ALGEBRAIC GEOMETRY OF SCHEMES

Antoine Chambert-Loir

Antoine Chambert-Loir
Laboratoire de mathématiques, Université Paris-Sud,
Bât. 425, Faculté des sciences d'Orsay, F-91405 Orsay Cedex.
E-mail : antoine.chambert-loir@u-psud.fr

Version of January 8, 2015, 0h49
The most up-do-date version of this text should be accessible online at address
http://www.math.u-psud.fr/~chambert/enseignement/2014-15/ga/ag.pdf

CONTENTS

CHAPTER 1

COMMUTATIVE ALGEBRA

1.1. Recollections (Uptempo)

1.1.1. Basic algebraic structures. — The concepts of *groups*, *rings*, *fields*, *modules* are assumed to be known, as well as the notion of morphisms of groups, rings, fields, modules, etc.

In this course, rings are always commutative and possess a unit element, generally denoted by 1. The multiplicative group of invertible elements of a ring A will be denoted by A^* or $A^\times$.

1.1.2. Algebras. — Let k be a ring. A *k-algebra* is a ring A endowed with a morphism of rings $f\colon k \to A$. When this morphism is injective, we will often understate the morphism f and consider that A is an overring of k, or that k is a subring of A... Let $(A, f\colon k \to A)$ and $(B, g\colon k \to B)$ we two k-algebras; a morphism of k-algebras is a ring morphism $\varphi\colon A \to B$ such that $g = \varphi \circ f$.

1.1.3. Polynomial algebras. — Let I be a set. One defines a k-algebra $k[(X_i)_{i\in I}]$ of polynomials with coefficients in k in a family $(X_i)_{i\in I}$ of indeterminates indexed by I. This algebra satisfies the following universal property: for every family $(a_i)_{i\in I}$ of elements of A, there exists a unique morphism $\varphi\colon k[(X_i)_{i\in I}] \to A$ of k-algebras such that $\varphi(X_i) = a_i$ for every $i \in I$. In other words, for every k-algebra A, the canonical map

$$\mathrm{Hom}_{k-\boldsymbol{Algebras}}(k[X_i], A) \to \mathrm{Hom}_{\boldsymbol{Ens}}(I, A), \qquad \varphi \mapsto (i \mapsto \varphi(X_i))$$

is a bijection.

When I has one, two, three,... elements, the indeterminates are often denoted by individual letters, say X, Y, Z,...

Let J be a subset of I, and let K be its complementary subset. The polynomial algebra $k[(X_i)_{i\in I}]$ is isomorphic to the polynomial algebra $k[(X_i)_{i\in J}][(X_i)_{i\in K}]$

in the indeterminates X_i (for $i \in K$) with coefficients in the polynomial algebra $k[(X_i)_{i\in J}]$ with coefficients in k in the indeterminates X_i (for $i \in J$).

We do not detail the notion of *degree* in one of the indeterminates (of degree, if I is a singleton).

There is a notion of euclidean division in polynomial rings. Let A be a ring, let $f, g \in A[X]$ be polynomials in one indeterminate X with coefficients in A. If the leading coefficient of g is invertible in A, there exist a unique pair (q, r) of polynomials in $A[X]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.

1.1.4. Ideals. — An *ideal* of a ring A is a non-empty subset I which is stable under addition, and such that $ab \in I$ for every $a \in A$ and every $b \in I$. In other words, this is a A-submodule of A.

The subsets $\{0\}$ and A are ideals. The intersection of a family of ideals of A is an ideal. If S is a subset of A, the ideal generated by S is the smallest ideal of A containing S (it is the intersection of all ideals of A which contain S). Let I and J be ideals of A; the ideal $I + J$ (resp. the ideal $I \cdot J$, also denoted by IJ) is the ideal generated by the set of sums $a + b$ (resp. the set of products ab) for $a \in I$ and $b \in J$. The ideal generated by a family of elements of A is often denoted by $((a_i)_{i\in I})$; for example (a), (a, b), (a_1, a_2, a_3)...

The image $\varphi(I)$ of an ideal I of A under a morphism of rings $\varphi\colon A \to B$ is generally not an ideal of B; the ideal it generates is often denoted by IB. However, the inverse image of an ideal J of B by such a morphism of rings is always an ideal of A. In particular, the *kernel* $\ker(\varphi) = \varphi^{-1}(0)$ of a morphism of rings is an ideal of A.

Let I be an ideal of A. The relation $x \sim y$ defined by $x - y \in I$ is an equivalence relation. The quotient set $A/\sim$, denoted by A/I, admits a unique ring structure such that the canonical surjection $\pi\colon A \to A/\sim$ is a morphism of rings. The so-called *quotient ring* A/I possesses the following universal property: for every ring B and every morphism of rings $f\colon A \to B$ such that $f(I) = \{0\}$, there exists a unique morphism of rings $\varphi\colon A/I \to B$ such that $f = \varphi \circ \pi$.

The kernel of the canonical morphism π is the ideal I itself. More generally, the map associating with an ideal J of A/I the ideal $\pi^{-1}(J)$ of A is a bijection between the (partially ordered) set of ideals of A/I and the (partially ordered) set of ideals of A which contain I.

1.1.5. Domains. — Let A be a ring. One says that an element $a \in A$ is a *zero-divisor* if there exists $b \in A$, such that $ab = 0$ and $b \neq 0$. One says that A is an *integral domain*, or a *domain*, if $A \neq \{0\}$ and if 0 is its only zero-divisor. Fields are integral domains.

1.1.6. Prime and maximal ideals. — One says that an ideal I of A is *prime* if the quotient ring A/I is an integral domain. This means that $I \neq A$ and that for every $a, b \in A$ such that $ab \in I$, either $a \in I$, or $b \in I$.

One says that an ideal I of A is *maximal* if the quotient ring A/I is a field. This means that I is a maximal element of the partially ordered set of ideals of A which are not equal to A. A maximal ideal is a prime ideal.

