Commutative Algebra

Refresher course

Andrea Fanelli

Collège Sciences et technologies
Université de Bordeaux

03 septembre 2024

Commutative algebra

Commutative algebra is...

... "linear algebra, replacing a filed k with a commutative ring R with unity".

Why ?

For instance, it provides technical tools for algebraic geometry, number theory, etc...

Reference

Olivier Brinon : *Complements of Commutative Algebra.*

Rings

R ring	Examples and facts
$R = k$ field	e.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{F}_p, \overline{\mathbb{Q}}, \ldots$ ideals : (0), k prime ideals : (0) maximal ideals : (0)
PID (principal ideal domain)	$\mathbb{Z}$ ideals : $n\mathbb{Z}$, with $n \in \mathbb{N}_0$ prime ideals : (0), $p\mathbb{Z}$, with p prime maximal ideals : $p\mathbb{Z}$, with p prime $k[x]$ ideals : $(f(x))$, with $f(x) \in k[x]$ prime ideals : (0), $(p(x))$, with $p(x) \in k[x]$ irreducible maximal ideals : $(p(x))$, with $p(x) \in k[x]$ irreducible **Fact :** nonzero prime ideals are maximal.
UFD (unique factorisation domain)	$\mathbb{Z}[x]$: ideals : $(2, x)$ is *not* principal prime ideals : **exercise** $k[x, y]$: ideals : (x, y) is *not* principal prime ideals : **exercise** Every element can be decomposed "uniquely" in irreducible factrors. **Fact :** irreducible elements are prime. **Fact :** prime ideal $\not\Rightarrow$ maximal ideal. **Theorem** : R UFD $\Rightarrow$ $R[x]$ UFD [main ingredient is **Gauss Lemma :** Let $K = \mathrm{Frac}(R)$ and $P \in R[x]$ such that $c(P) = 1$.Then P is irreducible in $R[x]$ iff it is irreducible in $K[x]$]

R-modules [category (R−Mod)]

Definition (objects)

An R-module is $(M, +, \cdot)$, where $(M, +)$ is an abelian group and the application $\cdot : R \times M \to M$ verifies :

1. $(a+b)\cdot m = a\cdot m + b\cdot m$ for all $a, b \in R$ and $m \in M$;
2. $(ab)\cdot m = a\cdot(b\cdot m)$ for all $a, b \in R$ and $m \in M$;
3. $a\cdot(m_1 + m_2) = a\cdot m_1 + a\cdot m_2$ for all $a \in R$ and $m_1, m_2 \in M$;
4. $1\cdot m = m$ for all $m \in M$.

This amounts to a ring homomorphism $R \to \mathrm{End}(M)$.

Definition (arrows)

Let M and N be R-modules. An R-linear map from M to N is a group homomorphism $f : M \to N$ such that $f(am) = af(m)$ for all $a \in R$ and $m \in M$.

The set of R-linear maps from M to N is an abelian group denoted $\mathrm{Hom}_R(M, N)$.

Definition (subobject)

Let M be an R-modules. A sub-R-module of M is an additive subgroup $N \subseteq M$ such that $n_1 + an_2 \in N$ for all $n_1, n_2 \in N$ and $a \in R$.

R-modules [category (R−Mod)]

Definition (kernel, image, isomorphism)

The kernel of $f \in \mathrm{Hom}_R(M, N)$ is the submodule $\ker(f) := f^{-1}(0)$ of M.
The image of f is the submodule $\mathrm{im}(f) := f(M) =$ of N.
One says that f is an isomorphism if $\ker(f) = \{0\}$ and $\mathrm{im}(f) = N$.

Definition (quotient)

Let M be an R-module and N a sub-R-module. The quotient group M/N is naturally endowed with a R-module structure. The R-module M/N is the quotient of M by N. ($+$ universal property).

Definition (generation)

Let M be an R-module.

- Let $X \subset M$ be a subset. There exists a smallest sub-R-module N of M such that $X \subset N$: it is the sub-R-module of M generated by X (it is the intersection of all sub-R-modules of M that contain X).
- A subset $X \subset M$ generates M when the sub-R-module of M generated by X is M itself.
- The R-module M is of **finite type** if it is generated by a finite part, i.e. if there exist $m_1, \ldots m_n \in M$ such that $M = Rm_1 + \cdots + Rm_n$.

R-modules [category $(R-Mod)$]

Definition (products and direct sums)

Let Λ be a set and $(M_\lambda)_{\lambda\in\Lambda}$ a family of R-modules.

