Algèbre et théorie de Galois

Anna Cadoret

Cours de Master 1 à Sorbonne Université - version 2019 (en cours d'actualisation)

20 juin 2021

Table des matières

Bibliographie

[AM69] M.F. Atiyah et I.G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[D18] J.F. Dat, *Algèbre et théorie de Galois*, polycopié de cours disponible sur : https ://webusers.imj-prg.fr/ jean-francois.dat/enseignement/AlgebreM1/ATG1718.pdf

[L02] S. Lang, *Algebra (3rd ed.)*, G.T.M. **211**, Springer, 2002.

[S68] J.P. Serre, *Corps locaux*, Hermann, 1968.

Remerciements : Sarah Wajsbrot (promotion 2018-19).

Ne pas hésiter à me signaler les coquilles et, le cas échéant, me demander de clarifier certains arguments/définitions. Tout commentaire permettant d'améliorer l'exposition est le bienvenu.

On utilisera les notations $X \twoheadrightarrow Y$, $X \hookrightarrow Y$, $X \tilde{\to} Y$ (ou $X \xrightarrow{\sim} Y$) pour une application ensembliste $X \to Y$ respectivement surjective, injective, bijective.

On aura parfois recours à l'axiome du choix sous l'une des formulations équivalentes suivantes :

— Un produit cartésien d'ensembles finis non vides est non vide.

— (Lemme de Zorn) tout ensemble non vide ordonné inductif admet un élément maximal. (On rappelle qu'un ensemble ordonné est dit inductif si toute suite croissante admet un majorant).

Première partie

Anneaux - généralités

Chapitre 1

Premières définitions et constructions

1.1 Définitions

Déroulons les définitions.

1.1.1 Monoïdes et groupes

Définition 1.1.1.1. Un *monoïde* est un couple $(M, \times)$ formé d'un ensemble M et d'une application $\times : M \times M \to M$ qui vérifient les axiomes suivants :

1. associativité : $(l \cdot m) \cdot n = l \cdot (m \cdot n)$, $l, m, n \in M$;
2. élément neutre : il existe $e_M \in M$ tel que $m \cdot e_M = m = e_M \cdot m$, $m \in M$.

On dit qu'un monoïde $(M, \times)$ est un *groupe* si, de plus

3. Inverse : pour tout $m \in M$ il existe $n \in M$ tel que $m \cdot n = e_M = n \cdot m$.

Un monoïde $(M, \cdot)$ est dit *abélien* ou *commutatif* si $m \cdot n = n \cdot m$, $m, n \in M$.

Définition 1.1.1.2. Étant donnés deux monoïdes M, N, un *morphisme de monoïdes* est une application $\phi : M \to N$ qui vérifie :

1. $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$, $m, n \in M$;
2. $\phi(e_M) = e_N$.

Remarquons que l'application identité $Id : M \to M$ est un morphisme de monoïdes et que si $\phi : L \to M$ et $\psi : M \to N$ sont des morphismes de monoïdes alors $\psi \circ \phi : L \to N$ est un morphisme de monoïdes.

On notera $Hom_{Mono}(M, N)$ l'ensemble des morphismes de monoïdes $\phi : M \to N$ et, si $M = N$, $End_{Mono}(M) := Hom_{Mono}(M, M)$. Étant donnés deux groupes M, N, un morphisme de groupes $\phi : M \to N$ est un morphisme entre les monoïdes sous-jacents. Dans ce cas, on notera plutôt $Hom_{Grp}(M, N)$ et $End_{Grp}(M)$ que $Hom_{Mono}(M, N)$, $End_{Mono}(M, N)$.

1.1.2 Anneaux

Définition 1.1.2.1. Un *anneau* est un triplet $(A, +, \cdot)$ formé d'un ensemble A et de deux applications $+, \cdot : A \times A \to A$ - appelées respectivement l'addition et la multiplication - vérifiant les axiomes suivants :

1. $(A, +)$ est un groupe abélien ; on note 0_A (ou simplement 0) son élément neutre (appelé zéro) et $-a$ l'inverse d'un élément $a \in A$.
2. $(A, \cdot)$ est un monoïde ; on note 1_A (ou simplement 1) son élément neutre (appelé unité).
3. La multiplication est distributive par rapport à l'addition *i.e.* $a \cdot (b + c) = a \cdot b + a \cdot c$ et $(b + c) \cdot a = b \cdot a + c \cdot a$, $a, b, c \in A$.

Un anneau A est dit *commutatif* si $a \circ b = b \circ a$, $\forall a, b \in A$.

Remarque 1.1.2.1. Dans la suite, on écrira presque toujours ab au lieu de $a \cdot b$, $0 := 0_A$, $1 := 1_A$. Par ailleurs, on omet presque toujours les données $+, \cdot$ des notations.

Le monoïde $(A, \cdot)$ n'est pas un groupe en général ; on note $A^\times \subset A$ le sous-ensemble des éléments inversibles *i.e.* l'ensemble des $a \in A$ tel qu'il existe $b \in A$ tel que $ab = 1 = ba$; c'est un groupe d'élément neutre 1. On note alors $a^{-1} \in A^\times$ l'inverse d'un élément de $a \in A^\times$.

On dit qu'un anneau A est *un anneau à division* ou un *corps gauche* si $1 \neq 0$ et $A \backslash \{0\} = A^\times$. Si A est de plus commutatif, on dit simplement que A est un *corps*.

Exemples 1.1.2.1. — L'*anneau nul* $A = \{0\}$ (on n'a pas exclu $1 \neq 0$ dans la définition d'anneaux).
— L'anneau $\mathbb{Z}$ des entiers. Dans ce cas $\mathbb{Z}^\times = \{\pm 1\}$.
— Les corps commutatifs, par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
— Si M est un groupe abélien, l'ensemble $End_{Grp}(M)$ des endomorphismes du groupe abélien M muni de $(\phi + \psi)(m) = \phi(m) + \psi(m)$ et $(\psi \cdot \phi)(m) = \psi \circ \phi(m)$ est un anneau (non commutatif en général) de zéro l'application nulle et d'unité l'application identité. Dans ce cas, $End_{Grp}(M)^\times = Aut_{Grp}(M)$.
— Si M est un espace vectoriel sur un corps commutatif k, l'ensemble $End_k(M)$ des endomorphismes du k-espace vectoriel M muni de $(\phi+\psi)(m) = \phi(m)+\psi(m)$ et $(\psi\cdot\phi)(m) = \psi\circ\phi(m)$ est un anneau (non commutatif si M est de k-dimension ≥ 2) de zéro l'application nulle et d'unité l'application identité. Dans ce cas, $End_k(M)^\times = GL_k(M)$.
— On rencontre aussi beaucoup d'anneaux en analyse : les anneaux $\mathcal{C}(X, \mathbb{R})$ ou $\mathcal{C}(X, \mathbb{C})$ de fonctions continues à valeurs réelles ou complexes sur un espace topologique X, les anneaux $L^p(X, \mu)$ de fonctions intégrables sur un espace mesuré (X, μ), les anneaux de séries entières *etc.*

Définition 1.1.2.2. Étant donnés deux anneaux A, B, un *morphisme d'anneaux* est une application $\phi : A \to B$ qui induit à la fois un morphisme de groupes $\phi : (A, +) \to (B, +)$ et de monoides unitaires $\phi : (A, \cdot) \to (B, \cdot)$ *i.e* qui vérifie :

1. $\phi(a + b) = \phi(a) + \phi(b)$, $a, b \in A$;q
2. $\phi(ab) = \phi(a)\phi(b)$, $a, b \in A$ et $\phi(1) = 1$;

On remarquera que l'application identité $Id : A \to A$ est un morphisme d'anneaux et que si $\phi : A \to B$ et $\psi : B \to C$ sont des morphismes d'anneaux alors $\psi \circ \phi : A \to C$ est un morphisme d'anneaux. On notera $Hom(A, B)$ l'ensemble des morphismes d'anneaux $\phi : A \to B$ et, si $A = B$, $End(A) := Hom(A, A)$.

On dit qu'un morphisme d'anneaux $\phi : A \to B$ est *injectif*, (resp. *surjectif*, resp. un *isomorphisme*) si l'application d'ensembles sous-jacente est injective (resp. surjective, resp. bijective). On vérifie que si $\phi : A \to B$ est un isomorphisme d'anneaux, l'application inverse $\phi^{-1} : B \to A$ est automatiquement un morphisme d'anneaux. Comme un morphisme d'anneaux $\phi : A \to B$ est en particulier un morphisme de groupes, $\phi : A \to B$ est injectif si et seulement si $\ker(\phi) := \phi^{-1}(0_B) = \{0_A\}$. On notera aussi $\mathrm{im}(\phi) := \phi(A)$.

Si $\phi : A \to B$ est un morphisme d'anneaux, on vérifie que $\phi(A^\times) \subset B^\times$ et que $\phi : A \to B$ induit par restriction un morphisme de groupes $\phi : A^\times \to B^\times$.

1.1.2.1 Sous-anneaux

Si A est un anneau, un sous-anneau de A est un sous-ensemble $A' \subset A$ tel que $1_A \in A'$ et $a' - b' \in A'$, $a' \cdot b' \in A'$, $a', b' \in A'$.

Exemples 1.1.2.2. — $\mathbb{Z}$ est un sous anneau de $\mathbb{Q}$, $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$, $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.

— Si M est un espace vectoriel sur un corps commutatif k, $End_k(M)$ est un sous-anneau de $End_{Grp}(M)$.

— $Z(A) := \{a \in A \mid a \cdot b = b \cdot a,\ b \in A\} \subset A$ est un sous-anneau de A, appelé le centre de A. Par exemple $Z(End_k(M)) = kId_M$ et $Z(A) = A$ si et seulement si A est commutatif.

— Si $\phi : A \to B$ est un morphisme d'anneaux, et $A' \subset A$ (resp. $B' \subset B$) est un sous-anneau alors $\phi(A') \subset B$ (resp. $\phi^{-1}(B') \subset A$) est un sous-anneau. En particulier, $\mathrm{im}(\phi) \subset B$ est un sous-anneau mais $\ker(\phi) \subset A$ n'est un sous-anneau que si A ou B est l'anneau nul, sinon il ne contient pas 1 (on verra un peu plus loin que $\ker(\phi)$ est ce qu'on appelle un idéal).

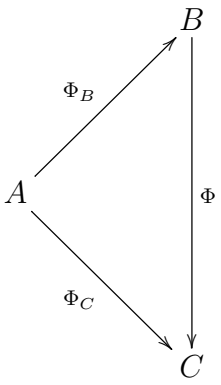
1.1.3 Algèbres sur un anneau commutatif

Soit A un anneau commutatif.

Définition 1.1.3.1. Une *A-algèbre* est un couple (B, ϕ) où B est un anneau et $\phi : A \to B$ est un morphisme d'anneaux tel que $\mathrm{im}(\phi) \subset Z(B)$.

On notera en général $\phi : A \to B$ ou simplement (lorsque la donnée de $\phi : A \to B$ ne peut prêter à confusion) B la A-algèbre (B, ϕ).

Définition 1.1.3.2. Étant données deux A-algèbres $\phi_B : A \to B$, $\phi_C : A \to C$, un *morphisme de A-algèbres* est un morphisme d'anneaux $\phi : B \to C$ tel que $\phi \circ \phi_B = \phi_C$:



On remarquera que l'application identité $Id : B \to B$ est un morphisme de A-algèbres et que si $\phi : B \to C$ et $\psi : C \to D$ sont des morphismes de A-algèbres alors $\psi \circ \phi : B \to D$ est un morphisme de A-algèbres. On notera $Hom_A(B, C)$ l'ensemble des morphismes de A-algèbres $\phi : B \to C$ et, si $B = C$, $End_A(B) := Hom_A(B, C)$. On dit encore qu'un morphisme de A-algèbres $\phi : B \to C$ est *injectif*, (resp. *surjectif*, resp. un *isomorphisme*) si l'application d'ensembles sous-jacente est injective (resp. surjective, resp. bijective). On vérifie que si $\phi : B \to C$ est un isomorphisme de A-algèbres l'application inverse $\phi^{-1} : C \to B$ est automatiquement un morphisme de A-algèbres.

Remarque 1.1.3.1. On verra dans la partie II du cours, qu'une A-algèbre $\phi : A \to B$ est aussi la même chose qu'un anneau B muni d'une structure de A-module et qu'avec cette terminologie un morphisme de A-algèbres est un morphisme d'anneaux qui est aussi un morphisme de A-modules.

Exemples 1.1.3.1. — Le *morphisme caractéristique* $c_A : \mathbb{Z} \to A$, $1 \to 1_A$ munit tout anneau A d'une structure de $\mathbb{Z}$-algèbre canonique et tout morphisme d'anneaux $\phi : A \to B$ est automatiquement un morphisme de $\mathbb{Z}$-algèbres pour ces structures (*i.e.* $\phi \circ c_A = c_B$).
— L'inclusion $\iota_A : Z(A) \hookrightarrow A$ munit tout anneau A d'une structure de $Z(A)$-algèbre canonique.
— Si A, B sont des anneaux commutatifs, tout morphisme d'anneaux $\phi : A \to B$ munit B d'une structure de A-algèbre.

Exercice 1.1.3.1 (Quaternions)**.** On considère le $\mathbb{R}$-espace vectoriel $\mathbb{H}$ de base $1, i, j, k$ muni du produit $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$ définie par $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

1. Montrer que $(\mathbb{H}, +, \cdot)$ est un anneau à division, non commutatif. Déterminer son centre et en déduire que c'est une $\mathbb{R}$-algèbre.
2. On note i une racine carré de -1 dans $\mathbb{C}$ et on considère les matrices

$$I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Montrer que le sous-$\mathbb{R}$-espace vectoriel de $M_2(\mathbb{C})$ engendré par Id, I, J, K est un sous-$\mathbb{R}$-algèbre de $(M_2(\mathbb{C}), +, \cdot)$ isomorphe à $\mathbb{H}$.

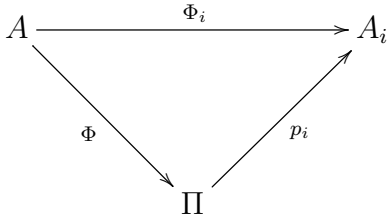
1.2 Produits

Si A_i, $i \in I$ est une famille d'anneaux, on peut munir le produit ensembliste $\prod_{i\in I} A_i$ d'une structure d'anneau en posant, pour $\underline{a} = (a_i)_{i\in I}$, $\underline{b} = (b_i)_{i\in I} \in \prod_{i\in I} A_i$

$$\underline{a} + \underline{b} = (a_i + b_i)_{i\in I}, \quad \underline{a} \cdot \underline{b} = (a_i \cdot b_i)_{i\in I}$$

On a alors $0 = (0_{A_i})_{i\in I}$, $1 = (1_{A_i})_{i\in I}$. De plus, les *projections* $p_i : \prod_{i\in I} A_i \to A_i$, $\underline{a} \to a_i$, $i \in I$ sont automatiquement des morphismes d'anneaux.

Proposition 1.2.0.1 (Propriété universelle du produit)**.** *Pour toute famille d'anneaux A_i, $i \in I$ il existe un anneau Π et une famille de morphisme d'anneaux $p_i : \Pi \to A_i$, $i \in I$ tels que pour tout anneau A et famille de morphisme d'anneaux $\phi_i : A \to A_i$, $i \in I$, il existe un unique morphisme d'anneaux $\phi : A \to \Pi$ tel que $p_i \circ \phi = \phi_i$, $i \in I$.*

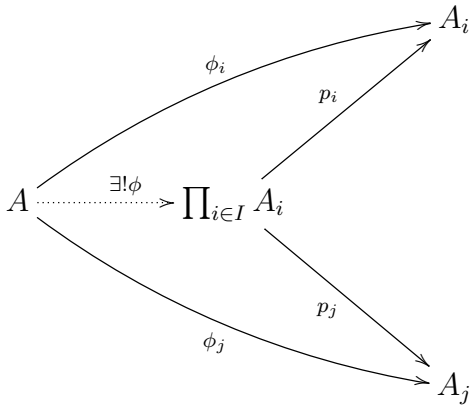


Démonstration. Vérifions que $\Pi := \prod_{i\in I} A_i$ et les $p_i : \prod_{i\in I} A_i \to A_i$, $\underline{a} \to a_i$, $i \in I$ conviennent. Si $\phi : A \to \prod_{i\in I} A_i$ existe, la condition $p_i \circ \phi = \phi_i$, $i \in I$ force $\phi(a) = (\phi_i(a))_{i\in I}$, $a \in A$. Cela montre l'unicité de ϕ sous réserve de son existence. Pour conclure, il faut vérifier que ϕ défini par $\phi(a) = (\phi_i(a))_{i\in I}$, $a \in A$ est bien un morphisme d'anneaux, ce qui résulte immédiatement des définitions. □

On peut aussi réécrire **??** en disant que, pour tout anneau A l'application canonique

$$\mathrm{Hom}(A, \prod_{i\in I} A_i) \to \prod_{i\in I} \mathrm{Hom}(A, A_i), \ \phi \to (p_i \circ \phi)_{i\in I}$$

est bijective ou encore, plus visuellement :



Supposons que l'on ait un autre anneau Π' et une famille de morphisme d'anneaux $p'_i : \Pi' \to A_i$, $i \in I$ vérifiant aussi la propriété du Lemme **??**.1. On a alors, formellement :

1. un unique morphisme d'anneaux $\phi : \Pi \to \Pi'$ tel que $p'_i \circ \phi = p_i$, $i \in I$;
2. un unique morphisme d'anneaux $\phi' : \Pi' \to \Pi$ tel que $p_i \circ \phi' = p'_i$, $i \in I$;
3. un unique morphisme d'anneaux $\psi : \Pi \to \Pi$ tel que $p_i \circ \psi = p_i$, $i \in I$;
4. un unique morphisme d'anneaux $\psi' : \Pi' \to \Pi'$ tel que $p'_i \circ \psi' = p'_i$, $i \in I$.

Mais on voit que dans (3) $\psi = \phi' \circ \phi$ et $\psi = Id_\Pi$ conviennent. L'unicité de ψ dans (3) impose donc $\phi' \circ \phi = Id_\Pi$. Le même argument dans (4) montre que $\phi \circ \phi' = Id_{\Pi'}$. Autrement dit, les morphismes d'anneaux $\phi : \Pi \to \Pi'$ de (1) et $\phi' : \Pi' \to \Pi$ de (2) sont inverses l'un de l'autre. On dit de façon un peu informelle que l'anneau produit $p_i : \prod_{i\in I} A_i \to A_i$, $i \in I$ est *unique à unique isomorphisme près*. On rencontrera beaucoup d'autres constructions de ce type dans la suite.

Remarque 1.2.0.1. Soit $\phi_i : A_i \to B_i$, $i \in I$ une famille de morphismes d'anneaux. En appliquant la propriété universelle des $p_j : \prod_{i\in I} B_i \to B_j$, $j \in I$ à la famille de morphismes d'anneaux

$$\prod_{i\in I} A_i \xrightarrow{p_j} A_j \xrightarrow{\phi_j} B_j,\ j \in I$$

on obtient un unique morphisme d'anneaux $\phi := \prod_{i\in I} \phi_i : \prod_{i\in I} A_i \to \prod_{i\in I} B_i$ tel que $p_i \circ \phi = \phi_i \circ p_i$, $i \in I$.

$$\begin{array}{ccc} A_i & \xrightarrow{\Phi_i} & B_i \\ {\scriptstyle \pi_i^A}\uparrow & & \uparrow{\scriptstyle \pi_i^B} \\ \prod_{i\in I} A_i & \xrightarrow{\Phi} & \prod_{i\in I} B_i \end{array}$$

Si $A_i = A$, $i \in I$, on note $\prod_{i\in I} A_i = A^I$. On peut voir A^I comme l'anneau des fonctions $a : I \to A$ muni de $(a+b)(i) = a(i) + b(i)$ et $(a \cdot b)(i) = a(i) \cdot b(i)$ de zéro l'application nulle et d'unité l'application constante de valeur 1_A. On notera qu'on a un morphisme d'anneaux injectif canonique $\Delta_A : A \hookrightarrow A^I$, $a \to (i \to a(i) = a)$ appelé morphisme diagonal (et qui, si A est commutatif, fait de A^I une A-algèbre de façon canonique).

Pour tout $\underline{a} = (a_i)_{i\in I} \in A^I$ notons $supp(\underline{a}) := \{i \in I \mid a_i \neq 0\} \subset I$ le *support* de $\underline{a}$. Notons

$$A^{(I)} := \{\underline{a} \in A^I \mid |supp(\underline{a})| < +\infty\} \subset A^I.$$

On observera que $A^{(I)} \subset A^I$ est stable par différence et produit mais que, si I est infini, ce n'est pas un sous-anneau de A^I car il ne contient pas 1_{A^I}.

1.3 Algèbres de polynômes

Soit A un anneau commutatif.

1.3.1 Construction de $A[X]$

Comme on vient de l'observer, le sous-ensemble $A^{(\mathbb{N})}$ de $A^{\mathbb{N}}$ est stable par différence et produit mais ce n'est pas un sous-anneau de $A^{\mathbb{N}}$ car il ne contient pas $1_{A^{\mathbb{N}}}$. En utilisant que $(\mathbb{N},+)$ est un monoide on peut cependant faire un anneau de $A^{(\mathbb{N})}$, en le munissant d'une autre multiplication que celle héritée de $A^{\mathbb{N}}$. Notons $e_n := (\delta_{m,n}1_A)_{m\in\mathbb{N}}$, $n \in \mathbb{N}$ et pour $a \in A$, $ae_n := (\delta_{m,n}a)_{m\in\mathbb{N}}$, $n \in \mathbb{N}$; $A^{(\mathbb{N})}$ contient les ae_n, $n \in \mathbb{N}$, $a \in A$ et, par définition, tout élément $\underline{a} \in A^{(\mathbb{N})}$ s'écrit de façon unique sous la forme $\underline{a} = \sum_{n\in\mathbb{N}} a_n e_n$. Munissons donc $A^{(\mathbb{N})}$ de l'addition héritée de celle de $A^{\mathbb{N}}$ et du produit 'de convolution' $*$ défini sur les éléments e_n, $n \in \mathbb{N}$ par : $e_m * e_n = e_{m+n}$ et en général par

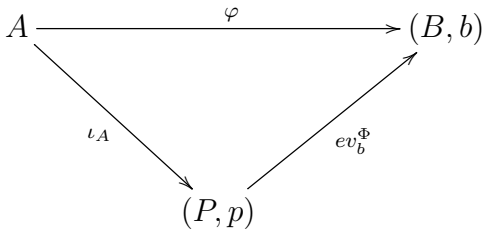
$$(\sum_{n\in\mathbb{N}} a_n e_n) * (\sum_{n\in\mathbb{N}} b_n e_n) = \sum_{n\in\mathbb{N}} (\sum_{i,j\in\mathbb{N}, i+j=n} a_i b_j) e_n \tag{1.1}$$

numérotation se fait automatiquement

On vérifie facilement que $(A^{(\mathbb{N})},+,*)$ est un anneau commutatif ayant pour unité e_0. L'application canonique $\iota_A : A \to A^{(\mathbb{N})}$, $a \to ae_0$ est un morphisme d'anneaux. On note traditionnellement cet anneau $(A[X],+,\cdot)$ et on dit que $\iota : A \to A[X]$ est la A-algèbre des polynômes à une inderminée. On pose aussi $X^n := e_n$, $n \in \mathbb{N}$ et $1 := X^0$ de sorte que (**??**.1) se réécrit de façon plus intuitive sous la forme :

$$(\sum_{n\in\mathbb{N}} a_n X^n)(\sum_{n\in\mathbb{N}} b_n X^n) = \sum_{n\in\mathbb{N}} (\sum_{i,j\in\mathbb{N}, i+j=n} a_i b_j) X^n. \tag{1.2}$$

Lemme 1.3.1.1 (Propriété universelle de la A-algèbre des polynômes à une indéterminée)**.** *Pour tout anneau commutatif A, il existe une A-algèbre $\iota_A : A \to P$ munie d'un élément $p \in P$ tels que pour toute A-algèbre $\phi : A \to B$ et $b \in B$, il existe un unique morphisme de A-algèbres $ev_b^\phi : P \to B$ tel que $ev_b^\phi(p) = b$.*



Démonstration. Vérifions que $\iota_A : A \to A[X]$ munie de X conviennent. Si $ev_b^\phi : A[X] \to B$ existe, on a par définition d'un morphisme de A-algèbres :

$$ev_b^\phi(\sum_{n\geq 0} a_n X^n) = \sum_{n\geq 0} ev_b^\phi(a_n) ev_b^\phi(X)^n = \sum_{n\geq 0} \phi(a_n) b^n,$$

d'où l'unicité de ev_b^ϕ sous réserve d'existence. Pour conclure, il faut vérifier que ev_b^ϕ défini par $ev_b^\phi(\sum_{n\geq 0} a_n X^n) = \sum_{n\geq 0} \phi(a_n) b^n$, est bien un morphisme d'anneaux, ce qui là encore résulte immédiatement des définitions. □

On adopte en général la notation plus intuitive $ev_b^\phi(P) = P(b)$ et on dit que ev_b^ϕ est le morphisme d'évaluation en b.

Remarque 1.3.1.1. Le même argument formel que celui utilisé dans **??**.2 montre que la A-algèbre $\iota_A : A \to A[X]$ est unique à unique isomorphisme près.

On peut aussi réécrire **??**.3 en disant que, pour toute A-algèbre $\phi : A \to B$ l'application canonique

$$\begin{aligned} \mathrm{Hom}_A(A[X], B) &\to B \\ f &\mapsto f(X) \end{aligned}$$

est bijective.

Soit $\phi : A \to B$ un morphisme d'anneaux commutatifs. En appliquant la propriété universelle des $\iota_A : A \to A[X]$ à la A-algèbre

$$A \xrightarrow{\phi} B \xrightarrow{\iota_B} B[X]$$

on obtient un unique morphisme d'anneaux $\tilde{\phi} : A[X] \to B[X]$ tel que $\iota_B \circ \phi = \phi \circ \iota_A$; explicitement $\tilde{\phi}(\sum_{n\geq 0} a_x X^n) = \sum_{n\geq 0} \phi(a_n) X^n$.

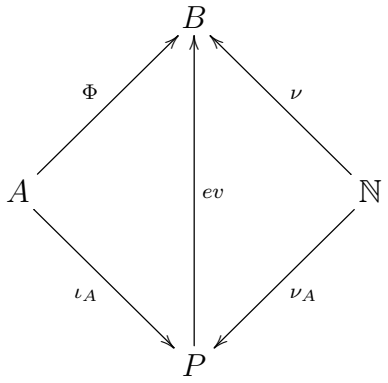
$$\begin{array}{ccc} A & \xrightarrow{\Phi} & B \\ \downarrow{\scriptstyle \iota_A} & & \downarrow{\scriptstyle \iota_B} \\ A[X] & \xrightarrow[\tilde{\Phi}]{} & B[X] \end{array}$$

Remarque 1.3.1.2. Ce qui nous a permis de définir le produit $*$ sur $A^{(\mathbb{N})}$ et le fait que $(\mathbb{N}, +)$ est un monoïde : on a utilisé l'addition pour définir $e_n * e_m = e_{n+m}$, l'associativité de $*$ résulte de celle de $+$ sur $\mathbb{N}$ et le fait que e_0 soit l'unité de $A^{(\mathbb{N})}$ du fait que 0 est l'unité de $\mathbb{N}$. Pour un monoïde $(M, \cdot)$ quelconque, l'application

$$\mathrm{Hom}_{Mono}(\mathbb{N}, M) \to M,\ f \to f(1)$$

est bijective d'inverse l'application qui à $m \in M$ associe le morphisme de monoïdes $f_m : (\mathbb{N}, +) \to (M, \cdot)$, $n \to m^n (= m \cdots m\ n \text{ fois})$. Dans **??**.3, se donner $p \in P$ et $b \in B$ revient donc à se donner des morphismes de monoïdes $\nu_A : (\mathbb{N}, +) \to (P, \cdot)$, $n \to p^n$ et $\nu : (\mathbb{N}, +) \to (B, \cdot)$, $n \to b^n$ et la condition $ev_b^\phi(p) = b$ signifie que $ev_b^\phi \circ \nu_A = \nu$. Avec ce point de vue, on peut reformuler **??**.3 comme suit.

Lemme 1.3.1.2 (Propriété universelle de la A-algèbre des polynômes à une indéterminée bis)**.** *Pour tout anneau commutatif A, il existe une A-algèbre $\iota_A : A \to P$ et un morphisme de monoïdes $\nu_A : (\mathbb{N}, +) \to (P, \cdot)$ tels que pour toute A-algèbre $\phi : A \to B$ et tout morphisme de monoïdes $\nu : (\mathbb{N}, +) \to (B, \cdot)$, il existe un unique morphisme de A-algèbres $ev_b^\phi : P \to B$ tel que $ev_b^\phi \circ \nu_A = \nu$.*



Ou encore : pour toute A-algèbre $\phi : A \to B$ l'application canonique

$$\mathrm{Hom}_A(A[X], B) \to \mathrm{Hom}_{Mono}(\mathbb{N}, B) \tag{1.3}$$
$$f \mapsto f \circ \nu_A. \tag{1.4}$$

est bijective. Explicitement, $\nu_A : (\mathbb{N}, +) \to (A[X], \cdot)$ est le morphisme qui envoie n sur X^n donc si $f : A[X] \to B$ est un morphisme de A-algèbres, $f \circ \nu_A : (\mathbb{N}, +) \to (B, \cdot)$ est le morphisme qui envoie n sur $f(X)^n$.

1.3.2 Construction de $A[N]$

Avec le point de vue développé dans la remarque **??**, on peut faire la construction précédente en remplaçant $(\mathbb{N}, +)$ par n'importe quel monoïde $(N, \cdot)$ (non nécessairement commutatif, non nécessairement dénombrable) d'unité 1_N. Notons toujours $e_n := (\delta_{m,n} 1_A)_{m \in N}$, $n \in N$ et pour $a \in A$, $ae_n := (\delta_{m,n} a)_{m \in N}$, $n \in N$; $A^{(N)}$ contient les ae_n, $n \in N$, $a \in A$ et, par définition, tout élément $\underline{a} \in A^{(N)}$ s'écrit de façon unique sous la forme $\underline{a} = \sum_{\underline{n} \in N^r} a_n e_n$. En munissant $A^{(N)}$ de l'addition héritée de celle de A^N et du produit 'de convolution' $*$ défini sur les éléments e_n, $n \in N$ par $e_m * e_n = e_{m \cdot n}$ et en général par

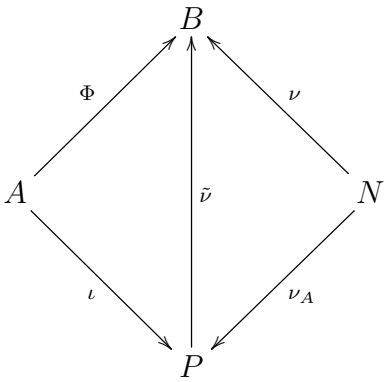
$$(\sum_{n \in N} a_n e_n) * (\sum_{n \in N} b_n e_n) = \sum_{n \in N} (\sum_{i,j \in N, i \cdot j = n} a_i b_j) e_n \tag{1.5}$$

on obtient un anneau (commutatif si $(N, \cdot)$ est commutatif) $(A^{(N)}, +, *)$ ayant pour unité $e_{\underline{1_N}}$. L'application canonique $\iota_A : A \to A^{(N)}$, $a \to ae_{1_N}$ est un morphisme d'anneaux et l'application $\nu_A : N \to A^{(N)}$, $n \to e_n$ prend ses valeur dans $A^{(N)} \setminus \{0\}$ et induit un morphisme de monoïdes $\nu_A : (N, \cdot) \to (A^{(N)} \setminus \{0\}, *)$. On note traditionnellement cet anneau $(A[N], +, \cdot)$ et on dit que $\iota_A : A \to A[N]$ est la A-algèbre du monoïde $(N, \cdot)$. On pose aussi $n := e_n$, $n \in N$ et $1 := 1_N$ de sorte que (**??**.5) se réécrit de façon plus intuitive sous la forme

$$(\mathbf{??}.7) \quad (\sum_{n \in N} a_n n) * (\sum_{n \in N} b_n n) = \sum_{n \in N} (\sum_{i,j \in N, i \cdot j = n} a_i b_j) n.$$

Lemme 1.3.2.1 (Propriété universelle de la A-algèbre du monoïde $(N, \cdot)$)**.** *Pour tout anneau commutatif A, il existe une A-algèbre $\iota_A : A \to P$ et un morphisme de monoïdes $\nu_A : (N, \cdot) \to$*

$(P,\cdot)$ tels que pour toute A-algèbre $\phi : A \to B$ et tout morphisme de monoïdes $\nu : (N,\cdot) \to (B,\cdot)$ il existe un unique morphisme de A-algèbres $\tilde{\nu} : P \to B$ tel que $\tilde{\nu} \circ \nu_A = \nu$.