One deduces from Zorn's theorem that every ideal of A which is distinct from A is contained in some maximal ideal. (Indeed, if I is an ideal of A such that $I \neq A$, the set of ideals J of A such that $I \subset J \subsetneq A$, ordered by inclusion, is inductive—every totally ordered subset admits an upper-bound) In particular, every non-zero ring contains maximal ideals.

Hilbert's Nullstellensatz (theorem 1.7.1 below) gives a description of the maximal ideals of polynomials rings over algebraically closed fields.

1.1.7. — If a ring admits exactly one maximal ideal, one says that it is a *local ring*. A ring is local if and only if its set of non-invertible elements is an ideal (*exercise!*).

Let A and B be local rings; let $\mathfrak{m}_A$ and $\mathfrak{m}_B$ be their maximal ideals; let $\kappa(A) = A/\mathfrak{m}_A$ and $\kappa(B) = B/\mathfrak{m}_B$ be their residue fields. A morphism $f\colon A \to B$ is said to be *local* if $f(\mathfrak{m}_A) \subset \mathfrak{m}_B$ or, equivalently, if $f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$. Observe that a local morphism $f\colon A \to B$ passes to the quotient and induces a morphism $\kappa(A) \to \kappa(B)$ between their residue fields.

1.1.8. — The intersection J of all maximal ideals of a ring A is called its Jacobson radical. It admits the following characterization: one has $a \in J$ if and only if $1 + ab$ is invertible in A for every $b \in A$ (*exercise!*).

1.1.9. — Let A be an integral domain and let K be its field of fractions. One says that A is a *valuation ring* if, for every non-zero element a of K, either $a \in R$, or $1/a \in R$ (or both).

Assume that A is a valuation ring. Let a, b be element of A which are not invertible. If $a = 0$, then $a + b = b$ is not invertible; assume that $a \neq 0$ and let

$x = b/a$. If $x \in R$, then $a + b = a(1 + x)$ is not invertible; otherwise, $x \neq 0$, hence $1/x \in R$ and $a + b = b(1 + 1/x)$ is not invertible as well. This implies that the set $A - A^\times$ of non-invertible elements of A is an ideal, hence *a valuation ring is a local ring.*

1.1.10. — Let A be an integral domain. One says that an element $a \in A$ is *irreducible* if it is not invertible and if the equality $a = bc$ for $b, c \in A$ implies that b or c is invertible. An element a is said to be prime if the principal ideal (a) is prime; this implies that a is irreducible but the converse does not hold (*exercise!*; show, for example, that the element $1 + i\sqrt{5}$ of the ring $\mathbf{Z}[i\sqrt{5}]$ is irreducible but not prime).

One says that the ring A is a *unique factorization domain* (UFD, in short) if the following two properties hold:

(a) Every strictly increasing sequence of principal ideals of A is finite;
(b) Every irreducible element of A generates a prime ideal.

Indeed, these two properties are equivalent to the fact that every non-zero element of A can be written as the product of an invertible element and of finitely many prime elements of A, in a unique way up to the order of the factors and to multiplication of the factors by units.

Condition (ii) is sometimes stated under the name of ''Gauss's lemma'': If A is a UFD, then *every irreducible element a which divides a product bc must divide one of the factors b or c*. Condition (i) obviously holds when A is noetherian. Consequently, a noetherian ring for which Gauss's lemma holds is a UFD.

Principal ideal rings are unique factorization domains, as well as polynomial rings over fields. In fact, if A is a UFD, then so is $A[X]$ (a theorem proved by Gauss for $A = \mathbf{Z}$).

1.2. Localization (Medium up)

Let A be a ring.

1.2.1. Nilpotent elements. — One says that an element $a \in A$ is *nilpotent* if there exists an integer $n \geqslant 1$ such that $a^n = 0$. The set of nilpotent elements of A is an ideal of A, called its *nilradical*. When 0 is the only nilpotent element of A, one says that A is *reduced*. More generally, when I is an ideal of A, one defines the *radical* of I, denoted by $\sqrt{I}$, as the set of all $a \in I$ for which there exists an

integer $n \geqslant 1$ such that $a^n \in I$; it is an ideal of A which contains I. An ideal which is equal to its radical is called a radical ideal.

1.2.2. Multiplicative subsets. — A *multiplicative subset* of A is a subset $S \subset A$ which contains 1 and such that $ab \in S$ for every $a, b \in S$.

1.2.3. — Let M be an A-module. The *fraction module* $S^{-1}M$ (sometimes also denoted by M_S) is the quotient of the set $M \times S$ by the equivalence relation $\sim$ such that $(m, s) \sim (m', s')$ if and only if there exists $t \in S$ such that $t(sm' - s'm) = 0$. Let us denote by m/s the class in $S^{-1}M$ of the pair $(m, s) \in M \times S$. The addition of the abelian group $S^{-1}M$ is given by the familiar formulas

$$(m/s) + (m'/s') = (s'm + sm')/ss',$$

for $m, m' \in M$, $s, s' \in S$; its zero is the element $0/1$. Its structure of an A-module is given by $a \cdot (m/s) = (am)/s$, for $a \in A$, $m \in M$ and $s \in S$.

For every $s \in S$, the multiplication by s is an isomorphism on $S^{-1}M$—one says that S acts by automorphisms on $S^{-1}M$. The map $\theta\colon M \to S^{-1}M$ given by $\theta(m) = m/1$ is a morphism of A-modules; it satisfies the following universal property: For every morphism of A-modules $f\colon M \to N$ such that S acts by automorphisms on N, there exists a unique morphism of A-modules $\varphi\colon S^{-1}M \to N$ such that $f = \varphi \circ \theta$ (explicitly: $f(m) = \varphi(m/1)$) for every $m \in M$).

1.2.4. — Let B be an A-algebra. Then the module of fractions $S^{-1}B$ has a natural structure of an A-algebra for which the multiplication is given by the familiar formulas

$$(b/s) \cdot (b'/s') = (bb')/(ss'),$$

for $b, b' \in B$ and $s, s' \in S$; its zero and unit are the elements $0/1$ and $1/1$. The canonical map $\theta\colon B \to S^{-1}B$ is a morphism of A-algebras, and the images of the elements of S are invertible in $S^{-1}B$. In fact, this morphism satisfies the following universal property: For every morphism of A-algebras $f\colon B \to B'$ such that the images of elements of S are units of B', there exists a unique morphism of A-Algebras $\varphi\colon S^{-1}B \to B'$ such that $f = \varphi \circ \theta$.

