Graduate Course

Algebra IV (Math. 203)

(Santa Cruz, fall 2006)

35 hours (+ 10 hours: problem sessions)

Table of contents

Part 0. Introduction

Rings are the most common objects in **algebra**. You encountered them in all areas:

LINEAR ALGEBRA: $\mathrm{Mat}_n(R)$, where R is a ring.

GROUP THEORY: Let G be a group (finite or not). Study of the group algebra $R[G]$ (or RG), where R is a commutative ring (*representation theory*).

NUMBER THEORY: $\mathbb{Z}$ or, more generally, the ring of algebraic integers of a finite algebraic extension of $\mathbb{Q}$.

ALGEBRAIC GEOMETRY: $K[X_1, \ldots, X_n]$ and all its quotients, where K is a field.

Among the theorems proved during this course, here are a few examples:

Skolem-Noether Theorem. *Let R be a commutative ring having only one maximal ideal (i.e. a commutative local ring) and let $\sigma : \mathrm{Mat}_n(R) \to \mathrm{Mat}_n(R)$ be an automorphism of R-algebras. Then there exists $a \in \mathrm{Mat}_n(R)^\times$ such that $\sigma(M) = aMa^{-1}$ for every $M \in \mathrm{Mat}_n(R)$.*

Theorem (Maschke, Wedderburn,...). *Let G be a finite group. Then there is an isomorphism of $\mathbb{C}$-algebras $\mathbb{C}[G] \simeq \mathrm{Mat}_{n_1}(\mathbb{C}) \times \cdots \times \mathrm{Mat}_{n_r}(\mathbb{C})$ for some n_i's. Moreover, r is the number of conjugacy classes of G.*

Hilbert's Basis Theorem. *Let I be an ideal of $K[X_1, \ldots, X_n]$. Then I is finitely generated.*

Hilbert's Nullstellensatz. *Let K be an algebraically closed field and let $\mathfrak{m}$ be a maximal ideal of $K[X_1, \ldots, X_n]$. Then the K-algebra $K[X_1, \ldots, X_n]/\mathfrak{m}$ is isomorphic to K.*

Theorem. *Let K be a finite algebraic extension of $\mathbb{Q}$ and let $\mathcal{O}_K$ denote the ring of integers of K (over $\mathbb{Z}$). Then $\mathcal{O}_K$ is integrally closed, all its ideals are finitely generated and all its non-zero prime ideals are maximal (i.e. $\mathcal{O}_K$ is a Dedekind domain).*

All these theorems have in common that their proof relies on the theory of modules. This course will be organized as follows:

Part I - some *category theory*: definition, examples, functors, equivalences...

Part II - module theory: tensor product, Noetherian rings and modules (including Hilbert's Basis Theorem), projective and injective modules, simple semisimple rings and modules, radical, Morita equivalences (application to Skolem-Noether Theorem)...

Part III - integral extensions, Dedekind domains...

Part IV - background of algebraic geometry: Hilbert's Nullstellensatz, affine varieties, tangent spaces...

Approximative schedule (one lecture = 1h45):

- Categories: 1 lecture
- Tensor products: 2 lectures
- Noetherian and Artinian modules and rings: 2 lectures
- Projective, injective modules: 2 lectures
- Jacobson radical: 2 lectures
- Semisimple rings and modules: 3 lectures
- Dedekind domains: 2 lectures
- Affine algebraic sets: 2 lectures
- Noether's Normalization Theorem and Hilbert's Nullstellensatz: 2 lectures
- Geometric properties of algebraic sets: 2 lectures

Part I. Categories

The aim of this part is to give an introduction to the language of *categories*, which will be used freely during this course.

1. Definition, examples

Definition 1.1. *A* ***category*** $\mathbf{Cat}$ *consists of:*

- *a class of objects* $\mathrm{ob}(\mathbf{Cat})$ *called the* ***objects*** *of* $\mathbf{Cat}$*;*
- *for any objects* C, $C' \in \mathrm{ob}(\mathbf{Cat})$*, a set* $\mathrm{Hom}_{\mathbf{Cat}}(C, C')$ *called the* ***morphisms*** *from* C *to* C'*;*
- *for any three objects* C, C' *and* $C'' \in \mathrm{ob}(\mathbf{Cat})$*, a map* $\mathrm{Hom}_{\mathbf{Cat}}(C, C') \times \mathrm{Hom}_{\mathbf{Cat}}(C', C'') \to \mathrm{Hom}_{\mathbf{Cat}}(C, C'')$*,* $(f, g) \mapsto g \circ f$ *called a* ***composition law****;*

satisfying:

(C1) $\mathrm{Hom}_{\mathbf{Cat}}(C_1, C_1')$ *is disjoint from* $\mathrm{Hom}_{\mathbf{Cat}}(C_2, C_2')$ *unless* $C_1 = C_2$ *and* $C_1' = C_2'$*;*

(C2) *for all* C, C', C'', $C''' \in \mathrm{ob}(\mathbf{Cat})$ *and all* $f \in \mathrm{Hom}_{\mathbf{Cat}}(C, C')$, $g \in \mathrm{Hom}_{\mathbf{Cat}}(C', C'')$ *and* $\mathrm{Hom}_{\mathbf{Cat}}(C'', C''')$*, we have* $h \circ (g \circ f) = (h \circ g) \circ f$ *(associativity);*

(C3) *for each* $C \in \mathrm{ob}(\mathbf{Cat})$*, there exists a morphism* $1_C \in \mathrm{Hom}_{\mathbf{Cat}}(C, C)$ *such that, for all* C', $C'' \in \mathrm{ob}(\mathbf{Cat})$ *and all* $f \in \mathrm{Hom}_{\mathbf{Cat}}(C, C')$ *and* $g \in \mathrm{Hom}_{\mathbf{Cat}}(C'', C)$*, we have* $f \circ 1_C = f$ *and* $1_C \circ g = g$*.*

Note that 1_C is uniquely determined by (C3) (it is called the *identity morphism* of C and is often denoted by Id_C). We will often write $f : C \to C'$ or $C \xrightarrow{f} C'$ to indicate that $f \in \mathrm{Hom}_{\mathbf{Cat}}(C, C')$. We also write $C \in \mathbf{Cat}$ instead of $C \in \mathrm{ob}(\mathbf{Cat})$.

Examples 1.2 - (1) **Sets** (respectively **sets**) the category of sets (respectively finite sets), with maps as morphisms and composition law as usual.

(2) **Groups** (respectively **groups**, **Ab**, **Rings**, $\mathbf{Rings}_c$, **Fields**,...) the category of groups (respectively finite groups, abelian groups, rings, commutative rings, fields,...) together with their natural homomorphisms (rings are assumed to be unitary and morphisms to be unitary morphisms).

(3) For $R \in \mathbf{Rings}$, let ${}_R\mathbf{Mod}$ (respectively ${}_R\mathbf{mod}$, $\mathbf{Mod}_R$, $\mathbf{mod}_R$) denote the category of left R-modules (respectively finitely generated left R-modules, right R-modules, finitely generated right R-modules). We write $\mathrm{Hom}_R(M, N)$ for $\mathrm{Hom}_{{}_R\mathbf{Mod}}(M, N)$ or $\mathrm{Hom}_{\mathbf{Mod}_R}(M, N)$. Recall that $f \in \mathrm{Hom}_R(M, N)$ if $f(m + m') = f(m) + f(m')$ and $f(rm) = rf(m)$ for all $r \in R$, m, $m' \in M$.

(4) **Top** the category of topological spaces where morphisms are continuous maps. □

2. Functors

Definition 2.1. *Let* $\mathbf{C}$ *and* $\mathbf{D}$ *be two categories. A* ***covariant functor*** $\mathcal{F} : \mathbf{C} \to \mathbf{D}$ *consists of "correspondences":*

- $\mathcal{F} : \mathrm{ob}(\mathbf{C}) \to \mathrm{ob}(\mathbf{D})$, $C \mapsto \mathcal{F}(C)$;
- *A map* $\mathcal{F} : \mathrm{Hom}_{\mathbf{C}}(C, C') \to \mathrm{Hom}_{\mathbf{D}}(\mathcal{F}(C), \mathcal{F}(C'))$, $f \mapsto \mathcal{F}(f)$ *for all* C, $C' \in \mathrm{ob}(\mathbf{C})$;

satisfying

(F1) *for all* C, C' *and* $C'' \in \mathrm{ob}(\mathbf{C})$ *and all* $f \in \mathrm{Hom}_{\mathbf{C}}(C, C')$ *and* $g \in \mathrm{Hom}_{\mathbf{C}}(C', C'')$, $\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$;

(F2) *for all* $C \in \mathrm{ob}(\mathbf{C})$, $\mathcal{F}(1_C) = 1_{\mathcal{F}(C)}$.

A *contravariant functor* $\mathcal{F} : \mathbf{C} \to \mathbf{D}$ is defined in the same way except that $\mathcal{F} : \mathrm{Hom}_{\mathbf{C}}(C, C') \to \mathrm{Hom}_{\mathbf{D}}(\mathcal{F}(C'), \mathcal{F}(C))$ reverse arrows and that the equality in (F1) is replaced by $\mathcal{F}(g \circ f) = \mathcal{F}(f) \circ \mathcal{F}(g)$.

Examples 2.2 - (1) $\mathrm{Id}_{\mathbf{C}} : \mathbf{C} \to \mathbf{C}$, $C \mapsto C$, $f \mapsto f$ is a covariant functor called the *identity functor*.

(2) Functors can be composed to get a new functor.

(3) *Forgetful functors:* a functor that *forgets* part of the structure of the objects. For instance, $\mathbf{Rings} \to \mathbf{Sets}$, $R \mapsto R$, $f \mapsto f$. Or $\mathbf{Fields} \to \mathbf{Ab}$, $K \mapsto K^+$, $f \mapsto f$...

(4) If $X \in \mathbf{C}$, then $\mathrm{Hom}_{\mathbf{C}}(X, -) : \mathbf{C} \to \mathbf{Sets}$, $C \mapsto \mathrm{Hom}_{\mathbf{C}}(X, C)$, $f \mapsto (g \mapsto f \circ g)$ is a covariant functor. On the other hand, $\mathrm{Hom}_{\mathbf{C}}(-, X) : \mathbf{C} \to \mathbf{Sets}$, $C \mapsto \mathrm{Hom}_{\mathbf{C}}(-, X)$, $f \mapsto (g \mapsto g \circ f)$ is a contravariant functor.

(5) $\mathcal{F} : \mathbf{Groups} \to \mathbf{Sets}$, $G \mapsto \mathcal{F}(G) = \{g \in G \mid g^2 = 1\}$, $f \mapsto f|_{\mathcal{F}(G)}$. □

Definition 2.3. *Let* $\mathcal{F}$, $\mathcal{G} : \mathbf{C} \to \mathbf{D}$ *be covariant functors between two categories* $\mathbf{C}$ *and* $\mathbf{D}$. *A* ***natural transformation*** *(or a* ***functorial morphism****)* $\varphi : \mathcal{F} \to \mathcal{G}$ *is a family of morphisms* $\varphi_C : \mathcal{F}(C) \to \mathcal{G}(C)$ *satisfying*

(NT) *For any morphism* $f : C \to C'$ *in* $\mathbf{C}$, *the following diagram*

$$\begin{array}{ccc} \mathcal{F}(C) & \xrightarrow{\varphi_C} & \mathcal{G}(C) \\ \Big\downarrow{\scriptstyle \mathcal{F}(f)} & & \Big\downarrow{\scriptstyle \mathcal{G}(f)} \\ \mathcal{F}(C') & \xrightarrow{\varphi_{C'}} & \mathcal{G}(C') \end{array}$$

is commutative.

One can define similarly a ***natural transformation*** *between contravariant functors.*

Definition 2.4. *A natural transformation* $\varphi : \mathcal{F} \to \mathcal{G}$ *between two (covariant or contravariant) functors is called a* ***natural isomorphism*** *if* φ_C *is an isomorphism for all* $C \in \mathbf{C}$. *Two functors* $\mathcal{F}$ *and* $\mathcal{G}$ *are said* ***naturally isomorphic*** *if there exists a natural isomorphism* $\mathcal{F} \to \mathcal{G}$: *we then write* $\mathcal{F} \sim \mathcal{G}$.

EXAMPLES 2.5 - (1) If $R \in \mathbf{Rings}_c$ and if M is a left R-module, we define $M^* = \mathrm{Hom}_R(M, R)$. Then $\mathcal{F} : {}_R\mathbf{Mod} \to {}_R\mathbf{Mod}$, $M \mapsto M^*$ is a functor (see Example 2.2 (4)). Now, we define $\varphi_M : M \to (M^*)^*$, $m \mapsto (\lambda \in M^* \mapsto \lambda(m) \in R)$. Then $\varphi : \mathrm{Id}_{{}_R\mathbf{Mod}} \to \mathcal{F} \circ \mathcal{F}$ is a natural transformation.

If R is a field, and if we replace ${}_R\mathbf{Mod}$ by ${}_R\mathbf{mod}$, then φ is a natural isomorphism.

(2) If $f : X \to X'$ is a morphism in the category $\mathbf{C}$, we define, for every $C \in \mathbf{C}$, $\tilde{f}_C : \mathrm{Hom}_{\mathbf{C}}(C, X) \to \mathrm{Hom}_{\mathbf{C}}(C, X')$, $g \mapsto f \circ g$. Then $\tilde{f}$ defines a natural transformation $\mathrm{Hom}_{\mathbf{C}}(-, X) \to \mathrm{Hom}_{\mathbf{C}}(-, X')$. It is a natural isomorphism if and only if f is an isomorphism. Similarly, one gets a natural transformation $\mathrm{Hom}_{\mathbf{C}}(X', -) \to \mathrm{Hom}_{\mathbf{C}}(X, -)$. □

Definition 2.6. *A covariant functor $\mathcal{F} : \mathbf{C} \to \mathbf{D}$ is called an **isomorphism of categories** if there exists a covariant functor $\mathcal{G} : \mathbf{D} \to \mathbf{C}$ such that $\mathcal{F} \circ \mathcal{G} = \mathrm{Id}_{\mathbf{D}}$ and $\mathcal{G} \circ \mathcal{F} = \mathrm{Id}_{\mathbf{C}}$. It is called an **equivalance of categories** if there exists a covariant functor $\mathcal{G} : \mathbf{D} \to \mathbf{C}$ such that $\mathcal{F} \circ \mathcal{G} \sim \mathrm{Id}_{\mathbf{D}}$ and $\mathcal{G} \circ \mathcal{F} \sim \mathrm{Id}_{\mathbf{C}}$.*

EXAMPLES 2.7 - (1) If R is a ring, we denote by R° the *opposite ring* of R: as a set, this is R but, if r and s are two elements of R, and if we denote them r° and s° when we see them in R°, then the multiplication is given by $r^\circ s^\circ = (sr)^\circ$. If $f : R \to S$ is an homomorphism of rings, let $f^\circ : R^\circ \to S^\circ$, $r^\circ \mapsto f(r)^\circ$. It is also an homomorphism of rings. Then $\mathbf{Rings} \to \mathbf{Rings}$, $R \mapsto R^\circ$, $f \mapsto f^\circ$ is a covariant functor. Note that if we compose it with itself, we get the identity functor. So it is an isomorphism of categories.

(2) If K is a field, then ${}_K\mathbf{mod} \to {}_K\mathbf{mod}$, $V \mapsto (V^*)^*$ is an equivalence of categories (see Example 2.5 (1)). Note that ${}_K\mathbf{Mod} \to {}_K\mathbf{Mod}$, $V \mapsto (V^*)^*$ is not an equivalence of categories.

(3) If M is a left R-module, we denote by M° the right R°-module defined as follows: as a set, this is M but $m^\circ.r^\circ = (rm)^\circ$, with obvious notation. Similarly, if M is a right R-module, then we can define M° to be a left R°-module. Then ${}_R\mathbf{Mod} \to \mathbf{Mod}_{R^\circ}$, $M \mapsto M^\circ$, $f \mapsto f$ is a covariant isomorphism of categories. □

Definition 2.8. *Let $\mathcal{F} : \mathbf{C} \to \mathbf{D}$ and $\mathcal{G} : \mathbf{D} \to \mathbf{C}$ be two covariant functors. We say that $\mathcal{F}$ is **left adjoint** to $\mathcal{G}$ (or $\mathcal{G}$ is **right adjoint** to $\mathcal{F}$) if, for all $C \in \mathbf{C}$ and $D \in \mathbf{D}$, we have a bijection $\gamma_{CD} : \mathrm{Hom}_{\mathbf{C}}(C, \mathcal{G}(D)) \to \mathrm{Hom}_{\mathbf{D}}(\mathcal{F}(C), D)$ such that, if $f : C \to C'$ in $\mathbf{C}$, the following diagram*

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{C}}(C', \mathcal{G}(D)) & \xrightarrow{\gamma_{C'D}} & \mathrm{Hom}_{\mathbf{D}}(\mathcal{F}(C'), D) \\ \downarrow{\scriptstyle \mathrm{Hom}_{\mathbf{C}}(f, \mathcal{G}(D))} & & \downarrow{\scriptstyle \mathrm{Hom}_{\mathbf{D}}(\mathcal{F}(f), D)} \\ \mathrm{Hom}_{\mathbf{C}}(C, \mathcal{G}(D)) & \xrightarrow{\gamma_{CD}} & \mathrm{Hom}_{\mathbf{D}}(\mathcal{F}(C'), D) \end{array}$$

and similarly for all $g : D \to D'$ in $\mathbf{D}$.

Exercises from Part I

Exercise I.1. Show that **Posets** (partially ordered sets together where morphisms are non-decreasing maps) is a category.

Exercise I.2. Let $\mathbf{C}$ and $\mathbf{D}$ be two categories. We define the product $\mathbf{C} \times \mathbf{D}$ as follows. First, $\mathrm{ob}(\mathbf{C} \times \mathbf{D})$ consists of ordered pairs (C, D) where $C \in \mathrm{ob}(\mathbf{C})$ and $D \in \mathrm{ob}(\mathbf{D})$. Then, if (C, D), $(C', D') \in \mathrm{ob}(\mathbf{C}, \mathbf{D})$, we define $\mathrm{Hom}_{\mathbf{C}\times\mathbf{D}}((C, D), (C', D')) = \mathrm{Hom}_{\mathbf{C}}(C, C') \times \mathrm{Hom}_{\mathbf{D}}(D, D')$. Finally, the composition law is defined by $(f, g) \circ (f', g') = (f \circ f', g \circ g')$. Show that $\mathbf{C} \times \mathbf{D}$ is a category (it is called the *product category* of $\mathbf{C}$ and $\mathbf{D}$).

Exercise I.3. Let **Cat** be a category. Let $\mathbf{Cat}^\circ$ be defined as follows: $\mathrm{ob}(\mathbf{Cat}^\circ) = \mathrm{ob}(\mathbf{Cat})$ and, if C, $C' \in \mathrm{ob}(\mathbf{Cat}^\circ)$, we set $\mathrm{Hom}_{\mathbf{Cat}^\circ}(C, C') = \mathrm{Hom}_{\mathbf{Cat}}(C', C)$ (and we reverse the composition law). Show that $\mathbf{Cat}^\circ$ is a category (it is called the *dual category* to **Cat**).

Let $\mathcal{D} : \mathbf{Cat} \to \mathbf{Cat}^\circ$, $C \mapsto C$, $f \in \mathrm{Hom}_{\mathbf{Cat}}(C, C') \mapsto f \in \mathrm{Hom}_{\mathbf{Cat}^\circ}(C', C)$. Show that $\mathcal{D}$ is a contravariant functor. Show that $\mathcal{D} \circ \mathcal{D} = \mathrm{Id}_{\mathbf{Cat}}$.

If $\mathbf{D}$ is another category, show that a covariant (respectively contravariant) functor $\mathcal{F} : \mathbf{Cat} \to \mathbf{D}$ induces a contravariant (respectively covariant) functor $\mathcal{F}^\circ : \mathbf{Cat}^\circ \to \mathbf{D}$.

Exercise I.4. Let R be a ring and let X be a set. Let $R[X]$ be the *free left module with basis* X: this is the set of formal R-linear combinations $\sum_{x\in X} r_x x$, where $(r_x)_{x\in X}$ is any family of elements of R such that all but a finite number of the r_x's are zero. An element $x \in X$ is identified with the formal R-linear combination $\sum_{y\in X} \delta_{xy} x$, where $\delta_{xy} = 1$ if $x = y$ and $\delta_{xy} = 0$ otherwise.

(a) Prove that $R[X]$ is naturally a left R-module.
(b) Prove that X is an R-basis of $R[X]$ for its structure of left module.
(c) Let $\varphi : X \to M$ be a map, where M is a left R-module. Show that there is a unique R-linear map $\gamma_{XM}(\varphi) : R[X] \to M$ which extends φ.
(d) If $f : X \to Y$ is a map, show that the map $f_* : R[X] \to R[Y]$, $\sum_{x\in X} r_x x \mapsto \sum_{x\in X} r_x f(x)$ is well-defined and is a morphism of R-modules.
(e) If $f : X \to Y$ and $g : Y \to Z$ are maps, prove that $(g \circ f)_* = g_* \circ f_*$.
(f) Show that, if f is surjective (respectively injective, respectively surjective), then so is f_*.
(g) In general, compute $\mathrm{Ker}\, f_*$ and $\mathrm{Im}\, f_*$.
(h) Prove that $\mathcal{F} : \mathbf{Sets} \to {}_R\mathbf{Mod}$, $X \mapsto R[X]$, $f \mapsto f_*$ is a covariant functor.
(i) Let $\mathcal{G} : {}_R\mathbf{Mod} \to \mathbf{Sets}$ be the forgetful functor. Show that $\mathcal{F}$ is a left adjoint to $\mathcal{G}$ (Hint: use (c)).

Exercise I.5. Let G be a group. Show that the map

$$\begin{array}{ccc} R[G] \times R[G] & \longrightarrow & R[G] \\ (\sum_{g\in G} r_g g, \sum_{g\in G} r'_g g) & \longmapsto & \sum_{g,g'\in G} r_g r'_{g'} gg' \end{array}$$

endows $R[G]$ with a ring structure.

If $f : G \to H$ is a morphism of groups, show that the map $f_* : R[G] \to R[H]$ defined in Exercise I.4 is a morphism of rings. Show that $\mathbf{Groups} \to \mathbf{Rings}$, $G \mapsto R[G]$, $f \mapsto f_*$ is a covariant functor.

Let $\mathrm{inv} : G \to G$, $g \mapsto g^{-1}$ and assume that R is commutative. Show that inv_* induces an isomorphism of rings $R[G] \simeq R[G]^\circ$.

Exercise I.6. Let $n \geqslant 1$. Let

$$I = \{ \begin{pmatrix} a_1 & \cdots & a_n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \mid a_1, \ldots, a_n \in R \}$$

and

$$J = \{ \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} \mid a_1, \ldots, a_n \in R \}.$$

(a) Show that I (respectively J) is a left (respectively right) ideal of $\mathrm{Mat}_n(R)$.
(b) Show that the map $\mathrm{Mat}_n(R^\circ) \to \mathrm{Mat}_n(R)^\circ$, $M \mapsto ({}^tM)^\circ$ is an isomorphism of rings.
(c) If R is commutative, show that $I \simeq J^\circ$.

Exercise I.7*. Let G be a group. A *G-set* is a set G endowed with an action of G. If X and Y are two G-sets, a map $f : X \to Y$ is called *G-equivariant* if, for all $g \in G$ and $x \in X$, we have $f(gx) = gf(x)$.

(a) Show that $G - \mathbf{Sets}$ (where objects are G-sets and morphisms are G-equivariant maps) is a category.
(b) Let H be a subgroup of G. If X is a G-set, let $\mathrm{Res}^G_H X$ denote the set X endowed with the H-action obtained by restriction from G. Show that $\mathrm{Res}^G_H : G - \mathbf{Sets} \to H - \mathbf{Sets}$ is a covariant functor.
(c) Let $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ (this is the *normalizer* of H in G). Show that $N_G(H)$ is a subgroup of G having H as a normal subgroup.
(d) If X is a G-set, let $X^H = \{x \in X \mid \forall\, h \in H,\ hx = x\}$. Show that $N_G(H)$ stabilizes X^H.
(e) Show that $G - \mathbf{Sets} \to N_G(H)/H - \mathbf{Sets}$, $X \mapsto X^H$ is a covariant functor.

Exercise I.8. If R is a ring, let $\mathcal{U}(R) = R^\times$ denote the group of units of R.

(a) Show that $\mathcal{U} : \mathbf{Rings} \to \mathbf{Groups}$ is a covariant functor.
(b) Show that $\mathrm{Mat}_n : \mathbf{Rings} \to \mathbf{Rings}$, $R \mapsto \mathrm{Mat}_n(R)$ is a covariant functor.
(c) Show that $\mathbf{GL}_n : \mathbf{Rings} \to \mathbf{Groups}$, $R \mapsto \mathbf{GL}_n(R)$ is a covariant functor.
(d) Show that $\det_R : \mathbf{GL}_n(R) \to \mathcal{U}(R)$, $g \mapsto \det(g)$ (which is only defined if R is commutative) defines a natural transformation between $\mathbf{GL}_n : \mathbf{Rings}_c \to \mathbf{Groups}$ and $\mathcal{U} : \mathbf{Rings}_c \to \mathbf{Groups}$.

Exercise I.9. Let $\mathcal{F} : \mathbf{C} \to \mathbf{D}$ be an equivalence of categories. Show that the map $\mathrm{Hom}_{\mathbf{C}}(C, C') \to \mathrm{Hom}_{\mathbf{D}}(\mathcal{F}(C), \mathcal{F}(C'))$, $f \mapsto \mathcal{F}(f)$ is bijective for all objects C, $C' \in \mathbf{C}$.

Part II. Modules

3. Tensor product

3.A. Definitions. Let M, N and A be three $\mathbb{Z}$-modules (i.e. abelian groups).

Definition 3.1. *A map $f : M \times N \to A$ is called **bilinear** if, for all m, $m' \in M$ and n, $n' \in N$, we have*

$$f(m+m',n) = f(m,n) + f(m',n)$$

and

$$f(m,n+n') = f(m,n) + f(m,n').$$

The set of bilinear maps $M \times N \to A$ forms an abelian group denoted by $\mathrm{Bil}(M,N;A)$.

Proposition 3.2. *If $f \in \mathrm{Bil}(M,N;A)$, if $(m,n) \in M \times N$ and if $z \in \mathbb{Z}$, then $f(zm,n) = f(m,zn) = zf(m,n)$. In particular, $f(0,n) = f(m,0) = 0$.*

Proposition 3.3. *We have:*

(a) $\mathrm{Bil}(M \oplus M', N; A) = \mathrm{Bil}(M,N;A) \oplus \mathrm{Bil}(M',N;A)$.
(b) $\mathrm{Bil}(M, N \oplus N'; A) = \mathrm{Bil}(M,N;A) \oplus \mathrm{Bil}(M,N';A)$.
(c) $\mathrm{Bil}(M,N; A \oplus A') = \mathrm{Bil}(M,N;A) \oplus \mathrm{Bil}(M,N;A')$.

Proof - We just prove (a) when $|I| = 2$ (the other properties are proved similarly). If $f \in \mathrm{Bil}(M \oplus M', N; A)$, let f_M denote its restriction to $M \times N$ ($\subseteq (M \oplus M') \times N$) and $f_{M'}$ denote its restriction to $M' \times N$. Then f_M and $f_{M'}$ are bilinear. Now, let

$$\begin{array}{rccc} \sigma : & \mathrm{Bil}(M \oplus M', N; A) & \longrightarrow & \mathrm{Bil}(M,N;A) \oplus \mathrm{Bil}(M',N;A) \\ & f & \longmapsto & f_M + f_{M'}. \end{array}$$

Then φ is injective: indeed, if $\varphi(f) = 0$, then $f_M = 0$ and $f_{M'} = 0$, then $f(m+m',n) = f_M(m,n) + f_{M'}(m',n) = 0$ for every $m \in M$, $m' \in M'$ and $n \in N$. So $f = 0$.

On the other hand, φ is surjective: if $g \in \mathrm{Bil}(M,N;A)$ and $g' \in \mathrm{Bil}(M',N;A)$, then the map $f : (M \oplus M') \times N \to A$, $(m+m',n) \mapsto g(m,n) + g'(m',n)$ is bilinear and $\varphi(f) = (g.g')$. ■

Examples 3.4 - (1) If R is a ring, the map $R \times R \to R$, $(a,b) \mapsto ab$ is bilinear.

(2) If $\sigma : A \to B$ is a morphism of abelian groups, then $\mathrm{Bil}(M,N;A) \to \mathrm{Bil}(M,N;B)$, $f \mapsto \sigma \circ f$ is well-defined.

(3) If $\gcd(m,n) = 1$, then $\mathrm{Bil}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}; A) = 0$. Indeed, if $f \in \mathrm{Bil}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}; A)$, let $(x,y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and let $a = f(x,y)$. Then $ma = f(mx,y) = f(0,y) = 0$. Similarly, $na = f(x,ny) = 0$. But, since m and n are coprime, there exists μ and ν in $\mathbb{Z}$ such that $\mu m + \nu n = 1$. Therefore, $a = \mu ma + \nu na = 0$. □

Definition 3.5. *Now, let R be a ring. If moreover M is a right R-module and N is a left R-module, a map $f : M \times N \to A$ is called* ***R-balanced*** *if $f(mr, n) = f(m, rn)$ for every $r \in R$, $m \in M$ and $n \in N$. The set of R-balanced bilinear maps $M \times N \to A$ will be denoted by $\mathrm{Bil}_{R-\mathrm{bal}}(M, N; A)$. It is an abelian group.*

Proposition 3.6. *We have:*

(a) $\mathrm{Bil}_{R-\mathrm{bal}}(M \oplus M', N; A) = \mathrm{Bil}_{R-\mathrm{bal}}(M, N; A) \oplus \mathrm{Bil}_{R-\mathrm{bal}}(M', N; A)$.
(b) $\mathrm{Bil}_{R-\mathrm{bal}}(M, N \oplus N'; A) = \mathrm{Bil}_{R-\mathrm{bal}}(M, N; A) \oplus \mathrm{Bil}_{R-\mathrm{bal}}(M, N'; A)$.
(c) $\mathrm{Bil}_{R-\mathrm{bal}}(M, N; A \oplus A') = \mathrm{Bil}_{R-\mathrm{bal}}(M, N; A) \oplus \mathrm{Bil}_{R-\mathrm{bal}}(M, N; A')$.
(d) $\mathrm{Bil}_{R-\mathrm{bal}}(R, N; A) \simeq \mathrm{Hom}(N, A)$ *and* $\mathrm{Bil}_{R-\mathrm{bal}}(M, R; A) \simeq \mathrm{Hom}(M, A)$.

Proof - (a), (b) and (c) can be proved similary as statements (a), (b) and (c) of Proposition 3.3. Let us prove here only the first statement of (d) (the second one can be proved similarly). Let

$$\begin{array}{rccc} \varphi : & \mathrm{Bil}_{R-\mathrm{bal}}(R, N; A) & \longrightarrow & \mathrm{Hom}(N, A) \\ & f & \longmapsto & \big(n \mapsto f(1, n)\big) \end{array}$$

and

$$\begin{array}{rccc} \psi : & \mathrm{Hom}(N, A) & \longrightarrow & \mathrm{Bil}_{R-\mathrm{bal}}(R, N; A) \\ & g & \longmapsto & \big((r, n) \mapsto g(rn)\big). \end{array}$$

It is clear that φ and ψ are well-defined homomorphisms of groups. Moreover, it is also clear that $\varphi \circ \psi = \mathrm{Id}_{\mathrm{Hom}(N,A)}$ and $\psi \circ \varphi = \mathrm{Id}_{\mathrm{Bil}_{R-\mathrm{bal}}(R,N;A)}$. ■

Examples 3.7 - (1) The map $R \times R \to R$, $(a, b) \mapsto ab$ is R-balanced and bilinear. More generally, the map $R \times N \to N$, $(r, n) \mapsto rn$ is R-balanced and bilinear.

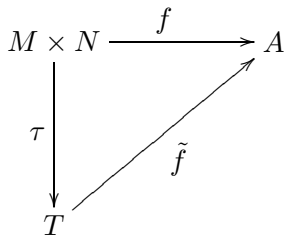
(2) Let us define a structure of right R-module on $\mathrm{End}_{\mathbb{Z}}(N)$ as follows: if $s \in \mathrm{End}_{\mathbb{Z}}(N)$ and if $r \in R$, let $\sigma r : N \to N$, $n \mapsto \sigma(rn)$. It is readily seen that it endows $\mathrm{End}_{\mathbb{Z}}(N)$ with a structure of right R-module. Then the map

$$\begin{array}{ccc} \mathrm{End}_{\mathbb{Z}}(N) \times N & \longrightarrow & N \\ (\sigma, n) & \longmapsto & \sigma(n) \end{array}$$

is R-balanced and bilinear. □

Definition 3.8. *A pair (T, τ) where T is an abelian group an $\tau : M \times N \to T$ is an R-balanced bilinear map is called a* ***tensor product of M and N over R*** *if it satisfies the following property:*

(**T**) *For every abelian group A and every $f \in \mathrm{Bil}_{R-\mathrm{bal}}(M, N; A)$, there exists a* ***unique*** *homomorphism $\tilde{f} : T \to A$ such that $f = \tilde{f} \circ \tau$.*



Tensor products exist and are all canonically isomorphic:

Theorem 3.9. *Let R be a ring, let M be a right R-module and let N be a left R-module.*

(a) *There exists a tensor product of M and N over R.*

(b) *If (T, τ) and (T', τ') are two tensor products of M and N over R, then there exists a unique group homomorphism $\alpha : T \to T'$ such that $\tau' = \alpha \circ \tau$. Moreover, such an α is an isomorphism.*

PROOF - (a) Let $F = \mathbb{Z}[M \times N]$: this is the free $\mathbb{Z}$-module with basis $M \times N$ (see Exercise I.4). Let I be the sub-$\mathbb{Z}$-module of F generated by all elements of the form

$$(m + m', n) - (m, n) - (m', n), \quad (m, n + n') - (m, n) - (m, n'), \quad (mr, n) - (m, rn)$$

for m, $m' \in M$, n, $n' \in N$ and $r \in R$. Let $T = F/I$ and, if $x \in F$, let $\bar{x}$ denote its image in T. Let $\pi : F \to T$ be the canonical projection and let $\tau : M \times N \to T$, $(m, n) \mapsto \overline{(m, n)}$ be the restriction of π.

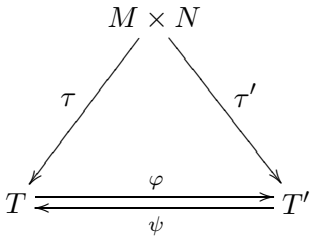
• Let us show that τ is bilinear. Let m, $m' \in M$ and $n \in N$. Then, by definition, $\overline{(m + m', n) - (m, n) - (m', n)} = 0$. In other words, $\tau(m + m', n) = \tau(m, n) + \tau(m', n)$. The other equality is proved similarly.

• We can also prove similarly that τ is R-balanced.

• Let us show now that the pair (T, τ) is a tensor product. Let $f : M \times N \to A$ be an R-balanced bilinear map. Then, by Exercise I.4 (c), f extends to a map $f_A : F \to A$. Moreover, by the definition of an R-balanced bilinear map, $f_A(I) = 0$. Therefore, f_A factors through an homomorphism $\bar{f}_A : T \to A$ such that $f_A = \bar{f}_A \circ \pi$. If we restrict this equality to $M \times N \subseteq F$, we get that $f = \bar{f}_A \circ \tau$.

Moreover, if $f' : T \to A$ is $\mathbb{Z}$-linear satisfies $f = f' \circ \tau$, by extending this equality by linearity, we get that $f_A = f' \circ \pi$. Therefore $f' = \bar{f}_A$ because π is surjective. This completes the proof of (a).

(b) By the very definition of a tensor product, there exist two maps $\varphi : T \to T'$ and $\psi : T' \to T$ such that $\tau = \tau' \circ \varphi$ and $\tau' = \tau \circ \psi$. We summarize the situation in the next diagram:



Therefore, $\tau = \tau \circ (\psi \circ \varphi)$. Now, by unicity, $\psi \circ \varphi = \mathrm{Id}_T$. Similarly, $\varphi \circ \psi = \mathrm{Id}_{T'}$. ■

Since there is only (up to a *unique* isomorphism) one tensor product, we shall denote by $M \otimes_R N$ *the* tensor product of M and N defined in the proof of the above Theorem. The R-balanced bilinear map $M \times N \to M \otimes N$ will be omitted and denoted by $(m, n) \mapsto m \otimes_R n$. As it can be seen from the proof of Theorem 3.9, $M \otimes_R N$ is generated, as a $\mathbb{Z}$-module, by the elements $m \otimes_R n$, where $(m, n) \in M \times N$. It must be noticed that there might be elements of $M \otimes_R N$ that are not of the form $m \otimes_R n$.

To define an homomorphism $M \otimes_R N \to A$, one only needs to define an R-balanced bilinear map $M \times N \to A$.

REMARK 3.10 - It might be difficult to prove that a sum $\sum_{i=1}^{l} m_i \otimes_R n_i$ is equal to or different from zero!! □

EXAMPLE 3.11 - If $\gcd(m,n) = 1$, then $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$. Indeed, this follows from Example 3.4 (3) and from the fact that the tensor product of two modules is generated by elementary tensor products. □

3.B. First properties. The last two statements of the next proposition are immediate consequences of the corresponding statements for R-balanced bilinear maps.

Proposition 3.12. *We have:*

(a) *If $f : M \to M'$ and $g : N \to N'$ are R-linear maps, then there is a unique map $f \otimes_R g : M \otimes_R N \to M' \otimes_R N'$, such that $(f \otimes_R g)(m \otimes_R n) = f(m) \otimes_R g(n)$ for all $(m,n) \in M \times N$. We have $(f \otimes_R g) \circ (f' \otimes_R g') = (f \circ f') \otimes_R (g \circ g')$.*

(b) *With the hypothesis of (a), if f and g are moreover surjective, then so is $f \otimes_R g$. If f and g are isomorphisms, then $f \otimes_R g$ are isomorphisms of $\mathbb{Z}$-modules.*

(c) $(M \oplus M') \otimes_R N = (M \otimes_R N) \oplus (M' \otimes_R N)$.

(d) $M \otimes_R (N \oplus N') = (M \otimes_R N) \oplus (M \otimes_R N')$.

PROOF - (a) The map $M \times N \to M' \otimes_R N'$, $(m,n) \mapsto f(m) \otimes g(n)$ is R-balanced and bilinear. So the existence of $f \otimes_R g$ follows from Theorem 3.9. The last property is obvious.

(b) If f and g are moreover surjective, let L denote the image of $f \otimes_R g$. Then $L \subseteq M' \otimes_R N'$. Moreover, if $m' \in M'$ and $n' \in N'$, then there exists $(m,n) \in M \times N$ such that $f(m) = m'$ and $g(m) = m'$. Therefore, $m' \otimes_R n' = (f \otimes_R g)(m \otimes_R n) \in L$. But since $M' \otimes_R N'$ is generated by the $m' \otimes_R n'$, we get that $L = M' \otimes_R N'$, as desired.

(c) and (d) follow easily from Proposition 3.6 (a) and (b). ■

REMARK 3.13 - Let I be any set, finite or not. Then it is easy to show that

$$\big(\bigoplus_{i\in I} M_i\big) \otimes_R N \simeq \bigoplus_{i\in I} \big(M_i \otimes_R N\big)$$

and

$$\big(M \otimes_R \bigoplus_{i\in I} N_i\big) \simeq \bigoplus_{i\in I} \big(M \otimes_R N_i\big).$$

This is left as an exercise. Note that the corresponding property for bilinear and R-balanced maps does not hold in general. □

REMARK 3.14 - In general, the statement (b) of the Proposition 3.12 is false if we replace *surjective* by *injective*. Indeed, let $m \geqslant 2$ be a natural number and let $f : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto nm$ and let $\mathrm{Id}_{\mathbb{Z}/m\mathbb{Z}} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Then f and $\mathrm{Id}_{\mathbb{Z}/m\mathbb{Z}}$ are injective but $(f \otimes_{\mathbb{Z}} \mathrm{Id}_{\mathbb{Z}/m\mathbb{Z}})(x \otimes_{\mathbb{Z}} \bar{y}) = xm \otimes_{\mathbb{Z}} \bar{y} = x \otimes_{\mathbb{Z}} m\bar{y} = 0$ and $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \neq 0$ by Proposition 3.16 below. □

REMARK 3.15 - Proposition 3.12 (a) shows that $- \otimes_R - : \mathbf{Mod}_R \times {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a functor (recall that the product of two categories has been defined in Exercice I.2).