Démonstration. Similaire à celle de **??**.3 en vérifiant que $\iota_A : A \to A[N]$ convient. □

Le même argument formel que celui utilisé dans **??**.2 montre que la A-algèbre $\iota_A : A \to A[N]$ est unique à unique isomorphisme près.

Remarque 1.3.2.1. On peut aussi réécrire **??**.8 en disant que, pour toute A-algèbre $\phi : A \to B$ l'application canonique

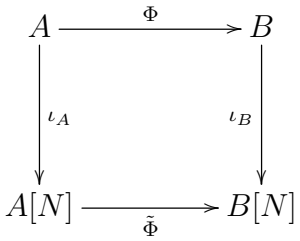
$$\mathrm{Hom}_A(A[N], B) \to \mathrm{Hom}_{Mono}(N, B),\ f \to f \circ \nu_A$$

est bijective. Son inverse est l'application qui à $\nu : (N,\cdot) \to (B,\cdot)$ associe l'unique morphisme de A-algèbres $\tilde{\nu} : A[N] \to B$ tel que $\tilde{\nu}(n) = \nu(n)$ (donc $\tilde{\nu}(\sum_{n\in N} a_n n) = \sum_{n\in N} \phi(a_n)\nu(n)$).

1.3.3 Exemples et autres constructions

Remarque 1.3.3.1. Si $(N,\cdot) = (\mathbb{N},+)$, on retrouve $A[\mathbb{N}] = A[X]$

Soit $(N,\cdot)$ un monoïde et $\phi : A \to B$ un morphisme d'anneaux commutatifs. La propriété universelle de $\iota_A : A \to A[N]$ appliquée avec $A \xrightarrow{\phi} B \xrightarrow{\iota_B} B[N]$ donne un unique morphisme de A-algèbres $\tilde{\phi} : A[N] \to B[N]$ tel que $\nu_B = \tilde{\phi} \circ \nu_A$. Explicitement $\tilde{\phi}(\sum_{n\geq 0} a_n e_n) = \sum_{n\geq 0} \phi(a_n) e_n$. Par construction, $\mathrm{im}(\tilde{\phi}) = \mathrm{im}(\phi)[N] \subset B[N]$ et $\ker(\tilde{\phi})$ est l'ensemble des éléments de la forme $\sum_{n\geq 0} a_n e_n \in A[N]$ tels que $a_n \in \ker(\phi)$, $n \geq 0$. On notera $\ker(\phi)[N] := \ker(\tilde{\phi}) \subset A[N]$.



Définition 1.3.3.1. Pour $(N,\cdot)$ un groupe, pour toute A-algèbre $\phi : A \to B$, tout morphisme de monoïdes $\nu : (N,\cdot) \to (B,\cdot)$ est automatiquement à valeur dans le groupe $(B^\times,\cdot)$. On dit dans ce cas que $A[N]$ est la A-algèbre du groupe $(N,\cdot)$.

1.3.3.1 Polynômes à plusieurs indeterminées

Posons $(N,\cdot)=(\mathbb{N}^r,+)$, où $+$ est l'addition termes à termes (pour $\underline{m}=(m_1,\dots,m_r),\underline{n}:=(n_1,\dots,n_r)\in\mathbb{N}^r$, $\underline{m}+\underline{n}=(m_1+n_1,\dots,m_r+n_r)\in\mathbb{N}^r$). Dans ce cas, on note $\underline{X}^{\underline{n}}:=X_1^{n_1}\cdots X_r^{n_r}:=e_{\underline{n}}$, $\underline{n}\in\mathbb{N}^r$ avec la convention $X_i^0=1$, $i=1,\dots,r$, et $1:=\underline{X}^{\underline{0}}$ de sorte que (**??**.5) se réécrit de façon plus intuitive sous la forme

$$(\sum_{\underline{n}\in\mathbb{N}^r}a_{\underline{n}}\underline{X}^{\underline{n}})(\sum_{\underline{n}\in\mathbb{N}^r}b_{\underline{n}}\underline{X}^{\underline{n}})=\sum_{\underline{n}\in\mathbb{N}^r}(\sum_{\underline{i},\underline{j}\in\mathbb{N}^r,\underline{i}+\underline{j}=\underline{n}}a_{\underline{i}}b_{\underline{j}})\underline{X}^{\underline{n}}.$$

On note également $A[X_1,\dots,X_r]:=A[\mathbb{N}^r]$ et on dit que $\iota_A:A\to A[X_1,\dots,X_r]$ est la A-algèbre des polynômes à r inderminées. Comme se donner un morphisme de monoïdes $\nu:(\mathbb{N}^r,+)\to(B,\cdot)$ revient à se donner les images $b_i\in B$ de $(\delta_{i,j})_{1\leq j\leq r}\in\mathbb{N}^r$, on peut reformuler **??**.7 de la façon suivante.

Définition 1.3.3.2 (Morphisme d'évaluation)**.** Pour toute A-algèbre $\phi:A\to B$, notons :

$$\mathfrak{B}_r:=\{\underline{b}=(b_1,\dots,b_r)\in B^r\mid b_ib_j=b_jb_i,\ 1\leq i,j\leq r\},$$

$$\begin{aligned}\mathrm{Hom}_A(A[X_1,\dots,X_r],B)&\to\mathfrak{B}_r\\ f&\mapsto(f(X_1),\dots,f(X_r))\end{aligned}$$

Cette application est bijective et son inverse est l'application qui à $\underline{b}=(b_1,\dots,b_r)\in\mathfrak{B}_r$ associe l'unique morphisme de A-algèbres $ev_{\underline{b}}^{\phi}:A[X_1,\dots,X_r]\to B$ tel que $ev_{\underline{b}}^{\phi}(X_i)=b_i$, $i=1,\dots r$ (donc $ev_{\underline{b}}^{\phi}(\sum_{\underline{n}\in\mathbb{N}^r}a_{\underline{n}}\underline{X}^{\underline{n}})=\sum_{\underline{n}\in\mathbb{N}^r}\phi(a_{\underline{n}})\underline{b}^{\underline{n}}$). On adopte en général la notation plus intuitive $ev_{\underline{b}}^{\phi}(P)=P(b_1,\dots,b_r)$ et on dit que $ev_{\underline{b}}^{\phi}$ est le morphisme d'évaluation en $\underline{b}$.

1.3.3.2 Polynômes de Laurent à une indeterminée

Prenons cette fois le groupe $(N,\cdot)=(\mathbb{Z},+)$, on obtient la A-algèbre (notations : $A[X,X^{-1}]:=A[\mathbb{Z}]$, $X^n:=e_n$, $n\in\mathbb{Z}$ donc en particulier $X^nX^{-n}=e_ne_{-n}=e_{n-n}=e_0=1$) des polynômes de Laurent à une indéterminée. Comme se donner un morphisme de monoïdes $\nu:(\mathbb{Z},+)\to(B,\cdot)$ revient à se donner l'image $b\in B^\times$ de $1\in\mathbb{Z}$, on peut reformuler **??**.7 de la façon suivante.

Définition 1.3.3.3 (Morphisme d'évaluation)**.** Pour toute A-algèbre $\phi:A\to B$, l'application canonique

$$\begin{aligned}\mathrm{Hom}_A(A[X,X^{-1}],B)&\to B^\times\\ f&\mapsto f(X)\end{aligned}$$

est bijective. Son inverse est l'application qui à $b\in B^\times$ associe l'unique morphisme de A-algèbres $ev_{\underline{b}}^{\phi}:A[X,X^{-1}]\to B$ tel que $ev_{\underline{b}}^{\phi}(X)=b$ (donc $ev_{\underline{b}}^{\phi}(\sum_{n\in\mathbb{Z}}a_n\underline{X}^{\underline{n}})=\sum_{n\in\mathbb{Z}}\phi(a_n)b^n$).

1.3.3.3 Polynômes de Laurent à plusieurs indeterminées

De même, pour $(N,\cdot)=(\mathbb{Z}^r,+)$, on obtient la A-algèbre (notations : $A[X_1,X_1^{-1},\cdots,X_r,X_r^{-1}]:=A[\mathbb{Z}^r]$, $\underline{X}^{\underline{n}}:=X_1^{n_1}\cdots X_r^{n_r}:=e_{\underline{n}}$, $\underline{n}\in\mathbb{Z}^r$ donc en particulier, $\underline{X}^{\underline{n}}\underline{X}^{-\underline{n}}=e_{\underline{n}}e_{-\underline{n}}=e_{\underline{n}-\underline{n}}=e_0=1$) des polynômes de Laurent à r indéterminées. Comme se donner un morphisme de monoïdes $\nu:(\mathbb{Z}^r,+)\to(B,\cdot)$ revient à se donner les images $b_i\in B^\times$ des $(\delta_{i,j})_{1\leq j\leq r}\in\mathbb{Z}$, $i=1,\ldots,r$ on peut reformuler **??**.8 de la façon suivante.

Définition 1.3.3.4 (Morphisme d'évaluation)**.** Pour toute A-algèbre $\phi:A\to B$, en notant

$$\mathfrak{B}_r^\times:=\{\underline{b}=(b_1,\ldots,b_r)\in(B^\times)^r\mid b_ib_j=b_jb_i,\ 1\leq i,j\leq r\},$$

l'application canonique

$$\begin{aligned}\mathrm{Hom}_A(A[X_1,X_1^{-1},\cdots,X_r,X_r^{-1}],B)&\to\mathfrak{B}_r^\times\\ f&\to(f(X_1),\ldots,f(X_r))\end{aligned}$$

est bijective. Son inverse est l'application qui à $\underline{b}=(b_1,\ldots,b_r)\in\mathfrak{B}_r^\times$ associe l'unique morphisme de A-algèbres $ev_{\underline{b}}^\phi:A[X_1,X_1^{-1},\cdots,X_r,X_r^{-1}]\to B$ tel que $ev_{\underline{b}}^\phi(X_i)=b_i$, $i=1,\ldots r$ (donc $ev_{\underline{b}}^\phi(\sum_{\underline{n}\in\mathbb{Z}^r}a_{\underline{n}}\underline{X}^{\underline{n}})=\sum_{\underline{n}\in\mathbb{Z}^r}\phi(a_{\underline{n}})\underline{b}^{\underline{n}}$)

1.3.4 Exercices

Exercice 1.3.4.1. Montrer qu'on a un morphisme surjectif A-algèbres canonique

$$A[X_1,Y_1,\ldots,X_r,Y_r]\twoheadrightarrow A[X_1,X_1^{-1},\ldots,X_r,X_r^{-1}].$$

Correction. Plus généralement, on peut montrer qu'on a une application canonique injective

$$\begin{array}{rccc}\tilde{-}:&\mathrm{Hom}_{Mono}(N_1,N_2)&\hookrightarrow&\mathrm{Hom}_A(A[N_1],A[N_2])\\&\nu:N_1\to N_2&\to&\tilde{\nu}:A[N_1]\to A[N_2]\end{array}$$

qui envoie morphismes de monoïdes injectifs (resp. surjectifs, resp. bijectifs) sur morphismes de A-algèbres injectifs (resp. surjectifs, resp. bijectifs). L'existence de $\tilde{-}:\mathrm{Hom}_{Mono}(N_1,N_2)\to\mathrm{Hom}_A(A[N_1],A[N_2])$ est une conséquence formelle de la propriété universelle de la A-algèbre de monoïdes $\iota_A:A\to A[N_1]$ appliquée avec la A-algèbre $\iota_A:A\to A[N_2]$ et le morphisme de monoïdes $N_1\xrightarrow{\nu}N_2\xrightarrow{\nu_A}A[N_2]$: il existe un unique morphisme de A-algèbre $\tilde{\nu}:A[N_1]\to A[N_2]$ tel que le diagramme suivant commute

$$\begin{array}{ccc}N_1&\xrightarrow{\nu_A}&A[N_1]\\ \downarrow{\scriptstyle\nu}&&\downarrow{\scriptstyle\tilde{\nu}}\\ N_2&\xrightarrow[\nu_A]{}&A[N_2]\end{array}$$

L'injectivité de $\tilde{-}:\mathrm{Hom}_{Mono}(N_1,N_2)\to\mathrm{Hom}_A(A[N_1],A[N_2])$ résulte de l'injectivité des $\nu_A:N_i\to A[N_i]$, $i=1,2$. Enfin, le fait que $\tilde{-}:\mathrm{Hom}_{Mono}(N_1,N_2)\to\mathrm{Hom}_A(A[N_1],A[N_2])$

envoie morphismes de monoïdes injectifs (resp. surjectifs, resp. bijectifs) sur morphismes de A-algèbres injectifs (resp. surjectifs, resp. bijectifs) résulte du fait que, par construction, tout élément de $A[N]$ s'écrit de façon unique sous la forme $\sum_{n\in N} ae_n$ (on verra dans le chapitre sur les modules que $A[N]$ est un A-module libre de base les e_n, $n \in N$) et que la condition $\nu_A \circ \nu = \tilde{\nu} \circ \nu_A$ impose $\tilde{\nu}(e_n) = e_{\nu(n)}$.

La question posée correspond au cas particulier du morphisme de monoïdes surjectif $\nu : (\mathbb{N}^2, +) \twoheadrightarrow (\mathbb{Z}, +)$ défini par $\nu(n_1, n_2) = n_1 - n_2$ (le $\tilde{\nu} : A[X_1, Y_1, \ldots, X_r, Y_r] \twoheadrightarrow A[X_1, X_1^{-1}, \ldots, X_r, X_r^{-1}]$ correspondant étant défini par $\tilde{\nu}(X_i) = Z_i$, $\tilde{\nu}(Y_i) = Z_i^{-1}$, $i = 1, \ldots, r$).

Exercice 1.3.4.2. Montrer qu'on a des isomorphismes de A-algèbres canonique

$$A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_r][X_i] \tilde{\to} A[X_1, \ldots, X_r],\ i = 1, \ldots, r.$$

Correction. Observons d'abord que toute permutation $\sigma \in \mathcal{S}_r$ induit un automorphisme du monoïde $(\mathbb{N}^r, +)$ par permutation des coordonnées donc, d'après (1), un automorphisme de la A-algèbre $A[X_1, \ldots, X_r]$. (Explicitement, $\sigma P(X_1, \ldots, X_r) = P(X_{\sigma(1)}, \ldots, X_{\sigma(r)})$). Il suffit donc de montrer le résultat pour $i = r$. Par unicité à unique isomorphisme près des objets universel, il suffit de montrer que

$\iota_A : A \to A[X_1, \ldots, X_r]$ et $A \xrightarrow{\iota_A} A[X_1, \ldots, X_{r-1}] \xrightarrow{\iota_{A[X_1,\ldots,X_{r-1}]}} A[X_1, \ldots, X_{r-1}][X_r]$ vérifie la même propriété universelle. Notons que par hypothèse $A[b_1, \ldots, b_r]$ est un anneau commutatif (*cf.* **??** pour la notation $A[b_1, \ldots, b_{r-1}]$). Soit donc $\phi : A \to B$ une A-algèbre et $b_1, \ldots, b_r \in B^r$ commutant deux à deux. Par la propriété universelle de $\iota_A : A \to A[X_1, \ldots, X_{r-1}]$, il existe un unique morphisme de A-algèbre $ev^{\phi}_{(b_1,\ldots,b_{r-1})} : A[X_1, \ldots, X_{r-1}] \to B$ tel que $\phi_1(X_i) := ev^{\phi}_{(b_1,\ldots,b_{r-1})}(X_i) = b_i$, $i = 1, \ldots, r-1$. Puis, par la propriété universelle de $\iota_{A[X_1,\ldots,X_{r-1}]} : A[X_1, \ldots, X_{r-1}] \to A[X_1, \ldots, X_r]$, il existe un unique morphisme de A-algèbre $ev^{\phi_1}_{b_r} : A[X_1, \ldots, X_{r-1}][X_r] \to A[b_1, \ldots, b_{r-1}][b_r] = A[b_1, \ldots, b_r]$ tel que $ev^{\phi_1}_{b_r}(X_r) = b_r$... On laisse le soin au lecteur de généraliser ce genre d'exercice formel un tantinet fastidieux.

1.4 Sous-anneau engendré par une partie

Soit $A_i \subset A$, $i \in I$ une famille de sous-anneaux. On vérifie immédiatement que $\cap_{i\in I} A_i \subset A$ est un sous-anneau. Pour tout sous-ensemble $X \subset A$, il existe un unique sous-anneau $\langle X \rangle \subset A$, contenant X et minimal pour $\subset$ *i.e.* tel que pour tout sous-anneau $A' \subset A$, $X \subset A'$ implique $\langle X \rangle \subset A'$.

Définition 1.4.0.1. On dit que $\langle X \rangle \subset A$ est le sous-anneau de A engendré par X.

Explicitement $\langle X \rangle$ est l'intersection de tous les sous-anneaux de A contenant X. On peut également décrire $\langle X \rangle$ comme l'ensemble des sommes finies de produits finis d'éléments de X.

Définition 1.4.0.2. Si $A = \langle X \rangle$, on dit que X est un système de générateurs de A comme anneau (ou que A est engendré par X comme anneau). Si on peut prendre de plus X fini, on dit que A est un anneau de type fini.

Définition 1.4.0.3. Lorsque les éléments de X commutent deux à deux, on note en général $\mathbb{Z}[X] := \langle X \rangle \subset A$ le sous-anneau de A engendré par X. Si $X = \{x_1, \ldots, x_r\}$ est fini, on note plutôt $\mathbb{Z}[x_1, \ldots, x_r] := \mathbb{Z}[X]$ et **??**.8 nous donne un unique morphisme d'anneaux - automatiquement surjectif - $ev_{\underline{x}} : \mathbb{Z}[X_1, \cdots, X_r] \twoheadrightarrow \mathbb{Z}[x_1, \ldots, x_r]$ tel que $ev_{\underline{x}}(X_i) = x_i$, $i = 1, \ldots, r$.

1.5 Sous-A-algèbre engendrée par une partie

Soit $\phi : A \to B$ une A-algèbre.

Définition 1.5.0.1. Une sous-A-algèbre de $\phi : A \to B$ est un sous-anneau $B' \subset B$ tel que $\mathrm{im}(\phi) \subset B'$ (noter que $Z(B) \cap B' \subset Z(B')$)

Le morphisme $\phi|^{B'} : A \to B'$ munit alors B' d'une structure de A-algèbre qui fait de l'inclusion $B' \subset B$ un morphisme de A-algèbres. Si $B_i \subset B$, $i \in I$ est une famille de sous-A-algèbres, $\cap_{i \in I} B_i \subset B$ est encore une sous-A-algèbre. Pour tout sous-ensemble $X \subset B$, il existe une unique sous-A-algèbre $\langle X \rangle_A \subset B$, contenant X et minimale pour $\subset$

Définition 1.5.0.2. On dit que $\langle X \rangle_A \subset B$ est la sous-A-algèbre de B engendrée par X.

Explicitement $\langle X \rangle_A$ est l'intersection de tous les sous-A-algèbres de B contenant X. On peut également décrire $\langle X \rangle_A$ comme le sous-anneau de B engendré par $X \cup \mathrm{im}(\phi)$.

Définition 1.5.0.3. Si $B = \langle X \rangle_A$, on dit que X est un système de générateurs de B comme A-algèbre (ou que B est engendré par X comme A-algèbre). Si on peut prendre X fini, on dit que B est une A-algèbre de type fini.

Lorsque les éléments de X commutent deux à deux, on note en général $A[X] := \langle X \rangle_A \subset B$ la sous-A-algèbre de B engendré par X. Si $X = \{x_1, \ldots, x_r\}$ est fini, , on note plutôt $A[x_1, \ldots, x_r] := A[X]$ et **??**.8 nous donne un unique morphisme de A-algèbres - automatiquement surjectif - $ev^{\phi}_{\underline{x}} : A[X_1, \cdots, X_r] \twoheadrightarrow A[x_1, \ldots, x_r]$ tel que $ev^{\phi}_{\underline{x}}(X_i) = x_i$, $i = 1, \ldots, r$.

** Dans la suite, sauf mention explicite du contraire, nous ne considérerons que des anneaux commutatifs **

** Dans la suite, sauf mention explicite du contraire, nous ne considérerons que des anneaux commutatifs **

Chapitre 2

Idéaux et quotients

2.1 Définitions, premiers exemples

2.1.1

Soit A un anneau (commutatif, donc). Un idéal de A est un sous-ensemble $I \subset A$ tel que $a'-b' \in I$, $a', b' \in I$ et $aa' \in I$, $a \in A$, $a' \in I$. On notera $\mathcal{I}_A$ l'ensemble des idéaux de A ; l'inclusion ensembliste $\subset$ munit $\mathcal{I}_A$ d'un ordre partiel. Pour un idéal $I \subset A$, on notera $V^{tot}(I) \subset \mathcal{I}_A$ le sous-ensemble des idéaux de A qui contiennent I

Exemples.
— Le singleton $\{0\}$ et A sont des idéaux de A.
— Si k est un corps commutatif, les seuls idéaux de k sont $\{0\}$ et k.
— Un idéal $I \subset A$ est en particulier un sous-groupe de $(A, +)$. Par exemple, les seuls candidats possibles pour les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \geq 0$ (division euclidienne). On vérifie immédiatement que les $n\mathbb{Z}$ sont bien des idéaux de $\mathbb{Z}$. Donc les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$, $n \geq 1$. On notera que $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si $m|n$. La k-algèbre $k[X]$ des polynômes à une indéterminée sur un corps est également munie d'une division euclidienne et on verra que dans ce cas aussi, tous les idéaux de $k[X]$ sont de la forme $Pk[X]$, $P \in k[X]$.
— Pour tout $a \in A$, $Aa \subset A$ est un idéal. Les idéaux de cette forme sont appelés principaux. On dit qu'un anneau A principal si tous ses idéaux sont principaux et s'il est intègre. Les anneaux $\mathbb{Z}$ et $k[X]$ sont principaux. Par contre, $k[X, Y]$ n'est pas principal, par exemple l'ensemble $I := \{XP + YQ \mid P, Q \in k[X, Y]\} \subset k[X, Y]$ est un idéal qui n'est pas principal.
— Si A_i, $i \in I$ est une famille d'anneaux, et, pour chaque $i \in I$, $I_i \subset A_i$ est un idéal, $\prod_{i\in I} I_i \subset \prod_{i\in I} A_i$ est un idéal. Mais les idéaux de $\prod_{i\in I} A_i$ ne sont pas tous de cette forme. Par exemple, $A^{(I)} \subset A^I$ est un idéal de A^I qui n'est pas un produit d'idéaux.
— Si $I \subset A$ est un idéal, $I[X_1, \ldots, X_r] := \{\sum_{\underline{n}\in\mathbb{N}^r} a_{\underline{n}} \underline{X^n} \mid a_{\underline{n}} \in I\} \subset A[X_1, \ldots, X_r]$ est un idéal.

2.1.2 Idéal engendré par une partie, sommes d'idéaux

Soit $\mathcal{I} \subset \mathcal{I}_A$ une famille d'idéaux. On vérifie immédiatement que $\cap_{I\in\mathcal{I}} I \subset A$ est idéal. Pour tout sous-ensemble $X \subset A$, il existe un unique idéal $\langle\langle X\rangle\rangle_A \subset A$, contenant X et minimal pour

$\subset$ *i.e.* tel que pour tout idéal $I \subset A$, $X \subset I$ implique $\langle\langle X\rangle\rangle_A \subset I$. On dit que $\langle\langle X\rangle\rangle_A \subset A$ est l'idéal engendré par X. Explicitement $\langle\langle X\rangle\rangle_A$ est l'intersection de tous les idéaux de A contenant X. On peut également décrire $\langle\langle X\rangle\rangle_A$ comme

$$\langle\langle X\rangle\rangle_A = \{\sum_{x\in X} a(x)x \mid a \in A^{(X)}\},$$

ce qui justifie la notation plus intuitive $\langle\langle X\rangle\rangle_A := \sum_{x\in X} Ax \subset A$. Si $\mathcal{I} \subset \mathcal{I}_A$ une famille d'idéaux, on note en particulier

$$\langle\langle \bigcup_{I\in\mathcal{I}} I \rangle\rangle_A := \sum_{I\in\mathcal{I}} I \subset A.$$

et on dit que $\sum_{I\in\mathcal{I}} I \subset A$ est la somme des I, $I \in \mathcal{I}$. Si $I = \sum_{x\in X} Ax$, on dit que X est un système de générateurs de I et si on peut prendre X fini, on dit que I est un idéal de type fini.

Exemples Les idéaux principaux d'un anneau A sont les idéaux engendrés par les singletons $\{a\}$, $a \in A$. En particulier, dans un anneau principal comme $\mathbb{Z}$ ou $k[X]$, tout idéal est de type fini. De façon plus surprenante, on verra que tous les idéaux de $k[X_1, \cdots, X_r]$ (et, partant, de toute k-algèbre de type fini) sont de type fini. Un anneau ayant cette propriété est dit noethérien. Les anneaux qui ne sont pas de type fini, par exemple $A^{\mathbb{N}}$, fournissent tautologiquement des idéaux qui ne sont pas de type fini. L'idéal $A^{(\mathbb{N})} \subset A^{\mathbb{N}}$ n'est pas de type fini.

2.1.3 Produits d'idéaux

Si $I_1, \ldots, I_r \subset A$ est une famille finie d'idéaux, on note $I_1 \cdots I_r \subset A$ l'idéal engendré par les éléments de la forme $a_1 \cdots a_r$, $a_i \in I_i$, $i = 1, \ldots, r$. On a toujours

$$(*)\ \ I_1 \cdots I_r \subset \bigcap_{1\leq i\leq r} I_i \subset I_i \subset \sum_{1\leq i\leq r} I_i.$$

Exemple. Dans $\mathbb{Z}$, on a pour tout $m_1, \ldots, m_r \in \mathbb{Z}$, $m_1\mathbb{Z} \cdots m_r\mathbb{Z} = (m_1 \cdot m_r)\mathbb{Z}$, $m_1\mathbb{Z} \cap \cdots \cap m_r\mathbb{Z} = \mathrm{ppcm}(m_1, \ldots, m_r)\mathbb{Z}$, $m_1\mathbb{Z} + \cdots + m_r\mathbb{Z} = \mathrm{pgcd}(m_1, \cdots, m_r)\mathbb{Z}$. Les inclusions $(*)$ ci-dessus correspondent aux relations de divisibilité

$$\mathrm{pgcd}(m_1, \cdots, m_r)|m_i|\,\mathrm{ppcm}(m_1, \cdots, m_r)|m_1 \cdots m_r.$$

2.1.4

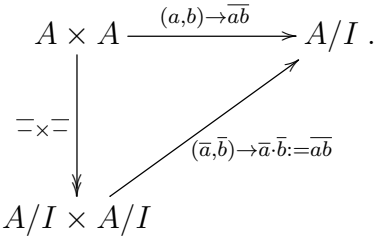
Si $\phi : A \to B$ un morphisme d'anneaux, et $J \subset B$ un idéal alors $\phi^{-1}(J) \subset A$ est un idéal. En particulier, $\ker(\phi) \subset A$ est un idéal. Si $\phi : A \twoheadrightarrow B$ est surjectif et $I \subset A$ est un idéal alors $\phi(I) \subset B$ est un idéal mais montrer par un contre-exemple que ce n'est plus vrai si on ne suppose pas $\phi : A \twoheadrightarrow B$ surjectif.

2.2 Quotient

Le noyau d'un morphisme d'anneaux $\phi : A \to B$ est un idéal. Réciproquement, on va voir que tout idéal est le noyau d'un morphisme d'anneaux. En effet, si A est un anneau, un idéal $I \subset A$ est en particulier un sous-groupe de $(A, +)$. On dispose donc du groupe quotient A/I, qui est un groupe abélien et de la projection canonique $p_I := \overline{-} : A \twoheadrightarrow A/I$ qui est un morphisme surjectif de groupes, de noyau I. Le groupe quotient A/I est muni d'une unique structure d'anneau telle que la projection canonique $p_I := \overline{-} : A \twoheadrightarrow A/I$ est un morphisme d'anneaux. La condition que $p_I := \overline{-} : A \twoheadrightarrow A/I$ soit un morphisme d'anneaux impose que $\overline{ab} = \overline{a}\overline{b}$. Il faut donc vérifier que $\overline{ab}$ ne dépend pas du choix des représentants a, b de $\overline{a}$, $\overline{b}$. ou encore que l'application

$$\begin{array}{ccc} A \times A & \to & A/I \\ (a, b) & \to & \overline{ab} \end{array}$$

se factorise en



Cela résulte de la relation $(a+I)(b+I) = ab+aI+Ib+I^2 \subset ab+I$, $a, b \in I$. On vérifie ensuite facilement que $(A/I, +, \cdot)$ ainsi défini vérifie bien les axiomes d'un anneau commutatif de zéro $\overline{0}$ et d'unité $\overline{1}$.

??.1 **Lemme.** (Propriété universelle du quotient) *Pour tout idéal $I \subset A$ il existe un morphisme d'anneaux $p : A \to Q$ tel que pour tout morphisme d'anneaux $\phi : A \to B$ avec $I \subset \ker(\phi)$, il existe un unique morphisme d'anneaux $\overline{\phi} : Q \to B$ tel que $\phi = \overline{\phi} \circ p$.*

Démonstration. Montrons que A/I muni de la structure d'anneau ci-dessus et la projection canonique $\overline{-} : A \twoheadrightarrow A/I$ conviennent. Soit $\phi : A \to B$ un morphisme d'anneaux tel que $I \subset \ker(\phi)$. Si $\overline{\phi} : A/I \to B$ existe, la condition $\phi = \overline{\phi} \circ p$ force $\overline{\phi}(\overline{a}) = \phi(a)$, $a \in A$. Cela montre l'unicité de $\overline{\phi}$ sous réserve de son existence. Il reste à voir que $\overline{\phi} : A/I \to B$ est automatiquement un morphisme d'anneaux. On sait déjà que c'est un morphisme de groupes additifs, donc il suffit de vérifier la compatibilité au produit. Cela résulte des définitions :

$$\overline{\phi}(\overline{a}\overline{b}) \overset{(1)}{=} \overline{\phi}(\overline{ab}) \overset{(2)}{=} \phi(ab) \overset{(3)}{=} \phi(a)\phi(b) \overset{(4)}{=} \overline{\phi}(\overline{a})\overline{\phi}(\overline{b}),$$

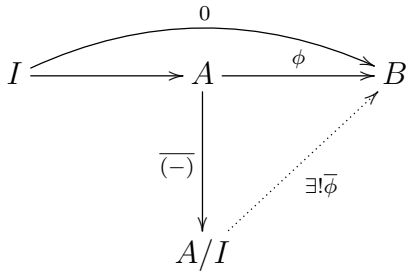
où (1) est par construction du produit sur A/I, (2) et (4) est la relation $\phi = \overline{\phi} \circ \overline{-}$ et (3) est le fait que ϕ est un morphisme d'anneaux. □

Comme d'habitude, la A-algèbre quotient $p_I := \overline{-} : A \twoheadrightarrow A/I$ est unique à unique isomorphisme près. Par construction $p_I : A \twoheadrightarrow A/I$ est surjectif de noyau I.