In particular, $S^{-1}A$ itself is an A-algebra.. Moreover, for every A-module M, the A-module $S^{-1}M$ has a natural structure of a $S^{-1}A$-module.

The ring $S^{-1}A$ is the zero ring if and only if $0 \in S$.

1.2.5. Examples. — Let us give examples of multiplicative subsets and let us describe the corresponding ring of fractions.

a) Let $a \in A$; the set $S = \{1, a, a^2, \ldots\}$ is a multiplicative subset which contains 0 if and only if a is nilpotent. The corresponding fraction ring is often denoted by A_a. Let $\varphi_1 : A[T] \to A_a$ be the morphism of rings given by $\varphi_1(P) = P(1/a)$; it is surjective and its kernel contains the polynomial $1 - aT$. Let $\varphi : A[T]/(1 - aT) \to A_a$ be the morphism of rings which is deduced from φ_1 by passing to the quotient; let us show that φ is an isomorphism by constructing its inverse.

The obvious morphism $\psi_1 : A \to A[T]/(1-aT)$ maps a to an invertible element of $A[T]/(1 - aT)$; by the universel property of the localization, there exists a unique morphism of rings $\psi : A_a \to A[T]/(1 - aT)$ such that $\psi(b) = b$ for every $b \in A$; one has $\psi(b/a^n) = b\,\mathrm{cl}(T)^n$ for every $b \in A$ and every integer $n \geqslant 0$. Moreover, $\varphi \circ \psi(b/a^n) = b/a^n$, so that $\varphi \circ \psi = \mathrm{id}$. In the other direction, $\psi \circ \varphi(b) = b$ for every $b \in A$ and $\psi \circ \varphi_1(T) = \psi(1/a) = \mathrm{cl}(T)$; consequently, $\psi \circ \varphi_1(P) = \mathrm{cl}(P)$ for every polynomial $P \in A[T]$, hence $\psi \circ \varphi = \mathrm{id}$. This shows that φ is an isomorphism, with inverse ψ, as claimed.

b) Let I be an ideal of A. The set $S = 1 + I = \{a \in I\,;\ a - 1 \in I\}$ is a multiplicative subset of A.

c) Let $f : A \to B$ be a morphism of rings, let T be a multiplicative subset of B and let $S = f^{-1}(T)$. Then S is a multiplicative subset of A and there is a unique morphism of rings $\varphi : S^{-1}A \to T^{-1}B$ such that $\varphi(a/1) = f(a)/1$ for every $a \in A$.

d) If A is an integral domain, then $S = A - \{0\}$ is a multiplicative subset of A; the fraction ring $S^{-1}A$ is a field, called the *field of fractions of* A.

e) Let $\mathfrak{p}$ be an ideal of A and let $S = A - \mathfrak{p}$. Then S is a multiplicative subset of A if and only if $\mathfrak{p}$ is a prime ideal of A; the fraction ring is denoted $A_{\mathfrak{p}}$.

1.2.6. — Let A be a ring, let S be a multiplicative subset of A. For every ideal I of A, the ideal $\theta(I)(S^{-1}A)$ generated by the image of I in $S^{-1}A$ is denoted by $S^{-1}I$. It is equal to $S^{-1}A$ if and only if $S \cap I \neq \varnothing$. Moreover, every ideal of $S^{-1}A$ is of this form.

Finally, the map $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ is a bijection from the set of prime ideals of A which do not meet S to the set of prime ideals of $S^{-1}A$.

In particular, for every prime ideal $\mathfrak{p}$ of A, the ring $A_{\mathfrak{p}}$ is a local ring, called the localization of A at $\mathfrak{p}$, and $\mathfrak{p}A_{\mathfrak{p}}$ is its maximal ideal.

Lemma **(1.2.7)**. — *Let* A *be a ring, let* S *be a multiplicative subset of* A *and let* I *be an ideal of* A. *If* I *does not meet* S, *then there exists a prime ideal* $\mathfrak{p}$ *of* A *which contains* I *and does not meet* S.

Proof. — Since $I \cap S = \varnothing$, the ideal $S^{-1}I$ is distinct from $S^{-1}A$, hence is contained in some maximal ideal of $S^{-1}A$, of the form $S^{-1}\mathfrak{p}$, for some prime (but non necessarily maximal) ideal $\mathfrak{p}$ of A. One then checks that $I \subset \mathfrak{p}$. Let indeed $a \in I$. Since one has $a/1 \in S^{-1}I \subset S^{-1}\mathfrak{p}$, there exists $b \in \mathfrak{p}$ and $s \in S$ such that $a/1 = b/s$. By definition of the ring $S^{-1}A$, there exists $t \in S$ such that $t(as - b) = 0$. In particular, $sta = tb \in \mathfrak{p}$. Since $st \in S$ and $S \cap \mathfrak{p} = \varnothing$, the definition of a prime ideal implies that $a \in \mathfrak{p}$, as was to be shown. □

Proposition **(1.2.8)**. — *The radical of an ideal is the intersection of the prime ideals which contain it. In particular, the nilradical of a ring is the intersection of its prime ideals.*

Proof. — Let A be a ring. Nilpotent elements are contained in every prime ideal of A. Conversely, let $a \in A$ be a non-nilpotent element. By definition, the multiplicative subset $S = \{1, a, a^2, \ldots\}$ is disjoint from the ideal $\{0\}$, hence there exists a prime ideal $\mathfrak{p}$ of A which does not meet S; in particular, $a \notin \mathfrak{p}$. □

Lemma **(1.2.9)**. — *Let* A *be a ring and let* M *be an* A*-module. The following properties are equivalent:*

(i) *One has* $M = 0$;
(ii) *One has* $M_{\mathfrak{p}}$ *for every prime ideal* $\mathfrak{p}$ *of* A;
(iii) *One has* $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m}$ *of* A.

