be expressed as polynomials with real coefficients in the elementary symmetric polynomials of $\xi_1, \ldots, \xi_{\deg P}$, that is, in the coefficients of P. In particular, the coefficients of Q are real numbers. By induction, Q has at least one root in $\mathbf{C}$.

This is true for every value of c. As $\mathbf{R}$ is infinite, there exists at least one pair (i, j) and two real numbers $c \neq c'$ such that $\xi_i+\xi_j+c\xi_i\xi_j$ and $\xi_i+\xi_j+c'\xi_i\xi_j$ both are complex numbers, from which we deduce that $a = \xi_i+\xi_j$ and $b = \xi_i\xi_j$ belong to $\mathbf{C}$. They are roots of the polynomial $R = X^2 - aX + b$, whose discriminant $\Delta = a^2 - 4b$ is a complex number. If we show that Δ is a square in $\mathbf{C}$, it will follow that the two roots of R, namely ξ_i and ξ_j, are complex numbers.

Let $\Delta = p + iq$. The equation $(x + iy)^2 = \Delta$ is equivalent to the equations

$$x^2 - y^2 = p \quad \text{and} \quad 2xy = q,$$

hence $(x^2 + y^2)^2 = p^2 + q^2$ and $x^2 + y^2 = \sqrt{p^2 + q^2}$. One obtains for x^2 and y^2 the following (nonnegative) values:

$$x^2 = \frac{1}{2}\big(p + \sqrt{p^2 + q^2}\big) \quad \text{and} \quad y^2 = \frac{1}{2}\big(-p + \sqrt{p^2 + q^2}\big),$$

hence values for x and y, by accounting their signs so that $q = xy/2$.

This shows that ξ_i and ξ_j are complex numbers and consequently that the initial polynomial P has a root in $\mathbf{C}$. By induction, the theorem is proved. □

Third proof. Again let P be any nonconstant polynomial with coefficients in $\mathbf{C}$. If $z \in \mathbf{C}$, we will denote by $\nu(z)$ the cardinality of the finite set $P^{-1}(z)$. The goal is to show that $\nu(0) > 0$ and we will in fact show that $\nu(z) > 0$ for every $z \in \mathbf{C}$.

Let $\Delta \subset \mathbf{C}$ be the set of $z \in \mathbf{C}$ such that $P'(z) = 0$, $U = \mathbf{C} \setminus \Delta$ and $V = \mathbf{C} \setminus P(\Delta)$. The sets U and V are the complementary subsets of finite sets in $\mathbf{C}$, so they are open and connected (*exercise*).

If $u = x + iy$ and $P(u) = A(x, y) + iB(x, y)$, one deduces easily (for example, from Cauchy's formulae in the theory of analytic functions) that

$$|P'(u)|^2 = \det \begin{pmatrix} \partial A/\partial x & \partial B/\partial x \\ \partial A/\partial y & \partial B/\partial y \end{pmatrix}.$$

Therefore, the implicit function theorem for functions $\mathbf{R}^2 \to \mathbf{R}^2$ implies that for any $u \in \mathbf{C}$ with $P'(u) \neq 0$, P defines a diffeomorphism from a neighborhood of u to a neighborhood of $P(u)$.

Now let $z \in V$. For every $u \in P^{-1}(z)$, one has $P'(u) \neq 0$, so that there exists a neighborhoods W_u and Ω_u of z such that P induces a diffeomorphism $W_u \to \Omega_u$. Let $\Omega = \bigcap_{u \in P^{-1}(z)} \Omega_u$; this is a neighborhood of z and any $w \in \Omega$ has at least $\nu(z)$ preimages by P, one in each W_u, $u \in P^{-1}(z)$. In particular, the set V^+ of $z \in V$ such that $\nu(z) > 0$ is *open* in V.

But it is also closed: let (z_j) be any sequence of points in V with $\nu(z_j) > 0$ such that $z_j \to z \in V$. Let us choose for every j an element $u_j \in \mathbf{C}$ such that $z_j = P(u_j)$. Since the sequence (z_j) is bounded and $|P(u)| \to +\infty$ when $|u| \to +\infty$, the sequence (u_j) is bounded too. It thus has a limit point $u \in \mathbf{C}$. Since P defines a continuous function, $P(u)$ is also a limit point of the sequence $(P(u_j))$. Necessarily $P(u) = z$, and hence $\nu(z) > 0$. This shows that V^+ is closed in V.

As V is connected, the nonempty subset V^+ cannot be both open and closed unless it is equal to all of V. In other words, $\nu(z) > 0$ for every $z \in V$.

If $z \notin V$, there exists by definition $u \in \Delta$ such that $P(u) = z$ and $\nu(z) > 0$. Finally, $\nu(z) > 0$ for every $z \in \mathbf{C}$. □

From an algebraically closed field, it is easy to construct an algebraic closure for any of its subfields.

Proposition 2.3.5. *Let Ω be an algebraically closed field and let K be a subfield in Ω. Let $\overline{K}$ be the set of elements in Ω which are algebraic over K. Then $K \subset \overline{K}$ is an algebraic closure of K.*

For instance, the set of algebraic numbers in $\mathbf{C}$ is an algebraic closure of $\mathbf{Q}$.

Proof. The extension $K \subset \overline{K}$ is algebraic by construction, for every element in $\overline{K}$ is algebraic over K.

Let $P \in \overline{K}[X]$ be a nonconstant polynomial and let us show that it has a root in $\overline{K}$. As $\overline{K} \subset \Omega$ and as Ω is algebraically closed, P has a root x in Ω. The element x is algebraic over $\overline{K}$ and since $\overline{K}$ is algebraic over K, x is also algebraic over K (Theorem 1.3.16). Therefore $x \in \overline{K}$ and P has a root in $\overline{K}$, as was to be shown. □

The proof of Steinitz's theorem is not very illuminating and relies upon a "transfinite induction" argument, hence requires the axiom of choice as soon as the field is not countable! We have shown how to add the roots of one polynomial, and all we have to do is to add roots for all of them, which requires the set of polynomials to be well-ordered.