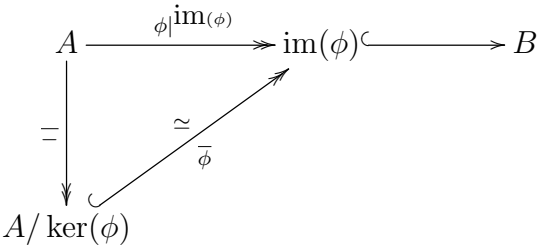
On peut aussi réécrire **??**.1 en disant que, pour tout anneau B l'application canonique

$$SHom(A/I, B) \to \{A \xrightarrow{\phi} B \mid I \subset \ker(\phi)\},\ \overline{\phi} \to \overline{\phi} \circ \overline{(-)}$$

est bijective ou encore, plus visuellement :



En particulier, tout morphisme d'anneaux $\phi : A \to B$ se décompose de façon canonique sous la forme



Exemples. (Caractéristique d'un anneau) Le noyau du morphisme caractéristique $c_A : \mathbb{Z} \to A$ est un idéal de $\mathbb{Z}$ donc de la forme $\ker(c_A) = n\mathbb{Z}$ pour un unique entier $n \geq 0$, appelé la caractéristique de A.

— $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0 ;
— $\mathbb{Z}/n$ est de caractéristique n, $n \geq 0$;
— Si $A' \subset A$ est un sous-anneau, A et A' ont même caractéristique. En particulier A, A^I, $A[X]$ ont même caractéristique. Si $\mathcal{P}$ est un ensemble infini de nombres premiers distincts, l'anneau produit $\prod_{p\in\mathcal{P}} \mathbb{Z}/p\mathbb{Z}$ est de caractéristique 0.
— Si $\phi : A \to B$ est une A-algèbre, la caractéristique de B divise la caractéristique de A.

Exercices.

1. Soit $I, J \subset A$ des idéaux ; notons $\overline{A} := A/I$ et $\overline{J} := P_I(J)$. Montrer que si $I \subset J$, on a un isomorphisme d'anneaux canonique $A/J \tilde{\to} \overline{A}/\overline{J}$. En déduire qu'on a toujours un isomorphisme d'anneaux canonique $A/(I+J) \tilde{\to} \overline{A}/\overline{J}$.

2. Soit $I \subset A$ un idéal. Montrer qu'on a un isomorphisme de A-algèbres canonique $A[X]/I[X] \tilde{\to} (A/I)[X]$.

3. Soit $f_1, \dots f_s \in A[X_1, \dots, X_r]$. Montrer que la A-algèbre quotient

$$A \to A[X_1, \dots, X_n]/\sum_{1\leq i\leq s} f_i A[X_1, \dots, X_r]$$

munie des images $\overline{X}_1, \cdots, \overline{X}_r$ de $X_1, \dots, X_r$ vérifie la propriété universelle suivante.

(Propriété universelle de $A \to A[X_1,\dots,X_n]/\sum_{1\le i\le s} f_i A[X_1,\dots,X_r]$) Il existe une A-algèbre $A \to \overline{P}$ munie d'éléments $\overline{p}_1,\dots,\overline{p}_r \in \overline{P}$ tels que pour tout A-algèbre $\phi : A \to B$ et $b_1,\dots,b_r \in B$ vérifiant $ev_{\underline{b}}^{\phi}(f_i) = 0$, $i = 1,\dots,s$ il existe un unique morphisme de A-algèbre $\overline{ev}_{\underline{b}}^{\phi} : \overline{P} \to B$ tel que $\overline{ev}_{\underline{b}}^{\phi}(\overline{p}_i) = b_i$, $i = 1,\dots,r$.

4. Montrer qu'on a un isomorphisme de A-algèbres canonique

$$A[X_1,Y_1,\dots,X_r,Y_r]/\sum_{1\le i\le r}(X_iY_i-1)A[X_1,Y_1,\dots,X_r,Y_r] \tilde{\to} A[X_1,X_1^{-1},\dots,X_r,X_r^{-1}].$$

??.2 Lemme. *Soit $I \subset A$ un idéal. La projection canonique $p_I : A \twoheadrightarrow A/I$ induit une bijection d'ensembles ordonnés $p_I : (V^{tot}(I),\subset) \tilde{\to} (\mathcal{I}_{A/I},\subset)$.*

Démonstration. Le fait que $p_I : V^{tot}(I) \to \mathcal{I}_{A/I}$ préserve l'inclusion est immédiat. Pour montrer que c'est une bijection, il suffit d'exhiber l'application inverse. Comme $\ker(p_I) = I$, $p_I^{-1} : \mathcal{I}_{A/I} \to \mathcal{I}_A$ est à valeur dans $V^{tot}(I)$ donc induit une application $p_I^{-1} : \mathcal{I}_{A/I} \to V^{tot}(I)$; vérifions que celle-ci convient. Comme $p_I : A \twoheadrightarrow A/I$ est surjective, on a toujours $p_I \circ p_I^{-1}(\overline{J}) = \overline{J}$, $\overline{J} \in \mathcal{I}_{A/I}$. Inversement, si $J \in \mathcal{I}_A$, on a $p_I^{-1} \circ p_I(J) = I + J$ donc, si on suppose de plus $I \subset J$, on a $p_I^{-1} \circ p_I(J) = I + J = J$. □

Soit $I_1,\dots,I_r \subset A$ des idéaux et considérons le produit des projections canoniques $p := \prod_{1\le i\le r} p_{I_i} : A \to \prod_{1\le i\le r} A/I_i$; c'est un morphisme d'anneaux de noyau $\cap_{1\le i\le r} I_i$. De plus

??.3 Lemme. (Restes chinois) *Si $I_i + I_j = A$, $1 \le i \ne j \le r$ alors $\cap_{1\le i\le r} I_i = I_1 \cdots I_r$ et $p : A \to \prod_{1\le i\le r} A/I_i$ est surjective. Inversement, si $p : A \to \prod_{1\le i\le r} A/I_i$ est surjective alors $I_i + I_j = A$, $1 \le i \ne j \le r$.*

Démonstration. Supposons d'abord que $I_i + I_j = A$, $1 \le i \ne j \le r$. On a toujours $\cap_{1\le i\le r} I_i \supset I_1 \cdots I_r$. Pour l'inclusion inverse et la surjectivité de $p := \prod_{1\le i\le r} p_{I_i} : A \to \prod_{1\le i\le r} A/I_i$, on procède par récurrence sur r. Si $r = 2$, il existe $a_i \in I_i$, $i = 1,2$ tels que $1 = a_1 + a_2$. En particulier,

— Pour tout $x \in I_1 \cap I_2$, $x = x1 = x(a_1 + a_2) = xa_1 + xa_2 = a_1x + xa_2 \in I_1 \cdot I_2$.
— Soit $x_1, x_2 \in A$ arbitraires. En posant $x = a_1x_2 + a_2x_1$ on a bien $p_{I_1}(x) = p_{I_1}(a_2)p_{I_1}(x_1) = p_{I_1}(x_1)$ et $p_{I_2}(x) = p_{I_2}(a_1)p_{I_2}(x_2) = p_{I_2}(x_2)$.

Si $r \ge 3$, on a par hypothèse de récurrence $I_2 \cap \cdots \cap I_r = I_2 \cdots I_r$ et $A/(I_2 \cap \cdots \cap I_r) \twoheadrightarrow \prod_{2\le i\le r} A/I_i$. Il suffit de montrer que $I_1 + I_2 \cdots I_r = A$. En effet, le cas $r = 2$ (et l'hypothèse de récurrence) nous donnera alors

— $I_1 \cap (I_2 \cap \cdots \cap I_r) = I_1 \cap (I_1 \cdots I_r) = I_1 \cdot (I_2 \cdots I_r) = I_1 \cdots I_r$.
— $A \twoheadrightarrow A/I_1 \times A/(I_2 \cap \cdots \cap I_r) \twoheadrightarrow A/I_1 \times \prod_{2\le i\le r} A/I_i \twoheadrightarrow \prod_{1\le i\le r} A/I_i$

Mais pour $i = 2,\dots,r$ il existe $a_i \in I_1$, $b_i \in I_i$ tels que $a_i + b_i = 1$. On a donc $1 = \prod_{2\le i\le r}(a_i + b_i) = \prod_{2\le i\le r} a_i + \cdots \in I_1 + I_2 \cdots I_r$.

Inversement, si $p : A \to \prod_{1\le i\le r} A/I_i$ est surjective, pour tout $1 \le i \ne j \le r$, il existe $x \in A$ tel que $p(x) = (\delta_{i,k})_{1\le k\le r} \in \prod_{1\le i\le r} A/I_i$ *i.e.* $x \in 1 + I_i$ et $x \in I_j$. Donc $1 = (1-x) + x \in I_i + I_j$. □

2.3 Corps et idéaux maximaux

Le singleton $\{0\}$ et A sont des ideaux de A. En général, un anneau contient beaucoup d'idéaux. L'ensemble des idéaux et leur 'position' dans l'anneau mesure la complexité de celui-ci. En ce sens, les anneaux les plus simples sont les corps.

??.1 Lemme. *Les propositions suivantes sont équivalentes :* *(i)* *A est un corps ;*
(ii) *Les seuls idéaux de A sont $\{0\}$ et A*

Démonstration. Si A est un corps, tout idéal $\{0\} \subsetneq I \subset A$ contient un élément $a \neq 0$ donc inversible. Mais alors $1 = a^{-1}a \in AI = I$ donc $A = A1 \subset AI = I$. Inversement, si les seuls idéaux de A sont $\{0\}$ et A, pour tout $a \neq 0$, $\{0\} \subsetneq Aa \subset A$ est un idéal donc $Aa = A$. En particulier $1 \in Aa$ *i.e.* il existe $a^{-1} \in A$ tel que $1 = a^{-1}a$. □

??.2 Lemme. *Soit $I \subsetneq A$ un idéal. Les propositions suivantes sont équivalentes* *(i)* *A/I est un corps*
(ii) *I est maximal da*

Démonstration. Cela résulte de **??**.2. □

On dit qu'un idéal qui vérifie les propriétés (i), (ii) de **??**.2 est *maximal*.

??.3 Lemme. [Utilise le Lemme de Zorn] *L'ensemble ordonné $(\mathcal{I}_A \setminus \{A\}, \subset)$ est (non-vide ; il contient $\{0\}$) inductif. En particulier, tout idéal $I \subsetneq A$ est contenu dans un idéal maximal.*

Démonstration. Il suffit d'observer que si $I_1 \subset I_2 \subset \cdots \subsetneq A$ est une suite d'ideaux de A distincts de A et croissante pour $\subset$, $I := \cup_{n\geq 1} I_n \subsetneq A$ est encore un idéal de A distincts de A. En effet, pour tout $a, b \in I$ il existe n tel que $a, b \in I_n$ donc $a - b \in I_n \subset I$ et pour tout $\alpha \in A$, $\alpha a \in I_n \subset I$; cela montre déja que $I \subset A$ est un idéal. Dans ce cas, $I = A$ si et seulement si $1 \in I$. Mais si $1 \in I$, il existerait $n \geq 1$ tel que $1 \in I_n$, ce qui n'est pas possible puisque par hypothèse $I_n \subsetneq A$. □

En particulier, pour tout $a \in A$, $a \notin A^\times \Leftrightarrow Aa \subsetneq A \Leftrightarrow a$ est contenu dans au moins un idéal maximal de A.

On notera $\mathrm{spm}(A)$ l'ensemble des idéaux maximaux de A et on dit que c'est le *spectre maximal* de A. D'après **??**.1, les projections canoniques $p_\mathfrak{m} : A \twoheadrightarrow A/\mathfrak{m}$, $\mathfrak{m} \in \mathrm{spm}(A)$ induisent un morphisme d'anneaux canonique

$$p_{max} : A \to \prod_{\mathfrak{m}\in \mathrm{spm}(A)} A/\mathfrak{m}$$

dont le noyau $\mathcal{J}_A := \ker(p_{max}) = \bigcap_{\mathfrak{m}\in \mathrm{spm}(A)} \mathfrak{m} \subset A$ est un idéal appelé *radical de Jacobson* de A.

Exercice. Soit $a \in A$. Montrer que $a \in \mathcal{J}_A$ si et seulement si $1 - ab \in A^\times$, $b \in A$.

2.3.1 Anneaux intègres et idéaux premiers

On dit qu'un élément $t \in A$ est de torsion (ou est un diviseur de zéro) s'il existe $0 \neq a \in A$ tel que $at = 0$. On notera $A_{tors} \subset A$ l'ensemble des éléments de torsion de A. On dit qu'un anneau A est *intègre* si $A_{tors} = \{0\}$.

Exemples.
— Les corps sont intègres, $\mathbb{Z}$ est intègre.
— Tout sous-anneau d'un anneau intègre est intègre. Si A est un anneau intègre, $A[X]$ est intègre. Par contre, le produit $A_1 \times A_2$ de deux anneaux non nuls n'est jamais intègre.
— $\mathbb{Z}/n$ est intègre si et seulement si n est un nombre premier.

Remarque. Pour tout $a \in A \setminus A_{tors}$ et pour tout $b, c \in A$ on a $ab = ac \Leftrightarrow a(b-c) = \Leftrightarrow b - c = 0$. Autrement dit, 'on peut simplifier par a'. En particulier, si A est intègre, on peut simplifier par tout élément $a \neq 0$.

??.1 **Lemme.** *Soit $I \subsetneq A$ un idéal. Les propositions suivantes (i) A/I est intègre ; (ii) Pour tout $a, b \in A$*

Démonstration. (i) $\Rightarrow$ (ii) : Si $ab \in I$ alors $\overline{a}\overline{b} = 0$ dans A/I. Par (i), on a forcément $\overline{a} = 0$ (*i.e.* $a \in I$) ou $\overline{b} = 0$ (*i.e.* $b \in I$) dans A/I. (ii) $\Rightarrow$ (i) : Pour tout $0 \neq \overline{a}, \overline{b} \in A/I$, choisissons $a, b \in A$ relevant $\overline{a}, \overline{b} \in A/I$. On a forcément $a, b \notin I$ donc, par (ii), $an \notin I$ *i.e.* $\overline{a}\overline{b} = \overline{ab} \neq 0$ in A/I. □

On dit qu'un idéal qui vérifie les propriétés (i), (ii) de **??**.2 est *premier*. On notera $\mathrm{Spec}(A)$ l'ensemble des idéaux premiers de A et on dit que c'est le *Spectre* de A. D'après **??**.1, les projections canoniques $p_{\mathfrak{p}} : A \twoheadrightarrow A/\mathfrak{p}$, $\mathfrak{p} \in \mathrm{Spec}(A)$ induisent un morphisme d'anneaux canonique

$$p_{prem} : A \to \prod_{\mathfrak{p} \in \mathrm{Spec}(A)} A/\mathfrak{p}$$

dont le noyau $\mathcal{R}_A := \ker(p_{prem}) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} \subset A$ est un idéal appelé *radical* de A.

On dit qu'un élément $a \in A$ est *nilpotent* s'il existe un entier $n \geq 1$ tel que $a^n = 0$ et, si $a \neq 0$, on dit que le plus petit entier $n \geq 1$ tel que $a^{n-1} \neq 0$ et $a^n = 0$ est l'indice de nilpotence de a (on dit parfois que 0 est d'indice de nilpotence 1). On note $\mathcal{N}_A \subset A$ l'ensemble des éléments nilpotents de A. On a évidemment $\mathcal{N}_A \subset A_{tors}$ donc, en particulier, si A est un anneau intègre, $\mathcal{N}_A = \{0\}$.

??.2 **Proposition.** [Utilise le Lemme de Zorn] *$\mathcal{N}_A \subset A$ est un idéal et $\mathcal{N}_A = \mathcal{R}_A$.*

Démonstration. Vérifions d'abord que $\mathcal{N}_A \subset A$ est un idéal. Pour tout $a, b \in \mathcal{N}_A$, il existe des entiers $m, n \geq 1$ tel que $a^m = b^n = 0$. Donc, par la formule du binôme de Newton

$$(a-b)^{m+n-1} = \sum_{0 \leq k \leq m+n-1} \binom{k}{m+n-1} (-1)^{m+n-k-1} a^k b^{m+n-k} = 0$$

puisque, si $k < m$, $m+n-k-1 > n-1$ donc $m+n-k-1 \geq n$. On a aussi pour tout $\alpha \in A$ $(\alpha a)^m = \alpha^m a^m = 0$.

Pour tout morphime d'anneaux $\phi : A \to B$ on a $\phi(\mathcal{N}_A) \subset \mathcal{N}_B$. En particulier, si B est un anneau intègre, $\mathcal{N}_A \subset \ker(\phi)$. En appliquant cette observation aux projections canoniques $p_{\mathfrak{p}} : A \twoheadrightarrow A/\mathfrak{p}$, $\mathfrak{p} \in \mathrm{Spec}(A)$, on en déduit l'inclusion $\mathcal{N}_A \subset \mathcal{R}_A$. Inversement, soit $a \notin \mathcal{N}_A$; on veut montrer que $a \notin \mathcal{R}_A$ *i.e.* il existe $\mathfrak{p} \in \mathrm{Spec}(A)$ tel que $a \notin \mathfrak{p}$ (ce qui équivaut aussi à $a^n \notin \mathfrak{p}$ pour n'importe quel entier $n \geq 1$). Notons $X_a := \{a^n \mid n \in \mathbb{Z}_{\geq 1}\}$ l'ensemble des puissances de a. On a par hypothèse $0 \notin X_a$ donc l'ensemble $\Sigma_a \subset \mathcal{I}_A$ des idéaux $I \subset A$ tels que $X_a \cap I = \varnothing$ est non-vide puisqu'il contient $\{0\}$. On vérifie immédiatement que $(\Sigma_a, \subset)$ est ordonné inductif donc, par le Lemme de Zorn, possède un élément maximal $I \in \Sigma_a$. Puisque $a \notin I$, il suffit de montrer que I est premier *i.e.* que A/I est intègre. Notons $\overline{a}$ l'image de a dans A/I. Par définition de I, $0 \notin X_{\overline{a}}$ mais pour tout idéal $\{0\} \subsetneq \overline{J} \subset A/I$, $X_{\overline{a}} \cap \overline{J} \neq \varnothing$. En particulier, pour tout $0 \neq \overline{b} \in A/I$, il existe $n_b \geq 1$ tel que $\overline{a}^{n_b} \in (A/I)\overline{b}$ donc pour tout $0 \neq \overline{b}, \overline{b'} \in A/I$, $\overline{a}^{n_b n_{b'}} \in (A/I)\overline{bb'}$ donc $\overline{bb'} \neq 0$. □

Exercice.

— Montrer que si $a \in A$ est nilpotent, $1 + a \in A^\times$. En déduire que la somme d'un élément nilpotent et d'un élément inversible est encore inversible.

— Montrer que $A[X]^\times$ est l'ensemble des polynômes $P = \sum_{n\geq 0} a_n X^n$ tels que $a_0 \in A^\times$ et a_n est nilpotent, $n \geq 1$. Déterminer $A[X_1, \ldots, X_r]^\times$.

??.3 Exercice.

1. Soit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ des idéaux premiers et $I \subset A$ un idéal. Si $I \subset \cup_{1\leq i\leq r}\mathfrak{p}_i$ il existe $1 \leq i \leq r$ tel que $I \subset \mathfrak{p}_i$;
2. Soit $I_1, \ldots, I_r$ des idéaux et $\mathfrak{p} \subset A$ un idéal premier. Si $\mathfrak{p} \supset \cap_{1\leq i\leq r} I_i$ il existe $1 \leq i \leq r$ tel que $\mathfrak{p} \supset I_i$.

2.3.2 Anneaux réduits et idéaux radiciels

On dit qu'un anneau A est *réduit* si $\mathcal{R}_A = \mathcal{N}_A = 0$.

Exemples. Les anneaux intègres sont réduits, l'anneau $\mathbb{Z} \times \mathbb{Z}$ est réduit non-intègre. Si p est un nombre premier l'anneau $\mathbb{Z}/p^n$ n'est pas réduit et contient un élément d'indice de nilpotence n, $n \geq 1$. Si on note p_n le nième nombre premier, l'anneau $\prod_{n\geq 1} \mathbb{Z}/p_n^n$ n'est pas réduit et contient un élément d'indice de nilpotence n pour tout $n \geq 1$.

Pour un idéal $I \subset A$, on note $\sqrt{I} := p_I^{-1}(\mathcal{N}_{A/I})$. Par définition,

$$I \subset \sqrt{I} = \bigcup_{n\geq 1} \{a \in A \mid a^n \in I\}.$$

On dit que $\sqrt{I}$ est la racine de I. Avec cette notation, $\mathcal{N}_A = \sqrt{\{0\}}$. Il résulte des définitions que pour un idéal $I \subsetneq A$ les propositions suivantes sont équivalentes (i) A/I est réduit ;
(ii) $I = \sqrt{I}$.

On dit qu'un idéal $I \subsetneq A$ qui vérifie les propriétés (i), (ii) ci-dessus est *radiciel*. On notera $\mathcal{I}_A^{red}$ l'ensemble des idéaux radiciels de A.

En résumé on a

$$\text{Maximal} \Rightarrow \text{Premier} \Rightarrow \text{Radicieł; } i.e. \ \operatorname{spm}(A) \subset \operatorname{Spec}(A) \subset \mathcal{I}_A^{red}$$

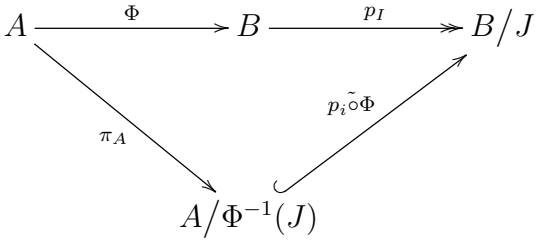
et

I	A/I
Maximal	Corps
Premier	Intègre
Radiciel	Réduit

Classification grossière des idéaux

2.3.3

Tout morphisme $\phi : A \to B$ d'anneaux commutatifs induit une application $\phi^{-1} : (\mathcal{I}_B, \subset) \to (\mathcal{I}_A, \subset)$ préservant $\subset$. De plus, si $I \in \mathcal{I}_B$, le noyau de $A \xrightarrow{\phi} B \overset{p_I}{\twoheadrightarrow} B/I$ est $\phi^{-1}(I)$, d'où un morphisme d'anneaux injectifs $A/\phi^{-1}(I) \hookrightarrow B/I$. Comme un sous-anneau d'un anneau intègre (resp. réduit) est intègre (resp. réduit), on en déduit que $\phi^{-1} : (\mathcal{I}_B, \subset) \to (\mathcal{I}_A, \subset)$ se restreint en des applications



$$\begin{array}{ccc} (\mathcal{I}_B, \subset) & \overset{\phi^{-1}}{\to} & (\mathcal{I}_A, \subset) \\ \bigcup & & \bigcup \\ (\mathcal{I}_B^{red}, \subset) & \overset{\phi^{-1}}{\to} & (\mathcal{I}_A^{red}, \subset) \\ \bigcup & & \bigcup \\ (\operatorname{Spec}(B), \subset) & \overset{\phi^{-1}}{\to} & (\operatorname{Spec}(A), \subset) \end{array}$$

Il n'est par contre pas vrai qu'un sous-anneau d'un corps est un corps (*e.g.* $\mathbb{Z} \subset \mathbb{Q}$) donc l'image inverse d'un idéal maximal par un morphisme d'anneau n'est, en général, pas maximal.

Chapitre 3

Anneaux noethériens

3.1 Lemme

Lemme 3.1.0.1. *Soit A un anneau. Les propositions suivantes sont équivalentes.*
1. *Tout idéal $I \subset A$ est de type fini.*
2. *Toute suite d'idéaux de A croissante pour $\subset$ est stationnaire à partir d'un certain rang.*
3. *Tout sous-ensemble non vide d'idéaux de A admet un élément maximal pour $\subset$.*

Démonstration. (1) $\Rightarrow$ (2). Supposons que tous les idéaux de A sont de type fini. Soit $I_0 \subset \cdots \subset I_n \subset I_{n+1} \subset \cdots \subset A$ une suite croissante d'idéaux pour $\subset$. L'ensemble $I := \cup_{n\geq 0} I_n \subset A$ est un idéal ; il existe donc un ensemble fini $X \subset A$ tels que $I = \sum_{x\in X} Ax$. Mais pour chaque $x \in X$, il existe $n_x \geq 0$ tel que $x \in I_{n_x}$. Donc avec $n := \max\{n_x \mid x \in X\}$, on a $X \subset I_n$ donc $I \subset I_n$.
(2) $\Rightarrow$ (3). Soit $\mathcal{I} \subset \mathcal{I}_A$ un sous-ensemble non-vide. Supposons que $\mathcal{I}$ n'admette pas d'élément maximal pour $\subset$. Soit $I_0 \in \mathcal{I}$. Puisque I_0 n'est pas maximal pour $\subset$, on peut trouver $I_1 \in \mathcal{I}$ tel que $I_0 \subsetneq I_1$. En réitérant l'argument on construit une suite strictement croissante $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \cdots$ d'élément de $\mathcal{I}$, ce qui contredit (1).
(3) $\Rightarrow$ (1). Soit $I \subset A$ un idéal. Notons $\mathcal{I} \subset \mathcal{I}_A$ le sous-ensemble des idéaux de type fini de A contenu dans I. $\mathcal{I}$ est non-vide puisqu'il contient $\{0\}$. Par (3), il admet donc un élément I° maximal pour $\subset$. Si $I^\circ \subsetneq I$, il existe $a \in I$ tel que $I^\circ \subsetneq I^\circ + Aa \subset I$. Par construction $I^\circ + Aa$ est de type fini, ce qui contredit la maximalité de I. □

Définition 3.1.0.1 (anneau noethérien)**.** On dit qu'un anneau A qui vérifie les propriétés équivalentes du Lemme **??** est *noethérien*.

3.2 Éxemples

Exemple 3.2.0.1. 1. Les anneaux principaux (*e.g.* k, $\mathbb{Z}$, $k[X]$, où k est un corps commutatif) sont noethériens.
2. Si k est un corps commutatif, une k-algèbre $\phi : k \to A$ est toujours munie d'une structure de k-espace vectoriel : $k \times A \to A$, $(\lambda, a) \to \phi(\lambda)a$. Avec cette structure de k-espace vectoriel, les idéaux de A sont automatiquement des sous-k-espace vectoriel. Si A est de dimension finie sur k, elle est donc noethérienne. Par exemple l'anneau $k[X]/X^n k[X]$ est un noethérien.

3. Tout quotient d'un anneau noethérien est noethérien. En effet, soit A est un anneau noethérien et $I \subset A$ un idéal ; notons $p_I : A \twoheadrightarrow A/I$ la projection canonique. Si $J \subset A/I$ est un idéal, $p_I^{-1}(J) \subset A$ est un idéal donc, en particulier, il est engendré par un nombre fini $a_1, \ldots, a_r$ d'éléments. Mais alors, $J = p_I p_I^{-1}(J)$ est engendré par les $p_I(a_1), \ldots, p_I(a_r)$.
4. Par contre un sous-anneau d'un anneau noethérien n'est pas forcément noethérien. Par exemple, on va voir (**??**) que si k est un corps commutatif, l'anneau $k[X_1, X_2]$ est noethérien mais la sous-k-algèbre engendrée par les $X_1 X_2^n$, $n \geq 0$ n'est pas un anneau noethérien.

La proposition suivante et son corollaire fournissent un très grand nombre d'exemples d'anneaux noethériens.

3.3 Proposition

Proposition 3.3.0.1 (transfert de noethérianité)**.** *A noethérien $\Rightarrow$ $A[X]$ noethérien.*

Démonstration. Soit $I \subset A[X]$ un idéal. Pour chaque $n \geq 0$ définissons $\mathfrak{I}_n \setminus \{0\} \subset A$ comme l'ensemble des $a \in A$ qui apparaissent comme coefficient dominant d'un polynôme de degré n dand I *i.e.* $a \in \mathfrak{I}_n$ si et seulement si il existe $a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + aX^n \in I$. Comme $I \subset A[X]$ est un idéal, les $\mathfrak{I}_n \subset A$ sont automatiquement des idéaux. De plus,

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + aX^n \in I \Rightarrow a_0 X + a_1 X^2 + \cdots + a_{n-1} X^n + aX^{n+1} \in I$$

donc on a

$$\mathfrak{I}_0 \subset \mathfrak{I}_1 \subset \cdots \subset \mathfrak{I}_n \subset \mathfrak{I}_{n+1} \subset \cdots$$

Comme A est noethérien, cette suite devient stationnaire à partir d'un certain rang, disons n. De plus, chaque $\mathfrak{I}_k$ est de type fini ; notons $a_{k,1}, \ldots, a_{k,r_k} \in \mathfrak{I}_k$ un ensemble fini de générateurs de $\mathfrak{I}_k$. Enfin, pour $k = 0, \ldots, n$, $l = 1, \ldots, r_k$, fixons un polynôme $P_{k,l} \in I$ de degré k et de coefficient dominant $a_{k,l}$. Il suffit de montrer que I est engendré par les $P_{k,l}$, $l = 1, \ldots, r_k$, $k = 0, \ldots, n$. Notons donc $I^\circ := \sum AP_{k,l} \subset I$ et montrons par induction sur le degré d de $P \in I$ que $P \in I^\circ$. Si $d = 0$, on a par définition $\mathfrak{I}_0 \subset I^\circ$. Supposons que I° contient tous les éléments de I de degré $\leq d$. Soit $P = a_0 + \cdots + a_d X^d + a_{d+1} X^{d+1} \in I$ de degré $d+1$. Si $d+1 \geq n$, on a $a_{d+1} \in \mathfrak{I}_{d+1} = \mathfrak{I}_n$ donc on peut écrire $a_{d+1} = \sum_{1 \leq i \leq r_n} \alpha_i a_{n,i}$ et $P - \sum_{1 \leq i \leq r_n} \alpha_i X^{d+1-n} P_{n,i}$ est encore dans I mais de degré $\leq d$ donc, par hypothèse de récurrence, dans I°. Si $d+1 \leq n$, $a_{d+1} \in \mathfrak{I}_{d+1}$ donc on peut écrire $a_{d+1} = \sum_{1 \leq i \leq r_n} \alpha_i a_{d+1,i}$ et $P - \sum_{1 \leq i \leq r_n} \alpha_i P_{d+1,i}$ est encore dans I mais de degré $\leq d$ donc, par hypothèse de récurrence, dans I°. □

3.4 Corollaire

Corollaire 3.4.0.1. *Si A est un anneau noethérien, toute A-algèbre de type fini est un anneau noethérien.*

Démonstration. Observons d'abord qu'en raisonnant par induction sur $n \geq 1$, l'isomorphisme

$$A[X_1, \ldots, X_n] \tilde{\to} A[X_1, \cdots, X_{n-1}][X_n]$$

et la proposition **??** impliquent que $A[X_1, \dots, X_n]$ est un anneau noethérien. On conclut par l'exemple **??** (3) puisque toute A-algèbre de type fini est quotient d'une A-algèbre de la forme $A[X_1, \dots, X_n]$. □

3.5 Exercices

Exercice 3.5.0.1. 1. Soit A un anneau noethérien. Montrer que pour tout idéal $I \subsetneq A$, $\sqrt{I}$ est l'intersection d'un nombre fini d'idéaux premiers. En déduire que A possède un nombre fini d'idéaux premiers minimaux pour $\subset$.

2. (Anneaux artiniens) Soit A un anneau. Montrer que les propositions suivantes sont équivalentes

   (a) Toute suite d'idéaux de A décroissante pour $\subset$ est stationnaire à partir d'un certain rang.

   (b) Tout sous-ensemble non vide d'idéaux de A admet un élément minimal pour $\subset$.

   On dit qu'un anneau A qui vérifie les propriétés équivalente ci-dessus est *artinien*. En dépit de la similitude des définitions, les anneaux artiniens et noethériens se comportent très différemment. Soit A un anneau artinien. Montrer que

   (a) Tout idéal premier de A est maximal.

   (b) A ne possède qu'un nombre fini d'idéaux (premiers=) maximaux.

   (c) A est noethérien.

   En fait, on peut montrer qu'un anneau est artinien si et seulement si il est noethérien et tous ses idéaux premiers sont maximaux.

Chapitre 4

Anneaux principaux, euclidiens

4.1

On dit qu'un anneau commutatif intègre A est

— *euclidien* s'il est munit d'une application - appelée stathme euclidien - $\sigma : A \setminus \{0\} \to \mathbb{N}$ vérifiant la propriété suivante (division euclidienne) : pour tout $0 \neq a, b \in A$ il existe $q, r \in A$ tels que

$$\begin{aligned} &b = qa + r \\ &r = 0 \text{ ou } r \neq 0 \text{ et } \sigma(r) < \sigma(a). \end{aligned}$$

— *principal* si tout idéal est de la forme Aa, $a \in A$.