Proof. — The implications (i)⇒(ii) and (ii)⇒(iii) are obvious. Let us assume that (iii) holds and let us show that $M = 0$. Let $x \in M$ and let I be the set of all elements $a \in A$ such that $ax = 0$; then I is an ideal of A. By assumption, for every $\mathfrak{m} \in \mathrm{Spm}(A)$, there exists an element $a \in A - \mathfrak{m}$ such that $ax = 0$; in other words, I is not contained in any maximal ideal of A. This implies that $I = A$, hence $1 \in A$ and $x = 0$. Consequently, $M = 0$, as claimed. □

1.3. Nakayama's lemma

Theorem **(1.3.1)** (''Cayley–Hamilton''). — *Let* A *be a ring and let* J *be an ideal of* A. *Let* M *be an* A*-module which is generated by n elements and let u be an*

endomorphism of M *such that* $u(M) \subset JM$. *Then there exists elements* $a_1 \in J$, $a_2 \in J^2, \ldots, a_n \in J^n$ *such that*

$$u^n + a_1 u^{n-1} + \cdots + a_{n-1} u + a_n \mathrm{Id}_M = 0.$$

Proof. — Let $(m_1, \ldots, m_n)$ be a finite family which generates M. For every $i \in \{1, \ldots, n\}$, there exist elements $a_{ij} \in I$ such that $u(m_i) = \sum_{j=1}^{n} a_{ij} m_j$; let P be the matrix (a_{ij}). We consider M as an $A[T]$-module, where T acts by u; we then let $n \times n$ matrices with coefficients in $A[T]$ act on M^n by the usual formulas. Let I_n be the identity matrix; then the matrix $TI_n - P$ annihilates the vector $(m_1, \ldots, m_n) \in M^n$. Let Q be the adjunct matrix of the matrix $TI_n - P$; one has $Q \cdot (TI_n - P) = \det(TI_n - P) I_n$. Consequently, the element $\det(TI_n - P)$ of $A[T]$ annihilates the vector $(m_1, \ldots, m_n)$ as well, that is, $\det(TI_n - P) \cdot m_i = 0$ for every i. Since $(m_1, \ldots, m_n)$ generates M as an A-module, it follows that $\det(TI_n - P) \cdot m = 0$ for every $m \in M$.

Expanding the determinant, there are elements $a_1, \ldots, a_n \in A$ such that $\det(TI_n - P) = T^n + a_1 T^{n-1} + \cdots + a_n$; moreover, $a_i \in J^i$ for every i. By the definition of the structure of $A[T]$-module on M, we conclude that $u^n + a_1 u^{n-1} + \cdots + a_n \mathrm{Id}_M = 0$. □

Corollary **(1.3.2)** (Nakayama's lemma). — *Let* A *be a ring, let* J *be an ideal of* A *and let* M *be a finitely generated* A*-module such that* $M = JM$. *There exists* $a \in J$ *such that* $(1 + a)M = 0$.

In particular, if J *is contained in the Jacobson radical of* A *(which happens, for example, if* A *is local and* J *is its maximal ideal), then* $M = 0$.

Proof. — Let us apply theorem 1.3.1 to the endomorphism $u = \mathrm{Id}_M$ of M. With the notation of that theorem, there exist an integer $n \geqslant 1$ and elements $a_1, \ldots, a_n \in J$ such that $(1 + a_1 + \cdots + a_n)\mathrm{Id}_M = 0$. It thus suffices to set $a = a_1 + \cdots + a_n$.

If J is contained in the Jacobson radical of A, one has $1 + a \in A^\times$; the relation $(1 + a)M = 0$ then implies that $M = 0$. □

Corollary **(1.3.3)**. — *Let* A *be a ring, let* J *be its Jacboson radical. Let* P *be an* A*-module, let* M *and* N *be submodules of* P *such that* $JM + N = M + N$. *If* M *is finitely generated, then* $M \subset N$.

Proof. — Let $M' = (M+N)/N = M/(M \cap N)$; it is a finitely generated A-module. Moreover, one has $JM' = (JM + N)/N = (M + N)/N = M'$. By corollary 1.3.2, one has $M' = 0$, hence $M = M \cap N$, that is, $M \subset N$. □

1.4. Integral and algebraic dependence relations

1.4.1. — Let $f\colon A \to B$ be a morphism of rings. One says that an element $x \in B$ is *integral* over A if there exists an integer $n \geqslant 1$, and elements $a_1, \ldots, \ldots, a_n \in A$ such that

$$x^n + f(a_1)x^{n-1} + \cdots + f(a_{n-1})x + f(a_n) = 0.$$

Such an equation is called an *integral dependence relation*. Very often, the morphism f is understated and the previous relation is written simply $x^n + a_1x^{n-1} + \cdots + a_n = 0$.

Proposition **(1.4.2)**. — *An element $x \in B$ is integral over A if and only if there exists a subring R of B which contains $A[x]$ and which is finitely generated as an A-module.*

Proof. — Let us assume that x possesses an integral dependence relation as above; then, the A-subalgebra $A[x]$ generated by x in B is generated as an A-module by the elements $1, x, \ldots, x^{n-1}$. It suffices to set $R = A[x]$.