Proposition 3.16. *Let I be a right ideal of R. Let IN be the sub-$\mathbb{Z}$-module of N generated by the rn, where $r \in I$ and $n \in N$. Then*

$$R/I \otimes_R N \simeq N/IN.$$

Similarly, if J is a left ideal of R, then

$$M \otimes_R R/J \simeq M/MJ.$$

Proof - Let

$$\begin{array}{rccc} \psi: & R/I \otimes_R N & \longrightarrow & N/IN \\ & \bar{r} \otimes_R m & \longmapsto & \overline{rm} \end{array}$$

and

$$\begin{array}{rccc} \varphi: & N/IN & \longrightarrow & R/I \otimes_R N \\ & \bar{m} & \longmapsto & \bar{1} \otimes_R m. \end{array}$$

Let us prove that ψ and φ are well-defined.

• Let $f : R/I \times N \to N/IN$, $(\bar{r}, m) \mapsto \overline{rm}$. Then f is well-defined: indeed, if $\bar{r} = \bar{s}$, then there exists $x \in I$ such that $s = x + r$. Therefore, $sm = xm + rm$. In other words, $sm - rm \in IN$, so $\overline{sm} = \overline{rm}$. Now it is also clear that f is bilinear. Let us prove that it is R-balanced: we have $f(\bar{r}.s, m) = f(\overline{rs}, m) = \overline{rsm} = f(\bar{r}, sm)$. So the existence of ψ follows from Theorem 3.9.

• Let m and m' be two elements of N such that $m - m' \in IN$. Then there exists $r_1, \ldots, r_l \in R$ and $m_1, \ldots, m_l \in N$ such that $m - m' = \sum_{i=1}^{l} r_i m_i$. But then

$$\begin{aligned} \bar{1} \otimes_R m &= \bar{1} \otimes_R m' + \sum_{i=1}^{l} \bar{1} \otimes_R r_i m_i \\ &= \bar{1} \otimes_R m' + \sum_{i=1}^{l} \bar{1}.r_i \otimes_R m_i \\ &= \bar{1} \otimes_R m' + \sum_{i=1}^{l} \bar{r}_i \otimes_R m_i \\ &= \bar{1} \otimes_R m' + \sum_{i=1}^{l} \bar{0} \otimes_R m_i \\ &= \bar{1} \otimes_R m'. \end{aligned}$$

So φ is well-defined. It is an homomorphism of abelian groups.

Now, ψ and φ are well-defined and it is readily seen that $\varphi \circ \psi = \mathrm{Id}_{R/I \otimes_R N}$ and $\psi \circ \varphi = \mathrm{Id}_{N/IN}$. ■

Corollary 3.17. *We have $R \otimes_R N \simeq N$ and $M \otimes_R R \simeq M$.*

Remark 3.18 - If I is a right ideal of R, it might happen that the map $I \otimes_R M \to IM$, $r \otimes_R m \mapsto rm$ is not injective. For instance, take $R = \mathbb{Z}$, $M = \mathbb{Z}/m\mathbb{Z}$, $I = m\mathbb{Z}$.

3.C. Bimodules. If S is another ring, an abelian group M is called an (R, S)-*bimodule* if it is both a left R-module and a right S-module and if moreover $(rm)s = r(ms)$ for

every $r \in R$, $m \in M$ and $s \in S$. In particular, we shall often write rms instead of $(rm)s$ or $r(ms)$. If M and M' are two (R,S)-bimodules, we denote by $\mathrm{Hom}_R(M,M')_S$ the set of maps $f : M \to M'$ which are both morphisms of left R-modules and right S-modules. The category of (R,S)-bimodules will be denoted by ${}_R\mathbf{Mod}_S$. Of course, if M is an (R,S)-bimodule, then M° is an (S°, R°)-bimodule. We get an isomorphism of categories ${}_R\mathbf{Mod}_S \to {}_{S^\circ}\mathbf{Mod}_{R^\circ}$, $M \mapsto M^\circ$. Note that a left (respectively right) R-module is an $(R,\mathbb{Z})$-bimodule (respectively a $(\mathbb{Z},R)$-bimodule).

If R is commutative, any left (or right R-module) is *naturally* an (R,R)-bimodule but, be careful (!!), it is no longer true that, to define an (R,R)-bimodule, we only need to define a structure of left R-module).

Proposition 3.19. *If R, S and T are three rings and if $M \in {}_R\mathbf{Mod}_S$ and $N \in {}_S\mathbf{Mod}_T$, then the maps*

$$\begin{array}{ccc} R \times (M \otimes_S N) & \longrightarrow & M \otimes_S N \\ (r, m \otimes_S n) & \longmapsto & rm \otimes_S n \end{array}$$

and

$$\begin{array}{ccc} T \times (M \otimes_S N) & \longrightarrow & M \otimes_S N \\ (t, m \otimes_S n) & \longmapsto & m \otimes_S nt \end{array}$$

are well-defined and endow $M \otimes_S N$ with a structure of (R,T)-bimodule.

Proof - Let $r \in R$. Then the map $f_r : M \times N \to M \otimes_S N$, $(m,n) \mapsto rm \otimes_S n$ is an S-balanced bilinear map. So it induces a map $\tilde{f}_r : M \otimes_S N \to M \otimes_S N$, $m \otimes_S N \mapsto rm \otimes_S N$. Now, let

$$\begin{array}{rccc} f: & R \times (M \otimes_S N) & \longrightarrow & M \otimes_S N \\ & (r, x) & \longmapsto & \tilde{f}_r(x). \end{array}$$

Then it is readily checked that f endows $M \otimes_S N$ with a structure of left R-module. Similarly, the second map defined in the Proposition 3.19 is well-defined and endows $M \otimes_S N$ with a structure of right T-module. It is also easy to check that, if $r \in R$, $x \in M \otimes_S N$ and $t \in T$, then $r(xt) = (rx)t$ (by linearity, this can be checked only if $x = m \otimes_S n$ for some $(m,n) \in M \times N$). ■

Proposition 3.20. *Let R, S, T and U be four rings and let $L \in {}_R\mathbf{Mod}_S$, $M \in {}_S\mathbf{Mod}_T$ and $N \in {}_T\mathbf{Mod}_U$. Then the map*

$$\begin{array}{ccc} L \otimes_S (M \otimes_T N) & \longrightarrow & (L \otimes_S M) \otimes_T N \\ l \otimes_S (m \otimes_T n) & \longmapsto & (l \otimes_S m) \otimes_T n \end{array}$$

is well-defined and is an isomorphism of (R,U)-bimodules.

Proof - This is left as an exercice (proceed as in the proof of Proposition 3.19). ■

Examples 3.21 - (1) Let $\sigma : R \to S$ be a morphism of rings. Then this endows S with a structure of (S,R)-bimodule: $s.s' = ss'$ and $s.r = s\sigma(r)$ ($r \in R$, s, $s' \in S$). So, if N is a left R-module, then $S \otimes_R N$ becomes a left S-module.

If N is free with R-basis $(e_i)_{i\in I}$, then

$$\begin{aligned} S\otimes_R N &= \bigoplus_{i\in I} S\otimes_R Re_i \\ &\simeq \bigoplus_{i\in I} S(1_S\otimes_R e_i) \end{aligned}$$

and

$$S\otimes_R Re_i \simeq S\otimes_R R\simeq S$$

by Corollary 3.13. In fact, we have proved that $(1\otimes_R e_i)_{i\in I}$ is an S-basis of $S\otimes_R N$.

Note that, if R is a field, then any R-module is free so that $S\otimes_R N$ is a free S-module for any N.

(2) Let I be a two-sided ideal of R. Then R/I is naturally endowed with a structure of (R,R)-bimodule, or $(R,R/I)$-bimodule, or $(R/I,R)$-bimodule... Also, if N is a left R-module, then IN is a left R-submodule of N. Therefore, N/IN can be viewed as a left R-module or as a left R/I-module. It is now easily checked that the isomorphism $R/I\otimes_R N\simeq N/IN$ constructed in Proposition 3.16 is an isomorphism of left R-modules (or R/I-modules).

(3) If R is commutative, then ${}_R\mathbf{Mod}\simeq\mathbf{Mod}_R$ and any left R-module is naturally an (R,R)-bimodule. Therefore, if M, $N\in{}_R\mathbf{Mod}$, then the tensor product $M\otimes_R N$ is well-defined and is naturally endowed with a structure of left R-module. Moreover, the map

$$\begin{aligned} M\otimes_R N &\longrightarrow N\otimes_R M \\ m\otimes_R n &\longmapsto n\otimes_R m \end{aligned}$$

is well-defined and is an isomorphism of R-modules.

If M and N are moreover R-free with basis $(m_i)_{i\in I}$ and $(n_j)_{j\in J}$ respectively, then $M\otimes_R N$ is R-free with basis $(m_i\otimes_R n_j)_{(i,j)\in I\times J}$. □

3.D. Bimodules as functors. Let $M\in{}_R\mathbf{Mod}_S$. Then

$$\begin{aligned} M\otimes_S -:{}_S\mathbf{Mod} &\longrightarrow {}_R\mathbf{Mod} \\ N &\longmapsto M\otimes_S N \\ f &\longmapsto \mathrm{Id}_M\otimes_S f \end{aligned}$$

is a covariant functor. If $N\in{}_S\mathbf{Mod}_T$, then the Proposition 3.20 shows that there is a natural isomorphism of functors $(M\otimes_S -)\circ(N\otimes_T -)\simeq(M\otimes_S N)\otimes_T -$. Also, if $f\in\mathrm{Hom}_R(M,M')_S$, then f induces a natural transformation $M\otimes_S -\to M'\otimes_S -$. If f is an isomorphism of (R,S)-bimodules, then this natural transformation is a natural isomorphism.

Now, if L is a left R-module, if $f\in\mathrm{Hom}_R(M,L)$, and if $s\in S$, we define $s.f:M\to L$, $m\mapsto f(ms)$. It is readily seen that this endows $\mathrm{Hom}_R(M,L)$ with a structure of left S-module. So this defines a covariant functor

$$\begin{aligned} \mathrm{Hom}_R(M,-):{}_R\mathbf{Mod} &\longrightarrow {}_S\mathbf{Mod} \\ L &\longmapsto \mathrm{Hom}_R(M,L) \\ f &\longmapsto \big(g\mapsto(f\circ g)\big). \end{aligned}$$

Theorem 3.22 (Adjointness of Hom and $\otimes$). *The functor $M \otimes_R -$ is a left adjoint to the functor $\mathrm{Hom}_R(M,-)$. The adjunction is given, for any $X \in {}_R\mathbf{Mod}$ and any $Y \in {}_S\mathbf{Mod}$, by*

$$\begin{array}{rccc} \gamma_{YX}: & \mathrm{Hom}_R(M \otimes_S Y, X) & \longrightarrow & \mathrm{Hom}_S(Y, \mathrm{Hom}_R(M,X)) \\ & f & \longmapsto & \big(y \mapsto (m \mapsto f(m \otimes_S y))\big). \end{array}$$

The inverse is given by

$$\begin{array}{rccc} \delta_{YX}: & \mathrm{Hom}_S(Y, \mathrm{Hom}_R(M,X)) & \longrightarrow & \mathrm{Hom}_R(M \otimes_S Y, X) \\ & f & \longmapsto & \big(m \otimes_S y \mapsto f(y)(m)\big). \end{array}$$

Proof - The proof is left as an exercice. ■

3.E. Tensor product over commutative rings. *From now on, and until the end of this section, we assume that R is a commutative ring.* If M and N are two left R-modules, then M can be seen as an (R,R)-bimodule as follows: if $r \in R$ and $m \in M$, we set $m.r = rm$. In particular, $M \otimes_R N$ inherits a structure of left R-module (see Proposition 3.19): $r.(m \otimes_R n) = (rm) \otimes_R n$. In particular, $r.(m \otimes_R n) = (m.r) \otimes_R n = m \otimes_R (rn)$.

If A is another R-module, a map $f : M \times N \to A$ is called R-bilinear if it is bilinear and if, for all $r \in R$, $m \in M$ and $n \in N$, we have

$$f(rm,n) = f(m,rn) = rf(m,n).$$

In particular, an R-bilinear map is an R-balanced bilinear map (where M is seen as a right R-module as above).

Theorem 3.23. *Assumme that R is **commutative**. Let A, M and N be three left R-modules and let $f : M \times N \to A$ be an R-bilinear map. Then the unique map $\tilde{f} : M \otimes_R N \to A$, $m \otimes_R n \mapsto f(m,n)$ is a morphism of R-modules.*

Proof - The proof is left as an exercise. ■

Recall that we still assume that R is commutative. An *R-algebra* is an R-module A endowed with a structure of ring such that the map $R \to A$, $r \mapsto r.1_A$ is a morphism of rings whose image is in the centre of A (the *centre* of a ring S is the subring of S consisting of the elements which commute to all the others).

Examples 3.24 - (1) The centre of $\mathrm{Mat}_n(R)$ is $R.I_n$, where I_n is the identity matrix. The ring $\mathrm{Mat}_n(R)$ is an R-algebra.

(2) If G is a group, $R[G]$ is an R-algebra.

(3) If K is a subfield of a field K', then K' is naturally a K-algebra.

(4) $R[X_1, \ldots, X_n]$ is an R-algebra.

(5) If I is an ideal of R, then R/I is an R-algebra. □

Theorem 3.25. *Assume that R is commutative. Let A and B be two R-algebras. Then the map*

$$\begin{array}{ccc} (A \otimes_R B) \times (A \otimes_R B) & \longrightarrow & A \otimes_R B \\ (a \otimes_R b, a' \otimes_R b') & \longmapsto & aa' \otimes_R bb' \end{array}$$

is a product which endows $A \otimes_R B$ with a structure of R-algebra.

If moreover A is commutative, then $A \otimes_R B$ is an A-algebra. If A and B are commutative, then so is $A \otimes_R B$.

Proof - The proof is left as an exercice. ■

Examples 3.26 - (1) If S is a commutative R-algebra, then $S \otimes_R R[G] \simeq S[G]$, $S \otimes_R R[X_1, \ldots, X_n] \simeq S[X_1, \ldots, X_n]$, $S \otimes_R \mathrm{Mat}_n(R) \simeq \mathrm{Mat}_n(S)$...

(2) Let X and Y be two indeterminates. Let us show that the map

$$\begin{array}{ccc} R[X] \otimes_R R[X] & \longrightarrow & R[X,Y] \\ P \otimes Q & \longmapsto & P(X)Q(Y) \end{array}$$

is an isomorphism of R-algebras. First, it is clear that it is a morphism of R-algebras. Let us show now that it is an isomorphism. First, $(X^i \otimes_R X^j)_{(i,j)\in\mathbb{Z}^2_{\geqslant 0}}$ is an R-basis of the R-module $R[X] \otimes_R R[X]$. On the other hand, $(X^iY^j)_{(i,j)\in\mathbb{Z}^2_{\geqslant 0}}$ is an R-basis of the R-module $R[X,Y]$. Since $X^i \otimes_R X^j$ is mapped to X^iY^j through this morphism, we get the desired result. □

4. Noetherian and Artinian modules and rings

In this section, we fix a ring R.

4.A. Definitions and characterizations. The notion of Noetherian and Artinian modules (or ring) involves chains of submodules:

Definition 4.1. *A left R-module M is called **Noetherian** (respectively **Artinian**) if it satisfies the **ascending chain condition** (ACC) (respectively the **descending chain condition** (DCC)) namely, if every chain of submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq$ ... (respectively $M_1 \supseteq M_2 \supseteq M_3 \supseteq$ ...) becomes stationary (i.e. $\exists\ n_0,\ \forall\ n \geqslant n_0,\ M_n = M_{n+1}$).*

*The ring R is called **left Noetherian** (respectively **left Artinian**) if the left R-module R is Noetherian (respectively Artinian).*

Remark - One can define similarly the notion of Noetherian (or Artinian) right modules and of *right Noetherian* (or *right Artinian*) rings. There are examples of rings which both left Noetherian and left Artinian but which are neither right Noetherian or right Artinian. □

Examples 4.2 - (1) A field is both Noetherian and Artinian.

(2) $\mathbb{Z}$ and, more generally, any principal ring is Noetherian. However, $\mathbb{Z}$ is not Artinian: indeed, $\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq 16\mathbb{Z} \supseteq \cdots$ is a non-stationary descending chain of ideals of $\mathbb{Z}$. Similarly, $K[X]$ is not Artinian (here, K is a field and X is an indeterminate).

(3) Any finite dimensional algebra over a field K is both Noetherian and Artinian. Any finite ring is both Noetherian and Artinian (for instance, $\mathbb{Z}/n\mathbb{Z}$).

(4) Let R be the ring of maps $\mathbb{Z} \to \mathbb{C}$ (with pointwise multiplication and addition). If $n \in \mathbb{Z}$, let

$$I_n = \{f : \mathbb{Z} \to \mathbb{C} \mid \forall\ k \geqslant n,\ f(k) = 0\}.$$

Then I_n is an ideal of R and it is easily checked that

$$\cdots \subsetneq I_{-2} \subsetneq I_{-1} \subsetneq I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

In particular, R is not Noetherian and not Artinian.

If we denote by J the ideal of function $f : \mathbb{Z} \to \mathbb{C}$ such that $f(k) = 0$ for all $k \in \mathbb{Z} \setminus \{0\}$, then J is a Noetherian and Artinian module. □

The next Theorem gives some characterizations of Noetherian or Artinian modules.

Theorem 4.3. *Let M be a left R-modules. Then:*

(a) *The following are equivalent:*
  (1) *M is Noetherian.*
  (2) *Every submodule of M is finitely generated.*
  (3) *Every non-empty set of submodules has a maximal element.*

(b) *The following are equivalent:*
  (1) *M is Artinian.*
  (2) *Every non-empty set of submodules has a minimal element.*

Proof - (a) The proof will proceed in several steps:

• (1) ⇒ (2): Let N be a submodule of M and assume that N is not finitely generated. Since N is not finitely generated, there exists a sequence $(n_i)_{i \geqslant 1}$ of elements of N such that n_{k+1} does not belong to the submodule N_k generated by $(n_i)_{1 \leqslant i \leqslant k}$. Then $N_k \subsetneq N_{k+1}$, so M is not Noetherian.

• (2) ⇒ (3): Let $\mathcal{M}$ be non-empty set of submodules of M and assume that $\mathcal{M}$ has no maximal element. Let $M_1 \in \mathcal{M}$. Then M_1 is not maximal, so there exists $M_2 \in \mathcal{M}$ such that $M_1 \subsetneq M_2$. Similarly, we can repeat the process and construct a sequence $(M_n)_{n \geqslant 1}$ of elements of $\mathcal{M}$ such that $M_n \subsetneq M_{n+1}$, so that $\bigcup_{n \geqslant 1} M_n$ cannot be finitely generated.

• (3) ⇒ (1): clear.

(b) The proof will proceed in two steps:

• (1) ⇒ (2): Let $\mathcal{M}$ be non-empty set of submodules of M and assume that $\mathcal{M}$ has no minimal element. The same argument as before shows that we can then construct a sequence $(M_n)_{n \geqslant 1}$ of elements of $\mathcal{M}$ such that $M_{n+1} \subsetneq M_n$, so M is not Artinian.

• (2) ⇒ (1): clear. ■

4.B. First properties. Recall that a *short exact sequence* of left R-modules is a sequence

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

of morphisms such that $\operatorname{Ker}\alpha = 0$, $\operatorname{Ker}\beta = \operatorname{Im}\alpha$ and $\operatorname{Im}\beta = N$. Of course, one can define similarly short exact sequences of right modules (or even of bimodules...)

Proposition 4.4. *Let*

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

be a short exact sequence. Then M is Noetherian (respectively Artinian) if and only if L and N are Noetherian (respectively Artinian).

Proof - We prove the result for Noetherian modules only (the argument is similar for Artinian modules). Since α is injective, we shall identify L with a submodule of M (and α is the canonical injection $L \hookrightarrow M$) and N with the quotient M/L (and β with the canonical surjection $M \to M/L$).

Assume first that L and N are Noetherian. Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq ...$$

be a chain of sub-R-modules of M. Then

$$\beta(M_1) \subseteq \beta(M_2) \subseteq \beta(M_3) \subseteq ...$$

is an ascending chain of submodules of N. Since N is Noetherian, there exists n_1 such that $\beta(M_n) = \beta(M_{n+1})$ if $n \geqslant n_1$. On the other hand,

$$L \cap M_1 \subseteq L \cap M_2 \subseteq L \cap M_3 \subseteq ...$$

is an ascending chain of submodules of L. Since L is Noetherian, there exists n_2 such that $L \cap M_n = L \cap M_{n+1}$ if $n \geqslant n_2$. Let $n_0 = \max(n_1, n_2)$. Then, if $n \geqslant n_0$, we have $L \cap M_n = L \cap M_{n+1}$ and $\beta(M_n) = \beta(M_{n+1})$. We shall prove that this implies that $M_n = M_{n+1}$. Indeed, if $m \in M_{n+1}$, then there exists $m' \in M_n$ such that $\beta(m) = \beta(m')$. So $m - m' \in M_{n+1} \cap L = \operatorname{Ker} \beta$. So $m - m' \in L \cap M_n$. Therefore, $m - m' \in M_n$, so $m \in M_n$, as desired.

Conversely, assume that M is Noetherian. Then L is obviously Noetherian because any ascending chain of submodules of L is an ascending chain of submodules of M. On the other hand, if

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq ...$$

is an ascending chain of submodules of N, then

$$\beta^{-1}(N_1) \subseteq \beta^{-1}(N_2) \subseteq \beta^{-1}(N_3) \subseteq ...$$

is an ascending chain of submodules of M. Since M is Noetherian, there exists n_0 such that $\beta^{-1}(N_n) = \beta^{-1}(N_{n+1})$ for all $n \geqslant n_0$. But, since $\beta(\beta^{-1}(N_n)) = N_n$, we get that $N_n = N_{n+1}$ for all $n \geqslant n_0$. So N is Noetherian. ■

Corollary 4.5. *We have:*

(a) *Let $M_1, \ldots, M_n$ be Noetherian (respectively Artinian) left R-modules. Then $M_1 \oplus \cdots \oplus M_n$ is Noetherian (respectively Artinian).*

(b) *If M is a left R-module and if $M_1, \ldots, M_n$ are Noetherian (respectively Artinian) submodules, then $M_1 + \cdots + M_n$ is Noetherian (respectively Artinian).*

Proof - This follows easily from Proposition 4.4 by induction on n. ■

Corollary 4.6. *If R is left Noetherian and if I is a two-sided ideal of R, then the ring R/I is left Noetherian.*

Definition 4.7. *A left R-module M is called* ***simple*** *(or* ***irreducible****) if $M \neq 0$ and the only submodules are M and 0. A* ***composition series*** *of a left R-module M is a finite sequence*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

such that M_{i+1}/M_i is simple. We say that the R-module M ***has finite length*** *if it has a composition series.*

REMARK 4.8 - A simple module is of course Noetherian and Artinian. □

EXAMPLES 4.9 - (1) If K is a field and V is a K-vector space, then V is simple if and only if it has dimension 1. It has finite length if and only if it is finite dimensional.

(2) $\mathbb{Z}/p\mathbb{Z}$ is a simple $\mathbb{Z}$-module if and only if p is a prime number.

(3) $0 \subset 2\mathbb{Z}/6\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z}$ is a composition series of $\mathbb{Z}/6\mathbb{Z}$. In fact, $\mathbb{Z}/n\mathbb{Z}$ has finite length for any $n \geqslant 1$.

(4) $\mathbb{Z}$ is not a simple $\mathbb{Z}$-module. It has not finite length. □

Let us recall the following

Theorem 4.10 (Jordan-Hölder). *Let M be a left R-module. If $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ and $0 = M'_0 \subset M'_1 \subset \cdots \subset M'_{n'} = M$ are two composition series of M, then $n = n'$ and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $M_i/M_{i-1} \simeq M'_{\sigma(i)}/M'_{\sigma(i)-1}$.*

PROOF - Let i_0 denote the minimal natural number such that $M_1 \subseteq M'_{i_0}$ and $M_1 \not\subseteq M'_{i_0-1}$. Let $f : M_1 \to M'_{i_0}/M'_{i_0-1}$ be the canonical map. Then $M_1 \cap M'_{i_0-1}$ is a submodule of M_1 which is different from M_1, so it is equal to 0 because M_1 is simple. In other words, f is injective. Similarly, $\operatorname{Im} f$ is a non-zero submodule of M'_{i_0}/M'_{i_0-1}, so f is surjective. Hence f is an isomorphism. In particular, $M_{i_0} = M_{i_0-1} \oplus M_1$.

Now, let $\bar{M} = M/M_1$ and, if N is a submodule of M, let $\bar{N}$ denote its image in M/M_1. Then

$$0 = \bar{M}_1 \subset \bar{M}_2 \subset \cdots \subset \bar{M}_n = M$$

is a composition series of $\bar{M}$. Also,

$$0 = \bar{M}'_0 \subset \bar{M}'_1 \subset \cdots \subset \bar{M}'_{i_0-1} \subset \bar{M}'_{i_0+1} = \bar{M}'_{i_0} \subset \cdots \subset \bar{M}'_{n'}$$

is another composition series of $\bar{M}$. By applying the induction hypothesis, we get the Theorem. ■

EXAMPLE 4.11 - $0 \subset 2\mathbb{Z}/6\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z}$ and $0 \subset 3\mathbb{Z}/6\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z}$ are composition series of $\mathbb{Z}/6\mathbb{Z}$. □

If M is a left R-module, we write $\lg(M) = \infty$ if M does not have finite length and we write $\lg(M) = n$ if M admits a composition series $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$. The number $\lg(M)$ is called the *length* of M: it will be sometimes denoted by $\lg_R(M)$ is we need to emphasize the ambient ring. By the Jordan-Hölder Theorem, the length of an R-module is well-defined. It is easily seen that, if

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

is a short exact sequence of left R-modules, then

$$\lg(M) = \lg(L) + \lg(N). \tag{4.12}$$

Proposition 4.13. *A left R-module has finite length if and only if it is both Noetherian and Artinian.*

PROOF - Let M be a left R-module. If M has finite length, then an easy induction argument on the length of M (using Proposition 4.4 and the fact that a simple module is Noetherian and Artinian) shows that M is Noetherian and Artinian.

Conversely, assume that M is Noetherian and Artinian. Let $M_0 = 0$. Since M is Artinian, it admits a minimal non-zero submodule M_1. Since it is minimal, M_1 is simple. Now, M/M_1 is also Artinian (see Proposition 4.4), so there exists a minimal non-zero submodule M_2'. Let M_2 be the inverse image of M_2' under the morphism $M \to M/M_1$ (in other words, M_2 is the unique submodule of M such that $M_2/M_1 = M_2'$. By the minimality of M_2', we get that M_2/M_1 is simple. By repeating the argument, we can construct a chain of submodules

$$M_0 \subset M_1 \subset M_2 \subset M_3 \subset \cdots$$

such that M_i/M_{i-1} is simple. Now, M is Noetherian, so this sequence must become stationary after some M_n, and M_n must be equal to M. ■

We close this subsection by a difficult result whose proof may be found for instance in C.W. CURTIS & I. REINER, "Representation theory of finite groups and associative algebras", Theorem 54.1.

Theorem 4.14 (Hopkin). *An Artinian ring is Noetherian.*

4.C. More on Noetherian modules and Noetherian rings. The next theorem gives a characterization of Noetherian modules whenever R is a Noetherian ring.

Proposition 4.15. *Assume that R is a left Noetherian ring. Then a left R-module M is Noetherian if and only if it is finitely generated.*

PROOF - If M is Noetherian, then it is finitely generated by Theorem 4.3 (a). Conversely, assume that M is finitely generated. Write $M = Rm_1 + \cdots + Rm_n$. Then the map

$$\begin{array}{ccc} R^n & \longrightarrow & M \\ (r_1, \ldots, r_n) & \longmapsto & r_1 m_1 + \cdots + r_n m_n \end{array}$$

is a surjective morphism of left R-modules. Now, by assumption, R is a Noetherian left R-module. So R^n is also a Noetherian left R-module by Corollary 4.5 (a). Therefore, M is Noetherian by Proposition 4.4. ■

The next Theorem gives a way to construct a huge family of Noetherian rings.

Hilbert's Basis Theorem. *Let R be a commutative Noetherian ring and let X be an indeterminate. Then the ring $R[X]$ is Noetherian.*

PROOF - Let I be a non-zero ideal of $R[X]$. If $P = r_nX^n + \cdots + r_1X + r_0$ with $r_n \neq 0$, we set $l(P) = r_n$ (r_n is called the *leading coefficient* of P). We set by convention $l(0) = 0$.

Now, let $J = l(I) \subseteq R$ and, for $d \geqslant 0$, let

$$J_d = \{l(P) \mid l \in I \text{ and } \deg P = d\}.$$

Then J is a left ideal of R. Indeed, if $r \in R$, and s, $s' \in J$ are such that $r(s - s') \neq 0$, then there exists two polynomials P and Q in I such that $l(P) = s$ and $l(Q) = s'$. Let p (respectively q) be the degree of P (respectively Q). By symmetry, we may assume that $p \geqslant q$. Then $r(P - X^{p-q}Q) \in I$, and $r(s - s') = l(P - X^{p-q}Q) \in J$. This proves that J is an ideal of R. Similary, J_d is an ideal of R.

Since R is Noetherian, there exists $r_1, \ldots, r_n \in J$ such that $J = Rr_1 + \cdots + Rr_n$. Let $f_1, \ldots, f_n$ be such that $f_i \in I$ and $l(f_i) = r_i$. Let $N_i = \deg f_i$ and let $N = \max\{N_i \mid 1 \leqslant i \leqslant n\}$. Now, for $0 \leqslant d \leqslant N - 1$, let $r_{d,1}, \ldots, r_{d,n_d}$ be generators of the ideal J_d. Let $f_{d,1}, \ldots, f_{d,n_d}$ be elements of I of degree d be such that $l(f_{d,i}) = r_{d,i}$. Now, let

$$I' = \sum_{i=1}^{n} R[X]f_i + \sum_{d=1}^{N-1} \sum_{i=1}^{n_d} R[X]f_{d,i}.$$

Then I' is a finitely generated ideal of $R[X]$ contained in I. We shall prove that $I' = I$. Let $f \in I$, $f \neq 0$. We shall prove by induction on the degree of f that $f \in I'$. So let $d = \deg f$.

If $d \geqslant N$, then $l(f) \in J$ so we can write $l(f) = \sum_{i=1}^{n} a_i r_i$. Now, $f - \sum_{i=1}^{n} a_i X^{d-N_i} f_i$ is an element of I of degree strictly smaller than d. So it belongs to I' by the induction hypothesis. Therefore, $f \in I'$.

On the other hand, if $d \leqslant N - 1$, then we can write $l(f) = \sum_{i=1}^{n_d} a_i r_{d,i}$. Then $f - \sum_{i=1}^{n_d} a_i f_{d,i}$ is an element of I of degree strictly smaller than d. So it belongs to I' by the induction hypothesis. Therefore, $f \in I'$. ■

Corollary 4.16. *If R is a commutative Noetherian ring, then $R[X_1, \ldots, X_n]$ is a Noetherian R-algebra.*

Definition 4.17. *If R is a commutative ring, then a commutative R-algebra S is called finitely generated (as an R-algebra) if there exists $s_1, \ldots, s_n \in S$ such that the morphism $R[X_1, \ldots, X_n] \to S$, $X_i \mapsto s_i$ is surjective. In this case, we also say that S is an R-algebra of finite type. We say that S is a finite R-algebra if S is finitely generated* **as an R-module**.

Since the quotient of any Noetherian ring is Noetherian (see Corollary 4.6), we get:

Corollary 4.18. *If R is a commutative Noetherian ring, and if S is a finitely generated commutative R-algebra, then S is Noetherian.*

5. Jacobson radical

As usual, R will denote a fixed ring.

5.A. Preliminaries. We shall start with some results that will be needed throughout this section.

Lemma 5.1. *Let M be a left (or right) R-module and let L be a proper R-submodule of M. If M/L is **finitely generated**, then there exists a maximal R-submodule L' of M containing L. In particular, this holds if M is finitely generated.*

Proof - Let $v_1,\dots, v_n$ be elements of M such that $M/L = \sum_{i=1}^{n} R(v_i+L)$. We denote by $\mathcal{M}$ the set of proper submodules of M containing L, ordered by inclusion. Then $\mathcal{M} \neq \varnothing$ (indeed, $L \in \mathcal{M}$). We want to show that $\mathcal{M}$ admits a maximal element. By Zorn's Lemma, it suffices to show that every totally ordered non-empty subset $\mathcal{N} \subseteq \mathcal{M}$ has an upper bound in $\mathcal{M}$.

So let $\mathcal{N}$ be a totally ordered non-empty subset of $\mathcal{M}$. Let $N^+ = \bigcup_{N\in\mathcal{N}} N$. Then N^+ is a submodule of M (because $\mathcal{N}$ is totally ordered) and contains all elements of $\mathcal{N}$. We only need to prove that $N^+ \neq M$. But, if $N^+ = M$, it means that there exits $N_1,\dots, N_n \in \mathcal{N}$ such that $v_i \in N_i$. Since $\mathcal{N}$ is totally ordered, $N = \max(N_1, N_2, \dots, N_n)$ is well-defined. Then $v_i \in N$ for all i, so N contains all the v_i's and also contains L, so $N = M$, which is impossible. ■

Corollary 5.2. *If I is a proper left (respectively right) ideal of R, there exists a maximal left (respectively right) ideal of R containing I.*

Proof - Indeed, R is a finitely generated R-module so the Lemma 5.1 can be applied. ■

If $M \in {}_R\mathbf{Mod}$, and if $X \subseteq M$, we set

$$\operatorname{ann}_R(X) = \{r \in R \mid \forall\ x \in X,\ rx = 0\}.$$

The set $\operatorname{ann}_R(X)$ is called the *annihilator* of X in R.

Lemma 5.3. $\operatorname{ann}_R(X)$ *is a left ideal of R. If moreover X is a submodule of M, then* $\operatorname{ann}_R(X)$ *is a two-sided ideal of R.*

Proof - It is clear that $\operatorname{ann}_R(X)$ is a sub-$\mathbb{Z}$-module of R. Now, let $r \in \operatorname{ann}_R(X)$, $x \in X$ and $a \in R$. Then $arx = a.(rx) = a.0 = 0$, so $ar \in \operatorname{ann}_R(X)$. This shows that $\operatorname{ann}_R(X)$ is a left ideal. On the oher hand, if X is a submodule of M, then $ax \in X$ so $rax = 0$. In particular, $ra \in \operatorname{ann}_R(X)$, so $\operatorname{ann}_R(X)$ is a two-sided ideal. ■

Lemma 5.4. *Let M be a simple left R-module and let $m \in M$, $m \neq 0$. Then:*

(a) $M \simeq R/\operatorname{ann}_R(m)$.
(b) $\operatorname{ann}_R(m)$ *is a maximal left ideal of R.*

PROOF - Let $\sigma : R \to M$, $r \mapsto rm$. Then σ is a morphism of R-modules. Since $m \neq 0$, the image of σ is a non-zero submodule of M. Since M is simple, σ is surjective. Moreover, by definition, we have $\operatorname{Ker}\sigma = \operatorname{ann}_R(m)$. So $M \simeq R/\operatorname{ann}_R(m)$. Now the maximality of $\operatorname{ann}_R(m)$ follows from the simplicity of M. ■

5.B. Definition. We denote by $\operatorname{Max}_l(R)$ (respectively $\operatorname{Max}_r(R)$) the set of maximal left (respectively right) ideals of R. If R is commutative, both sets will simply be denoted by $\operatorname{Max}(R)$. Note that these sets are non-empty by Corollary 5.2.

The *Jacobson radical* of R, denoted by $J(R)$, is the intersection of all maximal left ideals of R:

$$J(R) = \bigcap_{\mathfrak{m}\in\operatorname{Max}_l(R)} \mathfrak{m}.$$

In particular, $J(R)$ is a left ideal of R. We denote by $R^\times$ the group of units of R.

EXAMPLES 5.5 - (0) If K is a field, then $J(K) = 0$. More generally, if D is a division ring, then $J(D) = 0$ because 0 is the only proper (left or right) ideal of D.

(1) $J(\mathbb{Z}) = 0$. Indeed, if $\mathcal{P}$ denotes the set of prime numbers, then $\operatorname{Max}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \in \mathcal{P}\}$. So $J(\mathbb{Z}) = \bigcap_{p\in\mathcal{P}} p\mathbb{Z} = 0$.

(2) $J(\mathbb{Z}/p^n\mathbb{Z}) = p\mathbb{Z}/p^n\mathbb{Z}$ if p is a prime number. Indeed, $\mathbb{Z}/p^n\mathbb{Z}$ has only one maximal ideal.

(3) If K is a field, then $J(\operatorname{Mat}_n(K)) = 0$ (see Exercise II.19 for a more general statement). □

Theorem 5.6. *With the previous notation, we have:*

(a) $J(R) = \bigcap_{\substack{S\in {}_R\mathbf{Mod}\\ S \text{ simple}}} \operatorname{ann}_R(S)$. *In particular, $J(R)$ is a two-sided ideal of R.*

(b) *For $r \in R$, the following are equivalent:*
  (1) $r \in J(R)$.
  (2) *For all $x \in R$, $1 - xr$ has a left inverse.*
  (3) *For all x, $y \in R$, $1 - xry \in R^\times$.*

(c) *$J(R)$ is the maximal two-sided ideal I of R such that $1 + I \subseteq R^\times$.*

(d) $J(R) = \bigcap_{\mathfrak{m}\in\operatorname{Max}_r(R)} \mathfrak{m}$.

PROOF - (a) Let $J = \bigcap_{\substack{S\in {}_R\mathbf{Mod}\\ S \text{ simple}}} \operatorname{ann}_R(S)$. We want to show that $J = J(R)$.

If $S \in {}_R\mathbf{Mod}$ is simple, then $\operatorname{ann}_R(S) = \bigcap_{s\in S} \operatorname{ann}_R(s)$ is an intersection of maximal left ideal of R (see Lemma 5.4 (a)), so it contains $J(R)$. This shows that $J(R) \subseteq J$.

Conversely, if $\mathfrak{m} \in \operatorname{Max}_l(R)$, then $R/\mathfrak{m}$ is a simple R-module and $\operatorname{ann}_R(R/\mathfrak{m}) \subseteq \mathfrak{m}$. So

$$J \subseteq \bigcap_{\mathfrak{m}\in\operatorname{Max}_l(R)} \operatorname{ann}_R(R/\mathfrak{m}) \subseteq \bigcap_{\mathfrak{m}\in\operatorname{Max}_l(R)} \mathfrak{m} = J(R).$$

(b) It is clear that (3) $\Rightarrow$ (2). Let us show that (1) $\Rightarrow$ (2). Since $J(R)$ is a two-sided ideal, we only need to show that, if $r \in R$, then $1 - r$ has a left inverse. So let $r \in J(R)$. If $1 - r$ has no left inverse, then $R(1 - r) \neq R$, so there exists a maximal left ideal $\mathfrak{m}$ of R containing $1 - r$ (see Corollary 5.2). So $r \in 1 + \mathfrak{m}$. In particular, $r \notin \mathfrak{m}$, so $r \notin J(R)$.

Let us now show that (2) $\Rightarrow$ (1). Assume that $r \notin J(R)$. Then there exists a maximal left ideal $\mathfrak{m}$ of R such that $r \notin \mathfrak{m}$. In particular, $Rr + \mathfrak{m} = R$ since $\mathfrak{m}$ is maximal. So there exists $x \in R$ and $m \in \mathfrak{m}$ such that $xr + m = 1$. Therefore, $1 - xr \in \mathfrak{m}$, so $R(1 - xr) \subseteq \mathfrak{m}$, so $1 - xr$ has no left inverse in R.