Proof of Steinitz's theorem. Let K be a field whose algebraic closure is to be constructed. We are going to define an algebraic extension $K \to \Omega$ of K in which every polynomial of $K[X]$ is split. It will follow that Ω is an algebraic closure of K. Let P be a polynomial $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with coefficients in Ω. We have to show that P has a root in Ω. We may assume that P is irreducible. Since every coefficient a_i is algebraic over K, the subfield $L = K[a_0, \ldots, a_{n-1}] \subset \Omega$ which they generate is a finite algebraic extension of K. Necessarily P is irreducible in $L[X]$. Let us then introduce the finite algebraic extension $L \to L[X]/(P)$, in which P has a root α, with minimal polynomial P. Since L is algebraic over K, α is algebraic over K. Let Q denote its minimal polynomial in $K[X]$. As $Q(\alpha) = 0$, Q is a multiple of P in $L[X]$. By construction, Q is split in Ω. It follows that P is split too, so it has a root in Ω.

The method of constructing Ω consists of patiently "adding" the roots of every irreducible polynomial in $K[X]$. To that aim, endow the set $\mathscr{E}$ of all irreducible polynomials with a *well-ordering* $\prec$, that is, a total ordering such that every nonempty subset of $\mathscr{E}$ admits a least element. The standard ordering on $\mathbf{N}$ is a well-ordering and the existence of a well-ordering on any set is equivalent to the axiom of choice, or to Zorn's lemma. If K is countable, the set of all irreducible polynomials with coefficients in K is also countable and enumerating them gives us a well-ordering.

Once a set is well-ordered, the induction principle can be stated and proved in quite the same way as the classical induction over the integers. Let $(X, \prec)$ be a well-ordered set and let $\mathscr{P}$ be a property of elements in X. Assume that the following assertion holds (induction hypothesis):

> "Let $x \in X$; if, for every $y \in X$, $y \prec x$, $\mathscr{P}(y)$ is true, then $\mathscr{P}(x)$ is true."

Then $\mathscr{P}(x)$ is true for every $x \in X$. (Otherwise, the set of $x \in X$ such that $\mathscr{P}(x)$ does not hold admits a smallest element x_0. By definition, for every $y \prec x_0$, $\mathscr{P}(y)$ is true. By the assertion within quotes, $\mathscr{P}(x_0)$ is true; thus we have a contradiction. The first step of the induction, i.e. , checking $\mathscr{P}$ for the minimal element of X, follows by applying the induction hypothesis with $x = \min(X)$.)

Let us now show the existence of a family of algebraic extensions $j_P \colon K \to \Omega_P$, for $P \in \mathscr{E}$, in which P is split, and of homomorphisms $j_P^Q \colon \Omega_Q \to \Omega_P$ where P and Q are two polynomials in $\mathscr{E}$ with $Q \prec P$, satisfying $j_P = j_P^Q \circ j_Q$. (This means that Ω_P is an extension not only of K but also of all Ω_Q for $Q \prec P$.)

To show this by induction, two constructions are needed, where $P \in \mathscr{E}$.

– The first, which I do not want to do formally, is an *inductive limit* $\Omega_{\prec P}$ of all extensions Ω_Q with $Q \prec P$. This is essentially the union of all these fields; to compute in $\Omega_{\prec P}$, one chooses some Ω_Q where everything is defined and one computes there. Using the homomorphisms $j_{Q'}^Q$, one sees that the output of those calculations is essentially independent of the field where they were done. One has moreover homomorphisms $j_{\prec P}^Q \colon \Omega_Q \to \Omega_{\prec P}$.

– The second consists in adding to the field $\Omega_{\prec P}$ all roots of P; one defines Ω_P as a splitting extension of the polynomial P over the field $\Omega_{\prec P}$, hence a field homomor-

phism $j_P^{\prec P}\colon \Omega_{\prec P} \to \Omega_P$ which, composed with $j_{\prec P}^Q$, gives us the homomorphisms $j_P^Q\colon \Omega_Q \to \Omega_P$ we sought.

Once these (Ω_P, j_P^Q) are shown to exist, we define Ω as the inductive limit of all Ω_P.

To prove that two algebraic closures are isomorphic, we will use a theorem from the next chapter. Let $K \to \Omega'$ be an algebraic closure of K. We want to show that there exists a K-homomorphism from the algebraic closure we just constructed Ω to Ω'. Let us show by induction that there exists, for every $P \in \mathscr{E}$, a K-homomorphism $\alpha_P\colon \Omega_P \to \Omega'$ such that $\alpha_P \circ j_P^Q = \alpha_Q$ if $Q \prec P$. Let us now fix P. The homomorphisms $\alpha_Q\colon \Omega_Q \to \Omega'$ for $Q \prec P$, $Q \neq P$, define a field homomorphism from $\Omega_{\prec P}$, which is the inductive limit of the Ω_Q for $Q \prec P$, to Ω'. Applying Theorem 3.1.6 to the field Ω_P (which is a splitting extension of the polynomial P over $\Omega_{\prec P}$), there exists a morphism of field extensions $\Omega_P \to \Omega'$ which extends the morphism $\Omega_{\prec P} \to \Omega'$.

Together, the α_P define a K-homomorphism $\alpha\colon \Omega \to \Omega'$. Like any field homomorphism, α is injective. Let us show it is surjective. Let x be any element in Ω'. By definition, x is algebraic over K so let $P \in K[X]$ be its minimal polynomial. As Ω is an algebraic closure of K, P is split in Ω. Writing $P = \prod_{i=1}^{n}(X - x_i)$ in $\Omega[X]$, one then has

$$0 = P(x) = \prod_{i=1}^{n}(x - \alpha(x_i))$$

so that x is one of the $\alpha(x_i)$ and α is surjective, q.e.d. □

2.4 Appendix: Structure of polynomial rings

Recall that an *ideal* of a ring A is a subgroup $I \subset A$ such that for any $a \in A$ and $b \in I$, $ab \in I$. If a is any element of A, the *principal ideal* generated by a is the set of all ab for $b \in A$. We denote it aA or (a). Conversely, we say that a is a *generator* of the ideal (a).

Theorem 2.4.1. *For any ideal I in $K[X]$, there exists a polynomial $P \in K[X]$ such that $I = (P)$.*

An integral domain in which every ideal is a principal ideal is called a *principal ideal ring*.

