Chapter 2
Prerequisites and Complements
in Commutative Algebra

2.1 Finite Ring Extensions

Proposition 2.1. Let $A$ be a subring of a ring $B$, and let $x \in B$. The following assertions are equivalent:

(i) The element $x$ is integral over $A$, i.e., there exists a monic polynomial $P(t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n \in A[t]$ such that $P(x) = 0$.

(ii) The subring $A[x]$ of $B$ generated by $A$ and $x$ is a finitely generated $A$–module.

(iii) There exists a subring $A'$ of $B$, containing $A[x]$, which is a finitely generated $A$–module.

The proof is classical and is left to the reader.

2.1.1 Properties and Definitions

I1. If $A$ is a subring of $B$, the set of elements of $B$ which are integral over $A$ is a subring of $B$, called the integral closure of $A$ in $B$.

For $S$ a multiplicatively stable subset of $A$, if $\overline{A}$ denotes the integral closure of $A$ in $B$, then $S^{-1}\overline{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

I2. One says that $B$ is integral over $A$ if it is equal to the integral closure of $A$.

I3. One says that $B$ is finite over $A$ (or that $B/A$ is finite) if $B$ is a finitely generated $A$–module.

The following assertions are equivalent:

(i) The extension $B/A$ is finite.

(ii) $B$ is a finitely generated $A$–algebra and is integral over $A$.

(iii) $B$ is generated as an $A$–algebra by a finite number of elements which are integral over $A$.

I4. An integral domain $A$ is said to be integrally closed if it is integrally closed in its field of fractions.
Example 2.2.

- A unique factorisation domain, a Dedekind domain are integrally closed.
- The polynomial ring \( A[t_1, t_2, \ldots, t_r] \) is integrally closed if and only if \( A \) is integrally closed (see for example [Bou2], chap.5, §1, no3).

15. If \( B \) is integral over \( A \), then \( B \) is a field if and only if \( A \) is a field.

### 2.1.2 Spectra and Finite Extensions

In all the sequel, we suppose \( B/A \) finite.

**Proposition 2.3 (Cohen–Seidenberg Theorem).** The map \( \text{Spec}(B) \to \text{Spec}(A) \) is surjective: for each \( p \in \text{Spec}(A) \), there exists \( q \in \text{Spec}(B) \) such that \( q \cap A = p \) (we then say that \( q \) “lies above \( p \”)]. Moreover,

1. If both \( q_1 \) and \( q_2 \) lie above \( p \), then \( q_1 \subset q_2 \) implies \( q_1 = q_2 \).
2. If \( p_1, p \in \text{Spec}(A) \) with \( p_1 \subset p \), and if \( q_1 \in \text{Spec}(B) \) lies above \( p_1 \), then there exists \( q \in \text{Spec}(B) \) which lies above \( p \) and such that \( q_1 \subset q \).
3. For each \( p \in \text{Spec}(A) \), there is only a finite number of prime ideals of \( B \) which lie above \( p \).

**Proof (of 2.3).** We localize at \( p \): the extension \( B_p/A_p \) is finite, and the prime ideals of \( B \) which lie above \( p \) correspond to the prime ideals of \( B_p \) which lie above \( pA_p \). Since \( pA_p \) is maximal in \( A_p \), the proposition thus follows from the following lemma.

**Proposition 2.4.** Suppose that \( B/A \) is finite.

1. The map \( \text{Spec}(B) \to \text{Spec}(A) \) induces a surjective map

   \[
   \text{MaxSpec}(B) \to \text{MaxSpec}(A).
   \]

2. Any prime ideal of \( B \) which lies above a maximal ideal of \( A \) is also maximal.

**Proof (of 2.4).** To prove that \( n \) is a maximal ideal of \( B \) if and only if \( n \cap A \) is a maximal ideal of \( A \), we divide by \( n \), and we now have to prove that, if \( B \) is integral over \( A \), with \( B \) an integral domain, then \( B \) is a field if and only if \( A \) is a field (see I5 above).

To prove the surjectivity of the map \( \text{MaxSpec}(B) \to \text{MaxSpec}(A) \), it suffices to prove that, for \( m \in \text{MaxSpec}(A) \), we have \( mB \neq B \). Now if \( mB = B \), then there exists \( a \in m \) such that \((1-a)B = 0\) (it is left to the reader to prove that), whence \( 1 - a = 0 \) and \( 1 \in m \).
2.1 Finite Ring Extensions

2.1.3 Case of Integrally Closed Rings

Proposition 2.5. Let $A$ and $B$ be integrally closed rings with field of fractions $K$ and $L$ respectively. Suppose $B$ is a finite extension of $A$. Suppose the extension $L/K$ is normal, and let $G := \text{Aut}_K(L)$ be the Galois group of this extension. Then, for each $p \in \text{Spec}(A)$, the group $G$ acts transitively on the set of $q \in \text{Spec}(B)$ which lie above $p$.

Proof (of 2.5). We first suppose that the extension $L/K$ is separable, and thus is a Galois extension. Then we have $K = L^G$, so that $A = B^G$ (indeed, every element of $B^G$ is integral over $A$ and thus belongs to $K$, whence to $A$ since $A$ is integrally closed). Let $q$ and $q'$ be two prime ideals of $B$ which lie above $p$. Suppose that $q'$ is not contained in any of the $g(q)$'s ($g \in G$), and there exists $x \in q'$ which doesn’t belong to any of the $g(q)$'s ($g \in G$). But then $\prod_{g \in G} g(x)$ is an element of $A \cap q'$ which doesn’t belong to $A \cap q$, which is a contradiction.

We now deal with the general case. Let $p$ be the characteristic of $K$. Let $K' := L^G$. Then $L/K'$ is a Galois extension with Galois group $G$, and the extension $K'/K$ is purely inseparable, i.e., for each $x \in K'$, there exists an integer $n$ such that $x^{p^n} \in K$. Let $A'$ be the integral closure of $A$ in $K'$. Then there is a unique prime ideal of $A'$ which lies above $p$, namely $p' := \{x \in A' \mid (\exists n \in \mathbb{N})(x^{p^n} \in p)\}$. Proposition 2.5 thus follows from the above case $K' = K$.

Proposition 2.6. Let $A$ be an integrally closed ring and let $K$ be its field of fractions. Let $B$ be an $A$–algebra which is finite over $A$. Suppose $B$ is an integral domain and let $L$ be its field of fractions. Let $p, p_1 \in \text{Spec}(A)$ be such that $p \subset p_1$, and let $q_1 \in \text{Spec}(B)$ lie above $p_1$. Then there exists $q \in \text{Spec}(B)$ which lies above $p$ and such that $q \subset q_1$.

Proof (of 2.6). Let $M$ be a finite normal extension of $K$ containing $L$ and let $C$ be the normal closure of $A$ in $M$. By 2.3, we know that there exist prime ideals $r_1$ and $r$ of $C$ which lie above $q_1$ and $p$ respectively. Since $r_1$ lies above $p_1$, we also know that there exists $r_1' \in \text{Spec}(C)$ which lies above $p_1$, and such that $r \subset r_1'$. By 2.5, there exists $g \in \text{Gal}(M/K)$ such that $r_1 = g(r_1')$. We then set $q := g(r) \cap B$.

2.1.4 Krull Dimension: First Definitions

Let $A$ be a ring. A chain of length $n$ of prime ideals of $A$ is a strictly increasing sequence

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

of prime ideals of $A$. 
If the set of lengths of chains of prime ideals of $A$ is bounded, then the greatest of these lengths is called the Krull dimension of $A$, and written $\text{Krdim}(A)$. Otherwise, $A$ is said to have infinite Krull dimension. The Krull dimension of the ring 0 is, by definition, $-\infty$.

If $M$ is an $A$–module, then we call the Krull dimension of $M$ and write $\text{Krdim}_A(M)$ the Krull dimension of the ring $A/\text{Ann}_A(M)$. Note that $\text{Krdim}_A(M) \leq \text{Krdim}(A)$.

For $p \in \text{Spec}(A)$, we call the height of $p$ and write $\text{ht}(p)$ the Krull dimension of the ring $A_p$. Thus $\text{ht}(p)$ is the maximal length of chains of prime ideals of $A$ whose greatest element is $p$. The height of $p$ is also sometimes called the codimension of $p$.

Some properties.