4.2 Exemples

1. La valeur absolue usuelle $|-| : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ sur $\mathbb{Z}$ est un stathme euclidien. En effet, pour tout $0 \neq a, b \in \mathbb{Z}$ notons $R := \{b - qa \mid q \in \mathbb{Z}\}$. On a évidemment $R \cap \mathbb{N} \neq \varnothing$ donc on peut poser $r := \min R \cap \mathbb{N}$. Par définition de R, $b = qa + r$ et si $|a| \leq r$ on aurait $r - |a| \in R$: contradiction.

2. **Algèbres de polynômes sur un anneau intègre.** Soit A un anneau commutatif et $r \geq 1$ un entier. La A-algèbre $A[X_1, \ldots, X_r]$ n'est euclidienne que si A est un corps et $r = 1$ mais, lorsque A est intègre, elle se comporte presque comme un anneau euclidien.
   — $r = 1$. On rappelle que tout $P \in A[X]$ s'écrit de façon unique sous la forme $f = \sum_{n \in \mathbb{N}} a_n X^n$ avec $\underline{a} : n \to a_n \in A^{(\mathbb{N})}$. Cela permet de définir l'application degré :

$$\begin{array}{rlcl} \deg : & A[X] \setminus \{0\} & \to & \mathbb{N} \\ & f = \sum_{n \in \mathbb{N}} a_n X^n & \to & \max\{n \in \mathbb{N} \mid a_n \neq 0\} \end{array}$$

et une application 'coefficient dominant'

$$\begin{array}{rccc} \mathrm{CD}: & A[X]\setminus\{0\} & \to & A\setminus\{0\} \\ & f=\sum_{n\in\mathbb{N}} a_n X^n & \to & a_{\deg(f)} \end{array}$$

La définition du produit dans $A[X]$ montre que $\deg(fg)\leq \deg(f)+\deg(g)$ et que si l'un au moins de $\mathrm{CD}(f), \mathrm{CD}(g)$ n'est pas de torsion dans A, $\deg(fg)=\deg(f)+\deg(g)$, $\mathrm{CD}(fg)=\mathrm{CD}(f)\,\mathrm{CD}(g)$. On a aussi toujours $\deg(f+g)\leq \max\{\deg(f),\deg(g)\}$.

Lemme *Soit $0\neq f,g\in A[X]$ et supposons que $\mathrm{CD}(f)\in A^\times$. Alors il existe un unique couple $q,r\in A[X]$ tel que $g=fq+r$ et $r=0$ ou $\deg(r)<\deg(f)$.*

Démonstration. Montrons l'existence par récurrence sur $deg(g)$. Écrivons $f=\sum_{0\leq n\leq d_f} a_n X^n$, $g=\sum_{0\leq n\leq d_g} b_n X^n$, où $d_f:=\deg(f)$, $d_g:=\deg(g)$. Si $d_g=0$ et $d_f>0$, $q=0$ et $r=g$ conviennent. Si $d_g=d_f=0$, $f=a_0=a_{d_f}\in A^\times\subset A[X]^\times$ donc $q=f^{-1}g$ et $r=0$ conviennent. Si $d_g\geq 1$ et $d_f>d_g$, $q=0$ et $r=g$ conviennent. Supposons donc $d_f\leq d_g$. Comme $a_{d_f}\in A^\times$ on peut écrire

$$g=a_{d_g}a_{d_f}^{-1}X^{d_g-d_f}f+(g-a_{d_g}a_{d_f}^{-1}X^{d_g-d_f}f).$$

Par construction, $g_1:=(g-a_{d_g}a_{d_f}^{-1}X^{d_g-d_f}f)$ est de degré $\leq d_g-1$. Par hypothèse de récurrence il existe donc $q_1,r_1\in A[X]$ tels que $g_1=q_1f+r_1$ et $r_1=0$ ou $\deg(r_1)<\deg(f)$; $q:=a_{d_g}a_{d_f}^{-1}X^{d_g-d_f}+q_1$, $r:=r_1$ conviennent. Il reste à prouver l'unicité. Si $q',r'\in A[X]$ est un autre couple tel que $g=fq'+r'$ et $r'=0$ ou $\deg(r')<\deg(f)$, on a $f(q-q')=r'-r$. Si $r-r'\neq 0$, en prenant le degré

$$\deg(f)\geq \deg(f)+\deg(q-q')\overset{(1)}{=}\deg(f(q-q')=\deg(r-r')<\deg(f),$$

où (1) utilise encore que $\mathrm{CD}(f)\in A^\times$. On a donc forcément $r=r'$ donc $f(q-q')=0$ donc, toujours parce que $\mathrm{CD}(f)\in A^\times$, $q=q'$.

□

En particulier, si $A=k$ est un corps, le degré $\deg : k[X]\setminus\{0\}\to\mathbb{N}$ est un stathme euclidien sur $k[X]$.

— $r\geq 1$. En utilisant les isomorphismes canoniques $A[X_1,\dots,X_r]\tilde{\to}A[X_1,\dots,\hat{X}_i,\cdots,X_r][X_i]$, $i=1,\dots,r$, on peut encore appliquer le Lemme ci-dessus dans $A[X_1,\dots,X_r]$: les polynômes par lesquels on peut diviser sont ceux de la forme $aX_i^d+\sum_{\underline{n}\in\mathbb{N}^r,\,|\,n_i<d} a_{\underline{n}}\underline{X}^{\underline{n}}$, avec $a\in A[X_1,\dots,\hat{X}_i,\cdots,X_r]^\times=A^\times$ (car A est intègre donc réduit).

3. On peut montrer que le carré de la valeur absolue usuelle $|-|^2:\mathbb{Z}[w]\to\mathbb{N}$ est un stathme euclidien sur certains sous-anneaux de $\mathbb{C}$ de la forme $\mathbb{Z}[w]\subset\mathbb{C}$; c'est par exemple le cas pour $w=\sqrt{-1},^3\sqrt{-1},\sqrt{-2}$.

4.3 Lemme

Euclien ⇒ Principal.

Démonstration. Soit A un anneau euclidien et soit $I \subset A$ un idéal. Fixons $a \in I$ tel que $\sigma(a) = \min\sigma(I)$. Puisque $a \in I$, on a $Aa \subset I$. Réciproquement, pour tout $b \in I$, effectuons la division euclidienne de b par a : il existe $q, r \in A$ tels que $b = qa + r$ et $r = 0$ ou $\sigma(r) < \sigma(a)$. Mais comme $r = b - qa \in I$, on ne peut pas avoir $\sigma(r) < \sigma(a)$, donc $r = 0$.

□

(Contre-)Exemple. Les anneaux principaux ne sont pas tous euclidiens. Par exemple $A = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ est principal non euclidien.

4.4 Exercice

Montrer que $A[X]$ est principal si et seulement si A est un corps.

4.5 Lemme

Si A est un anneau principal, $\mathrm{spm}(A) = \mathrm{Spec}(A) \setminus \{0\}$.

Démonstration. On a toujours $\mathrm{spm}(A) \subset \mathrm{Spec}(A)$. Soit $\mathfrak{p} = Ap \in \mathrm{Spec}(A)$; on veut montrer que A/Ap est un corps. Supposons le contraire. Alors A/Ap contient un idéal maximal $\{\bar{0}\} \subsetneq \mathfrak{m} \subsetneq A/Ap$. Écrivons $p_{\mathfrak{p}}^{-1}(\mathfrak{m}) = Am$. On a des inclusions strictes $Ap \subsetneq Am \subsetneq A$ donc il existe $a \in A$ tel que $p = am$ donc $\bar{0} = \bar{a}\bar{m}$ dans A/Ap. Comme A/Ap est intègre et $\bar{m} \neq 0$, on en déduit $a \in Ap$. Écrivons donc $a = bp$; on a $p = am = pbm$. Comme A est intègre, on peut simplifier par p pour obtenir $1 = bm$, ce qui contredit $Am \subsetneq A$. □

Chapitre 5

Anneaux factoriels

Soit A un anneau commutatif intègre.

Pour tout $a, b \in A$ on a $Aa = Ab$ si et seulement si $A^\times a = A^\times b$. L'implication $A^\times a = A^\times b \Rightarrow Aa = Ab$ est toujours vraie (sans supposer A intègre). Réciproquement, si $a = 0$ alors $Ab = 0$ impose $b = 0$ puisque A est intègre. Supposons donc $a, b \neq 0$ et $Aa = Ab$. On peut écrire $a = \alpha b$ et $b = \beta a$ donc $a = \alpha\beta a$ et, comme A est intègre, on peut simplifier par a, ce qui montre que $\alpha, \beta \in A^\times$. On note $a \sim b$ (et on dit que a, b sont *associés* dans A) la relation $Aa = Ab$ ($\Leftrightarrow A^\times a = A^\times b$) ; c'est une relation d'équivalence sur A.

5.1 Éléments irréductibles, éléments premiers

On dit que $0 \neq p \in A \setminus A^\times$ est *irréductible* si pour tout $a, b \in A$, $p = ab$ implique $a \in A^\times$ ou $b \in A^\times$. On notera $\mathcal{P}_A^\circ \subset A$ l'ensemble des éléments irréductibles de A. On munit $\mathcal{P}_A^\circ$ de la relation d'équivalence $\sim$ définie par : pour tout $p, q \in \mathcal{P}_A^\circ$, $p \sim q$ si et seulement si $Ap = Aq$, ce qui est aussi équivalent à $A^\times p = A^\times q$.

On notera $\mathcal{P}_A \subset \mathcal{P}_A^\circ$ un système de représentants de $\mathcal{P}_A^\circ / \sim$.

Exemple. On a $\mathbb{Z}^\times = \{\pm 1\}$ et les irrd́uctibles de $\mathbb{Z}$ sont les nombres premiers. Si l'on veut déterminer si un entier $n \in \mathbb{Z}_{\geq 1}$ est premier, on dispose d'un algorithme évident consistant à lister tous les premiers $\leq \sqrt{n}$ et vérifier s'ils divisent n mais cet algorithme devient très vite inutilisable sur machine. Les arithméticiens ont beaucoup étudié et étudient encore le problème de la construction et de la rṕartition des nombres premiers. L'une de leurs motivations est l'application des nombres premiers en cryptographie. Parmi les énoncés classiques les plus spectaculaires, on trouve par exemple le théorème des nombres premiers, qui dit que si on note $\pi(n)$ le nombre de nombre premiers $0 \leq p \leq n$, on a $\pi(n) \sim_{n \to +\infty} \ln(n)/n$ ou le théorème de la progression arithmétique, qui dit que pour tout entier $0 \neq m, n$ premiers entre eux l'ensemble $m + \mathbb{Z}n$ contient une infinité de nombres premiers. Ces énoncés se démontrent souvent par des méthodes analytiques.

Exercice. Montrer directement le théorème de la progression arithmétique pour $(m, n) = (3, 4)$.

On dit que $0 \neq p \in A \setminus A^\times$ est *premier* si $Ap \in \mathrm{Spec}(A)$. On notera $\mathcal{P}_A^\dagger \subset A$ l'ensemble des éléments premiers de A.

??.1 **Lemme.** *On a toujours* $\mathcal{P}_A^\dagger \subset \mathcal{P}_A^\circ$.

Démonstration. En effet, si $Ap \in spec(A)$, pour tout $a, b \in A$, $p = ab$ implique $ab \in Ap$ donc comme Ap est premier, $a \in Ap$ ou $b \in Ap$. Supposons $a \in Ap$ *i.e.* $a = \alpha p$. On a alors $p = ab = \alpha bp$ et, comme A est intègre, on peut simplifier par p ce qui donne $\alpha b = 1$ donc $b \in A^\times$. □

(Contre-)exemple. En général $\mathcal{P}_A^\dagger \subsetneq \mathcal{P}_A^\circ$. Par exemple, dans $A = \mathbb{Z}[i\sqrt{5}]$, 2 est irréductible mais pas premier. En effet, introduisons la norme $N : A \to \mathbb{Z}_{\geq 0}$, $a + ib\sqrt{5} \to |a + ib\sqrt{5}|^2 = a^2 + 5b^2$. On vérifie immédiatement que $N(xy) = N(x)N(y)$, $N(x) = 0 \Leftrightarrow x = 0$ et que

$$x \in A^\times \Leftrightarrow N(x) = 1 \Leftrightarrow x = \pm 1.$$

Vérifions d'abord que $2 \in \mathcal{P}_A^\circ$. Si on écrit $2 = xy$ on doit avoir $4 = N(2) = N(xy) = N(x)N(y)$. En particulier, $N(x) = N(y) = 2$ ou $\{N(x), N(y)\} = \{1, 4\}$. Or $2 \notin N(A)$ donc nécessairement $N(x) = 1$ ou $N(y) = 1$ *i.e.* $x \in A^\times$ ou $y \in A^\times$. Montrons ensuite que 2 n'est pas premier. Pour cela, observons que

$$2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}) = 2 \times 3 \in 2A$$

mais que $1 \pm i\sqrt{5} \notin 2A$ car $N(1 \pm i\sqrt{5}) = 6 \notin N(2A) = 4N(A) \subset 4\mathbb{Z}_{\geq 0}$.

??.2 On dit qu'un anneau commutatif intègre A est *factoriel* si pour tout système de représentants $\mathcal{P}_A$ de $\mathcal{P}_A^\circ$ l'application

$$\begin{array}{rccc} (??.2.1) & A^\times \times \mathbb{N}^{(\mathcal{P}_A)} & \to & A \setminus \{0\} \\ & (u, \nu) & \to & u \displaystyle\prod_{p \in \mathcal{P}_A} p^{\nu(p)} \end{array}$$

est bijective *i.e.* pour tout $0 \neq a \in A$ il existe une unique application $v_-(a) : \mathcal{P}_A \to \mathbb{N}$ à support fini et un unique $u_a \in A^\times$ tels que $a = u_a \prod_{p \in \mathcal{P}_A} p^{v_p(a)}$ (on parle de 'la' décomposition en produit d'irréductibles de a).

On prendra garde au fait que l'élément $u_a \in A^\times$ dépend du choix du système de représentants $\mathcal{P}_A$ de $\mathcal{P}_A^\circ / \sim$ qu'on s'est fixé. Par contre, l'application $v_-(a) : \mathcal{P}_A \to \mathbb{N}$ n'en dépend pas ; si on note $\mathfrak{p} := Ap$, on peut la définir intrinsèquement par $v_\mathfrak{p}(a) = \max\{n \in \mathbb{N} \mid a \in \mathfrak{p}^n\}$. On dit que $v_p(a)$ est la multiplicité ou l'ordre de a en p ou, encore, la valuation p-adique de a.

??.3 Soit A un anneau factoriel. On prolonge les applications $v_p : A \setminus \{0\} \to \mathbb{N}$ en $v_p : A \to \overline{\mathbb{N}} := \mathbb{N} \cup \{\infty\}$ par $v_p(0) = \infty$. Avec les conventions $n + \infty = \infty$ et $n \leq \infty$, $n \in \overline{\mathbb{N}}$, il résulte immédiatement de l'unicité dans la définition d'anneaux factoriel que les applications $v_p : A \to \overline{\mathbb{N}}$, $p \in \mathcal{P}_A$ vérifient les propriétés élémentaires suivantes.

1. $v_p(ab) = v_p(a) + v_p(b)$, $a, b \in A$;

2. $v_p(a+b) \geq \min\{v_p(a), v_p(b)$ et si $v_p(a) \neq v_p(b)$, $v_p(a+b) = \min\{v_p(a), v_p(b)$, $a, b \in A$, $a \neq p$.

   En effet, écrivons $a = p^{v_p(a)}a'$, $b = p^{v_p(b)}b'$ avec $v_p(a') = v_p(b') = 0$. Si $v_p(a) > v_p(b)$, on a $a + b = p^{v_p(b)}(a'p^{v_p(a)-v_p(b)} + b')$ avec $v(a'p^{v_p(a)-v_p(b)} + b') = 0$ car $v_p(b') = 0$ et $v_p(a'p^{v_p(a)-v_p(b)}) = v_p(a) - v_p(b) > 0$. Si $v_p(a) = v_p(b) = v$, on a $v_p(a+b) = v + v_p(a'+b') \geq v$.

3. $v_p^{-1}(0) = A \setminus Ap$, $v_p^{-1}(\overline{\mathbb{N}} \setminus \{0\}) = Ap$.

On déduit de (1) et (3) que

??.4 **Lemme.** *A factoriel $\Rightarrow \mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$.*

Démonstration. On sait déjà que $\mathcal{P}_A^\dagger \subset \mathcal{P}_A^\circ$. Inversement, soit $p \in \mathcal{P}_A^\circ$. Alors pour tout $a, b \in A$, on a $ab \in Ap \Leftrightarrow v_p(a) + v_p(b) = v_p(ab) \geq 1 \Leftrightarrow v_p(a) \geq 1$ ou $v_p(b) \geq 1 \Leftrightarrow a \in Ap$ ou $b \in Ap$. □

5.2 Proposition

1. Principal $\Rightarrow$ (Noethérien intègre + $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$) $\Rightarrow$ factoriel.
2. [Utilise le Lemme de Zorn] Factoriel + $\mathrm{spm}(A) = \mathrm{Spec}(A) \setminus \{0\} \Rightarrow$ Principal.

??.1 Le lemme suivant montre que ce qui est 'profond' dans la définition d'anneau factoriel c'est surtout l'unicité de la décomposition en produit d'irréductibles. L'existence est vérifiée pour une classe d'anneaux beaucoup plus large.

Lemme. *Si A est un anneau notherien intègre, l'application*

$$\begin{array}{ccc} A^\times \times \mathbb{N}^{(\mathcal{P}_A)} & \to & A \setminus \{0\} \\ (u, \nu) & \to & u \prod_{p \in \mathcal{P}_A} p^{\nu(p)} \end{array}$$

est surjective.

Démonstration. Notons $\mathcal{F} \subset A$ l'image de $A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \to A \setminus \{0\}$. Observons que $\mathcal{F}$ est stable par produit et qu'il contient $\mathcal{P}_A^\circ$, $A^\times$. Si $a \notin \mathcal{F}$, $a \notin \mathcal{P}_A$ donc il existe $a_1, a_2 \notin A^\times$ tels que $a = a_1 a_2$. En particulier, $Aa \subsetneq Aa_1, Aa_2$. De plus, comme $\mathcal{F}$ est stable par produit, on a $a_1 \notin \mathcal{F}$ ou $a_2 \notin \mathcal{F}$. Supposons $a_1 \notin \mathcal{F}$. En itérant, $a_1 = a_{1,1}a_{1,2}$ avec $a_{1,1}, a_{1,2} \notin A^\times$ - donc $Aa_1 \subsetneq Aa_{1,1}, Aa_{1,2}$ - et $a_{1,1} \notin \mathcal{F}$ etc. on construit ainsi une suite strictement croissante $Aa \subsetneq Aa_1 \subsetneq Aa_{1,1} \subsetneq Aa_{1,1,1} \subsetneq Aa_{1,1,1,1} \subsetneq \cdots$ d'idéaux de A, ce qui contredit la noetherianité de A. □

Démonstration. 1. Principal $\Rightarrow$ (Noethérien intègre + $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$).

Soit A un anneau principal. On sait déjà que A est intègre (par définition) et noethérien (puisque tous ses idéaux sont engendrés par un seul élément). Soit $p \in A$ irréductible ; on veut montrer que Ap est premier. Il suffit de montrer qu'il est maximal. Considérons donc un idéal $Ap \subsetneq I$. Fixons $a \in I \setminus Ap$. Commme A est principal, $Ap \subsetneq Ap + Aa = Ab$ donc $p = \alpha b$ avec $\alpha \in A \setminus A^\times$ (puisque $Ap \subsetneq Ab$). Mais puisque p est irréductible, on a nécessairement $b \in A^\times$ *i.e.* $Ab = A$. En particulier $A = Ap + Aa \subset I$.

(Noethérien intègre + $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$) $\Rightarrow$ factoriel.

Par le Lemme **??**.1, on sait déjà que l'application $A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \to A \setminus \{0\}$ est surjective. Supposons que l'on ait

$$a := u \prod_{p \in \mathcal{P}_A} p^{\mu(p)} = v \prod_{p \in \mathcal{P}_A} p^{\nu(p)}$$

et que, $\nu(p) > \mu(p)$ pour un certain $p \in \mathcal{P}_A$. Comme A est intègre, on peut simplifier par $p^{\mu(p)}$; on peut donc supposer $\mu(p) = 0$ et $\nu(p) > 0$. Comme $\nu(p) > 0$, $\overline{a} = 0$ dans A/p. Comme $p \in \mathcal{P}_A^\dagger$, A/p est intègre et comme $\overline{v} \in (A/p)^\times$, il existe forcément $q \in \mathcal{P}_A$ tel que $\overline{q} = 0$ dans A/p *i.e.* $q \in Ap$, ce qui force $q = p$ puisque p, q sont irréductibles : contradiction.

2. Supposons A factoriel et $\mathrm{spm}(A) = \mathrm{Spec}(A) \setminus \{0\}$.

— Montrons d'abord que tout idéal premier est principal : si $\{0\} \subsetneq \mathfrak{p} \subsetneq A$ est premier, il contient un élément $0 \neq a \notin A^\times$. Comme a est factoriel, on peut écrire $a = u_a \prod_{p \in \mathcal{P}_A} p^{v_p(a)}$. Comme $A/\mathfrak{p}$ est intègre, il existe au moins un $p \in \mathcal{P}_A$ tel que $v_p(a) \geq 1$ et $\bar{p} = 0$ *i.e.* $p \in \mathfrak{p}$. En particulier $Ap \subset \mathfrak{p}$. Mais comme A est factoriel, $Ap \in \mathrm{Spec}(A)$ et comme $\mathrm{spm}(A) = \mathrm{Spec}(A)$ par hypothèse, $Ap = \mathfrak{p}$.

— Soit maintenant $\mathcal{E}$ l'ensemble des idéaux de A qui ne sont pas principaux. Supposons $\mathcal{E} \neq \varnothing$; comme $(\mathcal{E}, \subset)$ est un ensemble ordonné inductif, le Lemme de Zorn assure qu'il possède un élément $0 \subsetneq I \subsetneq A$ maximal pour $\subset$. Toujours par le Lemme de Zorn , I est contenu dans un idéal maximal $\mathfrak{m}$, dont on sait qu'il est principal $\mathfrak{m} = Ap$. Introduisons l'ensemble

$$J := \{a \in A \mid ap \in I\}$$

Puisque I est un idéal, $I \subset J$ et J est un idéal de A. De plus $I = Jp$. Par définition de J on a $Jp \subset I$ et, inversement, puisque $I \subset Ap$, tout $a \in I$ sécrit sous la forme $a = bp$ avec, par définition de J, $b \in J$. Si $I \subsetneq J$, par maximalité de I on aurait $J = Aa$ donc $I = Aap$, ce qui contredit $I \in \mathcal{E}$. Donc $I = J$. Ce qui signifie que la multiplication par p induit une bijection (rappelons que A est intègre) $- \cdot p : I \tilde{\to} I$. Cela contredit la factorialité de A. En effet, si $0 \neq a \in I$, on peut écrire $a = p^{v_p(a)} b$ avec $v_p(b) = 0$. Mais par définition de J, $p^{v_p(a)-1} b \in J = I = pI \Rightarrow p^{v_p(a)-2} b \in J = I = pI \Rightarrow \ldots \Rightarrow b \in J = I = pI \Rightarrow v_p(b) \geq 1$.

□

Remarque. Si on suppose A noethérien dans (2), on n'a pas besoin d'invoquer le Lemme

de Zorn.

??.2 (Contre-)Exemples. Les implications de **??** ne sont pas des équivalences. Par exemple,
— Anneau noethérien + $\mathcal{P}_A^\dagger = \mathcal{P}_A^\circ$ non principal : $k[X_1, X_2]$, où k est un corps commutatif ;
— Anneau factoriel non noethérien : $k[X_1, \dots, X_n, \dots, X_{n+1}, \dots]$, où k est un corps commutatif.

5.3 Polynômes sur les anneaux factoriels

5.3.1

Corps des fractions d'un anneau intègre. Nous allons d'abord construire le corps des fractions d'un anneau intègre. Il s'agit d'un cas particulier de localisation, construction que nous verrons en toute généralité un peu plus loin.

Soit donc A un anneau intègre. On munit le produit ensembliste $A \setminus \{0\} \times A$ de la relation $\sim$ définie par : pour tout $(s,a),(s',a') \in A \setminus \{0\} \times A$, $(s,a) \sim (s',a')$ si $s'a - sa' = 0$.

On vérifie facilement que $\sim$ est une relation d'équivalence. On note $\mathrm{Frac}(A) := A\setminus\{0\}\times A/\sim$ et

$$\begin{array}{rccc} -/- : & A \setminus \{0\} \times A & \to & \mathrm{Frac}(A) \\ & (s,a) & \to & a/s =: s^{-1}a \end{array}$$

la projection canonique. Considérons les applications $+,\cdot : (A \setminus \{0\} \times A) \times (A \setminus \{0\} \times A) \to \mathrm{Frac}(A)$ définies par

$$(s,a) + (t,b) = (ta+sb)/(st), \quad (s,a) \cdot (t,b) = (ab)/(st)$$

Si $(s,a) \sim (s',a')$, $(t,b) \sim (t',b')$ on a

$$s't'(ta+sb) - st(t'a'+s'b') = (s'a)(t't) + (ss')(t'b) - (sa')(tt') - (ss')(tb') = (s'a - sa')t't + (ss')(t'b - tb') = 0$$

$$(s't')(ab) - (st)(a'b') = (s'a)(t'b) - (sa')(tb') = 0$$

Cela montre que les applications $+,\cdot : (A \setminus \{0\} \times A) \times (A \setminus \{0\} \times A) \to \mathrm{Frac}(A)$ se factorisent en

$$\begin{array}{ccc} (A \setminus \{0\} \times A) \times (A \setminus \{0\} \times A) & \xrightarrow{+,\cdot} & \mathrm{Frac}(A) \\ \Big\downarrow{\scriptstyle -/-\times-/-} & \nearrow_{+,\cdot} & \\ \mathrm{Frac}(A) \times \mathrm{Frac}(A) & & \end{array}$$

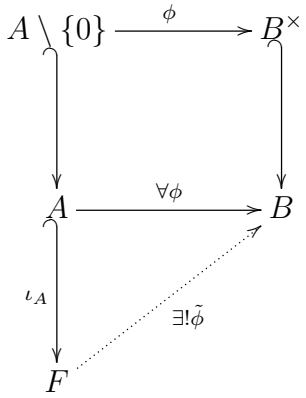
On laisse en exercice le soin de vérifier que $\mathrm{Frac}(A)$ muni des lois $+,\cdot : \mathrm{Frac}(A) \times \mathrm{Frac}(A) \to \mathrm{Frac}(A)$ ainsi définies vérifie bien les axiomes d'un anneau commutatif de zéro $0/1$ et d'unité $1/1$ et que, pour cette structure d'anneau, l'application canonique

$$\begin{array}{rccc} \iota_A : & A & \to & \mathrm{Frac}(A) \\ & a & \to & a/1 \end{array}$$

est un morphisme d'anneaux injectif. De plus, tout élément non nul $a/b \in \mathrm{Frac}(A)$ est inversible d'inverse b/a ; $\mathrm{Frac}(A)$ est donc un corps.

Lemme. (Propriété universelle du corps des fractions) *Pour tout anneau intègre A il existe un morphisme d'anneaux $\iota : A \to F$ tel que $\iota(A \setminus \{0\}) \subset F^\times$ et pour tout morphisme d'anneaux $\phi : A \to B$ tel que $\phi(A \setminus \{0\}) \subset B^\times$, il existe un unique morphisme d'anneaux $\tilde{\phi} : F \to B$ tel que $\phi = \tilde{\phi} \circ \iota$.*

Plus visuellement,



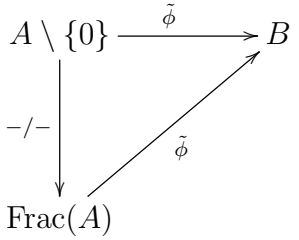
Démonstration. Montrons que $\mathrm{Frac}(A)$ muni de la structure d'anneau ci-dessus et le morphisme canonique $\iota_A : A \to \mathrm{Frac}(A)$ conviennent. Soit $\phi : A \to B$ un morphisme d'anneaux tel que $\phi(A \setminus \{0\}) \subset B^\times$. Si $\tilde{\phi} : \mathrm{Frac}(A) \to B$ existe la relation $\phi = \tilde{\phi} \circ \iota_A$ impose que $\tilde{\phi} : \mathrm{Frac}(A) \to B$ est unique puisqu'on doit nécessairement avoir

$$\tilde{\phi}(a/s) = \tilde{\phi}((a/1)(1/s)) = \tilde{\phi}(a/1)\tilde{\phi}((s/1)^{-1}) = \phi(a)\phi(s)^{-1},\ (s,a) \in A \setminus \{0\} \times A.$$

Considérons donc l'application $\begin{array}{rccc} \tilde{\phi} : & A \setminus \{0\} \times A & \to & B \\ & (s,a) & \to & \phi(s)^{-1}\phi(a). \end{array}$ Si $(s,a) \sim (s,a)'$ on a $\phi(s')\phi(a) - \phi(s)\phi(a') = \phi((s'a - sa')) = \phi(0) = 0$. Mais comme $\phi(s), \phi(s') \in B^\times$, on peut réécrire cette égalité comme

$$\tilde{\phi}(s,a) = \phi(s)^{-1}\phi(a) = \phi(s')^{-1}\phi(a') = \tilde{\phi}(s',a').$$

Cela montre que l'application $\tilde{\phi} : A \setminus \{0\} \to B$ se factorise en



Par construction $\phi = \tilde{\phi} \circ \iota_A$ et on vérifie que $\tilde{\phi} : \mathrm{Frac}(A) \to B$ est bien un morphisme d'anneaux. □

Comme d'habitude, le morphisme d'anneaux $\iota_A : A \to \mathrm{Frac}(A)$ est unique à unique isomorphisme près ; on dit que c'est le *corps des fractions* de A.

Exercice. On dit qu'un anneau A intègre de corps des fraction K est intégralement clos si

$$A = \{x \in K[X] \mid \exists\ P_x = T^d + \sum_{0 \leq n \leq d-1} a_n T^n \in A[X] \text{ tel que } P_x(x) = 0\}.$$

Montrer qu'un anneau factoriel est intégralement clos.

Exercice. On note $\mathbb{Q} := \mathrm{Frac}(\mathbb{Z})$ et si K est un corps, on note $K(X_1, \ldots, X_n) := \mathrm{Frac}(K[X_1, \ldots, X_n])$. Montrer que si A est un anneau intègre de corps des fractions K alors $\mathrm{Frac}(A[X_1, \ldots, X_n]) = K(X_1, \ldots, X_n)$.

5.3.2 Valuations p-adiques

Soit A un anneau factoriel (donc en particulier intègre) et $\iota_A : A \hookrightarrow K := \mathrm{Frac}(A)$ son corps des fractions. Pour chaque $p \in \mathcal{P}_A$, l'application

$$\begin{array}{rccc} v_p : & A \setminus \{0\} \times A & \to & \overline{\mathbb{Z}} := \mathbb{Z} \cup \{\infty\} \\ & (s, a) & \to & v_p(a) - v_p(s) \end{array}$$

vérifie $(s, a) \sim (s', a') \Rightarrow v_p(a) - v_p(s) = v_p(a') - v_p(s')$ donc se factorise *via*

$$\begin{array}{ccc} A \setminus \{0\} \times A & \xrightarrow{v_p} & \overline{\mathbb{Z}} \\ {\scriptstyle -/-}\downarrow & \nearrow_{v_p} & \\ K & & \end{array}$$

qui vérifie encore

1. $v_p(xy) = v_p(x) + v_p(y)$, $x, y \in K$;
2. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, $x, y \in K$;

De plus,

$$A^\times = \bigcap_{p \in \mathcal{P}_A} v_p^{-1}(0), \quad A = \bigcap_{p \in \mathcal{P}_A} v_p^{-1}(\overline{\mathbb{Z}}_{\geq 0}).$$

La bijection (**??**.2.1) s'étend également en une bijection

$$\begin{array}{ccc} A^\times \times \overline{\mathbb{Z}}^{(\mathcal{P}_A)} & \to & K \\ (u, \nu) & \to & u \prod_{p \in \mathcal{P}_A} p^{\nu(p)} \end{array}$$

d'inverse

$$\begin{array}{ccc} K & \to & A^\times \times \overline{\mathbb{Z}}^{(\mathcal{P}_A)} \\ x & \to & (x \prod_{p \in \mathcal{P}_A} p^{-v_p(x)}, p \to v_p(x)) \end{array}$$

5.3.3 Contenu

Supposons toujours A factoriel. Pour tout $p \in \mathcal{P}_A$ on étend $v_p : K \to \overline{\mathbb{Z}}$ en $v_p : K[X] \to \overline{\mathbb{Z}}$ par

$$v_p(P) := \min\{v_p(a_n) \mid n \geq 0\}, \quad P = \sum_{n\geq 0} a_n X^n \in K[X]$$

On définit l'application contenu $C_A : K[X] \to K$ par

$$C_A(P) = \prod_{p\in\mathcal{P}_A} p^{v_p(P)}, \quad P \in K[X].$$

Noter que comme P n'a qu'un nombre fini de coefficients non nuls, les $v_p(P)$ sont nuls sauf pour un nombre fini de $p \in \mathcal{P}_A$. On a

— $C_A(P) = 0$ si et seulement si $P = 0$;

— $C_A(P) \in A$ si et seulement si $P \in A[X]$;

— Pour tout $a \in K$, $C_A(aP) = aC_A(P)$. En particulier, pour tout $P \in K[X]$, $P = C_A(P)P_1$ avec $C_A(P_1) = 1$.