Proof. We essentially have to redo the argument of Proposition 1.3.9 of which this theorem is a particular case: just take for I the set of all polynomials $P \in K[X]$ such that $P(x) = 0$. If $I = \{0\}$, simply set $P = 0$. Otherwise, let $d \geqslant 0$ be the smallest degree of a nonzero element in I and let $P \in I$ be a polynomial of degree d. Since I is an ideal, $PQ \in I$ for any $Q \in K[X]$, so $(P) \subset I$. Conversely, let A be an element in I and consider the Euclidean division $A = PQ + R$ of A by P. One has $PQ \in I$, so that $R = A - PQ$

belongs to I. By definition, $\deg R < \deg P = d$. The definition of d implies $R = 0$ and $A = PQ \in (P)$. □

Also notice that a nonzero ideal in $K[X]$ has many generators. However, if P and Q are two generators of a nonzero ideal, then there exists a constant $\lambda \in K^*$ such that $P = \lambda Q$. Indeed, P and Q divide each other; writing $P = RQ$ and $Q = SP$ implies that R and S are nonzero constants. Consequently, every nonzero ideal of $K[X]$ has a unique generator which is a monic polynomial.

Corollary 2.4.2 (Bézout's theorem for polynomials). *Let A and B be two polynomials. The set $I = (A, B)$ consisting of all $AP + BQ$ with P, $Q \in K[X]$ is an ideal in $K[X]$. If D is a generator of this ideal, then*

a) *there exist U and $V \in K[X]$ such that $D = AU + BV$;*
b) *D divides A and B;*
c) *every polynomial dividing both A and B divides D.*

Consequently, D is a *greatest common divisor* of A and B. Assume that A and B are not both equal to zero. Then the ideal (A, B) is nonzero and its generators differ only by the multiplication by a nonzero element of K. In this case, we will agree to call the g.c.d. of A and B the unique monic polynomial generating (A, B). Recall that two polynomials A and B are said to be *coprime* if their only common divisors are the constant polynomials. By the preceding corollary, this amounts to saying that there exist two polynomials U and V such that $AU + BV = 1$, a statement sometimes referred to as Bézout's theorem.

Proof. I leave as an exercise to the reader the task of checking that I is actually an ideal in $K[X]$. By the very definition of D, $D \in I$ and there exist U and V in $K[X]$ such that $D = AU + BV$, hence *a*).

Since $A = A\cdot 1 + B\cdot 0$, $A \in I$ and there exists $P \in K[X]$ such that $A = PD$. Similarly, there exists $Q \in K[X]$ such that $B = QD$. It follows that A and B are both multiples of D, so that *b*) holds.

Finally, if C divides A and B, write $A = CP$ and $B = CQ$ for some polynomials P and Q. The relation $D = AU + BV$ implies $D = CPU + CQV = C(PU + QV)$, so that C divides D, which shows *c*). □

From that, one deduces that the g.c.d. of two polynomials does not depend on the field in which it is computed.

Proposition 2.4.3. *Let $K \subset L$ be a field extension, and let A and B be two polynomials in $K[X]$. Then the g.c.d. of A and B as polynomials in $L[X]$ is equal to the g.c.d. of A and B computed in $K[X]$.*

Proof. Let D be the g.c.d. of A and B in $K[X]$ and let E be their g.c.d. in $L[X]$. As D divides A and B in $K[X]$, it divides them in $L[X]$ and D divides E. To show the other divisibility, choose U and V in $K[X]$ such that $D = AU + BV$. As E divides A and B, it has to divide D! Since D and E are monic polynomials dividing each other, they are equal. □

One also deduces from Bézout's theorem the so-called Gauss's lemma, which is a crucial point in the proof that polynomial rings have the "unique factorization" property.

Lemma 2.4.4 (Gauss's lemma). *Let P be an irreducible polynomial in $K[X]$. Let A and B be two polynomials in $K[X]$ such that P divides AB. Then P divides A or P divides B.*

Proof. Assume that P does not divide A. Since P is irreducible, its only divisors are the constant polynomials $\lambda \in K^*$ and the multiples λP for $\lambda \in K^*$. Among those, only the constants divide A, so that A and P are coprime. By Bézout's theorem, we may find polynomials U and V such that $AU + PV = 1$. Multiplying this relation by B, one gets $ABU + PBV = B$. As P divides AB, one may write $AB = PQ$. Finally, $B = P(QU + BV)$ is a multiple of P, q.e.d. □

Theorem 2.4.5. *Any nonzero polynomial A in $K[X]$ admits a decomposition $A = a\prod_{i=1}^{m} P_i^{n_i}$ with $a \in K^*$, $m \geqslant 0$, P_i distinct monic irreducible polynomials, and n_i positive integers.*

Moreover, if $A = a'\prod_{j=1}^{m'} Q_j^{n'_j}$ is another decomposition, one has $a = a'$, $m = m'$ and there exists a permutation σ of $\{1, \ldots, m\}$ such that for every i, $P_i = Q_{\sigma(i)}$ and $n_i = n'_{\sigma(i)}$.

One says that the ring $K[X]$ is a *factorial ring* or a *unique factorization domain* (or ring).

Proof. The existence of such a decomposition is shown by induction on the degree of A. If A is irreducible, one just writes $A = aP$ where P is irreducible and monic and a is the leading coefficient of A. Otherwise, one may write $A = A_1A_2$ with two polynomials A_1 and A_2 whose degrees are less than $\deg A$, and we conclude by induction.

Uniqueness is the important point, and to prove that we also argue by induction. Considering the leading coefficients, we see at once that $a = a'$. The

polynomial P_1 is irreducible and divides A. By Gauss's lemma, it divides one of the Q_j, say $Q_{\sigma(1)}$. Since $Q_{\sigma(1)}$ is irreducible, P_1 and $Q_{\sigma(1)}$ are multiples one of another; being monic, they are equal. Now apply the inductive hypothesis to A/P_1. □

Let us give the general definition of a factorial ring.

Definition 2.4.6. *Let A be an integral domain. One says an element a in A is* irreducible *if* a) *a is not invertible in A;* b) *for any x and y in A such that $a = xy$, either x or y is invertible in A.*

One says the ring A is factorial *if the following two properties hold:*

a) *for every nonzero element $a \in A$, there exists an integer $r \geqslant 0$, irreducible elements $p_1, \dots, p_r$ and a unit u with $a = up_1 \dots p_r$* (existence of a decomposition into irreducible factors)*;*

b) *if $a = up_1 \dots p_r$ and $a = vq_1 \dots q_s$ are two decompositions then $r = s$ and there exists a permutation σ of $\{1, \dots, r\}$ and units u_j ($1 \leqslant j \leqslant r$) such that for every j, $q_j = u_j p_{\sigma(j)}$* ("uniqueness" of the decomposition in irreducible factors).