- $\text{Krdim}(A) = \sup \{ \text{ht}(m) \} \in \text{MaxSpec}(A),$
- $\text{Krdim}(A/\text{Nilrad}(A)) = \text{Krdim}(A),$
- If $B$ is an $A$–algebra which is finite over $A$, then $\text{Krdim}(B) = \text{Krdim}(A)$.

**Lemma 2.7.** Let $k$ be a field. The Krull dimension of the algebra of polynomials in $r$ indeterminates $k[t_1, t_2, \ldots, t_r]$ over $k$ is $r$.

**Proof (of 2.7).** We first note that there exists a chain of prime ideals of length $r$, namely the sequence $0 \subset (t_1) \subset (t_1, t_2) \subset \cdots \subset (t_1, t_1, \ldots, t_r)$. It is therefore sufficient to prove that the Krull dimension of $k[t_1, t_2, \ldots, t_r]$ is at most $r$.

If $K/k$ is a field extension, then we denote by $\text{trdeg}_k(K)$ its transcendence degree.

**Proposition 2.8.** Let $A$ and $B$ be two integral domains which are finitely generated $k$–algebras, with field of fractions $K$ and $L$ respectively. Suppose there exists a surjective $k$–algebra homomorphism $f : A \rightarrow B$.

1. We have $\text{trdeg}_k(L) \leq \text{trdeg}_k(K)$.
2. If $\text{trdeg}_k(L) = \text{trdeg}_k(K)$, then $f$ is an isomorphism.

**Proof (of 2.8).**

(1) Any generating system for $A$ as $k$–algebra is also a generating system for $K$ over $k$. Thus $K$ has a finite transcendence degree over $k$, and, if this degree is $n$ and if $n \neq 0$, then there exists a system of $n$ algebraically independent elements in $A$ which is a basis of transcendence for $K$ over $k$. The same conclusion applies to $B$ and $L$. Now, by inverse image by $f$, any $k$–algebraically independent system of elements of $B$ can be lifted to a system of $k$–algebraically independent elements of $A$. This proves the first assertion.

(2) Suppose that $\text{trdeg}_k(L) = \text{trdeg}_k(K)$.

If $\text{trdeg}_k(L) = \text{trdeg}_k(K) = 0$, then $K$ and $L$ are algebraic extensions of $k$, and, for each $a \in K$, $a$ and $f(a)$ have the same minimal polynomial over $k$. This proves that the kernel of $f$ is just 0.
Suppose now that \(\text{trdeg}_k(L) = \text{trdeg}_k(K) = n > 0\). We know (cf. proof of (1) above) that there exists a basis of transcendance \((a_1, a_2, \ldots, a_n)\) for \(K\) over \(k\) which consists of elements of \(A\), and such that \((f(a_1), f(a_2), \ldots, f(a_n))\) is a basis of transcendance for \(L\) over \(k\). In particular, we see that the restriction of \(f\) to \(k[a_1, a_2, \ldots, a_n]\) is an isomorphism onto \(k[f(a_1), f(a_2), \ldots, f(a_n)]\), and induces an isomorphism

\[
k(a_1, a_2, \ldots, a_n) \cong k(f(a_1), f(a_2), \ldots, f(a_n)).
\]

If \(a \in A\) has minimal polynomial \(P(t)\) over \(k(a_1, a_2, \ldots, a_n)\), then \(f(a)\) has minimal polynomial \(f(P(t))\) over \(k(f(a_1), f(a_2), \ldots, f(a_n))\), which proves that \(f\) is injective, whence is an isomorphism.

Let then \(p_0 \subset p_1 \subset \cdots \subset p_n\) be a chain of prime ideals of \(k[t_1, t_2, \ldots, t_r]\). Applying the above lemma to the sequence of algebras \(k[t_1, t_2, \ldots, t_r]/p_j\), we see that, for each \(j\) \((0 \leq j \leq n)\), writing \(K_j\) for the field of fractions of \(k[t_1, t_2, \ldots, t_r]/p_j\), we have \(\text{trdeg}_k K_j \leq \text{trdeg}_k K_0 - j \leq r - j\). It follows in particular that \(n \leq r\).

**Corollary 2.9.** Let \(A\) be an integral domain which is a finitely generated algebra over a field \(k\). Let \(K\) be its field of fractions. Then

\[
\text{Krdim}(A) = \text{trdeg}_k(K).
\]

**Proposition 2.10.** Let \(A = k[x_1, x_2, \ldots, x_r]\) be a finitely generated algebra over a field \(k\), generated by \(r\) elements \(x_1, x_2, \ldots, x_r\). We have \(\text{Krdim}(A) \leq r\), and \(\text{Krdim}(A) = r\) if and only if \(x_1, x_2, \ldots, x_r\) are algebraically independent.

**Proof (of 2.10).** Consider \(r\) indeterminates \(t_1, t_2, \ldots, t_r\). Let \(\mathfrak{A}\) be the kernel of the homomorphism from the polynomial algebra \(k[t_1, t_2, \ldots, t_r]\) to \(A\) such that \(t_j \mapsto x_j\). The algebra \(A\) is isomorphic to \(k[t_1, t_2, \ldots, t_r]/\mathfrak{A}\). We thus see that \(\text{Krdim}(A) \leq r\). Moreover, if \(\text{Krdim}(A) = r\), then we see that

\[
\text{Krdim}(k[t_1, t_2, \ldots, t_r]) = \text{Krdim}(k[t_1, t_2, \ldots, t_r]/\mathfrak{A}),
\]

whence \(\mathfrak{A} = 0\) since 0 is a prime ideal of \(k[t_1, t_2, \ldots, t_r]\).

## 2.2 Jacobson Rings and Hilbert’s Nullstellensatz

### 2.2.1 On Maximal Ideal of Polynomial Algebras

Let \(A\) be a commutative ring (with unity), and let \(A[X]\) be a polynomial algebra over \(A\).
Whenever \( \mathfrak{A} \) is an ideal of \( A[X] \), let us denote by \( \overline{\mathfrak{A}} \) and \( x \) respectively the images of \( A \) and \( x \) through the natural epimorphism \( A[X] \to A[X] / \mathfrak{A} \). Thus we have

\[
\overline{\mathfrak{A}} = A / \mathfrak{A} \cap \overline{\mathfrak{A}} \quad \text{and} \quad A[X] = \overline{\mathfrak{A}}[x].
\]

Note that if \( \mathfrak{P} \) is a prime ideal of \( A[X] \), then \( \mathfrak{P} \cap A \) is a prime ideal of \( A \). We shall be concerned by the case of maximal ideals.

Let us point out two very different behaviour of maximal ideals of \( A[X] \) with respect to \( A \).

- If \( \mathfrak{M} \) is a maximal ideal of \( \mathbb{Z}[X] \), then \( \mathfrak{M} \cap \mathbb{Z} \neq \{0\} \) (this will be proved below; see 2.11, (3)).

As a consequence, a maximal ideal \( \mathfrak{M} \) of \( \mathbb{Z}[X] \) can be described as follows: there is a prime number \( p \) and a polynomial \( P(X) \in \mathbb{Z}[X] \) which becomes irreducible in \( (\mathbb{Z}/p\mathbb{Z})[X] \) such that \( \mathfrak{M} = p\mathbb{Z}[X] + P(X)\mathbb{Z}[X] \).

Thus the quotients of \( \mathbb{Z}[X] \) by maximal ideals are the finite fields.

- Let \( p \) be a prime number, and let \( \mathbb{Z}_p := \{a/b \in \mathbb{Q} \mid p \nmid b\} \). Then \( \mathbb{Z}_p[1/p] = \mathbb{Q} \), which shows that \( \mathfrak{M} := (1-pX)\mathbb{Z}_p[X] \) is a maximal ideal of \( \mathbb{Z}_p[X] \). Notice that here \( \mathfrak{M} \cap \mathbb{Z}_p = \{0\} \).

Let us try to examine these questions through the following proposition.

**Proposition 2.11.**

1. If there is \( \mathfrak{M} \in \text{Spec}^{\max}(A[X]) \) such that \( \mathfrak{M} \cap A = \{0\} \), then there exists \( a \in A^* := A - \{0\} \) such that \( (1-aX)A[X] \in \text{Spec}^{\max}(A[X]) \).

   In other words: if there exists \( x \) in an extension of \( A[x] \) such that \( A[x] \) is a field, then there is \( a \in A^* \) such that \( A[1/a] \) is a field.