Lemme. *Pour tout $P, Q \in K[X]$ on a $C_A(PQ) = C_A(P)C_A(Q)$.*

Démonstration. Si $P \in K$ ou $Q \in K$, c'est clair. Supposons donc $P, Q \in K[X] \setminus K$. En écrivant $P = C_A(P)P_1$, $Q = C_A(Q)Q_1$ on a $C_A(PQ) = C_A(P)C_A(Q)C_A(P_1Q_1)$. Il suffit donc de montrer que si $C_A(P) = C_A(Q) = 1$ alors $C_A(PQ) = 1$. Observons que pour $F \in K[X]$ in $K[X]$ on a $C_A(F) = 1$ si et seulement si

1. $F \in A[X]$;
2. Pour tout $p \in \mathcal{P}_A$, $\overline{F} \neq 0$ in $A/pA[X]$,

où $\overline{F}$ est l'image de F par le morphisme canonique $A[X] \to A[X]/pA[X] \tilde{\to} (A/pA)[X]$. La propriété (1) est stable par produit puisque $A[X]$ est un anneau et la propriété (2) est stable par produit car $(A/pA)[X]$ est aussi un anneau intègre ; ici on utilise que p est irréductible donc premier puisque A est factoriel. □

5.3.4

Proposition. (Transfert de factorialité) *A factoriel $\Rightarrow$ $A[X]$ factoriel. De plus, les irréductible de $A[X]$ sont les irréductibles de A et les irréductible de $K[X]$ de contenu* 1.

Démonstration. L'idée est bien sûr d'exploiter que $K[X]$ est factoriel car euclidien. Fixons un système $\mathcal{P}_{K[X]}$ de représentants de $\mathcal{P}^{\circ}_{K[X]}$ de contenu 1 (il suffit de remplacer un système de représentants $\mathcal{P}$ donné par les $P/C_A(P)$, $P \in \mathcal{P}$). Notons $\mathcal{P}_{A[X]}$ l'union de $\mathcal{P}_A$ et de $\mathcal{P}_{K[X]}$. Comme A est intègre, on sait déjà que $A[X]^\times = A^\times$. On procède en deux temps.

1. Les éléments de $\mathcal{P}_{A[X]}$ sont irréductibles.

   Il suffit de montrer que les éléments de $\mathcal{P}_{A[X]}$ sont premiers.

   — Si $p \in \mathcal{P}_A$ comme A est factoriel et p est irréductible, p est premier donc A/pA est intègre. Cela implique que $(A/pA)[X]$ est intègre et on conclut par l'isomorphisme d'anneaux canoniques $A[X]/pA[X] \tilde{\to} (A/pA)[X]$.
   — Si $P \in \mathcal{P}_{K[X]}$, considérons le morphisme canonique $\phi : A[X] \hookrightarrow K[X] \twoheadrightarrow K[X]/PK[X]$. Par construction $PA[X] \subset \ker(\phi)$. Inversement, si $F \in \ker(\phi)$ alors $F = PQ$ dans $K[X]$. Par le Lemme **??**, $C_A(F) = C_A(P)C_A(Q) = C_A(Q)$ donc $C_A(Q) \in A$ *i.e.* $Q \in A[X]$. Donc $F \in PA[X]$ et le morphisme $\phi : A[X] \hookrightarrow K[X] \twoheadrightarrow K[X]/PK[X]$ se factorise en un morphisme d'anneaux injectif $A/PA[X] \hookrightarrow K[X]/PK[X]$. Comme $K[X]$ est factoriel et P est irréductible, P est premier donc $K[X]/PK[X]$ est intègre. Comme un sous-anneau d'un anneau intègre est intègre, $A[X]/PA[X]$ est donc intègre.

2. L'application canonique $A^\times \times \mathbb{N}^{(\mathcal{P}_A \cup \mathcal{P}_{K[X]})} \to A[X] \setminus \{0\}$ est bijective.

   Comme $K[X]$ est factoriel, l'application $K \setminus \{0\} \times \mathbb{N}^{(\mathcal{P}_{K[X]})} \to K[X] \setminus \{0\}$ est bijective. Elle se restreint en une application (injective !) $A \setminus \{0\} \times \mathbb{N}^{(\mathcal{P}_{K[X]})} \to A[X] \setminus \{0\}$. Cette dernière est en fait bijective car si $F = x \prod_{p \in \mathcal{P}_{K[X]}} P^{v(P)}$ (ici $x \in K \setminus \{0\}$) est dans $A[X]$, par multiplicativité du contenu, $C_A(F) = x \prod_{p \in \mathcal{P}_{K[X]}} C_A(P)^{v(P)}$ et comme par hypothèse $C_A(P) = 1$, $x \in A$. Enfin, par factorialité de A, l'application $A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \tilde{\to} A \setminus \{0\}$ est bijective donc on obtient la bijection voulue comme

$$A^\times \times \mathbb{N}^{(\mathcal{P}_A \cup \mathcal{P}_{K[X]})} \tilde{\to} A^\times \times \mathbb{N}^{(\mathcal{P}_A)} \times \mathbb{N}^{(\mathcal{P}_{K[X]})} \tilde{\to} A \setminus \{0\} \times \mathbb{N}^{(\mathcal{P}_{K[X]})} \tilde{\to} A[X] \setminus \{0\}.$$

Remarque. On a bien montré en passant que tout irréductible de $A[X]$ admet un représentant dans $\mathcal{P}_{A[X]}$: si $F \in A[X]$ est irréductible, il s'écrit de façon unique sous la forme

$$F = u \prod_{p \in \mathcal{P}_{A[X]}} p^{v_p(F)}$$

avec $u \in A^\times$ et comme F est par définition non inversible et ne peut s'écrire comme produit de deux éléments non-inversibles, on doit forcément avoir $v_p(F) = 1$ pour un certain $p \in \mathcal{P}_A \cup \mathcal{P}_{K[X]}$ et $v_q(F) = 0$, pour tout $p \neq q \in \mathcal{P}_A \cup \mathcal{P}_{K[X]}$ □

5.3.5

Corollaire. *Pour tout $n \geq 1$, A factoriel $\Rightarrow$ $A[X_1, \ldots, X_n]$ factoriel.*

Démonstration. Par induction sur n et en utilisant l'isomorphisme canonique

$$A[X_1, \ldots, X_n] \tilde{\to} A[X_1, \ldots, \ldots, X_{n-1}][X_n].$$

□

5.3.6

Exercice - critères d'irréductibilité pour les algèbres de polynômes sur les corps. Comme dans $\mathbb{Z}$, déterminer si un élément de $K[X]$ est irréductible est un problème délicat. Voici les deux critères d'irréductibilité les plus classiques pour les algèbres de polynômes.

1. **(Critère d'Eisenstein)** Soit A un anneau factoriel de corps des fractions K et $P = \sum_{n\geq 0} a_n X^n \in A[X]$. Montrer que s'il existe un irréductible p de A tel que $v_p(a_0) \leq 1$, $v_p(a_n) \geq 1$, $0 \leq n \leq \deg(P)-1$ et $v_p(a_{\deg(P)}) = 0$ alors P est irréductible dans $K[X]$.

   Application. Montrer que $P \in K[X]$ est irréductible si et seulement si $P(X+1) \in K[X]$ est irréductible. En déduire que pour tout nombre premier p, le polynôme $X^p+X^{p-1}+\cdots+X+1$ est irréductible dans $\mathbb{Q}[X]$.

2. **(Critère de réduction)** Soit A, B des anneaux intègres et L le corps des fractions de B. Soit $\phi : A \to B$ un morphisme d'anneaux. La propriété universelle de $\iota_A : A \to A[X]$ appliquée avec $A \xrightarrow{\phi} B \xhookrightarrow{\iota_B} B[X]$ donne un unique morphisme d'anneaux $\tilde{\phi} : A[X] \to B[X]$ tel que $\tilde{\phi}\circ\iota_A = \iota_B \circ \phi$ (explicitement $\tilde{\phi}(\sum_{n\geq 0} a_n X^n) = \sum_{n\geq 0} \phi(a_n)X^n$). Soit $P \in A[X]$. Montrer que si $\deg(\tilde{\phi}(P)) = \deg(P)$ et $\tilde{\phi}(P)$ est irréductible dans $L[X]$ alors P ne peut s'écrire sous la forme $P = P_1P_2$ avec $P_1, P_2 \in A[X]$ de degré ≥ 1.

   Correction. *Écrivons $P = P_1P_2$ avec $P_1, P_2 \in A[X]$ et $\deg(P_1) \leq \deg(P_2)$. On veut montrer que $P_1 \in A$. Notons que par construction $\deg(\tilde{\phi}(P)) \leq \deg(P)$. Puisque $\tilde{\phi} : A[X] \to B[X]$ est un morphisme d'anneaux, on a $\tilde{\phi}(P) = \tilde{\phi}(P_1)\tilde{\phi}(P_2)$ dans $L[X]$. Puisque $\tilde{\phi}(P) \in L[X]$ est irréductible par hypothèse, on a $\tilde{\phi}(P_1) \in K$ ou $\tilde{\phi}(P_2) \in K$. Enfin, puisque*

   $$\deg(P_1)+\deg(P_2) \geq \deg(\tilde{\phi}(P_1))+\deg(\tilde{\phi}(P_2)) = \deg(\tilde{\phi}(P)) = \deg(P) = \deg(P_1)+\deg(P_2),$$

   on a $\deg(\tilde{\phi}(P_i)) = \deg(P_i)$, $i = 1, 2$. Donc (on a supposé $\deg(P_1) \leq \deg(P_2)$) $\tilde{\phi}(P_1) \in K$, ce qui implique $\deg(P_1) = \deg(\tilde{\phi}(P_1)) = 0$ donc $P_1 \in A$ comme annoncé.

   Remarque. La terminologie 'critère de réduction' vient du fait qu'on applique en général ce critère avec les morphismes $p_I : A \twoheadrightarrow A/I$ de réduction modulo un idéal $I \subset A$. En général, on prend même $I = \mathfrak{m}$ maximal, ce qui permet de se ramener au cas de l'algèbre de polynôme $(A/\mathfrak{m})[X]$ qui est un anneau euclidien puisque $A/\mathfrak{m}$ est un corps. Typiquement, si $A = \mathbb{Z}$, on peut chercher un 'bon' nombre premier p tel que la réduction modulo p de $P \in \mathbb{Z}[X]$ soit irréductible dans $\mathbb{Z}/p[X]$. On verra dans la partie du cours sur la théorie de Galois, qu'on comprend plutôt bien les irréductibles de $\mathbb{Z}/p[X]$.

   Application. Montrer que $P = X^5 - 5X^3 - 6X - 1$ est irréductible dans $\mathbb{Q}[X]$.

   Correction. *En considérant $\phi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2$, on a $\tilde{\phi}(P) =: \overline{P} = X^5 + X^3 + 1$ dans $\mathbb{F}_2[X]$. Clairement $\overline{P}$ n'a pas de racine dans $\mathbb{F}_2$. Donc si $\overline{P}$ n'est pas irréductible, il s'écrit comme produit d'un polynôme de degré 2 et d'un polynôme de degré 3 :*

   $$\overline{P} = (X^3 + aX^2 + bX + c)(X^2 + dX + e).$$

En développant et en identifiant les coefficients, on obtient le systèmes d'équations dans $\mathbb{F}_2$

$$\begin{aligned} &d+a=0\\ &e+ad+b=1\\ &ae+bd+c=0\\ &be+cd=0\ ce=1 \end{aligned}$$

Mais dans $\mathbb{F}_2$, $d+a=0$ *implique* $a=d$. *Si* $a=d=0$, $c=0$ *: contradiction. Si* $a=d=1$, $e+b=0$, $e+b+c=0$ *donc* $c=0$ *: contradiction. Cela montre que* $\overline{P}$ *est irréductible dans* $\mathbb{F}_2[X]$. *Donc si* $P=P_1P_2$ *dans* $\mathbb{Z}[X]$ *avec* $\deg(P_1)\leq\deg(P_2)$, *on a forcément* $P_1\in\mathbb{Z}$ *(et en fait* $P_1=\pm1$ *car* $C_{\mathbb{Z}}(P)=1=C_{\mathbb{Z}}(P_1)C_{\mathbb{Z}}(P_2)=P_1C_{\mathbb{Z}}(P_2)$*). Si* $P=P_1P_2$ *dans* $\mathbb{Q}[X]$ *avec* $\deg(P_1)\leq\deg(P_2)$, *on a* $C_{\mathbb{Z}}(P_1)C_{\mathbb{Z}}(P_2)=C_{\mathbb{Z}}(P)=1$ *donc* $P=P_1P_2=\frac{P_1}{C_{\mathbb{Z}}(P_1)}\frac{P_2}{C_{\mathbb{Z}}(P_2)}$ *avec, cette fois-ci,* $\frac{P_1}{C_{\mathbb{Z}}(P_1)},\frac{P_2}{C_{\mathbb{Z}}(P_2)}\in\mathbb{Z}[T]$. *Donc* $P_1=C_{\mathbb{Z}}(P_1)\in\mathbb{Q}$. *Cela montre bien que* P *est irréductible dans* $\mathbb{Q}[X]$.

5.4 Valuations et anneaux factoriels

Soit K un corps.

5.4.1 Définitions et anneaux de valuation discrète

Définition 5.4.1.1. Une *valuation* (de rang 1) sur K est une application surjective [1] $v:K\to\overline{\mathbb{Z}}$ qui vérifie

1. $v(xy)=v(x)+v(b), x,y\in K$;
2. $v(x+y)\geq\min\{v(x),v(y)\}, x,y\in K$;
3. $v(x)=\infty\iff x=0$.

Remarque 5.4.1.1. La propriété (1) peut se réécrire en disant que $v:(K^\times,\cdot)\to(\mathbb{Z},+)$ est un morphisme de groupes.

Notons $A_v:=v^{-1}([0,\infty])\subset K$.

Définition 5.4.1.2. On dit qu'un anneau est *local* s'il possède un unique idéal maximal.

Lemme 5.4.1.1. *L'ensemble* $A_v\subset K$ *est un sous-anneau de* K, *de corps des fractions* K *et tel que* $A_v^\times=v^{-1}(0)$ *et* $\mathfrak{m}_v:=A_v\setminus A_v^\times\subset A_v$ *est un idéal. En particulier,* A_v *est local d'unique idéal maximal* $\mathfrak{m}_v$. *De plus les seuls idéaux de* A_v *sont les* $\pi^nA_v, n\in\mathbb{Z}_{\geq0}$, *où* $\pi\in A$ *est tel que* $v(\pi)=1$.

Démonstration. Montrons d'abord que $A_v\subset K$ est un sous-anneau. D'après la propriété (1) d'une valuation, $1\in A$ (utiliser $1^2=1$) et $a,b\in A_v$ implique $ab\in A$. De plus, pour tout $x\in K^\times$ la relation $(-x)^2=x^2$ et la propriété (1) d'une valuation montrent que $v(x)=v(-x)$

1. On fait cette hypothèse par commodité. Il suffit en fait de supposer que $v:K\to\overline{\mathbb{Z}}$ est non nulle ; on peut alors se ramener au cas surjectif en utilisant que tout sous groupe non-nul de $\mathbb{Z}$ est isomorphe à $\mathbb{Z}$.

ce qui, combiné à la propriété (2) d'une valuation montre que $a, b \in A_v$ implique $a - b \in A_v$. Observons également que la propriété (1) d'une valuation implique

$$A_v^\times = \{x \in K^\times \mid x, x^{-1} \in A_v\} = v^{-1}(0).$$

Les propriétés (1) (respectivement (2)) assurent également que $\mathfrak{m}_v$ est stable par multiplication par les éléments de A (respectivement par différence) donc que $\mathfrak{m}_v \subset A_v$ est un idéal. C'est automatiquement l'unique idéal maximal de A_v puisque $A_v \setminus \mathfrak{m}_v = A_v^\times$. Soit $\pi \in A$ tel que $v(\pi) = 1$ (on utilise ici la surjectivité de v). Pour un idéal $I \subset A_v$ arbitraire, notons $n := \min v(I)$. On a alors pour tout $a \in I, v(\pi^{-n}a) \geq 0$ donc $a \in A_v\pi^n$. Cela montre que $I \subset A\pi^n$. Inversement, soit $a \in I$ tel que $v(a) = n$. On a alors $v(\pi^{-n}a) = 0$ *i.e.* $A^\times a = A^\times \pi^n$ donc $A\pi^n = Aa \subset I$. Il reste à voir que K est le corps des fractions de A_v ; cela résulte du fait que tout $x \in K$ s'écrit sous la forme $x = (x\pi^{-v(x)})\pi^{v(x)}$ avec $x\pi^{-v(x)} \in A_v^\times$. □

Remarque 5.4.1.2. On dit qu'un anneau de la forme A_v est un *anneau de valuation discrète*. Ces anneaux jouent un rôle fondamental en géométrie arithmétique. Ils possèdent plusieurs caractérisations équivalentes. En voici quelques unes.

Exercice 5.4.1.1 (Difficile – *cf.* [**?**, I,§ 2])**.** Soit A un anneau commutatif. Montrer que les propriétés suivantes sont équivalentes.

1. A est un anneau de valuation discrète.
2. A est local, noethérien et son idéal maximal est principal, engendré par un élément non nilpotent.
3. A est intégralement clos et possède un unique idéal premier non nul.

5.4.2 Factorialité

Remarque 5.4.2.1. Si A est factoriel de corps des fractions $\iota_A : A \hookrightarrow K := \mathrm{Frac}(A)$, les applications $v_p : K \to \overline{\mathbb{Z}}$ pour $p \in \mathcal{P}_A$ sont donc des valuations sur K et la famille de valuations

$$\mathcal{V} := \{v_p : \mathrm{Frac}(A) \to \overline{\mathbb{Z}} \mid p \in \mathcal{P}_A\}$$

vérifie les propriétés suivantes :

— (**??**.1) pour tout $0 \neq x \in K$,

$$|\{v \in \mathcal{V} \mid v(x) \neq 0\}| < +\infty ;$$

— (**??**.2) il existe une famille d'élements $(p_v)_{v\in\mathcal{V}} \in K$ telle que $v(p_w) = \delta_{v,w}, v, w \in \mathcal{V}$;

— (**??**.3) $A = \bigcap_{v\in\mathcal{V}} A_v$.

Inversement, on a

Proposition 5.4.2.1. *Soit K un corps muni d'une famille $\mathcal{V}$ de valuations $v : K \to \overline{\mathbb{Z}}$ vérifiant les propriétés (??.1), (??.2). Alors*

$$A := \bigcap_{v\in\mathcal{V}} v^{-1}(\overline{\mathbb{N}}) \subset K$$

est un sous-anneau qui est factoriel et les p_v, $v \in \mathcal{V}$ forment un système de représentants de $\mathcal{P}_A^\circ$.

Démonstration. Observons d'abord que $A \subset K$ est un sous-anneau comme intersection de sous-anneaux (lemme **??**). La propriété (1) d'une valuation implique également que

$$A^\times = \{x \in K^\times \mid x, x^{-1} \in A\} = \bigcap_{v\in\mathcal{V}} v^{-1}(\{0\}).$$

Montrons ensuite que les $p_v, v \in \mathcal{A}$ sont irréductibles. Soit donc $v \in \mathcal{V}$. La condition $v(p_v) = 1$ assure déjà que $p \notin A^\times$. Écrivons $p_v = ab$ pour $a, b \in A$. On doit avoir $v(p_v) = 1 = v(a) + v(b)$ et $w(p_v) = 0 = w(a) + w(b)$ où $v \neq w \in \mathcal{V}$. Comme par définition de $A, w(a), w(b) \geq 0, w \in \mathcal{V}$, ces relations impliquent $v(a) = 1$ et $v(b) = 0$ ou $v(a) = 0$ et $v(b) = 1$ et $w(a) = w(b) = 0$, $v \neq w \in \mathcal{V}$. Donc $a \in A^\times$ ou $b \in A^\times$.
Soit maintenant $0 \neq a \in A$. Par (**??**.1), on peut définir

$$u_a := a \prod_{v\in\mathcal{V}} p_v^{-v(a)} \in K^\times,$$

qui vérifie par construction et la propriété (1) d'une valuation $v(u_a) = 0$, $v \in \mathcal{V}$ *i.e.* $u_a \in A^\times$. L'écriture $a = u_a \prod_{v\in\mathcal{V}} p_v^{v(a)}$ montre déjà que les p_v, $v \in \mathcal{V}$ forment un système de représentants des classes d'irréductibles de A. De plus, l'écriture $a = u_a \prod_{v\in\mathcal{V}} p_v^{v(a)}$ est unique. Si on a une écriture $a = u \prod_{v\in\mathcal{V}} p_v^{v'(a)}$ avec $u' \in A^\times$, $v'_-(a) : \mathcal{V} \to \mathbb{N} \in \mathbb{N}^{(\mathcal{V})}$, l'égalité

$$u'^{-1} u_a = \prod_{v\in\mathcal{V}} p_v^{v'(a)-v(a)} \in A^\times$$

implique, par évaluation en chacune des $v \in \mathcal{V}$ et en utilisant (**??**.2) que $v'(a) = v(a)$, $v \in \mathcal{V}$ et donc $u' = u_a$. □

5.4.3 ppcm et pgcd

Exercice 5.4.3.1. Soit A un anneau factoriel.

1. Montrer que $Aa \cap Ab$ est un idéal principal engendré par

$$\mathrm{ppcm}(a, b) := \prod_{p\in\mathcal{P}_A} p^{\max\{v_p(a), v_p(b)\}}.$$

On dit que les éléments de $A^\times$ ppcm(a, b) sont les plus petits communs multiples de a et b.

2. Montrer que l'ensemble des idéaux principaux de A qui contiennent $Aa + Ab$ admet un plus petit élément, engendré par

$$\mathrm{pgcd}(a,b) := \prod_{p \in \mathcal{P}_A} p^{\min\{v_p(a), v_p(b)\}}.$$

On dit que les éléments de $A^\times \,\mathrm{pgcd}(a,b)$ sont les plus grands communs diviseurs de a et b. Montrer sur un exemple qu'en général l'inclusion $Aa + Ab \subsetneq A\,\mathrm{pgcd}(a,b)$ est stricte.

3. Généraliser (1) et (2) à un nombre fini $a_1, \ldots, a_r$ d'éléments de A.
4. (Bézout) Supposons A principal. Montrer que $\mathrm{pgcd}(a_1, \ldots, a_r)A^\times = A^\times$ si et seulement si il existe $u_1, \ldots, u_r \in A$ tels que $u_1 a_1 + \cdots + u_r a_r = 1$.

Chapitre 6

Localisation, anneaux de fractions.

On va maintenant généraliser la construction du corps des fractions d'un anneau intègre à des anneaux non nécessairement intègre. Soit A un anneau commutatif non réduit à $\{0\}$.

6.1 Localisations

6.1.1 Parties multiplicatives

Définition 6.1.1.1. Une *partie multiplicative* de A est un sous-ensemble $S \subset A \setminus \{0\}$ stable par multiplication et contenant 1.

Exemples 6.1.1.1.
— $S := A \setminus A_{\text{tors}}$; en particulier, si A est intègre, $S := A \setminus \{0\}$;
— Pour $a \in A \setminus \sqrt{\{0\}}$, $S_a := \{a^n \mid n \in \mathbb{N}\}$;
— Pour $\mathfrak{p} \in \mathrm{Spec}(A)$, $S_{\mathfrak{p}} := A \setminus \mathfrak{p}$.

6.1.2 Définition

Soit $S \subset A \setminus \{0\}$ une partie multiplicative. On munit le produit ensembliste $S \times A$ de la relation $\sim$ définie par : pour tout $(s,a),(s',a') \in S \times A$, $(s,a) \sim (s',a')$ s'il existe $s'' \in S$ tel que $s''(s'a - sa') = 0$.

On vérifie que $\sim$ est une relation d'équivalence. On remarquera que si A est intègre, on peut, dans la définition de $\sim$, simplifier par s'' et la relation $\sim$ devient simplement $(s,a),(s',a') \in S \times A$, $(s,a) \sim (s',a')$ si $s'a - sa' = 0$. Mais on prendra garde que si A n'est pas intègre, la relation $(s,a) \sim (s',a')$ si $s'a - sa' = 0$ n'est pas transitive donc ne définit pas une relation d'équivalence.

On note $S^{-1}A := S \times A/\sim$ et

$$\begin{array}{rccc} -/- : & S \times A & \to & S^{-1}A \\ & (s,a) & \to & a/s \end{array}$$

la projection canonique.

Considérons les applications

$$\begin{array}{rccc} + & : (S\times A)\times(S\times A) & \to & S^{-1}A \\ & ((s,a),(t,b)) & \to & (ta+sb)/(st) \end{array}$$

et

$$\begin{array}{rccc} \cdot & : (S\times A)\times(S\times A) & \to & S^{-1}A \\ & ((s,a),(t,b)) & \to & (ab)/(st) \end{array}$$

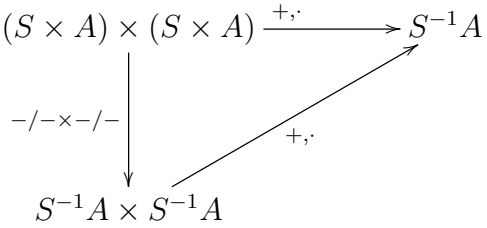
Si $(s,a)\sim(s',a')$, $(t,b)\sim(t',b')$ *i.e.* il existe $s'',t''\in S$ tels que $s''(s'a-sa')=0$, $t''(t'b-tb')=0$. Comme $s''t''\in S$ par multiplicativité, on a

$$\begin{aligned} s''t''(s't'(ta+sb)-st(t'a'+s'b')) &= s''s'a'tt't''-t'bss's''-s''t''st(t'a'+s'b') \\ &= s''sa''tt't''-tb'ss's''-s''t''st(t'a'+s'b') \\ &= 0. \end{aligned}$$

et

$$\begin{aligned} s''t''(s't'ab-sta'b') &= s''s'at''t'b-s''sa't''tb' \\ &= s''sa't''t'b-s''sa't''tb' \\ &= s''sa't''(t'b-tb') \\ &= 0. \end{aligned}$$

Cela montre que les applications $+,\cdot:(S\times A)\times(S\times A)\to S^{-1}A$ se factorisent en



On laisse en exercice le soin de vérifier que $S^{-1}A$ muni des lois $+,\cdot:S^{-1}A\times S^{-1}A\to S^{-1}A$ ainsi définies vérifie bien les axiomes d'un anneau commutatif de zéro $0/1$ et d'unité $1/1$ et que, pour cette structure d'anneau, l'application canonique

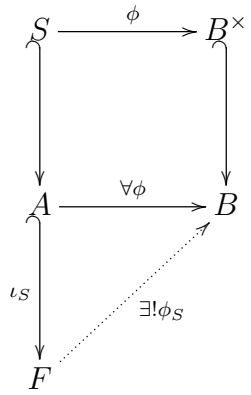
$$\begin{array}{rccc} \iota_S: & A & \to & S^{-1}A \\ & a & \to & a/1 \end{array}$$

est un morphisme d'anneaux de noyau $\ker(\iota_S)=\{a\in A\mid \exists s\in S,\ sa=0\}$. En particulier, si A est intègre (ou plus généralement si S ne contient pas d'éléments de torsion), $\iota_S:A\to S^{-1}A$ est injectif. De plus, $\iota_S(S)\subset(S^{-1}A)^\times$ puisque $s/1\cdot 1/s=s/s=1/1$.

6.1.3 Propriété universelle

Lemme 6.1.3.1 (Propriété universelle de la localisation)**.** *Pour toute partie multiplicative $S \subset A \setminus \{0\}$ il existe un anneau F et morphisme d'anneaux $\iota_S : A \to F$ tel que $\iota_S(S) \subset F^\times$ et pour tout morphisme d'anneaux $\phi : A \to B$ tel que $\phi(S) \subset B^\times$, il existe un unique morphisme d'anneaux $\phi_S : F \to B$ tel que $\phi = \phi_S \circ \iota_S$.*

Plus visuellement,



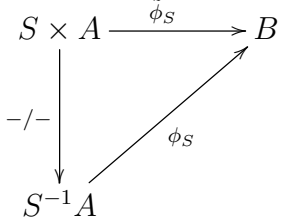
Démonstration. Montrons que $S^{-1}A$ muni de la structure d'anneau ci-dessus et le morphisme canonique $\iota_S : A \to S^{-1}A$ conviennent. Soit $\phi : A \to B$ un morphisme d'anneaux tel que $\phi(S) \subset B^\times$. Si $\phi_S : S^{-1}A \to B$ existe la relation $\phi = \phi_S \circ \iota_S$ impose que $\phi_S : S^{-1}A \to B$ est unique puisqu'on doit nécessairement avoir

$$\phi_S(a/s) = \phi_S((a/1)(1/s)) = \phi_S(a/1)\phi_S((s/1)^{-1}) = \phi(a)\phi(s)^{-1},\ (s,a) \in S \times A.$$

Considérons donc l'application $\tilde{\phi} : \begin{array}{ccc} S \times A & \to & B \\ (a,s) & \to & \phi(s)^{-1}\phi(a). \end{array}$ Si $(s,a) \sim (s',a')$ *i.e.* il existe $s'' \in S$ tels que $s''(s'a - sa') = 0$, on a $\phi(s'')(\phi(s')\phi(a) - \phi(s)\phi(a')) = \phi(s''(s'a - sa')) = \phi(0) = 0$. Mais comme $\phi(s), \phi(s'), \phi(s'') \in B^\times$, on peut réécrire cette égalité comme

$$\phi_S(s,a) = \phi(s)^{-1}\phi(a) = \phi(s')^{-1}\phi(a') = \phi_S(s',a').$$

Cela montre que l'application $\phi_S : S \times A \to B$ se factorise en

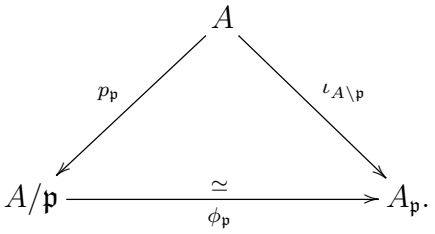


Par construction $\phi = \phi_S \circ \iota_S$ et on vérifie que $\phi_S : S^{-1}A \to B$ est bien un morphisme d'anneaux. □

Comme d'habitude, le morphisme d'anneaux $\iota_S : A \to S^{-1}A$ est unique à unique isomorphisme près et on dit que c'est 'la' localisation de A en S. Localiser A en S revient donc à inverser formellement les éléments de S.

