Master Mathématiques et applications

Mohamed Aqalmoun

Cahier-Cours

Commutative algebra

Module $M03$

ENS-FES

Avant-propos

This course workbook (version $\frac{1}{2}$-course) is intended for students of "Master Mathematics and applications" at higher Normal School-Fez. It offers an incomplete course (without proofs) on commutative algebra: Rings and morphisms, Modules, Localization, tensor product, Chains condition, Integral extension, Krull dimension.

Contents

Chapter 1

Rings and morphisms

1.1 Rings and morphisms

Definition 1.1.

A ring is a set with two binary operations $(R, +, \times)$ *such that:*
• $(R, +)$ *is an Abelian group .*
• *The multiplication* $\times$ *is associative, that is, for all* $a, b, c \in R$, $a(bc) = (ab)c$.
• *The multiplication* $\times$ *is distributive with respect to the addition* $+$, *that is , for all* $a, b, c \in A$, $(a+b)\times c = a\times c + b\times c$ *et* $a\times(b+c) = a\times b + a\times c$.
The ring R *unitary if,* $\times$ *has an identity element called the unit, and denote it by* 1_R *or* 1.
The ring R *is commutative if the multiplication* $\times$ *is commutative.*

Throughout this course by **ring** we mean a commutative ring with identity.
Let $(A_i)_{i\in I}$ be a family of rings. Define two binary operations on the Cartesian product $\prod_{i\in} A_i$ as follow:

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I},\ \ (x_i)_{i\in I}(y_i)_{i\in I} = (x_i y_i)_{i\in I}$$

Then $(\prod_{i\in I} A_i, +, \times)$ is a commutative ring called the direct product of the rings A_i, $i \in I$.
A ring is trivial if it is a singleton, in this case $1 = 0$.
Let R be a ring and $a \in R$. We say that a is invertible if there exists $b \in R$ such that $ab = 1$, in this case b is unique and it is denoted a^{-1}. The set of invertible

elements of R is denoted $R^\times$ called the group of units. It is easy to see that $R^\times$ is a group (with respect to multiplication).

Definition 1.2.

Let R be a ring and $a \in R$.

1. *a is a zero-divisor if there exists a non zero element $b \in R$ such that $ab = 0$. The set of zero-divisor is denoted $\mathrm{Z}(R)$.*
2. *a is a nilpotent element if there exists $n \in \mathbb{N}$ such that $a^n = 0$.*

Remark :

1. An invertible element is not a zero-divisor.
2. If R is a non trivial ring, any nilpotent element is a zero-divisor.
3. A zero divisor element is not necessarily a nilpotent element: $(1,0)$ is a zero divisor in the ring $\mathbb{Z} \times \mathbb{Z}$, but it is not nilpotent.

Definition 1.3.

A ring R is an integral domain if;

1. *R non trivial $(1 \neq 0)$,*
2. *For all $a, b \in R$, $ab = 0 \Longrightarrow a = 0$ or $b = 0$.*

A ring R is an integral domain if R is non trivial and $Z(R) = \{0\}$.

Example :

1. $\mathbb{Z}$ is an integral domain.
2. $\mathbb{R}[X]$ is an integral domain.
3. $\mathbb{Z}^2$ is not integral, since $(1,0)(0,1) = 0$.

Definition 1.4.

A ring R is a field if

1. *R is non trivial $(1 \neq 0)$,*

2. *$R^\times = R\setminus\{0\}$, that is every nonzero element is invertible.*

If R is a field then R is an integral domain.

Definition 1.5.

Let R be a ring and B be a subset of R. We say that B is a subring of R if, $(B,+)$ is a subgroup of $(R,+)$, B is stable with respect to multiplication and $1\in B$.

Definition 1.6.

Let R and R' be a rings and $f: A\to B$. We say that f is a morphism of rings if: for all $a,b\in A$, $f(a+b)=f(a)+f(b)$, $f(ab)=f(a)f(b)$ and $f(1)=1$.