2. Let \( \text{Spec}^*(A) \) be the set of all nonzero prime ideals of \( A \). We have

\[
\bigcap_{p \in \text{Spec}^*(A)} \mathfrak{p} = \{0\} \cup \{a \in A^* \mid A[1/a] \text{ is a field}\}.
\]

3. Assume \( \bigcap_{p \in \text{Spec}^*(A)} \mathfrak{p} = \{0\} \). Then for all \( \mathfrak{M} \in \text{Spec}^{\max}(A[X]) \) we have \( \mathfrak{M} \cap A \neq \{0\} \).

   In other words: there is no \( x \) such that \( A[x] \) is a field.

**Proof (of 2.11).**

(1) Assume that \( A[x] \) is a field. Then \( A \) is an integral domain, and if \( F \) denotes its field of fractions, we have \( A[x] = F[x] \). Since \( F[x] \) is a field, \( x \) is algebraic over \( F \), hence a root of a polynomial with coefficients in \( A \). If \( a \) is the coefficient of the highest degree term of that polynomial, \( x \) is integral over \( A[1/a] \). Whence \( A[x] \) is integral over \( A[1/a] \), and since \( A[x] \) is a field, it follows that \( A[1/a] \) is a field.

(2) Assume first that \( a \in \bigcap_{p \in \text{Spec}^*(A)} \mathfrak{p} \) and \( a \neq 0 \). We must show that \( A[1/a] \) is a field.

   There is a maximal ideal \( \mathfrak{M} \) of \( A[X] \) containing \( (1-aX)A[X] \).
2.2 Jacobson Rings and Hilbert’s Nullstellensatz

- We then have $\mathfrak{M} \cap A = \{0\}$. Indeed, if it were not the case, we would have $\mathfrak{M} \cap A \in \text{Spec}^*(A)$, hence $a \in \mathfrak{M} \cap A$, then $a \in \mathfrak{M}$, $aX \in \mathfrak{M}$, so 1 $\in \mathfrak{M}$.

- Let $x$ be the image of $X$ in $A[X]/\mathfrak{M}$. Thus $A[x]$ is a field. But $1 - ax = 0$, proving that $x = 1/a$ and $A[1/a]$ is a field.

Assume now that $A[1/a]$ is a field, hence $(1 - aX)A[X] \in \text{Spec}^{\max}(A[X])$. Let $p \in \text{Spec}^*(A)$. Then $p \nsubseteq (1 - aX)A[X]$, since $(1 - aX)A[X] \cap A = \{0\}$.

It follows that $pA[X] + (1 - aX)A[X] = A$. Interpreted in the polynomial ring $(A/p)[X]$, that equality shows that the polynomial $1 - \overline{a}X$ is invertible, which implies that $\overline{1} = 0$, i.e., $a \in \mathfrak{p}$.

(3) Assume that $A[x]$ is a field. By (1), there is $a \in A^*$ such that $A[1/a]$ is a field. By (2), we know that $a \in \bigcap_{p \in \text{Spec}^*(A)} p$, a contradiction.

**Remark 2.12.** The assertion (3) of the preceding proposition shows in particular that if $A$ is a principal ideal domain with infinitely many prime ideals (like $\mathbb{Z}$ or $k[X]$ for example), then whenever $\mathfrak{M} \in \text{Spec}^{\max}(A[X])$, we have $\mathfrak{M} \cap A \neq \{0\}$, hence $\mathfrak{M} \cap A \in \text{Spec}^{\max}(A)$.

**Theorem–Definition 2.13** The following assertions are equivalent:

(J1) Whenever $p \in \text{Spec}(A)$, we have

$$p = \bigcap_{m \in \text{Spec}^{\max}(A), \ m \subseteq p} m.$$  

(J2) Whenever $\mathfrak{M} \in \text{Spec}^{\max}(A[X])$, we have $\mathfrak{M} \cap A \in \text{Spec}^{\max}(A)$.

A ring which fulfills the preceding conditions is called a Jacobson ring.

**Proof (of 2.13).** Let us first notice that both properties (J1) and (J2) transfer to quotients: if $A$ satisfies (J1) (respectively (J2)), and if $a$ is an ideal of $A$, then $A/a$ satisfies (J1) (respectively (J2)) as well.

Let us show (J1) $\implies$ (J2). Let $\mathfrak{M} \in \text{Spec}^{\max}(A[X])$. We set $A[X]/\mathfrak{M} = (A/\mathfrak{M} \cap A)[X]$.

We have $\mathfrak{M} \cap A \in \text{Spec}(A)$, hence $\mathfrak{M} \cap A$ is an intersection of maximal ideals of $A$. If $\mathfrak{M} \cap A$ is not maximal, it is an intersection of maximal ideals in which it is properly contained, thus in the ring $A/\mathfrak{M} \cap A$, we have

$$\bigcap_{p \in \text{Spec}^*(A/\mathfrak{M} \cap A)} p = \{0\},$$

which shows (by 2.11, (3)) that $(A/\mathfrak{M} \cap A)[X]$ cannot be a field, a contradiction.

Let us show (J2) $\implies$ (J1). Let $p \in \text{Spec}(A)$. Working in $A/p$, we see that it suffices to prove that if $A$ is an integral domain which satisfies (J2), then the intersection of maximal ideals is $\{0\}$.

Let $a \in \bigcap_{m \in \text{Spec}^{\max}(A)} m$. Thus whenever $\mathfrak{M} \in \text{Spec}^{\max}(A[X])$, we have $a \in \mathfrak{M}$, hence $aX \in \mathfrak{M}$, which proves that $1 - aX$ is invertible, hence $a = 0$. 

Let us emphasize the defining property of Jacobson rings, by stating the following proposition (which is nothing but a reformulation of property (J2)).

**Proposition 2.14.** The following two assertions are equivalent:

(i) $A$ is a Jacobson ring.

(ii) If $\overline{A}[x]$ is a quotient of $A[X]$ which is a field, then $\overline{A}$ is a field and $x$ is algebraic over $\overline{A}$.

**Remark 2.15.** Let us immediately quote some examples and counterexamples of Jacobson rings:

- Examples of Jacobson rings: fields, principal ideal domains with infinitely many prime ideals, quotients of Jacobson rings.
- Non Jacobson rings: discrete valuation rings.

The next theorem enlarges the set of examples of Jacobson ring to all the finitely generated algebras over a Jacobson ring.

**Theorem 2.16.** Let $A$ be a Jacobson ring.

1. $A[X]$ is a Jacobson ring.
2. If $B$ is a finitely generated $A$–algebra, then $B$ is a Jacobson ring.

**Lemma 2.17.**

1. Let $A$ be a Jacobson ring. Assume that $\overline{A}[v_1, v_2, \ldots, v_r]$ is a finitely generated $A$–algebra which is a field. Then $\overline{A}$ is a field, and $\overline{A}[v_1, v_2, \ldots, v_r]$ is an algebraic (hence finite) extension of $\overline{A}$.

2. Let $k$ be a field. If $k[v_1, v_2, \ldots, v_r]$ is a finitely generated $k$–algebra which is a field, then it is an algebraic (hence finite) extension of $k$.

3. Let $k$ be an algebraically closed field. If $k[v_1, v_2, \ldots, v_r]$ is a finitely generated $k$–algebra which is a field, then it coincides with $k$.

Assertion (3) of the preceding corollary may be reformulated as Hilbert’s Nullstellensatz.

**Theorem 2.18 (Hilbert’s Nullstellensatz).** Let $k$ be an algebraically closed field. The map

$$k^{r} \to \text{Spec}^{\text{max}}(k[v_1, v_2, \ldots, v_r])$$

$$(\lambda_1, \lambda_2, \ldots, \lambda_r) \mapsto \langle v_1 - \lambda_1, v_2 - \lambda_2, \ldots, v_r - \lambda_r \rangle$$

is a bijection.

**Proof (of 2.16).** Let us prove (1).

Let $\mathfrak{M}$ be a maximal ideal of $A[X, Y]$. We set

$$\overline{A} := A/\mathfrak{M} \cap A,$$

$$\overline{A}[x] := A[X]/\mathfrak{M} \cap A[X] \text{ and } \overline{A}[y] := A[Y]/\mathfrak{M} \cap A[Y],$$

$$\overline{A}[x, y] := A[X, Y]/\mathfrak{M}.$$

We have to prove that $\overline{A}[x]$ is a field.
Since \( \mathbb{A}[x, y] \) is a field, \( \mathbb{A} \) is an integral domain, and if \( k \) denotes its field of fractions, we have \( \mathbb{A}[x, y] = k[x, y] \).