We now know that (1) $\Leftrightarrow$ (2) and that (3) $\Rightarrow$ (2), so it remains to prove that (1) $\Rightarrow$ (3). Since $J(R)$ is a two-sided ideal, we only need to show that $1 - r \in R^\times$ for any $r \in J(R)$. So let $r \in J(R)$. Since (1) $\Rightarrow$ (2), there exists $s \in R$ such that $s(1-r) = 1$. Then $1-s = -sr \in J(R)$. Again, this implies that there exists $t \in R$ such that $t(1-(1-s)) = 1$. In other words, $ts = 1$. Therefore, $ts(1 - r) = t = 1 - r$. So $(1 - r)s = 1$, so $1 - r \in R^\times$.

(c) By (b), we have $1 + J(R) \subseteq R^\times$. On the other hand, if I is a two-sided ideal of R satisfying $1 + I \subseteq R^\times$, then every element $r \in I$ satisfies the condition (3) of statement (b). So $I \subseteq J(R)$.

(d) By symmetry, one can define $J'(R) = \bigcap_{\mathfrak{m} \in \mathrm{Max}_r(R)} \mathfrak{m}$. As in (b), one can show that $r \in J'(R)$ if and only if $1 - xry \in R^\times$ for all x, $y \in R$. So $J'(R) = J(R)$. ■

REMARK 5.7 - If I is a two-sided ideal of R contained in $J(R)$, then $1 + I$ is a subgroup of $R^\times$. □

If M is a left R-module, we define the *radical* of M (and we denote it by $\mathrm{rad}(M)$) as the intersection of all maximal submodules of M (if M has no maximal submodule, then $\mathrm{rad}(M) = M$). If we need to emphasize the ambient ring, we write $\mathrm{rad}_R(M)$ for $\mathrm{rad}(M)$. For instance, $\mathrm{rad}_R(R) = J(R)$.

Proposition 5.8. *If M is a left R-module, then $J(R)M \subseteq \mathrm{rad}(M)$.*

PROOF - Let L be a maximal submodule of M. Then M/L is simple. Let $I = \mathrm{ann}_R(M/L)$. Then $J(R) \subseteq I$ by Theorem 5.6 (a) so $IM \subseteq L$ by definition. So $J(R)M \subseteq L$. ■

Theorem 5.9 (Nakayama's Lemma). *Let M be a left R-module and let L be a submodule of M such that M/L is **finitely generated**. Then:*

(a) *If $L + \mathrm{rad}(M) = M$, then $L = M$.*
(b) *If $L + J(R)M = M$, then $L = M$.*
(c) *If M is finitely generated and $J(R)M = M$, then $M = 0$.*

PROOF - (a) assume that $L + \mathrm{rad}(M) = M$. If L is a proper submodule of M, then there exists a maximal submodule L' of M containing L (by Lemma 5.1). So $\mathrm{rad}(M) \subseteq L'$ and $L \subseteq L'$, so $L + \mathrm{rad}(M) \subseteq L'$, which contradicts the fact that $L + \mathrm{rad}(M) = M$. So $L = M$.

(b) follows easily from (a) and from Proposition 5.8.

(c) follows by applying (b) to the case where $L = 0$. ■

5.C. Nilpotency. An element $r \in R$ is called *nilpotent* if there exists $n \geqslant 1$ such that $r^n = 0$. A left (respectively right) ideal I of R is called a *nil left ideal* (respectively *nil right ideal*) if every element of I is nilpotent. A two-sided ideal I of R is called *nilpotent* if $I^n = 0$ for some $n \geqslant 1$. Of course, a nilpotent two-sided ideal is a nil left (or right) ideal.

Lemma 5.10. *If I is a nil left ideal, then $I \subseteq J(R)$.*

PROOF - If $r \in I$ and if $x \in R$, then $xr \in I$ so xr is nilpotent. Let $n \geqslant 1$ be such that $(xr)^n = 0$. Then

$$(1 + xr + (xr)^2 + \cdots + (xr)^{n-1})(1 - xr) = 1,$$

so $1 - xr$ has a left inverse. So $r \in J(R)$ by Theorem 5.6 (b). ■

Corollary 5.11. *If R is **commutative** and if $r \in R$ is nilpotent, then $r \in J(R)$.*

PROOF - Indeed, if $x \in R$, then xr is still nilpotent (because R is commutative). So Rr is a nil left ideal of R. So $Rr \subseteq J(R)$ by Lemma 5.10. ■

EXAMPLE 5.12 - It might happen that a nilpotent element of R does not belong to the radical of R. Indeed, let $R = \mathrm{Mat}_n(K)$ where K is a field. Then $J(R) = 0$ by Example 5.5 (3), but R contains non-zero nilpotent elements (if $n \geqslant 2$). □

Proposition 5.13. *If R is Artinian, then $J(R)$ is nilpotent.*

PROOF - Since R is Artinian, the descending chain of ideals

$$J(R) \supseteq J(R)^2 \supseteq J(R)^3 \supseteq \ldots$$

becomes stationary. So there exists $n \geqslant 1$ such that $J(R)^n = J(R)^{n+i}$ for all $i \geqslant 0$. Let $I = J(R)^n$. Then $I^2 = I$.

If $I \neq 0$, then the set $\mathcal{I}$ of non-zero left ideals L of R such that $IL = L$ is non-empty (it contains I). So it admits a minimal element L_0 (because R is Artinian). Let $a \in L_0$, $a \neq 0$. Then $Ia \in \mathcal{I}$ and $Ia \subseteq L_0$, so $Ia = L_0$. So there exists $b \in I$ such that $ba = a$. In other words $(1 - b)a = 0$, so $a = 0$ because $1 - a$ is invertible. This leads to a contradiction. ■

REMARK - If we admit Hopkin's Theorem (see Theorem 4.14), then the proof of the above result becomes much easier. Indeed, once we know that $J(R)^n = J(R)^{n+1}$, then, R being Artinian, it is also Noetherian, so $J(R)^n$ is a finitely generated R-module and $J(R).J(R)^n = J(R)^n$. So $J(R)^n = 0$ by Nakayama's Lemma. □

5.D. Idempotents. An element $e \in R$ is called *idempotent* if $e^2 = e$. For instance, 0 and 1 are idempotents.

Proposition 5.14. *Let $e \in R$ be an idempotent. Then eRe is a unitary ring (for the multiplication in R and with identity e) and $J(eRe) = eJ(R)e$.*

PROOF - If r, $s \in R$, then $ere.ese = e(res)e \in eRe$ and $ere - ese = e(r - s)e$ so eRe is stable under addition and multiplication. Also, $e.ere = ere.e = ere$ since $e^2 = e$, so e is the identity of eRe.

Now, if $r \in eJ(R)e$, and if $x \in eRe$, then $xr \in J(R)$ so there exists $s \in R$ such that $s(1-xr) = 1$. So $es(1-xr)e = e$, so $ese(e-xr) = e$. In other words, $e - xr$ admits a left inverse in eRe. So $r \in J(eRe)$ by Theorem 5.6 (b).

Conversely if $r \in J(eRe)$, since $r = ere$, it is sufficient to show that $r \in J(R)$. Let M be a simple left R-module. It is sufficient to show that $rM = 0$. We first need the following result:

Lemma 5.15. *If M is a simple left R-module and if $eM \neq 0$, then eM is a simple left eRe-module.*

PROOF - Let L be a non-zero sub-eRe-module of eM. Since M is simple, we have $RL = M$. Since $eL = L$, we have $eReL = eM$ and, since $eReL \subseteq L$, we get that $L = eM$. □

Now, $rM = reM = r.eM = 0$ since eM is simple and $r \in J(eRe)$. ■

REMARK 5.16 - If $e \in R$ is an idempotent, then $R = Re \oplus R(1-e)$. Indeed, if $r \in R$, then $r = re + r(1-e)$ so that $R = Re + R(1-e)$. Now, let $r \in Re \cap R(1-e)$. Write $r = xe = y(1-e)$ with x, $y \in R$. Then $re = xe^2 = xe = r$, but $re = y(1-e)e = y(e-e^2) = 0$. So $r = 0$. □

6. Projective, injective, flat modules

6.A. Exactness. Let R be a ring and let M be a left R-module. We shall study here properties of the functors $- \otimes_R M : \mathbf{Mod}_R \to \mathbf{Ab}$, $\mathrm{Hom}_R(M, -) : {}_R\mathbf{Mod} \to \mathbf{Ab}$ and $\mathrm{Hom}_R(-, M) : {}_R\mathbf{Mod} \to \mathbf{Ab}$.

Proposition 6.1. *Let M be a left R-module.*

(a) *If $X \to X' \to X'' \to 0$ is an exact sequence in $\mathbf{Mod}_R$, then the sequence of abelian groups $X \otimes_R M \to X' \otimes_R M \to X'' \otimes_R M \to 0$ is exact.*
(b) *If $X \to X' \to X'' \to 0$ is an exact sequence in ${}_R\mathbf{Mod}$, then the sequence of abelian groups $0 \to \mathrm{Hom}_R(X'', M) \to \mathrm{Hom}_R(X', M) \to \mathrm{Hom}_R(X, M)$ is exact.*
(c) *If $0 \to X \to X' \to X''$ is an exact sequence in ${}_R\mathbf{Mod}$, then the sequence of abelian groups $0 \to \mathrm{Hom}_R(M, X) \to \mathrm{Hom}_R(M, X') \to \mathrm{Hom}_R(M, X'')$ if exact.*

PROOF - (a) Let $X \xrightarrow{f} X' \xrightarrow{f'} X'' \to 0$ be an exact sequence in $\mathbf{Mod}_R$. Then, by Proposition 3.12 (b), the sequence $X' \otimes_R M \xrightarrow{f' \otimes_R \mathrm{Id}_M} X'' \otimes_R M \to 0$ is exact. Moreover, $(f' \otimes_R \mathrm{Id}_M) \circ (f \otimes_R \mathrm{Id}_M) = (f' \circ f) \otimes_R \mathrm{Id}_M = 0$. So it remains to show that $\mathrm{Ker}(f' \otimes_R \mathrm{Id}_M) \subseteq \mathrm{Im}(f \otimes_R \mathrm{Id}_M)$. In other words, if $\psi : (X' \otimes_R M)/(\mathrm{Im}(f \otimes_R \mathrm{Id}_M)) \to X'' \otimes_R M$ denotes the morphism induced by $f' \otimes_R M$, we must show that ψ is an isomorphism. For this, we shall construct its inverse.

Let $\varphi : X'' \times M \to (X' \otimes_R M)/(\mathrm{Im}(f \otimes_R \mathrm{Id}_M))$ be defined as follows. If $(x'', m) \in X'' \times M$, there exists $x' \in X'$ such that $f'(x') = x''$. We then set $\varphi(x'', m) = \overline{x' \otimes_R m}$, where $\overline{x' \otimes_R m}$ denotes the class of $x' \otimes_R m$ in $(X' \otimes_R M)/(\mathrm{Im}(f \otimes_R \mathrm{Id}_M))$. Let us first show that φ is well-defined. In other words, we must show that, if $f'(x'_1) = f'(x'_2)$ with x'_1, $x'_2 \in X'$, then $\overline{x'_1 \otimes_R m} = \overline{x'_2 \otimes_R m}$. But, if $f'(x'_1) = f'(x'_2)$, then $x'_1 - x'_2 \in \mathrm{Ker}\, f' = \mathrm{Im}\, f$,

so there exists $x \in X$ such that $x_2' = f(x) + x_1'$. Then $(x_1' \otimes_R m) - (x_2' \otimes_R m) = f(x) \otimes_R m \in \mathrm{Im}(f \otimes_R \mathrm{Id}_M)$, as expected.

It is now routine to check that φ is bilinear and R-balanced, and that the induced morphism of abelian groups $X'' \otimes_R M \to (X' \otimes_R M)/(\mathrm{Im}(f \otimes_R \mathrm{Id}_M))$, $x'' \otimes_R m \mapsto \varphi(x'', m)$ is an inverse of the map ψ.

(b) and (c) are left as exercises. ■

The left R-module M is called *flat* (respectively *injective*) if, for all exact sequences

$$0 \longrightarrow X \longrightarrow X'$$

in $\mathbf{Mod}_R$ (respectively ${}_R\mathbf{Mod}$), the sequence of abelian groups

$$0 \longrightarrow X \otimes_R M \longrightarrow X' \otimes_R M$$

(respectively

$$\mathrm{Hom}_R(X', M) \longrightarrow \mathrm{Hom}_R(X, M) \longrightarrow 0 \quad)$$

is exact. It is called *projective* if, for all exact sequences

$$X \longrightarrow X' \longrightarrow 0$$

in ${}_R\mathbf{Mod}$, the sequence

$$\mathrm{Hom}_R(M, X) \longrightarrow \mathrm{Hom}_R(M, X') \longrightarrow 0)$$

is exact. Of course, one can also define the notions of flatness, injectivity and projectivity for right R-modules.

Lemma 6.2. *Let $(M_i)_{i \in I}$ be a family of left R-modules. Then $\oplus_{i \in I} M_i$ is flat (respectively injective, respectively projective) if and only if M_i is flat (respectively injective, respectively projective) for all $i \in I$.*

Proof - Clear... ■

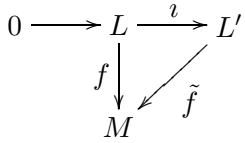
Example 6.3 - A free left R-module is projective and flat. Indeed, the flatness follows from Lemma 6.2 and from the fact that $X \otimes_R R \simeq X$ (see Corollary 3.17). The projectivity follows from Lemma 6.2 and from the fact that the map $\mathrm{Hom}_R(R, X) \to X$, $f \mapsto f(1)$ is an isomorphism of left R-modules (recall that, since R is an (R, R)-bimodule, $\mathrm{Hom}_R(R, M)$ is naturally endowed with a structure of left R-module by §3.D). □

Theorem 6.4. *Let M be a left R-module. Then:*

(a) *The following are equivalent:*
   (1) *M is flat.*
   (2) *For all exact sequence $L \to L' \to L''$ in $\mathbf{Mod}_R$, the sequence of abelian groups $L \otimes_R M \to L' \otimes_R M \to L'' \otimes_R M$ is exact.*

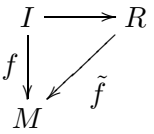
(b) *The following are equivalent:*
   (1) *M is injective.*

(2) *For all morphisms of left R-modules $\imath : L \to L'$ and $f : L \to M$ such that $\imath$ is injective, there exists a morphism of left R-modules $\tilde{f} : L' \to M$ such that $\tilde{f} \circ \imath = f$.*



(3) *For all exact sequences $L \to L' \to L''$ in ${}_R\mathbf{Mod}$, the sequence of abelian groups $\mathrm{Hom}_R(L'', M) \to \mathrm{Hom}_R(L', M) \to \mathrm{Hom}_R(L, M)$ is exact.*

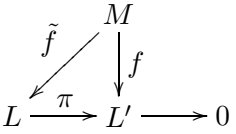
(4) *For all left ideal I of R and all morphisms of R-modules $f : I \to M$, there exists a morphism of left R-modules $\tilde{f} : R \to M$ extending f (**Baer's criterion**).*



(c) *The following are equivalent:*

(1) *M is projective.*

(2) *For all morphisms of left R-modules $\pi : L \to L'$ and $f : M \to L'$ such that π is surjective, there exists a morphism or left R-modules $\tilde{f} : M \to L$ such that $\pi \circ \tilde{f} = f$.*



(3) *For all exact sequences $L \to L' \to L''$ in ${}_R\mathbf{Mod}$, the sequence of abelian groups $\mathrm{Hom}_R(M, L) \to \mathrm{Hom}_R(M, L') \to \mathrm{Hom}_R(M, L'')$ is exact.*

(4) *M is a isomorphic to a direct summand of a free left R-module.*

Proof - (a) is easy. Let us now prove (b). It is easy to see that (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3). It is clear that (2) $\Rightarrow$ (4): indeed, apply (2) to the case where $L = I$, $L' = R$ and $\imath : I \to R$ is the canonical injection. Let us prove that (4) $\Rightarrow$ (2). So assume that (4) holds and let $\imath : L \hookrightarrow L'$ be an injective morphism of R-modules and let $f : L \to M$ be a morphism of R-modules. We may assume that $L \subseteq L'$ and that $\imath$ is the canonical injection. Let $\mathcal{E}$ be the set of pairs $(\tilde{L}, \tilde{f})$ such that $\tilde{L}$ is a submodule of L' containing L and $\tilde{f} : \tilde{L} \to M$ extends f. We define an order $\leqslant$ on $\mathcal{E}$ as follows: we write $(\tilde{L}_1, \tilde{f}_1) \leqslant (\tilde{L}_2, \tilde{f}_2)$ if $\tilde{L}_1 \subseteq \tilde{L}_2$ and $\tilde{f}_1$ is the restriction of $\tilde{f}_2$ to $\tilde{L}_1$. If $\mathcal{S}$ is a totally ordered subset of $\mathcal{E}$, we then set $\tilde{L}^+ = \bigcup_{(\tilde{L},\tilde{f})\in\mathcal{S}} \tilde{L}$ and we define $\tilde{f}^+ : \tilde{L}^+ \to M$ by $\tilde{f}^+(l) = \tilde{f}(l)$ whenever $l \in \tilde{L}$ for some $(\tilde{L}, \tilde{f}) \in \mathcal{S}$ (it is easy to check that $\tilde{f}^+$ is well-defined). Then $(\tilde{L}^+, \tilde{f}^+) \in \mathcal{E}$ and is an upper bound for $\mathcal{S}$. So, by Zorn's Lemma, $\mathcal{E}$ admits a maximal element $(\tilde{L}, \tilde{f})$. We only need to prove that $\tilde{L} = L'$. Let $x \in L'$. Let $I = \{r \in R \mid rx \in \tilde{L}\}$. Then I is a left R-ideal of R. Let $g : I \to M$, $r \mapsto \tilde{f}(rx)$. Then g is a well-defined R-linear map. So, since (4) holds,

there exists $\tilde{g} : R \to M$ extending g. We now set

$$\begin{array}{rccc} \tilde{f}' : & \tilde{L} + Rx & \longrightarrow & M \\ & l + rx & \longmapsto & \tilde{f}(l) + \tilde{g}(r). \end{array}$$

It is readily seen that $\tilde{f}'$ is well-defined and is R-linear. Moreover, it extends $\tilde{f}$, so $(\tilde{L} + Rx, \tilde{f}') \in \mathcal{E}$. Since $(\tilde{L}, \tilde{f})$ is maximal, we get that $\tilde{L} + Rx = \tilde{L}$, that is $x \in \tilde{L}$. So $\tilde{L} = L'$.

Let us now prove (c). It is easy to show that (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3). The fact that (4) $\Rightarrow$ (1) follows from Example 6.3 and Proposition 6.2. Let us now show that (2) $\Rightarrow$ (4). Let $(m_i)_{i \in I}$ be a family of generators of M. Let $\pi : R[I] \to M$, $\sum_{i \in I} r_i i \mapsto \sum_{i \in I} r_i m_i$. It is a surjective R-linear map. By (2) applied to π and $f = \mathrm{Id}_M$, there exists $\tilde{f} : M \to R[I]$ such that $f \circ \tilde{f} = \mathrm{Id}_M$. It is then easy to check that $R[I] \simeq \tilde{f}(M) \oplus \mathrm{Ker}\, f$ (see Exercise II.1), and $\tilde{f}(M) \simeq M$ because $\tilde{f}$ is injective. ■

Corollary 6.5. *A projective module is flat.*

Proof - This follows from Theorem 6.4 (c) and from Lemma 6.2. ■

Corollary 6.6. *Assume that M is finitely generated. Then M is projective if and only if it is isomorphic to a direct summand of a free R-module of finite rank.*

Proof - This follows from the proof of Theorem 6.4. ■

Examples 6.7 - (1) If $e \in R$ is an idempotent, then Re is a projective left R-module. Indeed, $R = Re \oplus R(1 - e)$ (see Remark 5.16), so Re is a direct summand of the free R-module R. It is in particular flat.

(2) If R is a principal ideal domain, then any finitely generated projective R-module is free. This follows from Theorem 6.4 and from the fact that a submodule of a finitely generated free module is always free in this case.

(3) Assume again in this example that R is a principal ideal domain. The R-module M is called *divisible* if, for all $r \in R$, $r \neq 0$, we have $rM = M$ (for instance, $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{R}/\mathbb{Z}$ are divisible $\mathbb{Z}$-modules). We shall prove here the following result:

> *If R is a principal ideal domain, then a left R-module is injective if and only if it is divisible.*

First, assume that M is not divisible. Then there exists $r \in R$, $r \neq 0$ and $m \in M$ such that $m \notin rM$. Let $\imath : Rr \to R$ be the canonical injection and let $f : Rr \to M$, $ar \mapsto am$. Then f cannot be extended to a map $\tilde{f} : R \to M$ because, if such a map exists, then $\tilde{f}(1)$ must satisfied $r\tilde{f}(1) = \tilde{f}(r) = f(r) = m$, which is impossible. So M is not injective.

Conversely, assume that M is divisible. We shall use Baer's criterion to show that M is injective. Let I be an ideal of R and let $f : I \to M$ be an R-linear map. We may assume that $I \neq 0$, for otherwise, it is easy to find an extension of f. Since R is a principal ideal domain, there exists $r \in R$ such that $I = Rr$. Let $m = f(r)$. Since M is divisible, there exists $m' \in M$ such that $rm' = m$. We then defined $\tilde{f} : R \to M$, $a \mapsto am'$. Then $\tilde{f}(r) = m$ so $\tilde{f}$ is an extension of f. So M is injective.

(4) We shall give in Exercise 6.7 an example of a projective module over a commutative integral domain which is not free. □

Proposition 6.8. *Let M be a left R-module. Then:*

(a) *There exists an injective module I and an injective morphism $M \to I$.*
(b) *There exists a projective module P and a surjective morphism $P \to M$. If M is finitely generated, then P can be chosen finitely generated.*

PROOF - (b) has already been proved in Theorem 6.4 (c).

Let us now prove (a). This will be done in several steps. We first show the following

> **Lemma 6.9.** *If D is a divisible abelian group, then $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module.*
>
> PROOF - Recall that, since R is naturally a $(\mathbb{Z}, R)$-bimodule, the abelian group $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is naturally endowed with a structure of left R-module (see §3.D). Let $0 \longrightarrow X \longrightarrow X'$ be an exact sequence of left R-modules. We must show that the sequence $\mathrm{Hom}_R(X', \mathrm{Hom}_{\mathbb{Z}}(R, D)) \longrightarrow \mathrm{Hom}_R(X, \mathrm{Hom}_{\mathbb{Z}}(R, D)) \longrightarrow 0$ is exact. But, by the adjointness of Hom and $\otimes$ (see Theorem 3.22), this amounts to show that the sequence $\mathrm{Hom}_{\mathbb{Z}}(X', D) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X, D) \longrightarrow 0$ is exact. But this follows from the fact that D is an injective $\mathbb{Z}$-module by Example 6.7 (3). ■

So assume first that the result has been proved whenever $R = \mathbb{Z}$. Then there exists an injective morphism of abelian groups $M \hookrightarrow D$, where D is divisible. Then the map $\mathrm{Hom}_{\mathbb{Z}}(R, M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, D)$ is injective (see Proposition 6.1 (c)) and $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module by Lemma 6.9. On the other hand, the map $M \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$, $m \mapsto (r \mapsto rm)$ is an injective R-linear map. So we get an injective R-linear map by composition $M \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, D)$.

Therefore, it remains to show that the result holds whenever $R = \mathbb{Z}$, which we assume now. Let $M^\wedge = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. Then the natural map $M \to (M^\wedge)^\wedge$, $m \mapsto (f \mapsto f(m))$ is a morphism of abelian groups, and it is easily checked that it is injective. It remains to show that $(M^\wedge)^\wedge$ can be embedded in a divisible abelian group. Let $F \longrightarrow M^\wedge$ be a surjective map, where F is free (such a map exists by the statement (b) of this proposition). Then, by Proposition 6.1 (b), the map $(M^\wedge)^\wedge \to F^\wedge$ is injective. So it remains to show that $F^\wedge$ is divisible. But, since F is free, $F^\wedge$ is isomorphic to a direct sum of copies of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}$, which are all divisible. ■

Corollary 6.10. *Let M be a left R-module. Then:*

(a) *M is injective if and only if all injective morphisms $\imath : M \hookrightarrow M'$ split (i.e. there exists $\pi : M' \to M$ such that $\pi \circ \imath = \mathrm{Id}_M$).*
(b) *M is projective if and only if all surjective morphisms $\pi : M' \to M$ split (i.e. there exists $\imath : M \to M'$ such that $\pi \circ \imath = \mathrm{Id}_M$).*

PROOF - The proofs of (a) and (b) are entirely similar. Let us prove only (b). If M is projective, then it is clear that any surjective morphism $M' \to M$ splits (by applying Theorem 6.4 (2) to the case where $L = M'$, $L' = M$ and $f = \mathrm{Id}_M$). Conversely, assume that all surjective morphisms $M' \to M$ split. By Proposition 6.8 (b), there exists a surjective morphism $M' \to M$ where M' is projective (even free if we want). Since this

morphism splits, this gives an embedding of M as a direct summand of a projective module (see Exercise II.1), so M is projective by Lemma 6.2. ■

6.B. Local rings.

Definition 6.11. *The ring R is called **local** if it has only one maximal left ideal.*

Examples 6.12 - (1) A field (or a division ring) is a local ring.

(2) $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring if p is a prime.

(3) $\mathbb{Z}$ is not a local ring. □

Proposition 6.13. *The following are equivalent:*

(1) *R is local.*
(2) *R has only one maximal right ideal.*
(3) *$R/J(R)$ is a division ring.*
(4) *$R^\times = R \setminus J(R)$.*
(5) *$R \setminus R^\times$ is a two-sided ideal of R.*

Proof - Let $\bar{R} = R/J(R)$ and, if $r \in R$, we denote by $\bar{r}$ its image in $\bar{R}$.

(1) $\Rightarrow$ (3): if R is local, then $J(R)$ is a maximal left ideal of R. So 0 is the only maximal left ideal of $\bar{R}$. In particular, any non-zero element of $\bar{R}$ has a left inverse. Now, let $\bar{r} \in \bar{R}$. Then there exists $\bar{s} \in \bar{R}$ such that $\bar{s}\bar{r} = \bar{1}$. Now $\bar{s} \neq 0$, so $\bar{s}$ has a left inverse (say $\bar{t}$). Then $\bar{r}\bar{s} = (\bar{t}\bar{s})(\bar{r}\bar{s}) = \bar{t}(\bar{s}\bar{r})\bar{s} = \bar{1}$, so $\bar{s}$ is also a right inverse. This shows that $\bar{R}$ is a division ring.

(3) $\Rightarrow$ (2) is clear and (3) $\Rightarrow$ (1) are clear. By symmetry, we also have that (2) $\Rightarrow$ (3). So (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3).

It is also clear that (4) $\Rightarrow$ (5). The fact that (5) $\Rightarrow$ (4) follows from Theorem 5.6 (c). Moreover, if (4) holds, then any non-zero element in $\bar{R}$ is invertible, so $\bar{R}$ is a division ring. In oter words, (4) $\Rightarrow$ (3). Now, if (3) holds and if $r \notin J(R)$, then there exists $s \in R$ such that $\bar{s}\bar{r} = \bar{r}\bar{s} = \bar{1}$. So $sr \in 1 + J(R)$, so sr has a left inverse. In particular, r has a left inverse. Similarly, r has a right inverse. So $r \in R^\times$, so (4) holds and we are done. ■

Theorem 6.14. *If R is a local ring then every finitely generated projective R-module is free.*

Proof - Let M be a projective left R-module. Let $\bar{R} = R/J(R)$ and $\bar{M} = M/J(R)M \simeq \bar{R} \otimes_R M$. Then $\bar{M}$ is an $\bar{R}$-module. But $\bar{R}$ is a division ring, so $\bar{M}$ is free (and finitely generated): let $m_1, \ldots, m_n$ be elements of M such that $(\bar{m}_1, \ldots, \bar{m}_n)$ is an $\bar{R}$-basis of $\bar{M}$. Let $L = Rm_1 + \cdots + Rm_n$. Then L is a submodule of M and $L + J(R)M = M$. So, by Nakayama's Lemma (Theorem 5.9) and since M is finitely generated, $L = M$. In other words, the R-linear map

$$\begin{array}{rccc} \pi : & R^n & \longrightarrow & M \\ & (r_1, \ldots, r_n) & \longmapsto & \sum_{i=1}^n r_i m_i \end{array}$$

is surjective. Since M is projective, there exists a splitting $\imath : M \to R^n$ of this morphism, i.e. $\pi \circ \imath = \mathrm{Id}_M$. So $\imath$ is injective.

Let us show that it is surjective. But the maps $\bar{\pi} : \bar{R}^n \to \bar{M}$ and $\bar{\imath} : \bar{M} \to \bar{R}^n$ induced by π and $\imath$ satisfies $\bar{\pi} \circ \bar{\imath} = \mathrm{Id}_{\bar{M}}$. Also, by construction, $\bar{\pi}$ is an isomorphism. So $\bar{\imath}$ is surjective. In particular, $R^n = (\mathrm{Im}\, \imath) + J(R)^n$ so, again by Nakayama's Lemma, $\mathrm{Im}\, \imath = R^n$, that is $\imath$ is surjective. ■

7. Morita equivalences and Skolem-Noether Theorem

7.A. Morita equivalences. Let R and S be two rings.

Definition 7.1. *A **Morita equivalence** between R and S is the following datum:*

- *an (R,S)-bimodules A and an (S,R)-bimodule B;*
- *an isomorphism of (R,R)-bimodule $\varphi : A \otimes_S B \simeq R$;*
- *an isomorphism of (S,S)-bimodules $\psi : B \otimes_R A \simeq S$.*

*If (A, B, φ, ψ) is a Morita equivalence between R and S, we say that the rings R and S are **Morita equivalent**.*

Assume in this section that we are given a Morita equivalence (A, B, φ, ψ) between R and S. Let

$$\begin{array}{rccc} \mathcal{F} : & {}_S\mathbf{Mod} & \longrightarrow & {}_R\mathbf{Mod} \\ & N & \longmapsto & A \otimes_S N \end{array}$$

and

$$\begin{array}{rccc} \mathcal{G} : & {}_R\mathbf{Mod} & \longrightarrow & {}_S\mathbf{Mod} \\ & M & \longmapsto & B \otimes_S M \end{array}$$

be the functors induced by these bimodules. Then, since $A \otimes_S B \simeq R$ and $B \otimes_R A \simeq S$, we have natural isomorphisms of functors $\tilde{\varphi} : \mathcal{F} \circ \mathcal{G} \xrightarrow{\sim} (A \otimes_S B) \otimes_R - \xrightarrow{\sim} \mathrm{Id}_{{}_R\mathbf{Mod}}$ and $\tilde{\psi} : \mathcal{G} \circ \mathcal{F} \xrightarrow{\sim} \mathrm{Id}_{{}_S\mathbf{Mod}}$ induced by φ and ψ respectively (see §3.D). In other words, $\mathcal{F}$ and $\mathcal{G}$ are equivalences of categories.

Remark 7.2 - If (A, B, φ, ψ) is a Morita equivalence between R and S, then, by symmetry, the functors $- \otimes_R A$ and $- \otimes_S B$ are equivalences of categories between $\mathbf{Mod}_R$ and $\mathbf{Mod}_S$. □

Proposition 7.3. *If M and M' are two left R-modules, then the map*

$$\mathcal{G} : \mathrm{Hom}_R(M, M') \longrightarrow \mathrm{Hom}_S(\mathcal{G}(M), \mathcal{G}(M'))$$

is an isomorphism of abelian groups. If $M = M'$, this is an isomorphism of rings.

A similar statement holds for the functor $\mathcal{F}$.

Proof - The fact that $\mathcal{G}$ is a morphism of abelian groups is clear (as it is also clear that it is a morphism of rings whenever $M = M'$). The fact that it is bijective follows from Exercise I.9. ■

As a consequence of the previous proposition, we shall see now that a Morita equivalence preserves many properties of modules, namely the ones that are defined only in terms of the category of modules (and without reference to the ring). We need another definition.

Definition 7.4. *A left R-module M is called* ***decomposable*** *if $M \simeq M' \oplus M''$ for some non-zero modules M' and M''. The left R-module M is called* ***indecomposable*** *if $M \neq 0$ and M is not decomposable.*

Corollary 7.5. *Let $f : M \to M'$ be a morphism of left R-modules. Then:*

(a) *$M \neq 0$ if and only if $\mathcal{G}(M) \neq 0$.*
(b) *M is an indecomposable R-module if and only if $\mathcal{G}(M)$ is an indecomposable S-module.*
(c) *M is a projective R-module if and only if $\mathcal{G}(M)$ is a projective S-module.*
(d) *$M \to M' \to M''$ is an exact sequence of R-modules if and only if $\mathcal{G}(M) \to \mathcal{G}(M') \to \mathcal{G}(M'')$ is an exact sequence of S-modules.*
(e) *M is a simple R-module if and only if $\mathcal{G}(M)$ is simple S-module.*
(f) *M is a flat R-module if and only if $\mathcal{G}(M)$ is a flat S-module.*
(g) *M is an injective R-module if and only if $\mathcal{G}(M)$ is an injective S-module.*

Proof - (a) follows from the fact that $\mathcal{F}(\mathcal{G}(M)) \simeq M$. (b) follows from (a). Let us now prove(c). By symmetry, we only need to prove the "only if" part. So assume that M is projective. Let $\pi : F \to \mathcal{G}(M)$ be a surjective morphism where F is a free S-module. Then, by Proposition 6.1 (a), the map $\mathcal{F}(\pi) : \mathcal{F}(F) \to \mathcal{F}(\mathcal{G}(M))$ is surjective. Since $\mathcal{F}(\mathcal{G}(M)) \simeq M$ is projective, there exists a map $\jmath : \mathcal{F}(\mathcal{G}(M)) \to \mathcal{F}(F)$ such that $\mathcal{F}(\pi) \circ \jmath = \mathrm{Id}_{\mathcal{F}(\mathcal{G}(M))}$. By Proposition 7.3, there exists $\imath : F \to \mathcal{G}(M)$ such that $\mathcal{F}(\imath) = \jmath$. Then $\mathcal{F}(\pi \circ \imath) = \mathrm{Id}_{\mathcal{F}(\mathcal{G}(M))}$, so $\pi \circ \imath = \mathrm{Id}_{\mathcal{G}(M)}$ again by Proposition 7.3. So the map π splits, hence $\mathcal{G}(M)$ is isomorphic to a direct summand of the free module F (see Exercise II.1), so $\mathcal{G}(M)$ is projective.

(d) Now, by (c), $B = \mathcal{G}(S)$ is projective as a left R-module. By symmetry, B is projective as a right S-module. Similarly, A is projective as a left S-module and as a right R-module. So B is flat as a right S-module. This shows (d).

(e) Again, by symmetry, we only need to prove the "only if" part. So assume that M is simple. Let L be a non-zero submodule of $\mathcal{G}(M)$. Then the exact sequence $0 \to L \to \mathcal{G}(M)$ induces an exact sequence $0 \to \mathcal{F}(L) \to \mathcal{F}(\mathcal{G}(M))$ by (d). But, by (a), $\mathcal{F}(L) \neq 0$. Since $\mathcal{F}(\mathcal{G}(M)) \simeq M$ is simple, we get that $\mathcal{F}(L) = \mathcal{F}(\mathcal{G}(M))$, in other words, the map $\mathcal{F}(L) \to \mathcal{F}(\mathcal{G}(M))$ is an isomorphism. So, again by (d), the map $L \to \mathcal{G}(M)$ is an isomorphism, so $L = \mathcal{G}(M)$. This shows that $\mathcal{G}(M)$ is simple.

(f) and (g) are left as exercises. ■

7.B. Example: matrix rings. Let $n \geqslant 1$ and let $\mathrm{Col}_n(R)$ (respectively $\mathrm{Row}_n(R)$) be the set of column vectors (respectively row vectors) of length n with coefficients in R (as a set, it is canonically in bijection with R^n). We view $\mathrm{Col}_n(R)$ (respectively $\mathrm{Row}_n(R)$) as a $(\mathrm{Mat}_n(R), R)$-bimodule (respectively $(R, \mathrm{Mat}_n(R))$-bimodule) in the natural way. Now, let

$$\begin{array}{rccc} \varphi : & \mathrm{Row}_n(R) \otimes_{\mathrm{Mat}_n(R)} \mathrm{Col}_n(R) & \longrightarrow & R \\ & V \otimes_{\mathrm{Mat}_n(R)} U & \longmapsto & VU \end{array}$$

and

$$\begin{array}{rccc} \psi : & \mathrm{Col}_n(R) \otimes_R \mathrm{Row}_n(R) & \longrightarrow & \mathrm{Mat}_n(R) \\ & U \otimes_R V & \longmapsto & UV. \end{array}$$

Theorem 7.6. *The datum* $(\mathrm{Row}_n(R), \mathrm{Col}_n(R), \varphi, \psi)$ *is a Morita equivalence between the rings* R *and* $\mathrm{Mat}_n(R)$.

PROOF - We only need to show that φ and ψ are isomorphisms of bimodules. First, it is easily checked that φ is a morphism of (R,R)-bimodule and that ψ is a morphism of $(\mathrm{Mat}_n(R), \mathrm{Mat}_n(R))$-bimodules.

We denote by E_{ij} the $n \times n$ matrix whose (i,j)-entry is 1 and whose all other entries are zero. We denote by C_i (respectively R_j) the column (respectively row) matrix whose i-th term (respectively j-th term) is 1 and whose all other entries are 0. Then

$$E_{ij} = C_i R_j \tag{1}$$

and

$$R_j C_i = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

• Let us first prove that ψ is an isomorphism. First, by (1), ψ is surjective. Now, let $x \in \mathrm{Ker}\,\psi$. Since $(C_i)_{1 \leqslant i \leqslant n}$ and $(R_j)_{1 \leqslant j \leqslant n}$ are R-basis of $\mathrm{Col}_n(R)$ and $\mathrm{Row}_n(R)$ respectively, there exists $r_{ij} \in R$ such that $x = \sum_{i,j} C_i r_{ij} \otimes_R R_j$. So $\psi(x) = \sum_{i,j} r_{ij} E_{ij} = 0$, so all the r_{ij}'s are zero. In particular, $x = 0$. So ψ is an isomorphism.

• Let us now prove that φ is an isomorphism. First φ is surjective by (2). Now, let $x \in \mathrm{Ker}\,\varphi$. Again, we can write $x = \sum_{i,j} r_{ij}(R_j \otimes_{\mathrm{Mat}_n(R)} C_i)$ But $R_j = R_1 E_{1j}$, $E_{1j} C_i = 0$ if $i \neq j$ and $E_{1i} C_i = C_1$. So $R_j \otimes_{\mathrm{Mat}_n(R)} C_i$ is equal to 0 or $R_1 \otimes_{\mathrm{Mat}_n(R)} C_1$. So $x = rR_1 \otimes_{\mathrm{Mat}_n(R)} C_1$ for some $r \in R$. Since $\varphi(R_1 \otimes_{\mathrm{Mat}_n(R)} C_1) = 1$ by (2). Hence $r = 0$ because $\varphi(x) = 0$. So $x = 0$ and φ is injective. ■

7.C. Skolem-Noether Theorem via Morita equivalences. We are now ready to prove the following result:

Theorem 7.7 (Skolem-Noether). *Let* R *be a commutative ring such that all finitely generated projective* R*-modules are free. Let* $\sigma : \mathrm{Mat}_n(R) \to \mathrm{Mat}_n(R)$ *be an automorphism of* R*-algebras. Then there exists an element* $g \in \mathrm{Mat}_n(R)^\times$ *such that* $\sigma(x) = gxg^{-1}$ *for all* $x \in \mathrm{Mat}_n(R)$.

EXAMPLE 7.8 - If R is a field, or if R is a principal ideal domain, or if R is a commutative local ring then all finitely generated projective R-modules are free (for local rings, see Theorem 6.14). So Skolem-Noether's Theorem can be applied to these rings. It is also true that, if $R = K[X_1, \ldots, X_n]$ where K is a field, then any projective R-module is free (this difficult result was first conjectured by Serre and proved by Quillen). □

PROOF - We shall use here the notation of the previous subsection 7.B and the Theorem 7.6. So we assume here that $S = \mathrm{Mat}_n(R)$, that $A = \mathrm{Row}_n(R)$ and $B = \mathrm{Col}_n(R)$. We shall prove several intermediate results. Let us fix a left R-module M.