In a factorial ring, any two nonzero elements have a g.c.d., which is well defined up to multiplication by a unit. The arguments of this Section show that any principal ideal ring is a factorial ring. See Exercises 2.6 and 2.7 for applications.

Theorem 2.4.7 (Gauss). *If A is a factorial ring, then $A[X]$ is a factorial ring too.*

The proof begins by describing the irreducible elements in $A[X]$; besides the irreducible elements in A, these are polynomials in $A[X]$ whose coefficients are coprime and which are irreducible as coefficients in K, where K denotes the field of fractions of A. Now we shall generalize the result proved in Exercise 1.9 to arbitrary factorial rings. Let the *content* of a nonzero polynomial in $A[X]$ be the g.c.d. of its coefficients. Then, *if P and Q are two nonzero polynomials in $A[X]$, the content of their product PQ is equal to the product of the contents of P and Q* (up to a unit).

A field is a factorial ring, and so is the ring of integers. The following important corollary follows by induction.

Corollary 2.4.8. *The rings $\mathbf{Z}[X_1, \dots, X_n]$ and, if K is a field, $K[X_1, \dots, X_n]$, are factorial rings.*

2.5 Appendix: Quotient rings

In this section, I explain how the construction of the ring of remainders done in Section 2.1 can be generalized.

The situation is as follows. One is given a ring A and an ideal I of A; the goal is to construct a *quotient ring*, which will be denoted A/I, and a surjective ring homomorphism $\pi\colon A \to A/I$ with kernel I. Therefore two elements a and b have the same image in A/I if and only if their difference $a - b$ belongs to I; one then says that a and b are in the same *residue class modulo* I. (*Exercise:* check that this is an equivalence relation.) In Section 2.1, we considered the case where $A = K[X]$ and $I = (P)$ is the ideal generated by a polynomial $P \in K[X]$. In that case, the remainder in the Euclidean division of a polynomial by P gives us a canonical element in the residue class modulo I of any polynomial in $K[X]$. When $A = \mathbf{Z}$ and $I = (n)$, one still has a canonical element in each class, for instance, the integers in the set $\{0, \ldots, n-1\}$. This will be the case in any *Euclidean ring*, that is, in any ring admitting some kind of Euclidean division, but not in general. Such a difficulty should not bother us too much. The choice of this element has no importance at all and any element will do. A more elegant way consists of defining A/I as *the set of all residue classes modulo* I so that elements of A/I are just subsets of A; instead of choosing some element, we take them all together. If $a \in A$, let us denote by $\overline{a}$ the class of a in A/I. We define a map $\pi\colon A \to A/I$ by the simple formula $\pi(a) = \overline{a}$.

To say that A/I is a ring and that π is a ring homomorphism amounts to saying that addition and multiplication in A/I are defined to be compatible with those of A and with the map $a \mapsto \overline{a}$. One thus needs to check that if $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$, $\overline{a+c} = \overline{b+d}$ and $\overline{ac} = \overline{bd}$, for this will allow us to define addition and multiplication in A/I by the formulae $\overline{a} + \overline{c} = \overline{a+c}$ and $\overline{a} \cdot \overline{c} = \overline{ac}$. But $(b+d) - (a+c) = (b-a) + (c-d)$ and $bd - ac = (b-a)d + a(d-c)$ are both the sum of two elements in I, so belong to I. The other axioms of a ring structure and of a ring homomorphism are checked in the same way.

If I is an ideal in A, it may be interesting to express the algebraic properties that the quotient ring A/I might possess, in terms of the ideal I.

Proposition 2.5.1. a) *The ring A/I is null if and only if $A = I$;*

b) *the ring A/I is an integral domain if and only if $I \neq A$ and if for any x and y in $A \setminus I$, $xy \notin I$;*

c) *the ring A/I is a field if and only if $I \neq A$ and if the only ideals of A containing I are I and A.*

In case b), one says I is a *prime ideal*; in case c), it is a *maximal ideal*.

Proposition 2.5.2. *Let A be a principal ideal ring which is not a field. Then its prime ideals are* a) *the null ideal* (0)*;* b) *the ideals generated by a irreducible element.*

Among these, only the null ideal is not maximal.

The following abstract theorem concerns the existence of prime or maximal ideals in an arbitrary ring.

Theorem 2.5.3 (Krull). *Let A be a ring. Every ideal of A not equal to A is contained in a maximal ideal.*

Proof. Let I be an ideal in A, with $I \neq A$. Let us endow A with a well-ordering $\prec$.

We will define by induction increasing families $(J_x)_{x\in A}$ and $(I_x)_{x\in A}$ of ideals of A, satisfying $I \subset J_x \subset I_x \neq A$, as follows.

If x is the minimal element of A, set $J_{\prec x} = I$.

Let $x \in A$, distinct from the minimal element of A, and assume that I_y has been constructed for $y \prec x$. We first set $J_x = \bigcup_{y\prec x} I_y$; since the union is increasing, observe that J_x is an ideal of A. Indeed, let a, $a' \in I_{\prec x}$; there are y and $y' \prec x$ such that $a \in I_y$ and $a' \in I_{y'}$. Since the ordering $\prec$ is total, one has $y \preceq y'$ or $y' \preceq y$. In the first case, $I_y \subset I_{y'}$, hence $a + a' \in I_{y'}$; in the second case, $a + a' \in I_y$. Consequently, $a + a' \in I_{\prec x}$. Let $a \in I_{\prec x}$ and $b \in A$. If $y \prec x$ is such that $a \in I_y$, one has $ba \in I_y$, hence $ba \in I_{\prec x}$.

Since $1 \notin I_y$ for $y \prec x$, $1 \notin J_x$ and $J_x \neq A$. Moreover, J_x contains all I_y for $y \prec x$, hence J_x contains I.

Finally, consider the ideal $J_x+(x)$. If it is distinct from A, set $I_x = J_x+(x)$; otherwise, set $I_x = J_x$.