Since \( k[x, y] = k[x][y] \) is a field, \( x \) is not transcendental (by 2.11, (3)) over \( k \), hence \( k[x] \) is a field. As in the proof of 2.11, (1), we see that there exists \( a \in A^* \) such that \( x \) is integral over \( A[1/a] \).

Similarly, there exists \( b \in A^* \) such that \( y \) is integral over \( A[1/b] \). It follows that \( A[x, y] \) is integral over \( A[1/ab] \). Since \( A[x, y] \) is a field, it implies that \( A[1/ab] \) is a field.

Now since \( A \) is a Jacobson ring, it follows from Proposition 3 that \( \mathbb{A} \) is a field, i.e., \( \mathbb{A} = k \). We have already seen that \( k[x] \) is a field, proving that \( \mathbb{A}[x] \) is a field.

Let us prove (2).

By induction on \( r \), it follows from (1) that, for all \( r \), \( A[v_1, v_2, \ldots, v_r] \) is a Jacobson ring. So are the quotients of these algebras, which are the finitely generated \( A \)-algebras.

Proof (of 2.17).

(1) Assume that \( \mathbb{A}[v_1, v_2, \ldots, v_r] \) is a field. Since \( \mathbb{A}[v_1, v_2, \ldots, v_{r-1}] \) is a Jacobson ring (by theorem 4, (2)), it follows from Proposition 3 that \( \mathbb{A}[v_1, v_2, \ldots, v_{r-1}] \) is a field over which \( v_r \) is algebraic. Repeating the argument leads to the required statement.

(2) and (3) are immediate consequences of (1).

### 2.2.2 Radicals and Jacobson Rings, Application to Algebraic Varieties

**Theorem–Definition 2.19**

1. The Jacobson radical of a ring \( A \) is the ideal

   \[
   \text{Rad}(A) := \bigcap_{m \in \text{Spec}^\text{max}(A)} m.
   \]

   The Jacobson radical coincides with the set of elements \( a \in A \) such that, for all \( x \in A \), \( (1 - ax) \) is invertible.

2. The nilradical of a ring \( A \) is the ideal

   \[
   \text{Nilrad}(A) := \bigcap_{p \in \text{Spec}(A)} p.
   \]

   The nilradical coincides with the set of nilpotent elements of \( A \).

**Proof** (of 2.19). We prove only (2). It is clear that any nilpotent element of \( A \) belongs to \( \text{Nilrad}(A) \). Let us prove the converse.

Whenever \( \mathfrak{M} \) is a maximal ideal of \( A[X] \), we know that \( \mathfrak{M} \cap A \) is a prime ideal of \( A \). It implies that \( \text{Nilrad}(A) \subset \text{Rad}(A) \), and thus for \( a \in \text{Nilrad}(A) \), the polynomial \( (1 - aX) \) is invertible, which implies that \( a \) is nilpotent.
Now if $A$ is a Jacobson ring, it follows from 2.13 that
\[ \text{Rad}(A) = \text{Nilrad}(A). \]
Applying that remark to a quotient $A/\mathfrak{a}$ of a Jacobson ring, we get the following proposition.

**Lemma 2.20.** Let $A$ be a Jacobson ring, and let $\mathfrak{a}$ be an ideal of $A$. We have
\[ \bigcap_{\mathfrak{m} \in \text{Spec}_{\text{max}}(A)} \mathfrak{a} \subseteq \mathfrak{m} = \{ a \in A \mid (\exists n \geq 0)(a^n \in \mathfrak{a}) \}. \]

Applying the preceding proposition to the case where $A = k[X_1, \ldots, X_r]$ for $k$ algebraically closed gives the “strong form” of Hilbert’s Nullstellensatz.

**Corollary 2.21 (Strong Nullstellensatz).** Let $k$ be an algebraically closed field. For $A$ an ideal of $k[X_1, X_2, \ldots, X_r]$, let us set
\[ V(\mathfrak{a}) := \{ (\lambda_1, \lambda_2, \ldots, \lambda_r) \in k^r \mid (\forall P \in \mathfrak{a})(P(\lambda_1, \lambda_2, \ldots, \lambda_r) = 0) \}. \]

If $Q \in k[X_1, X_2, \ldots, X_r]$ is such that
\[ (\forall (\lambda_1, \lambda_2, \ldots, \lambda_r) \in V(\mathfrak{a}))(Q(\lambda_1, \lambda_2, \ldots, \lambda_r)) = 0, \]
then there exists $n \geq 0$ such that $Q^n \in \mathfrak{a}$.

**Proof (of 2.21).** Translating via the dictionary $k^r \longleftrightarrow \text{Spec}^{\text{max}}(k[X_1, X_2, \ldots, X_r])$, we see that
\[ V(\mathfrak{a}) \longleftrightarrow \{ \mathfrak{m} \in \text{Spec}^{\text{max}}(k[X_1, X_2, \ldots, X_r]) \mid \mathfrak{a} \subseteq \mathfrak{m} \}, \]
while the hypothesis on $Q$ translates to
\[ Q \in \bigcap_{\mathfrak{m} \in \text{Spec}_{\text{max}}(k[X_1, X_2, \ldots, X_r])} \mathfrak{m}. \]

2.3 Graded Algebras and Modules

2.3.1 Graded Modules

Let $k$ be a ring. We call *graded* $k$–module any $k$–module of the form
\[ M = \bigoplus_{n=-\infty}^{n=\infty} M_n \]
where, for each $n$, $M_n$ is a finitely generated $k$–module, and $M_n = 0$ whenever $n < N$ for some integer $N$ (i.e., “for $n$ small enough”).

For each integer $n$, the non-zero elements of $M_n$ are said to be homogeneous of degree $n$. If $x = \sum_n x_n$ where $x_n \in M_n$, then the element $x_n$ is called the homogeneous component of degree $n$ of $x$.

A graded module homomorphism $M \rightarrow N$ is a linear map $f : M \rightarrow N$ such that, for each $n \in \mathbb{Z}$, we have $f(M_n) \subset N_n$.

From now on, we suppose that $k$ is a field. The graded $k$–modules are then called graded $k$–vector spaces.

We set $\mathbb{Z}(q) := \mathbb{Z}[[q]][q^{-1}]$, the ring of formal Laurent series with coefficients in $\mathbb{Z}$. The graded dimension of $M$ is the element of $\mathbb{Z}(q)$ defined by

$$\text{grdim}_k(M) := \sum_{n=-\infty}^{\infty} \dim_k(M_n)q^n.$$ 

### 2.3.2 Elementary Constructions

- **Direct sum:** if $M$ and $N$ are two graded modules, then the graded module $M \oplus N$ is defined by the condition $(M \oplus N)_n := M_n \oplus N_n$. If $k$ is a field, then we have

  $$\text{grdim}_k(M \oplus N) = \text{grdim}_k(M) + \text{grdim}_k(N).$$

- **Tensor product:** if $M$ and $N$ are two graded modules, then the graded module $M \otimes N$ is defined by the condition $(M \otimes N)_n := \bigoplus_{i+j=n} M_i \otimes N_j$. If $k$ is a field, then we have

  $$\text{grdim}_k(M \otimes N) = \text{grdim}_k(M)\text{grdim}_k(N).$$

- **Shift:** if $M$ is a graded module and $m$ is an integer, then the graded module $M[m]$ is defined by the condition $M[m]_n := M_{m+n}$. If $k$ is a field, then we have

  $$\text{grdim}_k(M[m]) = q^{-m}\text{grdim}_k(M).$$

**Example 2.22.** Let $k$ be a field.

- If $t$ is transcendental over $k$ and of degree $d$, then we have $\text{grdim}_k(k[t]) = 1/(1 - q^d)$.

- More generally, if $t_1, t_2, \ldots, t_r$ are algebraically independent elements over $k$ of degree $d_1, d_2, \ldots, d_r$ respectively, then we have $k[t_1, t_2, \ldots, t_r] \simeq k[t_1] \otimes k[t_2] \otimes \cdots \otimes k[t_r]$ and

  $$\text{grdim}_k(k[t_1, t_2, \ldots, t_r]) = \frac{1}{(1 - q^{d_1})(1 - q^{d_2})\cdots(1 - q^{d_r})}.$$
• If $M$ has dimension 1 and is generated by an element of degree $d$, then we have $M \cong k[-d]$, and $\text{grdim}_k(M) = q^d$.