(1) *M is finitely generated if and only if $\mathcal{G}(M)$ is finitely generated.*

PROOF - This is left as an exercise. ■

(2) *Assume that M is finitely generated. Then M is indecomposable and projective if and only if $M \simeq R$.*

PROOF - If $M \simeq R$, and if $M \simeq M' \oplus M''$, then M' and M'' are projective hence are free: $M' \simeq R[I]$ and $M' \simeq R[J]$ where I and J are disjoint sets. Then $R \simeq R[I \cup J]$. Let $\mathfrak{m}$ be a maximal ideal of R. Then, by tensorizing with $R/\mathfrak{m}$, we get that $R/\mathfrak{m} \simeq R/\mathfrak{m}[I \cup J]$ and, since R is commutative, this is an isomorphism of $R/\mathfrak{m}$-modules, and $R/\mathfrak{m}$ is a field. So $|I \cup J| = 1$, so $I = \varnothing$ or $J = \varnothing$, that is $M' = 0$ or $M'' = 0$. This shows that M is indecomposable.

Conversely, if M is indecomposable and projective, then M is free and so, since it is indecomposable, we must have $M \simeq R$. ■

(3) $\mathrm{Col}_n(R)$ *is the unique finitely generated projective indecomposable module.*

PROOF - This follows from (2) and from Corollary 7.5 (b) and (c). ■

If V is a left $\mathrm{Mat}_n(R)$-module, we denote by $V^{(\sigma)}$ the left $\mathrm{Mat}_n(R)$-module whose underlying abelian group is still V, but on which $x \in \mathrm{Mat}_n(R)$ acts by multiplication by $\sigma(x)$. Then:

(4) $\mathrm{Mat}_n(R)^{(\sigma)} \simeq \mathrm{Mat}_n(R)$.

PROOF - Indeed, $\sigma : \mathrm{Mat}_n(R) \to \mathrm{Mat}_n(R)^{(\sigma)}$ is an isomorphism of $\mathrm{Mat}_n(R)$-modules. ■

(5) *If V is a projective (respectively indecomposable, respectively finitely generated) $\mathrm{Mat}_n(R)$-module, then so is $V^{(\sigma)}$.*

PROOF - Indeed, $(V \oplus W)^{(\sigma)} = V^{(\sigma)} \oplus M^{(\sigma)}$ so, if V is a direct summand of a free $\mathrm{Mat}_n(R)$-module, it follows from (4) that $V^{(\sigma)}$ is also a direct summand of a free module. The statements about indecomposable and finitely generated modules are clear. ■

By (3) and (5), we have that $\mathrm{Col}_n(R)^{(\sigma)}$ is isomorphic to $\mathrm{Col}_n(R)$ as a $\mathrm{Mat}_n(R)$-module. Let $f : \mathrm{Col}_n(R) \to \mathrm{Col}_n(R)^{(\sigma)}$ be such an isomorphism. By identifying $\mathrm{Col}_n(R)$ with R^n, and since R is commutative, f is given by a matrix $g \in \mathrm{Mat}_n(R)^\times$: we have $f : \mathrm{Col}_n(R) \to \mathrm{Col}_n(R)^{(\sigma)}$, $C \mapsto gC$.

Now, if $x \in \mathrm{Mat}_n(R)$, we have $f(xC) = \sigma(x)f(C)$, so that $gxC = \sigma(x)gC$, that is $xC = g^{-1}\sigma(x)gC$. Since this holds for all $C \in \mathrm{Col}_n(R)$, we have that $x = g^{-1}\sigma(x)g$ as desired. ■

8. Semisimple rings and modules

As usual, R will denote a fixed ring.

8.A. Semisimple modules.

Definition 8.1. *A left R-module M is called **semisimple** if it is isomorphic to a direct sum of simple modules.*

Since the definition of a semisimple module involves only the category of modules ${}_R\mathbf{Mod}$ and not the ring R itself, we are not surprised that a Morita equivalence preserves semisimplicity of modules:

Lemma 8.2. *Let R and S be two Morita equivalent rings and let $\mathcal{G} : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ be the equivalence of categories induced by a Morita equivalence between R and S. Let M be a left R-module. Then M is semisimple if and only if $\mathcal{G}(M)$ is semisimple.*

PROOF - This follows from Corollary 7.5 (e) and from the fact that the functor $\mathcal{G}$ is compatible with direct sums. ■

Theorem 8.3. *The following are equivalent:*

(1) *M is semisimple.*
(2) *M is a sum (not necessarily direct) of simple modules.*
(3) *Every submodule of M is a direct summand of M.*

PROOF - It is clear that (1) $\Rightarrow$ (2). Let us now show the following

> **Lemma 8.4.** *Assume that (2) holds and let L be a submodule of M. Then there exist simple submodules $(S_a)_{a\in A}$ of M such that $M = L \oplus (\underset{a\in A}{\oplus} S_a)$.*
>
> PROOF - Let $(S_i)_{i\in I}$ denote the set of all simple submodules of M. By hypothesis, $M = \sum_{i\in I} S_i$. We denote by $\mathcal{M}$ the set of subsets A of I such that the sum $\sum_{a\in A} S_a$ is direct and the sum $L + (\sum_{a\in A} S_a)$ is direct. We have $\in \mathcal{M}$, so that $\mathcal{M}$ is not empty. Also, it is readily seen that $\mathcal{M}$ satisfies the hypothesis of Zorn's Lemma. Hence $\mathcal{M}$ admits a maximal element: let A be a maximal element of $\mathcal{M}$. Let $L' = L \oplus (\underset{a\in A}{\oplus} S_a)$. We want to show that $L' = M$, so that the lemma will be proved.
>
> Assume that $M/L' \neq 0$. Let $\pi : M \to M/L'$ be the canonical projection. Since $M = \sum_{i\in I} S_i$, there exists $i \in I$ such that $\pi(S_i) \neq 0$. In particular, S_i is not contained in L', so $L' \subseteq S_i$ is a proper submodule of S_i. Since S_i is simple, we have that $L' \cap S_i = 0$. This shows that $A \cup \{i\} \in \mathcal{M}$. Since A is maximal, we get that $i \in A$, so $S_i \subseteq L'$, which is impossible. So $M/L' = 0$. ■

Now, by the Lemma 8.4, we get that (2) $\Rightarrow$ (1) (indeed, take $L = 0$ in Lemma 8.4) and that (2) $\Rightarrow$ (3). Let us now show that (3) $\Rightarrow$ (2). So assume that (3) holds. Let $(S_i)_{i\in I}$ denote the set of all simple submodules of M. Let $L = \sum_{i\in I} S_i$. We want to show that $L = M$. So assume that $L \neq M$. By (3), there exists a submodule L' of M such that $M = L \oplus L'$. Then $L' \neq 0$. Let $v \in L$ be such that $v \neq 0$. Let $f : R \to M$, $r \mapsto rv$. Since $v \neq 0$, the kernel of f is a proper left ideal of R so, by Corollary 5.2, there exists a maximal left ideal I of R such that $\operatorname{Ker} f \subseteq I$. Then Iv is a submodule of M so, by (3), there exists a submodule N of M such that $M = Iv \oplus N$. Let $S = N \cap Rv$. Then it is easy to see that $Rv = Iv \oplus S$. Then $S \simeq Rv/Iv$. But $Rv/Iv \simeq R/I$ because I contains $\operatorname{Ker} f$ and R/I is simple because I is maximal. So S is simple. But $S \subseteq Rv \subseteq L'$ and $L' \cap L = 0$. So $S \cap L = 0$: this contradicts the fact that L contains all the simple submodules of M. ■

REMARKS 8.5 - (1) If $0 \to L \to M \to N \to 0$ is an exact sequence and if M is semisimple, then it follows easily from Theorem 8.3 that L and N are semisimple. Indeed,

let $\pi : M \to N$ be surjective. Since M is the sum of its simple submodules, we have that N is the sum of all $\pi(S)$, where S runs over the set of simple submodules of M. But $\pi(S)$ is 0 or simple, so N is a sum of simple submodules. On the other hand, if L is a submodule of M, there exists a submodule L' of L such that $M = L \oplus L'$: in particular, there exists a surjective map $\tau : M \to L$, so the previous argument can be applied to show that L is semisimple.

(2) If M is semisimple, then $\mathrm{rad}(M) = J(R)M = 0$. Indeed, if $M = \oplus_{a\in A}\mathcal{S}_a$, where $\mathcal{S}_a$ is a simple left R-module, then $M_{a_0} = \oplus_{a\neq a_0}\mathcal{S}_a$ is a maximal submodule of M (and $M/M_{a_0} \simeq \mathcal{S}_{a_0}$) for all $a_0 \in A$, and $\bigcap_{a\in A} M_a = 0$.

(3) The isomorphy classes of simple left R-modules form a set. Indeed, let $\equiv$ denote the equivalence relation on $\mathrm{Max}_l(R)$ defined by $\mathfrak{m} \equiv \mathfrak{m}'$ if the R-modules $R/\mathfrak{m}$ and $R/\mathfrak{m}'$ are isomorphic. Then, if $(\mathfrak{m}_i)_{i\in I}$ is a set of representative of equivalence classes of maximal left ideals of R, then $(R/\mathfrak{m}_i)_{i\in I}$ is a set of representatives of isomorphy classes of simple left R-modules (see Lemma 5.4).

(4) Let I be a two-sided ideal of R and assume that $IM = 0$. Then M can be viewed as an $\bar{R}$-module, where $\bar{R} = R/I$. Then M is R-semisimple if and only if it is $\bar{R}$-semisimple. □

Before studying the semisimple modules, we shall review some properties of simple modules:

Theorem 8.6 (Schur's Lemma). *Let S and T be two simple left R-modules. Then:*

(a) *If $f \in \mathrm{Hom}_R(S,T)$ and if $f \neq 0$, then f is an isomorphism.*
(b) *If $S \not\simeq T$, then $\mathrm{Hom}_R(S,T) = 0$.*
(c) *$\mathrm{End}_R(S)$ is a division ring.*

Proof - (a) Assume that $f \in \mathrm{Hom}_R(S,T)$ and that $f \neq 0$. Then $\mathrm{Ker}\, f$ (respectively $\mathrm{Im}\, f$) is a non-zero submodule of R (respectively T), so $\mathrm{Ker}\, f = S$ (respectively $\mathrm{Im}\, f = T$) because S (respectively T) is simple. So f is injective and surjective: it is an isomorphism.
(b) and (c) now follow easily from (a). ■

We now fix once and for all a family $(S_i)_{i\in I}$ of representatives of isomorphy classes of simple left R-modules (see Remark 8.5 (3)). We set

$$D_i = \mathrm{End}_R(S_i)$$

for all $i \in I$. By Schur's Lemma, D_i is a division ring.

Theorem 8.7. *Let M be a semisimple left R-module. Let $(S_i)_{i\in I}$ denotes a set of representatives of isomorphy classes of simple left R-modules. For each $i \in I$, let M_i denote the submodule of M equal to the sum of all its simple submodules which are isomorphic to S_i. Then:*

(a) *$M = \underset{i\in I}{\oplus} M_i$.*
(b) *If S is a simple submodule of M_i, then $S \simeq S_i$.*

(c) *Let $\pi_i : M \to M_i$ and $\imath_i : M_i \to M$ be the canonical projection and injection respectively. Then the map*

$$\begin{array}{ccc} \mathrm{End}_R(M) & \longrightarrow & \prod_{i\in I} \mathrm{End}_R(M_i) \\ f & \longmapsto & (\pi_i f \imath_i)_{i\in I} \end{array}$$

is a ring isomorphism.

(d) *Write $M_i = \underset{a\in A_i}{\oplus} S_{i,a}$, where $S_{i,a}$ are simple submodules of M_i (which are isomorphic to S_i by (b)). If moreover A_i is finite and has cardinality n_i, then*

$$\mathrm{End}_R(M_i) \simeq \mathrm{Mat}_{n_i}(D_i).$$

Proof - Let us first prove (b). Let S be a simple submodule of M_i. By Remark 8.5 (1), M_i is semisimple so, by Theorem 8.3, there exists a submodule N of M_i such that $M_i = S \oplus N$. Let $\pi : M_i \to S$ be the projection on the first component. Now, M_i is a sum of submodules isomorphic to S_i. So there exists a submodule S' of M_i which is isomorphic to S_i and such that $\pi(S') \neq 0$. By Schur's Lemma (a), we get that $S' \simeq S$, so that $S \simeq S_i$.

(a) It is clear that $M = \sum_{i\in I} M_i$. Let us now show that this sum is direct. By Theorem 8.3, there exists a submodule L of M such that $M = L \oplus M_i$. Let $j \in I$, $j \neq i$. It is enough to show that $M_j \subseteq L$. Let $\pi : M \to M_i$, $l + m_i \mapsto m_i$ for all $l \in L$ and $m_i \in M_i$. Assume that $\pi(M_j) \neq 0$. Then there exists a simple submodule S of M_j such that $\pi(S) \neq 0$. But then $\pi(S)$ is a simple submodule of M_i. So $S \simeq \pi(S)$ by Schur's Lemma (a). But $S \subseteq M_j$ and $\pi(S) \subseteq M_i$ so, by (a), $S \simeq S_j$ and $S \simeq S_i$. This contradicts the fact that S_i and S_j are not isomorphic.

(c) It is enough to show that, if $f \in \mathrm{End}_R(M)$, then $f(M_i) \subseteq M_i$. Let $\mathcal{M}_i$ denote the set of simple submodules of M_i. Then $f(M_i) = \sum_{S\in\mathcal{M}_i} f(S)$. But, if $S \in \mathcal{M}_i$, then $f(S)$ is equal to 0 or isomorphic to S_i, so $f(S) \subseteq M_i$.

(d) We have an isomorphism $S_i^{n_i} \simeq M_i$, so we only need to show that $\mathrm{End}_R(S_i^{n_i}) \simeq \mathrm{Mat}_{n_i}(D_i)$. But

$$\mathrm{End}_R(S_i^{n_i}) = \underset{1\leqslant a,b\leqslant n_i}{\oplus} \mathrm{Hom}_R(S_i, S_i) = \underset{1\leqslant a,b\leqslant n_i}{\oplus} D_i$$

and it is easy to see that the composition rule corresponds to the multiplication of matrices. ■

8.B. Semisimple rings.

Definition 8.8. *The ring R is called **left semisimple** if R is a semisimple left R-module. One can define similarly the notion of **right semisimple ring**.*

We shall see later that left semisimple rings are right semisimple and conversely.

Theorem 8.9. *Assume that $R \neq 0$. Then the following are equivalent:*

(1) *The ring R is left semisimple.*
(2) *Every left R-module is semisimple.*
(3) *$R = L_1 \oplus \cdots \oplus L_n$ where L_i are some minimal left ideals.*
(4) *R is left Artinian and $J(R) = 0$.*

PROOF - (1) $\Rightarrow$ (2): assume that R is left semisimple. Then $R = \sum_{a\in A} L_a$, where L_a is a simple left submodule of R (i.e. a minimal left ideal). If M is a left R-module, then $M = \sum_{a\in A}\sum_{m\in M} L_a m$. But $L_a m$ is a submodule of M which is a quotient of L_a, so it is simple or zero. This shows that M is semisimple.

(2) $\Rightarrow$ (3): Assume that all left R-modules are semisimple. Then we can write $R = \oplus_{i\in I} L_i$ where L_i are minimal left ideals of R. We must show that I is finite. Let us write $1 = \sum_{i\in I} l_i$ with $l_i \in L_i$. Let $J = \{i \in I \mid l_i \neq 0\}$. Then J is finite and we must show that $J = I$. But $R = R.1 \subseteq \sum_{i\in J} Rl_i \subseteq \sum_{i\in J} L_i$. So $I = J$, as desired.

(3) $\Rightarrow$ (4): assume that (3) holds. It follows that R is left Artinian (as a left R-module) by Corollary 4.5 and that $J(R) = J(R)R = 0$ by Remark 8.5 (2).

So it remains to show that (4) $\Rightarrow$ (1). Assume that (4) holds. Let $\mathcal{M}$ be the set of left ideals of R which are *finite* intersections of maximal left ideals. Since R is Artinian, there exists a minimal element I in $\mathcal{M}$. Now, let $\mathfrak{m}$ be a maximal left ideal of R. Then $I \cap \mathfrak{m} \in \mathcal{M}$ and $I \cap \mathfrak{m} \subseteq I$. Since I is a minimal element of $\mathcal{M}$, we have that $I \cap \mathfrak{m} = I$: in other words, $I \subset \mathfrak{m}$. So I is contained in all maximal left ideals of R, so $I = 0$ because $J(R) = 0$.

Now, write $0 = I = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, where $\mathfrak{m}_i \in \mathrm{Max}_l(R)$. Then the canonical map

$$R \longrightarrow R/\mathfrak{m}_1 \oplus \cdots \oplus R/\mathfrak{m}_n$$

is injective. Since $R/\mathfrak{m}_i$ is simple, we get that $R/\mathfrak{m}_1 \oplus \cdots \oplus R/\mathfrak{m}_n$ is semisimple, so R is a semisimple left R-module by Remark 8.5 (1). ■

Corollary 8.10. *Let R and S be two Morita equivalent rings. Then R is left semisimple if and only if S is left semisimple.*

PROOF - Indeed, by Theorem 8.9, the ring R is left semisimple if and only if all the left R-modules are semisimple. So the result follows from Lemma 8.2. ■

Corollary 8.11. *If $R/J(R)$ is left Artinian and M is a left R-module, then M is semisimple if and only if $J(R)M = 0$.*

PROOF - By Remark 8.5 (1), if M is semisimple, then $J(R)M = 0$. Conversely, assume that $R/J(R)$ is left Artinian and that $J(R)M = 0$. Then M can be viewed as a left $\bar{R}$-module, where $\bar{R} = R/J(R)$. Since $J(\bar{R}) = 0$ (see Exercise II.18), we get that M is a semisimple $\bar{R}$-module by Theorem 8.9. So M is a semisimple R-module by Remark 8.5 (4). ■

Corollary 8.12. *If $R/J(R)$ is left Artinian, then $R/J(R)$ is left semisimple. In particular, if R is left Artinian, then $R/J(R)$ is left semisimple.*

PROOF - This follows from Theorem 8.9 and from Exercise II.18. ■

EXAMPLE 8.13 - Let D be a division ring. Then the ring D is (left and right) semisimple. Therefore, by Theorem 7.6 and by Corollary 8.10, the ring $\mathrm{Mat}_n(D)$ is (left and right) semisimple. □

We are now ready to prove the following

Theorem 8.14 (Wedderburn). *The following are equivalent:*

(1) *R is a left semisimple ring.*
(2) *R is a right semisimple ring.*
(3) *There exists natural numbers $n_1,\dots, n_k$ and division rings $D_1,\dots, D_k$ such that $R \simeq \prod_{i=1}^k \mathrm{Mat}_{n_i}(D_i)$.*

PROOF - (1) $\Rightarrow$ (3): If $r \in R$, let $\rho_r : R \to R$, $s \mapsto sr$. Then $\rho_r \in \mathrm{End}_R(R)$ (where R is viewed as a left R-module). Moreover, the map $R^\circ \to \mathrm{End}_R(R)$, $r \mapsto \rho_r$ is a morphism of rings. It is clearly injective and surjective. So $R^\circ \simeq \mathrm{End}_R(R)$. If R is moreover assumed to be left semisimple, then it follows from Theorem 8.7 (c) and (d) and from Theorem 8.9 that $R^\circ \simeq \prod_{i=1}^k \mathrm{Mat}_{n_i}(D_i)$ for some natural numbers n_i's and some division rings D_i's. This shows (3) because $\mathrm{Mat}_{n_i}(D_i)^\circ \simeq \mathrm{Mat}_{n_i}(D_i^\circ)$ (by using the transpose map: see Exercise I.6).

(3) $\Rightarrow$ (1): assume that $R \simeq \prod_{i=1}^k \mathrm{Mat}_{n_i}(D_i)$. By Example 8.13 and by Theorem 8.9, the rings $\mathrm{Mat}_{n_i}(D_i)$ are Artinian and their radical is 0. Then it follows that R is Artinian (see Exercise II.13) and $J(R) = 0$ (see Exercise II.17). So R is left semisimple by Theorem 8.9.

Now, the fact that (2) $\Leftrightarrow$ (3) is proved similarly. ■

From now on, we will speak only about *semisimple* rings (and not about left or right semisimple rings).

8.C. Simple rings. We shall now come to the notion of simple rings. As for semisimple rings, we define the notion of *left simple* and *right simple* rings and we shall see later that these notions coincide.

Definition 8.15. *A ring R is called **left simple** if $R \neq 0$, R is left Artinian and 0 and R are the only two-sided ideals of R. One defines similarly the notion of right simple rings.*

Here is an example of a simple ring:

Theorem 8.16. *Let D be a division ring and let V be a **right** D-module with $\dim_D V = n$ and $A = \mathrm{End}_D(V)$. Note that $A \simeq \mathrm{Mat}_n(D)$. Then:*

(a) *A is a (left or right) simple ring.*
(b) *$J(A) = 0$.*
(c) *V is a simple left A-module.*
(d) *Up to isomorphism, V is the only simple left A-module.*
(e) *$\mathrm{End}_A(V) \simeq D^\circ$.*
(f) *If $U \subseteq V$ is a sub-D-vector space, let $\mathcal{L}_U = \{f \in A \mid U \subseteq \mathrm{Ker}\, f\}$ and $\mathcal{R}_U = \{f \in A \mid \mathrm{Im}\, f \subseteq U\}$. Then $\mathcal{L}_U$ (respectively $\mathcal{R}_U$) is a left ideal (respectively a right ideal) of A. Moreover, all left ideals (respectively right ideals) of A are of this form.*

PROOF - Homework. ■

It turns out that the rings studied in the previous theorems are the only simple rings:

Theorem 8.17. *The following are equivalent:*

(1) *R is left simple;*
(2) *R is right simple;*
(3) *There exists a division ring D and a natural number n such that $R \simeq \mathrm{Mat}_n(D)$;*
(4) *R is semisimple and has only one simple module.*

PROOF - We shall prove that (1) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4). The fact that (2) $\Leftrightarrow$ (3) is proved similarly.

• By Corollary 8.13 and by Theorem 8.16, we know that (3) $\Rightarrow$ (1) and that (3) $\Rightarrow$ (4).

• If R is left simple, then it is left Artinian and $J(R) = 0$, so it is semisimple by Theorem 8.9. So, by Wedderburn's Theorem, $R \simeq \mathrm{Mat}_n(D)$ for some division ring D and some natural number n (if there are at least to terms in a Wedderburn decomposition of R, then there are non-trivial two-sided ideals). So (1) $\Rightarrow$ (3).

• It remains to show that (4) $\Rightarrow$ (3). This follows from Wedderburn's Theorem: is there are at least to terms in a Wedderburn decomposition of R, there are at least to isomorphy classes of simple modules. ■

Theorem 8.17 (equivalence between (1) and (4)) gives a characterization of simple rings in terms of their category of modules (see also Theorem 8.9). Therefore:

Corollary 8.18. *Let R and S be two Morita equivalent rings. Then R is simple if and only if S is simple.*

The next result describes the simple modules of a semisimple ring, once we have a Wedderburn's decomposition. As a consequence, we obtain that a Wedderburn decomposition is essentially unique.

Proposition 8.19. *Let $n_1, \ldots, n_k$ be natural numbers and let $D_1, \ldots, D_k$ be division rings. Let $R = \prod_{i=1}^{k} \mathrm{Mat}_{n_i}(D_i)$. Then:*

(a) *R has exactly k isomorphy classes of simple left R-modules: they are the $S_i = D_i^{n_i}$, where $(A_1, \ldots, A_k) \in R$ acts on $\begin{pmatrix} d_1 \\ \vdots \\ d_{n_i} \end{pmatrix}$ by multiplication by A_i.*
(b) *$D_i \simeq \mathrm{End}_R(S_i)^\circ$.*
(c) *If $R = L_1 \oplus \cdots \oplus L_n$ where L_j are minimal left ideals, then $n = \sum_{i=1}^{k} n_i$ and, for all i, there are exactly n_i of the L_j's which are isomorphic to S_i.*
(d) *If $R \simeq \prod_{i=1}^{l} \mathrm{Mat}_{m_i}(E_i)$, then $k = l$ and there exists a permutation $\sigma \in \mathfrak{S}_k$ such that $m_i = n_{\sigma(i)}$ and $E_i \simeq D_{\sigma(i)}$.*

PROOF - The proof is left as an exercise. ■

8.D. Example: finite dimensional algebras. Let K be a field and let A be a finite dimensional K-algebra. Then A is left and right Artinian. Moreover, by Corollary 8.12, the K-algebra $A/J(A)$ is semisimple.

A left A-module M is also a K-vector space and the map $\rho_M : A \to \mathrm{End}_K(M)$, $a \mapsto (m \mapsto am)$ is a morphism of unitary K-algebras. Conversely, if V is a K-vector space and $\rho : A \to \mathrm{End}_K(V)$ is a morphism of unitary K-algebras, then V can be endowed with a structure of left A-module as follows: for all $a \in A$ and $v \in V$, we set $a.v = \rho(a)(v)$. In other words:

> *The datum of a left A-module is equivalent to the datum of a K-vector space V and a morphism of K-algebras $A \to \mathrm{End}_K(V)$.*

Now, if M is an A-module (and if $\rho_M : A \to \mathrm{End}_K(M)$ denotes the corresponding morphism of K-algebras), then $\mathrm{End}_A(M)$ is the set of endomorphism of the K-vector space M which commute with all elements of $\rho(A)$. In particular, $\mathrm{End}_A(M)$ is a K-algebra.

Now, since isomorphy classes of simple A-modules are in bijection with isomorphy classes of simple $A/J(A)$-modules, it follows from Wedderburn Theorem that there are only finitely many such isomorphy classes. Let $S_1,\dots, S_k$ denote a family of representatives of simple A-modules. Let $s_i = \dim_K S_i$, $D_i = \mathrm{End}_A(S_i)$, $d_i = \dim_K D_i$ and write $A/J(A) \simeq \overset{r}{\underset{i=1}{\oplus}} S_i^{n_i}$. Then:

Proposition 8.20. *With the above notation, we have:*

(a) *D_i is a division ring which is also a finite dimensional K-algebra.*
(b) $A/J(A) \simeq \prod_{i=1}^k \mathrm{Mat}_{n_i}(D_i)$.
(c) $\dim_K A/J(A) = \displaystyle\sum_{i=1}^k s_i n_i = \sum_{i=1}^k d_i n_i^2$.
(d) *If K is **algebraically closed**, then $D_i = K$ (so $d_i = 1$), $s_i = n_i$ and $A/J(A) \simeq \prod_{i=1}^k \mathrm{Mat}_{n_i}(K)$. Moreover, if S is a simple A-module, then $\rho_S : A \to \mathrm{End}_K(S)$ is surjective (Burnside).*

Proof - Clear (for (d), use Exercise II.27). ■

8.E. Example: group algebras. Let G be a finite group and let K be a field. Let p denote the characteristic of K. Then:

Theorem 8.21 (Maschke). *The group algebra $K[G]$ is semisimple if and only if p does not divide $|G|$.*

Proof - First, assume that p divides the order of G. Let $e = \sum_{g\in G} g$. Then $ge = e$ for every $g \in G$. Therefore, we have $K[G]e = Ke$. So Ke is a left ideal of $K[G]$. Moreover, $e^2 = \sum_{g\in G} ge = |G|e = 0$ because p divides $|G|$. So e is a nilpotent element of $K[G]$. Therefore, Ke is a nil left ideal of $K[G]$. In particular, $J(K[G]) \neq 0$ by Lemma 5.10, so $K[G]$ is not semisimple by Theorem 8.9.

Conversely, assume that p does not divide $|G|$. Let V be a $K[G]$-module and let W be a sub-$K[G]$-module of V. Then V is in particular a K-vector space and W is a K-vector

subspace. Let W' be a K-vector subspace of V such that $V = W \oplus W'$. Let $\pi_0 : V \to W$ be the projection on the first factor. Now, for $v \in V$, we set

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}v).$$

Recall that π is well-defined because $|G|$ is invertible in K. Then $\pi : V \to W$ is a K-linear map. Moreover, if $h \in G$ and $v \in V$, we have

$$\pi(hv) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}hv) = h\Big(\frac{1}{|G|} \sum_{g \in G} (h^{-1}g)\pi_0((h^{-1}g)^{-1}v)\Big) = h\pi(v).$$

Therefore, π is a morphism of $K[G]$-modules.

Now, let $i : W \hookrightarrow V$ denote the canonical injection. Then, for all $w \in W$, we have

$$\pi(i(w)) = \pi(w) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}w).$$

But, if $g \in G$, then $g^{-1}w \in W$ (because W is a $K[G]$-submodule) and so $\pi_0(g^{-1}w) = g^{-1}w$. So we get

$$\pi(i(w)) = w.$$

In other words, $\pi \circ i = \mathrm{Id}_W$, so $V = W \oplus \operatorname{Ker} \pi$. Since π is a morphism of $K[G]$-modules, $\operatorname{Ker} \pi$ is a sub-$K[G]$-module of V. This shows that V is semisimple. ■

Corollary 8.22 (Maschke, Wedderburn). *If p does not divide the order of G and if K is algebraically closed, then $K[G] \simeq \prod_{i=1}^{k} \mathrm{Mat}_{n_i}(K)$ for some natural numbers n_i. Moreover, k is the number of conjugacy classes of G.*

Proof - The first statement follows from Maschke's Theorem, and from Proposition 8.20 (d). Let us prove the second statement. Let $Z(R)$ denote the centre of the ring R, that is

$$Z(R) = \{r \in R \mid \forall\ x \in R,\ xr = rx\}.$$

Then it is clear that $Z(\mathrm{Mat}_n(K)) = KI_n$, where I_n is the identity matrix. So

$$(*) \qquad \dim_K Z\Big(\prod_{i=1}^{k} \mathrm{Mat}_{n_i}(K)\Big) = k.$$

On the other hand, let $\mathcal{C}(G)$ denote the set of conjugacy classes of G. If $C \in \mathcal{C}(G)$, let

$$\hat{C} = \sum_{g \in C} g.$$

It is readily seen that $(\hat{C})_{C \in \mathcal{C}(G)}$ is a K-basis of $Z(K[G])$. So

$$(**) \qquad \dim_K Z(K[G]) = |\mathcal{C}(G)|.$$

Now the last statement follows from the comparison of $(*)$ and $(**)$. ■

Exercises from Part II

Exercise II.1. Let $\imath : M \to M'$ and $\pi : M' \to M$ be two morphisms of R-modules such that $\pi \circ \imath = \mathrm{Id}_M$. Show that $\imath$ is injective, π is surjective and $M' = (\mathrm{Ker}\,\pi) \oplus (\mathrm{Im}\,\imath)$.

Exercise II.2. Let m, $n \in \mathbb{N}$. Compute $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Exercise II.3. Let M be a left R-module and let $e \in R$ be an *idempotent* (that is, $e^2 = e$). Show that the map $eR \otimes_R M \to eM$, $r \otimes_R m \mapsto rm$ is an isomorphism of $\mathbb{Z}$-modules (compare with Remark 3.18).

Exercise II.4. Assume that R is commutative. Let X and Y be two sets. Show that $R[X \times Y] \simeq R[X] \otimes_R R[Y]$ as R-modules.

Exercise II.5. Show that the map $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \times \mathbb{C}$, $z \otimes_{\mathbb{R}} z' \mapsto (zz', z\bar{z}')$ is an isomorphism of $\mathbb{C}$-algebras.

Exercice II.6 (Quaternions). Let $\mathbb{H}$ denote the $\mathbb{R}$-vector space consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{C})$ such that $d = \bar{a}$ and $b = -\bar{c}$ (here, $\bar{z}$ denotes the complex conjugate of $z \in \mathbb{C}$).

(a) Show that $\mathbb{H}$ is an $\mathbb{R}$-algebra.
(b) Show that $\mathbb{H}$ is a division ring (i.e. any non-zero element is a unit).
(c) Show that the map $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \to \mathrm{Mat}_2(\mathbb{C})$, $\lambda \otimes_{\mathbb{R}} M \mapsto \lambda M$ is an isomorphism of $\mathbb{C}$-algebras.

Exercise II.7. Assume that R is commutative. Let A, A', B and B' be four R-algebras.

(a) Let I and J be two left ideals of A and B respectively. Show that the image of the map $I \otimes_R J \to A \otimes_R B$, $a \otimes_R b \mapsto a \otimes_R b$ (!) is a left ideal of $A \otimes_R B$. Show that similar statements hold for right and two-sided ideals.
(b) If $f : A \to A'$ and $g : B \to B'$ are morphisms of R-algebras, show that $f \otimes_R g : A \otimes_R B \to A' \otimes_R B'$ is a morphism of R-algebras.

Exercise II.8. Let i denote a complex number such that $i^2 = -1$. Let

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

and

$$\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}.$$

If p is a prime number, we denote by $\mathbb{F}_p$ the field $\mathbb{Z}/p\mathbb{Z}$.

(a) Show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ and that $\mathbb{Q}[i]$ is a subfield of $\mathbb{C}$.
(b) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[i] \simeq \mathbb{Q}[i]$ (as $\mathbb{Q}$-algebras).
(c) Show that $\mathbb{F}_2 \otimes_{\mathbb{Z}} \mathbb{Z}[i] \simeq \mathbb{F}_2[X]/(X^2)$ (as $\mathbb{F}_2$-algebras).
(d) Show that $\mathbb{F}_3 \otimes_{\mathbb{Z}} \mathbb{Z}[i]$ is a field with 9 elements.
(e) Show that $\mathbb{F}_5 \otimes_{\mathbb{Z}} \mathbb{Z}[i] \simeq \mathbb{F}_5 \times \mathbb{F}_5$ (as $\mathbb{F}_5$-algebras).

(f) Let R be the set of $(\alpha, \beta) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ such that $\alpha - \beta \in 2\mathbb{Z}[i]$. Show that R is a sub-$\mathbb{Z}[i]$-algebra of $\mathbb{Z}[i] \times \mathbb{Z}[i]$ and that the map $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Z}[i] \to \mathbb{Z}[i] \times \mathbb{Z}[i]$, $\alpha \otimes_{\mathbb{Z}} \beta \mapsto (\alpha\beta, \alpha\bar{\beta})$ is an injective morphism of $\mathbb{Z}[i]$-algebras whose image is R (in other words, $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Z}[i] \simeq R$).

Exercise II.9. Assume that R is commutative. Let G and H be two groups. Show that $R[G \times H] \simeq R[G] \otimes_R R[H]$ as R-algebras.

Exercise II.10. Assume that R is commutative. Let M and N be two left R-modules. Assume that $(m_i)_{i \in I}$ (respectively $(n_j)_{j \in J}$) is a family of generators of M (respectively N). Show that $(m_i \otimes_R n_j)_{(i,j) \in I \times J}$ is a family of generators of the R-module $M \otimes_R N$.

Exercise II.11. Assume that R is commutative and Noetherian. Show that the tensor product of two Noetherian left R-modules is still Noetherian (Hint: use Exercise II.10).

Exercise II.12. Let M be an R-module and let L be a submodule. Assume that M/L and L are finitely generated. Show that M is finitely generated.

Exercise II.13. Let R_1 and R_2 be two rings and let M_1 and M_2 be left modules for R_1 and R_2 respectively. Show that $M_1 \times M_2$ is naturally endowed with a structure of $(R_1 \times R_2)$-module.

Show that $M_1 \times M_2$ is Noetherian (respectively Artinian) if and only if M_i is Noetherian (respectively Artinian) for all $i \in \{1, 2\}$.

Show that the ring $R_1 \times R_2$ is left Noetherian (respectively Artinian) if and only if the rings R_1 and R_2 are left Noetherian (respectively Artinian).

Show that $R_1 \times R_2$ is semisimple if and only if R_1 and R_2 are semisimple.

Exercise II.14. Let R be a Noetherian commutative ring and let S be a multiplicative subset of R. Show that $S^{-1}R$ is Noetherian.

Exercice II.15 (Fitting's Lemma). Let M be a Noetherian and Artinian left R-module and let $\sigma : M \to M$ be an endomorphism of M.

(a) Show that there exists $n_0 \in \mathbb{N}$ such that $\operatorname{Im} \sigma^{n_0} = \operatorname{Im} \sigma^{n_0+1}$ and $\operatorname{Ker} \sigma^{n_0} = \operatorname{Ker} \sigma^{n_0+1}$.
(b) Show that $\operatorname{Im} \sigma^n = \operatorname{Im} \sigma^{n+1}$ and $\operatorname{Ker} \sigma^n = \operatorname{Ker} \sigma^{n+1}$ for all $n \geqslant n_0$.
(c) Show that $M = (\operatorname{Im} \sigma^{n_0}) \oplus (\operatorname{Ker} \sigma^{n_0})$.

Exercise II.16. Let K be a field and let $\sigma : K[X, Y] \to K[X, Y]$, $P(X, Y) \mapsto P(-X, -Y)$. We denote by S the ring $K[X, Y]$ and we set

$$R = \{P \in S \mid \sigma(P) = P\}.$$

(a) Show that σ is an automorphism of the K-algebra S and that $\sigma \circ \sigma = \mathrm{Id}_S$.
(b) Show that R is a sub-K-algebra of S. Find a K-basis of R.
(c) Show that the K-algebra R is generated, as a K-algebra, by X^2, XY and Y^2.
(d) Let U, V and W be three other indeterminates. Let $\pi : K[U, V, W] \to S$, $P(U, V, W) \mapsto P(X^2, XY, Y^2)$. Show that the image of π is R.
(e) Show that the kernel of π is generated (as an ideal of $K[U, V, W]$) by $V^2 - UW$.

(f) Show that R is isomorphic to $K[U,V,W]/(V^2-UW)$.
(g*) Show that $S = RX + RY$ but that S is not a free R-module.

Exercise II.17. Let R_1 and R_2 be two rings and let $\mathfrak{m}$ be a maximal left ideal of $R_1 \times R_2$. Show that $\mathfrak{m} = R_1 \times \mathfrak{m}_2$ for some $\mathfrak{m}_2 \in \mathrm{Max}_l(R_2)$ or that $\mathfrak{m} = \mathfrak{m}_1 \times R_2$ for some $\mathfrak{m}_2 \in \mathrm{Max}_l(R_2)$.

Deduce that $J(R_1 \times R_2) = J(R_1) \times J(R_2)$.

Exercise II.18. Let I be a two-sided ideal of R contained in $J(R)$. Show that $J(R/I) = J(R)/I$.

Exercise II.19. Let R be a ring and let n be a natural number. We propose to prove in several steps that $J(\mathrm{Mat}_n(R)) = \mathrm{Mat}_n(J(R))$ (by $\mathrm{Mat}_n(J(R))$, we mean the set of $n \times n$ matrices with coefficients in $J(R)$: it is not a unitary ring).

Let $E_{ij} \in \mathrm{Mat}_n(R)$ denote the matrix whose entries are all zero except the (i,j)-entry which is equal to 1. We denote by $\mathbf{1}_n$ the identity matrix. Let $I = \mathrm{Mat}_n(J(R))$ and $J = J(\mathrm{Mat}_n(R))$. For $j \in \{1,2,\ldots,n\}$, we set $I_j = \oplus_{i=1}^n J(R)E_{ij}$. We shall first prove that $I \subseteq J$.

(a) Show that I is a two-sided ideal of $\mathrm{Mat}_n(R)$.
(b) Show that I_j is a left ideal of $\mathrm{Mat}_n(R)$ and that $I = \oplus_{j=1}^n I_j$.
(c) Assume here, ond only in this question, that R is *commutative*, so that $\det : \mathrm{Mat}_n(R) \to R$ is well-defined. Show that $\det(\mathbf{1}_n - a) \in 1 + J(R)$ for any $a \in I$. Deduce that $I \subseteq J$ in this case.
(d) Let $a \in I_j$. Write $a = \sum_{i=1}^n \alpha_i E_{ij}$, with $\alpha_i \in J(R)$. Since $1-\alpha_j$ is invertible, we can define $\beta_i = \alpha_i(1-\alpha_j)^{-1}$. Let $b = -\sum_{i=1}^n \beta_i E_{ij}$. Show that $(\mathbf{1}_n - b)(\mathbf{1}_n - a) = \mathbf{1}_n$.
(e) Deduce from (b) and (d) that $I_j \subseteq J$ and $I \subseteq J$.