It remains to set $J = \bigcup_{y\in A} I_x$. Since the family (I_x) is increasing, this is an ideal of A, not equal to A. Moreover, for any $x \in A \setminus J$, one has $x \notin I_x$, hence $A = J_x + (x)$ by construction, and $A = J + (x)$ *a fortiori*. This shows that the ideal J is a maximal ideal of A. □

Corollary 2.5.4. *Let A be a ring. An element in A is invertible if and only if no maximal ideal contains it.*

Proof. Let $I = (a)$ be the ideal generated by the element $a \in A$. If a is invertible, there exists $b \in A$ such that $ab = 1$, so that $1 \in I$, hence $I = A$ and I cannot be contained in a maximal ideal. Consequently, there is no maximal ideal in A containing a. Conversely, if a is not a unit, $I \neq A$. By Krull's theorem 2.5.3, there is a maximal ideal containing I and this maximal ideal automatically contains a. □

2.6 Appendix: Puiseux's theorem

This appendix is devoted to Puiseux's theorem, a result which can be viewed in two different ways:

– from an analytic point of view, it shows that solutions of a polynomial equation whose coefficients are holomorphic functions (power series) can be *parametrized* and give holomorphic functions in a parameter $t^{1/n}$;

– for the algebraist, it describes explicitly the algebraic closure of the field of meromorphic functions in a neighborhood of the origin.

If $r > 0$, $\mathscr{A}(r)$ denotes the set of continuous functions on the closed disk $\overline{D}(0,r) \subset \mathbf{C}$ whose restriction to the open disc $D(0,r)$ is holomorphic. This is a ring; by the principle of isolated zeroes, it is an integral domain. For $f \in \mathscr{A}(r)$, set $\|f\| = \sup_{|z| \leqslant r} |f(z)|$. This is a norm on $\mathscr{A}(r)$, and it defines on it the topology of uniform convergence. A uniform limit of continuous functions is continuous, and a uniform limit of holomorphic functions is again holomorphic. It follows that this norm endows $\mathscr{A}(r)$ with the structure of a Banach space, and even with the structure of a *Banach algebra* since one has $\|fg\| \leqslant \|f\| \, \|g\|$ for any f and g in $\mathscr{A}(r)$.

A function f in $\mathscr{A}(r)$ has the power-series expansion

$$f(z) = \sum_{n=0}^{\infty} a_n z^n,$$

which converges for $|z| < r$, as can be seen, *e.g.*, using Cauchy estimates of derivatives of analytic functions. Two different functions have two different expansions, which will enable us to identify elements of $\mathscr{A}(r)$ to some power-series. A word on notation: we shall have to manipulate polynomials with coefficients in $\mathscr{A}(r)$, *i.e.* polynomials the coefficients of which are *functions*. We shall denote by X the polynomial indeterminate, and by z the argument of functions in $\mathscr{A}(r)$. For example, in the next theorem, $P(z^e, X)$ is the polynomial of $\mathbf{C}[X]$ obtained by evaluating each coefficient of the polynomial $P \in \mathscr{A}(r)[X]$ at z^e.

Theorem 2.6.1 (Puiseux). *Let P be a monic polynomial of degree n with coefficients in $\mathscr{A}(r)$. There exists an integer $e \geqslant 1$, a real number $\rho \in (0, r^{1/e}]$, and functions $x_1, \ldots, x_n \in \mathscr{A}(\rho)$ such that*

$$P(z^e, X) = \prod_{i=1}^{n} (X - x_i(z)).$$

In particular, for $|z| < r$, the n roots of the polynomial $P(z)$ are parametrized by power series $x_i(z^{1/e})$ in a fractional power of z. Let us give some simple examples that show the necessity of introducing such a fractional power, and also that the radius of convergence of the solutions can be smaller than the one of the coefficients.

a) The roots of $P = X^2 - 2zX - 1$ are

$$x_1(z) = z + \sqrt{1+z^2} = 1 + z + \sum_{n=1}^{\infty} \binom{1/2}{n} z^{2n}$$

and

$$x_2(z) = z - \sqrt{1+z^2} = -1 + z + \sum_{n=1}^{\infty} \binom{1/2}{n} (-1)^n z^{2n},$$

two power series converging for $|z| < 1$.

b) The roots of $P = X^2 - z(1+z)$ are

$$\pm z^{1/2}\sqrt{1+z} = \pm \sum_{n=0}^{\infty} \binom{1/2}{n} (z^{1/2})^{2n+1},$$

two power series converging for $|z| < 1$. In that case, one has $e = 2$.
Theorem 2.6.1 is proved by induction on n.

Proposition 2.6.2. *Let $P \in \mathscr{A}(r)[X]$ be a monic polynomial with degree n. Let Q_0 and $R_0 \in \mathbf{C}[X]$ be two monic polynomials of degrees $< n$, such that $P(0,X) = Q_0(X)R_0(X)$. If Q_0 and R_0 are coprime, then there exists $\rho \in (0,r]$ and two monic polynomials Q and R with coefficients in $\mathscr{A}(\rho)$, such that $Q(0,X) = Q_0(X)$, $R(0,X) = R_0(X)$ and $P = QR$.*

Proof. This is an application of the implicit function theorem, in its holomorphic version. To prove it, however, we will go back to Banach's fixed-point theorem.

Set $P_0 = P(0,X)$ and let $P_1 \in \mathscr{A}(r)[X]$ be such that $P = P_0 + zP_1$. Let $m = \deg Q_0$, $p = \deg R_0$; one has $m + p = n$. We are looking for Q and R such that $Q = Q_0 + zU$ and $R = R_0 + zV$, where U has degree $< m$ and V has degree $< p$. The equation $P = QR$ can be rewritten as

$$P_1 = UR_0 + VQ_0 + zUV.$$

If a is an integer, identify $\mathbf{C}^a$ with polynomials of degree $< a$ and introduce the linear map $\varphi\colon \mathbf{C}^m \times \mathbf{C}^p \to \mathbf{C}^{m+p}$ defined by $\varphi(U,V) = UR_0 + VQ_0$. It is *injective*, for if $\varphi(U,V) = 0$, R_0 divides VQ_0 but is prime to Q_0, so it divides V. Since $\deg V < p = \deg Q_0$, that forces $V = 0$. Similarly $U = 0$. Like any injective linear map between vector spaces of the same finite dimension, φ is an isomorphism, the inverse of which, $\varphi^{-1}\colon \mathbf{C}^{m+p} \to \mathbf{C}^m \times \mathbf{C}^p$, is also linear.