If $f: R\to R'$ is a rings morphism then $f(0)=0$, $f(a-b)=f(a)-f(b)$, moreover if a is an invertible element of R then $f(a)$ is invertible and $(f(a))^{-1}=f(a^{-1})$.
Let $f: R\to R'$ be a morphism of rings. We say that f is an isomorphism if it is bijective.
Two rings R and R' are isomorphic if there is an isomorphism between them.

1.2 Ideals

Definition 2.1.

Let R be a ring and I be a subset of R. We say that I is an ideal of R if;

1. *I is a subgroup of $(R,+)$,*
2. *$\forall a\in R, \forall x\in I, ax\in I$.*

Remark :

1. $\{0\}$ et R are ideals of R.
2. If I is an ideal of R containing an invertible element, then $I=R$.

3. A non trivial ring R is a field if and only if $\{0\}$ and R are the only ideals of R.

Proposition 2.2.

Let R be a ring.

- *If I and J are ideals of R, then $I+J := \{x+y \;/\; (x,y)\in I\times J\}$ is an ideal of R called the sum of I and J.*
- *If $(I_\alpha)_{\alpha\in\Gamma}$ is a family of ideals of R, then $\cap_{\alpha\in\Gamma} I_\alpha$ is an ideal of R.*

Proof : ....

Let S be a subset of R. The intersection of all ideals of R containing S is an ideal of R, and is called the ideal generated by S it is denoted (S). That is

$$(S) = \bigcap_{I \text{ ideal of } R,\; I\supseteq S} I$$

Proposition 2.3.

Let R be a ring and S be a nonempty subset of R, then

- $(S) = \left\{\sum_{i=1}^{m} a_i s_i \;/\; m\geq 1,\; a_i\in R, s_i\in S\right\}.$
- $(\emptyset) = \{0\}$.

Proof : ....

Remark : If $S = \{s_1,\ldots,s_n\}$, then $(S) = \left\{\sum_{i=1}^{n} a_i s_i \;/\; a_i\in R\right\}$, also it is denoted $(s_1,\ldots,s_n)$.

Definition 2.4.

Let R be a ring.

1. *Let I,J be ideals of R. The product of I and J denoted IJ is the ideal generated by all elements ab, where $a\in I$ and $b\in J$.*
2. *Let $(I_\alpha)_{\alpha\in\Gamma}$ be a family of ideals of R. The sum of the ideals I_α, $\alpha\in\Gamma$ is the ideal generated by $\bigcup_{\alpha\in\Gamma} I_\alpha$ it is denoted $\sum_{\alpha\in\Gamma} I_\alpha$*

The elements of IJ are $\sum_{k=1}^{m} a_k b_k$, where $a_k \in I$ and $b_k \in J$.
The elements of $\sum_{\alpha\in\Gamma} I_\alpha$ are $\sum_{\alpha\in\Gamma} a_\alpha$, where $a_\alpha \in I_\alpha$ and all but finite set are zero.
The product of a finitely many ideals $I_1, \ldots, I_m$, is the ideal generated by all products $a_1 \cdots a_m$, where $a_k \in I_k$.

Definition 2.5.

Let R be a ring and I be an ideal of R.

1. *We say that I is a principal ideal if it is generated by one element, that is $I = (a)$, where $a \in R$.*
2. *We say that I is a finitely generated ideal if it is generated by a finitely many elements, that is $I = (a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in R$.*

Example :

1. In the ring $\mathbb{Z}[X]$, the ideal $I = \{P \in \mathbb{Z}[X] \ / \ P(0) = 0\}$ is principal. In fact $I = (X)$.
2. If I and J are finitely generated ideals, then so are IJ and $I + J$. In fact; ...

Definition 2.6.

A ring is a principal domain[1] if it is an integral domain and all its ideals are principal.

Examples :

1. $\mathbb{Z}$ is a principal domain.
2. $\mathbb{R}[X]$ is a principal domain.

Let I be an ideal of R. The quotient group R/I inherits a uniquely defined multiplication from R ($\overline{x}\,\overline{y} = \overline{xy}$), which makes it a (commutative) ring, called the quotient ring. Moreover, the maps $\pi : R \to R/I$ defined by $\pi(x) = \overline{x}$ is a rings morphism.