We shall now prove that $J \subseteq I$. Let $a \in J$ and write $a = \displaystyle\sum_{1 \leqslant i,j \leqslant n} \alpha_{ij} E_{ij}$. We want to prove that $\alpha_{ij} \in J(R)$ for all (i,j). So fix i and j in $\{1,2,\ldots,n\}$.

(f) Let $b = E_{ii} a E_{ji}$. Show that $b = \alpha_{ij} E_{ii}$.
(g) Show that $\mathbf{1}_n - rb$ is invertible for any $r \in R$.
(h) Deduce that $1 - r\alpha_{ij}$ is invertible for any $r \in R$. Conclude.

Exercise II.20. Let G be a finite group and let $\theta : G \to \mathbb{C}^\times$ be a morphism of groups. Let

$$e_\theta = \frac{1}{|G|} \sum_{g \in G} \theta(g)^{-1} g \quad \in \mathbb{C}[G].$$

Show that e_θ is an idempotent of $\mathbb{C}[G]$ and that $e_\theta \mathbb{C}[G] e_\theta \simeq \mathbb{C}$.

Exercise II.21. Let R be a commutative integral domain. Let I and J be two non-zero ideals of R such that the ideal IJ is principal. We shall prove that I (and J) are projective modules. For this, let $r \in R$ be such that $IJ = Rr$ and write $r = \sum_{i=1}^n x_i y_i$ with $x_i \in I$ and $y_i \in J$. Let

$$\begin{array}{rccc} \varphi : & I & \longrightarrow & (Rr)^n \\ & x & \longmapsto & (xy_1, \ldots, xy_n) \end{array}$$

and

$$\begin{array}{rccc} \psi : & (Rr)^n & \longrightarrow & I \\ & (r_1, \ldots, r_n) & \longmapsto & \sum_{i=1}^n (r_i x_i)/r. \end{array}$$

(a) Show that φ and ψ are well-defined morphisms of R-modules.
(b) Show that the image of φ is contained in $(Rr)^n$.
(c) Show that $\psi \circ \varphi = \mathrm{Id}_I$.
(d) Show that φ is injective and that $(Rr)^n = \varphi(I) \oplus \operatorname{Ker} \psi$.
(e) Deduce that I is a projective R-module.

Exercise II.22. Let $R = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

(a) Show that R is a subring of $\mathbb{C}$.

Let $\mathfrak{p}$ (respectively $\mathfrak{p}'$) be the ideal of R generated by 3 and $1 + i\sqrt{5}$ (respectively 3 and $1 - i\sqrt{5}$).

(b) Show that $\mathfrak{p}\mathfrak{p}' = 3R$.
(c) Show that $\mathfrak{p}$ and $\mathfrak{p}'$ are not principal ideal.
(d) Show that $\mathfrak{p}$ and $\mathfrak{p}'$ are projective R-modules (Hint: use Exercise II.21) but are not free (use (b)).

Exercise II.23. Prove that the following are equivalent:

(a) Every left R-module is projective.
(b) Every left R-module is injective.

Exercise II.24. Let M and N be two flat left R-modules and assume that R is *commutative*. Show that the left R-module $M \otimes_R N$ is flat.

Exercise II.25. Let G be a ***finite p-group*** and let $R = \mathbb{F}_p[G]$ be the group algebra of G over $\mathbb{F}_p$. The aim of this exercise is to prove that R is a local ring. We first recall the following result from group theory: if X is a G-set (i.e. a set endowed with an action of G) and if we denote by $X^G = \{x \in x \mid \forall\ g \in G,\ g.x = x\}$, then

$$(*) \qquad |X| \equiv |X^G| \mod p.$$

We now need some more notation. Let

$$\begin{array}{rccc} \sigma : & R & \longrightarrow & \mathbb{F}_p \\ & \sum_{g \in G} a_g g & \longmapsto & \sum_{g \in G} a_g \end{array}$$

and

$$\mathfrak{m} = \operatorname{Ker} \sigma.$$

(a) Show that σ is a morphism of $\mathbb{F}_p$-algebras.
(b) Show that $\mathfrak{m}$ is a two-sided ideal and is a maximal left ideal of R.

Let S be a simple R-module. We also view S as a G-set (because $G \subseteq R^\times$ acts on S). Let $x \in S$, $x \neq 0$.

(c) Show that S is an $\mathbb{F}_p$-vector space.
(d) Show that the map $\pi : R \to S$, $r \mapsto rx$ is a surjective morphism of R-modules (and of $\mathbb{F}_p$-vector spaces). Deduce that S is finite dimensional.

(e) Show that S^G is an R-submodule of S.
(f) Show that $S^G \neq 0$ (use $(*)$). Deduce that $S = S^G$.
(g) Show that $\mathfrak{m} = \operatorname{Ker} \pi$.
(h) Show that $J(R) = \mathfrak{m}$ and that R is a local ring.

Exercise II.26. Let R be a commutative ring such that all finitely generated projective modules are free. Let $\sigma : \mathrm{Mat}_n(R) \to \mathrm{Mat}_n(R)$ be an anti-automorphism of the R-algebra $\mathrm{Mat}_n(R)$ (i.e. σ is an isomorphism of R-modules satisfying $\sigma(xy) = \sigma(y)\sigma(x)$ for all x, $y \in \mathrm{Mat}_n(R)$). Show that there exists $g \in \mathrm{Mat}_n(R)^\times$ such that $\sigma(x) = g^t x g^{-1}$ for all $x \in \mathrm{Mat}_n(R)$ (here, ${}^t x$ denotes the transposed of x).

Exercise II.27. Let K be an algebraically closed field and let D be a finite dimensional K-algebra. Assume that D is a division ring. Show $D \simeq K$ as a K-algebra.

Exercice II.28* (Burnside). Let K be a field, let V be a finite dimensional vector space and let A be a sub-K-algebra of $\mathrm{End}_K(V)$. We assume that, viewed as an A-module, V is simple. Show that $A = \mathrm{End}_K(V)$.

Exercice II.29* (Kolchin?). Let K be a field and let G be a subgroup of $\mathbf{GL}_n(K)$ such that all elements of G are unipotent (i.e. have $(X-1)^n$ as characteristic polynomial). Show that there exists $g \in \mathbf{GL}_n(K)$ such that gGg^{-1} is contained in the group $\mathbf{U}_n(K)$ of unipotent upper triangular matrices.

Part III. Dedekind domains

All along this part, we fix a ***commutative*** *ring R. Unless otherwise specified, rings will be* ***commutative.*** The proofs of the theorems/propositions/lemmas/corollaries are not written: they have been given in class (except for the Theorems 10.11 and 10.12 which have been stated without proof).

9. Integral elements, integral extensions

Notation - If L is a field which is a finite extension of the field K and if $\alpha \in L$, we denote by $\chi_{L/K}(\alpha) \in K[X]$ the characteristic polynomial of the K-linear map $L \to L$, $x \mapsto \alpha x$. The minimal polynomial of α over K is denoted by $\min_K(\alpha)$. The trace (respectively the determinant) of this map will be denoted by $\mathrm{Tr}_{L/K}(\alpha)$ (respectively $N_{L/K}(\alpha)$) and will be called the *trace* of α (respectively the *norm* of α) relative to the extension L/K. If L/K is Galois with group $G = \mathrm{Gal}(L/K)$, then

$$\chi_{L/K}(\alpha) = \prod_{\sigma \in G} (X - {}^{\sigma}x). \tag{9.1}$$

Consequently,

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) \tag{9.2}$$

and

$$N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha). \tag{9.3}$$

9.A. Definitions. Let S be a commutative R-algebra: in other words, we are given a morphism of rings $R \to S$ with S commutative (for instance, R can be a subring of S and the morphism $R \to S$ is the canonical injection).

Definition 9.4. *An element $s \in S$ is said* ***integral over*** *R if there exists a* ***monic*** *polynomial $P(X) \in R[X]$ such that $P(s) = 0$.*

The ring S is called an ***integral extension of*** *R (or S is said to be* ***integral over*** *R) if every $s \in S$ is integral over R.*

The ***integral closure*** *of R in S is the set of elements $s \in S$ which are integral over R.*

Examples 9.5 - (0) If $\sigma : S \to S'$ is a morphism of rings (and view S' as an R-algebra through the composition $R \longrightarrow S \xrightarrow{\sigma} S'$) and if $s \in S$ is integral over R, then $\sigma(s)$ is integral over R.

(1) If R and S are fields, then an element $s \in S$ is integral over R if and only if it is algebraic over R.

(2) An element $x \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if it belongs to $\mathbb{Z}$. Also, $\sqrt[3]{2}$, $e^{2i\pi/n}$ and $i = \sqrt{-1}$ are integral over $\mathbb{Z}$.

(3) If S is a ring on which a *finite* group G acts and if $R = S^G = \{r \in S \mid \forall\ \sigma \in G,\ \sigma(r) = r\}$, then S is integral over R.

(4) If I is an ideal of S and if I' denotes the inverse image of I in R (for instance $I' = I \cap R$ if $R \subset S$), then S/I is an R/I'-algebra. Moreover, if S is integral over R, then S/I is integral over R/I'. □

REMARK 9.6 - Let R' be the subring $R.1_S$ of S. Then an element $s \in S$ is integral over R if and only if it is integral over R'. In particular, the integral closure of R in S is the integral closure of R' in S. □

Definition 9.7. *If $R \subset S$, we say that R is **integrally closed** in S if it is equal to its integral closure. If R is an integral domain, the integral closure of R in its field of fractions is called the **normalization of** R. An integral domain is called **integrally closed** (or **normal**) if it is integrally closed in its field of fractions.*

EXAMPLES 9.8 - (1) By Example 9.5 (2), $\mathbb{Z}$ is integrally closed.

(2) More generally, a unique factorization domain is integrally closed.

(3) If K is a field, then $K[X^2, X^3]$ (which is a subring of $K[X]$) is an integral domain which is not integrally closed. □

9.B. First properties. If $s \in S$, we denote by $R[s]$ the subring of S equal to

$$R[s] = \{P(s) \mid P(X) \in R[X]\}.$$

It is a sub-R-algebra of S. The following proposition characterizes integral elements:

Proposition 9.9. *Let $s \in S$. Then the following are equivalent:*

(1) *s is integral over R.*
(2) *The subring $R[s]$ of S is a finitely generated R-module.*
(3) *There exists a commutative ring T containing $R[s]$ which is a finitely generated R-module.*

Corollary 9.10. *If s and t are elements of S which are integral over R, then $s + t$, $s - t$ and st are integral over R. In particular, the integral closure of R in S is a subring of S.*

Corollary 9.11. *Let T be a commutative S-algebra (so in particular it is an R-algebra). If S is integral over R and T is integral over S, then T is integral over R.*

Corollary 9.12. *Assume that S is integral over R. Then S is a finitely generated R-algebra if and only if it is a finitely generated R-module.*

Corollary 9.13. *If S is a finitely generated R-module, then S is integral over R.*

EXAMPLE 9.14 - Let G be a finite group and let $\mathcal{C}(G)$ denotes the set of conjugacy classes in G. If $C \in \mathcal{C}(G)$, let

$$\hat{C} = \sum_{g \in C} g \in R[G].$$

Then, as in the proof of Corollary 8.22, $(\hat{C})_{C\in\mathcal{C}(G)}$ is an R-basis of the centre of $R[G]$ (which we denote by $Z(R[G])$. Consequently, $Z(R[G])$ is a commutative R-algebra which is a finitely generated R-module. So $Z(R[G])$ is integral over R. □

9.C. Integral/algebraic. In this subsection, we fix an integral domain R with field of fractions K. We also fix a finite extension L of K of degree n and we denote by S the integral closure of R in L. We set $\overline{R} = S \cap K$. Then $\overline{R}$ is the normalization of R.

Proposition 9.15. *Let $x \in L$. The following are equivalent:*

(a) *x is integral over R.*
(b) *x is integral over $\overline{R}$.*
(c) *$\chi_{L/K}(x) \in \overline{R}[X]$.*
(d) *$\min_K(x) \in \overline{R}[X]$.*

Corollary 9.16. *Let $x \in S$. Then $\mathrm{Tr}_{L/K}(x) \in \overline{R}$ and $N_{L/K}(x) \in \overline{R}$.*

Theorem 9.17. *Assume that R is integrally closed and that L/K is a separable extension. Then:*

(a) *If R is Noetherian, then S is an R-module of finite type. In particular, S is Noetherian.*
(b) *If R is principal, then S is a free R-module of rank $n = [L : K]$. Moreover, any R-basis of S is a K-basis of L.*

Corollary 9.18. *Let $x \in S$. Then $x \in S^\times$ if and only if $N_{L/K}(x) \in \overline{R}^\times$.*

9.D. Integral extensions and prime ideals. If $\sigma : R \to S$ is a morphism of rings and if $\mathfrak{q}$ is a prime ideal of S, then $\sigma^{-1}(\mathfrak{q})$ is a prime ideal of R. We denote by $\mathrm{Spec}(R)$ the set of prime ideals of R and by $\sigma^{-1} : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$, $\mathfrak{q} \mapsto \sigma^{-1}(\mathfrak{q})$.

Proposition 9.19. *Assume that $R \subset S$ and that S is integral over R.*

(a) *If $r \in R$, then $r \in R^\times$ if and only if $r \in S^\times$.*
(b) *Assume that S is an integral domain. Then S is a field if and only if R is a field.*

The next corollary gives further results about the map $\sigma^{-1} : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ in the case of integral extensions:

Corollary 9.20. *Assume that S is integral over R (and denote by $\sigma : R \to S$, $r \mapsto r1_S$).*

(a) *Let $\mathfrak{q}$ be a prime ideal of S. Then $\mathfrak{q}$ is a maximal ideal of S if and only if $\sigma^{-1}(\mathfrak{q})$ is maximal in R.*
(b) *Let $\mathfrak{p}$ be a prime ideal of R. Then there exists a prime ideal $\mathfrak{q}$ of S such that $\mathfrak{p} = \sigma^{-1}(\mathfrak{q})$. In other words, the map $\sigma^{-1} : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective.*

Theorem 9.21 (Going-up Theorem). *Assume that S is integral over R. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals in R, let $m < n$ and suppose there is a chain $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m$ of prime ideals of S such that $\sigma^{-1}(\mathfrak{q}_i) = \mathfrak{p}_i$ for $1 \leqslant i \leqslant m$. Then there exists a chain $\mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$ of prime ideals of S such that $\mathfrak{q}_m \subseteq \mathfrak{q}_{m+1}$ and $\sigma^{-1}(\mathfrak{q}_i) = \mathfrak{p}_i$ for $m + 1 \leqslant i \leqslant n$.*

Theorem 9.22 (Going-down Theorem). *Assume that $R \subset S$ and that R is integrally closed in S. Let $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a chain of prime ideals in R, let $m < n$ and suppose there is a chain $\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m$ of prime ideals of S such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leqslant i \leqslant m$. Then there exists a chain $\mathfrak{q}_{m+1} \supseteq \cdots \supseteq \mathfrak{q}_n$ of prime ideals of S such that $\mathfrak{q}_m \supseteq \mathfrak{q}_{m+1}$ and $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $m+1 \leqslant i \leqslant n$.*

9.E. Agebraic integers. Let K be a field of characteristic 0. An element $x \in K$ is called an *algebraic integer* if it is integral over $\mathbb{Z}$. We denote by $\mathcal{O}_K$ the ring of algebraic integers of K.

Theorem 9.23. *Let K be a finite extension of $\mathbb{Q}$ of degree n. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. Moreover, any $\mathbb{Z}$-basis of $\mathcal{O}_K$ is a $\mathbb{Q}$-basis of K.*

Examples 9.24 - (1) $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

(2) If $n \geqslant 1$ and if $\zeta_n \in \mathbb{C}^\times$ is a primitive n-th root of unity, then $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. □

Let K be a finite extension of $\mathbb{Q}$ of degree n. First, note that the symmetric bilinear form $K \times K \to \mathbb{Q}$, $(\alpha, \beta) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta)$ is non-degenerate. Let $(\alpha_1, \ldots, \alpha_n)$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. We then set

$$\Delta(K) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{1 \leqslant i,j \leqslant n}.$$

The number $\Delta(K)$ is called the discriminant of K (it does not depend on the choice of the $\mathbb{Z}$-basis of $\mathcal{O}_K$).

10. Dedekind domains

10.A. Definition.

Definition 10.1. *The ring R is called a **Dedekind domain** if it satisfies the following three conditions:*

(D1) *R is Noetherian;*
(D2) *R is an integral and integrally closed domain;*
(D3) *Every non-zero prime ideal is maximal.*

Examples 10.2 - (1) A field and, more generally, a principal ideal domain are Dedekind domains.

(2) If K is a field, then $K[X, Y]$ is Noetherian, integral, integrally closed and even a unique factorization domain but is not a Dedekind domain. □

Theorem 10.3 (Dedekind). *Let R be a Dedekind domain and let K denote its field of fractions. Let L be a finite separable extension of K and let S be the integral closure of R in L. Then S is a Dedekind domain and is a finitely generated R-module.*

Corollary 10.4. *If K is a finite extension of $\mathbb{Q}$, then $\mathcal{O}_K$ is a Dedekind domain.*

10.B. Fractional ideals. *From now on, R will denote an integral domain and K will denote its field of fractions.*

Definition 10.5. *A **fractional ideal** of R is an R-submodule I of K such that $dI \subset R$ for some $d \in R \setminus \{0\}$.*

EXAMPLE 10.6 - If I and J are fractional ideals of R, then $I+J$ and IJ are also fractional ideals of R. □

Definition 10.7. *A fractional ideal I of R is called **invertible** if there exists a fractional ideal J of R such that $IJ = R$.*

REMARK 10.8 - If I and J are two fractional ideals of R such that $IJ = R$, then $J = \{x \in K \mid xI \subset R\}$. □

EXAMPLE 10.9 - Let $R = \mathbb{Z}[i\sqrt{5}]$ and let $\mathfrak{p} = (3, 1 + i\sqrt{5})$ and $\mathfrak{p}' = (3, 1 - i\sqrt{5})$. Then $\mathfrak{p}.(\mathfrak{p}'/3) = R$ by Exercise II.22 (a). So $\mathfrak{p}$ and $\mathfrak{p}'$ are invertible. □

Proposition 10.10. *If I is an invertible fractional ideal of R, then R is a finitely generated projective R-module.*

Theorem 10.11. *The following are equivalent:*

(1) *R is a Dedekind domain.*
(2) *For each $\mathfrak{p} \in \mathrm{Spec}(R)$, $R_{\mathfrak{p}}$ is principal.*
(3) *Every non-zero fractional ideal of R is invertible.*
(4) *Every non-zero fractional ideal is a projective R-module.*
(5) *Every non-zero proper ideal I of R is a (finite) product of prime ideals.*

Moreover, if these conditions are satisfied and if $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are prime ideals such that $\mathfrak{p}_1 \ldots \mathfrak{p}_r = \mathfrak{q}_1 \ldots \mathfrak{q}_s$, then $r = s$ and there exists a permutation $\sigma \in \mathfrak{S}_r$ such that $\mathfrak{q}_{\sigma(i)} = \mathfrak{p}_i$ for all i.

Let R be a Dedekind domain and let K be its field of fractions. Let L be a finite algebraic extension of K of degree n. Let S be the integral closure of R in L. Let $\mathfrak{p}$ be a prime number. Write

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_r^{e_r}$$

where $\mathfrak{q}_i$ are distinct prime ideals of S. Then:

Theorem 10.12. *With the above notation, we have:*

(a) *$\mathfrak{q}_i \cap R = \mathfrak{p}$.*
(b) *If $\mathfrak{q}$ is a prime ideal of S containing p, then $\mathfrak{q} \in \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$.*
(c) *Let f_i be the natural number such that $\mathcal{O}_K/\mathfrak{q}_i$ is a finite extension of $R/\mathfrak{p}$ of degree f_i. Then $\sum_{i=1}^{r} e_i f_i = n$.*

Exercises from Part III

Exercise III.1. Let $D \in \mathbb{Z}$ be square-free (i.e., if $n \in \mathbb{Z}$ is such that n^2 divides D, then $n = \pm 1$). Compute the rings of algebraic integers of $\mathbb{Q}(\sqrt{D})$.

Exercice III.2 (Gauss). Let R be a unique factorization domain and let K be its field of fractions. If $P(X) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$, we define

$$\mathcal{C}(P) = \mathrm{lcm}(a_0, a_1, \ldots, a_n).$$

(a) Show that $\mathcal{C}(PQ) = \mathcal{C}(P)\mathcal{C}(Q)$ (first, reduce to the case where $\mathcal{C}(P) = \mathcal{C}(Q) = 1$).
(b) Assume that $a_n = 1$. Show that P is irreducible in $R[X]$ if and only if P is irreducible in $K[X]$.

Exercice III.3 (Eisenstein's criterion). Let R be a principal ideal domain and let K be its field of fractions. Let $p \in R$ be irreducible. Let $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$. Assume that $p | a_i$ for all i and that p^2 does not divide a_0. Show that P is irreducible in $K[X]$ (Hint: use Exercise III.2 and reduce modulo p).

Exercise III.4. Let $n \geqslant 1$ and let ζ_n be a primitive n-th root of unity in $\mathbb{C}$, that is, a generator of the cyclic group $\boldsymbol{\mu}_n(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1\}$ (for instance, $\zeta_n = e^{2i\pi/n}$). Let $\Phi_n(X)$ denote the n-th cyclotomic polynomial

$$\Phi_n(X) = \prod_{\substack{1 \leqslant j \leqslant n \\ \gcd(n,j)=1}} (X - \zeta_n^j).$$

Let $\varphi(n)$ denote the degree of $\Phi_n(X)$ (i.e. the Euler φ-function).

(a) Compute Φ_n for $1 \leqslant n \leqslant 6$.
(b) Show that $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
(c) Deduce by induction that $\Phi_n(X)$ belongs to $\mathbb{Z}[X]$ and is monic.
(d) Let p be a prime number. Compute Φ_p and show that Φ_p is irreducible (Hint: compute $\Phi_p(X+1)$ and use Eisenstein's criterion of Exercise III.3).

The aim of the next questions is to show that Φ_n is irreducible for all n. Write $\Phi_n(X) = P(X)Q(X)$ where $P(X)$, $Q(X) \in \mathbb{Z}[X]$ are monic and P is irreducible in $\mathbb{Q}[X]$. Let ζ be a root of P and let p be any prime number not dividing n. We denote by $\overline{P}(X) \in \mathbb{F}_p[X]$ the reduction modulo p of $P(X) \in \mathbb{Z}[X]$. Since ζ^p is a root of Φ_n, we must have $P(\zeta^p) = 0$ or $Q(\zeta^p) = 0$.

(e) Assume that $Q(\zeta^p) = 0$. Show that $P(X)$ divides $Q(X^p)$.
(f) Show that $\overline{Q}(X^p) = \overline{Q}(X)^p$.
(g) Assume that $Q(\zeta^p) = 0$ and let $f \in \mathbb{F}_p[X]$ be any irreducible factor of $\overline{P}$.
  (g1) Deduce from (e) and (f) that f also divides $\overline{Q}$.
  (g2) Deduce that f^2 divides $X^n - 1$ and that f divides nX^{n-1} (Hint: take the derivative) so that f divides also X^{n-1}. Show that it is impossible.

(h) Deduce from (g) that $P(\zeta^p) = 0$ for all prime number p which does not divide n. Deduce that $P = \Phi_n$, and that Φ_n is irreducible.

The fact that Φ_n is irreducible shows that the field $\mathbb{Q}(\zeta_n)$ is isomorphic to $\mathbb{Q}[X]/(\Phi_n)$ and that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Let $\mathcal{O}_n$ denote the ring of integers of $\mathbb{Q}(\zeta_n)$. Then it is clear that $\mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_n$. It can be proved that $\mathcal{O}_n = \mathbb{Z}[\zeta_n]$. The aim of the next questions is to prove this result whenever n is a prime number (note that the case $n = 2$ is trivial). So let p be an odd prime number.

(i) Show that $\det(\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_p^i\zeta_p^j)) = \pm p^{p-2}$.
(j) Deduce that, if $\alpha \in \mathcal{O}_p$, then there exists $r \in \mathbb{Z}_{\geqslant 0}$ such that $p^r\alpha \in \mathbb{Z}[\zeta_p]$.
(k) Show that, if $1 \leqslant i \leqslant p-1$, then $(1-\zeta_p^i)/(1-\zeta_p) \in \mathcal{O}_p^\times$.
(l) Show that $\prod_{i=1}^{p-1}(1-\zeta_p^i) = \Phi_p(1) = p$ (Hint: use (d)).
(m) Let $\mathfrak{p} = (1-\zeta_p)\mathbb{Z}[\zeta_p]$ and $\mathfrak{q} = (1-\zeta_p)\mathcal{O}_p$. Deduce from (k) and (l) that $\mathfrak{p}^{p-1} = p\mathbb{Z}[\zeta_p]$ and $\mathfrak{q}^{p-1} = p\mathcal{O}_p$.
(n) Show that $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\zeta_p]$ and that $\mathbb{Z}[\zeta_p]/\mathfrak{p} \simeq \mathbb{F}_p$.
(n) Deduce from (m) that $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_p$ and that $\mathcal{O}_p/\mathfrak{q} \simeq \mathbb{F}_p$ (use Theorem 10.12 (c)).
(o) Deduce from (m) and (n) that $\mathfrak{p} = \mathfrak{q} \cap \mathbb{Z}[\zeta_p]$.
(p) Deduce that $\mathfrak{p}^i = \mathfrak{q}^i \cap \mathbb{Z}[\zeta_p]$ for all $i \geqslant 1$.
(q) Deduce from (j) that $\mathcal{O}_p = \mathbb{Z}[\zeta_p]$.

Exercise III.5. Let $n \geqslant 1$ and let ζ_n be primitive n-th root of unity. Let $K_n = \mathbb{Q}(\zeta_n)$. If $k \in \mathbb{Z}/n\mathbb{Z}$, we still denote by ζ_n^k the number $\zeta_n^{\dot{k}}$ where $\dot{k}$ is a representative of k in $\mathbb{Z}$.

(a) Show that K_n is a Galois extension of $\mathbb{Q}$.
(b) Let $\Gamma_n = \mathrm{Gal}(K_n/\mathbb{Q})$. Let $\sigma \in \Gamma_n$. Show that there exists a unique $k(\sigma) \in \mathbb{Z}/n\mathbb{Z}$ such that $\sigma(\zeta_n) = \zeta_n^{k(\sigma)}$. Show that $k(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$.
(c) Show that the map $\Gamma_n \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\sigma \mapsto k(\sigma)$ is an isomorphism of groups (Hint: use the irreducibility of the n-th cyclotomic polynomial: see Exercise III.4 (h)).
(d) Let $\xi_1, \ldots, \xi_r$ denote roots of unity in $\mathbb{C}$ and assume that $(\xi_1 + \cdots + \xi_r)/r$ is an algebraic integer. Show that $\xi_1 + \cdots + \xi_r = 0$ or that $\xi_1 = \xi_2 = \cdots = \xi_r$ (Hint: compute the norm using 9.3).

Part IV. Algebraic geometry

All along this part, we fix a field K of characteristic $p \geqslant 0$. If R is a ring and if E is a subset of R, we denote by $\langle E \rangle$ (or $\langle E \rangle_R$ if necessary) the ideal of R generated by E.

REMARK - Most of the *geometric* theorems of algebraic geometry are based on *algebraic* theorems about rings. We have gathered in the Appendix the results we need. The section 15 and this Appendix have not been treated in class. □

11. The maps $\mathcal{Z}$ and $\mathcal{I}$

11.A. Definitions and first properties. We denote by $\mathbf{A}^n(K)$ the affine space K^n. Let E be a subset of $K[X_1, \ldots, X_n]$. We set

$$\mathcal{Z}(E) = \{(x_1, \ldots, x_n) \in \mathbf{A}^n(K) \mid \forall f \in E,\ f(x_1, \ldots, x_n) = 0\}.$$

Let X be subset of $\mathbf{A}^n(K)$. We set

$$\mathcal{I}(X) = \{f \in K[X_1, \ldots, X_n] \mid \forall x \in X,\ f(x) = 0\}.$$

Proposition 11.1. *With the above notation, we have:*

(a) *If $E \subseteq F \subseteq K[X_1, \ldots, X_n]$, then $\mathcal{Z}(F) \subseteq \mathcal{Z}(E)$.*
(b) *$\mathcal{Z}(E) = \mathcal{Z}(\langle E \rangle)$*
(c) *If $(E_\lambda)_{\lambda \in \Lambda}$ is a family of subsets of $K[X_1, \ldots, X_n]$, then $\bigcap_{\lambda \in \Lambda} \mathcal{Z}(E_\lambda) = \mathcal{Z}(\bigcup_{\lambda \in \Lambda} E_\lambda)$.*
(d) *If E and F are two subsets of $K[X_1, \ldots, X_n]$, then $\mathcal{Z}(E) \cup \mathcal{Z}(F) = \mathcal{Z}(E * F)$, where $E * F = \{ab \mid a \in E \text{ and } b \in F\}$.*
(e) *$\mathcal{Z}(\varnothing) = \mathbf{A}^n(K)$ and $\mathcal{Z}(1) = \varnothing$.*

PROOF - Easy. ■

Corollary 11.2. *Let $(I_\lambda)_{\lambda \in \Lambda}$ be a family of ideals of $K[X_1, \ldots, X_n]$. Then:*

(a) $\bigcap_{\lambda \in \Lambda} \mathcal{Z}(I_\lambda) = \mathcal{Z}(\sum_{\lambda \in \Lambda} I_\lambda)$.
(b) *If Λ is finite, then* $\bigcup_{\lambda \in \Lambda} \mathcal{Z}(I_\lambda) = \mathcal{Z}(\prod_{\lambda \in \Lambda} I_\lambda)$.

PROOF - Easy. ■

Proposition 11.3. *With the above notation, we have:*

(a) *If $X \subseteq Y \subseteq \mathbf{A}^n(K)$, then $\mathcal{I}(Y) \subseteq \mathcal{I}(X)$.*
(b) *If $(X_\lambda)_{\lambda \in \Lambda}$ is a family of subsets of $\mathbf{A}^n(K)$, then $\sum_{\lambda \in \Lambda} \mathcal{I}(X_\lambda) \subseteq \mathcal{I}\big(\bigcap_{\lambda \in \Lambda} X_\lambda\big)$.*
(c) *If $(X_\lambda)_{\lambda \in \Lambda}$ is a family of subsets of $\mathbf{A}^n(K)$, then $\mathcal{I}\big(\bigcup_{\lambda \in \Lambda} X_\lambda\big) = \bigcap_{\lambda \in \Lambda} \mathcal{I}(X_\lambda)$. If moreover Λ is finite, then $\prod_{\lambda \in \Lambda} \mathcal{I}(X_\lambda) \subseteq \mathcal{I}\big(\bigcup_{\lambda \in \Lambda} X_\lambda\big)$.*
(d) *$\mathcal{I}(\varnothing) = K[X_1, \ldots, X_n]$ and, if K is **infinite**, then $\mathcal{I}(\mathbf{A}^n(K)) = 0$.*

PROOF - Easy. ■

Proposition 11.4. *We have:*

(a) *If $E \subseteq K[X_1, \dots, X_n]$, then $\langle E \rangle \subseteq \mathcal{I}(\mathcal{Z}(E))$ and $\mathcal{Z}(E) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(E)))$.*
(b) *If $X \subseteq \mathbf{A}^n(K)$, we have $X \subseteq \mathcal{Z}(\mathcal{I}(X))$ and $\mathcal{I}(X) = \mathcal{I}(\mathcal{Z}(\mathcal{I}(X)))$.*

PROOF - Easy. ■

11.B. Algebraic sets.

Definition 11.5. *A subset V of $\mathbf{A}^n(K)$ is called an **affine algebraic set** (or just an **algebraic set**) if there exists a subset E of $K[X_1, \dots, X_n]$ such that $V = \mathcal{Z}(E)$ (or, equivalently, if there exists an ideal I of $K[X_1, \dots, X_n]$ such that $V = \mathcal{Z}(I)$).*

If V is an algebraic set, then

$$V = \mathcal{Z}(\mathcal{I}(V)). \tag{11.6}$$

PROOF - By Proposition 11.4 (b), we have $V \subseteq \mathcal{Z}(\mathcal{I}(V))$. On the other hand, there exists an ideal I of $K[X_1, \dots, X_n]$ such that $V = \mathcal{Z}(I)$. Therefore, by Proposition 11.4 (a), we have $I \subseteq \mathcal{I}(V)$. So $\mathcal{Z}(\mathcal{I}(V)) \subseteq \mathcal{Z}(I) = V$ by Proposition 11.3 (a). ■

An immediate consequence of 11.6 is the following:

(11.7) *If V and W are two algebraic sets such that $V \subsetneq W$, then $\mathcal{I}(W) \subsetneq \mathcal{I}(V)$.*

EXAMPLES 11.8 - (0) $\varnothing$ and $\mathbf{A}^n(K)$ are algebraic sets (see Proposition 11.1 (e)).

(1) If $(a_1, \dots, a_n) \in \mathbf{A}^n(K)$, then $\{(a_1, \dots, a_n)\}$ is an algebraic set. Indeed,

$$\{(a_1, \dots, a_n)\} = \mathcal{Z}(X_1 - a_1, \dots, X_n - a_n).$$

It then follows from Proposition 11.1 (c) that any finite subset of $\mathbf{A}^n(K)$ is an algebraic set.

(2) If $V \subseteq \mathbf{A}^1(K)$, then V is an algebraic set if and only if $V = \mathbf{A}^1(K)$ or V is finite.

(3) The curve $\{(x, y) \in \mathbf{A}^2(K) \mid y^2 = x^3\}$ is an algebraic set.

(4) Let V be the set of matrices $M \in \mathrm{Mat}_n(K)$ which are not invertible. Then V is an algebraic set: indeed, $X = \mathcal{Z}(\det)$ and det is a polynomial in n^2 variables. □

Definition 11.9. *The **Zariski topology** on $\mathbf{A}^n(K)$ is the topology for which the closed subsets are the algebraic sets.*

The statements (c) and (d) of Proposition 11.1 show that this indeed defines a topology on $\mathbf{A}^n(K)$. If X is a subset of $\mathbf{A}^n(K)$, we denote by $\overline{X}$ its closure for the Zariski topology. Then

$$\overline{X} = \mathcal{Z}(\mathcal{I}(X)). \tag{11.10}$$

PROOF - Let $V = \mathcal{Z}(\mathcal{I}(X))$. By Proposition 11.4 (b), we have $X \subseteq V$, and V is closed by definition. So $\overline{X} \subseteq V$. On the other hand, since $\overline{X}$ is an algebraic set, there exists an ideal

I of $K[X_1, \dots, X_n]$ such that $\overline{X} = \mathcal{Z}(I)$. Since $X \subseteq \overline{X}$, we have $I \subseteq \mathcal{I}(X)$ by Proposition 11.3 (a), so $V = \mathcal{Z}(\mathcal{I}(X)) \subseteq \mathcal{Z}(I) = \overline{X}$ by Proposition 11.1 (a). ■

EXAMPLE 11.11 - If $K = \mathbb{C}$, then $\overline{\mathbb{Z}} = \mathbf{A}^1(\mathbb{C})$ ($\mathbb{Z}$ is dense in $\mathbb{C}$!). □

If $V \subseteq \mathbf{A}^n(K)$ is an algebraic set, we define the *Zariski topology* to be the topology induced by the Zariski topology on $\mathbf{A}^n(K)$: by Proposition 11.1 (c), the closed subsets of V for the Zariski topology are the algebraic sets V' which are contained in V.

A topological space $\mathcal{X}$ is called *irreducible* if, for all closed subsets Z and Z' of $\mathcal{X}$ such that $\mathcal{X} = Z \cup Z'$, we have $Z = \mathcal{X}$ or $Z' = \mathcal{X}$. For instance, an algebraic set is irreducible (for the Zariski topology) is it is not the union of two proper algebraic subsets.

Proposition 11.12. *Let $V \subseteq \mathbf{A}^n(K)$ be an algebraic set. Then V is irreducible if and only if $\mathcal{I}(V)$ is a prime ideal.*

PROOF - Assume that V is not irreducible. Write $V = V_1 \cup V_2$, where V_1 and V_2 are proper algebraic subsets of V and let $I_1 = \mathcal{I}(V_1)$, $I_2 = \mathcal{I}(V_2)$ and $I = \mathcal{I}(V)$. Recall from 11.6 that $V = \mathcal{Z}(I)$, $V_i = \mathcal{Z}(I_i)$. Moreover, $I_1 I_2 \subseteq I$ by Proposition 11.3 (c). By 11.7, we have $I \subsetneq I_1$ and $I \subsetneq I_2$. So there exists $f \in I_1$ and $g \in I_2$ such that $f \notin I$ and $g \notin I$. But $fg \in I$, so I is not prime.

Conversely, assume that I is not prime. Let f_1, $f_2 \in K[X_1, \dots, X_n]$ be such that $f_1 \notin I$, $f_2 \notin I$ and $f_1 f_2 \in I$. Let $I_1 = I + Rf_1$ and $I_2 = I + Rf_2$ and let $V_i = \mathcal{Z}(I_i)$. Then $V_i \subseteq V$ by Proposition 11.1 (a) and, since $I_1 I_2 \subseteq I$, we get that $V \subseteq V_1 \cup V_2$ by Proposition 11.1 (c). So $V = V_1 \cup V_2$. It remains to show that $V_i \neq V$. But, since $f_i \notin \mathcal{I}(V)$, there exists $x \in V$ such that $f_i(x) \neq 0$. So $x \notin V_i$. ■

Corollary 11.13. *If K is **infinite**, then $\mathbf{A}^n(K)$ is irreducible.*

11.C. Regular maps. We fix an algebraic set $V \subseteq \mathbf{A}^n(K)$.

Definition 11.14. *A map $f : V \to K$ is called **regular** (or **polynomial**) if there exists $\tilde{f} \in K[X_1, \dots, X_n]$ such that $f(x) = \tilde{f}(x)$ for all $x \in V$.*

*We denote by $K[V]$ the set of regular maps $V \to K$: it is called the **coordinate ring** of V.*

It is readily seen that $K[V]$ is a K-algebra. Moreover, the map $K[X_1, \dots, X_n] \to K[V]$, $\tilde{f} \mapsto (x \in V \mapsto \tilde{f}(x) \in K)$ is a surjective morphism of algebras, whose kernel is $\mathcal{I}(V)$. So

$$K[V] \simeq K[X_1, \dots, X_n]/\mathcal{I}(V). \tag{11.15}$$

We shall identify $K[V]$ and $K[X_1, \dots, X_n]/\mathcal{I}(V)$ in the rest of this part. Note that the Proposition 11.12 can be reinterpreted as follows:

Proposition 11.16. *V is irreducible if and only $K[V]$ is an integral domain.*

The Proposition 11.16 is the first illustration of what is the essential subject of Algebraic Geometry:

Relate "geometric" properties of V and algebraic properties of $K[V]$.

Note that $K[V]$ is, by 11.15, a finitely generated K-algebra, so it is Noetherian by Hilbert's Basis Theorem.

REMARK 11.17 - Even though its definition is simple, the computation of the ideal $\mathcal{I}(V)$ can be very difficult. For instance, if $K = \mathbb{Q}$, if p is a prime number and if $V = \mathcal{Z}(X^p+Y^p+Z^p)$, then it took more than 400 years (!) to compute $\mathcal{I}(V)$: this is Fermat's last Theorem, proved by Wiles and Taylor in the 1990's (it says that $\mathcal{I}(V) = \langle X^p + Y^p + Z^p, XYZ\rangle$).