Similarly, identify $\mathscr{A}(r)^a$ with polynomials of degree $< a$ with coefficients in $\mathscr{A}(r)$ and let us consider the map $\Phi\colon \mathscr{A}(r)^m \times \mathscr{A}(r)^p \times \mathscr{A}(r)^{m+p}$ given by $\Phi(U,V) = UR_0 + VQ_0$, U and V being polynomials with coefficients in $\mathscr{A}(r)$ of degrees $< m$ and $< p$. By construction, one $\Phi(U,V)(z) = \varphi(U(z),V(z))$

for any $z \in \overline{D}(0,r)$. The map Φ is bijective and its inverse is the map $\Psi\colon \mathscr{A}(r)^{m+p} \to \mathscr{A}(r)^m \times \mathscr{A}(r)^p$ defined by $\Psi(P)(z) = \varphi(P(z))$. The equation $P = QR$ can thus be rewritten as

$$(U,V) = \Psi(P_1 - zUV).$$

The right hand side of this equation will be denoted by $T(U,V)$.

For any integer a, endow $\mathscr{A}(r)^a$ with the norm $\|(f_1,\dots,f_a)\| = \|f_1\| + \cdots + \|f_a\|$. Again, this a Banach space. The linear maps Φ and Ψ are continuous and Lipschitz with these norms. In fact, if $\mathbf{C}^a$ is endowed with the norm $\|(z_1,\dots,z_a)\| = |z_1| + \cdots + |z_a|$, then their Lipschitz constants are the same as those of φ and φ^{-1}. Set $A = \|\Psi\|$.

For any $U \in \mathscr{A}(r)^m$ and $V \in \mathscr{A}(r)^p$, one has $\|UV\| \leqslant \|U\|\,\|V\|$. In fact, writing $U = f_0 + f_1X + \cdots + f_{m-1}X^{m-1}$ and $V = g_0 + g_1X + \cdots + g_{p-1}X^{p-1}$, one has

$$\begin{aligned}\|UV\| = \sum_{j=0}^{m+p-1} \left\| \sum_{k+\ell=j} f_k g_\ell \right\| &\leqslant \sum_{j=0}^{m+p-1} \sum_{k+\ell=j} \|f_k\|\,\|g_\ell\| \\ &\leqslant \sum_{k=0}^{m-1} \|f_k\| \sum_{\ell=0}^{p-1} \|g_\ell\| \leqslant \|U\|\,\|V\|\,.\end{aligned}$$

It follows that the map T from $\mathscr{A}(r)^m \times \mathscr{A}(r)^p$ to itself satisfies

$$\|T(U,V)\| \leqslant A\,\|P_1\| + Ar\,\|U\|\,\|V\|\,.$$

If R and r are real numbers satisfying $R > A\,\|P_1\|$, and if $r < r_1 = (R - A\,\|P_1\|)/AR^2$, then the ball B_R defined by $\|U\| + \|V\| \leqslant R$ in $\mathscr{A}(r)^{m+p}$ is stable under T.

Moreover, if (U,V) and $(U',V') \in B_R$,

$$\begin{aligned}\|T(U,V) - T(U',V')\| &= \|\Psi(-zUV + tU'V')\| \\ &\leqslant Ar\,\|UV - U'V'\| \\ &\leqslant Ar\,\|U(V-V') + V'(U-U')\| \\ &\leqslant ArR\big(\,\|U-U'\| + \|V-V'\|\,\big).\end{aligned}$$

Consequently, if $r < r_2 = 1/AR$, T is a contracting map.

It remains to observe that we can fix some $R > A\,\|P_1\|$ and then choose $\rho < \min(r, r_1, r_2)$. With those choices, the linear map T from $\mathscr{A}(\rho)^m \times \mathscr{A}(\rho)^p$ to itself stabilizes the ball B_R defined by $\|U\| + \|V\| \leqslant R$ and is contracting there. By Banach's fixed point theorem, T has a unique fixed point in B_R, hence a factorization $P = QR$ in the ring $\mathscr{A}(\rho)[X]$. □

This first step (Proposition 2.6.2) will allow us to assume that $P(0,X)$ has a unique root. Consider a factorization $P(0,X) = \prod_j (X - z_j)^{n_j}$, with *distinct* complex numbers z_j; by the Proposition, it extends to a factorization $P = \prod_j P_j$, with $P_j \in \mathscr{A}(\rho)[X]$ and $P_j(0,X) = (X - z_j)^{n_j}$. Assume that for any j, the polynomial P_j satisfies the conclusion of Puiseux's Theorem, i.e. , that there exists $e_j \geqslant 1$, and functions $x_{j,i} \in \mathscr{A}(\rho_j)$, $1 \leqslant i \leqslant n_j$, such that

$$P_j(z^{e_j}, X) = \prod_{j=1}^{n_j} (X - x_{j,i}(z)).$$

Then we may set $e = \mathrm{l.c.m.}(e_1, \dots, e_j, \dots)$ and $f = j = e/e_j$, so that

$$P(z^e, X) = \prod_j P_j\big((z^{f_j})^{e_j}, X\big) = \prod_j \prod_{i=1}^{n_j} \big(X - x_{j,i}(z^{f_j})\big),$$

which proves the assertion of Puiseux's theorem for P, with $\rho = \min(\rho_j^{1/f_j})$.

Consequently, we can assume that $P(0,X)$ has a unique root α. Replacing the polynomial $P = X^n + a_1 X^{n-1} + \dots$ by $P(X - a_1/n)$, we may moreover assume that the coefficient of X^{n-1} in P is zero, which means that the sum of all roots of P is zero. In particular, $\alpha = 0$ and $P(0,X) = X^n$.

The next proposition refers to the order of vanishing at zero of a nonzero function $f \in \mathscr{A}(r)$: if its expansion as a power series is $f = \sum_{n \geqslant 0} a_n z^n$, the order of vanishing at zero of f is the smallest integer n such that $a_n \neq 0$. It is also the highest power of z dividing f. We will denote it by $v(f)$.