- The product $\prod_{\lambda\in\Lambda} M_\lambda$ is the R-module of maps $\Lambda \to \bigcup_{\lambda\in\Lambda} M_\lambda$ such that $f(\lambda) \in M_\lambda$ for all $\lambda \in \Lambda$.
- The direct sum $\bigoplus_{\lambda\in\Lambda} M_\lambda$ is the sub-R-module of $\prod_{\lambda\in\Lambda} M_\lambda$ consisting of maps $\Lambda \to \bigcup_{\lambda\in\Lambda} M_\lambda$ such that the set $\{\lambda \in \Lambda \mid f(\lambda) \neq 0\}$ is finite.
- If $M_\lambda = M$ for all $\lambda \in \Lambda$, the product and the direct sum are denoted by M^Λ and $M^{(\Lambda)}$ respectively. If $\Lambda = \{1, \dots, n\}$, both are denoted by M^n.

Definition (free modules)

A free R-module is an R-module isomorphic to $R^{(\Lambda)}$ for some set Λ.

The theory of free modules is very similar to the one of vector spaces. For instance, if M and N are two free R-modules of rank n and m respectively, one has $\mathbf{Hom}_R(M, N) \simeq \mathbf{Mat}_{n\times m}(R)$.

But many modules are not free (e.g. $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$).

Exercise

Let M an R-module of finite type and $f\colon M \to R^n$ a surjective morphism. Show that $M = N \oplus \ker(f)$, where N is a submodule of M isomorphic to R^n through f. Show that $\ker(f)$ is of finite type.

R-modules [category (R−Mod)]

Definition (torsion)

- Let M be an R-module and $m \in M$. The annihilator of m is the ideal of R defined by $\mathrm{ann}_R(m) = \{a \in R \mid am = 0\}$.
- One says m is torsion if $\mathrm{ann}_R(m) \neq \{0\}$, i.e. if it exists a $a \in R \setminus \{0\}$ such that $am = 0$. One denotes by M_{tors} the set of torsion elements in M.
- One says that M is torsion-free (resp. is torsion) if $M_{\mathrm{tors}} = \{0\}$ (resp. $M_{\mathrm{tors}} = M$).

Exercise

Assume R is an integral domain, then M_{tors} is a sub-module of M and M/M_{tors} is torsion-free.

Assume R is PID, then every torsion-free module of finite type is free (this is a theorem !).

R-algebras [category (R$-$Alg)]

Definition

- An R-algebra is a ring homomorphism $R \to A$, whose image lies in the centre of A.
- A morphism between two R-algebras A_1 and A_2 is a ring homomorphism $f: A_1 \to A_2$ such that the following diagram commutes

$$\begin{tikzcd} A_1 \arrow[rr, "f"] & & A_2 \\ & R \arrow[ul] \arrow[ur] & \end{tikzcd}$$

An R-algebra $R \to A$ (usually denoted by A) is naturally endowed with an R-module structure.

- Any field extension L/K is a K-algebra.
- The polynomial ring $R[x_\lambda]_{\lambda \in \Lambda}$ is an R-algebra.

Definition (vocabulary)

Let $\phi: R \to A$ be an R-algebra.

- A sub-R-algebra is a subring $A' \subseteq A$ such that the inclusion map is a morphism of R-algebras.
- Let $X = \{x_\lambda\}_{\lambda \in \Lambda} \subset A$ be a subset. There exists a smallest sub-R-algebra $R[x_\lambda]_{\lambda \in \Lambda}$ of M of B such that $X \subset N$: it is the sub-R-algebra of A generated by X.
- An R-algebra is of **finite type** if it is generated by a finite set (i.e. there exists a surjective morphism of R-algebras $R[x_1, \ldots, x_n] \to B$).
- An R-algebra is **finite** if it is finite as R-module.

Exercise

Describe the set of prime ideals of R, when $R = k[x, y]$ and $\mathbb{Z}[x]$.

Exercise

Let M an R-module of finite type and $f : M \to R^n$ a surjective morphism. Show that $M = N \oplus \ker(f)$, where N is a submodule of M isomorphic to R^n through f. Show that $\ker(f)$ is of finite type.

Exercise

Assume R is an integral domain and M and R-module. Then M_{tors} is a sub-module of M and M/M_{tors} is torsion-free.

Noetherianity

Definition/Proposition

Let M be an R-module. The following properties are equivalent :

1. M is noetherian, i.e. all its sub-R-modules are of finite type ;
2. every ascending sequence of sub-R-modules of M is stationary ;
3. every non empty subset of submodules of M has a maximal element (for the inclusion).

A ring R is noetherian if it is noetherian as R-module.