Conversely, let R be an A-subalgebra of B which contains x and which is finitely generated as an A-module. By theorem 1.3.1, applied to the endomorphism u of R given by multiplication by x and to the ideal $J = A$, there exist an integer n and elements $a_1, \ldots, a_n \in A$ such that $u^n + a_1u^{n-1} + \cdots + a_n = 0$ as an endomorphism of R. Considering the image of 1, we obtain an integral dependence relation for x, as required. □

Corollary **(1.4.3)**. — *Let $f\colon A \to B$ be a morphism of rings. The set of all elements $x \in B$ which are integral over A is an A-subalgebra of B, called the* integral closure *of A in B.*

Proof. — Let $\widetilde{A}$ be this subset of B. Let x, y be elements of $\widetilde{A}$. Let m and n be the degrees of integral dependence relations for x and y respectively, and let R be the A-submodule of B generated by the finite family $(x^i y^j)$, for $0 \leqslant i < m$ and $0 \leqslant j < n$; it is a subring of B. Since it contains $x + y$ and xy, this shows that these elements are integral over A, hence belong to $\widetilde{A}$. Moreover, every element of $f(A)$ is integral over A; in particular, 0 and 1 are integral over A. This shows that $\widetilde{A}$ is a subring of B; since it contains $f(A)$, it is an A-subalgebra of B. □

1.4.4. — One says that a morphism of rings $f\colon A \to B$ is *integral*, or that B is integral over A, or also that B is an integral A-algebra, if every element of B is integral over A.

If B is finitely generated as an A-module, then B is integral over A. Conversely, if B is finitely generated as an A-algebra, and if it is integral over A, then it is finitely generated as an A-module. We say that B is a *finite* A-algebra.

Lemma **(1.4.5)**. — *Let* B *be an integral domain and let* A *be a subring of* B *such that* B *is integral over* A. *Then* A *is a field if and only if* B *is a field.*

Proof. — Let us assume that A is a field. Let $b \in B$ be a non-zero element and let $b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0$ be an integral dependence relation of *minimal degree* for b. Let $c = b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}$, so that $bc + a_n = 0$. If $a_n = 0$, one would have $bc = 0$, hence, since $b \neq 0$ and B is an integral domain, $c = 0$, which is an integral dependence relation of degree $n - 1$ for b. This contradicts the definition of n, so that $a_n \neq 0$. Since A is a field, a_n is invertible in A; let $d \in A$ be such that $a_n d = 1$. Then $bcd = -a_n d = -1$; consequently, b is invertible in B, with inverse $-cd$. This shows that B is a field.

Let us now assume that B is a field. Let $a \in A$ be any non-zero element and let b be its inverse in B. By assumption, b is integral over A; let $b^n + a_1 b^{n-1} + \cdots + a_{n-1} b + a_n = 0$ be an integral dependence relation. Since $ab = 1$, one has

$$b = a^{n-1} b^n = -a^{n-1}\left(a_1 b^{n-1} + \cdots + a_n\right) = -\left(a_1 + a_2 a + \cdots + a_n a^{n-1}\right).$$

In particular, $b \in A$, so that a is invertible in A. □

1.4.6. — It is crucial that the leading coefficient of an integral dependence relation be equal to 1 (it could be a unit). When A and B are fields, this becomes pointless; in this setting, one usually replaces the adjective *integral* by the adjective *algebraic*. One thus speaks of *algebraic dependence relation*, of an *algebraic* element, of the *algebraic closure* of A in B, etc.

Let $f\colon K \to L$ be an extension of fields. Elements of L which are not algebraic over K are said to be *transcendental*. A field K is said to be algebraically closed if it is algebraically closed in every extension L of K.

Every field K possesses an *algebraic closure*: this is an algebraic extension $K \to \overline{K}$ which is algebraic and algebraically closed. Any two algebraic closures of a field K are isomorphic (as K-algebras).

1.4.7. — Let $f\colon K \to L$ be an extension of fields. One says that a family $(a_i)_{i\in I}$ of elements of L is *algebraically independent* if there does not exist a non-zero polynomial $P \in K[(X_i)_{i\in I}]$ such that $P((a_i)) = 0$, in other words if the canonical morphism of K-algebras $K[(X_i)_{i\in I}] \to L$ which, for every i, maps X_i to a_i is injective.

A *transcendence basis* of L over K is an algebraically independent family (a_i) such that L be algebraic over the subextension of L generated by the a_i.

Transcendence basis exist. More precisely, the following analogue of the incomplete basis theorem holds: *Let* $A \subset C$ *be two subsets of* L*, where* A *is algebraically independent over* K*, and* L *is algebraic over the subextension generated by* C*; then there exists a transcendence basis* B *such that* $A \subset B \subset C$. Two transcendence basis have the same cardinality, called the *transcendence degree* of L over K and denoted $\mathrm{tr.deg}_K(L)$, or even $\mathrm{tr.deg}(L)$ if the field K is clear from the context. Finally, let $K \to L$ and $L \to M$ be two field extensions. One has the relation

$$\mathrm{tr.deg}_K(L) + \mathrm{tr.deg}_L(M) = \mathrm{tr.deg}_K(M).$$

By abuse of language, we will sometimes make use of the words algebraic, algebraically independent, transcendence degree, in the context of a K-algebra A which is an integral domain, to speak of the corresponding notions of the field of fractions of A.

1.5. The spectrum of a ring

1.5.1. — Let A be a ring. The set of all prime ideals of A is called the *spectrum* (or the prime spectrum) of A and denoted by $\mathrm{Spec}(A)$; the subset $\mathrm{Spm}(A)$ of all maximal ideals of A is called its maximal spectrum.

Every non-zero ring possesses maximal ideals. Consequently, the following assertions are equivalent:

(i) A is the zero ring;
(ii) Its spectrum $\mathrm{Spec}(A)$ is empty;
(iii) Its maximal spectrum $\mathrm{Spm}(A)$ is empty.

For every subset E of A, let $V(E)$ be the set of prime ideals $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $E \subset \mathfrak{p}$. One also writes $V(a, b, \dots)$ for $V(\{a, b, \dots\})$.

The following properties essentially follow from the definitions.

Lemma **(1.5.2)**. — a) *One has* $V(\varnothing) = \mathrm{Spec}(A)$ *and* $V(1) = \varnothing$*;*

b) *If* E *and* E' *are subsets of* A *such that* $E \subset E'$*, one has* $V(E') \subset V(E)$*;*

c) *For every family* $(E_\lambda)_{\lambda\in L}$ *of subsets of* A*, one has* $V(\bigcup_{\lambda\in L} E_\lambda) = \bigcap_{\lambda\in L} V(E_\lambda)$*;*

d) *Let* E, E' *be two subsets of* A *and let* EE' *be the set of all products* ab*, for* $a \in E$ *and* $b \in E'$*; then one has* $V(EE') = V(E) \cup V(E')$*;*

e) *Let* E *be a subset of* A *and let* I *be the ideal of* A *generated by* E*; then one has* $V(E) = V(I)$.