[1] It is quasi-principal if its ideals are principal (without integral condition).

Proposition 2.7.

Let R be a ring and I be an ideal of R. The morphism $\pi : A \to A/I$ induce a bijection between ideal of R/I and ideals of R containing I.

Proof : ....

Proposition 2.8.

Let $f : R \to R'$ be a rings morphism.

1. *If J is an ideal of R' then $f^{-1}(J)$ is an ideal of R. In particular $\ker f$ is an ideal of R.*
2. *$\operatorname{Im} f$ is a subring of R'.*

Proof : ....

Theorem 2.9. (First isomorphism theorem)

Let $f : R \to R'$ be rings. Then the maps

$$\overline{f} : A/\ker f \to \operatorname{Im} f,\ \ \overline{f}(\overline{x}) = f(x)$$

is well defined and is an isomorphism.

Proof : ....

Remarks :

1. Second isomorphism theorem: Let R' be a subring of a ring R and I be an ideal of R. Then $R' + I$ is a subring of R, $R' \cap I$ is an ideal of R, moreover the rings $(B + I)/I$ et $B/(B \cap I)$ are isomorphic.

2. Third isomorphism theorem: Let R be a ring and $I \subseteq J$ be ideals of R. Then J/I is an ideal of R/I, moreover the rings $(R/I)/(J/I)$ and R/J are isomorphic.

1.3 Prime and maximal ideals

Definition 3.1.

Let R be a ring.

1. *An ideal P is a prime ideal of R if $P \neq R$ and $\forall x, y \in A$, $xy \in P \Rightarrow x \in P$ or $y \in P$.*

2. *An ideal M is a maximal ideal of R if $M \neq R$ and there is no ideal I of R such that $M \subset I \subset R$ (strict inclusion).*

The set of prime ideals of R is called the prime spectrum of R and is denoted $\mathrm{Spec}(R)$, whereas the set of maximal ideals of R is called maximal spectrum of R and is denoted $\mathrm{MaxSpec}(R)$ or $\mathrm{Max}(R)$.

Examples :

1. In the ring $\mathbb{R}[X]$ the ideal (X) is prime.
2. In the ring $\mathbb{Z}$ the ideal (3) is maximal.
3. In the ring $\mathbb{Z}^2$ the ideal $((0,6))$ is not a prime ideal.

Proposition 3.2.

Let R be a ring.

1. *An ideal P is prime if and only if R/P is an integral domain.*
2. *An ideal M is maximal if and only if R/M is a field.*

Proof : ....

Proposition 3.3.

1. *A maximal ideal is a prime ideal.*
2. *Let $f : R \to R'$ be a rings morphism. If P is a prime ideal of R' then $f^{-1}(P)$ is a prime ideal of R.*

Proof :

Theorem 3.4. (Krull)

Let R be a non trivial ring i.e $R \neq 0$, then $\mathrm{Max}(R) \neq \emptyset$*. That is R contains at last a maximal ideal.*

Proof : (by Zorn's Lemma) ....

Corollary 3.5.

Let R be a ring.

1. *Every proper ideal (i.e $\neq R$) of R is contained in a maximal ideal.*
2. *If $a \in R$ is non invertible, then a is contained in a maximal ideal.*

Proof : ....

Remark : As a consequence of the previous corollary;

$$A^{\times} = A \setminus \left(\bigcup_{M \in \mathrm{Max}(A)} M \right)$$

Definition 3.6.

Let R be a ring and $P \in \mathrm{Spec}(R)$. We say that P is a minimal prime ideal of R if it is minimal in the set $\mathrm{Spec}(R)$ with respect to inclusion, that is if $Q \in \mathrm{Spec}(R)$ such that $Q \subseteq P$ then $Q = P$.

Examples :

1. (0) is a minimal prime ideal of $\mathbb{Z}$. Moreover if R is an integral domain, then (0) is a minimal prime ideal of R.
2. $\mathbb{Z} \times \{0\}$ is a minimal prime ideal of $\mathbb{Z} \times \mathbb{Z}$.

Theorem 3.7.

Let R be a ring and $P \in \mathrm{Spec}(R)$. Then P contains at last a minimal prime ideal.