• If $V$ is a vector space of finite dimension $r$, then the symmetric algebra $S(V)$ and the exterior algebra $\Lambda(V)$ of $V$ are naturally endowed with structures of graded vector spaces, and we have

$$\text{grdim}_k(S(V)) = \frac{1}{(1 - q)^r} \quad \text{and} \quad \text{grdim}_k(\Lambda(V)) = (1 + q)^r.$$  

A linear map $f : M \to N$ between two graded vector spaces is said to be of degree $m$ if, for all $n$, we have $f(M_n) \subset N_{n+m}$. Thus, a map of degree $m$ defines a homomorphism from $M$ to $N[m]$.

Suppose then that

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

is an exact sequence of $k$–vector spaces, where $M'$, $M$, and $M''$ are graded, and where $\alpha$ and $\beta$ are maps of degree $a$ and $b$ respectively. We then have an exact sequence of graded vector spaces

$$0 \to M' \xrightarrow{\alpha} M[a] \xrightarrow{\beta} M''[a+b] \to 0,$$

whence the formula

$$\text{grdim}_k(M'') - q^b \text{grdim}_k(M) + q^{a+b} \text{grdim}_k(M') = 0.$$  

### 2.3.3 Koszul Complex

Let $V$ be a vector space of dimension $r$. Let $S := S(V)$ and $A := A(V)$. The Koszul complex is the complex

$$0 \to S \otimes A^r \xrightarrow{\delta_r} S \otimes A^{r-1} \xrightarrow{\delta_{r-1}} \cdots \xrightarrow{\delta_1} S \otimes A^0 \xrightarrow{k} 0$$

where the homomorphism $S \otimes A^0 \to k$ is the homomorphism defined by $v \mapsto 0$ for all $v \in V$, and where the homomorphism $\delta_j$ is defined in the following way:

$$\delta_j(y \otimes (x_1 \wedge \cdots \wedge x_j)) = \sum_i (-1)^{i+1} yx_i \otimes (x_1 \wedge \cdots \wedge \hat{x_i} \wedge \cdots \wedge x_j).$$
If we endow $S \otimes A^j$ with the graduation of $S$, the homomorphism $\delta_j$ has thus degree 1, and the homomorphism $S \otimes A^0 \to k$ has degree 0.

One can prove (see for example [Ben], lemma 4.2.1) that the Koszul complex is exact. It follows that

$$1 = \sum_{j=0}^r (-1)^j \dim(A^j) \dim_k(S),$$

or, equivalently,

$$1 = \dim_k(A)(-q) \dim_k(S)(q).$$

### 2.3.4 Graded Algebras and Modules

Let $k$ be a (noetherian) ring. We call graded $k$–algebra any finitely generated algebra over $k$ of the form $A = \bigoplus_{n=0}^{\infty} A_n$, with $A_0 = k$, and $A_n A_m \subset A_{n+m}$ for any integers $n$ and $m$. We then write $\mathfrak{M}$ for the maximal ideal of $A$ defined by

$$\mathfrak{M} := \bigoplus_{n=1}^{\infty} A_n.$$

A graded $A$–module $M$ is then a (finitely generated) $A$–module of the form $M = \bigoplus_{n=-\infty}^{\infty} M_n$ where $A_n M_m \subset M_{n+m}$ for all $n$ and $m$, and where $M_n$ is zero if $n < N$ for some integer $N$.

Each homogeneous component $M_n$ is a finitely generated $k$–module.

Indeed, $A$ is a noetherian ring, and we have $M_n \cong \bigoplus_{m \geq n} M_m / \bigoplus_{m > n} M_m$, which proves that $M_n$ is finitely generated over $A/\mathfrak{M}$.

A graded $A$–module homomorphism is an $A$–module homomorphism which is a graded $k$–module homomorphism.

A submodule $N$ of a graded $A$–module is an $A$–submodule such that the natural injection is a graded $k$–module homomorphism, i.e., such that $N = \bigoplus_{n} (N \cap M_n)$.

A graded (or “homogeneous”) ideal of $A$ is a graded submodule of $A$, seen as graded module over itself. If $\mathfrak{a}$ is an ideal of $A$, then the following conditions are equivalent:

(i) $\mathfrak{a}$ is a graded ideal,

(ii) $\mathfrak{a} = \bigoplus_{n} (\mathfrak{a} \cap A_n),$

(iii) for all $a \in \mathfrak{a}$, each homogeneous component of $a$ belongs to $\mathfrak{a},$

(iv) $\mathfrak{a}$ is generated by homogeneous elements.

### 2.3.5 The Hilbert–Serre Theorem

**Theorem 2.23.** Let $k$ be a field. Let $A = k[x_1, x_2, \ldots, x_r]$ be a graded $k$–algebra, generated by homogeneous elements of degree $d_1, d_2, \ldots, d_r$.
respectively. Let $M$ be a graded $A$–module. Then there exists $P(q) \in \mathbb{Z}[q, q^{-1}]$ such that the graded dimension of $M$ over $k$ is

$$\text{grdim}_k(M) = \frac{P(q)}{(1 - q^{d_1})(1 - q^{d_2}) \cdots (1 - q^{d_r})}.$$ 

**Proof (of 2.23).** We use induction on $r$. The theorem is obvious if $r = 0$, so we suppose that $r > 0$. Let $M'$ and $M''$ be the kernel and cokernel of multiplication by $x_r$ respectively. We thus have the following exact sequence of graded $A$–modules:

$$0 \to M' \xrightarrow{x_r} M \xrightarrow{x_r} M'[d_r] \to M''[d_r] \to 0,$$

whence the equality

$$q^{d_r} \text{grdim}_k(M') - q^{d_r} \text{grdim}_k(M) + \text{grdim}_k(M) - \text{grdim}_k(M'') = 0.$$ 

Now $M'$ and $M''$ are both graded modules over $k[x_1, \ldots, x_{r-1}]$, so that, by the induction hypothesis, there exist $P'(q), P''(q) \in \mathbb{Z}[q, q^{-1}]$ such that

$$\text{grdim}_k(M') = \frac{P'(q)}{(1 - q^{d_1})(1 - q^{d_2}) \cdots (1 - q^{d_{r-1}})}$$

and

$$\text{grdim}_k(M'') = \frac{P''(q)}{(1 - q^{d_1})(1 - q^{d_2}) \cdots (1 - q^{d_{r-1}})}.$$ 

The theorem follows immediately.

### 2.3.6 Nakayama’s Lemma

Let $k$ be a (commutative) field, and let $A$ a graded $k$-algebra.

**Convention**

We make the convention that

- “ideal of $A$” means “graded ideal of $A$”,
- “element of $A$” means “homogeneous element of $A$”.

It can be shown that the “graded Krull dimension” of $A$, (i.e., the maximal length of chains of (graded) prime ideals of $A$) coincides with its “abstract” Krull dimension (i.e., the maximal length of chains of any prime ideals of $A$).
Nakayama’s Lemma

With the above conventions, Nakayama’s lemma takes the following form.

**Lemma 2.24.** Let $A$ be a graded $k$–algebra, with maximal ideal $\mathfrak{M}$, and let $M$ be an $A$–module. If $\mathfrak{M}M = M$, then $M = 0$.

**Proof (of 2.24).** Indeed, then we know that there exists $a \in \mathfrak{M}$ such that $(1 - a)M = 0$. If $M \neq 0$, then let $m$ be a non-zero (homogeneous) element of $M$. The equality $m = am$ yields a contradiction.

**Lemma 2.25.**

(S1) If $M'$ is a submodule of the $A$–module $M$, then $M' = M$ if and only if $M = M' + \mathfrak{M}M$.

(S2) If $f : M \to N$ is an $A$–module homomorphism which induces a surjection from $M$ onto $N/\mathfrak{M}N$, then $f$ is surjective.

(S3) A system $(x_1, x_2, \ldots, x_s)$ of elements of $M$ is a generating system for $M$ if and only if its image in $M/\mathfrak{M}M$ is a generating system of the $k$–vector space $M/\mathfrak{M}M$. In particular, all the minimal generating systems have the same order, which is the dimension of $M/\mathfrak{M}M$ over $k$.

**Proof (of 2.25).** For (S1), we apply 2.24 to the module $M/M'$.

For (S2), we apply (S1) to the module $N$ and the submodule $f(M)$.