Proof. — a) The first property is obvious, and the second follows from the fact that A is not a prime ideal of itself.

b) Let $\mathfrak{p} \in V(E')$; then $\mathfrak{p}$ is a prime ideal of A such that $E' \subset \mathfrak{p}$; it follows that $E \subset \mathfrak{p}$, hence $\mathfrak{p} \in V(E)$.

c) Let $\mathfrak{p}$ be a prime ideal of A. One has $\mathfrak{p} \in V(\bigcup E_\lambda)$ if and only if $\mathfrak{p}$ contains E_λ for every λ, which means that $\mathfrak{p}$ belongs to $V(E_\lambda)$ for every λ.

d) Let $\mathfrak{p} \in V(E)$. Let $a \in E$ and $b \in E'$; one has $a \in \mathfrak{p}$, hence $ab \in \mathfrak{p}$, so that $\mathfrak{p} \in V(EE')$. This shows that $V(E) \subset V(EE')$, and the inclusion $V(E') \subset V(EE')$ follows by symmetry. Conversely, let $\mathfrak{p} \in V(EE')$. Assume that $\mathfrak{p} \notin V(E')$ and let us show that $\mathfrak{p} \in V(E)$; let $b \in E'$ be such that $b \notin \mathfrak{p}$. For every $a \in E$, one has $ab \in EE'$, hence $ab \in \mathfrak{p}$; Since $\mathfrak{p}$ is a prime ideal, this implies that $a \in \mathfrak{p}$. Consequently, $\mathfrak{p} \in V(E)$, as was to be shown. □

1.5.3. The spectral topology. — Let us decree that a subset of $\mathrm{Spec}(A)$ is *closed* if it is of the form $V(E)$ for some subset E of A. By property *d*) of lemma 1.5.2, we may even assume that E is an ideal.

By property *a*) of that lemma, the empty set and $\mathrm{Spec}(A)$ are closed subsets. According to property *c*), the intersection of a family of closed subsets is closed; by property *d*), the union of two closed subsets is closed.

The sets $V(E)$, where E runs among all subsets of A, are the closed subsets of a topology on the spectrum $\mathrm{Spec}(A)$. We call it the *spectral topology*, or the *Zariski topology*

1.5.4. — For every subset Z of $\mathrm{Spec}(A)$, let $j(Z)$ be the set of $a \in A$ such that $Z \subset V(a)$. One thus has $j(Z) = \bigcap_{\mathfrak{p}\in Z} \mathfrak{p}$; in particular, $j(Z)$ is a radical ideal of A.

Lemma **(1.5.5)**. — a) *If* Z *and* Z' *are subsets of* $\mathrm{Spec}(A)$ *such that* $Z \subset Z'$*, then* $j(Z') \subset j(Z)$*;*

b) *If* $(Z_\lambda)_{\lambda\in L}$ *is a family of subsets of* $\mathrm{Spec}(A)$*, then* $j(\bigcup_{\lambda\in L} Z_\lambda) = \bigcap_{\lambda\in L} j(Z_\lambda)$*;*

c) *For every subset* Z *of* $\mathrm{Spec}(A)$*, one has the inclusion* $Z \subset V(j(Z))$*, with equality if and only if* Z *is of the form* $V(E)$ *for some subset* E *of* A.

d) *For every subset* E *of* A*, one has the inclusion* $E \subset j(V(E))$*, with equality if and only if* E *is of the form* $j(Z)$*, for some subset* Z *of* $\mathrm{Spec}(A)$.

Proof. — Only the cases of equality in assertions *c*) and *d*) do not follow directly from the definitions.

For *c*), it suffices to prove that $V(E) = V(j(V(E)))$. We already know that $V(E) \subset V(j(V(E))$; by the inclusion *d*), one has $E \subset j(V(E))$; applying the map V, we conclude that $V(j(V(E))) \subset V(E)$.

Similarly, we prove *d*) by establishing that $j(Z) = j(V(j(Z))$. We know the inclusion $j(Z) \subset j(V(j(Z))$. According to the general inclusion *c*), we have $Z \subset V(j(Z))$; applying the map j, we conclude that $j(V(j(Z))) \subset j(Z)$. □

Proposition **(1.5.6)**. — a) *For every ideal* I *of* A*, one has* $j(V(I)) = \sqrt{I}$.

b) *For every subset* Z *of* $\mathrm{Spec}(A)$*, one has* $V(j(Z)) = \overline{Z}$*, the closure of* Z *for the spectral topology.*

c) *The maps* $E \mapsto V(E)$ *and* $Z \mapsto j(Z)$ *induce bijections, inverse one of the other, between the set of radical ideals of* A *and the set of closed subsets of* $\mathrm{Spec}(A)$.

Proof. — a) By definition, $V(I)$ is the set of prime ideals containing I, so that $j(V(I))$ is the intersection of all prime ideals containing I. By proposition 1.2.8, one has $j(V(I)) = \sqrt{I}$.

b) Since $V(j(Z))$ is closed and contains Z, it contains its closure $\overline{Z}$ for the spectral topology. Conversely, let Z' be a closed subset of $\mathrm{Spec}(A)$ containing Z and let us show that $Z' \supset V(j(Z))$. Applying the map $V \circ j$ to the inclusion $Z \subset Z'$, we obtain $V(j(Z)) \subset V(j(Z'))$. Since Z' is of the form $V(E)$, one has $V(j(Z')) = Z'$, hence $V(j(Z)) \subset Z'$, as was to be shown.

c) This follows directly from properties *a*) and *b*). □

Exercise **(1.5.7)**. — Let A be a ring and let X be the topological space $\mathrm{Spec}(A)$. An idempotent element of A is an element e such that $e^2 = e$. Show that the map $a \mapsto V(a)$ defines a bijection between the set of idempotents of A and the set of open and closed subsets of $\mathrm{Spec}(A)$. (If e is idempotent, observe that $X = V(e) \cup V(1 - e)$.) In particular, X is connected if and only if the only idempotent elements of A are 0 and 1.