If K is algebraically closed, then Hilbert's Nullstellensatz (see next section) gives a very efficient way to compute $\mathcal{I}(V)$. □

We shall now define maps $\mathcal{Z}_V$ and $\mathcal{I}_V$ in the same way as the maps $\mathcal{Z}$ and $\mathcal{I}$. If E is a subset of $K[V]$, we set

$$\mathcal{Z}_V(E) = \{x \in V \mid \forall\ f \in E,\ f(x) = 0\}.$$

If X is a subset of V, we set

$$\mathcal{I}_V(X) = \{f \in K[V] \mid \forall\ x \in X,\ f(x) = 0\}.$$

It is clear that

(11.18) $$\mathcal{Z}_V(E) = \mathcal{Z}(\tilde{E}),$$

where $\tilde{E}$ is the inverse image of E in $K[X_1, \ldots, X_n]$ (under the isomorphism 11.15). In particular,

(11.19) *$\mathcal{Z}_V(E)$ is an algebraic subset of V.*

Also

(11.20) $$\mathcal{I}_V(X) = \mathcal{I}(X)/\mathcal{I}(V).$$

Proposition 11.21. *Let $f \in K[V]$ (and view it as a map $V \to \mathbf{A}^1(K)$). Then f is continuous.*

PROOF - This amounts to show that $f^{-1}(W)$ is an algebraic subset of V for all algebraic subsets W of $\mathbf{A}^1(K)$. If $W = \mathbf{A}^1(K)$, this is easy. So we may assume that $W \neq \mathbf{A}^1(K)$. Then W is finite by Example 11.8 (2). Write $W = \{\alpha_1, \ldots, \alpha_r\}$, with $\alpha_i \in K$. Then

$$f^{-1}(W) = \mathcal{Z}_V(\prod_{i=1}^{r}(f - \alpha_i)).$$

So $f^{-1}(W)$ is an algebraic subset of V by 11.19. ■

Definition 11.22. *Let A be a K-algebra. A maximal ideal $\mathfrak{m}$ of A is called K-**rational** if the natural map $K \to A/\mathfrak{m}$ is an isomorphism. We denote by $\mathrm{Max}_K(A)$ the set of K-rational maximal ideals of A.*

Let $V \subseteq \mathbf{A}^n(K)$ be an algebraic set. If $x \in V$, we denote by $\mathfrak{m}_x$ (or $\mathfrak{m}_x^V$ is necessary) the ideal $\mathcal{I}_V(x)$. Then the map $K[V] \to K$, $f \mapsto f(x)$ is surjective and its kernel is $\mathfrak{m}_x$. In particular, $\mathfrak{m}_x$ is a K-rational maximal ideal of $K[V]$. In fact:

Proposition 11.23. *If V is an algebraic set, then the map $V \to \mathrm{Max}_K(K[V])$, $x \mapsto \mathfrak{m}_x$ is bijective.*

PROOF - The map $K[X_1, \ldots, X_n] \to K$, $f \mapsto f(x)$ is surjective and has kernel $\mathcal{I}(x)$, so $\mathcal{I}(x) \in \mathrm{Max}_K(K[X_1, \ldots, X_n])$. Then, if $x = (x_1, \ldots, x_n)$, then

$$\mathcal{I}(x) = \langle X_1 - x_1, \ldots, X_n - x_n \rangle. \tag{11.24}$$

In particular, $\mathcal{Z}(\mathcal{I}(x)) = \{x\}$. So

$$x \in \mathcal{Z}(E) \text{ } \textit{if and only if} \text{ } E \subseteq \mathcal{I}(x). \tag{11.25}$$

Let us now show the following result:

$$\textit{The map } \mathbf{A}^n(K) \to \mathrm{Max}_K(K[X_1, \ldots, X_n]),\ x \mapsto \mathcal{I}(x) \textit{ is bijective.} \tag{11.26}$$

First, the equality 11.24 shows that this map is injective. Let us now show that it is surjective. Now, let $\mathfrak{m} \in \mathrm{Max}_K(K[X_1, \ldots, X_n])$. Then the natural map $\sigma : K \to K[X_1, \ldots, X_n]/\mathfrak{m}$ is an isomorphism. Let $x_i = \sigma^{-1}(\overline{X}_1)$. Then $X_i - x_i \in \mathfrak{m}$ by construction. So, if $x = (x_1, \ldots, x_n)$, then $\mathcal{I}(x) \subseteq \mathfrak{m}$. Since $\mathcal{I}(x)$ is maximal, we get that $\mathfrak{m} = \mathcal{I}(x)$, as desired.

Now, let $\pi_V : K[X_1, \ldots, X_n] \to K[V]$ be the canonical morphism of algebras. Then the map $\mathrm{Max}_K(K[V]) \to \mathrm{Max}_K(K[X_1, \ldots, X_n])$, $\mathfrak{m} \mapsto \pi_V^{-1}(\mathfrak{m})$ is a bijection and it is clear that, if $x \in V$, then $\mathfrak{m}_x^V = \pi_V(\mathcal{I}(x)) = \mathcal{I}(x)/\mathcal{I}(V)$. So the result follows. ■

11.D. Morphisms. Let $V \subseteq \mathbf{A}^n(K)$ and $W \subseteq \mathbf{A}^m(K)$ be two algebraic sets.

Definition 11.27. *A map $\varphi : V \to W$ is called a **morphism of algebraic sets** (or a **polynomial map**, or a **regular map**) if, for all regular maps $f : V \to K$, the map $f \circ \varphi : W \to K$ is regular.*

If $\varphi : V \to W$ is a morphism of algebraic sets, we denote by $\varphi^* : K[V] \to K[W]$, $f \mapsto f \circ \varphi$ the map induced by φ (it is an homomorphism of K-algebras).

The morphism $\varphi : V \to W$ is called an isomorphism if $\varphi^{-1} : W \to V$ is a morphism of algebraic sets.

In particular, if φ is an isomorphism of algebraic sets, then φ^* is an isomorphism of K-algebras. We shall see later (see Corollary 11.33) that in fact φ is an isomorphism *if and only if* φ^* is an isomorphism of K-algebras.

We denote by $\mathrm{Mor}_K(V, W)$ the set of morphisms of algebraic sets $V \to W$. If A and B are two K-algebras, we denote by $\mathrm{Hom}_{K-\mathrm{alg}}(A, B)$ the set of homomorphisms of K-algebras $A \to B$.

Proposition 11.28. *Let V, W and X be three algebraic sets and let $\varphi : V \to W$ and $\psi : W \to X$ be two morphisms of algebraic sets. Then $\psi \circ \varphi : V \to X$ is a morphism of algebraic sets, and $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.*

PROOF - Clear. ■

The Proposition 11.28 shows that there is a well-defined category $\mathrm{Aff}(K)$ whose objects are algebraic sets and morphisms are morphisms of algebraic sets. If we denote by ${}_K\mathbf{alg}$

the category of finitely generated K-algebras, the Proposition 11.28 shows also that

$$\begin{array}{rcl} \mathrm{Aff}(K) & \longrightarrow & {}_K\mathbf{alg} \\ V & \longmapsto & K[V] \\ \varphi & \longmapsto & \varphi^* \end{array}$$

is a *contravariant functor.*

Proposition 11.29. *Let $\varphi : V \to W$ be a map. Then the following are equivalent:*

(1) *φ is a morphism of algebraic sets.*
(2) *There exists regular maps $\varphi_1, \ldots, \varphi_m \in K[V]$ such that, for all $x \in V$, $\varphi(x) = (\varphi_1(x), \ldots, \varphi_m(x))$.*
(3) *There exists polynomials $\varphi_1, \ldots, \varphi_m \in K[X_1, \ldots, X_n]$ such that, for all $x \in V$, $\varphi(x) = (\varphi_1(x), \ldots, \varphi_m(x))$.*

Proof - It is clear that (2) and (3) are equivalent. Assume that (1) holds. Then the map $\mathcal{X}_i : W \to K$, $(x_1, \ldots, x_n) \mapsto x_i$ is regular, so $\varphi_i := \mathcal{X}_i \circ \varphi$ is also a regular map on V. Then it is immediately checked that $\varphi(x) = (\varphi_1(x), \ldots, \varphi_m(x))$ for all $x \in V$, so (2) holds.

Conversely, assume that (3) holds. Let $f \in K[W]$ and let $\tilde{f} \in K[X_1, \ldots, X_m]$ be such that $f(x) = \tilde{f}(x)$ for all $x \in W$. Now, let $\tilde{g} = \tilde{f}(\varphi_1(X_1, \ldots, X_n), \ldots, \varphi_m(X_1, \ldots, X_n))$. Then $\tilde{g} \in K[X_1, \ldots, X_n]$ and let $g : V \to K$, $x \mapsto \tilde{g}(x)$. Then g is a regular map by definition and it is readily seen that $g = f \circ \varphi$. This shows (1). ■

Corollary 11.30. *If $\varphi : V \to W$ is a morphism of algebraic sets and if V' and W' are algebraic subsets of V and W respectively such that $\varphi(V') \subseteq W'$, then the map $V' \to W'$, $x \mapsto \varphi(x)$ (the restriction of φ) is a morphism of algebraic sets.*

Proposition 11.31. *The map $\mathrm{Mor}_K(V, W) \to \mathrm{Hom}_{K-\mathrm{alg}}(K[W], K[V])$, $\varphi \mapsto \varphi^*$ is bijective.*

Proof - Let us denote by θ the map $\mathrm{Mor}_K(V, W) \to \mathrm{Hom}_{K-\mathrm{alg}}(K[W], K[V])$, $\varphi \mapsto \varphi^*$.

Let us first show that θ is injective. Let φ and ψ be two morphisms of algbebraic sets such that $\varphi^* = \psi^*$. Write $\varphi(x) = (\varphi_1(x), \ldots, \varphi_m(x))$ and $\psi(x) = (\psi_1(x), \ldots, \psi_m(x))$ for all $x \in V$, where the φ_i's and the ψ_i's are regular maps $V \to K$. Let $\mathcal{X}_i : W \to K$, $(x_1, \ldots, x_m) \mapsto x_i$. Then $\mathcal{X}_i$ is regular, so $\mathcal{X}_i \circ \varphi = \mathcal{X}_i \circ \psi$, so $\varphi_i = \psi_i$ for all i. So $\varphi = \psi$.

Let us now show that θ is surjective. Let $\gamma : K[W] \to K[V]$ be a morphism of K-algebras. Let $\varphi_i = \gamma(\mathcal{X}_i) \in K[V]$ and let $\varphi : V \to \mathbf{A}^m(K)$, $x \mapsto (\varphi_1(x), \ldots, \varphi_m(x))$. We only need to show that $\varphi(V) \subseteq W$ (see Corollary 11.30). Let $\tilde{f} \in \mathcal{I}(W)$ and let $x \in V$. We only need to show that $\tilde{f}(\varphi(x)) = 0$. Let $\tilde{\gamma} : K[X_1, \ldots, X_m] \to K[V]$ be the composition $K[X_1, \ldots, X_m] \longrightarrow K[W] \xrightarrow{\gamma} K[V]$. Then, by definition, $\varphi_i = \tilde{\gamma}(X_i)$. So $\tilde{f} \circ \varphi = \tilde{\gamma}(\tilde{f})$. But $\tilde{\gamma}(\tilde{f}) = 0$ by construction. So $\varphi(x) \in \mathcal{Z}(\mathcal{I}(V)) = V$. ■

Remark 11.32 - The Proposition 11.31 says that the functor $\mathrm{Aff}(K) \to {}_K\mathbf{alg}$, $V \mapsto K[V]$ is *fully faithful.* □

Corollary 11.33. *A morphism of algebraic sets $\varphi : V \to W$ is an isomorphism if and only if φ^* is an isomorphism of K-algebras.*

We shall now show that the map $\mathrm{Mor}_K(V,W) \to \mathrm{Hom}_{K-\mathrm{alg}}(K[W],K[V])$ is "compatible" with the bijections $V \xrightarrow{\sim} \mathrm{Max}_K(K[V])$ and $W \xrightarrow{\sim} \mathrm{Max}_K(K[W])$ described in Proposition 11.23.

Proposition 11.34. *Let $\varphi : V \to W$ be a morphism of algebraic sets and let $x \in V$. Then*

$$\varphi^{*-1}(\mathfrak{m}_x^V) = \mathfrak{m}_{\varphi(x)}^W.$$

PROOF - Easy. ■

11.E. Image, inverse image. A morphism of algebraic sets $\varphi : V \to W$ is called *dominant* if $\overline{\varphi(V)} = W$.

Proposition 11.35. *Let $\varphi : V \to W$ be a morphism of algebraic sets and let I be an ideal of $K[V]$. Then $\mathcal{I}_W(\varphi(V)) = \mathrm{Ker}\,\varphi^*$. In particular, $\overline{\varphi(V)} = \mathcal{Z}_W(\mathrm{Ker}\,\varphi^*)$ and $\mathcal{I}_W(\overline{\varphi(V)}) = \mathrm{Ker}\,\varphi^*$.*

PROOF - Easy. ■

Corollary 11.36. *A morphism of algebraic sets $\varphi : V \to W$ is dominant if and only if φ^* is injective.*

PROOF - Clear. ■

Proposition 11.37. *Let $\varphi : V \to W$ be a morphism of algebraic sets and let $E \subseteq K[W]$. Then $\varphi^{-1}(\mathcal{Z}_W(E)) = \mathcal{Z}_V(\varphi^*(E))$.*

PROOF - Let $x \in V$. Then $\varphi(x) \in \mathcal{Z}_W(E)$ if and only if $f(\varphi(x)) = 0$ for all $f \in E$. In other words, $\varphi(x) \in \mathcal{Z}_W(E)$ if and only if $\varphi^*(f)(x) = 0$ for all $f \in E$ that is, if and only if $x \in \mathcal{Z}_V(\varphi^*(E))$. ■

Corollary 11.38. *A morphism of algebraic sets is continuous.*

11.F. Finite morphisms.

Definition 11.39. *A morphism $\varphi : V \to W$ of algebraic sets is called finite if $K[V]$ is a finitely generated $K[W]$-module (here, $K[V]$ is viewed as a $K[W]$-algebras through the morphism $\varphi^* : K[W] \to K[V]$).*

REMARK 11.40 - If φ is a finite morphism, then $K[V]$ is integral over $K[W]$. In fact, the converse is also true. Indeed, if $K[V]$ is integral over $K[W]$ then, since $K[V]$ is a finitely generated K-algebra, it is a fortiori a finitely generated $K[W]$-algebra, so the result follows from Proposition 9.9. □

Here is a geometric consequence of such notion:

Proposition 11.41. *Let $\varphi : V \to W$ be a finite morphism of algebraic sets and let $w \in W$. Then $\varphi^{-1}(w)$ is finite.*

PROOF - Recall from Proposition 11.37 that $\varphi^{-1}(w) = \mathcal{Z}_V(\varphi^*(\mathfrak{m}_w^W))$. So, by Proposition 11.23 (and its proof), an element $v \in V$ lies in $\varphi^{-1}(w)$ if and only if $\mathfrak{m}_v^V$ contains $\varphi^*(\mathfrak{m}_w^W)$. So it is sufficient to show that the set of maximal ideals of $K[V]$ containing $\varphi^*(\mathfrak{m}_w^W)$ is finite. Let I be the ideal of $K[V]$ generated by $\varphi^*(\mathfrak{m}_w^W)$. Then φ^* induces a morphism $\sigma : K[W]/\mathfrak{m}_w^W \to K[V]/I$. Two case may occur:

• If $I = K[V]$, then $K[V]/I = 0$ so $\varphi^{-1}(w) = \varnothing$.

• If $I \neq K[V]$, then σ is injective because $K[V]/\mathfrak{m}_w^W \simeq K$. Moreover, $K[V]/I$ is integral over K (because $K[V]$ is integral over $K[W]$). Moreover, $K[V]/I$ is finitely generated over K. So $A = K[V]/I$ is a finite dimensional commutative K-algebra. Therefore, $A/J(A)$ is a finite dimensional commutative semisimple K-algebra and we only need to show that such an algebra has a finite number of maximal ideals. But, by Wedderburn's Theorem, A is a finite product of fields: this shows the result. ■

12. Noether's Normalization Theorem, Hilbert's Nullstellensatz

Since geometric properties of algebraic sets are intimately related to algebraic properties of finitely generated algebras, it will be useful to study these algebras *a priori*. The first important result about these algebras is the following:

Noether's Normalization Theorem. *Let A be a commutative K-algebra which is generated by n elements. Then there exists $m \in \{0, 1, 2, \dots, n\}$ and elements $x_1, \dots, x_m$ of A which are algebraically independent and such that A is integral over $K[x_1, \dots, x_m]$.*

REMARK - A family of elements $(x_i)_{1 \leqslant i \leqslant n}$ of a K-algebra $\mathcal{A}$ are called *algebraically independent* (over K) if the map $K[X_1, \dots, X_n] \to \mathcal{A}$, $f \mapsto f(x_1, \dots, x_n)$ is injective. □

PROOF - We argue by induction on n. The result is obvious if $n = 0$. So we assume that $n \geqslant 1$ and that it is true for all algebras generated by n' elements, with $n' < n$.

Let $y_1, \dots, y_n$ be generators of A. First, if they are algebraically independent, we take $m = n$ and $(x_1, \dots, x_m) = (y_1, \dots, y_n)$. So we may, and we will, assume that $(y_1, \dots, y_n)$ are not algebraically independent. Then there exists $P \in K[Y_1, \dots, Y_n]$ such that $P(y_1, \dots, y_n) = 0$, where the Y_i's are algebraically independent indeterminates. Let us write

$$P = \sum_{(d_1,\dots,d_n)\in\mathcal{D}} a_{d_1,\dots,d_n} Y_1^{d_1} \dots Y_n^{d_n}$$

where $\mathcal{D}$ is a finite subset of $(\mathbb{Z}_{\geq 0})^n$ and $a_{\mathbf{d}} \neq 0$ for all $\mathbf{d} \in \mathcal{D}$. We define the *degree* of P to be

$$\deg P = \max_{(d_1,\dots,d_n)\in\mathcal{D}} d_1 + \dots + d_n.$$

Let $d = \deg P$ and let $\alpha_i = (1 + d)^i$. Then $d \geqslant 1$ because P is not constant. Now, let

$$Q(Y_1, \dots, Y_n) = P(Y_1 + Y_n^{\alpha_1}, \dots, Y_{n-1} + Y_n^{\alpha_{n-1}}, Y_n)$$

and

$$z_i = y_i - y_n^{\alpha_i}.$$

Then $z_1,\ldots,\ z_{n-1},\ y_n$ generate A and $Q(z_1,\ldots,z_{n-1},y_n)=0$. If $(d_1,\ldots,d_n)\in\mathcal{D}$, we define

$$\begin{aligned}\mathbf{e}(d_1,\ldots,d_n) &= \alpha_1 d_1+\alpha_2 d_2+\cdots+\alpha_{n-1}d_{n-1}+d_n\\ &= d_n+d_1(1+d)+d_2(1+d)^2+\cdots+d_{n-1}(1+d)^{n-1}.\end{aligned}$$

Then the map $\mathcal{D}\to\mathbb{N}$, $\mathbf{d}\mapsto\mathbf{e}(\mathbf{d})$ is injective (because $d_i\leqslant d$ for all $(d_1,\ldots,d_n)\in\mathcal{D}$). Let $\mathbf{d}_0\in\mathcal{D}$ be such that $\mathbf{e}(\mathbf{d}_0)$ is maximal. Then

$$Q(Y_1,\ldots,Y_n)=a_{\mathbf{d}_0}Y_n^{\mathbf{e}(\mathbf{d}_0)}+\sum_{i<\mathbf{e}(\mathbf{d}_0)}h_i(Y_1,\ldots,Y_{n-1})Y_n^i$$

for some $h_i\in K[Y_1,\ldots,Y_{n-1}]$. Let A' be the subalgebra of A generated by $z_1,\ldots,\ z_{n-1}$. Since K is a field, we can define

$$Q_0=T^{\mathbf{e}(\mathbf{d}_0)}+a_{\mathbf{d}_0}^{-1}\sum_{i<\mathbf{e}(\mathbf{d}_0)}h_i(z_1,\ldots,z_{n-1})T^i.$$

Then $Q_0\in A'[X]$ is monic and $Q_0(y_n)=0$. So $A=A'[y_n]$ is integral over A', so it is a finitely generated A'-module.

Now, by the induction hypothesis (and since A' is generated by $n-1$ elements), there exists $m\leqslant n-1$ and a family $(x_1,\ldots,x_m)$ of algebraically independent elements of A' such that A' is a finitely generated $K[x_1,\ldots,x_m]$-module. So A is a finitely generated $K[x_1,\ldots,x_m]$-module. ■

Remark 12.1 - If $V\subseteq\mathbf{A}^n(K)$ is an algebraic set, then $K[V]$ is a K-algebra generated by n elements (see 11.15). So, by Noether's normalization Theorem, there exists $x_1,\ldots,\ x_m$ in $K[V]$ which are algebraically independent and such that $K[V]$ is a finitely generated $K[x_1,\ldots,x_m]$-module. Let $\varphi^*:K[X_1,\ldots,X_m]\to K[V]$ be the morphism of K-algebras $X_i\mapsto x_i$. Then, by Proposition 11.31, φ^* corresponds to a morphism of algebraic sets $\varphi:V\to\mathbf{A}^m(K)$. By construction, this morphism is finite (so, by Proposition 11.41, $\varphi^{-1}(x)$ is finite for all $x\in\mathbf{A}^m(K)$) and is dominant (by Proposition 11.36). □

Corollary 12.2. *Let A be a finitely generated commutative K-algebra. We assume that A is a field. Then A is a finite algebraic extension of K.*

Proof - This follows from Noether's Normalization Theorem and from Proposition 9.19 (b). ■

Corollary 12.3. *Let A and B be two finitely generated K-algebras, let $\varphi^*:A\to B$ be a morphism of K-algebras and let $\mathfrak{m}\in\mathrm{Max}(B)$. Then $\varphi^{*-1}(\mathfrak{m})\in\mathrm{Max}(A)$.*

Corollary 12.4. *Let A be a finitely generated commutative K-algebra and assume that K is **algebraically closed**. Then $\mathrm{Max}(A)=\mathrm{Max}_K(A)$.*

Proof - Let $\mathfrak{m}\in\mathrm{Max}(A)$. Then $A/\mathfrak{m}$ is a finitely generated commutative K-algebra which is a field, so it is a finite extension of K. Since K is algebraically closed, it must be equal to the image of K. ■

Corollary 12.5 (Hilbert's Nullstellensatz - weak form). *Assume that K is **algebraically closed** and let I be a proper ideal of $K[X_1,\ldots,X_n]$. Then $\mathcal{Z}(I)\neq\varnothing$.*

PROOF - Indeed, by Corollary 5.2, there exists a maximal ideal $\mathfrak{m}$ of $K[X_1, \ldots, X_n]$ containing I. By Corollary 12.4, $\mathfrak{m}$ is K-rational. So $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ for some $a = (a_1, \ldots, a_n) \in \mathbf{A}^n(K)$. The fact that $I \subseteq \mathfrak{m}$ implies that $a \in \mathcal{Z}(I)$. ■

Hilbert's Nullstellensatz. *Let $E \subseteq K[X_1, \ldots, X_n]$ and assume that K is **algebraically closed**. Then $\mathcal{I}(\mathcal{Z}(E)) = \sqrt{\langle E \rangle}$.*

REMARK - For the definition of the radical $\sqrt{I}$ of an ideal I, see the Appendix. □

PROOF - It is clear that $\sqrt{\langle E \rangle} \subseteq \mathcal{I}(\mathcal{Z}(E))$. Let us now prove the reverse inclusion. Let $f \in \mathcal{I}(\mathcal{Z}(E))$. We may assume that $f \neq 0$. Let I be the ideal of $K[X_1, \ldots, X_n, T]$ generated by E and $1 - Tf$. Then

$$\begin{aligned} \mathcal{Z}(I) &= \{(x_1, \ldots, x_n, t) \in \mathbf{A}^{n+1}(K) \mid \forall g \in E,\ g(x_1, \ldots, x_n) = 0 \text{ and } f(x_1, \ldots, x_n)t = 1\} \\ &= \{(x_1, \ldots, x_n, t) \mid (x_1, \ldots, x_n) \in \mathcal{Z}(E) \text{ and } f(x_1, \ldots, x_n)t = 1\} \\ &= \varnothing \end{aligned}$$

because $f(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in \mathcal{Z}(E)$. So, by Corollary 12.5, $I = K[X_1, \ldots, X_n, T]$. So there exists $P_1, \ldots, P_r \in E$ and $Q_1, \ldots, Q_r, Q$ in $K[X_1, \ldots, X_n, T]$ such that

$$1 = (1 - Tf)Q + \sum_{i=1}^{n} P_i Q_i.$$

Now, by working in the field of fractions $K(X_1, \ldots, X_n)$, we can specialize the previous equality through $T \mapsto 1/f$. We get

$$1 = \sum_{i=1}^{n} P_i(X_1, \ldots, X_n) Q_i(X_1, \ldots, X_n, 1/f).$$

Now, let $N \in \mathbb{N}$ be large enough so that $R_i = f^N Q_i(X_1, \ldots, X_n, 1/f) \in K[X_1, \ldots, X_n]$ for all i. Then

$$f^N = \sum_{i=1}^{n} P_i R_i \in \langle E \rangle,$$

as desired. ■

13. Algebraic sets over algebraically closed fields

From now on, and until the end of this part, we assume that K is algebraically closed. We define an *affine variety* (over K) to be an irreducible algebraic subset of some $\mathbf{A}^n(K)$.

EXAMPLE 13.1 - Let $f \in K[X_1, \ldots, X_n]$ be non-constant. Let us factorize $f = f_1^{r_1} \ldots f_k^{r_k}$ where $r_i \geqslant 1$ and the f_i's are irreducible and distincts. Then $\mathcal{Z}(f) = \mathcal{Z}(f_1 \ldots f_k) = \mathcal{Z}(f_1) \cup \cdots \cup \mathcal{Z}(f_k)$ and $\mathcal{I}(\mathcal{Z}(f)) = \langle f_1 \ldots f_k \rangle$ by Hilbert's Nullstellensatz. We say that $\mathcal{Z}(f)$ is an *hypersurface* if $k = 1$: this is equivalent to say that $\mathcal{Z}(f)$ is irreducible. □

13.A. Properties of the correspondence $V \mapsto K[V]$. Recall that the definitions of the radical of an ideal and of the nilradical of a commutative ring are given in the Appendix.

Definition 13.2. *A commutative K-algebras A is called **reduced** if its nilradical is 0 (in other words, if 0 is the only nilpotent element). We denote by ${}_K\mathbf{alg}_{\mathrm{red}}$ the category of finitely generated commutative reduced K-algebras.*

If $V \subseteq \mathbf{A}^n(K)$, then $K[V] \in {}_K\mathbf{alg}_{\mathrm{red}}$. Moreover, as explained in §11.D, the correspondence

$$\begin{array}{ccc} \mathrm{Aff}(K) & \longrightarrow & {}_K\mathbf{alg}_{\mathrm{red}} \\ V & \longmapsto & K[V] \\ \varphi & \longmapsto & \varphi^* \end{array}$$

is a contravariant functor which is fully faithful. We shall now show that it is essentially surjective (i.e. that, for $A \in {}_K\mathbf{alg}_{\mathrm{red}}$, there exists an algebraic set V such that $K[V] \simeq A$) and will study further the properties of this functor.

Theorem 13.3. *Recall that K is algebraically closed. Let $V \in \mathrm{Aff}(K)$. Then:*

(a) *The functor $K[-] : \mathrm{Aff}(K) \to {}_K\mathbf{alg}_{\mathrm{red}}$ is essentially surjective.*
(b) *The map $W \mapsto \mathcal{I}_V(W)$ induces a bijection between algebraic subsets of V and radical ideals of $K[V]$.*
(c) *The map $W \mapsto \mathcal{I}_V(W)$ induces a bijection between **irreducible** algebraic subsets of V and **prime** ideals of $K[V]$.*
(d) *The map $x \mapsto \mathfrak{m}_x^V$ induces a bijection between V and maximal ideals of $K[V]$.*
(e) *V is irreducible if and only if $K[V]$ is integral.*
(f) *If $W \in \mathrm{Aff}(K)$, then the map $\mathrm{Mor}_K(V,W) \to \mathrm{Hom}_{K-\mathrm{alg}}(K[W], K[V])$, $\varphi \mapsto \varphi^*$ is bijective.*

Proof - (a) Let $A \in {}_K\mathbf{alg}_{\mathrm{red}}$. Let $x_1, \ldots, x_n \in A$ be such that $A = K[x_1, \ldots, x_n]$. Let $\pi : K[X_1, \ldots, X_n] \to A$ denote the unique morphism of K-algebras such that $\pi(X_i) = x_i$ for all i. Let $I = \mathrm{Ker}\,\pi$. Then $A \simeq K[X_1, \ldots, X_n]/I$ so I is a radical ideal. In particular $\mathcal{I}(\mathcal{Z}(I)) = I$ by Hilbert's Nullstellensatz, so $K[X_1, \ldots, X_n]/I \simeq K[\mathcal{Z}(I)]$. Therefore, $A \simeq K[\mathcal{Z}(I)]$.

(b) and (c) follow easily from Hilbert's Nullstellensatz (note that a prime ideal is always radical).

(d) follows from Proposition 11.23 and the weak form of Hilbert's Nullstellensatz (Corollary 12.5).

(e) is Proposition 11.16.

(f) is Proposition 11.32. ■

We shall study *geometric properties* of algebraic sets: by geometric properties, we mean properties which are "functorial" with respect to morphism of algebraic sets and in particular which are invariant under isomorphism of algebraic sets.

13.B. Irreducible components. Since an isomorphism of algebraic sets is an homeomorphism, the topology of an algebraic set is "part" of its geometry. For instance, being irreducible is a property which is stable by homeomorphism (and which is functorial by

Exercise IV.1. For general topological spaces (not necessarily irreducible), we introduce the following notion:

Definition 13.4. *If $\mathcal{X}$ is a topological space and if $Z \subseteq \mathcal{X}$, we say that Z is an **irreducible component** of $\mathcal{X}$ if Z is an irreducible closed subset of $\mathcal{X}$ which is maximal for these properties. We denote by $\mathrm{Irr}(\mathcal{X})$ the set of irreducible components of $\mathcal{X}$.*

Proposition 13.5. *Let $V \in \mathrm{Aff}(K)$. The map $W \mapsto \mathcal{I}_V(W)$ induces a bijection between irreducible components of V and minimal prime ideals of $K[V]$. Moreover, $\mathrm{Irr}(V)$ is a finite set and*

$$V = \bigcup_{Z \in \mathrm{Irr}(V)} Z.$$

Also, if E is a proper subset of $\mathrm{Irr}(V)$, then

$$V \neq \bigcup_{Z \in E} Z.$$

Proof - This follows from Theorem 13.3 and from Proposition 16.6 (see the Appendix). ■

Example 13.6 - Keep the notation of Example 13.1. Then

$$\mathrm{Irr}(\mathcal{Z}(f)) = \{\mathcal{Z}(f_1), \ldots, \mathcal{Z}(f_r)\}$$

and $\mathcal{Z}(f_i) \neq \mathcal{Z}(f_j)$ if $i \neq j$. □

13.C. Dimension. There is an intuitive notion of dimension for an algebraic set: for instance, we would like that an hypersurface in $\mathbf{A}^n(K)$ has dimension $n-1$. The following definition, which holds for any topological space, meets this requirement:

Definition 13.7. *If $\mathcal{X}$ is a topological space, we define the **dimension** of $\mathcal{X}$ (and we denote by $\dim \mathcal{X}$) to be the maximal number n such that there exists a chain $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ of non-empty irreducible closed subsets of $\mathcal{X}$.*

Theorem 13.8. *Let $V \in \mathrm{Aff}(K)$. Then:*

(a) $\dim V = \mathrm{Krulldim}\, K[V]$.

(b) *If $x_1, \ldots, x_m$ are algebraically independent elements of $K[V]$ such that $K[V]$ is integral over $K[x_1, \ldots, x_m]$ (such a family exists by Noether's Normalization Theorem), then $\dim V = m$.*

Proof - This follows from Theorems 13.3 (c) and 17.5 and from Proposition 17.3 (see the Appendix). ■

Corollary 13.9. $\dim \mathbf{A}^n(K) = n$.

Note also that, if $V \in \mathrm{Aff}(K)$, then

$$\dim V = \sup_{Z \in \mathrm{Irr}(\mathcal{X})} \dim Z. \tag{13.10}$$

EXAMPLE 13.11 - Keep the notation of Example 13.1. Then it follows from the proof of Noether's Normalization Theorem that $\dim \mathcal{Z}(f) = n - 1$. □

13.D. Tangent space. If $v \in \mathbf{A}^n(K)$ and if $f \in K[X_1, \ldots, X_n]$, we denote by $d_v f : K^n \to K$ the differential of f at v: it is a linear form. We have

$$d_v f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(v) x_i. \tag{13.12}$$

Now, let V be an algebraic subset of $\mathbf{A}^n(K)$ and let $v \in V$.

Definition 13.13. *A vector $x \in K^n$ is called a **tangent vector to** V **at** v if, for all $f \in \mathcal{I}(V)$, $d_v f(x) = 0$. The **tangent space** of V at v is the set of tangent vectors to V at v. It will be denoted by $T_v(V)$.*

We have, by definition,

$$T_v(V) = \bigcap_{f \in \mathcal{I}(V)} \operatorname{Ker} d_v f. \tag{13.14}$$

In particular,

$$T_v(V) \text{ is a vector space.} \tag{13.15}$$

Also, if W is an algebraic subset of V containing v, then

$$T_v(W) \subseteq T_v(V). \tag{13.16}$$

(Indeed, $\mathcal{I}(V) \subseteq \mathcal{I}(V)$.) Note also that

$$T_v(\mathbf{A}^n(K)) = K^n. \tag{13.17}$$

The next proposition gives an efficient way for computing the tangent space of V at v:

Proposition 13.18. *Let $v \in V$ and let E be a set of generators of the ideal $\mathcal{I}(V)$. Then*

$$T_v(V) = \bigcap_{f \in E} \operatorname{Ker} d_v f.$$

REMARK - Since $\mathcal{I}(V)$ is finitely generated, if one can find a finite set of generators of $\mathcal{I}(V)$, then the computation of the tangent space of V at v is reduced to solving a finite system of linear equations. □

PROOF - Let $x \in \bigcap_{f \in E} \operatorname{Ker} d_v f$ and let $g \in \mathcal{I}(V)$. By definition, we only need to show that $d_v g(x) = 0$. Since $g \in \mathcal{I}(V)$, there exists $f_1, \ldots, f_r \in E$ and $g_1, \ldots, g_r \in K[X_1, \ldots, X_n]$ such that $g = g_1 f_1 + \cdots + g_r f_r$. Since $f_i(v) = 0$ for all i, we have $d_v g = g_1(v) d_v f_1 + \cdots + g_r(v) d_v f_r$, whence the result. ■

EXAMPLE 13.19 - Let $V = \mathcal{Z}(Y^2 - X^3)$ and let $v = (a, b) \in V$. We shall compute the tangent space of V at v. First, note that $\mathcal{I}(V) = \langle Y^2 - X^3 \rangle$. Therefore, $(x, y) \in T_v(V)$ if and only if $3a^2 x - 2by = 0$. So, if $v = (0, 0)$, then $\dim T_v(V) = 2$ and, if $v \neq (0, 0)$, then a and b are not 0 so $3a^2$ and $2b$ cannot be both zero (even in positive characteristic) so $\dim T_v(V) = 1$ in this case. □

If $f_1,\dots,\ f_r \in K[X_1,\dots,X_n]$ and if $v \in \mathbf{A}^n(K)$, we define the *Jacobian matrix of* $(f_1,\dots,f_r)$ *at* v to be the matrix

$$J_v(f_1,\dots,f_r) = \Big(\frac{\partial f_i}{\partial X_j}(v)\Big)_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant n}}.$$

Then, if $v \in V$ and $\mathcal{I}(V) = \langle f_1,\dots,f_r\rangle$, then

$$\textbf{(13.20)} \qquad T_v(V) = \operatorname{Ker} J_v(f_1,\dots,f_r) = \{(x_1,\dots,x_n) \in K^n \mid J_v(f_1,\dots,f_r)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0\}.$$

We shall now define the differential of a morphism of algebraic sets. Before, we must define the differential of a regular map. So let $f \in K[V]$ and let $v \in V$. If $\tilde{f}$ and $\tilde{f}'$ are two elements of $K[X_1,\dots,X_n]$ which represent f, and if $x \in T_v(V)$, then $d_v\tilde{f}(x) = d_v\tilde{f}'(x)$ by definition of $T_v(V)$. So we can define the *differential of* f *at* v to be the map

$$\begin{array}{rccc} d_vf: & T_v(V) & \longrightarrow & K \\ & x & \longmapsto & d_v\tilde{f}(x). \end{array}$$

It is a linear form that is, an element of the dual of $T_v(V)$.

Proposition 13.21. *Let $W \subseteq \mathbf{A}^m(K)$ be an algberaic set and let $\varphi : V \to W$, $v \mapsto (\varphi_1(v),\dots,\varphi_m(v))$ be a morphism of algebraic sets with $\varphi_i \in K[V]$. Let $v \in V$. Then:*

(a) *If $x \in T_v(V)$, then $(d_v\varphi_1(x),\dots,d_v\varphi_m(x)) \in T_{\varphi(v)}(W)$.*
(b) *Let $d_v\varphi : T_v(V) \to T_{\varphi(v)}(W)$, $x \mapsto (d_v\varphi_1(x),\dots,d_v\varphi_m(x))$. Then $d_v\varphi$ is K-linear. It is called the* ***differential of*** φ ***at*** v.
(c) *If $\psi : W \to X$ is a morphism of algebraic sets, then $d_v(\psi\circ\varphi) = d_{\varphi(v)}\psi \circ d_v\varphi$.*

Proof - Only (a) needs a proof, the other statements being straightforward. Let $f \in \mathcal{I}(W)$. Let $\tilde{\varphi}_1,\dots,\ \tilde{\varphi}_n$ be elements of $K[X_1,\dots,X_n]$ representing $\varphi_1,\dots,\ \varphi_n$ respectively. Now, let $g = f(\tilde{\varphi}_1(X_1,\dots,X_n),\dots,\tilde{\varphi}_m(X_1,\dots,X_m)) \in K[X_1,\dots,X_n]$. Then, for all $v \in V$, we have $g(v) = f(\varphi(v)) = 0$, so $g \in \mathcal{I}(V)$. In particular, $d_vg(x) = 0$. But

$$d_vg(x) = (d_{\varphi(v)}f)(d_v\varphi_1(x),\dots,d_v\varphi_m(x)) = 0,$$

as desired. ■

Corollary 13.22. *Let $\varphi : V \to W$ be an isomorphism of algebraic sets. Then $d_v\varphi$ is an isomorphism of vector spaces for all $v \in V$.*

The next problem, still unsolved, is particularly difficult:

> **Jacobian Conjecture.** *Assume that K is an algebraically closed field of characteristic 0. Let $\varphi : \mathbf{A}^n(K) \to \mathbf{A}^n(K)$ be a morphism of algebraic sets such that $d_v\varphi$ is an isomorphism of vector spaces. Then φ is an isomorphism of algebraic sets.*

EXAMPLE 13.23 - Let V be the hyperbola $\mathcal{Z}(XY-1)$ and let $\varphi : V \to V$, $(x,y) \mapsto (x^2, y^2)$. Assume here that K has characteristic different from 2. Then $T_v(V)$ has dimension 1 and $d_v\varphi$ is an isomorphism of vector spaces for all $v \in V$. However, φ is not an isomorphism of affine varieties. □

13.E. Smoothness. We shall define the notion of smooth affine algebraic variety. For this, we need to obtain a description of the tangent space of V at v in algebraic terms.

So we fix an algebraic set V and a point $v \in V$. If $x \in T_v(V)$, then the map $\partial_v^x : K[V] \to K$, $f \mapsto (d_v f)(x)$ is well-defined and satisfies

$$\partial_v^x(fg) = f(v)\partial_v^x(g) + g(v)\partial_v^x(f). \tag{13.24}$$

In particular, $\mathfrak{m}_v^2$ is contained in the kernel of ∂_v^x. We shall denote by $\tilde{\partial}_v^x : \mathfrak{m}_v/\mathfrak{m}_v^2 \to K$ the map induced by ∂_v^x. So we have constructed a map

$$\begin{array}{rccc} \tilde{\partial}_v : & T_v(V) & \longrightarrow & (\mathfrak{m}_v/\mathfrak{m}_v^2)^* \\ & x & \longmapsto & \tilde{\partial}_v^x. \end{array}$$

It is readily seen to be K-linear. In fact:

Proposition 13.25. *The map $\tilde{\partial}_v : T_v(V) \longrightarrow (\mathfrak{m}_v/\mathfrak{m}_v^2)^*$ is an isomorphism of K-vector spaces.*

PROOF - Let $x \in T_v(V)$ be such that $\tilde{\partial}_v^x = 0$. Then, since $d_v f(x) = 0$ for all constant functions, we have that $d_v f(x) = 0$ for all $f \in K[V]$. Now, if $\tilde{f} \in K[X_1, \ldots, X_n]$, then $d_v\tilde{f}(x) = d_v f(x) = 0$ (where f denotes the image of $\tilde{f}$ in $K[V] = K[X_1, \ldots, X_n]/\mathcal{I}(V)$). In other words,

$$\sum_{i=1}^{n} x_i \frac{\partial P}{\partial X_i}(v) = 0$$

for all $P \in K[X_1, \ldots, X_n]$. If we apply this equality for $P = X_i$, we get that $x_i = 0$ for all i, so $x = 0$. Hence $\tilde{\partial}_v$ is injective.