Exercices 6.1.3.1. 1. Montrer qu'on a un isomorphisme d'anneaux canonique $S^{-1}(A[X])\tilde{\to}(S^{-1}A)[X]$.
Correction. *On va utiliser les propriétés universelles de la localisation et de l'algèbre des polynômes à une indéterminée pour construire un morphisme dans les deux sens. Considérons le morphisme d'anneaux* $\phi : A \overset{\iota_S}{\to} S^{-1}A \overset{\iota_{S^{-1}A}}{\to} (S^{-1}A)[X]$. *Par propriété universelle de* $\iota_A : A \to A[X]$, *il s'étend en un unique morphisme de* A*-algèbre* $\phi : A[X] \to (S^{-1}A)[X]$ *tel que* $\phi(X) = X$. *De plus,* $\phi(S) = \iota_{S^{-1}A}(\iota_S(S)) \subset \iota_{S^{-1}A}((S^{-1}A)^\times) = (S^{-1}A)[X]^\times$ *donc par propriété universelle de* $\iota_S : A[X] \to S^{-1}(A[X])$, $\phi : A[X] \to (S^{-1}A)[X]$ *s'étend en un unique morphisme d'anneaux* $\phi_S : S^{-1}(A[X]) \to (S^{-1}A)[X]$ *tel que* $\phi_S \circ \iota_S = \phi$. *Dans l'autre sens, considérons le morphisme d'anneaux* $\psi : A \overset{\iota_A}{\to} A[X] \overset{\iota_S}{\to} S^{-1}A([X])$. *On a* $\psi(S) = \iota_S(\iota_A(S)) \subset S^{-1}A([X])^\times$ *donc par propriété universelle de* $\iota_S : A \to S^{-1}A$ *il existe un unique morphisme d'anneaux* $\psi_S : S^{-1}A \to S^{-1}A([X])$ *tel que* $\psi_S \circ \iota_S = \psi$. *Enfin, par la propriété universelle de* $\iota_{S^{-1}A} : S^{-1}A \to S^{-1}A$, *il existe un unique morphisme de* $S^{-1}A$*-algèbre* $\psi_S : (S^{-1}A)[X] \to S^{-1}(A[X])$ *tel que* $\psi_S(X) = X$. *On vérifie immédiatement sur les constructions que* $\psi_S \circ \phi_S = Id$ *et* $\phi_S \circ \psi_S = Id$.

2. Soit p, q deux premiers distincts. Déterminer les idéaux premiers $\mathfrak{p}$ de $A := \mathbb{Z}/pq$ et déterminer dans chaque cas le localisé $(A \setminus \mathfrak{p})^{-1}A$.
Correction. *Les idéaux de* A *sont les images par la projection canonique* $\mathbb{Z} \twoheadrightarrow A$ *des idéaux de* $\mathbb{Z}$ *contenant l'idéal* $pq\mathbb{Z}$. *Or* $\mathbb{Z}$ *est principal donc ses idéaux sont tous de la forme* $n\mathbb{Z}$ *et la condition* $pq\mathbb{Z} \subset n\mathbb{Z}$ *est équivalente à* $n|pq$. *On n'a donc que quatre possibilités :* A, $\{0\}$, $\mathfrak{p} := p\mathbb{Z}/pq\mathbb{Z}$ *et* $\mathfrak{q} := q\mathbb{Z}/pq\mathbb{Z}$. *On a* $\mathbb{Z}/p\mathbb{Z}\tilde{\to}A/\mathfrak{p}$ *et* $\mathbb{Z}/q\mathbb{Z}\tilde{\to}A/\mathfrak{q}$ *donc* $spec(A) = \{\mathfrak{p}, \mathfrak{q}\}$. *J'affirme qu'on a un isomorphisme (nécessairement unique)* $\phi_\mathfrak{p} : A/\mathfrak{p}\tilde{\to}A_\mathfrak{p}$ *tel que le diagramme canonique suivant commute*



(et idem pour $\mathfrak{q}$*). On va utiliser les propriétés universelles de* $p_\mathfrak{p} : A \to A/\mathfrak{p}$ *et* $\iota_{A\setminus\mathfrak{p}} : A \to A_\mathfrak{p}$. *Par le lemme chinois* $A\tilde{\to}\mathbb{Z}/p\times\mathbb{Z}/q$ *et* $\mathfrak{p}$ *s'identifie à l'idéal engendré par* $e_2 := (0, 1)$ *; notons aussi* $e_1 := (1, 0)$. *Soit* $\iota_\mathfrak{p} : A \to A_\mathfrak{p}$ *le morphisme de localisation. On a pour tout* $a \in \mathfrak{p}$, $e_1 a = 0$. *Or, comme* $e_1 \in A \setminus \mathfrak{p}$, *on a* $\iota_\mathfrak{p}(e_1) \in A_\mathfrak{p}^\times$ *donc* $0 = \iota_\mathfrak{p}(e_1 a) = \iota_\mathfrak{p}(e_1)\iota_\mathfrak{p}(a)$ *implique en simplifiant par* $\iota_\mathfrak{p}(e_1) \in A_\mathfrak{p}^\times$, $\iota_\mathfrak{p}(a) = 0$. *Autrement dit, on vient de montrer que* $\mathfrak{p} \subset \ker(\iota_\mathfrak{p})$ *; le morphisme canonique* $\iota_\mathfrak{p} : A \to A_\mathfrak{p}$ *se factorise donc en un unique morphisme* $\phi_\mathfrak{p} : A/\mathfrak{p} \to A_\mathfrak{p}$ *tel que* $\phi_\mathfrak{p} \circ p_\mathfrak{p} = \iota_\mathfrak{p}$. *Considérons maintenant la projection canonique* $p_\mathfrak{p} : A \to A/\mathfrak{p}$. *Puisque* $\mathfrak{p}$ *est maximal, pour tout* $a \in A \setminus \mathfrak{p}$ *il existe* $b \in A$ *tel que* $ab - 1 \in \mathfrak{p}$ *donc* $1 = p_\mathfrak{p}(ab) = p_\mathfrak{p}(a)p_\mathfrak{p}(b)$. *Ce qui montre que* $p_\mathfrak{p}(A \setminus \mathfrak{p}) \subset (A/\mathfrak{p})^\times$. *Donc il existe un unique morphisme d'anneaux* $\psi_\mathfrak{p} : A_\mathfrak{p} \to A/\mathfrak{p}$ *tel que* $\psi_\mathfrak{p} \circ \iota_{A\setminus\mathfrak{p}} = p_\mathfrak{p}$. *Mais on a alors par construction* $\psi_\mathfrak{p} \circ \phi_\mathfrak{p} \circ p_\mathfrak{p} = p_\mathfrak{p}$, *ce qui par unicité dans la propriété universelle de* $p_\mathfrak{p} : A \to A/\mathfrak{p}$ *(appliquée à* $p_\mathfrak{p} : A \to A/\mathfrak{p}$ *!) impose* $\psi_\mathfrak{p} \circ \phi_\mathfrak{p} = Id$. *De même avec la localisation,* $\phi_\mathfrak{p} \circ \psi_\mathfrak{p} \circ \iota_{A\setminus\mathfrak{p}} = \iota_{A\setminus\mathfrak{p}}$ *impose* $\phi_\mathfrak{p} \circ \psi_\mathfrak{p} = Id$.

3. Montrer que si A est intègre (resp. réduit, resp. intégralement clos, resp. factoriel) alors $S^{-1}A$ l'est aussi.

Exemples 6.1.3.1. 1. On dit que $(A \setminus A_{tors})^{-1}A$ est l'anneau des fractions de A. Si A est un anneau intègre, on retrouve le corps des fractions de A. Si A n'est pas intègre, $(A \setminus A_{tors})^{-1}A$ n'est pas un corps (le vérifier sur un exemple).

2. Pour $a \in A \setminus \sqrt{\{0\}}$ on note $A_a := S_a^{-1}A$;
3. Pour $\mathfrak{p} \in \mathrm{Spec}(A)$, on note $A_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}A$. Noter que si A est intègre $\{0\} \in \mathrm{Spec}(A)$ et, dans ce cas, $A_{\{0\}} = \mathrm{Frac}(A)$.

6.1.4 Morphismes

Soit $\phi : A \to B$ un morphisme d'anneaux et $S \subset A$, $T \subset B$ des parties multiplicatives telles que $\phi(S) \subset T$. On a en particulier $\iota_T \circ \phi(S) \subset \iota_T(T) \subset (T^{-1}B)^\times$ donc par propriété universelle de $\iota_S : A \to S^{-1}A$ il existe un unique morphisme d'anneaux $\phi_{S,T} : S^{-1}A \to T^{-1}B$ tel que $\iota_T \circ \phi = \phi_{S,T} \circ \iota_S$; explicitement $\phi_{S,T}(a/s) = \phi(a)/\phi(s)$ dans $T^{-1}B$. Si $\phi : A \to B$, $\psi : B \to C$ sont des morphismes d'anneaux et $S \subset A$, $T \subset B$, $U \subset C$ des parties multiplicatives telles que $\phi(S) \subset T$, $\psi(T) \subset U$, on a $(\psi \circ \phi)_{S,U} = \psi_{T,U} \circ \phi_{S,T}$.

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ {\scriptstyle \iota_S}\downarrow & & \downarrow{\scriptstyle \iota_T} \\ S^{-1}A & \xrightarrow{\tilde{\phi}} & T^{-1}B \end{array}$$

Exemples 6.1.4.1. 1. Soit $\phi : A \to B$ un morphisme d'anneaux et $\mathfrak{q} \subset \mathrm{Spec}(B)$. On a alors $\mathfrak{p} := \phi^{-1}(\mathfrak{q}) \in \mathrm{Spec}(A)$ et $\phi(A \setminus \mathfrak{p}) \subset B \setminus \mathfrak{q}$ donc $\phi : A \to B$ induit un morphisme d'anneaux canonique $\phi_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{q}}$.

2. Si A est intègre, $\{0\} \in \mathrm{Spec}(A)$ et pour toute partie multiplicative $S \subset A \setminus \{0\}$, en appliquant ce qui précède à $\phi = \mathrm{Id} : A \to A$, $S = S$, $T = A \setminus \{0\}$, on obtient un morphisme canonique $\phi : S^{-1}A \to A_{\{0\}} =$
$Frac(A)$ dont on vérifie immédiatement qu'il est injectif.

$$\begin{array}{ccc} A & \xrightarrow{\mathrm{Id}} & A \\ {\scriptstyle \iota_S}\downarrow & & \downarrow{\scriptstyle \iota_T} \\ S^{-1}A & \xrightarrow{\tilde{\mathrm{Id}}} & \mathrm{Frac}(A) \end{array}$$

6.2 Idéaux

Soit $S \subset A$ une partie multiplicative. Pour un sous-ensemble $X \subset A$, notons

$$S^{-1}X := \left\{ \frac{a}{s} \mid a \in X,\ s \in S \right\} \subset S^{-1}A.$$

On vérifie immédiatement que si $I \subset A$ est un idéal alors $S^{-1}I \subset S^{-1}A$ est aussi un idéal. On a donc une application bien définie et croissante pour $\subset$

$$S^{-1} : (\mathcal{I}_A, \subset) \to (\mathcal{I}_{S^{-1}A}, \subset).$$

Dans l'autre direction on a l'application

$$\iota_S^{-1} : (\mathcal{I}_{S^{-1}A}, \subset) \to (\mathcal{I}_A, \subset)$$

induite par le morphisme de localisation $\iota_S : A \to S^{-1}A$.

— Pour $I \subset A$ un idéal, on a

$$\iota_S^{-1}S^{-1}I = \left\{ a \in A \mid \frac{a}{1} \in S^{-1}I \right\} = \{a \in A \mid Sa \cap I \neq \varnothing\} = \bigcup_{s \in S} (s\cdot)^{-1}I.$$

Où $s\cdot$ est l'application de multiplication par s, pour tout s dans S. En particulier, $S^{-1}I = S^{-1}A$ (si et seulement si $\iota_S^{-1}S^{-1}I = A$) si et seulement si $S \cap I \neq \varnothing$.

— Pour $I \subset S^{-1}A$ un idéal, on a

$$S^{-1}\iota_S^{-1}I = \left\{ \frac{a}{s} \in S^{-1}I \mid a \in \iota_S^{-1}I \right\} \supset I$$

et comme pour tout $a/s \in I$ on a $a/1 = (s/1)^{-1}(a/s) \in I$ donc $a \in \iota_S^{-1}I$, on a en fait $S^{-1}\iota_S^{-1}I = I$.

On a donc montré :

Lemme 6.2.0.1. *L'application $S^{-1} : (\mathcal{I}_A, \subset) \to (\mathcal{I}_{S^{-1}A}, \subset)$ est surjective, croissante pour $\subset$ et se restreint en une surjection*

$$S^{-1} : \{I \in \mathcal{I}_A \mid I \cap S = \varnothing\} \twoheadrightarrow \mathcal{I}_{S^{-1}A} \setminus \{S^{-1}A\}.$$

L'application $\iota_S^{-1} : (\mathcal{I}_{S^{-1}A}, \subset) \to (\mathcal{I}_A, \subset)$ est injective, croissante pour $\subset$ et induit une bijection

$$\iota_S^{-1} : \mathcal{I}_{S^{-1}A} \xrightarrow{\sim} \{I \in \mathcal{I}_A \mid I = \bigcup_{s \in S} (s\cdot)^{-1}I\}.$$

Lemme 6.2.0.2. *Les applications $S^{-1} : \mathcal{I}_A \to \mathcal{I}_{S^{-1}A}$ et $\iota_S^{-1} : \mathcal{I}_{S^{-1}A} \to \mathcal{I}_A$ se restreignent en des bijections inverses l'une de l'autres*

$$\mathrm{Spec}(S^{-1}A) \underset{S^{-1}}{\overset{\iota_S^{-1}}{\rightleftarrows}} \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\}$$

Démonstration. Si $\mathfrak{p} \in \mathrm{Spec}(A)$ est tel que $S \cap \mathfrak{p} = \varnothing$ alors $\mathfrak{p} = \bigcup_{s\in S}(s\cdot)^{-1}\mathfrak{p}$ (si $s \in S$, $a \in \mathfrak{p}$, $sa \in \mathfrak{p}$ implique $a \in \mathfrak{p}$) donc $\iota_S^{-1}S^{-1}\mathfrak{p} = \mathfrak{p}$. Comme on a toujours $S^{-1}\iota_S^{-1} = \mathrm{Id}$, et $\iota_S^{-1}\,\mathrm{Spec}(S^{-1}A) \subset \mathrm{Spec}(A)$, il reste seulement à montrer que si $\mathfrak{p} \in \mathrm{Spec}(A)$ est tel que $S\cap\mathfrak{p} = \varnothing$ alors $S^{-1}\mathfrak{p} \in \mathrm{Spec}(S^{-1}A)$. Soit donc $\mathfrak{p} \in \mathrm{Spec}(A)$ et $a/s, b/t \in S^{-1}A$ tels que $(ab)/(st) \in S^{-1}\mathfrak{p}$ *i.e.* il existe $p \in \mathfrak{p}$ et $u, v \in S$ tels que $v(uab - stp) = 0$ ou encore $vuab = vstp \in \mathfrak{p}$. Mais comme $\mathfrak{p} \in \mathrm{Spec}(A)$ et $vu \notin \mathfrak{p}$, on a $ab \in \mathfrak{p}$ donc $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. □

Exemple 6.2.0.1 (Corps résiduel)**.** Si $\mathfrak{p} \in \mathrm{Spec}(A)$, $A_\mathfrak{p}$ est local d'unique idéal maximal $\mathfrak{p}A_\mathfrak{p}$. Le corps $\kappa(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est appelé le corps résiduel de $\mathrm{Spec}(A)$ en $\mathfrak{p}$. Si on reprend les notations de l'Exemple **??**, le morphisme $\phi : A_\mathfrak{p} \to B_\mathfrak{q}$ envoie $\mathfrak{p}$ dans $\mathfrak{q}$ donc induit par passage au quotient un morphisme de corps — nécessairement injectif — $\kappa(\mathfrak{p}) \hookrightarrow \kappa(\mathfrak{q})$.

Corollaire 6.2.0.1. *Si A est noethérien (resp. principal) alors $S^{-1}A$ l'est aussi.*

Exercices 6.2.0.1.

1. Soit $\mathfrak{p} \in \mathrm{Spec}(A)$. Montrer qu'on a un morphisme d'anneaux canonique injectif $A/\mathfrak{p} \to \kappa(\mathfrak{p})$. Montrer que si $\mathfrak{p}$ est maximal, ce morphisme est un isomorphisme.
2. Montrer que les localisés d'un anneau principal en ses idéaux premiers sont des anneaux de valuation discrète.
3. Si $I, J \subset A$ sont des idéaux, montrer que $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$ et $S^{-1}(I + J) = S^{-1}I + S^{-1}J$.
4. Si $I \subset J$ sont des idéaux et si on note $\overline{S} \subset A/I$ l'image de S *via* la projection canonique $A \twoheadrightarrow A/I$, montrer qu'on a un isomorphisme canonique

$$S^{-1}I/S^{-1}J \xrightarrow{\sim} \overline{S}^{-1}(I/J).$$

Chapitre 7

Complétion (Hors programme)

7.1 Limites projectives

Un système projectif d'ensembles est une suite d'applications ensemblistes

$$(X_\bullet, \phi_\bullet) \quad \cdots X_{n+1} \overset{\pi_{n+1}}{\to} X_n \overset{\pi_n}{\to} X_{n-1} \overset{\pi_{n-1}}{\to} \cdots \overset{\pi_1}{\to} X_0.$$

Étant donné un système projectif $(X_\bullet, \phi_\bullet)$ d'ensembles, on note

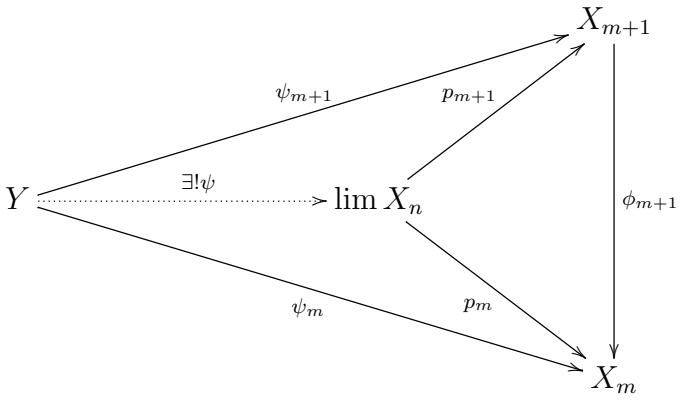
$$\lim X_n := \{\underline{x} = (x_n)_{n\geq 0} \in \prod_{n\geq 0} X_n \mid \pi_{n+1}(x_{n+1}) = x_n,\ n \geq 0\} \subset \prod_{n\geq 0} X_n$$

et pour chaque $m \geq 0$, on note $p_m : \lim X_n \to X_m$ la restriction à $\lim X_n$ de la $m$ième projection $p_m : \prod_{n\geq 0} X_n \to X_m$.

7.1.1

Lemme. (Propriété universelle de la limite projective) *Pour tout système projectif $(X_\bullet, \phi_\bullet)$ d'ensembles il existe des applications ensemblistes $p_m : P \to X_m$, $m \geq 0$ telles que pour toute famille d'applications ensemblistes $\psi_m : Y \to X_m$, $m \geq 0$ telles que $\phi_{m+1} \circ \psi_{m+1} = \psi_m$, il existe une unique application ensembliste $\psi : Y \to \lim X_n$ telle que $p_m \circ \psi = \psi_m$, $m \geq 0$.*

Plus visuellement



Démonstration. Comme d'habitude, on montre que les $p_m : \lim X_n \to X_m$, $m \geq 0$ vérifie la propriété universelle. La condition $\phi_{m+1} \circ \psi_{m+1} = \psi_m$, $m \geq 0$ impose que si $\psi : Y \to \lim X_n$ existe, elle est unique, définie par

$$\psi : Y \to \prod_{n\geq 0} X_n,\ y \to (\psi_n(y))_{n\geq 0}.$$

On vérifie ensuite immédiatement que $\psi(Y) \subset \lim X_n$ et que $p_m \circ \psi = \psi_m$, $m \geq 0$. □

Comme d'habitude, la suite d'applications $p_m : \lim X_n \to X_m$, $m \geq 0$ est unique à unique isomorphisme près et on dit que c'est 'la' limite projective de $(X_\bullet, \phi_\bullet)$.

Si les applications $\phi_{n+1} : X_{n+1} \to X_n$, $n \geq 0$ sont des morphismes de monoïdes (resp. de groupes, resp. d'anneaux), on verifie immédiatement que $\lim X_n \subset \prod_{n\geq 0} X_n$ est un sous-monoïde (resp. unesous- groupe, resp. un sous-anneaux) et que les projections $p_m : \prod_{n\geq 0} X_n \to X_m$, $m \geq 0$ sont des morphismes de monoïdes (resp. de groupes, resp. d'anneaux). Le Lemme **??** admet la variante suivante dont on laisse la preuve en exercice au lecteur.

7.1.2

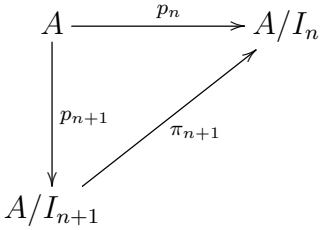
Lemme. *Pour tout système projectif $(X_\bullet, \phi_\bullet)$ de monoïdes (resp. de groupes, resp. d'anneaux), il existe des morphismes de monoïdes (resp. de groupes, resp. d'anneaux) $p_m : P \to X_m$, $m \geq 0$ telles que pour toute famille de morphismes de monoïdes (resp. de groupes, resp. d'anneaux) $\psi_m : Y \to X_m$, $m \geq 0$ telles que $\phi_{m+1} \circ \psi_{m+1} = \psi_m$, il existe un unique morphismes de monoïdes (resp. de groupes, resp. d'anneaux) $\psi : Y \to \lim X_n$ tel que $p_m \circ \psi = \psi_m$, $m \geq 0$.*

7.2

Soit A un anneau commutatif et

$$A := I_0 \supset I_1 \supset I_2 \supset \cdots \supset I_n \supset I_{n+1} \supset \cdots$$

une suite décroissante d'idéaux tels que $I_m I_n \subset I_{m+n}$. Par définition, la projection canonique $p_n : A \to A/I_n$ se factorise en



d'où un système projectif de morphismes d'anneaux

$$\cdots A/I_{n+1} \overset{\pi_{n+1}}{\to} A/I_n \overset{\pi_n}{\to} A/I_{n-1} \overset{\pi_{n-1}}{\to} \cdots \overset{\pi_1}{\to} A/I$$

et, par propriété universelle de la limite projective, un unique morphisme d'anneaux

$$c_I : A \to \widehat{A} := \lim A/I_n.$$

On note

$$\widehat{I_n} := \{\underline{a} \in \widehat{A} \mid a_m = 0,\ m \leq n\}$$

7.2.1

Toute suite décroissante d'idéaux

$$A := I_0 \supset I_1 \supset I_2 \supset \cdots \supset I_n \supset I_{n+1} \supset \cdots$$

tels que $I_m I_n \subset I_{m+n}$ munit A d'une topologie définie par les systèmes fondamentaux de voisinages $a + I_n$, $n \geq 0$. Pour cette topologie, $+, \cdot : A \times A \to A$ sont continues. Une suite de Cauchy dans A est alors une suite $\underline{a} \in A^{\mathbb{N}}$ telle que pour tout $N \geq 0$ il existe $n \geq 0$ tel que $a_{n+p} - a_n \in I_N$, $p \geq 0$. Si toute suite de Cauchy est convergente dans A, on dit que A est complet. On laisse la preuve du lemme suivant en exercice.

Lemme. *Avec les notations ci-dessus, le morphisme canonique d'anneaux $c_I : A \to \widehat{A}$ est continu (pour les topologies définies par les suites I_n, $n \geq 0$ et $\widehat{I_n}$, $n \geq 0$). De plus, $\widehat{A}$ est complet, séparé et $c_I : A \to \widehat{A}$ induit des isomorphismes canoniques $A/I_n \tilde{\to} \widehat{A}/\widehat{I_n}$.*

On dit que $c_I : A \to \widehat{A}$ est 'la' completion de A pour la topologie définie par la suites I_n, $n \geq 0$ (ce morphisme vérifie une propriété universelle que le lecteur devrait à peu près deviner mais que nous ne formulerons pas).

7.2.2

Le cas le plus fréquent d'application de la construction ci-dessus est pour $I_n = I^n$, $n \geq 0$ et $I \subset A$ un idéal. On parle alors de topologie I-adique et de completion I-adique. Voici deux exemples importants.

1. $A = \mathbb{Z}$, $I = p\mathbb{Z}$ pour p un nombre premier. Dans ce cas on note $\widehat{\mathbb{Z}} := \mathbb{Z}_p$ et on dit que $\mathbb{Z} \to \mathbb{Z}_p$ est la complétion p-adique de $\mathbb{Z}$ (ou l'anneau des entiers p-adiques). Si on munit $\mathbb{Z}$ de la valeur absolue p-adique définie par $|n| = p^{-v_p(n)}$, on peut vérifier que $\mathbb{Z} \to \mathbb{Z}_p$ est la complétion de $\mathbb{Z}$ (au sens usuel des espaces métriques) pour la distance $d_p(m, n) = |m - n|_p$).

   Remarque. On peut montrer (théorème d'Ostrowski) que les seules valeurs absolues sur $\mathbb{Q}$ sont (à équivalence près) la valeur absolue usuelle est les valeurs absolues p-adiques.

   Exercice. Montrer que si $n \in \mathbb{Z}$ est premier à p alors $c_{p\mathbb{Z}}(n) \in \mathbb{Z}_p^\times$. En déduire qu'on a un isomorphisme canonique $\widehat{\mathbb{Z}_{p\mathbb{Z}}} \tilde{\to} \mathbb{Z}_p$, où $\widehat{\mathbb{Z}_{p\mathbb{Z}}} \to \widehat{\mathbb{Z}_{p\mathbb{Z}}}$ est la complétion $p\mathbb{Z}_{p\mathbb{Z}}$-adique de $\mathbb{Z}_{p\mathbb{Z}}$.

2. Soit A un anneau commutatif intègre. $A = A[X]Z$, $I = XA[X]$. Plus précisément, reprenons les notations du paragraphe **??**. On munit $A^{\mathbb{N}}$ des lois $+, \cdot : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$ définies par

$$\underline{a} + \underline{b} = (a_n + b_n)_{n\geq 0}, \quad \underline{a} \cdot \underline{b} = (\sum_{0\leq k\leq n} a_k b_{n-k}).$$

On vérifie facilement que $(A^{\mathbb{N}}, +, \cdot)$ est un anneau de zéro la suite nulle et d'unité la suite e_0. On note cet anneau $A[[X]]$ et ses éléments $\underline{a} = (a_n)_{n\geq 0} \sum_{n\geq 0} a_n X^n$. L'inclusion naturelle $A^{(\mathbb{N})} \hookrightarrow A^{\mathbb{N}}$ induit un morphisme d'anneaux $A[X] \hookrightarrow A[[X]]$, dont on vérifie facilement que c'est la complétion de $A[X]$ par rapport à l'idéal $XA[X]$. On dit que $A[[X]]$ est l'anneau des séries formelles de A en l'indéterminée X.

Exercice. Montrer que si $P \in A[X]$ est premier à X alors $c_{XA[X]}(P) \in A[[X]]^\times$. En déduire qu'on a un isomorphisme canonique $\widehat{A[X]_{XA[X]}} \tilde{\to} A[[X]]$, où $A[X] \to A[[X]]$ est la complétion $XA[X]_{XA[X]}$-adique de $A[X]_{XA[X]}$.

Chapitre 8

Un peu de géométrie (Hors programme)

L'objectif[1] de ce chapitre est de fournir une motivation géométrique aux (nombreuses) définitions algébriques énoncées dans les chapitres précédents.

Définition 8.0.0.1 (variété algébrique affine)**.** On appelle *variété algébrique (affine)* le lieu d'annulation de r polynômes à n indéterminées $P_1, \dots, P_r \in \mathbb{C}[X_1, \dots, X_n]$. On la note $V(P_1, \dots, P_r) := \{\underline{x} \in \mathbb{C}^n : \forall i \in [\![1, \dots, n]\!], P_i(\underline{x}) = 0\}$ ou encore $V(\langle P_1, \dots, P_r\rangle) := \{\underline{x} \in \mathbb{C}^n : \forall P \in \langle P_1, \dots, P_r\rangle, P(\underline{x}) = 0\}$.

Remarque 8.0.0.1. Les deux définitions sont bien équivalentes. Le lecteur est invité à le vérifier.

On peut vouloir munir une telle variété d'une topologie. La topologie de Zariski répond à cette volonté.

Définition 8.0.0.2 (topologie de Zariski)**.** Soient $P_1, \dots, P_r \in \mathbb{C}[X_1, \dots, x_n]$. La topologie de Zariski sur la variété algébrique $V(P_1, \dots, P_r)$ est la topologie dont les fermés sont les idéaux $V(I)$ où I est un idéal de $\mathbb{C}[X_1, \dots, X_n]$ contenant l'idéal $\langle P_1, \dots, P_r\rangle$.

Nous allons maintenant donner un exemple fondamental de variétés algébriques que nous reprendrons tout au long du chapitre.

Exemple 8.0.0.1 (courbes planes dans $\mathbb{C}^2$)**.** On considère ici des variétés $C = V(P)$ où $P \in \mathbb{C}[X, Y]$.

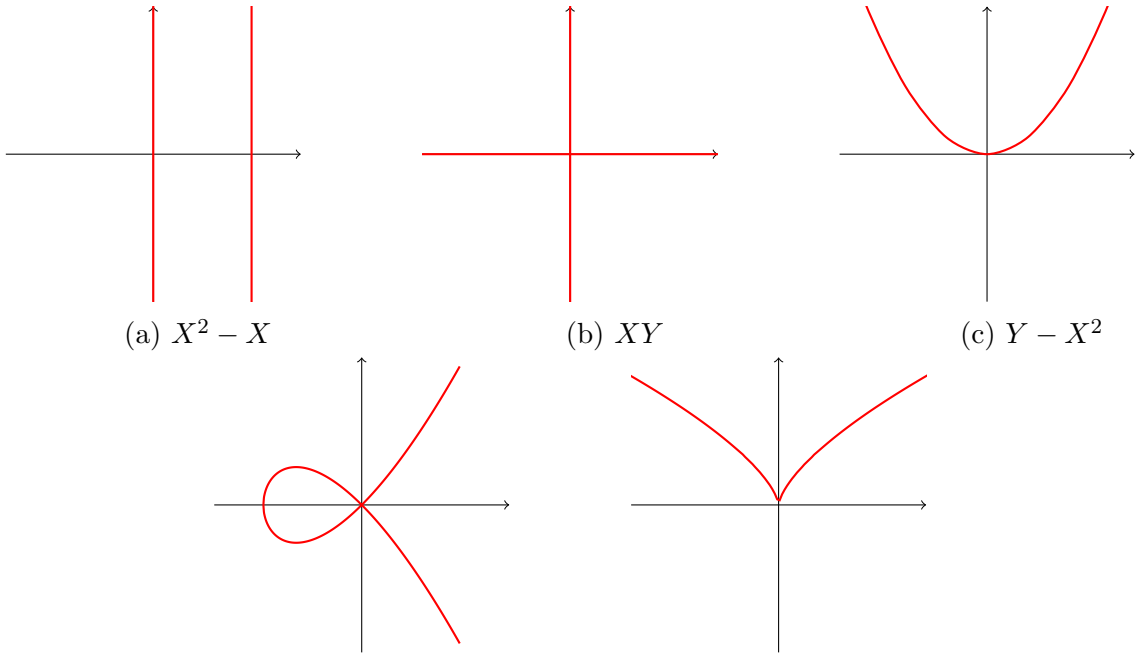
Remarque 8.0.0.2. En général, $V(P_1, \dots, P_r)$ est très difficile à comprendre. L'idée fondamentale est donc d'édudier $V := V(P_1, \dots, P_r)$ via les fonctions algébriques sur $V \subset \mathbb{C}^n$.