For (S3), we apply (S2) to the module $F := \bigoplus_j A[\deg(x_j)]$ and the homomorphism $F \to M$ defined by the system we consider.

If $M$ is an $A$–module, we write $r(M)$ and call rank of $M$ the dimension of $M/\mathfrak{M}M$ over $k$.

**Proposition 2.26.** Let $R$ be a graded algebra, with maximal graded ideal $\mathfrak{M}$. Let $(u_1, u_2, \ldots, u_n)$ be a family of homogeneous elements of $R$ with positive degrees.

1. The following assertions are equivalent:
   (i) $R = k[u_1, u_2, \ldots, u_n]$,
   (ii) $\mathfrak{M} = Ru_1 + Ru_2 + \cdots + Ru_n$,
   (iii) $\mathfrak{M}/\mathfrak{M}^2 = ku_1 + ku_2 + \cdots + ku_n$.

2. Assume moreover that $R$ is a graded polynomial algebra with Krull dimension $r$. Then the following assertions are equivalent:
   (i) $n = r$, $(u_1, u_2, \ldots, u_r)$ are algebraically independent, and $R = k[u_1, u_2, \ldots, u_r]$,
   (ii) $(u_1, u_2, \ldots, u_n)$ is a minimal set of generators of the $R$–module $\mathfrak{M}$,
   (iii) $(u_1, u_2, \ldots, u_n)$ is a basis of the $k$–vector space $\mathfrak{M}/\mathfrak{M}^2$. 
Proof (of 2.26).

(1) The implications (i)⇒(ii)⇒(iii) are clear. The implication (iii)⇒(ii) is a direct application of Nakayama’s lemma to the \( R \)-module \( \mathfrak{M} \). Finally if (ii) holds, the image of \( k[u_1, u_2, \ldots, u_n] \) modulo \( \mathfrak{M} \) is \( k \), hence \( k[u_1, u_2, \ldots, u_n] = R \) again by Nakayama’s lemma.

(2) The equivalence between (ii) and (iii) follows from Nakayama’s lemma. If (i) holds, then \( (u_1, u_2, \ldots, u_n) \) generates \( \mathfrak{M} \) by (1), and if it contains a proper system of generators of \( R \), say \( (u_1, u_2, \ldots, u_m) \) \((m < r)\) then again by (1) we have \( R = k[u_1, u_2, \ldots, u_m] \), a contradiction with the hypothesis about the Krull dimension of \( R \).

Assume (iii) holds. Since \( R \) is a polynomial algebra with Krull dimension \( r \), and since (i)⇒(iii), we see that the dimension of \( \mathfrak{M}/\mathfrak{M}^2 \) is \( r \). Hence \( n = r \), and since \( R = k[u_1, u_2, \ldots, u_r] \) (by (1)), we see that \( (u_1, u_2, \ldots, u_r) \) is algebraically independent (otherwise the Krull dimension of \( R \) would be less than \( r \)).

Lemma 2.27. Let \( A \) be a graded \( k \)-algebra, and let \( M \) be a finitely generated projective \( A \)-module. Then \( M \) is free.

Proof (of 2.27). Let \( \mathfrak{M} := \sum_{n \geq 1} A_n \) be the unique maximal ideal of \( A \). Then \( M/\mathfrak{M}M \) is a (left) finite dimensional vector space over the field \( k \). Let \( d \) denote its dimension. The isomorphism \( k^d = (A/\mathfrak{M})^d \cong M/\mathfrak{M}M \) can be lifted (by projectivity of \( A^d \)) to a morphism \( A^d \to M \), which is onto by Nakayama’s lemma. Since \( M \) is projective, we get a split short exact sequence

\[
0 \to M' \to A^d \to M \to 0.
\]

Note that \( M' \) is then a direct summand of \( A^d \), hence is also finitely generated. Tensoring with \( k = A/\mathfrak{M}A \), this exact sequence gives (since it is split) the short exact sequence

\[
0 \to M'/fM' \to k^d \to M/\mathfrak{M}M \to 0,
\]

which shows that \( M'/\mathfrak{M}M' = 0 \), hence again by Nakayama’s lemma \( M' = 0 \). Thus we get that \( M \) is isomorphic to \( A^d \).

2.4 Polynomial Algebras and Parameters Subalgebras

2.4.1 Degrees and Jacobian

Let \( S = k[v_1, v_2, \ldots, v_r] \) be a polynomial graded algebra over the field \( k \), where \( (v_1, v_2, \ldots, v_r) \) is a family of algebraically independent, homogeneous elements, with degrees respectively \( e_1, e_2, \ldots, e_r \). Assume \( e_1 \leq e_2 \leq \cdots \leq e_r \).
Let \((u_1, u_2, \ldots, u_r)\) be a family of homogeneous elements with degrees \(d_2, d_2, \ldots, d_r\) such that \(d_1 \leq d_2 \leq \cdots \leq d_r\).

**Lemma 2.28.** Assume that \((u_1, u_2, \ldots, u_r)\) is algebraically free.

1. For all \(i \ (1 \leq i \leq r)\), we have \(e_i \leq d_i\).
2. We have \(e_i = d_i\) for all \(i \ (1 \leq i \leq r)\) if and only if \(S = k[u_1, u_2, \ldots, u_r]\).

**Proof (of 2.28).**

(1) Let \(i\) such that \(1 \leq i \leq r\). The family \((u_1, u_2, \ldots, u_i)\) is algebraically free, hence it cannot be contained in \(k[v_1, v_2, \ldots, v_{i-1}]\). Hence there exist \(j \geq i\) and \(l \leq i\) such that \(v_j\) does appear in \(u_l\). It follows that \(e_j \leq u_l\), hence \(e_i \leq e_j \leq d_l \leq d_i\).

(2) We know that \(\text{grdim} R = (\prod_{i=1}^{r} (1 - q^{e_i}))^{-1}\). Thus it suffices to prove that \(\prod_{i=1}^{r} (1 - q^{e_i}) = \prod_{i=1}^{r} (1 - q^{d_i})\) if and only if \(e_i = d_i\) for all \(i \ (1 \leq i \leq r)\), which is left as an exercise.

By 2.28, we see in particular that the family \((e_1, e_2, \ldots, e_r)\) (with \(e_1 \leq e_2 \leq \cdots \leq e_r\)) is uniquely determined by \(R\). Such a family is called the **family of degrees of** \(R\).

Let us now examine the algebraic independance of the \((u_1, u_2, \ldots, u_r)\).

**Definition 2.29.** The **Jacobian** of \((u_1, u_2, \ldots, u_r)\) relative to \((v_1, v_2, \ldots, v_r)\) is the homogeneous element of degree \(\sum_i (d_i - e_i)\) defined by

\[
\text{Jac}((u_1, u_2, \ldots, u_r)/(v_1, v_2, \ldots, v_r)) := \det \left( \frac{\partial u_i}{\partial v_j} \right)_{i,j}.
\]

**Proposition 2.30.**

1. \(\text{Jac}((u_1, u_2, \ldots, u_r)/(v_1, v_2, \ldots, v_r))\) is a homogeneous element of \(S\) with degree \(\sum_i (d_i - e_i)\).
2. The family \((u_1, u_2, \ldots, u_r)\) is algebraically free if and only if \(\text{Jac}((u_1, u_2, \ldots, u_r)/(v_1, v_2, \ldots, v_r)) \neq 0\).
3. We have \(k[u_1, u_2, \ldots, u_r] = k[v_1, v_2, \ldots, v_r]\) if and only if \(\text{Jac}((u_1, u_2, \ldots, u_r)/(v_1, v_2, \ldots, v_r)) \in k^\times\).

**Proof (of 2.30).**

(1) is trivial.

Proof of (2).

(a) Assume that \((u_1, u_2, \ldots, u_r)\) is algebraically dependant.
Let $P(t_1, t_2, \ldots, t_r) \in k[t_1, t_2, \ldots, t_r]$ be a minimal degree polynomial subject to the condition $P(u_1, u_2, \ldots, u_r) = 0$. Let us differentiate that equality relatively to $v_j$:

$$
\sum_i \frac{\partial P}{\partial t_i}(u_1, u_2, \ldots, u_r) \frac{\partial u_i}{\partial v_j} = 0.
$$

There is $i$ such that $\frac{\partial P}{\partial t_i} \neq 0$, and by minimality of $P$ we have $\frac{\partial P}{\partial t_i}(u_1, \ldots, u_r) \neq 0$, which shows that the matrix $(\frac{\partial u_i}{\partial v_j})_{i,j}$ is singular and so that

$$
\text{Jac}((u_1, u_2, \ldots, u_r)/(v_1, v_2, \ldots, v_r)) = 0.
$$

(b) Assume that $(u_1, u_2, \ldots, u_r)$ is algebraically free.