Proof : ....

Remarks :

1. Every non trivial ring has at last a minimal prime ideal.
2. A minimal prime ideal can contain strictly an ideal.

Theorem 3.8. (Avoidance Lemma)

Let R be a ring, let $P_1, \ldots, P_n \in \operatorname{Spec}(R)$ and I be an ideal of R such that $I \subseteq \bigcup_{k=1}^{n} P_k$. Then $I \subseteq P_l$ for some $1 \le l \le n$.

Proof : ....

Theorem 3.9. (Intersection Lemme)

Let R be a ring, let $P \in \operatorname{Spec}(R)$ and $I_1, \ldots, I_n$ be ideals of R such that $\bigcap_{k=1}^{n} I_k \subseteq P$. Then there exists $1 \le l \le n$ such that $I_l \subseteq P$.

Proof : ....

1.4 Radical

An element $a \in A$ is nilpotent if there exists $n \in \mathbb{N}$ such that $a^n = 0$. The set of nilpotent elements of R is denoted $\operatorname{Nil}(R)$ called the nilradical of R. That is

$$\operatorname{Nil}(R) = \{a \in R \;/\; \exists n \in \mathbb{N},\ a^n = 0\}$$

Proposition 4.1.

Let R be a ring. The nilradical of R is an ideal of R.

Proof : ....

Theorem 4.2.

Let R be a ring. Then

$$\operatorname{Nil}(A) = \bigcap_{P \in \operatorname{Spec}(A)} P$$

Proof : ....

Definition 4.3.

Lett R be a ring and I be an ideal of R. The radical of I denoted $\sqrt{I}$ is;

$$\sqrt{I} := \{a \in A \ / \ \exists n \in \mathbb{N},\ a^n \in I\}$$

Examples :

1. $\sqrt{(0)} = \mathrm{Nil}(R)$.
2. In the ring $\mathbb{Z}$, $\sqrt{(8)} = (2)$, and $\sqrt{(24)} = (6)$.

Proposition 4.4.

Let R be a ring and I, J be ideals of R.

1. *$\sqrt{I}$ is an ideal of R containing I.*
2. *If $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.*
3. *$\sqrt{\sqrt{I}} = \sqrt{I}$.*
4. *$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*
5. *$\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.*

Proof : ....

Theorem 4.5.

Let R be a ring and I be an ideal of R. Then

$$\sqrt{I} = \bigcap_{P \in \mathrm{Spec}(A), I \subseteq P} P$$

Proof : ....

Definition 4.6.

Let R be a ring. The Jacobson radical of R denoted $\mathrm{J}(R)$ is the ideal

$$\mathrm{J}(A) := \bigcap_{M \in \mathrm{Max}(A)} M$$

Remark : Let R be a ring, then $\text{Nil}(R) \subseteq J(R)$.

Proposition 4.7.

Let R be a ring and $a \in R$. Then $a \in \text{J}(R)$ if and only if for all $x \in 4$, $1 - ax \in R^\times$. That is

$$J(R) = \{a \in R \;/\; \forall x \in R,\;\; 1 - ax \in R^\times\}$$

Proof : ....

1.5 Exercises

Exercise 1.1

Let R be a ring. Let $(a, x) \in \text{Nil}(R) \times R^\times$. Show that $a + x \in R^\times$.

Exercise 1.2

Let R be a ring and I be an ideal of R such that $\cap_{n\geq 1} I^n = (0)$. Show that for any $x \in I$, $1 + x \notin Z(A)$.

Exercise 1.3

Let R be a ring, $(P_\alpha)_{\alpha\in\Gamma}$ be a family of prime ideals of R, and $I = \bigcap_{\alpha\in\Gamma} P_\alpha$. Show that $\sqrt{I} = I$.

Exercise 1.4

Let R be a ring such that for any $x \in R$, there exists $n \geq 2$ such that $x^n = x$. Show that every prime ideal is maximal.