Proposition 2.6.3. *Let $P = X^n + a_2 X^{n-2} + \dots + a_n$ be a monic polynomial with coefficients in $\mathscr{A}(r)$. Let $\nu = \min_{2 \leqslant j \leqslant n} v(a_j)/j$; write $\nu = m/e$ where m and e are two coprime nonnegative integers. Then there exists a monic polynomial Q, of degree n, with coefficients in $\mathscr{A}(r^{1/e})$ such that*

$$z^{mn} Q(z, X) = P(z^e, z^m X).$$

At $z = 0$, $Q(0,X) \neq X^n$.

Before we prove this proposition, let us finish the proof of Puiseux's theorem. Since $Q(0,X) \neq X^n$, and since the sum of its roots is zero, not all of the roots of $Q(0,X)$ are equal and Proposition 2.6.2 allows us to factor Q as $Q = RS$ (in a certain $\mathscr{A}(\rho)$). By induction, we thus see that there exist an integer $f \geqslant 1$, a real number ρ and power series $y_j(z) \in \mathscr{A}(\rho)$ such that

$$Q(z^f, X) = \prod_{j=1}^{n} (X - y_j(z)).$$

Thus

$$P(z^{ef}, z^m X) = z^{mn} \prod_{j=1}^{n} (X - y_j(z^f))$$

and

$$P(z^{ef}, X) = \prod_{j=1}^{n} (X - z^m y_j(z^f)),$$

so that the $x_j = z^m y_j(z^f)$ are the power series we were searching for.

Proof of Proposition 2.6.3. In the expansion

$$P(z^e, z^m X) = \sum_{j=0}^{n} a_j(z^e) z^{m(n-j)} X^{n-j},$$

the coefficient $a_j(z^e)z^{m(n-j)}$ is a power series whose order of vanishing at 0 is equal to $ev(a_j)+m(n-j) = mn+e(v(a_j)-j\nu) \geqslant mn$. Therefore one can find a power series $b_j \in \mathscr{A}(r^{1/e})$ such that $a_j(z^e)t^{m(n-j)} = z^{mn}b_j(z)$. Moreover, if the integer $j \geqslant 2$ is chosen so that $v(a_j)/j = \nu$, one has $v(b_j) = 0$, which means $b_j(0) \neq 0$. Consequently, $Q(0) \neq X^n$. □

Exercises

Exercise 2.1. **a)** If $d_1, \ldots, d_r$ are positive integers, show that $d_1! \ldots d_r!$ divides $(d_1 + \cdots + d_r)!$.

b) Following the steps of the construction of a splitting extension for a polynomial of degree d, show that it is a finite extension and that its degree divides $d!$.

Exercise 2.2. Let p be a prime number, $p \geqslant 3$.

a) Show that $\prod_{a \in (\mathbf{Z}/p\mathbf{Z})^*} a = -1$ (*Wilson's theorem*). — Hint: in the product, group a and $1/a$, provided they are distinct.

b) For $a \in (\mathbf{Z}/p\mathbf{Z})^*$, let $S_a = \{a, -a, 1/a, -1/a\}$. Show that for a and b in $(\mathbf{Z}/p\mathbf{Z})^*$, either $S_a = S_b$, or $S_a \cap S_b = \emptyset$.

c) Computing the cardinality of S_a according to whether $a^2 = \pm 1$ or not, show that -1 is a square in $(\mathbf{Z}/p\mathbf{Z})^*$ if and only if $p \equiv 1 \pmod 4$. If it exists, can you find a formula for a square root of -1?

Exercise 2.3. An algebraically closed field is infinite.

Exercise 2.4. Let K be a field, p a prime number and let a be an element in K. Show that the polynomial $X^p - a$ is reducible in $K[X]$ if and only if it has a root in K. (If $X^p - a = P(X)Q(X)$, what can $P(0)$ be equal to?)

Exercise 2.5 (Gauss). For $n \in \mathbf{N}^*$, let $\Phi_n \in \mathbf{C}[X]$ be the monic polynomial with simple roots, given by the primitive nth roots of unity in $\mathbf{C}$.

a) Show that $\prod_{d|n} \Phi_d = X^n - 1$. Deduce by induction that for any n, $\Phi_n \in \mathbf{Z}[X]$.

Let ζ be any primitive nth root of unity and let $P \in \mathbf{Q}[X]$ be its monic minimal polynomial.

b) Show that P has integer coefficients and that it divides Φ_n.

c) Let p be a prime number. Show that there exists a polynomial $Q \in \mathbf{Z}[X]$ such that $P(X^p) - P(X)^p = pQ(X)$. Prove the existence of $b \in \mathbf{Z}[\zeta]$ such that $P(\zeta^p) = pb$.

d) Let p be a prime number that does not divide n. If $P(\zeta^p) \neq 0$, show by differentiating the polynomial $X^n - 1$ that there exists $c \in \mathbf{Z}[\zeta]$ with $n\zeta^{n-1} = pc$. Deduce from that a contradiction, hence $P(\zeta^p) = 0$.

e) Show that $P = \Phi_n$, that is the polynomial Φ_n is irreducible in $\mathbf{Q}[X]$.

Exercise 2.6. Let A be the subring $\mathbf{Z}[i]$ in $\mathbf{C}$ (ring of Gaussian integers).

a) Show that for any a and b in A, with $b \neq 0$, there exist q and r in A with $a = bq + r$ and $|r| < |b|$.

b) Show that A is a principal ideal ring. In particular, it is a factorial ring.

c) Let p be a prime number. Show that one of the following is true: 1) either p is irreducible in A; or 2) there exist a and b in $\mathbf{N}$ such that $p = a^2 + b^2$, and $p = (a+ib)(a-ib)$ is a decomposition of p as a product of irreducible elements in A.

d) Show that prime numbers congruent to 3 modulo 4 are irreducible in A. Show that 2 is not.

e) Let p be a prime number. Define a ring isomorphism from A/pA to the ring $(\mathbf{Z}/p\mathbf{Z})[X]/(X^2+1)$. Deduce that p is reducible in A if and only if the polynomial $X^2 + 1$ has a root in the field $\mathbf{Z}/p\mathbf{Z}$. By Exercise 2.2, this happens exactly when p is equal to 1 modulo 4.