Définition 8.0.0.3. Soit $V := V(P_1, \dots, P_r)$ (où $P_1, \dots, P_r \in \mathbb{C}[X_1, \dots, X_r]$) une variété algébrique. On a alors un morphisme d'anneaux

$$I_v : \mathbb{C}[X_1, \dots, X_n] \to \mathbb{C}^V \tag{8.1}$$

$$F \mapsto \underline{x} \in V \mapsto \underline{F}(\underline{x}) \in \mathbb{C} \tag{8.2}$$

1. Chapitre rédigé par Quentin Dupré, à partir du cours dispensé en classe par Anna Cadoret



(a) $X^2 - X$ (b) XY (c) $Y - X^2$

(d) $Y^2 - X^2 - X^3$ (e) $X^2 - Y^3$

FIGURE 8.1 – Courbes algébriques dans $\mathbb{C}^2$

où la fonction $\underline{F}$ est polynomiale. Ce morphisme se factorise en $\mathbb{C}[X_1, \ldots, X_n]/\sqrt{\langle P_1, \ldots, P_r\rangle} \to \mathbb{C}[V]$. On dit que $\mathbb{C}[V] \subset \mathbb{C}^V$ est *l'anneau des fonctions algébriques sur* V. $\sqrt{\langle P_1, \ldots, P_r\rangle} \subset \mathrm{Ker}(I_v : \mathbb{C}[X_1, \ldots, X_n] \twoheadrightarrow \mathbb{C}[V])$ (théorème des zéros de Hilbert).

Remarque 8.0.0.3. Ce qui est remarquable en géométrie algébrique est l'existence d'une correspondance bijective (équivalence de catégories) entre deux mondes a priori distincts.

$$\begin{array}{c} \mathbb{C}\text{-algèbres de type fini} \\ \text{morphismes de } \mathbb{C}\text{-algèbres} \\ \mathbb{C}[V] \end{array} \quad \leftrightarrow \quad \begin{array}{c} \text{variétés algébriques affines} \\ \text{morphismes } F^{V_2}_{|V_1} \to V_2 \\ V \end{array}$$

On dispose ainsi d'un dictionnaire :

$$\begin{array}{c} \text{propriétés algébriques de } \mathbb{C}[V] \\ \leftrightarrow \\ \text{« preuve »} \end{array} \qquad \begin{array}{c} \text{propriétés géonétriques de } V \\ \\ \text{« intuition »} \end{array}$$

Exemple 8.0.0.2. Si l'on considère les courbes **??** et **??**, on semble y trouver en zéro les mêmes types de propriétés, alors que celles-ci paraissent différentes sur la courbe **??**. Cette intuition géométrique et visuelle se montre algébriquement.

Insérer ici le dictionnaire sur la topologie

Exemple 8.0.0.3. Courbe ?? $\mathbb{C}[V] = \mathbb{C}[X,Y]/(X^2-X) \simeq \mathbb{C}[X,Y]/(X) \times \mathbb{C}[X,Y]/(X-1)$ d'après le théorème chinois. V n'est pas connexe : il y a deux composantes connexes $V(X)$ et $V(X-1)$.

Courbe ?? $\mathbb{C}[V] = \mathbb{C}[X,Y]/(XY)$ n'est pas intègre car $\overline{XY} = 0$ alors que $\overline{X} \neq 0$ et $\overline{Y} \neq 0$. Deux idéaux premiers minimaux $\langle X\rangle, \langle Y\rangle$ qui correspondent aux deux composantes irréductibles $V(X)$ et $V(Y)$.
En revanche, V est connexe. $\mathbb{C}[X,Y]/(XY) \not\simeq A_1 \times A_2$ car il n'existe pas d'idempotent.
$e_1 = (1,0), e_2 = (0,1)$
$e_1^2 = e_1, e_2^2 = e_2, e_1e_2 = 0, e_1, e_2 \notin \{0,1\}$
Soit $\overline{P} \in \mathbb{C}[X,Y]/(XY)$ tel que $\overline{P} \neq \overline{0}, \overline{1}$ et $\overline{P}^2 = \overline{P}$. Alors $\overline{P}^2 - \overline{P} = \overline{0}$ donc $XY \mid P(P-1)$.
En utilisant la factorialité de $\mathbb{C}[X,Y]$, on a $X \mid P$ ou $X \mid P-1$ et $Y \mid P$ ou $Y \mid P-1$.
Les différentes possibilités sont alors :

- $X, Y \mid P \implies XY \mid P \implies \overline{P} = \overline{0}$,
- $X, Y \mid P-1 \implies XY \mid P-1 \implies \overline{P} = \overline{1}$,
- $(X \mid P, Y \mid P-1) \implies P = UX = 1+VY$ contradictoire avec le choix d'irréductibles (on peut aussi évaluer ce polynôme en $(0,0)$ pour obtenir une contradiction).

Dans tous les cas, on obtient une contradiction. Un tel $\overline{P}$ n'existe donc pas.

Courbes ??, ?? et ?? $Y - X^2, Y^2 - X^2 - X^3$ et $X^2 - Y^3$ sont irréductibles dans $\mathbb{C}[X,Y]$ donc premiers par factorialité de l'anneau, V est par conséquent irréductible et $\mathbb{C}[V]$ est intègre.

Ici le dictionnaire sur les singularités.

Exemple 8.0.0.4.

Remarque 8.0.0.4. Pour étudier plus finement les singularités, il faut en quelque sorte zoomer sur celles-ci. Algébriquement, cela correspond à localiser ou à compléter. Pour étudier V en $(0,0)$, on localise $A/I = \mathbb{C}[V]$ en $\mathfrak{m}/I = \langle \overline{X}, \overline{Y}\rangle$ où $\mathfrak{m}/I$ est un idéal maximal, $A = \mathbb{C}[X_1, \ldots, X_n], I = \langle P_1, \ldots, P_r\rangle$ et $\mathfrak{m} = \langle X, Y\rangle$.

Définition 8.0.0.4. Une bonne définition de « être lisse » pour une courbe algébrique est :
V est lisse $\iff \forall m \in \mathrm{spm}(\mathbb{C}[V])$, $\mathbb{C}[V]_m$ est un anneau de valuation discrète.

Pour la complétion, on a :

$$\mathbb{C}[V]_m \quad \leftrightarrow \quad \text{Complétion par la topologie m-adique } \widehat{\mathbb{C}[V]_m}$$

Deuxième partie

Modules sur un anneaux

On rappelle que sauf mention explicite du contraire tous les anneaux sont commutatifs.

Chapitre 9

Premières définitions et constructions

9.1 Définitions

Définition 9.1.0.1. Soit A un anneau, un A-module (à gauche) est un couple $((M,+),\cdot)$ formé d'un groupe abélien $(M,+)$ (on notera 0 son élément neutre et $-m$ l'inverse d'un élément $m \in M$)) et d'une application $\cdot : A \times M \to M$ - appelée la multiplication extérieure - vérifiant les axiomes suivants :

1. $a \cdot (m+n) = a \cdot m + a \cdot n$, $a \in A$, $m, n \in M$;
2. $(a+b) \cdot m = a \cdot m + b \cdot m$, $a, b \in A$, $m \in M$;
3. $(a \cdot b) \cdot m = a \cdot (b \cdot m)$, $a, b \in A$, $m \in M$;
4. $1 \cdot m = m$, $m \in M$.

De façon équivalente, l'application

$$\begin{aligned} A &\to \mathrm{End}_{Grp}(M) \\ a &\mapsto a.\mathrm{Id} \end{aligned}$$

est un morphisme d'anneaux.

Définition 9.1.0.2. Étant donnés deux A-modules M, N, un morphisme de A-modules est un morphisme de groupes $f : (M,+) \to (N,+)$ A-linéaire *i.e* qui vérifie :

$$f(a \cdot m) = a \cdot f(m),\ a \in A,\ m \in M.$$

On remarquera que l'application identité $\mathrm{Id} : M \to M$ est un morphisme de A-modules et que si $f : M \to N$ et $g : N \to P$ sont des morphismes de A-modules alors $g \circ f : M \to P$ est un morphisme de A-modules.

Définition 9.1.0.3. On notera $\mathrm{Hom}_A(M,N)$ l'ensemble des morphismes de A-modules $\phi : M \to N$ et, si $M = N$, $\mathrm{End}_A(M) := \mathrm{Hom}_A(M,M)$.

On dit qu'un morphisme de A-modules $f : M \to N$ est injectif, (resp. surjectif, resp. un isomorphisme) si l'application d'ensemble sous-jacente est injective (resp. surjective, resp. bijective). On vérifie que si $f : M \to N$ est un isomorphisme de A-modules l'application inverse $f^{-1} : N \to M$ est automatiquement un morphisme de A-modules.

9.1.1 Exemples

— Si $A = \mathbb{Z}$, les $\mathbb{Z}$-modules sont les groupes abéliens.

— Si $A = k$ est un corps commutatif, les k-modules sont les k-espaces vectoriels.

— On peut toujours voir un anneau A comme un A-module sur lui-même en prenant pour multiplication extérieure le produit $\cdot : A \times A \to A$. Cet exemple qui semble tautologique est en fait fondamental ! On va s'en rendre compte rapidement. Plus généralement, tout idéal $I \subset A$ muni de $\cdot : A \times I \to I$ induite par le produit de A est un A-module. On dit alors que A est *le* A-module régulier.
— Si N, N sont deux A-modules, $\mathrm{Hom}_A(M, N)$ est naturellement muni d'une structure de A-module pour les lois $(f + g)(m) = f(m) + g(m)$, $(a \cdot f)(m) = a \cdot (f(m))$.
— Si $\phi : A \to B$ est un morphisme d'anneaux tout B-module M est naturellement un A-module pour la multiplication extérieure $A \times M \to M$, $(a, n) \to \phi(a) \cdot n$. On notera $\phi^* M$ ou $M|_A$ lorsqu'il n'y a pas d'ambiguité sur $\phi : A \to B$ le A-module ainsi obtenu à partir du B-module N. On notera que tout morphisme de B-modules $f : M \to N$ est automatiquement un morphisme de A-modules $f|_A = f : M|_A \to N_A$. En particulier, une structure de A-algèbre $\phi : A \to B$ sur un anneau B détermine une structure de A-module $\phi^* B$ sur B. Inversement, une structure de A-module $\cdot : A \times B \to B$ sur le groupe abélien sous-jacent $(B, +)$ d'un anneau B détermine une structure de A-algèbre $\phi : A \to B$ sur B en posant $\phi(a) = a \cdot 1_B$. En particulier, si M est un A-module, $\mathrm{End}_A(M)$ est naturellement muni d'une structure de A-algèbre.
— Soit A un anneau commutatif. Par la propriété universelle de $\iota_A : A \to A[X_1, \ldots, X_n]$, la donnée d'un $A[X_1, \ldots, X_1]$-module est équivalente à la donnée d'un couple $(M, \underline{\phi})$, où M est un A-module et $\underline{\phi} := (\phi_1, \ldots, \phi_n)$ est un n-uplet d'endomorphismes A-linéaires de M qui commutent deux à deux. Par exemple, si V est un k-espace vectoriel de dimension finie, et $u \in \mathrm{End}_k(V)$, on peut munir V de la structure V_u de $k[X]$-module définie par $P(X) \cdot v = P(u)(v)$. Si $u, u' \in \mathrm{End}_k(V)$, on a

$$\mathrm{Hom}_{k[X]}(V_u, V_{u'}) = \{\varphi : V \to V \mid \varphi \circ u = u' \circ \varphi\}.$$

Un certain nombre de résultats d'algèbre linéaire s'interprètent (et deviennent bien plus naturels !) en termes de $k[X]$-modules.

Définition 9.1.1.1 (Sous-module)**.** Si M est un A-module, un sous A-module de M est un sous-ensemble $M' \subset M$ tel que $am' + bn' \in M'$, $a, b \in A$, $m', n' \in M'$.

Exemple 9.1.1.1. — Les sous-A-modules du A-module régulier A sont les idéaux de A.

— Si $f : M \to N$ est un morphisme de A-module et $M' \subset M$ (resp. $N' \subset N$) est un sous-A-module alors $f(M') \subset N$ (resp. $f^{-1}(N') \subset M$) est un sous-A-module. En particulier, $\mathrm{im}(f) \subset N$ et $\ker(f) \subset M$ sont des sous-A-modules.

— Si $I \subset A$ est un idéal et M un A-module,

$$IM := \{ \sum_{m \in M} a(m)m \mid a : M \to I \text{ à support fini} \} \subset M$$

est un sous-A-module.

9.2 Produits et sommes directes

Soit M_i, $i \in I$ une famille de A-modules.

On munit le groupe abélien produit $\prod_{i \in I} M_i$ de la structure de A-module

$$\begin{array}{ccc} A \times \prod_{i \in I} M_i & \to & \prod_{i \in I} M_i \\ (a, \underline{m} = (m_i)_{i \in I}) & \to & a \cdot \underline{m} = (a \cdot m_i)_{i \in I}. \end{array}$$

Avec cette structure de A-module, les projections canoniques $p_j : \prod_{i \in I} M_i \to M_j$, $j \in I$ deviennent des morphismes de A-modules.

Définition 9.2.0.1 (Somme directe)**.** On appelle somme directe de la famille $M_i, i \in I$ et l'on note $\bigoplus_{i \in I} M_i \subset \prod_{i \in I} M_i$ le sous A-module des $\underline{m} = (m_i)_{i \in I}$ tels que

$$|\{i \in I \mid m_i \neq 0\}| < +\infty.$$

Les injections canoniques $\iota_j : M_j \hookrightarrow \bigoplus_{i \in I} M_i$, $j \in I$ sont des morphismes de A-modules. Si I est fini, on a tautologiquement $\bigoplus_{i \in I} M_i = \prod_{i \in I} M_i$.

Lemme 9.2.0.1 (Propriété universelle du produit et de la somme directe)**.** *Pour toute famille M_i, $i \in I$ de A-modules, il existe des morphismes de A-modules $p_i : \Pi \to M_i$, $i \in I$ et $\iota_i : M_i \to \Sigma$, $i \in I$ tels que*

1. *Pour toute famille de morphismes de A-modules $f_i : M \to M_i$, $i \in I$ il existe un unique morphisme de A-modules $f : M \to \Pi$ tel que $p_i \circ f = f_i$, $i \in I$.*
2. *Pour toute famille de morphismes de A-modules $f_i : M_i \to M$, $i \in I$ il existe un unique morphisme de A-modules $f : \Sigma \to M$ tel que $f \circ \iota_i = f_i$, $i \in I$.*

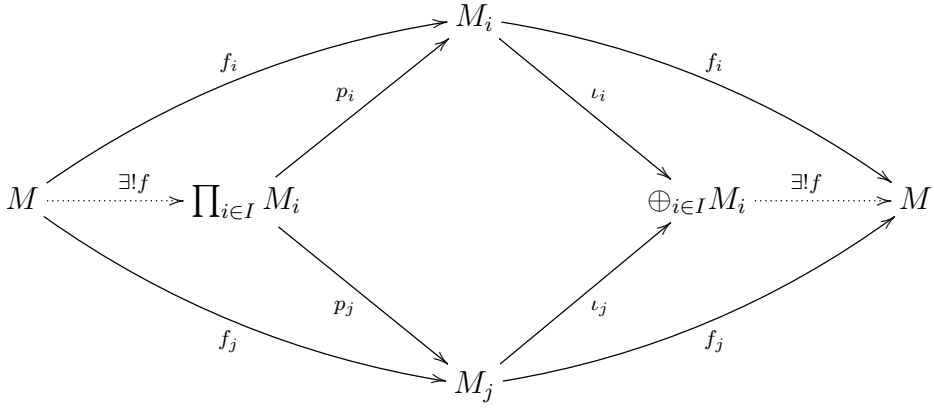
Démonstration. On vérifie comme d'habitude que les morphismes de A-modules $p_j : \prod_{i \in I} M_i \to M_j$, $j \in I$ et $\iota_j : M_j \hookrightarrow \bigoplus_{i \in I} M_i$, $j \in I$ construits ci-dessus conviennent. □

Remarque 9.2.0.1. On peut aussi réécrire le lemme en disant que, pour tout A-module M les morphismes canoniques

$$\begin{array}{ccc} \mathrm{Hom}_A(M, \prod_{i \in I} M_i) & \to & \prod_{i \in I} \mathrm{Hom}_A(M, M_i) \\ f & \mapsto & (p_i \circ f)_{i \in I} \end{array}$$

$$\begin{aligned}\mathrm{Hom}_A(\oplus_{i\in I} M_i, M) &\to \prod_{i\in I} \mathrm{Hom}_A(, M_i M)\\ f &\mapsto (f\circ \iota_i)_{i\in I}\end{aligned}$$

sont des isomorphismes ou encore, plus visuellement :



Comme d'habitude, le produit $p_j : \prod_{i\in I} M_i \to M_j$, $j \in I$ et la somme directe $\iota_j : M_j \hookrightarrow \bigoplus_{i\in I} M_i$, $j \in I$ sont uniques à *unique* isomorphisme près.

Remarque 9.2.0.2. Si $M_i = M$ pour tout $i \in I$, on notera $M^I := \prod_{i\in I} M_i$ et $M^{(I)} := \oplus_{i\in I} M_i$. Par construction, on a des isomorphismes canoniques

$$\mathrm{Hom}(A^{(I)}, M) \simeq \prod_{i\in I} \mathrm{Hom}(A, M) \simeq M^I$$

et on dit que $A^{(I)}$ est le *A-module libre de base I*.

Soit $f_i : M_i \to N_i$, $i \in I$ une famille de morphismes de A-modules. En appliquant la propriété universelle des $p_j : \prod_{i\in I} N_i \to N_j$, $j \in I$ à la famille de morphismes de A-modules

$$\prod_{i\in I} M_i \xrightarrow{p_j} M_j \xrightarrow{f_j} N_j,\ j \in I$$

on obtient un unique morphisme de A-modules $f := \prod_{i\in I} f_i : \prod_{i\in I} M_i \to \prod_{i\in I} N_i$ tel que $p_i \circ f = f \circ p_i$, $i \in I$. De même, en appliquant la propriété universelle des $\iota_j : M_j \to \oplus_{i\in I} M_i$, $j \in I$ à la famille de morphismes de A-modules

$$M_j \xrightarrow{f_j} N_j \xrightarrow{\iota_j} \oplus_{i\in I} M_i,\ j \in I$$

on obtient un unique morphisme de A-modules $f := \oplus_{i\in I} f_i : \oplus_{i\in I} M_i \to \oplus_{i\in I} N_i$ tel que $f \circ \iota_i = \iota_i \circ f$, $i \in I$.

9.3 Sous-module engendré par une partie, sommes

Si $M_i \subset M$, $i \in I$ est une famille de sous A-modules de M, on vérifie immédiatement que l'intersection

$$\bigcap_{i\in I} M_i \subset M$$

est encore un sous-A-module de M.

Définition 9.3.0.1. Si $X \subset M$ est un sous-ensemble, on note $\langle X\rangle$ l'intersection de tous les sous A-modules $M' \subset M$ contenant X. D'après ce qui précède, c'est encore un sous A-module de M et, par construction, c'est le plus petit sous A-module de M contenant X. On dit que $\langle X\rangle$ est le *sous A-module* engendré par X.

Remarque 9.3.0.1. On vérifie qu'il coincide avec l'ensemble des éléments de la forme $\sum_{x\in X} a(x)x$, où $a : X \to A$ est une application à support fini.

La propriété universelle de $\iota_x : A \hookrightarrow A^{(X)}$, $x \in X$ appliquée aux morphismes de A-modules $-x : A \to M,\ a \to ax$, $x \in X$ nous donne un unique morphisme de A-modules $p_X : A^{(X)} \to M$ tel que $p_X \circ \iota_x(a) = ax$, $x \in X$. On vérifie immédiatement que les propriétés suivantes sont équivalentes :

1. $M = \langle X\rangle$;
2. Le morphsime de A-modules $p : A^{(X)} \to M$ est surjectif.

On dit alors que X est un système de générateurs de M comme A-modules (ou que M est engendré par X comme A-module). Si on peut prendre X fini, on dit que M est un A-module *de type fini*.

Exemple 9.3.0.1.
— Si A est un corps, les A-modules de type fini sont les A-espaces vectoriels de dimension finie.
— Si A est noethérien, tout sous A-module de A (c'est à dire les idéaux de l'anneau A) est de type fini.
— Si $\mathrm{card}(X) < +\infty$, $A^{(X)}$ est un A-module de type fini, engendré par les $e_x := (\delta_{xy})_{y\in X}$.

Si $M_i \subset M$, $i \in I$ est une famille de sous A-modules de M, on note

$$\sum_{i\in I} M_i = \left\langle \bigcup_{i\in I} M_i \right\rangle = \left\{ \sum_{i\in I} m_i : m_I \in M_I, \mathrm{card}\{i \in I : m_i \neq 0\} < +\infty \right\} \subset M.$$

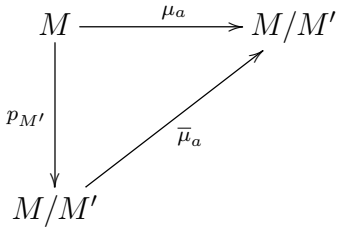
Là encore la propriété universelle de $\iota_i : M_i \hookrightarrow \oplus_{i\in I} M_i$, $i \in I$ appliquée aux morphismes de A-modules $M_i \subset \sum_{i\in I} M_i$ (inclusion), $i \in I$ nous donne un unique morphisme de A-modules - automatiquement surjectif - $p : \oplus_{i\in I} M_i \twoheadrightarrow \sum_{i\in I} M_i (\subset M)$ tel que $p \circ \iota_i(m_i) = m_i$, $m_i \in M_i$, $i \in I$.

9.4 Quotients

Soit $M' \subset M$ un sous A-module. C'est en particulier un sous groupe abélien et on dispose donc du quotient $p_{M'} : M \to M/M'$, $m \to p_{M'}(m) =: \overline{m}$ comme groupe abélien . On peut munir M/M' d'une structure de A-module comme suit. Pour tout $a \in A$, l'application

$$\begin{array}{rccc} \mu_a : & M & \to & M/M' \\ & m & \to & \overline{a \cdot m} \end{array}$$

est un morphisme de groupes abéliens tel que $M' \subset \ker(\mu_a)$; il se factorise donc en



On pose alors

$$\begin{array}{rcl} A \times M/M' & \to & M/M' \\ (a, \overline{m}) & \to & a \cdot \overline{m} := \overline{\mu}_a(m)(= \overline{a \cdot m}). \end{array}$$

On vérifie immédiatement que cela définit bien une structure de A-module sur M/M' et que c'est l'unique structure de A-module sur M/M' qui fait de $p_{M'} : M \to M/M'$ un morphisme de A-modules. De plus,

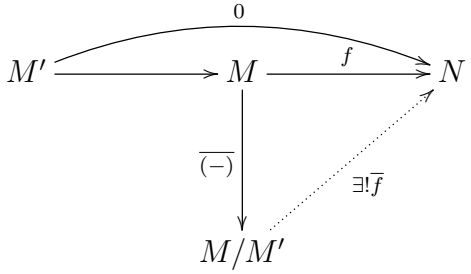
Lemme 9.4.0.1 (Propriété universelle du quotient)**.** *Pour tout sous-A-module $M' \subset M$ il existe un morphisme de A-modules $p : M \to Q$ tel que pour tout morphisme de A-modules $f : M \to N$ tels que $M' \subset \ker(f)$, il existe unique morphisme de A-modules $\overline{f} : Q \to N'$ tel que $\overline{f} \circ p = f$.*

Démonstration. On vérifie comme d'habitude que le morphisme de A-modules $p'_M : M \twoheadrightarrow M/M'$ construit ci-dessus convient. □

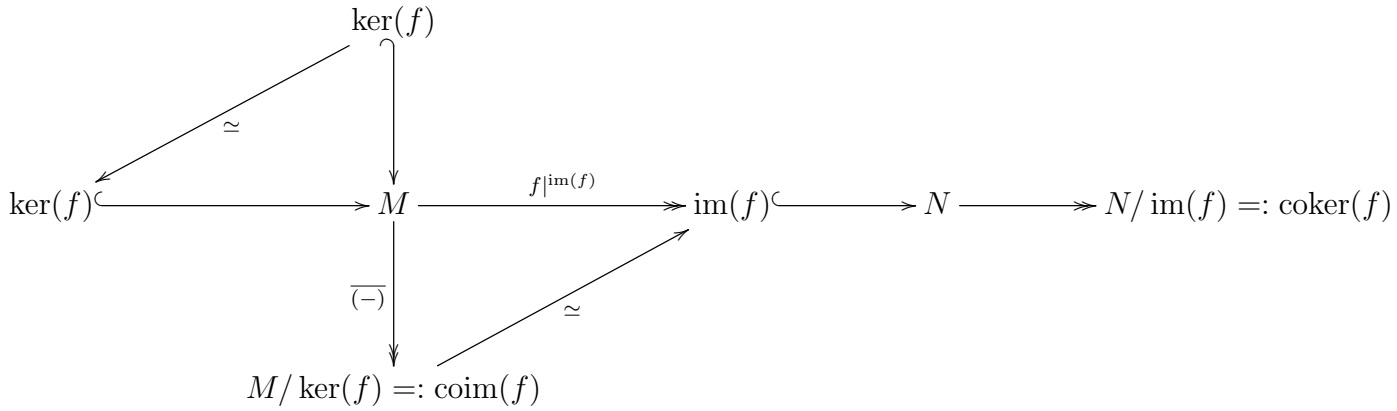
Remarque 9.4.0.1. On peut aussi réécrire **??** en disant que, pour tout A-module N le morphisme canonique

$$\mathrm{Hom}_A(M/M', N) \to \{M \xrightarrow{f} N \mid M' \subset \ker(f)\},\ \overline{f} \to \overline{f} \circ \overline{(-)}$$

est un isomorphisme ou encore, plus visuellement :



On observera que $M' = \ker(\overline{(-)})$ et $M/M' = \mathrm{im}(\overline{(-)})$. Inversement, si $f : M \to N$ est un morphisme de A-modules, on a un diagramme commutatif canonique de morphismes de A-modules



Définition 9.4.0.1 (Coimage, conoyau)**.** On a donc une correspondance bijective entre sous A-modules et noyaux de morphismes de A-modules d'une part et A-modules quotients et images de morphismes de A-modules d'autre part. Même si les A-modules $\mathrm{im}(f)$ et $M/\ker(f)$ sont isomorphes, on notera parfois $\mathrm{coim}(f) := M/\ker(f)$ (coimage). On note $\mathrm{coker}(f) := M'/\mathrm{im}(f)$ (conoyaux).

9.4.1 Suites exactes, lemme du serpent, lemme des cinq

Définition 9.4.1.1. On dit qu'une suite de morphismes de A-modules

$$\cdots M_{n-1} \overset{u_{n-1}}{\to} M_n \overset{u_n}{\to} M_{n+1} \overset{u_{n+1}}{\to} \cdots$$

est exacte si $\mathrm{im}(u_n) = \ker(u_{n+1})$ pour tout n.

Définition 9.4.1.2. Une suite exacte courte est une suite exacte de la forme :

$$0 \to M' \overset{u}{\to} M \overset{v}{\to} M'' \to 0.$$

Autrement dit $\ker(v) = \mathrm{im}(u)$; $\ker(u) = \{0\}$, *i.e.* u est injectif et $\mathrm{im}(v) = M''$, *i.e.* v est surjectif.

Remarque 9.4.1.1. La notion de suite exacte est au coeur de l'étude de la structure des A-modules. La raison première est que c'est l'outil qui permet de 'dévisser' un A-module compliqué (M) en deux A-modules plus simples (M' et M'').
En général si $M' \subset M$ est un sous-module de M il n'existe pas forcément un sous A-module $M'' \subset M$ tel que $M \simeq M' \oplus M''$. Plus précisément :

Lemme 9.4.1.1. *Soit*

$$0 \to M' \overset{u}{\to} M \overset{v}{\to} M'' \to 0$$

une suite exacte courte de A-modules. Les propriétés suivantes sont équivalentes :

1. *il existe un morphisme de A-modules $s : M'' \to M$ tel que $v \circ s = \mathrm{Id}_{M''}$;*

2. *il existe un morphisme de A-modules $r : M \to M'$ tel que $r \circ u = \mathrm{Id}_{M'}$;*
3. *il existe un isomorphisme de A modules $f : M \tilde{\to} M' \oplus M''$ tel que $\iota_{M'} = f \circ u$ et $p_{M''} \circ f = v$.*

Définition 9.4.1.3. On dit qu'une suite exacte courte vérifiant les conditions équivalentes ci-dessus est *scindée*.

Démonstration. On peut par exemple montrer (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2) : Si $s : M'' \to M$ est un morphisme de A-modules tel que $vs = \mathrm{Id}_{M''}$ on vérifie que le morphisme de A-modules $\mathrm{Id} - sv : M \to M$ a son image contenue dans $\ker(v) = u(M')$ et que $t := (u|^{u(M')})^{-1} \circ (\mathrm{Id} - sv) : M \to M'$ vérifie bien $tu = \mathrm{Id}_{M'}$.

(2) $\Rightarrow$ (3) : Si $r : M \to M'$ est un morphisme de A-modules tel que $r \circ u = \mathrm{Id}_{M'}$, on peut considérer $f := s \oplus v : M \to M' \oplus M''$. Par construction, $p_{M''} \circ f = v$ et $f \circ u(s(m)) = s(m) = \iota_{M'}(s(m))$ donc, comme $s : M \to M'$ est surjective, $f \circ u = \iota_{M'}$. Enfin, $f : M \to M' \oplus M''$ est un isomorphisme. Il est injectif car si $f(m) = 0$ alors $v(m) = 0$ *i.e.* $m \in \ker(v) = u(M')$ donc $m = u(m')$ et $m' = r \circ u(m') = 0$. Donc, en fait $m = 0$. Il est surjectif car pour tout $m' \in M'$, $m'' \in M''$, on peut écrire $m'' = v(m) = v(m - ur(m) + u(m'))$ et $m' = ru(m') = s(m - us(m) + u(m'))$.

(3) $\Rightarrow$ (1) : Si $f : M \tilde{\to} M' \oplus M''$ est un isomorphisme de A-modules tel que $p_{M''} \circ f = v$ et $f \circ u = \iota_{M'}$, on peut considérer $s := f^{-1} \circ \iota_{M''} : M'' \to M$. Par construction $vs(m) = vf^{-1}\iota_{M''} = p_{M''}\iota_{M''} = \mathrm{Id}_{M''}$. □

??.2

Exercices 9.4.1.1. 1. Montrer que, si $n \geq 2$ est un entier, la suite exacte courte de $\mathbb{Z}$-modules $0 \to \mathbb{Z} \xrightarrow{n\cdot} \mathbb{Z} \to \mathbb{Z}/n \to 0$ n'est pas scindée.

2. On considère les structure de $\mathbb{Z}[X]$-modules suivantes sur $\mathbb{Z}^2$

1. $X \cdot (a, b) = (a + b, b)$ et la suite exacte courte $0 \to \mathbb{Z} \xrightarrow{a \to (a,0)} \mathbb{Z}^2 \to \mathbb{Z} \to 0$.
2. $X \cdot (a, b) = (b, a)$ et la suite exacte courte $0 \to \mathbb{Z} \xrightarrow{a \to (a,a)} \mathbb{Z}^2 \to \mathbb{Z} \to 0$

Déterminer si ces suites exactes courtes sont scindées. Même question si l'on remplace $\mathbb{Z}$ par $\mathbb{Q}$

??.3 **Exercice.** (Lemme du serpent)

1. Soit

$$\begin{array}{ccc} M' & \xrightarrow{u'} & M \\ \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} \\ N' & \xrightarrow[v']{} & N \end{array}$$

un diagramme commutatif de morphismes de A-modules. Montrer que $u' : M' \to M$ induit un morphisme canonique $\ker(\alpha') \to \ker(\alpha)$ et que $v' : N' \to N$ induit un morphisme canonique $\operatorname{coker}(\alpha') \to \operatorname{coker}(\alpha)$.

2. Soit

$$\begin{array}{ccccccc} M' & \xrightarrow{u'} & M & \xrightarrow{u} & M'' & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} & & \\ 0 & \longrightarrow & N' & \xrightarrow[v']{} & N & \xrightarrow[v]{} & N'' \end{array}$$

un diagramme commutatif de morphismes de A-modules dont les lignes horizontales sont exactes.

   (a) Construire un morphisme 'naturel' $\delta : \ker(\alpha'') \to \operatorname{coker}(\alpha')$;

   (b) Montrer que la suite de morphismes

$$\ker(\alpha') \to \ker(\alpha) \to \ker(\alpha'') \xrightarrow{\delta} \operatorname{coker}(\alpha') \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\alpha'')$$

   est exacte.

   (c) Montrer que si α', α'' sont injectives (resp. surjectives) alors α est injective (resp. surjective).

   (d) On suppose de plus que $u' : M' \to M$ est injective et $v : N \to N''$ est surjective. Montrer que si deux des trois morphismes α, α', α'' sont des isomorphismes alors le troisième l'est aussi.