Exercise 1.5

Let R be a ring such that every prime ideal is principal. We well show that every ideal is principal. Assume the contrary, that is R has a non *principal ideal. Set*

$$X = \{I \text{ idéal de } R \ / \ I \text{ non principal}\}$$

1. *Show that X is a nonempty inductive set.*
2. *Deduce that X has a maximal element, say P.*
3. *Let $x, y \in R$ such that $xy \in P$ and $x, y \notin P$. Set $J = P + (y)$ et $J' = (P : J) = \{z \in A \ / \ zJ \subseteq P\}$.*
   (a) *Show that that J et J' are principal ideals.*
   (b) *Show that $P = JJ'$, deduce that P is principal.*
4. *Show that P is prime.*
5. *Conclusion.*

Exercise 1.6

Let $R_1, \ldots, R_m$ be a rings, $R = R_1 \times \ldots \times R_m$ their direct product. For $1 \leq k \leq m$, denote $s_k : R \to R_k$ the kth projection.

1. *For $1 \leq k \leq m$, let I_k be an ideal of A_k. Show that $I_1 \times \ldots \times I_m$ is an ideal of R.*
2. *Let I be an ideal of R. Set $I_k = s_k(I)$.*
   (a) *For $1 \leq k \leq m$, show that I_k is an ideal of R_k.*
   (b) *Show that $I = I_1 \times \ldots \times I_m$.*
3. *Let $P \in \mathrm{Spec}(A)$, write $P = P_1 \times \ldots \times P_m$, where P_k is an ideal of R_k. For $1 \leq k \leq m$, denote e_k the element of R whose components are all zero except the kth, which is equal to 1.*
   (a) *Show that $\sum_{k=1}^{m} e_k = 1 (= 1_A)$, $e_k e_l = 0$ if $k \neq l$ and $e_k^2 = e_k$.*
   (b) *Show that there exists $1 \leq j \leq m$ such that $e_j \notin P$.*
   (c) *Let $1 \leq k \leq m$ with $k \neq j$. Show that $e_k \in P$.*

(d) *Deduce that* $P_k = A_k$ *si* $k \neq j$ *and that* P_j *is a prime ideal of* R_j.

(e) *Show that if* P *is a maximal ideal of* R *then* P_j *is a maximal ideal of* R_j.

Exercise 1.7

Let R *be an integral domain. Show that* $A[X]$ *is an integral domain.*

Exercise 1.8

Let R *be a ring. Show that* $A[X]$ *is a principal if and only if* R *is a field.*

Exercise 1.9

Let R *be a ring and* $P = \sum_{k=0}^{n} a_k X^k \in A[X]$.

1. *Show that* P *is invertible if and only if,* a_0 *is invertible and* $a_1, \ldots, a_n$ *are nilpotents.*
2. *Show that* P *is nilpotent if and only if the* a_k *are nilpotents.*
3. *Deduce that* $\mathrm{Nil}(A[X]) = \mathrm{J}(A[X])$.

Exercise 1.10

Let R *be a ring and* I *be an ideal of* R. *Set*

$$I[X] = \{\sum_{k=0}^{n} a_k X^k \in A[X] \ / \ n \geq 0, \ a_k \in I\}$$

$I[X]$ *the set of polynomials with à coefficients in* I.

1. *Show that* $I[X]$ *is an ideal of* $R[X]$.
2. *Show that* $A[X]/I[X]$ *is isomorphic to* $(A/I)[X]$.
3. *Deduce that* I *is prime if and only if* $I[X]$ *is prime.*

Exercise 1.11

Let R be a ring and $I_1,\ldots,I_m$ be ideals of R such that $\sum_{k=1}^{m} I_k = R$. Let $l_1,\ldots,l_m \in \mathbb{N}$. Show that $\sum_{k=1}^{m} I_k^{l_k} = R$

Exercise 1.12

Let R be a ring and I, J be ideals of R.