The polynomial ring $R[x_\lambda]_{\lambda\in\Lambda}$ with Λ infinite is not noetherian, since the ideal generated by $\{x_\lambda\}_{\lambda\in\Lambda}$ is not of finite type.

Theorem (Hilbert)

If R is noetherian, so is $R[x]$.

Exercice

- Let M be an R-module and N an R-submodule of M. Prove that M is noetherian iff N and M/N are both noetherian.
- Prove that the product of two noetherian R-modules is noetherian.
- Prove that if R is a noetherian ring, any R-module of finite type is a noetherian.

Exercice

Show that if R is noetherian domain, non-zero non-invertible elements can be factored into a product of irreducible elements.

Tensor product of modules

Let M and N be R-modules. Let L be an R-module.
A map $f\colon M \times N \to L$ is bilinear if it left and right linear.

Construction

Consider the R-module $R^{(M\times N)}$ and its canonical basis $(e_{(m,n)})_{(m,n)\in M\times N}$.
Let K be the submodule of $R^{(M\times N)}$ generated by the following elements :

- $e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}$ for $m_1, m_2 \in M$ and $n \in N$;
- $e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}$ for $m \in M$ and $n_1, n_2 \in N$;
- $e_{(am,n)} - ae_{(m,n)}$ and $e_{(m,an)} - ae_{(m,n)}$ for $a \in R$, $m \in M$ and $n \in N$.

Define the **tensor product** $M \otimes_R N := R^{(M\times N)}/K$.
Consider the composition $\phi = \pi \circ i$ where $i\colon M \times N \to R^{(M\times N)}$, $(m,n) \mapsto e_{(m,n)}$ and $\pi\colon R^{(M\times N)} \to M \otimes_R N$ the canonical projection. By construction, ϕ is bilinear.

The tensor product comes with a universal property.

Tensor product of algebras

Construction

Let A and B be R-algebras. The multiplication on A (resp. B) provides maps $m_A\colon A \otimes_R A \to A,\ x \otimes y \mapsto xy$ and $m_B\colon B \otimes_R B \to B,\ x \otimes y \mapsto xy$. Moreover, there is an isomorphism $\varepsilon\colon A \otimes_R B \to B \otimes_R A,\ x \otimes y \mapsto y \otimes x$. Consider the composite

$$(A \otimes_R B) \otimes_R (A \otimes_R B) \xrightarrow{\mathrm{Id}_A \otimes \varepsilon \otimes \mathrm{Id}_B} (A \otimes_R A) \otimes_R (B \otimes_R B) \xrightarrow{m_A \otimes m_B} A \otimes_R B$$

This map endows the product $A \otimes_R B$ with an R-algebra structure : the product is simply given by

$$(x_1 \otimes y_1) \cdot (x_2 \otimes y_2) = (x_1 x_2 \otimes y_1 y_2).$$

There are natural morphisms of R-algebras $i_A\colon A \to A \otimes_R B,\ x \mapsto x \otimes 1_B$ and $i_B\colon B \to A \otimes_R B,\ y \mapsto 1_A \otimes y$

The tensor product comes with a universal property.

Remark

If A and B are commutative, the tensor product $(A \otimes_R B, i_A, i_B)$ is the coproduct in the category of **commutative** R-algebras.

Localisation

Definition

A subset $S \subseteq R$ is called multiplicative if $0 \notin S$, $1 \in S$ and if S is stable under multiplication.

For example, the following are multiplicative sets :

- $R^\times$;
- $\{f^n\}_{n \in \mathbb{Z}_{\geq 0}}$, where $f \in R$ is not nilpotent ;
- $R \setminus \mathfrak{p}$ where $\mathfrak{p} \subset R$ is a prime ideal.

Construction

Let $S \subseteq R$ be a multiplicative set. Endow the set $R \times S$ with the binary relation $\sim$ defined by

$$(a_1, s_1) \sim (a_2, s_2) \quad \text{if} \quad (\exists t \in S) \quad t(a_1 s_2 - a_2 s_1) = 0.$$

This is an equivalence relation. Denote by $S^{-1}R := (R \times S)/\sim$ the quotient set. One denotes by $\frac{a}{s}$ the image of (a, s) via the quotient map. One can define sum and product making $S^{-1}R$ a commutative ring with unity. The map

$$\iota \colon R \to S^{-1}R \qquad a \mapsto \frac{a}{1}$$

is a ring homomorphism.

The R-algebra $S^{-1}R$ is the **localisation** of R with respect to the multiplicative set S.

The localisation comes with a universal property.

Localisation

Properties

- When R is an integral domain, the relation $\sim$ is nothing but the "usual" relation $(a_1, s_1) \sim (a_2, s_2)$ if $a_1 s_2 = a_2 s_1$.
- $\ker(\iota) = \{a \in R \mid (\exists s \in S) sa = 0\}$ so ι is injective when R is an integral domain.