In particular, prime numbers equal to 1 modulo 4 are sums of two squares of integers (Fermat, 1659).

Exercise 2.7 (Every integer is a sum of four squares). Let $\mathbf{H}$ be the noncommutative field of quaternions. We identify it with $\mathbf{Q}^4$, the canonical basis of which is denoted $(1, i, j, k)$ and with multiplication defined by $i^2 = j^2 = k^2 = -1$ and $ij = k$.

a) If $z = a + bi + cj + dk \in \mathbf{H}$, set $\overline{z} = a - bi - cj - dk$ and $N(z) = z\overline{z}$. Show that $N(z) = a^2 + b^2 + c^2 + d^2$ and that $N(zz') = N(z)N(z')$. Conclude that if two integers are sums of four squares of integers, then their product is again a sum of four squares.

b) Show that the set A_0 of $x + yi + zj + tk \in \mathbf{H}$ with x, y, z, $t \in \mathbf{Z}$ is a (noncommutative) subring of $\mathbf{H}$.

c) Let $\varepsilon = (1 + i + j + k)/2$. Compute ε^2. Show that the set A of all $a \in \mathbf{H}$ such that either $a \in A_0$ or $a - \varepsilon \in A_0$ is a subring of $\mathbf{H}$.

If $z \in A$, show that $N(z) \in \mathbf{N}$. (This is clear for $z \in A_0$. Otherwise, find $u = \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \in A^*$ and $b \in A_0$ with $z = u + 2b$. Observe that zu^{-1} belongs to A_0.) Show also that $z \in A$ is invertible if and only if $N(z) = 1$.

d) Show that A is a Euclidean ring: if a and $b \in A$, with $b \neq 0$, find q and $r \in A$ with $N(r) < N(b)$ and $a = bq + r$. Deduce that any (left) ideal in A is a principal ideal (of the form Az for some $z \in A$).

e) Let p be an odd prime number. Show that there exist integers a and b such that $a^2 + b^2 + 1$ is divisible by p. (How many elements of $\mathbf{Z}/p\mathbf{Z}$ are of the form $x^2 + 1$? and of the form $-y^2$?) Let I be the left ideal in A generated by p and $1 + ai + bj$. If $I = Az$, show that $N(z) = p$ and conclude that p is a sum of four squares of integers.

f) Show that for any integer $n \geqslant 0$, there exist integers a, b, c and d such that $n = a^2 + b^2 + c^2 + d^2$; any positive integer is a sum of four squares of integers (Lagrange, 1770).

Exercise 2.8. Prove that the only ideals of a field are itself and the null ideal. Conversely, show that a nonzero ring admitting only these two ideals is a field.

Exercise 2.9. Let A be the subring $\mathbf{Z}[\sqrt{-5}]$ in $\mathbf{C}$.

a) Show that any element of A can be written in a unique way as $a + b\sqrt{-5}$ with integers a and b. Show that the map $N\colon A \to \mathbf{Z}$ defined by $N(a+b\sqrt{-5}) = a^2+5b^2$ satisfies $N(xy) = N(x)N(y)$.

b) Show that an element $x \in A$ is a unit if and only if $N(x) = 1$.

c) Show that the elements 2, 3, $1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ are irreducible in A.

d) Conclude that A is not a factorial ring.

Exercise 2.10. Let A be a ring.

a) Let I and J be two ideals of A. Show that the set $I+J$ consisting of sums $a+b$ with $a \in I$ and $b \in J$ is an ideal of A.

b) Let I be an ideal in A. Let R_I be the set of $a \in A$ such that there exists $n \in \mathbf{N}$ with $a^n \in I$. Show that R_I is an ideal in A, and that it contains I. If $I \neq A$, show that $R_I \neq A$.

c) If $A = \mathbf{Z}$, $I = (12)$, compute R_I. Generalize to any principal ideal ring.

Exercise 2.11. Let K be a field.

a) Show that the two polynomials X and Y in $K[X, Y]$ are coprime.

b) Let $I = (X, Y)$ be the ideal in $K[X, Y]$ that they generate. Show that for any polynomial $P \in I$, one has $P(0, 0) = 0$. Conclude that there is no U and V in $K[X, Y]$ such that $UX + VY = 1$.

c) Show that the map $A \to K$, $P \mapsto P(0, 0)$ is a ring morphism, with kernel I. Show that I is a maximal ideal in $K[X, Y]$.

Exercise 2.12. One says that a ring A is a *Noetherian ring* if any ideal in A is generated by a finite number of its elements.

a) If K is a field, show that $K[X]$ is Noetherian.

b) If A is Noetherian and if I is an ideal in A, show that the quotient ring A/I is Noetherian too.

c) Show that a ring is Noetherian if and only if any increasing sequence of ideals is ultimately constant.

Exercise 2.13 (Hilbert's theorem). Let A be a Noetherian ring and let $B = A[X]$. This exercise aims to prove that B is also a Noetherian ring. Let I be an ideal in $A[X]$.

For any integer n, let J_n be the ideal in A generated by the leading coefficients of polynomials $P \in I$ which have degree n.

a) Show that for any n, $J_n \subset J_{n+1}$. Deduce that there exists an integer N with $J_n = J_N$ for $n \geqslant N$.

b) For any integer n, show that there exist polynomials $P_{n,1}, \ldots, P_{n,m_n} \in I$ of degree n whose leading coefficients generate J_n.

c) Show that the polynomials $P_{n,j}$ for $n \leqslant N$ and $1 \leqslant j \leqslant m_n$ generate I. (Proceed by induction on the degree: if I_0 denotes the ideal of B generated by these polynomials, and if $P \in I$ has degree n, construct a polynomial $P_n \in I_0$ such that $P - P_0$ has degree $\leqslant n - 1$.)

d) For any field K, show that $K[X_1, \ldots, X_n]$ is a Noetherian ring. Similarly, show that $\mathbf{Z}[X_1, \ldots, X_n]$ is a Noetherian ring.

Exercise 2.14. In a factorial ring, irreducible elements generate prime ideals.

http://www.springer.com/978-0-387-21428-3

A Field Guide to Algebra
Chambert-Loir, A.
2005, X, 198 p., Hardcover
ISBN: 978-0-387-21428-3