1. *Show that if $\sqrt{IJ} = A$ then $I = J = R$.*
2. *Let $P \in \mathrm{Spec}(R)$ such that $IJ = P$. Show that $I = P$ or $J = P$.*

Exercise 1.13 ((Zarisky Topology))

Let R be a ring. For I ideal of R, denote $V(I)$ the set of prime ideals of R containing I, that is

$$V(I) = \{P \in \mathrm{Spec}(R) \ / \ I \subseteq P\}$$

1. *Lett I be an ideal of R. Show that $V(I) = V(\sqrt{I})$.*
2. *Lett I, J be ideals of R. Show that $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.*
3. *Show that $V(0) = \mathrm{Spec}(A)$ and $V(A) = \emptyset$.*
4. *Let I, J be ideals of R. Show that $V(I \cap J) = V(I) \cup V(J)$.*
5. *Let $(I_\alpha)_{\alpha\in\Gamma}$ be a family of ideals of R. show that $\cap_{\alpha\in\Gamma} V(I_\alpha) = V(\sum_{\alpha\in\Gamma} I_\alpha)$.*

   We deduce, from the previous properties, that there exists a unique topology of $\mathrm{Spec}(R)$ whose closed subsets are the $V()I$, where I is an ideal of R. this topology is called the Zariski Topology on $\mathrm{Spec}(R)$. For I ideal of R denote $D(I) = \mathrm{Spec}(A) \setminus V(I) = \{P \in \mathrm{Spec}(A) \ / \ I \not\subseteq P\}$.

6. *Show that* $D((f))$, *where* $f \in A$ *form a basis*[a] *of open subsets with respect to Zariski topology.*

7. *Show that* $\mathrm{Spec}(A)$ *is quasi-compact.*

8. *Let* $f \in A$. *Show that* $D(f) = \emptyset$ *if and only if* $f \in \mathrm{Nil}(A)$.

   Let $f : A \to B$ *be a morphism of rings. denote* $f^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *de maps defined for each* $P \in \mathrm{Spec}(B)$ *by* $f^*(P) = f^{-1}(P)$.

9. *Let* I *be an ideal of* R. *Show that* $f^{*-1}(V(I)) = V(f(I)B)$ *(where* $f(I)B$ *is that ideal of* B *generated by* $f(I)$*).*

10. *Deduce that* f^* *is continuous.*

11. *Let* I *be an ideal of* R. *Show that* $\mathrm{Spec}(A/I)$ *is homeomorphic to* $V(I)$

[a] That is, stable under finite intersection and each open is union of elements of this basis

Exercise 1.14

Let R *be a ring, we endowed* $\mathrm{Spec}(R)$ *with the Zariski topology.*
Show that $\mathrm{Spec}(A)$ *est connected id and only if the only idempotent*[a] *elements of* R *are* 0 *et* 1.

[a] An element $a \in R$ is idempotent if $a^2 = a$

Exercise 1.15

Let I *be an ideal the ring* R *and* $P \in \mathrm{Spec}(R)$.

1. *Show that* $\overline{\{P\}} = V(P)$.

2. *deduce that* $\{P\}$ *is closed subset if and only if* $P \in \mathrm{Max}(R)$.

Exercise 1.16

Let I be an ideal of R. Show that $D(I)$ is quasi-compact if and only if there exists $a_1,\dots,a_m \in R$ such that $\sqrt{I} = \sqrt{(a_1,\dots,a_m)}$.

Exercise 1.17

Let R be a ring, let I be an ideal of R and $a \in R$ such that $I+(a)$ and $(I:a) := \{x \in A \ / \ xa \in I\}$ are finitely generated.

1. *Show that there exists $d_1,\dots,d_m \in I$ such that $I+(x) = (d_1,\dots,d_m,x)$.*
2. *Let x be an element of I of the form $x = \sum_{k=1}^{m} \alpha_k d_k + rx \in I$. Justifies that $r \in (P:a)$.*
3. *Deduce that I id finitely generated.*

Exercise 1.18

Let R be a ring whose prime ideals are finitely generated. Set

$$X = \{I \text{ idéal de } R \ / \ I \text{ not finitely generated}\}$$

Assume that X is not empty.

1. *Show that X has a maximal element P.*
2. *Show that there exists $a, b \in A$ such that $ab \in P$ and $a, b \notin P$.*
3. *Show that $P+(a)$ and $(P:a)$ are finitely generated.*
4. *deduce that P is finitely generated.*
5. *Conclude.*