Examples

- Assume R is an integral domain. Then $R \setminus \{0\}$ is multiplicative and $(R \setminus \{0\})^{-1} R = \mathrm{Frac}(R)$ is the fraction field of R.
- Let $f \in R$. We denote by R_f the localisation of R with respect to the multiplicative set $\{f^n\}_{n \in \mathbb{Z}_{\geq 0}}$. One can easily show that $R_f \simeq R[x]/(fx - 1)$;
- If $\mathfrak{p} \subset R$ is a prime ideal, we denote by $R_{\mathfrak{p}}$ the localization of R with respect to the multiplicative set $R \setminus \mathfrak{p}$.

Localisation

Definition

Let $S \subseteq R$ be a multiplicative set and M an R-module. The localisation $S^{-1}M$ of M with respect to S is defined as the quotient $M \times S$ with the relation $\sim$ defined by

$$(m_1, s_1) \sim (m_2, s_2) \quad \text{if} \quad (\exists t \in S) \quad t(s_2 m_1 - s_1 m_2) = 0.$$

This is a $S^{-1}R$-module.
An R-linear map $f : M \to N$ induces a $S^{-1}R$-linear map $f_S : S^{-1}M \to S^{-1}N, \ m/s \mapsto f(m)/s$ and the natural map

$$\mathrm{Hom}_{S^{-1}R}(S^{-1}M, N) \to \mathrm{Hom}_R(M, N)$$

is an isomorphism.

Localisation

We denote by Spec(R) the set of prime ideals if R.

Proposition

Let $S \subset R$ be a multiplicative set. The maps

$$\{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\} \leftrightarrow \mathrm{Spec}(S^{-1}R)$$

$$\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$$

$$\mathfrak{q} \cap R := \iota^{-1}(\mathfrak{q}) \leftarrow\!\shortmid \mathfrak{q}$$

are increasing (for the inclusion) bijections inverse to each other.

Definition

A **local ring** is a ring having only one maximal ideal.

Easy fact

The localisation $R_{\mathfrak{p}}$ at a prime ideal $\mathfrak{p} \subset R$ is a local ring.

Nakayama's Lemma

Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module such that $M = \mathfrak{m}M$. Then $M = 0$.

Exercise

Let M be an R-module. Then $M = \{0\}$ if and only if $M_{\mathfrak{m}} = \{0\}$ for all maximal ideal $\mathfrak{m} \subset R$.

Exercise

- Let $\sqrt{(0)} \subset R$ be the nilradical of R, i.e. $\sqrt{(0)} := \{r \in R \mid r^n = 0 \text{ for some } n\}$. Show that
$$\sqrt{(0)} = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$$
- Suppose that R is noetherian and show that $\sqrt{(0)}$ is a *finite* intersection of prime ideals.

Exercice

- $(\mathbb{Z}/a\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/b\mathbb{Z}) \simeq \mathbb{Z}/gcd(a,b)\mathbb{Z}$ for all $a, b \in \mathbb{Z}_{>0}$;
- $(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) = 0$;

Exercise

Let $R = k(x) \otimes_k k(y)$ be the tensor product of two purely transcendental extensions of k of transcendence degree 1.

- Show that R is isomorphic to the localisation of $k[x, y]$ with respect to the multiplicative system S of non-zero elements of the form $f(x)g(y) \in k[x, y]$.
- let $\mathfrak{m}$ be a maximal ideal of $k[x, y]$. Show that there exists a $f(x) \in \mathfrak{m} \setminus \{0\}$. Deduce that $S \cap \mathfrak{m} \neq \emptyset$.
- Describe maximal ideals of R.

Integral extensions

Let $f : R \to A$ be an R-algebra.

Definition

An element $a \in A$ is integral over R if there exists a monic polynomial $P \in R[x]$ such that $P(a) = 0$. The equality $P(a) = 0$ is then called an equation of integral dependence of a over R.
One says that A is integral over R if all its element are integral over R.

Proposition

Let $a \in A$. The following are equivalent :

- a is integral over R ;
- $R[a]$ is a finite R-algebra.

Definition/Proposition

The set of elements in A that are integral over R is a sub-R-algebra of A, which is called the **integral closure** of R in A.

Assume R is an integral domain and put $K = \mathrm{Frac}(R)$. The integral closure of R is its integral closure in K.

One says that R is integrally closed if it is equal to its integral closure, i.e. when the only element in K that are integral over R are elements in R.

Proposition

UFD are integrally closed.