1.5.8. Basic open sets. — For every $a \in A$, one defines $D(a) = \mathrm{Spec}(A) - V(a)$. It is an open subset of $\mathrm{Spec}(A)$. One has $D(1) = \mathrm{Spec}(A)$ and $D(a) = \varnothing$ if a is nilpotent.

Let E be a subset of A. Since $V(E) = \bigcap_{a\in E} V(a)$, we have $\mathrm{Spec}(A) - V(E) = \bigcup_{a\in E} D(a)$. This shows that the open sets of the form $D(a)$, for $a \in A$, form a basis of the topology of $\mathrm{Spec}(A)$.

Exercise **(1.5.9)**. — a) Let x be a point of $\mathrm{Spec}(A)$ and let $\mathfrak{p} = j(\{x\})$ be the corresponding prime ideal of A. Prove that the point $\{x\}$ is closed in $\mathrm{Spec}(A)$ if and only if $\mathfrak{p}$ is a maximal ideal.

b) Let x, y be two points of $\mathrm{Spec}(A)$ such that $x \neq y$. Prove that $x \notin \overline{\{y\}}$ or $y \notin \overline{\{x\}}$. (This says that $\mathrm{Spec}(A)$ is a Kolmogorov topological space, aka T_0.)

c) Describe the topological space $\mathrm{Spec}(\mathbf{Z})$. Show in particular that it is not Hausdorff.

d) Prove that every open cover of $\mathrm{Spec}(A)$ has a finite subcover (one says that it is quasi-compact).

Proposition **(1.5.10)**. — a) *Let* $\varphi\colon A \to B$ *be a morphism of rings. For every prime ideal* $\mathfrak{q}$ *of* B*, the ideal* $\varphi^{-1}(\mathfrak{q})$ *is a prime ideal of* A*. The associated map* ${}^a\varphi\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *given by* ${}^a\varphi(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q})$ *is continuous.*

b) *Let* I *be an ideal of* A *and let* $\varphi\colon A \to A/I$ *be the canonical morphism. The associated map* ${}^a\varphi$ *is a homeomorphism from* $\mathrm{Spec}(A/I)$ *to the subspace* $V(I)$ *of* $\mathrm{Spec}(A)$.

c) *Let* S *be a multiplicative subset of* A *and let* $\theta\colon A \to S^{-1}A$ *be the canonical morphism. The associated map* ${}^a\theta$ *is a homeomorphism from* $\mathrm{Spec}(S^{-1}A)$ *to its image in* $\mathrm{Spec}(A)$*, which is the set of prime ideals of* A *disjoint from* S.

If $S = \{1, a, a^2, \ldots\}$*, then* ${}^a\theta$ *identifies* $\mathrm{Spec}(S^{-1}A)$ *with the open subset* $D(a)$ *of* $\mathrm{Spec}(A)$.

Proof. — a) Since $\mathfrak{q} \neq B$, one has $1 \notin \mathfrak{q}$, hence $1 = \varphi(1) \notin \varphi^{-1}(\mathfrak{q})$; consequently, $\varphi^{-1}(\mathfrak{q}) \neq A$. Moreover, let $a, b \in A$ be such that $ab \in \varphi^{-1}(\mathfrak{q})$; then $\varphi(ab) = \varphi(a)\varphi(b) \in \mathfrak{q}$, hence $\varphi(a) \in \mathfrak{q}$ or $\varphi(b) \in \mathfrak{q}$, by definition of a prime ideal. This implies that a or b belongs to $\varphi^{-1}(\mathfrak{q})$, proving that $\varphi^{-1}(\mathfrak{q})$ is a prime ideal of A.

To prove that the map ${}^a\varphi$ is continuous, we need to show that the inverse image of a closed subset is closed. So let E be a subset of A. A prime ideal $\mathfrak{q}$ of B belongs to $({}^a\varphi)^{-1}(V(E))$ if and only if ${}^a\varphi(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q})$ belongs to $V(E)$, which

means that $E \subset \varphi^{-1}(\mathfrak{q})$, and is equivalent to the inclusion $\varphi(E) \subset \mathfrak{q}$. In other words, we have ${}^a\varphi)^{-1}(V(E)) = V(\varphi(E))$; this is a closed subset of $\mathrm{Spec}(B)$.

b) We known that the map $J \mapsto \varphi^{-1}(J)$ is a bijection from the set of ideals of A/I to the set of ideals of A which contain J. Moreover, for every ideal J of A/I, the morphism φ induces an isomorphism from $A/\varphi^{-1}(J)$ to $(A/I)/J$. In particular, an ideal J of B is prime if and only if the associated ideal $\varphi^{-1}(J)$ is prime, and the prime ideals of A of this form are exactly those containing I. This shows that the map ${}^a\varphi$ is a bijection from $\mathrm{Spec}(A/I)$ to the closed subset $V(I)$ of $\mathrm{Spec}(A)$.

Moreover, for every ideal J of A/I, one has ${}^a\varphi(V(J)) = V(\varphi^{-1}(J))$, so that ${}^a\varphi$ is a closed map. Since it is a continuous bijection, it is a homeomorphism.

c) We know that the continous $J \mapsto \theta^{-1}(J)$ induces a continous bijection from the set $\mathrm{Spec}(S^{-1}A)$ of prime ideals of $S^{-1}A$ to the subset X of $\mathrm{Spec}(A)$ consisting of prime ideals of A which do not meet S.