For each $i$, let us denote by $P_i(t_0, t_1, \ldots, t_r) \in k[t_0, t_1, \ldots, t_r]$ a polynomial with minimal degree such that $P_i(v_i, u_1, u_2, \ldots, u_r) = 0$. Let us differentiate that equality relatively to $v_j$:

$$
\frac{\partial P_i}{\partial t_0}(v_i, u_1, u_2, \ldots, u_r) + \sum_l \frac{\partial P_i}{\partial t_l}(v_i, u_1, u_2, \ldots, u_r) \frac{\partial u_l}{\partial v_j} = 0,
$$

which can be rewritten as an identity between matrices:

$$
(\frac{\partial P_i}{\partial t_l}(v_i, u_1, u_2, \ldots, u_r))_{i,l} \cdot (\frac{\partial u_l}{\partial v_j})_{i,j} = -D((\frac{\partial P_i}{\partial t_0}(v_i, u_1, u_2, \ldots, u_r))_{i,l}),
$$

where $D((\lambda_i))$ denotes the diagonal matrix with spectrum $(\lambda_i)$.

Since, for all $i$, we have $\frac{\partial P_i}{\partial t_0}(v_i, u_1, u_2, \ldots, u_r) \neq 0$ (by minimality of $P_i$), we see that the matrix $(\frac{\partial u_l}{\partial v_j})_{i,j}$ is nonsingular.

(3) follows from 2.28 and from (1).

### 2.4.2 Systems of Parameters

Let $A$ be a finitely generated graded $k$–algebra.

**Definition 2.31.** A system of parameters of $A$ is a family $(x_1, x_2, \ldots, x_r)$ of homogeneous elements in $A$ such that

1. $(x_1, x_2, \ldots, x_r)$ is algebraically free,
2. $A$ is a finitely generated $k[x_1, x_2, \ldots, x_r]$–module.
We ask the reader to believe, to prove, or to check in the appropriate literature the following fundamental result.

**Theorem 2.32.**

1. There exists a system of parameters.
2. All systems of parameters have the same cardinal, equal to $\text{Krdim}(A)$.
3. If $(x_1, x_2, \ldots, x_m)$ is a system of homogeneous elements of $A$ such that $m \leq \text{Krdim}(A)$ and if $A$ is finitely generated as a $k[x_1, x_2, \ldots, x_m]$-module, then $m = \text{Krdim}(A)$ and $(x_1, x_2, \ldots, x_m)$ is a system of parameters of $A$.
4. The following assertions are equivalent.
   (i) There is a system of parameters $(x_1, x_2, \ldots, x_r)$ of $A$ such that $A$ is a free module over $k[x_1, x_2, \ldots, x_r]$.
   (ii) Whenever $(x_1, x_2, \ldots, x_r)$ is a system of parameters of $A$, $A$ is a free module over $k[x_1, x_2, \ldots, x_r]$.

In that case we say that $A$ is a Cohen-Macaulay algebra.

We shall now give some characterizations or systems of parameters of a polynomial algebra.

In what follows, we denote by

- $k$ an algebraically closed field,
- $S = k[v_1, v_2, \ldots, v_r]$ a polynomial algebra, where $(v_1, v_2, \ldots, v_r)$ is a family of homogeneous algebraically independent elements with degrees $(e_1, e_2, \ldots, e_r)$,
- $(u_1, u_2, \ldots, u_r)$ is a family of nonconstant homogeneous elements of $S$ with degrees respectively $(d_1, d_2, \ldots, d_r)$
- $R := k[u_1, u_2, \ldots, u_r]$, and $\mathfrak{M}$ the maximal graded ideal of $R$.

**Proposition 2.33.**

1. The following assertions are equivalent.
   (i) $(x = 0)$ is the unique solution in $k^r$ of the system
       
       $u_1(x) = u_2(x) = \cdots = u_r(x) = 0$.

   (ii) $S/\mathfrak{M}S$ is a finite dimensional $k$-vector space.
   (iii) $S$ is a finitely generated $R$-module.
   (iv) $(u_1, u_2, \ldots, u_r)$ is a system of parameters of $S$.

2. If the preceding conditions hold, then

3. $S$ is a free $R$-module, and its rank is $\prod_i d_i / \prod_i e_i$.

4. The map

   \[
   \begin{cases}
   k^r \rightarrow k^r \\
   x \mapsto (u_1(x), u_2(x), \ldots, u_r(x))
   \end{cases}
   
   
   is onto.
Proof (of 2.33). Let us prove (1).

- (i)⇒(ii). Since $S/\mathfrak{M}S$ is a finitely generated $k$–algebra, it suffices to prove that $S/\mathfrak{M}S$ is algebraic over $k$. Since the set $V(\mathfrak{M}S)$ of zeros of $\mathfrak{M}S$ reduces to $\{0\}$ by assumption, and since all the indeterminates $v_i$ vanish on that set, it follows from the strong Nullstellensatz that for all $i$ there is an integer $n_i \geq 1$ such that $v_i^{n_i} \in \mathfrak{M}S$, hence $v_i^{n_i} = 0$ in $S/\mathfrak{M}S$, proving that $S/\mathfrak{M}S$ is indeed an algebraic extension of $k$.

- (ii)⇒(iii) results from Nakayama lemma.

- (iii)⇒(iv) results from the general properties of systems of parameters (see 2.32, (3)).

- (iv)⇒(i). Let $V(\mathfrak{M}S)$ be the set of zeros of $\mathfrak{M}S$. In order to prove that $|V(\mathfrak{M}S)| \leq \dim(S/\mathfrak{M}S)$. Let $x_1, x_2, \ldots, x_n \in V(\mathfrak{M}S)$ be pairwise distinct. Consider the map

$$
\begin{cases}
S \to k^n \\
u \mapsto (u(x_1), u(x_2), \ldots, u(x_n))
\end{cases}
$$

That map factorizes through $S/\mathfrak{M}S$. But the interpolation theorem shows that it is onto, which proves that $n \leq \dim(S/\mathfrak{M}S)$.

Remark 2.34 (The interpolation theorem). Let $V$ be a $k$–vector space with dimension $r$, and let $S$ be its symmetric algebra, isomorphic to the algebra polynomial in $r$ indeterminates. Let $x_1, x_2, \ldots, x_n$ be pairwise distinct elements of $V$. Then the map

$$
\begin{cases}
S \to k^n \\
u \mapsto (u(x_1), u(x_2), \ldots, u(x_n))
\end{cases}
$$

is onto.

Indeed, for each pair $(i, j)$ with $i \neq j$, let us choose a linear form $t_{i,j} : V \to k$ such that $t_{i,j}(x_i) \neq t_{i,j}(x_j)$. Then the polynomial function $u_i$ on $V$ defined by

$$
\begin{align*}
u_i(v) := \prod_{i \neq j} \frac{t_{i,j}(v) - t_{i,j}(x_j)}{t_{i,j}(x_i) - t_{i,j}(x_j)}
\end{align*}
$$

satisfies $u_i(x_j) = \delta_{i,j}$.

Let us prove (2)

(a) Since $S$ is free over itself, it is Cohen-Macaulay (see 2.32, (4), hence is free over $R$. Thus we have

$S \simeq R \otimes_k (S/\mathfrak{M}S)$, which implies $\text{grdim}(S) = \text{grdim}(R)\text{grdim}(S/\mathfrak{M}S)$. 
It follows that
\[ \text{grdim}(S/M) = \prod_i (1 + q + \cdots + q^{d_i-1}) \]
\[ \prod_i (1 + q + \cdots + q^{e_i-1}) \]
hence
\[ \dim(S/M) = \text{grdim}(S/M)_{q=1} = \prod_i d_i \prod_i e_i. \]

(b) Let \( \lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r) \in k^r \). We are looking for \( \mu = (\mu_1, \mu_2, \ldots, \mu_r) \in k^r \) such that, for all \( i \) (1 \( \leq i \leq r \)), we have \( u_i(\mu) = \lambda_i \).