Now, let us show that $\tilde{\partial}_v$ is surjective. Let $\tau : (\mathfrak{m}_v/\mathfrak{m}_v^2) \to K$ be K-linear. Write $v = (a_1, \ldots, a_n)$ and denote by $\mathcal{X}_i : V \to K$ the image of X_i. Then $\mathcal{X}_i - a_i \in \mathfrak{m}_v$ and we denote by x_i the image, via τ, of the projection of $\mathcal{X}_i - a_i$ on $\mathfrak{m}_V/\mathfrak{m}_v^2$. Let $x = (x_1, \ldots, x_n)$. We shall prove that $x \in T_v(V)$ and that $\tilde{\partial}_v^x = \tau$. First, let $\tau^+ : K[X_1, \ldots, X_n] \to K$, $P \mapsto \tau(\overline{P - P(v)})$, where $\overline{P - P(v)}$ denotes the image of $P - P(v)$ in $\mathfrak{m}_v/\mathfrak{m}_v^2$. Then it is readily seen that $\tau^+(PQ) = P(v)\tau^+(Q) + Q(v)\tau^+(P)$. To prove our claim, we only need to show that $d_v P(x) = \tau(P)$ for all P. By the previous equality, we only need to prove it for $P = X_i$, but this is just the definition of τ. ■

We define the *Zariski tangent space* of V at v to be the dual of $\mathfrak{m}_v/\mathfrak{m}_v^2$. Note that, by the previous proposition, the Zariski tangent space is canonically isomorphic to $T_v(V)$, so that in particular it has finite dimension. We shall explain now why the isomorphism $\tilde{\partial}_v$ is "functorial". We first need some notation: if $\varphi : V \to W$ is a morphism of algebraic sets and if $v \in V$, then $\varphi^{*-1}(\mathfrak{m}_v^V) = \mathfrak{m}_{\varphi(v)}^W$ (see Proposition 11.34). In other words, $\varphi^*(\mathfrak{m}_{\varphi(v)}^W) \subseteq \mathfrak{m}_v^V$. This also implies that $\varphi^*((\mathfrak{m}_{\varphi(v)}^W)^2) \subseteq (\mathfrak{m}_v^V)^2$. Therefore, φ^* induces a

K-linear map $\varphi_v^* : \mathfrak{m}_{\varphi(v)}^W/(\mathfrak{m}_{\varphi(v)}^W)^2 \longrightarrow \mathfrak{m}_v^V/(\mathfrak{m}_v^V)^2$. We denote by ${}^t\varphi_v^*$ its transpose. Then the diagram

(13.26)

$$\begin{array}{ccc} T_v(V) & \xrightarrow{\tilde{\partial}_v^V} & \left(\mathfrak{m}_v^V/(\mathfrak{m}_v^V)^2\right)^* \\ \Big\downarrow{\scriptstyle d_v\varphi} & & \Big\downarrow{\scriptstyle {}^t\varphi_v^*} \\ T_{\varphi(v)}(V) & \xrightarrow{\tilde{\partial}_{\varphi(v)}^W} & \left(\mathfrak{m}_{\varphi(v)}^W/(\mathfrak{m}_{\varphi(v)}^W)^2\right)^* \end{array}$$

is commutative. The proof is left as an exercise.

Theorem 13.27. *If V is an affine algebraic variety and if $v \in V$, we have* $\dim T_v(V) = \dim \mathfrak{m}_v/\mathfrak{m}_v^2 \geqslant \operatorname{Krulldim} K[V] = \dim V$.

PROOF - See any good book dealing with "Commutative Algebra" (Matsumura, or Atiyah-McDonald...). We shall prove it only in the case where V is an hypersurface (see Example 13.1). So we assume that $V = \mathcal{Z}(f)$, where f is an irreducible polynomial in $K[X_1, \ldots, X_n]$. Then $\dim V = n - 1$ by Example 13.11 and, since $\mathcal{I}(V) = \langle f \rangle$, we have $\dim T_v(V) = \operatorname{Ker} d_v f$ by Proposition 13.18. This shows the result. ■

Definition 13.28. *If V is an affine algebraic variety and if $v \in V$, we say that V is* ***smooth at*** *v (or that v is a* ***regular*** *or* ***smooth*** *point of V) if* $\dim T_v(V) = \dim V$. *The variety V is said to be* ***smooth*** *(or* ***non-singular****, or* ***regular****) if it is smooth at each of its points.*

We denote by $\operatorname{Sing}(V)$ *the set of singular points of V.*

Theorem 13.29. *If V is an affine algebraic variety, then* $\operatorname{Sing}(V)$ *is a closed subset of V and $V \setminus \operatorname{Sing}(V)$ is not empty.*

PROOF - Let $f_1, \ldots, f_r$ be a set of generators of the ideal $\mathcal{I}(V)$. Then $T_v(V)$ is the kernel of the Jacobian $J_v(f_1, \ldots, f_r)$. By Theorem 13.27, we know that the rank of this matrix is always greater than or equal to $n - \dim V$. And $v \in \operatorname{Sing}(V)$ if and only if this rank is $< n - \dim V$. But this last condition is then equivalent to the vanishing of all determinant of submatrices of $J_v(f_1, \ldots, f_r)$ of size $(n - \dim V) \times (n - \dim V)$. So $\operatorname{Sing}(V)$ is a closed subset of V.

We shall prove the second statement only whenever V is an hypersurface (for the general case, see R. HARTSHORNE, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Part I, Theorem 5.3). So assume that $V = \mathcal{Z}(f)$, where f is an irreducible polynomial of $K[X_1, \ldots, X_n]$ and assume that $V = \operatorname{Sing}(V)$. By the proof of Theorem 13.27, this means that we have $d_v f = 0$ for all $v \in V$. In other words, $\dfrac{\partial f}{\partial X_i}(v) = 0$ for all i and all $v \in V$. Since $\mathcal{I}(\mathcal{Z}(f)) = \langle f \rangle$, this implies that $\dfrac{\partial f}{\partial X_i} = 0$ for all i. If K has characteristic 0, this is impossible. Assume that K has positive characteristic p. Then this means that f is

a polynomial in $X_1^p, \ldots, X_n^p$. So f is the p-th power of some polynomial, so f is not irreducible: we also get a contradiction. ■

14. Examples

We shall need in the sequel the following theorem:

Theorem 14.1. *Let $\varphi : V \to W$ be a morphism of algebraic sets and assume that V is irreducible. Let $r = \dim V - \dim \overline{\varphi(V)}$. Then $\varphi(V)$ and $\overline{\varphi(V)}$ are irreducible and there exists an open subset U of $\overline{\varphi(V)}$ such that:*

(a) *$U \subseteq \varphi(V) \subseteq \overline{\varphi(V)}$;*
(b) *$U \neq \varnothing$;*
(c) *For all $x \in U$, $\dim \varphi^{-1}(x) = r$.*

Example 14.2 - Let $P \in K[X_1, \ldots, X_{n-1}]$ and let

$$V = \{(x_1, \ldots, x_n) \in \mathbf{A}^n(K) \mid x_n = P(x_1, \ldots, x_{n-1})\}$$

Then V is an hypersurface in $\mathbf{A}^n(K)$ (indeed, $X_n - P(X_1, \ldots, X_{n-1})$ is irreducible) and the map $\pi : V \to \mathbf{A}^{n-1}(K)$, $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-1})$ is an isomorphism (its inverse is given by $(x_1, \ldots, x_{n-1}) \mapsto (x_1, \ldots, x_{n-1}, P(x_1, \ldots, x_{n-1}))$. □

Example 14.3 - Let $P \in K[X]$ and let $\mathcal{C} = \{(x, y) \in \mathbf{A}^2(K) \mid y^2 = P(x)\}$. We assume that P is not the square of a polynomial in $K[X]$. We also assume that the characteristic of K is different from 2. Then $Y^2 - P(X)$ is irreducible, so $\mathcal{I}(\mathcal{C}) = \langle Y^2 - P(X)\rangle$ by Hilbert's Nullstellensatz and $\mathcal{C}$ is an affine curve (i.e. an affine variety of dimension 1). A point $(x, y) \in \mathcal{C}$ is singular if and only if $2y = P'(x) = 0$. In other words,

$$\mathrm{Sing}(\mathcal{C}) = \{(x, 0) \mid P(x) = P'(x) = 0\}.$$

So

$\mathcal{C}$ is smooth if and only if P and P' are relatively prime. □

Example 14.4 - If $a \in K^\times$ and $b \in K$, we denote by $\sigma_{a,b} : \mathbf{A}^1(K) \to \mathbf{A}^1(K)$, $x \mapsto ax + b$. Let $\mathcal{A} = \{\sigma_{a,b} \mid a \in K^\times,\ b \in K\}$. Then $\mathcal{A}$ is a subgroup of $\mathrm{Aut}(\mathbf{A}^1(K))$, the group of automorphisms of $\mathbf{A}^1(K)$ as an affine variety. Moreover,

$$\mathcal{A} \simeq K^\times \ltimes K.$$

In fact, it is easy to check that

$$\mathcal{A} = \mathrm{Aut}(\mathbf{A}^1(K))$$

by investigating the automorphisms of the K-algebra $K[X]$. Finally, note that $\sigma_{a,b}$ is an involution if and only if $a = -1$. □

Example 14.5 - Assume that K has characteristic different from 2 and 3. Let $\mathcal{C} = \{(x, y) \in \mathbf{A}^2(K) \mid y^2 = x^3 - x + 1\}$. Then, by Example 14.3, $\mathcal{C}$ is a smooth curve. We shall prove here that $\mathcal{C}$ is not isomorphic to $\mathbf{A}^1(K)$.

First, let $\sigma : \mathcal{C} \to \mathcal{C}$, $(x, y) \mapsto (x, -y)$. Then σ is an involutive automorphism of $\mathcal{C}$. In particular, σ^* is an involutive automorphism of the K-algebra $A = K[\mathcal{C}] = K[X, Y]/(Y^2 - X^3 + X - 1)$.

So assume that that $\mathcal{C} \simeq \mathbf{A}^1(K)$. Then $K[T] \simeq A$: we denote by t the image of T in A through this isomorphism. Then, by example 14.4, there exists $b \in K$ such that $\sigma^*(t) = b - t$. If we write $t = P(\bar{X}) + \bar{Y}Q(\bar{X})$ where P and Q are (uniquely determined) polynomials in one variable and $\bar{X}$ and $\bar{Y}$ denote respectively the images of X and Y in A, then $\sigma^*(t) = P(\bar{X}) - \bar{Y}Q(\bar{X})$ so $P(\bar{X}) = b - P(\bar{X})$. This show that $P(\bar{X}) = b/2$. So, by translating the variable T, we may assume that $t = \bar{Y}Q(\bar{X})$. But $K[t] = A$, which is impossible. □

Example 14.6 - Assume that K has characteristic different from 2 and 3. Let $\mathcal{C} = \{(x, y) \in \mathbf{A}^2(K) \mid y^2 = x^3 + x^2\}$. Then $\mathcal{C}$ is not smooth: $(0, 0)$ is the unique singular point of $\mathcal{C}$. Let $\varphi : \mathbf{A}^1(K) \to \mathcal{C}$, $t \mapsto (t^2 - 1, t(t^2 - 1))$. Then φ is a surjective morphism of varieties. Let $A = K[\mathcal{C}]$. Then $\varphi^* : A \hookrightarrow K[T]$, and $K[T]$ is contained in the field of fractions of A (indeed, $\varphi^*(\bar{Y}/\bar{X}) = T$). In fact, $K[T]$ is the normalization of A. □

Example 14.7 - Let A and B be the matrices in $\mathbf{GL}_2(\mathbb{C})$ equal to

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let $C = AB$. Then

$$AB = -BA = C, \quad BC = -CB = A \quad \text{and} \quad CA = -AC = B.$$

Also

$$A^2 = B^2 = C^2 = -I,$$

where I is the identity matrix. This shows that

$$G = \langle A, B \rangle = \{I, -I, A, -A, B, -B, C, -C\}.$$

It is called the *quaternion group of order* 8. Then G acts on $\mathbf{A}^2(\mathbb{C})$ by matrix multiplication. It is readily seen that the polynomials

$$u = X^4 + Y^4, \quad v = X^2Y^2 \quad \text{and} \quad w = XY(X^4 - Y^4)$$

are elements of $\mathbb{C}[X, Y]^G$. Moreover, $w^2 = v(u^2 - 4v^2)$. In particular, the morphism of algebras $\mathbb{C}[U, V, W] \to \mathbb{C}[X, Y]^G$, $U \mapsto u$, $V \mapsto v$, $W \mapsto w$ induces a well-defined morphism of $\mathbb{C}$-algebras

$$\pi^* : \mathbb{C}[U, V, W]/\langle W^2 - V(U^2 - 4V^2)\rangle \to \mathbb{C}[X, Y]^G.$$

It turns out that π^* is an isomorphism of algebras.

In other words, $\mathbf{A}^2(\mathbb{C})/G$ is isomorphic to the variety $\{(a, b, c) \in \mathbf{A}^3(\mathbb{C}) \mid c^2 = b(a^2 - 4b^2)\}$. Its only singular point is $(0, 0, 0)$. □

Example 14.8 - Let $V = \mathcal{Z}(Z^2 - XY^2)$. The polynomial $Z^2 - XY^2$ being irreducible, V is an hypersurface and $\mathcal{I}(V) = \langle Z^2 - XY^2 \rangle$. In particular, $\mathrm{Sing}(V) = \mathcal{Z}(Y, Z)$.

Let $a \in K$. Then $V \cap \mathcal{Z}(X - a)$ is the union of two lines if $a \neq 0$. Also $V \cap \mathcal{Z}(Y - a)$ is a parabola if $a \neq 0$. And $V \cap \mathcal{Z}(Z - a)$ is isomorphic to $\mathcal{Z}(XY^2 - a^2) \subseteq \mathbf{A}^2(K)$: it is smooth except if $a \neq 0$. □

EXAMPLE 14.9 - Let p be the characteristic of K and assume that $p > 0$. Let q be a power of p and let $\mathbb{F}_q = \{x \in K \mid x^q = x\}$: it is the unique subfield of cardinal q. Then the additive finite group $\mathbb{F}_q$ acts on $\mathbf{A}^1(K)$ by translation (an element $\xi \in \mathbb{F}_q$ acts through $t \mapsto t + \xi$). Then the map $\pi : \mathbf{A}^1(K) \to \mathbf{A}^1(K)$, $t \mapsto t^q - t$ is a quotient of $\mathbf{A}^1(K)$ by the action of $\mathbb{F}_q$ (see the Homework).

Proposition 14.10. *Let C be a smooth affine variety of dimension 1 (a smooth affine curve) and let G be a finite group acting on C. Assume that $C/G \simeq \mathbf{A}^1(K)$ and that, for all $g \in G$, $g \neq 1$, we have $g(v) \neq v$ for all $v \in C$. Then G is generated by its Sylow p-subgroups.*

More astonishing is the following result, which can be seen as an inverse Galois problem for the affine line in positive characteristic:

Theorem 14.11 (Raynaud). *Let G be a finite group generated by its Sylow p-subgroups. Then there exists a smooth affine curve C endowed with an action of G and such that:*

(1) *$C/G \simeq \mathbf{A}^1(K)$;*
(2) *For all $g \in G$, $g \neq 1$ and for all $v \in C$, we have $g(v) \neq v$.*

SUB-EXAMPLE - The finite group $\mathbf{SL}_2(\mathbb{F}_q)$ is generated by its Sylow p-subgroups (check it!). So there must exists a smooth affine curve C endowed with an action of $\mathbf{SL}_2(\mathbb{F}_q)$ satisfying the requirements in Raynaud's Theorem. An example is given in Exercise IV.7 (Deligne-Lusztig curve). □

EXAMPLE 14.12 - Identify $\mathrm{Mat}_n(K)$ with $\mathbf{A}^{n^2}(K)$. Let $\mathcal{N}_n$ be the set of nilpotent matrices in $\mathrm{Mat}_n(K)$. In fact,

$$\mathcal{N}_n = \{M \in \mathrm{Mat}_n(K) \mid M^n = 0\}. \tag{14.13}$$

In particular, $\mathcal{N}_n$ is an algebraic set.

Let $\mathbf{SL}_n(K) = \{M \in \mathrm{Mat}_n(K) \mid \det M = 1\}$ and $\mathbf{N}_n(K)$ be the set of triangular nilpotent matrices in $\mathrm{Mat}_n(K)$. Then $\mathbf{N}_n(K) \simeq \mathbf{A}^{n(n-1)/2}(K)$ is irreducible. Also, the polynomial $\det - 1$ is irreducible, so $\mathbf{SL}_n(K)$ is an hypersurface in $\mathrm{Mat}_n(K)$ (in particular, it is irreducible). Now, the map

$$\begin{array}{rccc} \varphi : & \mathbf{SL}_n(K) \times \mathbf{N}_n(K) & \longrightarrow & \mathcal{N}_n \\ & (g, M) & \longmapsto & gMg^{-1} \end{array}$$

is a morphism of algebraic sets (indeed, the map $\mathbf{SL}_n(K) \to \mathbf{SL}_n(K)$, $g \mapsto g^{-1}$ is polynomial). The map is surjective by Jordan decomposition. So, by Exercise IV.1,

$$\mathcal{N}_n \text{ is irreducible.} \tag{14.14}$$

If $M \in \mathrm{Mat}_n(K)$, we denote by $\sigma_1(M), \ldots, \sigma_n(M)$ the coefficients of $X^{n-1}, \ldots, X$, 1 respectively in the characteristic polynomial of M ($\sigma_1 = \pm \mathrm{Tr}$ and $\sigma_n = \pm \det$). Then the map

$$\begin{array}{rccc} \sigma : & \mathrm{Mat}_n(K) & \longrightarrow & \mathbf{A}^n(K) \\ & M & \longmapsto & (\sigma_1(M), \ldots, \sigma_n(M)) \end{array}$$

is a morphism of algebraic sets. It is surjective. Moreover,

$$\mathcal{N}_n = \sigma^{-1}(0). \tag{14.15}$$

Let $J_n = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix}$. We denote by $\mathcal{P}(n)$ the set of partitions of n, i.e. the set of finite sequences $\lambda = (\lambda_1, \dots, \lambda_r)$ of natural numbers such that $\lambda_1 + \dots + \lambda_r = n$ and $\lambda_1 \geqslant \lambda_2 \geqslant \dots \geqslant \lambda_r \geqslant 1$. We denote by J_λ the matrix which is diagonal by blocks, the blocks being equal to $J_{\lambda_1}, \dots, J_{\lambda_r}$. Finally, we denote by $\mathcal{C}_\lambda$ the orbit of J_λ under the action (by conjugacy) of $\mathbf{SL}_n(K)$: $\mathcal{C}_\lambda = \{gJ_\lambda g^{-1} \mid g \in \mathbf{SL}_n(K)\}$. Then, by Jordan decomposition,

$$\mathcal{N}_n = \bigcup_{\lambda \in \mathcal{P}(n)} \mathcal{C}_\lambda, \tag{14.16}$$

and this is the partition of $\mathcal{N}_n$ into $\mathbf{SL}_n(K)$-orbits. If $\lambda \in \mathcal{P}(n)$, the closure of $\mathcal{C}_\lambda$ is stable under the action of $\mathbf{SL}_n(K)$, We then define a relation $\trianglelefteq$ on $\mathcal{P}(n)$ as follows:

$$\lambda \trianglelefteq \mu \Longleftrightarrow \mathcal{C}_\lambda \subseteq \overline{\mathcal{C}_\mu} \quad (\Longleftrightarrow \overline{\mathcal{C}_\lambda} \subseteq \overline{\mathcal{C}_\mu}).$$

We also define a morphism of varieties

$$\begin{array}{rccc} \varphi_\lambda : & \mathbf{SL}_n(K) & \longrightarrow & \mathcal{N}_n \\ & g & \longmapsto & gJ_\lambda g^{-1} \end{array}$$

Then the image of φ_λ is $\mathcal{C}_\lambda$, so

$$\mathcal{C}_\lambda \text{ and } \overline{\mathcal{C}_\lambda} \text{ are irreducible subsets of } \mathcal{N}_n. \tag{14.17}$$

Moreover,

$$\mathcal{C}_\lambda \text{ is an open subset of } \overline{\mathcal{C}_\lambda}. \tag{14.18}$$

Indeed, by Theorem 14.1, there exists a non-empty open subset U of $\overline{\mathcal{C}_\lambda}$ containing the image of φ_λ (which is $\mathcal{C}_\lambda$). Then $\mathcal{C}_\lambda = \bigcup_{g \in \mathbf{SL}_n(K)} gUg^{-1}$ is still open in $\overline{\mathcal{C}_\lambda}$.

Theorem 14.19. *Let λ, $\mu \in \mathcal{P}(n)$. Then:*

(a) *$\mathcal{C}_\lambda$ is an open irreducible subset of the irreducible closed set $\overline{\mathcal{C}_\lambda}$.*
(b) $\dim \mathcal{C}_\lambda = n^2 - 1 - \dim C_{\mathbf{SL}_n(K)}(J_\lambda)$.
(c) *If $\lambda \lhd \mu$, then $\dim \mathcal{C}_\lambda < \dim \mathcal{C}_\mu$.*
(d) *$\trianglelefteq$ is a partial order on $\mathcal{P}(n)$.*
(e) $\mathcal{C}_n = \{M \in \mathcal{N}_n \mid M^{n-1} \neq 0\}$.
(f) *$\mathcal{C}_n$ is open and dense in $\mathcal{N}_n$.*
(g) $\dim \mathcal{N}_n = n^2 - n$.
(h) *If $M \in \mathcal{C}_n$, then M is a smooth point of $\mathcal{N}_n$.*
(i) *Let $\lambda = (\lambda_1, \dots, \lambda_r)$ and $\mu = (\mu_1, \dots, \mu_s)$ be two partitions of n. Then $\lambda \trianglelefteq \mu$ if and only if $\lambda_1 + \dots + \lambda_i \leqslant \mu_1 + \dots + \mu_i$ for all $\geqslant 1$ (here, by convention, $\lambda_{r+1} = \lambda_{r+2} = \dots = \mu_{s+1} = \mu_{s+2} = \dots = 0$).*

15. Localization

If $\mathcal{X}$ is a set, we denote by $\mathrm{Maps}(\mathcal{X}, K)$ the set of maps $\mathcal{X} \to K$: this is a K-algebra.

15.A. Regular functions on open subsets. Let V be an algebraic set, let U be an open subset of V and let $x \in U$. A map $f : U \to K$ is called *regular at* x if there exists an open subset U' of U containing x and two regular functions P, $Q \in K[V]$ such that Q does not vanish on U' and $f(y) = P(y)/Q(y)$ for all $y \in U'$. A map $f : U \to K$ is called *regular* if it is regular at all elements of U. We denote by $\mathcal{O}_V(U)$ the set of regular functions on U. It is clearly a commutative K-subalgebra of $\mathrm{Maps}(U, K)$.

Remark - If $U = V$, we have defined two notions of regular functions on V: this one and the one defined in §11.C. We shall prove in Corollary 15.2 that these notions coincide, i.e. that $\mathcal{O}_V(V) = K[V]$ (note that it is clear from the definitions that $K[V] \subseteq \mathcal{O}_V(V)$). □

If $f \in K[V]$, we denote by $V_f = \{x \in V \mid f(x) \neq 0\}$. By definition, V_f is an open subset of V (it is the complement of $\mathcal{Z}_V(f)$ in V): it is called a *principal open subset* of V. Since any closed subset is a finite intersection of some $\mathcal{Z}_V(f)$, any open subset is a finite union of principal open subsets.

Since $K[V]$ is reduced, f is not nilpotent. If $f \neq 0$, we shall denote by $K[V]_f$ the localization of $K[V]$ at the multiplicative set $\{f^n \mid n \geqslant 0\}$ (this last set does not contain 0). In other words, $K[V]_f = K[V][1/f] \simeq K[V][T]/\langle 1 - Tf \rangle$.

Proposition 15.1. *Let $f \in K[V]$, $f \neq 0$. Then $\mathcal{O}_V(V_f) \simeq K[V]_f$.*

Proof - See Hartshorne. ■

Corollary 15.2. $\mathcal{O}_V(V) = K[V]$.

Proof - Apply the Proposition 15.1 to $f = 1$. ■

15.B. Sheaves of functions. If $X \subseteq X'$ are two sets and if $f : X' \to K$ is a map, we denote by $f|_X$ (or $\mathrm{Res}_X f$, or $\mathrm{Res}_X^{X'} f$) the restriction of f to X.

If $\mathcal{X}$ is a topological space, a *sheaf of functions* on $\mathcal{X}$ (with values in K) is a collection $\mathcal{F} = (\mathcal{F}(\mathcal{U}))_{\mathcal{U} \text{ open in } \mathcal{X}}$ such that, for all open subsets $\mathcal{U}$ of $\mathcal{X}$, $\mathcal{F}(\mathcal{U}) \subseteq \mathrm{Maps}(\mathcal{U}, K)$ and satisfying the following axioms:

- (S1) If $\mathcal{U} \subseteq \mathcal{U}'$ are two open subsets of $\mathcal{X}$ and if $f \in \mathcal{F}(\mathcal{U}')$, then $f|_{\mathcal{U}} \in \mathcal{F}(\mathcal{U}, K)$.
- (S2) If $(\mathcal{U}_i)_{i \in I}$ is a family of open subsets of $\mathcal{X}$ and if $f \in \mathrm{Maps}(\mathcal{U}, K)$ (where $\mathcal{U}$ is the union of the $\mathcal{U}_i$'s) is such that $f|_{\mathcal{U}_i} \in \mathcal{F}(\mathcal{U}_i)$ for all i, then $f \in \mathcal{F}(\mathcal{U})$.

If $\mathcal{F}$ is a sheaf of functions on $\mathcal{X}$, we say that $\mathcal{F}$ is a *sheaf of K-vector spaces* (respectively a *sheaf of K-algebras*) if, for all open subsets $\mathcal{U}$ of $\mathcal{X}$, $\mathcal{F}(\mathcal{U})$ is a K-vector subspace (respectively a K-subalgebra) of $\mathrm{Maps}(\mathcal{U}, K)$.

Example 15.3 - (0) $(\mathrm{Maps}(U, K))_{U \text{ open in } \mathcal{X}}$ is a sheaf of functions on $\mathcal{X}$.

(1) Assume that K is endowed with a topology (for instance the usual topology if $K = \mathbb{R}$ or $\mathbb{C}$, or the Zarisky topology, or the p-adic topology if K is an algebraic extension of $\mathbb{Q}_p$), then the collection $(\mathrm{Cont}(\mathcal{U}, K))_{\mathcal{U} \text{ open in } \mathcal{X}}$ is a sheaf (where $\mathrm{Cont}(\mathcal{U}, K)$ denotes the set of continuous functions on $\mathcal{U}$).

(2) If V is an algebraic set, then $\mathcal{O}_V$ is a sheaf of K-algebras on V. □

A *ringed space* is a pair $(\mathcal{X}, \mathcal{O})$, where $\mathcal{X}$ is a topological space and $\mathcal{O}$ is a sheaf of algebras on $\mathcal{X}$. If $(\mathcal{X}', \mathcal{Y}')$ is another ringed space, a *morphism* from $(\mathcal{X}, \mathcal{O})$ to $(\mathcal{X}', \mathcal{O}')$ is a continuous map $\varphi : \mathcal{X} \to \mathcal{X}'$ such that, for any open subset $\mathcal{U}$ of $\mathcal{X}'$ and any $f \in \mathcal{O}'(\mathcal{U})$, the map $f \circ \varphi : \varphi^{-1}(\mathcal{U}) \to K$ belongs to $\mathcal{O}(\varphi^{-1}(\mathcal{U}))$.

Example 15.4 - If V is an algebraic set, then $(V, \mathcal{O}_V)$ is a ringed space. The sheaf $\mathcal{O}_V$ is called the *structural sheaf* on V. Moreover, if $\varphi : V \to W$ is a morphism of algebraic sets, then φ is a morphism of ringed spaces. Conversely, if $\varphi : (V, \mathcal{O}_V) \to (W, \mathcal{O}_W)$ is a morphism of ringed spaces (where V and W are two algebraic sets), then, for all $f \in K[W] = \mathcal{O}_W(W)$, we have that $f \circ \varphi \in \mathcal{O}_V(V) = K[V]$, so φ is a morphism of algebraic sets. □

Example 15.5 - Let $(\mathcal{X}, \mathcal{O})$ be a ringed space and let $\mathcal{U}$ be an open subset of $\mathcal{X}$. We denote by $\mathcal{O}|_{\mathcal{U}}$ the sheaf on $\mathcal{U}$ obtained by restriction of $\mathcal{O}$ (i.e., if $\mathcal{V} \subseteq \mathcal{U}$ is open, we set $\mathcal{O}|_{\mathcal{U}}(\mathcal{V}) = \mathcal{O}(\mathcal{V})$). Then $(\mathcal{U}, \mathcal{O}|_{\mathcal{U}})$ is a ringed space.

15.C. Variety. A *scheme of finite type* (over K) is a ringed space $(\mathcal{X}, \mathcal{O})$ satisfying the following axiom:

(Sch) There exists open subsets $\mathcal{U}_1, \ldots, \mathcal{U}_n$ of $\mathcal{X}$ such that $\mathcal{X} = \bigcup_{i=1}^n \mathcal{U}_i$ and such that, for all i, there exists an algebraic set V_i such that $(\mathcal{U}_i, \mathcal{O}|_{\mathcal{U}_i}) \simeq (V_i, \mathcal{O}_{V_i})$.

Let $(\mathcal{X}, \mathcal{O})$ and $(\mathcal{X}', \mathcal{O}')$ be two schemes of finite type over K. We shall define a topology on $\mathcal{X} \times \mathcal{X}'$ which is in general different from the product topology. Let $(\mathcal{U}_i)_{1 \leqslant i \leqslant n}$ and $(\mathcal{U}'_j)_{1 \leqslant j \leqslant m}$ be a covering of $\mathcal{X}$ and $\mathcal{X}'$ respectively satisfying the axiom (Sch). Then we endow $\mathcal{X} \times \mathcal{X}'$ with the topology generated by the open subsets of the $\mathcal{U}_i \times \mathcal{U}'_j$.

Then a scheme of finite type $(\mathcal{X}, \mathcal{O})$ is called *separated* if the image of the map $\Delta : \mathcal{X} \to \mathcal{X} \times \mathcal{X}$, $x \mapsto (x, x)$ is closed in $\mathcal{X} \times \mathcal{X}$.

*An **algebraic variety** (over K) is a scheme of finite type which is irreducible and separated. A **morphism** of algebraic varieties is a morphism of ringed spaces. A variety is called **affine** if it is isomorphic to some $(V, \mathcal{O}_V)$ where V is an irreducible algebraic set.*

15.D. Example: open subsets of varieties. Let $(V, \mathcal{O})$ be a variety and let U be an open subset of V. Then $(U, \mathcal{O}|_U)$ is a variety. Indeed, we only need to prove it whenever V is affine. Then $U = \bigcup_{i=1}^r V_{f_i}$ for some $f_i \in \mathcal{O}(V) = K[V]$, so we are reduced to prove that $(V_f, \mathcal{O}|_{V_f})$ is an affine variety for all $f \in K[V]$, $f \neq 0$. Assume that $V \subseteq \mathbf{A}^n(K)$ and let

$$W = \{(x_1, \ldots, x_n, t) \in \mathbf{A}^{n+1}(K) \mid (x_1, \ldots, x_n) \in V \text{ and } f(x_1, \ldots, x_n)t - 1 = 0\}.$$

Let $\pi : W \to V$, $(x_1, \ldots, x_n, t) \mapsto (x_1, \ldots, x_n)$. Then W is an affine algebraic set and the map π is a morphism of algebraic sets. Moreover, the image of π is equal to V_f. it is now readily seen that $\pi : W \to V_f$ is an isomorphism of ringed spaces.

EXAMPLE 15.6 - Let $\mathbf{GL}_n(K) = \{M \in \mathrm{Mat}_n(K) \mid \det(M) \neq 0\}$ viewed as an open set of the affine space $\mathrm{Mat}_n(K)$. Then $\mathbf{GL}_n(K) = \mathrm{Mat}_n(K)_{\det}$ and it is readily seen that the maps

$$\begin{array}{ccc} \mathbf{GL}_n(K) \times \mathbf{GL}_n(K) & \longrightarrow & \mathbf{GL}_n(K) \\ (M, N) & \longmapsto & MN \end{array}$$

$$\begin{array}{ccc} \mathbf{GL}_n(K) & \longrightarrow & \mathbf{GL}_n(K) \\ M & \longmapsto & M^{-1} \end{array}$$

are morphisms of varieties (the last one is an isomorphism). □

15.E. Example: projective varieties. We denote by $K[X_0, X_1, \ldots, X_n]_h$ the set of homogeneous polynomials in $K[X_0, X_1, \ldots, X_n]$. If $E \subseteq K[X_0, X_1, \ldots, X_n]_h$, we set

$$\mathcal{Z}_h(E) = \{[x_0, x_1, \ldots, x_n] \in \mathbf{P}^n(K) \mid \forall\ f \in E,\ f(x_0, x_1, \ldots, x_n) = 0\}.$$

Then the map $\mathcal{Z}_h$ shares almost the same properties as the map $\mathcal{Z}$: in particular, if we define a *projective algebraic set* as an element of the image of $\mathcal{Z}_h$, then projective algebraic sets are the closed subsets of some topology on $\mathbf{P}^n(K)$, the *Zariski topology* on $\mathbf{P}^n(K)$.

If $V \subseteq \mathbf{P}^n(K)$ is a projective algebraic set and if U is an open subset of V, then a map $f : U \to K$ is called *regular* if, for all $x \in U$, there exists an open subset U' of U and two ***homogeneous*** polynomials P and Q ***of the same degree*** such that $Q(v) \neq 0$ for all $u \in U'$ and $f(u) = P(u)/Q(u)$ for all $u \in U'$. This defines a sheaf $\mathcal{O}_V$ on V.

We denote by $\mathbf{A}^n_{(i)}(K)$ the subset of $\mathbf{P}^n(K)$ consisting of the $[x_0, x_1, \ldots, x_n]$ such that $x_i \neq 0$. Then the map $\mathbf{A}^n(K) \to \mathbf{A}^n_{(i)}(K)$, $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n)$ is an homeomorphism.

If $V = \mathcal{Z}_h(E) \subseteq \mathbf{P}^n(K)$, let $V_{(i)} = V \cap \mathbf{A}^n_{(i)}(K)$. Then $V = \bigcup_{i=0}^n V_{(i)}$ and $(V_{(i)}, \mathcal{O}_V|_{V_{(i)}})$ is an affine variety (it is isomorphic to $\mathcal{Z}(E_{(i)})$, where

$$E_{(i)} = \{f(X_1, \ldots, X_{i-1}, 1, X_i, \ldots, X_n) \mid f \in E\} \quad).$$

In fact,

(15.7) $(V, \mathcal{O}_V)$ *is a separated scheme of finite type.*

A variety is called *projective* if it is isomorphic to some $(V, \mathcal{O}_V)$ where V is an irreducible projective algebraic set.

Exercises from Part III

In all these exercises, we assume that ***K is algebraically closed.***

Exercise IV.1. Let $f : \mathcal{X} \to \mathcal{Y}$ be a continuous map between topological spaces. Show that $f(\mathcal{X})$ is an irreducible subset of $\mathcal{Y}$.

Exercise IV.2. Let $\mathcal{X}$ be a topological space and let $\mathcal{Y}$ be an irreducible subset of $\mathcal{X}$. Show that $\overline{\mathcal{Y}}$ is irreducible.

Exercise IV.3. Find the irreducible components of the following algebraic sets:

(a) $\mathcal{Z}(X^2 + Y^2 - 5, XY - 2)$.
(b) $\mathcal{Z}(X^2 - Y^2)$.
(c) $\mathcal{Z}(X^2 - YZ, XZ - X)$.

Exercise IV.4. Let $\varphi : \mathbf{A}^1(K) \to \mathbf{A}^3(K)$, $t \mapsto (t^3, t^4, t^5)$. Let V denote the image of φ.

(a) Show that φ is a morphism of varieties.
(b) Show that $\mathcal{I}(V) = (X^3 - YZ, Y^2 - XZ, Z^2 - X^2Y)$ and that $V = \mathcal{Z}(\mathcal{I}(V))$ (in other words, $V = \overline{V}$).
(c) Show that $\dim V = 1$.
(d) Show that $\mathcal{I}(V)$ cannot be generated by two elements.
(e) Show that V is irreducible.

Exercise IV.5. Determine the set $\mathrm{Sing}(V)$ in the following cases:

(a) $V = \mathcal{Z}(Y^2 - X^3 - X^2)$.
(b) $V = \mathcal{Z}(Z^2 - X^2 - Y^2)$.
(c) $V = \mathcal{Z}(XY^2 - Z^2)$.

Exercise IV.6. Assume that K has characteristic $p > 0$. Show that the map $\varphi : \mathbf{A}^1(K) \to \mathbf{A}^1(K)$, $t \mapsto t^p - t$ is not an isomorphism. Nevertheless, show that $d_t\varphi$ is an isomorphism for all $t \in \mathbf{A}^1(K)$. Compare with the Jacobian Conjecture.

Exercice IV.7* (Deligne-Lusztig). Assume that the characteristic p of K is ***positive***. Let q be a power of p. We denote by $\mathbb{F}_q$ the subfield of K with q elements (i.e. $\mathbb{F}_q = \{x \in K \mid x^q = x\}$). Let

$$G = \mathbf{SL}_2(\mathbb{F}_q) = \{g \in \mathbf{GL}_2(\mathbb{F}_q) \mid \det g = 1\}.$$

Let $V = \mathcal{Z}(XY^q - YX^q - 1) \subseteq \mathbf{A}^2(K)$. If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, we let it act on $\mathbf{A}^2(K)$ through the map $\mathbf{A}^2(K) \to \mathbf{A}^2(K)$, $(x, y) \mapsto (ax + by, cx + dy)$ $(= g.(x, y))$.

(a) Compute $\dim V$.
(b) Show that V is smooth.
(c) Show that G acts on $\mathbf{A}^2(K)$ as a group of automorphisms of varieties.
(d) Show that G stabilizes V.
(e***) Show that $V/G \simeq \mathbf{A}^1(K)$.

Exercise IV.8. Identify $\mathrm{Mat}_n(K)$ with $A^{n^2}(K)$ and let $\det : \mathrm{Mat}_n(K) \to K$ and $\mathrm{Tr} : \mathrm{Mat}_n(K) \to K$ be respectively the determinant and the trace. We also identify $\mathrm{Mat}_n(K)$ with the tangent space $T_M \mathrm{Mat}_n(K)$ for all $M \in \mathrm{Mat}_n(K)$. If V is an algebraic subset of $\mathrm{Mat}_n(K)$ and if $v \in V$, then we shall identify $T_v(V)$ with the corresponding subspace of $\mathrm{Mat}_n(K)$. If $a \in K$, we denote by V_a the algebraic set $\mathcal{Z}(\det - a)$.

(a) Show that $\det - a$ is an irreducible polynomial in n^2 variables.
(b) Deduce that V_a is irreducible. Compute $\dim V_a$.
(c) Let $M \in \mathrm{Mat}_n(K)$. Show that $d_M \det : \mathrm{Mat}_n(K) \to K$, $X \mapsto \mathrm{Tr}(\mathcal{C}(M)X)$, where $\mathcal{C}(M)$ is the matrix of the cofactors of M.
(d) Let $a \in K$. Show that $a \,\mathrm{Id}_n \in V_{a^n}$ (where Id_n denotes the identity matrix) and compute $T_{a\,\mathrm{Id}_n} V_{a^n}$.
(e) Show that V_a is smooth if and only if $a \neq 0$.