Let us show that this bijection is closed. Let E be a subset of $S^{-1}A$; let E' be the set of elements $a \in A$ such that there exists $s \in S$ with $a/s \in E$, and let us show that ${}^a\theta(V(E)) = V(E')$. Let $\mathfrak{p}$ be a prime ideal of A which does not meet S, let $\mathfrak{q} = S^{-1}\mathfrak{p}$, so that $\mathfrak{p} = \theta^{-1}(\mathfrak{q})$. Then $\mathfrak{p}$ belongs to ${}^a\varphi(V(E))$ if and only if $S^{-1}\mathfrak{p} \in V(E)$, that is if and only if $E \subset S^{-1}\mathfrak{p}$; on the other hand, $\mathfrak{p}$ belongs to $V(E')$ if and only if $E' \subset \mathfrak{p}$. It thus remains to show that for a prime ideal $\mathfrak{p}$ of A which does not meet S, the conditions $E \subset S^{-1}\mathfrak{p}$ and $E' \subset \mathfrak{p}$ are equivalent. Let us assume that $E \subset S^{-1}\mathfrak{p}$; let $a \in E'$ and let $s \in S$ be such that $a/s \in E$; then $a/s \in S^{-1}\mathfrak{p}$, hence $\theta(a) \in S^{-1}\mathfrak{p}$, hence $a \in \mathfrak{p}$; this shows that $E' \subset \mathfrak{p}$. Conversely, let us assume that $E' \subset \mathfrak{p}$; let $b \in E$ and let $(a, s) \in A \times S$ be such that $b = a/s$; then $a \in E'$, hence $a \in \mathfrak{p}$; consequently, $b = a/s \in S^{-1}\mathfrak{p}$; we have shown that $E \subset S^{-1}\mathfrak{p}$.

□

Remark **(1.5.11)**. — Let $\varphi\colon A \to B$ be a morphism of rings. Classical algebraic geometry is essentially concerned with finitely generated algebras over a field. In that context, corollary 1.6.3 shows that ${}^a\varphi$ maps $\mathrm{Spm}(B)$ into $\mathrm{Spm}(A)$, as the simple example of the canonical morphism $\varphi\colon \mathbf{Z} \to \mathbf{Q}$ shows. This is an indication that the spectrum of a ring is a more natural object than its maximal spectrum. Indeed, spectra of rings were the basic block of Grothendieck's refoundation of algebraic geometry in the 1960s.

1.6. Finitely generated algebras over a field

Theorem **(1.6.1)** (Noether normalization lemma). — *Let* K *be a field and let* A *be a finitely generated* K*-algebra; we assume that* $A \neq 0$. *Then there exist an integer* $n \geqslant 0$, *elements* $a_1, \dots, a_n \in A$ *such that the unique morphism of* K*-algebras* $\varphi\colon K[X_1, \dots, X_n] \to A$ *which maps* X_i *to* a_i *is injective and integral.*

Proof. — Let $(x_1, \dots, x_m)$ be a family of elements of A such that $A = K[x_1, \dots, x_m]$. Let us prove the result by induction on m. If $m = 0$, then $A = K$ and the result holds with $n = 0$. We thus assume that the result for any K-algebra which is finitely generated by at most $m - 1$ elements.

Let $\varphi\colon K[X_1, \dots, X_m] \to A$ be the unique morphism of K-algebras such that $\varphi(X_i) = x_i$. If φ is injective, the result holds, taking $n = m$ and $a_i = x_i$ for every i.

Let us assume that there is a non-zero polynomial $P \in K[X_1, \dots, X_m]$ such that $P(x_1, \dots, x_m) = 0$. We are going to show that there exist strictly positive integers $r_1, \dots, r_{m-1}$ such that A is integral over the subalgebra generated by $y_2, \dots, y_m$, where $y_i = x_i - x_1^{r_i}$ for $i \in \{2, \dots, m\}$. Let $B = K[y_2, \dots, y_m]$ be the subalgebra of A generated by $y_2, \dots, y_m$.

Let $(c_{\mathbf{n}})$ be the coefficients of P, so that

$$P = \sum_{\mathbf{n} \in \mathbf{N}^m} c_{\mathbf{n}} \prod_{i=1}^{m} X_i^{n_i}.$$

Let r be an integer strictly greater than the degree of P in each variable; in other words, $c_{\mathbf{n}} = 0$ if there exists i such that $n_i \geqslant r$; then set $r_i = r^{i-1}$ and $y_i = x_i - x_1^{r_i}$ for $i \in \{2, \dots, m\}$. We define a polynomial $Q \in B[T]$ by

$$\begin{aligned} Q(T) &= P(T, y_2 + T^{r_2}, \dots, y_m + T^{r_m}) \\ &= \sum_{\mathbf{n} \in \mathbf{N}^m} c_{\mathbf{n}} T^{n_1} (y_2 + T^{r_2})^{n_2} \dots (y_m + T^{r_m})^{n_m} \\ &= \sum_{\mathbf{n} \in \mathbf{N}^m} \sum_{j_2=0}^{n_2} \dots \sum_{j_m=0}^{n_m} \binom{n_2}{j_2} \dots \binom{n_m}{j_m} c_{\mathbf{n}} y_2^{n_2 - j_2} \dots y_m^{n_m - j_m} T^{n_1 + \sum_{i=2}^{m} j_i r_i} \end{aligned}$$

and observe that $Q(x_1) = P(x_1, x_2, \dots, x_m) = 0$.

Order $\mathbf{N}^m$ with the "reverse lexicographic order": $(n'_1, \dots, n'_m) < (n_1, \dots, n_m)$ if and only if $n'_m < n_m$, or $n'_m = n_m$ and $n'_{m-1} < n_{m-1}$, etc. Let $\mathbf{n}$ be the largest multi-index in $\mathbf{N}^m$ such that $c_{\mathbf{n}} \neq 0$. For any other $\mathbf{n}' \in \mathbf{N}^m$ such that $c_{\mathbf{n}'} \neq 0$, one has $n'_i < r$ for every i, so that for any $j_2 \in \{0, \dots, n'_2\}, \dots, j_m \in \{0, \dots, n_m\}$,

$$n'_1 + j_2 r_2 + \dots + j_m r_m \leqslant n'_1 + n'_2 r + \dots + n'_m r^{m-1} < n_1 + n_2 r + \dots + n_m r^{m-1}.$$