Consider the maximal ideal \( M_{\lambda} \) of \( R \) defined by \( \lambda \), i.e., the kernel of the morphism
\[ \varphi_{\lambda}: \begin{cases} R = k[u_1, u_2, \ldots, u_r] \longrightarrow k \\ u_j \mapsto \lambda_j. \end{cases} \]
By Cohen-Seidenberg theorem, there is a maximal ideal \( N \) of \( S \) such that \( N \cap R = M_{\lambda} \). By Nullstellensatz, there is \( \mu = (\mu_1, \mu_2, \ldots, \mu_r) \in k^r \) such that \( N = N_{\mu} \), i.e., \( N \) is the kernel of the morphism
\[ \psi_{\mu}: \begin{cases} S = k[v_1, v_2, \ldots, v_r] \longrightarrow k \\ v_i \mapsto \mu_i. \end{cases} \]
which, restricted to \( R \), is \( \varphi_{\lambda} \). Thus for all \( i \) we have \( u_i(\mu) = \lambda_i \).

### 2.4.3 The Chevalley Theorem

**Theorem 2.35.** Let \( S \) a polynomial algebra: there exist a system \((v_1, v_2, \ldots, v_r)\) of homogeneous algebraically independent elements such that \( S = k[v_1, v_2, \ldots, v_r] \). Let \( R \) be a graded subalgebra of \( S \) such that \( S \) is a finitely generated \( R \)-module.

The following assertions are equivalent:

(i) \( S \) is a free \( R \)-module,

(ii) \( R \) is a polynomial algebra: whenever \((u_1, u_2, \ldots, u_n)\) is a system of homogeneous elements of \( R \) which is a generating system for the maximal graded ideal \( M \) of \( R \), and such that \( n \) is minimal for that property, then \( n = r \), \( R = k[u_1, u_2, \ldots, u_r] \), and \((u_1, u_2, \ldots, u_n)\) is algebraically independent.

**Proof (of 2.35).** The implication (ii)\( \Rightarrow \) (i) results from the fact that \( S \) is Cohen–Macaulay (see 2.32).

**Remark 2.36.** The implication (i)\( \Rightarrow \) (ii) has a natural homological proof (see for example [Se2]): in order to prove that \( R \) is a regular graded algebra, it
suffices to prove that it has finite global dimension, which results easily from the same property for \( S \) and from the fact that \( S \) is free over \( R \). We provide below a self-contained and elementary proof, largely inspired by [Bou1], chap. V, §5, Lemme 1.

Let \((u_1, u_2, \ldots, u_n)\) be a system of homogeneous elements of \( R \) which is a generating system for the maximal graded ideal \( \mathfrak{M} \) of \( R \), and assume that \( n \) is minimal for that property. It is clear that \( R \) is generated by \((u_1, u_2, \ldots, u_n)\) as a \( k \)-algebra. We shall prove that \((u_1, u_2, \ldots, u_n)\) is algebraically independent (from which it results that \( n = r \)).

Assume not. Let \( k[t_1, t_2, \ldots, t_n] \) be the polynomial algebra in \( n \) indeterminates, graduated by \( \deg t_i := \deg u_i \). Let \( P(t_1, t_2, \ldots, t_m) \in k[t_1, t_2, \ldots, t_m] \) be a homogeneous polynomial with minimal degree such that

\[ P(u_1, u_2, \ldots, u_n) = 0. \]

Let us set \( \delta_i := \frac{\partial P}{\partial t_i}(u_1, u_2, \ldots, u_n) \) and let us denote by \( \delta \mathfrak{M} \) the (graded) ideal of \( R \) generated by \((\delta_1, \delta_2, \ldots, \delta_n)\).

Choose \( I \subseteq \{1, 2, \ldots, n\} \) minimal such that \( \delta \mathfrak{M} \) is generated by the family \((\delta_i)_{i \in I} \). So we have

\[ (\forall j \notin I) \quad \delta_j = \sum_{i \in I} a_{i,j} \delta_i \quad \text{with } a_{i,j} \in R. \]

Since we have for all \( l \)

\[ 0 = \frac{\partial P}{\partial v_l}(u_1, u_2, \ldots, u_n) = \sum_{i=1}^{n} \delta_i \cdot \frac{\partial u_i}{\partial v_l}(u_1, u_2, \ldots, u_n), \]

replacing \( \delta_j \) (for \( j \notin I \)) by its value we get

\[ \sum_{i \in I} \delta_i \left( \frac{\partial u_i}{\partial v_l} + \sum_{j \notin I} a_{i,j} \frac{\partial u_j}{\partial v_l} \right) = 0 \quad (\star) \]

Let us set \( x_{i,l} := \frac{\partial u_i}{\partial v_l} + \sum_{j \notin I} a_{i,j} \frac{\partial u_j}{\partial v_l} \) so that the relation \((\star)\) becomes

\[ \sum_{i \in I} x_{i,l} \delta_i = 0. \quad (\star) \]

- We shall prove that \( x_{i,l} \in \mathfrak{M} S \).

For that purpose, let us remember the hypothesis by introducing a basis \((e_\alpha)_\alpha\) of \( S \) as an \( R \)-module. We have
2.4 Polynomial Algebras and Parameters Subalgebras

\[ x_{i,l} = \sum_{\alpha} \lambda_{i,l,\alpha} e_{\alpha} \]

with \( \lambda_{i,l,\alpha} \in R \). We want to prove that, for all \( i, j, \alpha \), we have \( \lambda_{i,l,\alpha} \in \mathfrak{M} \).

The relation (*) implies that, for all \( l \) and \( \alpha \),

\[ \sum_{i \in I} \lambda_{i,l,\alpha} \delta_{i} = 0. \]

Assume that for some \( i_0, l_0, \alpha_0 \), we have \( \lambda_{i_0,l_0,\alpha_0} \notin \mathfrak{M} \). Let us then consider the projection of the above equality onto the space of elements with degree \( \deg \delta_{i_0} \). We get a relation

\[ \sum_{i \in I} \lambda'_{i_0,l_0,\alpha_0} \delta_{i} = 0 \text{ where } \lambda'_{i_0,l_0,\alpha_0} \in k^x, \]

i.e., an expression of \( \delta_{i_0} \) as linear combination of the \( \delta_{i} \) (\( i \neq i_0 \)), a contradiction with the minimality of \( I \).

\[ \bullet \] Let us multiply by \( v_l \) both sides of the equality \( x_{i,l} := \frac{\partial u_i}{\partial v_l} + \sum_{j \in I} a_{i,j} \frac{\partial u_j}{\partial v_l} \)

which defines \( x_{i,l} \), and then sum up over \( l = 1, 2, \ldots, r \). By the Euler relation, we get (for \( i \in I \))

\[ \deg(u_i)u_i + \sum_{j \notin I} a_{i,j} \deg(u_j)u_j = \sum_{l} x_{i,l} v_l. \]

Since \( x_{i,l} \in \mathfrak{M}S \), the above equality shows that (for \( i \in I \))

\[ \deg(u_i)u_i + \sum_{j \notin I} a_{i,j} \deg(u_j)u_j = \sum_{l} x_{i,l} u_l \]

where, for all \( l \), \( x_l \) is a positive degree (homogeneous) element of \( S \). Projecting onto the space of elements with degree \( \deg(u_i) \), we get that, for all \( i \in I \), \( u_i \) is a linear combination (with coefficients in \( S \)) of the \( u_j \) (\( j \neq i \)).

\[ \bullet \] Since \( S \) is free as an \( R \)-module, it results from Nakayama’s lemma that any system of elements of \( S \) which defines a \( k \)-basis of \( R/\mathfrak{M}R \) is also an \( R \)-basis of \( S \). In particular there exists a basis of \( S \) over \( R \) which contains \( 1 \), and so there is an \( R \)-linear projection \( \pi : S \twoheadrightarrow R \).

Now if \( u_i = \sum_{l \neq i} y_l u_l \) with \( y_l \in S \), by applying \( \pi \) to that equality we get \( u_i = \sum_{l \neq i} \pi(y_l)u_l \), an \( R \)-linear dependance relation on the set of \( (u_l)_{1 \leq l \leq n} \), a contradiction with the minimality of \( n \).
Introduction to Complex Reflection Groups and Their Braid Groups
Broué, M.
2010, XII, 144 p., Softcover
ISBN: 978-3-642-11174-7