Exercise IV.9*. Let $f \in K[X, Y]$ be irreducible and let $V = \mathcal{Z}(f)$. Show that V is smooth if and only if $K[V] = K[X, Y]/\langle f \rangle$ is integrally closed.

Appendix. Algebraic background for algebraic geometry

We fix a ***commutative*** ring.

16. Radical ideals

Definition 16.1. *If I is an ideal of a commutative ring R, we define the **radical** of I to be the set*

$$\sqrt{I} = \{x \in R \mid \exists\ n \in \mathbb{N},\ x^n \in I\}.$$

*The radical of the zero ideal (that is, the set of **nilpotent** elements of R, see §5.C) is called the **nilradical** of R. An ideal I of R is called **radical** if it is equal to its radical.*

Recall that, if R is Artinian, then the nilradical of R is equal to its Jacobson radical.

Proposition 16.2. *Let I be an ideal of the commutative ring R. Then:*

(a) $I \subseteq \sqrt{I}$.
(b) $\sqrt{\sqrt{I}} = \sqrt{I}$.
(c) $\sqrt{I}$ *is an ideal.*
(d) $\sqrt{I}/I$ *is the nilradical of* R/I.

Proof - (a), (b) and (d) are easy. Let us prove (c). Let $x \in R$ and $y \in \sqrt{I}$. It is then clear that $xy \in \sqrt{I}$. The only difficult part is to show that, if moreover $x \in \sqrt{I}$, then $x - y \in \sqrt{I}$. Let m and n be two natural numbers such that $x^m \in I$ and $y^n \in \sqrt{I}$. Then, since R is commutative, we have

$$(x-y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i}.$$

Let $i \in \{0, 1, 2, \ldots, m+n\}$. If $i \leqslant m$, then $m+n-i \geqslant n$ and so $y^{m+n-i} \in I$, so $x^i y^{m+n-i} \in I$. If $i \geqslant m$, then $x^i \in I$ and again $x^i y^{m+n-i} \in I$. So $(x-y)^{m+n} \in I$. ■

Examples 16.3 - (1) Prime ideals are radical.

(2) If $R = \mathbb{Z}$, then $\sqrt{\langle 180\rangle} = \langle 30\rangle$. □

Proposition 16.4. *Let I be an ideal of the commutative ring R. Then*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \mathrm{Spec}(R) \\ I \subseteq \mathfrak{p}}} \mathfrak{p}.$$

Proof - By Proposition 16.2 (d), we may, and we will, assume that $I = 0$. Let

$$J = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}.$$

It is clear $\sqrt{0} \subseteq J$. It remains to show that $J \subset \sqrt{0}$. In other words, we must show that, if $r \in R$ is not nilpotent, then $r \notin J$. So let $r \in R$ which is not nilpotent. Let $\mathcal{M}$ be the set of ideals of R which does not contain any positive power of r. Then $0 \in \mathcal{M}$ because r

is not nilpotent, so $\mathcal{M}$ is not empty. It is readily seen from Zorn's Lemma that $\mathcal{M}$ has a maximal element. Let $\mathfrak{p}$ be a maximal element of $\mathcal{M}$.

We only need to show that $\mathfrak{p}$ is a prime ideal. So let a and b be two elements of R such that $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. By the maximality of $\mathfrak{p}$, there exist k, $l \geqslant 1$ such that $r^k \in \mathfrak{p} + Ra$ and $r^l \in \mathfrak{p} + Rb$. Therefore, $r^{k+l} \in \mathfrak{p} + Rab$. Therefore, $ab \notin \mathfrak{p}$. ■

Proposition 16.5. *Let I be an ideal of the commutative **Noetherian** ring R. Then there exists $k \geqslant 1$ such that $(\sqrt{I})^k \subseteq I$.*

Proof - By Proposition 16.2 (d), we may assume that $I = 0$. Since $R$is Noetherian, there exists $r_1,\ldots, r_n \in R$ such that $\sqrt{0} = \langle r_1, \ldots, r_n\rangle$. For each i, there exists $k_i \geqslant 1$ such that $r_i^{k_i} \in I$. Let $k = k_1 + \cdots + k_n$. Then, if we proceed as in the proof of Proposition 16.2 (c), it is easily checked that $(\sqrt{I})^k \subseteq I$. ■

We conclude this section with a result concerning minimal prime ideals in Noetherian rings.

Proposition 16.6. *Let R be a commutative Noetherian ring and let I be an ideal of R and let $\mathcal{P}$ denote the set of prime minimal prime ideals containing I. Then $\mathcal{P}$ is non-empty, finite and $\sqrt{I} = \bigcap_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}$. Moreover, if $\mathcal{P}'$ is a proper subset of $\mathcal{P}$, then $\sqrt{I} \subsetneq \bigcap_{\mathfrak{p}\in\mathcal{P}'} \mathfrak{p}$.*

Proof - Let $\mathcal{M}$ be the set of proper radical ideals of R which cannot be written as a finite intersection of prime ideals. We want to show that $\mathcal{M}$ is empty. If $\mathcal{M} \neq \varnothing$, then there exists a maximal element J in $\mathcal{M}$ because R is Noetherian. By construction, J is not prime, so there exists two elements a and b in R such that $a \notin J$, $b \notin J$ and $ab \in J$. Let $J' = \sqrt{J + Ra}$, $J'' = \sqrt{J + Rb}$. Then $J \subseteq J' \cap J''$ and $J \subsetneq J'$ and $J \subsetneq J''$. Let us show that $J = J' \cap J''$. Let $x \in J' \cap J''$. Then there exists m and $n \in \mathbb{N}$, $j' \in J$, $j'' \in J$ and r and $s \in R$ such that $x^m = j' + ra$ and $x^n = j'' + sb$. Therefore $x^{m+n} \in J$, so $x \in J$ because J is radical. In particular, J' and J'' are proper ideal of R. So they do not belong to $\mathcal{M}$ by the maximality of J. But then $J = J' \cap J''$ can be written as a finite intersection of prime ideals. So we have proved the following result:

$(*)$ *Every radical ideal of R is a finite intersection of prime ideals of R.*

Let us now come back to the proof of the proposition. By working with R/I instead of R, we may assume that $I = 0$. Also, by Proposition 16.4, we may assume that the nilradical of R is 0. Let $\mathcal{P}_0$ be a set of minimal cardinality such that $\sqrt{I} = \bigcap_{\mathfrak{p}\in\mathcal{P}_0} \mathfrak{p}$. To prove the proposition, we only need to show that $\mathcal{P} = \mathcal{P}_0$. In other words, we only need to show that, if $\mathfrak{p} \in \mathrm{Spec}(R)$, then there exists $\mathfrak{p}_0 \in \mathcal{P}_0$ such that $\mathfrak{p}_0 \subseteq \mathfrak{p}$. We shall need the following easy result:

> **Lemma 16.7.** *Let $\mathfrak{p}$ be a prime ideal of R and let $I_1,\ldots, I_n$ be ideals of R such that $I_1 \ldots I_n \subseteq \mathfrak{p}$. Then there exists $k \in \{1, 2, \ldots, n\}$ such that $I_k \subseteq \mathfrak{p}$.*
>
> Proof - By an easy induction argument, we are reduce to prove this lemma whenever $n = 2$. So we assume that $I_1 I_2 \subseteq \mathfrak{p}$. We also may assume that $I_1 \not\subseteq \mathfrak{p}$.

Let $a \in I_1$ be such that $a \notin \mathfrak{p}$. Then, for all $b \in I_2$, we have $ab \in I_1 I_2 \subseteq \mathfrak{p}$ so $b \in \mathfrak{p}$ because $\mathfrak{p}$ is prime. So $I_2 \subseteq \mathfrak{p}$. □

Let us now come back to the proof of the Proposition 16.6. If $\mathfrak{p} \in \mathrm{Spec}(R)$, then

$$\prod_{\mathfrak{p}_0 \in \mathcal{P}_0} \mathfrak{p}_0 \subseteq \bigcap_{\mathfrak{p}_0 \in \mathcal{P}_0} \mathfrak{p}_0 = 0 \subseteq \mathfrak{p}.$$

So, by Lemma 16.7, there exists $\mathfrak{p}_0 \in \mathcal{P}_0$ such that $\mathfrak{p}_0 \subseteq \mathfrak{p}$. The proof of the Proposition is complete. ■

17. Krull dimension

Definition 17.1. *Let $\mathfrak{p}$ be a prime ideal of R. We define the **height** of $\mathfrak{p}$, and we denote by* $\mathrm{height}(\mathfrak{p})$*, the maximal $n \geqslant 0$ such that there exists a chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$. We define the Krull dimension of R, and we denote by* $\mathrm{Krulldim}(R)$*, the number*

$$\mathrm{Krulldim}(R) = \max_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathrm{height}(\mathfrak{p}).$$

Note that it might happen that $\mathrm{height}(\mathfrak{p}) = \infty$ or that $\mathrm{Krulldim}(R) = \infty$ even if $\mathrm{height}(\mathfrak{p})$ is finite for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Note also that, by Corollary 5.2, we have

$$\mathrm{Krulldim}(R) = \max_{\mathfrak{m} \in \mathrm{Spec}(R)} \mathrm{height}(\mathfrak{m}). \tag{17.2}$$

The first result about Krull dimension is that it is preserved by integral extensions:

Proposition 17.3. *Let R and S be two rings such that $R \subseteq S$ and S is integral over R. Then* $\mathrm{Krulldim}(R) = \mathrm{Krulldim}(S)$.

Proof - Let $m = \mathrm{Krulldim}(R)$ and $n = \mathrm{Krulldim}(S)$. By definition, there exists a chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ of R. So, by the Going-up Theorem 9.21, there exists a chain $\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ of prime ideals of S such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$. So $m \leqslant n$.

Conversely, let us show that $n \leqslant m$. There exists a chain $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ of prime ideals of S. Let $\mathfrak{p}_i = \mathfrak{q}_i \cap R$. Then $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ is a chain of prime ideals of R. We only need to show that $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$. By working in the integral ring extension $R/\mathfrak{p}_i \hookrightarrow S/\mathfrak{q}_i$, we are reduced to show the following:

> **Lemma 17.4.** *Let R and S be two **integral** rings such that $R \subseteq S$ and let $\mathfrak{q}$ be a non-zero prime ideal of S. Then $\mathfrak{q} \cap R \neq 0$.*
>
> Proof - Let $x \in \mathfrak{q}$, $x \neq 0$. Let $P(X) \in R[X]$ be a monic polynomial of minimal degree such that $P(x) = 0$. Write $P(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_1 X + a_0$. Then $a_0 \neq 0$ by the minimality of the degree of P and because S is integral. On the other hand,
>
> $$a_0 = -x(a_1 + \cdots + a_{r-1}x^{r-2} + x^{r-1}) \in \mathfrak{q} \cap S = \mathfrak{p}.$$
>
> The proof of the lemma is complete. ■

Theorem 17.5. *Let K be a field. Then* $\operatorname{Krulldim} K[X_1, \ldots, X_n] = n$.

PROOF - Let $f(n) = \operatorname{Krulldim} K[X_1, \ldots, X_n]$. First,

$$0 \subsetneq \langle X_1 \rangle \subsetneq \langle X_1, X_2 \rangle \subsetneq \cdots \subsetneq \langle X_1, \ldots, X_n \rangle$$

is a chain of prime ideals of $K[X_1, \ldots, X_n]$. So $f(n) \geqslant n$.

We shall show by induction on n that $f(n) \leqslant n$. Let $0 = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{f(n)}$ be a chain of prime ideals of $K[X_1, \ldots, X_n]$. We shall first need the following result:

> **Lemma 17.6 (Krull's Hauptidealsatz).** *Let R be a unique factorization domain and let $\mathfrak{p}$ be a prime ideal of height 1. Then $\mathfrak{p}$ is principal.*
>
> PROOF - Let $f \in \mathfrak{p}$, $f \neq 0$. Since R is a U.F.D., we can write $f = f_1 \ldots f_r$, where the f_i are irreducible elements of R. Since $\mathfrak{p}$ is prime, there exists i such that $f_i \in \mathfrak{p}$. Therefore, $Rf_i \subseteq \mathfrak{p}$. But Rf_i is a prime ideal because R is a U.F.D. So $Rf_i = \mathfrak{p}$ because $\mathfrak{p}$ has height 1. ■

By construction, $\mathfrak{p}_1$ is a prime ideal of height 1, so, by Krull's Hauptidealsatz, $\mathfrak{p}_1 = \langle f \rangle$ for some $f \in K[X_1, \ldots, X_n]$ (since $K[X_1, \ldots, X_n]$ is a U.F.D.). Now, by Noether's Normalization Theorem (and its proof), there exists $m < n$ and algebraically independent elements $u_1, \ldots, u_m$ of $A = K[X_1, \ldots, X_n]/\mathfrak{p}_1$ such that A is integral over $K[u_1, \ldots, u_m]$. In particular, $\operatorname{Krulldim}(A) = \operatorname{Krulldim}(K[u_1, \ldots, u_m])$ by Proposition 17.3. So, by the induction hypothesis, we have $\operatorname{Krulldim}(A) \leqslant m < n$. But $0 = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{f(n)}/\mathfrak{p}_1$ is chain of prime ideals of A, so $f(n) - 1 \leqslant \operatorname{Krulldim}(A)$. Therefore, $f(n) - 1 < n$, so $f(n) \leqslant n$, as desired. ■

The previous Theorem has for consequence that, in the statement of Noether's Normalization Theorem, the number m of algebraically independent elements $(x_i)_{1 \leqslant i \leqslant m}$ of A such A is integral over $K[x_1, \ldots, x_m]$ is uniquely determined by A:

Corollary 17.7. *Let K be a field and let A be a finitely generated K-algebra. Let $(x_i)_{1 \leqslant i \leqslant m}$ and $(y_i)_{1 \leqslant i \leqslant n}$ be two finite families of algebraically independent elements of A such that A is integral over $K[x_1, \ldots, x_m]$ and also integral over $K[y_1, \ldots, y_n]$. Then $m = n$.*

PROOF - Indeed, by Proposition 17.3, we have $\operatorname{Krulldim}(A) = \operatorname{Krulldim}(K[x_1, \ldots, x_m]) = \operatorname{Krulldim}(K[y_1, \ldots, y_n])$. So $m = n$ by Theorem 17.5. ■

Homeworks

Homework for Wednesday, October 11

Exercise 1. Let M be a left R-module and let $e \in R$ be an *idempotent* (that is, $e^2 = e$). Show that the map $eR \otimes_R M \to eM$, $r \otimes_R m \mapsto rm$ is an isomorphism of $\mathbb{Z}$-modules (compare with Remark 3.18).

Exercise 2. Let i denote the complex number such that $i^2 = -1$. Let

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

and

$$\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}.$$

If p is a prime number, we denote by $\mathbb{F}_p$ the field $\mathbb{Z}/p\mathbb{Z}$.

(a) Show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ and that $\mathbb{Q}[i]$ is a subfield of $\mathbb{C}$.
(b) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[i] \simeq \mathbb{Q}[i]$ (as $\mathbb{Q}$-algebras).
(c) Show that $\mathbb{F}_2 \otimes_{\mathbb{Z}} \mathbb{Z}[i] \simeq \mathbb{F}_2[X]/(X^2)$ (as $\mathbb{F}_2$-algebras).
(d) Show that $\mathbb{F}_3 \otimes_{\mathbb{Z}} \mathbb{Z}[i]$ is a field with 9 elements.
(e) Show that $\mathbb{F}_5 \otimes_{\mathbb{Z}} \mathbb{Z}[i] \simeq \mathbb{F}_5 \times \mathbb{F}_5$ (as $\mathbb{F}_5$-algebras).
(f) Let R be the set of $(\alpha, \beta) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ such that $\alpha - \beta \in 2\mathbb{Z}[i]$. Show that R is a sub-$\mathbb{Z}[i]$-algebra of $\mathbb{Z}[i] \times \mathbb{Z}[i]$ and that the map $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Z}[i] \to \mathbb{Z}[i] \times \mathbb{Z}[i]$, $\alpha \otimes_{\mathbb{Z}} \beta \mapsto (\alpha\beta, \alpha\bar{\beta})$ is an injective morphism of $\mathbb{Z}[i]$-algebras whose image is R (in other words, $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Z}[i] \simeq R$).

Problem. First part. Let R be a commutative ring and let M be an R-module. For $n \in \mathbb{Z}_{\geqslant 0}$, we define

$$T^n(M) = \underbrace{M \otimes_R \cdots \otimes_R M}_{n \text{ times}},$$

with the convention that $T^0(M) = R$. Let

$$T(M) = \bigoplus_{n \in \mathbb{Z}_{\geqslant 0}} T^n(M).$$

We have then a natural map

$$\begin{array}{ccc} T^n(M) \times T^{n'}(M) & \longrightarrow & T^{n+n'}(M) \\ (x, y) & \longmapsto & x \otimes_R y \end{array}$$

(see Proposition 3.20). This extends to a map

$$\otimes_R : \begin{array}{ccc} T(M) \times T(M) & \longrightarrow & T(M) \\ (x, y) & \longmapsto & x \otimes_R y. \end{array}$$

(a) Show that the R-module $T(M)$ together with the product $\otimes_R$ is an R-algebra. It is called the *tensor algebra* of M over R.

Second part. Let $f : M \to M'$ be a morphism of R-modules. For each $n \in \mathbb{Z}_{\geqslant 0}$, we define

$$T^n(f) = \underbrace{f \otimes_R \cdots \otimes_R f}_{n \text{ times}} : T^n(M) \longrightarrow T^n(M').$$

Let $T(f) = \bigoplus_{n\in\mathbb{Z}_{\geqslant 0}} T^n(f)$ be the morphism of R-modules $T(M) \to T(M')$.

(b) Show that $T(f)$ is a morphism of R-algebras.

(c) Show that $T : {}_R\mathbf{Mod} \to {}_R\mathbf{Alg}$, $M \mapsto T(M)$, $f \mapsto T(f)$ is a functor. Here, ${}_R\mathbf{Alg}$ denotes the category of R-algebras (where morphisms are morphisms of R-algebras).

(d) Let A be an R-algebra and let $f : M \to A$ be a morphism of R-modules. Show that there exists a unique morphism of R-algebras $f^T : T(M) \to A$ such that the restriction of f^T to $T^1(M) = M$ coincides with f.

(e) **(optional)** Let $\mathcal{F} : {}_R\mathbf{Alg} \to {}_R\mathbf{Mod}$, $A \mapsto A$, $f \mapsto f$ be the forgetful functor. Show that the functor T is left adjoint to $\mathcal{F}$ (use (d)).

Third part (examples). We denote by $R\{X_1, \ldots, X_n\}$ the ring of *non-commutative* polynomials in the variables X_1,..., X_n. If necessary, we denote by $T_R(M)$ the R-algebra $T(M)$.

(f) Assume here that M is free with basis $(e_1, \ldots, e_n)$. Show that there is a unique morphism of R-algebras $R\{X_1, \ldots, X_n\} \to T(M)$ that sends X_i to e_i. Show that it is an isomorphism.

(g) Show that $T_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}) \simeq (\mathbb{Z}/m\mathbb{Z})[X]$ and $T_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}[X]/(mX)$, where X is an indeterminate.

(h) Show that $T_{\mathbb{Z}}(\mathbb{Q}) \simeq \{P \in \mathbb{Q}[X] \mid P(0) \in \mathbb{Z}\}$.

Fourth part (optional). Let $I(M)$ be the two-sided ideal of $T(M)$ generated by the elements of the form $m \otimes_R m' - m' \otimes_R m$, for m, $m' \in M$. Let $S(M) = T(M)/I(M)$.

(i) Show that $S(M)$ is a commutative R-algebra. It is called the *symmetric algebra of* M.

(j) If $f : M \to M'$ is a morphism of R-modules, show that $T(f)(I(M)) \subseteq I(M')$. Deduce from this that $T(f)$ induces a morphism of algebras $S(f) : S(M) \to S(M')$.

(k) Show that $S : {}_R\mathbf{Mod} \to {}_R\mathbf{Alg}_c$, $M \mapsto S(M)$, $f \mapsto S(f)$ is a functor. Here, ${}_R\mathbf{Alg}_c$ denotes the category of *commutative* R-algebras.

(l) If $n \in \mathbb{Z}_{\geqslant 0}$, let $I^n(M) = I(M) \cap T^n(M)$ and $S^n(M) = T^n(M)/I^n(M)$. Show that $I(M) = \bigoplus_{n\in\mathbb{Z}_{\geqslant 0}} I^n(M)$ and that $S(M) = \bigoplus_{n\in\mathbb{Z}_{\geqslant 0}} S^n(M)$.

(m) Show that $I^1(M) = 0$ and $S^1(M) = M$.

(n) Let A be a commutative R-algebra and let $f : M \to A$ be a morphism of R-modules. Show that there exists a unique morphism of R-algebras $f^S : T(M) \to A$ such that the restriction of f^S to $S^1(M) = M$ coincides with f.

(o) Let $\mathcal{F}_c : {}_R\mathbf{Alg}_c \to {}_R\mathbf{Mod}$, $A \mapsto A$, $f \mapsto f$ be the forgetful functor. Show that the functor S is left adjoint to $\mathcal{F}_c$.

(p) Show that $S(M \oplus_R M') \simeq S(M) \otimes_R S(M')$.

(q) Assume here that M is free with basis $(e_1, \ldots, e_n)$. Show that there is a unique morphism of R-algebras $R[X_1, \ldots, X_n] \to S(M)$ that sends X_i to e_i. Show that it is an isomorphism.

Homework for Wednesday, October 18

Exercise 1 (Fitting's Lemma). Let M be a Noetherian and Artinian left R-module and let $\sigma : M \to M$ be an endomorphism of M.

(a) Show that there exists $n_0 \in \mathbb{N}$ such that $\operatorname{Im}\sigma^{n_0} = \operatorname{Im}\sigma^{n_0+1}$ and $\operatorname{Ker}\sigma^{n_0} = \operatorname{Ker}\sigma^{n_0+1}$.

(b) Show that $\operatorname{Im}\sigma^n = \operatorname{Im}\sigma^{n+1}$ and $\operatorname{Ker}\sigma^n = \operatorname{Ker}\sigma^{n+1}$ for all $n \geqslant n_0$.

(c) Show that $M = (\operatorname{Im}\sigma^{n_0}) \oplus (\operatorname{Ker}\sigma^{n_0})$.

Exercise 2. Let R be a ring and let n be a natural number. We propose to prove in several steps that $J(\mathrm{Mat}_n(R)) = \mathrm{Mat}_n(J(R))$ (by $\mathrm{Mat}_n(J(R))$, we mean the set of $n \times n$ matrices with coefficients in $J(R)$: it is not a unitary ring).

Let $E_{ij} \in \mathrm{Mat}_n(R)$ denote the matrix whose entries are all zero except the (i,j)-entry which is equal to 1. We denote by $\mathbf{1}_n$ the identity matrix. Let $I = \mathrm{Mat}_n(J(R))$ and $J = J(\mathrm{Mat}_n(R))$. For $j \in \{1, 2, \ldots, n\}$, we set $I_j = \oplus_{i=1}^n J(R)E_{ij}$. We shall first prove that $I \subseteq J$.

(a) Show that I is a two-sided ideal of $\mathrm{Mat}_n(R)$.

(b) Show that I_j is a left ideal of $\mathrm{Mat}_n(R)$ and that $I = \oplus_{j=1}^n I_j$.

(c) Assume here, ond only in this question, that R is *commutative*, so that $\det : \mathrm{Mat}_n(R) \to R$ is well-defined. Show that $\det(\mathbf{1}_n - a) \in 1 + J(R)$ for any $a \in I$. Deduce that $I \subseteq J$ in this case.

(d) Let $a \in I_j$. Write $a = \sum_{i=1}^n \alpha_i E_{ij}$, with $\alpha_i \in J(R)$. Since $1-\alpha_j$ is invertible, we can define $\beta_i = \alpha_i(1-\alpha_j)^{-1}$. Let $b = -\sum_{i=1}^n \beta_i E_{ij}$. Show that $(\mathbf{1}_n - b)(\mathbf{1}_n - a) = \mathbf{1}_n$.

(e) Deduce from (b) and (d) that $I_j \subseteq J$ and $I \subseteq J$.

We shall now prove that $J \subseteq I$. Let $a \in J$ and write $a = \displaystyle\sum_{1 \leqslant i,j \leqslant n} \alpha_{ij} E_{ij}$. We want to prove that $\alpha_{ij} \in J(R)$ for all (i,j). So fix i and j in $\{1, 2, \ldots, n\}$.

(f) Let $b = E_{ii} a E_{ji}$. Show that $b = \alpha_{ij} E_{ii}$.

(g) Show that $\mathbf{1}_n - rb$ is invertible for any $r \in R$.

(h) Deduce that $1 - r\alpha_{ij}$ is invertible for any $r \in R$. Conclude.

Homework for Wednesday, October 25

Exercise 1. Let G be a finite p-group and let $R = \mathbb{F}_p[G]$ be the group algebra of G over $\mathbb{F}_p$. The aim of this exercise is to prove that R is a local ring. We first recall the following result from group theory: if X is a G-set (i.e. a set endowed with an action of G) and if we denote by $X^G = \{x \in x \mid \forall\ g \in G,\ g.x = x\}$, then

$$(*) \qquad |X| \equiv |X^G| \mod p.$$

We now need some more notation. Let

$$\begin{array}{rccc} \sigma : & R & \longrightarrow & \mathbb{F}_p \\ & \sum_{g\in G} a_g g & \longmapsto & \sum_{g\in G} a_g \end{array}$$

and

$$\mathfrak{m} = \operatorname{Ker} \sigma.$$

(a) Show that σ is a morphism of $\mathbb{F}_p$-algebras.
(b) Show that $\mathfrak{m}$ is a two-sided ideal and is a maximal left ideal of R.

Let S be a simple R-module. We also view S as a G-set (because $G \subseteq R^\times$ acts on S). Let $x \in S$, $x \neq 0$.

(c) Show that S is a $\mathbb{F}_p$-vector space.
(d) Show that the map $\pi : R \to S$, $r \mapsto rx$ is a surjective morphism of R-modules (and of $\mathbb{F}_p$-vector spaces). Deduce that S is finite dimensional.
(e) Show that S^G is an R-submodule of S.
(f) Show that $S^G \neq 0$ (use $(*)$). Deduce that $S = S^G$.
(g) Show that $\mathfrak{m} = \operatorname{Ker} \pi$.
(h) Show that $J(R) = \mathfrak{m}$ and that R is a local ring.

Exercise 2. Let R be a commutative integral domain. Let I and J be two non-zero ideals of R such that the ideal IJ is principal. We shall prove that I (and J) are projective modules. For this, let $r \in R$ be such that $IJ = Rr$ and write $r = \sum_{i=1}^n x_i y_i$ with $x_i \in I$ and $y_i \in J$. Let

$$\begin{array}{rccc} \varphi : & I & \longrightarrow & (Rr)^n \\ & x & \longmapsto & (xy_1, \ldots, xy_n) \end{array}$$

and

$$\begin{array}{rccc} \psi : & (Rr)^n & \longrightarrow & I \\ & (r_1, \ldots, r_n) & \longmapsto & \sum_{i=1}^n (r_i x_i)/r. \end{array}$$

(a) Show that φ and ψ are well-defined morphisms of R-modules.
(b) Show that the image of φ is contained in $(Rr)^n$.
(c) Show that $\psi \circ \varphi = \mathrm{Id}_I$.
(d) Show that φ is injective and that $(Rr)^n = \varphi(I) \oplus \operatorname{Ker} \psi$.
(e) Deduce that I is a projective R-module.

Homework for Wednesday, November 1st

Exercise. Prove Theorem 8.16. Hint: identify V with $\mathrm{Col}_n(D)$ as a right D-module and A with $\mathrm{Mat}_n(D)$ acting on V on the left; for (a) and (b), use the Homework for October 18 (Exercise 2); for (c), (d) and (e), you can use (if you want...) the Morita equivalence between A and D (tensorizing with $\mathrm{Col}_n(D) = V$ and $\mathrm{Row}_n(D)$); (f) is standard.

Homework for Wednesday, November 8

Exercise 1. Let K be a field and let n be a natural number. We denote by A the K-subalgebra of $\mathrm{Mat}_n(K)$ consisting of upper triangular matrices. Let J denote the set of nilpotent upper triangular matrices in $\mathrm{Mat}_n(K)$.

(a) Show that $J = J(A)$.
(b) Show that $A/J(A) \simeq K \times \cdots \times K$ (n times) as K-algebras.
(c) Determine the number and the dimension of the simple A-modules.
(d) Let V be an A-module of finite type. Show that V is a finite dimensional K-vector space, that V has finite length and that $\lg(V) = \dim_K V$.

Exercise 2. Let R be a semisimple ring. Show that every R-module is injective and projective.

Exercise 3. Let K be a field and let $P(X) \in K[X]$ be a polynomial. Show that the K-algebra $K[X]/(P(X))$ is semisimple if and only if P and P' are relatively prime.

Exercise 4. Let G be a finite group. Show that G is abelian if and only if all simple $\mathbb{C}[G]$-modules have dimension 1.

Exercise 5. Let C be a cyclic group of order 6. Find the number and the dimension of the simple $\mathbb{Q}[C]$-modules.

Homework for Wednesday, November 15

Problem. Let $n \geqslant 1$ and let ζ_n be a primitive n-th root of unity in $\mathbb{C}$, that is, a generator of the cyclic group $\boldsymbol{\mu}_n(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1\}$ (for instance, $\zeta_n = e^{2i\pi/n}$). Let $\Phi_n(X)$ denote the n-th cyclotomic polynomial

$$\Phi_n(X) = \prod_{\substack{1 \leqslant j \leqslant n \\ \gcd(n,j)=1}} (X - \zeta_n^j).$$

Let $\varphi(n)$ denote the degree of $\Phi_n(X)$ (i.e. the Euler φ-function).

(a) Compute Φ_n for $1 \leqslant n \leqslant 6$.

(b) Show that $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

(c) Deduce by induction that $\Phi_n(X)$ belongs to $\mathbb{Z}[X]$ and is monic.

(d) Let p be a prime number. Compute Φ_p and show that Φ_p is irreducible (Hint: compute $\Phi_p(X+1)$ and use Eisenstein's criterion of Exercise III.3).

The aim of the next questions is to show that Φ_n is irreducible for all n. Write $\Phi_n(X) = P(X)Q(X)$ where $P(X)$, $Q(X) \in \mathbb{Z}[X]$ are monic and P is irreducible in $\mathbb{Q}[X]$. Let ζ be a root of P and let p be any prime number not dividing n. We denote by $\overline{f}(X) \in \mathbb{F}_p[X]$ the reduction modulo p of $f(X) \in \mathbb{Z}[X]$. Since ζ^p is a root of Φ_n, we must have $P(\zeta^p) = 0$ or $Q(\zeta^p) = 0$.

(e) Assume that $Q(\zeta^p) = 0$. Show that $P(X)$ divides $Q(X^p)$.

(f) Show that $\overline{Q}(X^p) = \overline{Q}(X)^p$.

(g) Assume that $Q(\zeta^p) = 0$ and let $f \in \mathbb{F}_p[X]$ be any irreducible factor of $\overline{P}$.

(g1) Deduce from (e) and (f) that f also divides $\overline{Q}$.

(g2) Deduce that f^2 divides $X^n - 1$ and that f divides nX^{n-1} (Hint: take the derivative) so that f divides also X^{n-1}. Show that it is impossible.

(h) Deduce from (g) that $P(\zeta^p) = 0$ for all prime number p which does not divide n. Deduce that $f = \Phi_n$, and that Φ_n is irreducible.

The fact that Φ_n is irreducible shows that the field $\mathbb{Q}(\zeta_n)$ is isomorphic to $\mathbb{Q}[X]/(\Phi_n)$ and that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Let $\mathcal{O}_n$ denote the ring of integers of $\mathbb{Q}(\zeta_n)$. Then it is clear that $\mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_n$. It can be proved that $\mathcal{O}_n = \mathbb{Z}[\zeta_n]$. The aim of the next questions is to prove this result whenever n is a prime number (note that the case $n = 2$ is trivial). So let p be an odd prime number.

(i) Show that $\det(\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_p^i \zeta_p^j))_{0 \leqslant i,j \leqslant p-2} = \pm p^{p-2}$.

(j) Deduce that, if $\alpha \in \mathcal{O}_p$, then there exists $r \in \mathbb{Z}_{\geqslant 0}$ such that $p^r \alpha \in \mathbb{Z}[\zeta_p]$.

(k) Show that, if $1 \leqslant i \leqslant p-1$, then $(1 - \zeta_p^i)/(1 - \zeta_p) \in \mathcal{O}_p^\times$.

(l) Show that $\prod_{i=1}^{p-1}(1 - \zeta_p^i) = \Phi_p(1) = p$ (Hint: use (d)).

(m) Let $\mathfrak{p} = (1-\zeta_p)\mathbb{Z}[\zeta_p]$ and $\mathfrak{q} = (1-\zeta_p)\mathcal{O}_p$. Deduce from (k) and (l) that $\mathfrak{p}^{p-1} = p\mathbb{Z}[\zeta_p]$ and $\mathfrak{q}^{p-1} = p\mathcal{O}_p$.

(n) Show that $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\zeta_p]$ and that $\mathbb{Z}[\zeta_p]/\mathfrak{p} \simeq \mathbb{F}_p$.

(o) Deduce from (m) that $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_p$ and that $\mathcal{O}_p/\mathfrak{q} \simeq \mathbb{F}_p$ (use Theorem 10.12 (c)).

(p) Deduce from (m) and (n) that $\mathfrak{p} = \mathfrak{q} \cap \mathbb{Z}[\zeta_p]$.

(q) Deduce that $\mathfrak{p}^i = \mathfrak{q}^i \cap \mathbb{Z}[\zeta_p]$ for all $i \geqslant 1$.
(r) Deduce from (j) that $\mathcal{O}_p = \mathbb{Z}[\zeta_p]$.

Homework for Monday, November 27

Problem: quotient of affine varieties by finite groups. Let K be a field, let A be a finitely generated commutative K-algebra and let G be a finite group acting on A by automorphisms of K-algebras. The aim of this problem is to study the algebra A^G, where

$$A^G = \{a \in A \mid \forall\ \sigma \in G,\ \sigma(a) = a\},$$

and to see some geometric consequences.

(a) Show that A^G is a commutative K-algebra.

Part I. The aim of this part is to show that A^G is a finitely generated K-algebra and that A is a finitely generated A^G-module. If $a \in A$, we set

$$P_a(X) = \prod_{\sigma \in G} (X - \sigma(a)) \in A[X].$$

We fix some elements $a_1, \ldots, a_n \in A$ such that $A = K[a_1, \ldots, a_n]$. Let $\mathcal{E}$ be the set of coefficients of the polynomials $P_{a_i}(X)$, $1 \leqslant i \leqslant n$. Then $\mathcal{E}$ is ***finite*** and let B be the subalgebra of A generated by $\mathcal{E}$: it is a finitely generated commutative K-algebra.

(a) Show that $P_a \in A^G[X]$.

(b) Deduce that $B \subseteq A^G$ and that A is integral over B. In particular, A is integral over A^G (see also Example 9.5 (3)).

(c) Show that A is a finitely generated B-module (show that monomials $a_1^{r_1} \ldots a_n^{r_n}$ for $0 \leqslant r_i \leqslant |G| - 1$ form a set of generators of the B-module A).

(d) Deduce that A^G is a finitely generated B-module (Hint: recall that, since B is finitely generated, then B is Noetherian by Hilbert's Basis Theorem).

(e) Deduce that A^G is a finitely generated K-algebra and that A is a finitely generated A^G-module.

Part II. The aim of this part is to study the map $\pi : \mathrm{Spec}(A) \to \mathrm{Spec}(A^G)$, $\mathfrak{p} \mapsto \mathfrak{p} \cap A^G$.

(f) Show that π is surjective and that $\pi(\mathfrak{p})$ is maximal if and only if $\mathfrak{p}$ is maximal.

(g) Show that, if $\sigma \in G$ and $\mathfrak{p} \in \mathrm{Spec}(A)$, then $\sigma(\mathfrak{p}) \in \mathrm{Spec}(A)$ and $\pi(\sigma(\mathfrak{p})) = \pi(\mathfrak{p})$. Show also that $\mathfrak{p}$ is maximal if and only if $\sigma(\mathfrak{m})$ is maximal.

(h) Let $\mathfrak{m}_1$ and $\mathfrak{m}_2 \in \mathrm{Max}(A)$ such that $\pi(\mathfrak{m}_1) = \pi(\mathfrak{m}_2)$. Show that there exists $\sigma \in G$ such that $\mathfrak{m}_2 = \sigma(\mathfrak{m}_1)$ (Hint: Assume that $\mathfrak{m}_2 \neq \sigma(\mathfrak{m}_1)$ for all $\sigma \in G$, and consider an element $a \in A$ such that $a \equiv 0 \mod \mathfrak{m}_2$ and $a \equiv 1 \mod \sigma(\mathfrak{m}_1)$ for all $\sigma \in G$. Such an element exists by the Chinese Remainder Theorem: then consider $x = \prod_{\sigma \in G} \sigma(a)$).

(i*) **(Optional)** Let $\mathfrak{p}_1$ and $\mathfrak{p}_2 \in \mathrm{Spec}(A)$ such that $\pi(\mathfrak{p}_1) = \pi(\mathfrak{p}_2)$. Show that there exists $\sigma \in G$ such that $\mathfrak{p}_2 = \sigma(\mathfrak{p}_1)$ (Hint: let $\mathfrak{p} = \pi(\mathfrak{p}_1) = \pi(\mathfrak{p}_2)$, let $D = A^G \setminus \mathfrak{p}$ and consider the extension $S^{-1}A^G \subseteq S^{-1}A$. Then apply (h)).

Part III. We shall now apply the previous results to a geometric situation. ***From now on, and until the end of this problem, we assume that K is algebraically closed.*** Let V be an affine variety (over K) and let G be a finite group of automorphisms of V. If $f \in K[V]$, let $\sigma(f) = f \circ \sigma^{-1}$ (in other words, we denote by σ the automorphism

$\sigma^{*-1} = (\sigma^{-1})^*$ of A). Then G can also be viewed as a finite group of automorphisms of $K[V]$.

A pair (W, π), where W is an affine variety and $\pi : V \to W$ is a morphism of varieties, is called a *geometric quotient of V by G* if the following two conditions are satisfied:

(Q1) π is surjective and, if $w \in W$, $\pi^{-1}(w)$ is a G-orbit.

(Q2) If $\varphi : V \to V'$ is a morphism of algebraic varieties which is constant on the G-orbits, there exists a unique morphism of varieties $\tilde{\varphi} : W \to V'$ such that $\varphi = \tilde{\varphi} \circ \pi$.

(j) Let (W, π) and (W', π') be two geometric quotients of V by G. Show that there exists a unique isomorphism of varieties $\varphi : W \to W'$ such that $\pi' = \varphi \circ \pi$.

We shall now show that there exists a geometric quotient of V by G. By (e), there exists $f_1, \ldots, f_n \in K[V]^G$ such that $K[V]^G = K[f_1, \ldots, f_n]$. Let γ be the unique morphism of K-algebras $K[X_1, \ldots, X_n] \to K[V]^G$, $X_i \mapsto f_i$, let I denote its kernel and let $W = \mathcal{Z}(I)$.

(k) Show that $K[X_1, \ldots, X_n]/I$ is an integral domain which is isomorphic to $K[V]^G$.

(l) Deduce that $I = \mathcal{I}(W)$ (Hint: use Hilbert's Nullstellensatz).

(m) Show that γ induces an injective morphism of algebras $\tilde{\gamma} : K[W] \to K[V]$. Let $\pi : V \to W$ be the morphism of varieties such that $\pi^* = \tilde{\gamma}$.

(n) Show that (W, π) is a quotient of V by G (hint: use (h) and Proposition 11.34).

(o) Recall that π^* is injective (see (m)). Show also that π is a finite morphism. Deduce that $\dim V = \dim W$.