   (e) Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de groupes abéliens et soit p un nombre premier. Montrer qu'on a une suite exacte longue canonique de groupes abéliens

$$M'[p] \to M[p] \to M''[p] \to\!\!\to M'/p \to M/p \to M''/p \to 0,$$

   (où on a noté $M[p] := \{m \in M \mid pm = 0\}$ et $M/p := M/(pM)$).

3. (Lemme des cinq) Soit

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

un diagramme commutatif de morphismes de A-modules dont les lignes horizontales sont exactes.

   (a) Montrer que si α_1 est surjective et α_2, α_4 sont injectives alors α_3 est injective.

   (b) Montrer que si α_5 est injective et α_2, α_4 sont surjectives alors α_3 est surjective.

Chapitre 10

Conditions de finitude

Soit A un anneau commutatif.

10.1 Lemme

Lemme 10.1.0.1. *Soit M un A-module. Les conditions suivantes sont équivalentes.*

1. *Toute suite croissante de sous-A-modules de M est stationnaire.*
2. *Tout ensemble non vide de sous-A-modules de M admet un élément maximal pour l'inclusion.*
3. *Tout sous-A-module de M est de type fini.*

Définition 10.1.0.1. Un A-module M vérifiant les conditions équivalentes du lemme **??** est dit *noethérien*.

Démonstration. (1) $\Rightarrow$ (2) : Si (2) n'était pas vrai, il existerait un ensemble non vide $\mathcal{E}$ de sous A-modules de M ne contenant aucun élément maximal pour l'inclusion. Soit $M_0 \in \mathcal{E}$. Comme M_0 n'est pas maximal pour l'inclusion, il existe $M_1 \in \mathcal{E}$ tel que $M_0 \subsetneq M_1$. On itère l'argument avec M_1 et on construit ainsi une suite strictement croissante infinie de sous A-modules de M, ce qui contredit (1).
(2) $\Rightarrow$ (3) : Soit $M' \subset M$ un sous A-module et $\mathcal{E}$ l'ensemble des sous A-modules de type fini de M'. Comme le module trivial $\{0\}$ est dans $\mathcal{E}$, $\mathcal{E}$ est non-vide donc admet un élément M'' maximal pour l'inclusion. Pour tout $m \in M'$, le A-module $M'' + Am$ est dans $\mathcal{E}$ et contient M''. Par maximalité de M'', on a $M'' + Am = M''$ donc $m \in M''$.
(3) $\Rightarrow$ (1) : Soit

$$M_0 \subset M_1 \subset \cdots \subset M_n \subset M_{n+1} \subset \cdots \subset M$$

une suite croissante de sous A-modules. La réunion

$$U := \bigcup_{n \geq 0} M_n \subset M$$

est un sous A-module. Soit $m_1, \ldots, m_r$ une famille de générateurs de U. Chaque m_i est dans M_{n_i} pour un certain $n_i \geq 0$. Avec

$$N := \max\{n_i \mid i = 1, \ldots, r\}$$

on a $M_n = M_N$, $n \geq N$. □

Remarque. Un anneau A est en particulier noethérien au sens de **??** s'il l'est comme A-module sur lui-même.

10.2 Lemme

Soit M un A-module. Les conditions suivantes sont équivalentes.

1. *Toute suite décroissante de sous A-modules*

$$M \supset \cdots \supset M_0 \supset M_1 \supset \cdots \supset M_n \supset M_{n+1} \supset \ldots$$

   est stationnaire à partir d'un certain rang ;

2. *Tout ensemble non vide de sous A-modules de M possède un élément minimal pour l'inclusion.*

Un A-module M vérifiant les conditions équivalentes du lemme **??** est dit *artinien*. On laisse en exercice la preuve du lemme **??**, qui est exactement similaire à celle du lemme **??**

10.3 Exemple

1. Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est ni noetherien ni artinien. En effet, on a la suite infinie de sous $\mathbb{Z}$-modules

$$\cdots \subsetneq p^{n+1}\mathbb{Z} \subsetneq p^n\mathbb{Z} \subsetneq \cdots \subsetneq p\mathbb{Z} \subsetneq \mathbb{Z} \subsetneq p^{-1}\mathbb{Z} \subsetneq \cdots \subsetneq p^{-n}\mathbb{Z} \subsetneq p^{-n-1}\mathbb{Z} \subsetneq \cdots$$

2. Le $\mathbb{Z}$-module régulier est noetherien mais pas artinien. Il est noetherien car $\mathbb{Z}$ est principal donc tous ses idéaux sont de type fini (et même engendrés par un seul élément). Il n'est pas artinien car on a toujours la suite infinie

$$\cdots \subsetneq p^{n+1}\mathbb{Z} \subsetneq p^n\mathbb{Z} \subsetneq \cdots \subsetneq p\mathbb{Z} \subsetneq \mathbb{Z}$$

3. Le $\mathbb{Z}$-module $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ est artinien mais pas noetherien. En effet, les éléments de $M := \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ sont tous d'ordre fini, une puissance de p. Pour chaque $n \in \mathbb{Z}$, $n \geq 0$ notons $M_n := \mathbb{Z}\frac{1}{p^n} + \mathbb{Z}/\mathbb{Z} \subset \mathbb{Z}$. On a la suite strictement croissante de sous-$\mathbb{Z}$-modules

$$M_0 = \{0\} \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots M$$

   donc M n'est pas noetherien. Soit maintenant $N \subset M$ un sous-$\mathbb{Z}$-module. Distinguons deux cas.

(a) Le sup des ordres des éléments de N est fini, égal à p^n. Soit $a \in N$ d'ordre maximal p^n ; on peut donc écrire $a = \frac{b}{p^n} \in \mathbb{Z}[\frac{1}{p}] + \mathbb{Z}/\mathbb{Z}$ avec $1 \leq b \leq p^n - 1$, $p \nmid b$. Comme p est premier, il existe $u, v \in \mathbb{Z}$ tels que $ub + vp^n = 1$ donc $ua = \frac{1}{p_n} \in N$. Cela montre que $M_n \subset N$. Inversement, tout élément $a \in N$ s'écrit sous la forme $a = \frac{u}{p^m} \in \mathbb{Z}[\frac{1}{p}] + \mathbb{Z}/\mathbb{Z}$ avec $1 \leq b \leq p^m - 1$, $p \nmid b$ et $m \leq n$. Mais on peut aussi écrire $a = \frac{up^{n-m}}{p^n}$. Cela montre que $N \subset M_n$.

(b) Il existe une application strictement croissante $\phi : \mathbb{N} \to \mathbb{N}$ tel que N contient un élément a_n d'ordre exactement $p^{\phi(n)}$, $n \geq 0$. L'argument précédent montre que $\mathbb{Z}a_n = M_{\phi(n)} \subset N$. Donc $M = \cup_{n \geq 0} M_n \subset N$.

Les seuls sous $\mathbb{Z}$-modules de M sont donc M et les M_n, $n \geq 0$. Comme ils sont strictement ordonnés pour l'inclusion $M_0 = \{0\} \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots M$, on en déduit que M est artinien.

4. Tout $\mathbb{Z}$-module fini est à la fois noetherien et artinien. Si A est une algèbre sur un corps k, tout A-module de k-dimension finie est à la fois noetherien et artinien.

10.4 Lemme

1. *Soit* $0 \to M' \to M \to M'' \to 0$ *une suite exacte courte de A-modules. Alors M est noethérien (resp. artinien) si et seulement si* M' *et* M'' *sont noethériens (resp. artininens).*
2. *Une somme directe finie de A-modules noethériens (resp. artiniens) est encore noethérien (resp. artinien).*
3. *Tout module de type fini sur un anneau noethérien (resp. artinien) est noethérien (resp. artinien). Montrer que tout module de type fini sur un anneau noethérien est de présentation finie.*

Démonstration. 1. Supposons M noethérien (resp. artinien). Toute suite croissante (resp. décroissante) de sous-A modules de M' est une suite de sous-A modules de M donc stationne à partir d'un certain rang. De même, l'image inverse dans M de toute suite croissante (resp. décroissante) de sous-A modules de M'' est une suite de sous-A modules de M donc stationne à partir d'un certain rang. Supposons M' et M'' noethériens (resp. artiniens). Soit $M_1 \subset \cdots \subset M_n \subset M_{n+1} \subset \ldots M$ une suite croissante de sous-A modules de M. Il existe un entier N tel que $M_N \cap M' = M_n \cap M'$ et $(M_N + M')/M' = (M_n + M')/M'$n $n \geq N$. La conclusion résulte du lemme du serpent appliqué à

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_N \cap M' & \longrightarrow & M_N & \longrightarrow & (M_N + M')/M' & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & M_n \cap M' & \longrightarrow & M_n & \longrightarrow & (M_n + M')/M' & \longrightarrow & 0 \end{array}$$

L'assertion pour 'artinien' se montre de la même façon.

2. On procède par induction sur n en utilisant 1.3.4 (1) et la suite exacte courte de A-modules

$$0 \to \oplus_{1 \leq i \leq n} M_i \to \oplus_{1 \leq i \leq n+1} M_i \to M_{n+1} \to 0.$$

3. D'après 1.3.4 (2) $A^{\oplus n}$ est noethérien (resp. artinien) et, par définition, tout A-module de type fini est quotient d'un A-module de la forme $A^{\oplus n}$. Donc la conclusion résulte de 1.3.4 (1).

□

La propriété d'être noethérien et artinien est la bonne généralisation de la notion de dimension finie lorsque $A = k$ est un corps. Les points (1) et (2) du lemme suivant, par exemple, servent de substitut au Lemme du rang.

10.5 Lemme

(Fitting) *Soit $f : M \to M$ un endomorphisme de A-module.*

1. *Si M est noethérien et f surjectif alors f est un isomorphisme.*
2. *Si M est artinien et f injectif alors f est un isomorphisme.*
3. *(Lemme de 'Fitting') Si M est artinien et noethérien alors il existe une décomposition $M = f^\infty(M) \oplus f^{-\infty}(0)$ en somme directe de deux sous A-modules f-stables tels que la restriction de f à $f^\infty(M)$ soit un automorphisme et la restriction de f à $f^{-\infty}(0)$ soit nilpotente.*

Démonstration. 1. Il existe un entier $N \geq 1$ tel que $\ker(f^N) = \ker(f^n)$, $n \geq N$ et on applique le lemme du serpent à

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(f^N) & \longrightarrow & M & \xrightarrow{f^N} & M & \longrightarrow & 0 \\ & & \downarrow \simeq & & \downarrow \simeq \mathrm{Id} & & \downarrow f & & \\ 0 & \longrightarrow & \ker(f^{N+1}) & \longrightarrow & M & \xrightarrow[f^{N+1}]{} & M & \longrightarrow & 0 \end{array}$$

2. Il existe un entier $N \geq 1$ tel que $\mathrm{im}(f^N) = \mathrm{im}(f^n)$, $n \geq N$ et on applique le lemme du serpent à

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{f^{N+1}} & M & \longrightarrow & M/\mathrm{im}(f^{N+1}) & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow \simeq \mathrm{Id} & & \downarrow \simeq & & \\ 0 & \longrightarrow & M & \xrightarrow[f^N]{} & M & \longrightarrow & M/\mathrm{im}(f^N) & \longrightarrow & 0 \end{array}$$

3. (3) Comme Mest artinien et noethérien, il existe un entier $N \geq 1$ tel que

$$f^\infty(M) := \bigcap_{n\geq 0} \mathrm{im}(f^n) = \mathrm{im}(f^N), \quad f^{-\infty}(M) := \bigcup_{n\geq 0} \ker(f^n) = \ker(f^N).$$

On vérifie que $f^{\infty}(M)$, $f^{-\infty}(M)$ ainsi définis conviennent. Le seul point un peu astucieux est $M = f^{\infty}(M) + f^{-\infty}(M)$. On a envie d'écrire $m = f^N(m) + m - f^N(m)$ mais ça ne marche pas. Il faut ajuster en utilisant que $\mathrm{im}(f^N) = \mathrm{im}(f^{2N})$ et donc qu'il existe $\mu \in M$ tel que $f^N(m) = f^{2N}(\mu)$. La décomposition $m = f^N(\mu) + m - f^N(\mu)$ elle, convient.

□

Chapitre 11

Modules indécomposables, Krull-schmidt

11.1 Modules indécomposables

Un A-module M est dit *indécomposable* s'il est non nul et ne peut s'écrire sous la forme $M = M' \oplus M''$ avec $M', M'' \subset M$ deux sous A-modules non nuls. Un A-module M est dit *totalement décomposable* s'il peut s'écrire sous la forme $M = M_1 \oplus \cdots \oplus M_r$ avec $M_1, \ldots, M_r \subset M$ des sous A-modules indécomposables.

Un anneau E est dit *local* si $E \setminus E^\times$ est un idéal ; auquel cas, $E \setminus E^\times$ est l'unique idéal bilatère maximal de E.

11.2

Lemme. *Soit M un A-module. Si $E := \mathrm{End}_A(M)$ est local, M est indécomposable. Réciproquement, si M est indécomposable, artinien et noethérien, E est local.*

Démonstration. Supposons E local et qu'on puisse écrire $M = M' \oplus M''$ avec $M', M'' \subset M$ deux sous A-modules non nuls. Notons $e := \iota_{M'} \circ p_{M'} \in E$ la projection de M sur M' parallèlement à M''. On a $e, 1-e \in E \setminus E^\times$. Mais si E est local, $E \setminus E^\times$ est un idéal donc $1 = e + (1-e) \in E \setminus E^\times$: contradiction. Supposons maintenant que M est un A-module artinien et noethérien indécomposable, d'après l'Lemme **??** (3), tout élément non nul de E est soit inversible soit nilpotent. En particulier $J := E \setminus E^\times$ est l'ensemble des éléments nilpotents de E. Il suffit de montrer que J est un idéal bilatère. Soit donc $j \in J$ et $e \in E$. Comme j est nilpotent on a $\ker(j) \neq 0$ et $\mathrm{im}(j) \neq M$ (Lemme **??** (1), (2)). Donc aussi $\ker(ej) \neq 0$ et $\mathrm{im}(je) \neq M$, ce qui montre que $ej, je \in E \setminus E^\times = J$. Donc $EJ = JE = J$. Il reste à voir que J est stable par addition. Soit $j, j' \in J$, si $j + j' \in E^\times$ il existerait $e \in E$ tel que $ej = 1 - ej'$. Comme $ej' \in J$, on a forcément $1 - ej' \in E^\times$ (d'inverse $\sum_{n \geq 0} (ej')^n$), ce qui contredit le fait que $j \in J$. □

11.3 Théorème de Krull-Schmidt

Notons $Ind(A)$ l'ensemble des classes d'isomorphismes de A-modules indécomposables.

11.3.1

Théorème. (Krull-Schmidt) *Soit M un A-module artinien ou noethérien. Alors il existe une application à support finie $\kappa : Ind(A) \to \mathbb{Z}_{\geq 0}$ telle que*

$$M = \bigoplus_{N \in Ind(A)} N^{\oplus \kappa(N)}.$$

Si M est à la fois artinien et noethérien alors $\kappa : Ind(A) \to \mathbb{Z}_{\geq 0}$ est unique ; on la notera $\kappa_M : Ind(A) \to \mathbb{Z}_{\geq 0}$.

Démonstration. Commençons par montrer l'existence de la décomposition. Raisonnons par l'absurde. Si M n'est pas totalement décomposable, M n'est en particulier pas indécomposable donc

$$M = M_1^{(0)} \oplus M_2^{(0)}$$

avec $0 \neq M_1^{(0)}, M_2^{(0)} \subset M$ deux sous A-modules dont l'un au moins des deux - disons $M_1^{(0)}$ n'est pas totalement décomposable. On itère l'argument pour obtenir une suite de décompositions en sommes directes de sous A-modules non nuls

$$M = M_1^{(1)} \oplus M_2^{(1)} \oplus M_2^{(0)}$$

$$\cdots$$

$$M = M_1^{(n+1)} \oplus M_2^{(n+1)} \oplus M_2^{(n)} \oplus M_2^{(n-1)} \oplus \cdots \oplus M_2^{(1)} \oplus M_2^{(0)}$$

avec, à chaque fois, $M_1^{(n)}$ qui n'est pas totalement décomposable. On obtient en particulier une suite strictement croissante de sous A-modules

$$\{0\} \subset M_2^{(0)} \subset M_2^{(1)} \oplus M_2^{(0)} \subset \cdots \subset M_2^{(n)} \oplus \cdots M_2^{(1)} \oplus M_2^{(0)} \subset \cdots$$

et une suite strictement décroissante de sous A-modules

$$M \supset M_1^{(0)} \supset M_1^{(0)} \supset \cdots \supset M_1^{(n)} \supset M_1^{(n+1)} \supset \cdots$$

Supposons maintenant que M est artinien et noethérien et montrons l'unicité de la décomposition. D'après le Lemme **??** et par récurrence, il suffit de montrer que si on a un isomorphisme de A-modules noethérien et artinien

$$M \oplus M' \simeq N_1 \oplus \cdots \oplus N_s =: N$$

avec $E := \mathrm{End}_A(M)$ local et les $N_1, \ldots, N_s$ indécomposables alors il existe $1 \leq i \leq s$ tel que $M \simeq N_i$ et $M' \simeq \oplus_{j \neq i} N_j$. Soit $\Phi = (\phi \ \phi') : M \oplus M' \tilde{\to} N$ un isomorphisme de A-modules d'inverse

$$\Psi = \begin{pmatrix} \psi \\ \psi' \end{pmatrix} : N \tilde{\to} M \oplus M'.$$

Par le lemme **??**, $E \setminus E^\times$ est un idéal bilatère et l'égalité

$$\mathrm{Id}_M = \psi \circ \phi = \sum_{1 \leq i \leq s} \psi \circ \iota_i \circ p_i \circ \phi$$

implique que $\chi_i := \psi \circ \iota_i \circ p_i \circ \phi \in E^\times$ pour au moins un $i = 1, \ldots, s$. On a alors $p_i \circ \phi : M \hookrightarrow N_i$ injectif, $\psi \circ \iota_i : N_i \twoheadrightarrow M$ surjectif et

$$0 \longrightarrow \ker(\psi \circ \iota_i) \longrightarrow N_i \underset{p_i \circ \phi \circ \chi_i^{-1}}{\overset{\psi \circ \iota_i}{\rightleftarrows}} \mathrm{im}(\psi \circ \iota_i) \longrightarrow 0$$

donc

$$N_i = \ker(\psi \circ \iota_i) \oplus \mathrm{im}(p_i \circ \phi).$$

Comme par hypothèse N_i est indécomposable on a forcément $\ker(\psi \circ \iota_i) = 0$ et $\mathrm{im}(p_i \circ \phi) = N_i$. Donc $p_i \circ \phi : M \tilde{\to} N_i$ et $\psi \circ \iota_i : N_i \tilde{\to} M$ sont des isomorphismes. Il reste à voir que $M' \simeq \oplus_{j \neq i} N_j$. Pour cela, considérons les suites exactes courtes de A-modules :

$$0 \to M \xrightarrow{\iota} M \oplus M' \xrightarrow{p} M' \to 0$$

$$0 \to \bigoplus_{i \neq j} N_j \xrightarrow{\Psi \circ \iota'_i} M \oplus M' \xrightarrow{p_i \circ \Phi} N_i \to 0.$$

On sait que $p_i \circ \Phi \circ \iota = p_i \circ \phi : M \tilde{\to} N_i$ est un isomorphisme et on voudrait montrer que $p \circ \Psi \circ \iota'_i : \bigoplus_{i \neq j} N_j \to M'$ en est un aussi. Cela découle du petit lemme suivant, dont on laisse la preuve en exercice au lecteur. □

11.3.2

Lemme.

1. *Soit* $0 \to K \xrightarrow{\alpha} M \xrightarrow{\beta} Q$ *et* $0 \to K' \xrightarrow{\alpha'} M \xrightarrow{\beta'} Q'$ *deux suites exactes de* A*-modules. Alors* $\beta'\alpha$ *est injectif si et seulement si* $\beta\alpha'$ *est injectif.*
2. *Soit* $K \xrightarrow{\alpha} M \xrightarrow{\beta} Q \to 0$ *et* $K' \xrightarrow{\alpha'} M \xrightarrow{\beta'} Q' \to 0$ *deux suites exactes de* A*-modules. Alors* $\beta'\alpha$ *est surjectif si et seulement si* $\beta\alpha'$ *est surjectif.*

Chapitre 12

Modules de type fini sur les anneaux principaux

12.1 Préambule

Supposons que A soit un anneau principal, et soit M un A-module. Un élément $m \in M$ est dit *de torsion* s'il existe $0 \neq a \in A$ tel que $am = 0$. On note $T_M \subset M$ l'ensemble des éléments de torsion de M. On vérifie immédiatement que c'est un sous A-module et que le A-module M/T_M est sans torsion. Le A-module M s'insère donc dans la suite exacte courte

$$(*)\ \ 0 \to T_M \to M \to M/T_M \to 0,$$

où T_M est de torsion et M/T_M est sans torsion. Cela indique la voie pour classifier les A-modules de type fini : montrer que la suite exacte courte $(*)$ se scinde, ce qui par le Lemme **??**.1 impliquera automatiquement que

$$M \tilde{\to} T_M \oplus M/T_M$$

et réduit donc le problème de la classification des A-modules de type fini à

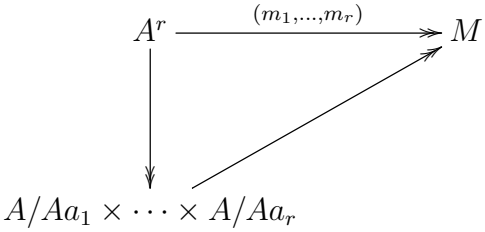
- la classification des A-modules de type fini sans torsion ;
- la classification des A-modules de type fini de torsion.

En fait, on va plutôt procéder dans l'ordre suivant. Notons que comme A est noethérien (car principal) et M de type fini, M est noethérien. Donc T_M et M/T_M sont aussi noethériens donc de type fini.

1. Tout d'abord, la raison pour laquelle on se restreint aux A-modules de type fini provient du lemme suivant.

   Lemme 12.1.0.1. *Un A-module de type fini est noethérien. Un A-module de type fini et de torsion est noethérien et artinien.*

Démonstration. Comme A est principal, tous ses sous A-modules (=idéaux) sont de type fini donc A est noethérien ; la première partie de l'énoncé résulte donc du Lemme **??**. Supposons M de torsion. Soit $m_1, \dots, m_r \in M$ un système de générateurs. Pour chaque $i = 1, \dots, r$ on peut trouver un élément $0 \neq a_i \in A$ tel que $a_i m_i = 0$. On a donc une factorisation



D'après le Lemme **??**, il suffit donc de montrer que les A-module de la forme A/Aa avec $0 \neq a \in A$ sont artiniens. Soit

$$A/Aa =: M_0 \supset M_1 \supset \cdots \supset M_n \supset M_{n+1} \supset \cdots$$

une suite décroissante de sous A-modules. Notons $\pi : A \to A/Aa$ la projection canonique et posons :

$$I_n := \pi^{-1}(M_n),\ n \geq 0.$$

Par construction on obtient une suite décroissante d'idéaux

$$A = I_0 \supset I_1 \supset \cdots \supset I_n \supset I_{n+1} \supset \cdots Aa.$$

Chacun de ces idéaux est de la forme $I_n = Aa_n$ avec $0 \neq a_n \in A$ et $a_n | a$. Mais comme un anneau principal est factoriel, a n'a qu'un nombre fini de diviseurs deux à deux non associés. Il n'y a donc qu'un nombre fini d'idéaux dans la suite I_n, $n \geq 0$. □

2. On va ensuite montrer que tout A-modules libre (sur un anneau intègre) est classifié par son rang et qu'un A-module de type fini sans torsion sur un anneau principal est libre de rang fini. Cela permettra aussi d'appliquer l'observation suivante.

Lemme 12.1.0.2. *Si M'' est un A-module libre alors toute suite exacte courte de A-modules $0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ est scindée.*

Démonstration. On construit une section en utilisant la propriété universelle de la somme directe. Plus précisément, quitte à composer v par un isomorphisme, on peut supposer que $M'' = A^{(I)}$. Pour chaque $i \in I$ notons $e_i = (\delta_{i,j})_{j \in I} \in A^{(I)}$ et choisissons $m_i \in I$ tel que $v(m_i) = e_i$. Le choix de m_i définit un morphisme de A-module $s_i : Ae_i \xrightarrow{e_i \to m_i} Am_i \hookrightarrow M$. Par propriète universelle des $\iota_i : Ae_i \to A^{(I)}$, $i \in I$, on en déduit un unique morphisme $s : A^{(I)} \to M$ tel que $s \circ \iota_i = s_i$, $i \in I$. Par construction $v \circ s = \mathrm{Id}$. On conclut par l'Exercice **??**.1. □

3. D'après le Lemme **??**.1 et le Théorème de Krull-Schmidt **??**, T_M est totalement décomposable ; le point sera donc de classifier les modules indécomposables de torsion sur un anneau principal A. On montrera que ce sont exactement les A-modules de la forme $A/\mathfrak{p}^n$, où $\mathfrak{p}$ est un idéal premier (=maximal) de A et $n \geq 0$.

12.2 Classification des A-modules de type fini sans torsion

Supposons d'abord que A est seulement un anneau commutatif intègre.

Lemme 12.2.0.1. *Un A-module de type fini sans torsion est isomorphe à un sous A-module d'un A-module libre de type fini.*

Démonstration. Soit $m_1, \dots m_r \in M$ un système de générateur. L'ensemble

$$\mathcal{S} := \{I \subset \{1, \dots, r\} \mid A^I \overset{(m_i)_{i\in I}}{\hookrightarrow} M\}$$

est non vide puisque M est sans torsion donc contient un élément $I \subset \{1, \dots, r\}$ maximal pour l'inclusion. Notons

$$N := \sum_{i\in I} Am_i \simeq A^I.$$

Par maximalité de I, pour chaque $j \in I^c := \{1, \dots, r\} \setminus I$ il existe $0 \neq a_j \in A$ tel que $a_j m_j \in N$. Notons $a := \prod_{j\in I^c} a_j \in A$; c'est un élément non nul de A puisque A est intègre. On en déduit que le morphisme de A-module

$$\begin{array}{ccc} M & \to & N \\ m & \to & am \end{array}$$

est injectif, puisque M est sans torsion. □

Lemme 12.2.0.2 (Classification des A-modules libres de type fini par le rang)**.**

1. *Le A-module libre $A^{(I)}$ est de type fini si et seulement si $|I| < +\infty$.*
2. *Soit I, J deux ensembles finis. Alors $A^{(I)}$ et $A^{(J)}$ sont isomorphes comme A-modules si et seulement si $|I| = |J|$.*

Démonstration. L'idée est de se ramener au cas des espaces vectoriels sur un corps pour lesquels le lemme est connu. Soit donc M un A-module libre de type fini et $\mathfrak{m} \subset A$ un idéal maximal. Comme M est de type fini, le $k := A/\mathfrak{m}$ espace vectoriel $M/\mathfrak{m}M$ est de dimension finie - disons r - sur k. Soit I un ensemble pour lequel on a un isomorphisme de A-modules

$$f : A^{(I)} \tilde{\to} M.$$

Posons $m_i := f(e_i)$, où e_i est le 'i-ème vecteur de la base canonique', $i \in I$. On va montrer que $|I| = r$. Pour cela, il suffit de montrer que les images $\overline{m}_i$, $i \in I$ des m_i, $i \in I$ dans $M/\mathfrak{m}M$ forment une k-base de $M/\mathfrak{m}M$. Puisque f est surjective, les $\overline{m}_i$, $i \in I$ forment une famille génératrice. Montrons qu'elle est libre. Soit $a : I \to A$ à support fini telle que

$$\sum_{i\in I} a(i)m_i \in \mathfrak{m}M.$$

Comme $M = \oplus_{i\in I} Am_i$ et $A \tilde{\to} Am_i$, $a \to am_i$, $i \in I$, cela implique $a(i) \in \mathfrak{m}$ donc $\overline{a}_i = 0$, $i \in I$. □

Le Lemme **??** montre en particulier que si M est un A-module libre de type fini il existe un unique entier $r \geq 1$ tel que $M \simeq A^{\oplus r}$. On appelle cet entier le *rang* du A-module libre M. C'est également la dimension du $A/\mathfrak{m}$-espace vectoriel $M/\mathfrak{m}M$, pour $\mathfrak{m}$ un idéal maximal de 1.

Supposons maintenant que A *est principal.*

Lemme 12.2.0.3. *Un sous A-module d'un A-module libre de rang fini r est un A-module libre de rang $\leq r$.*

Démonstration. On procède par récurrence sur r. Si $r = 1$, cela résulte du fait que A est principal. Supposons que l'énoncé du Lemme **??** est vérifié pour tout A-module libre de rang $\leq r$. Soit $M \subset A^{\oplus(r+1)}$ un sous A-module. Notons $p_{r+1} : A^{\oplus(r+1)} \twoheadrightarrow A$ la $r+1$-ième projection canonique. Comme $\ker(p_{r+1}) \simeq A^{\oplus r} \subset A^{\oplus(r+1)}$ est un A-module libre de rang r, par hypothèse de récurrence, le sous A-module $M \cap \ker(p_{r+1}) \subset \ker(p_{r+1})$ est un A-module libre de rang $s \leq r$. Comme $p_{r+1}(M) \subset A$ est un idéal et que A est principal, il existe $d_0 \in A$ et $m_0 \in M$ tel que $p_{r+1}(M) = Ad_0 \overset{\cdot d_0}{\xleftarrow{\sim}} A$ et on conclut par le Lemme **??**.2. □

On vient donc de montrer

Corollaire 12.2.0.1. *Un A-module de type fini sans torsion est libre de rang fini. Plus précisément, l'application $\mathbb{Z}_{\geq 0} \to \mathrm{Mod}_{/A}$, $r \to A^{\oplus r}$ induit une bijection de $\mathbb{Z}_{\geq 0}$ sur l'ensemble des classes d'isomorphismes de A-modules de type fini sans torsion.*

En particulier, M/T_M est un A-module libre de rang fini - disons r - donc, par le Lemme **??**.2 on a

$$M \simeq T_M \oplus M/T_M \simeq T_M \oplus A^{\oplus r}.$$

Il reste à classifier les A-modules de type fini qui sont de torsion.

12.3 Classification des A-modules de type fini de torsion

Soit A un anneau principal.

Théorème 12.3.0.1. *Les A-modules de type fini de torsion qui sont indécomposables sont exactement les A-modules de la forme $A/\mathfrak{p}^n$, où $\mathfrak{p} \subset A$ est un idéal premier non nul et $n \in \mathbb{Z}_{\geq 0}$.*

Démonstration. Vérifions d'abord qu'un A-module de la forme $A/\mathfrak{p}^n$ est indécomposable. Observons que

$$\mathrm{End}_A(A/\mathfrak{p}^n) \simeq \mathrm{End}_{A/\mathfrak{p}^n}(A/\mathfrak{p}^n) \simeq A/\mathfrak{p}^n$$

a un unique idéal maximal (c'est par exemple la factorialité de A) - $\mathfrak{p}/\mathfrak{p}^n$, donc est local (ici $A/\mathfrak{p}^n$ est commutatif). Le fait que $A/\mathfrak{p}^n$ est indécomposable résulte alors du lemme **??**.
Montrons maintenant que tout A-module indécomposable est de cette forme. Soit M un A-module. Pour tout $m \in M$, on note

$$Ann_A(m) := \{a \in A \mid am = 0\} \subset A$$

l'idéal annulateur de m et on se fixe un générateur $a_m \in Ann_A(m)$. On note également

$$Ann_A(M) := \bigcap_{m \in M} Ann_A(m) \subset A$$

l'idéal annulateur de M.

??.1.

Lemme 12.3.0.1. *Il existe $m \in M$ tel que $Ann_A(m) = Ann_A(M)$.*

Notons $B := A/Ann_A(m) = A/Ann_A(M)$ et considérons la suite exacte courte

$$0 \to B \xrightarrow{\cdot m} M \to M/Am \to 0.$$

On notera que comme $Ann_A(M)$ annnule M, cette suite est également une suite de B-modules.

Lemme 12.3.0.2. *La suite exacte courte de B-modules*

$$0 \to B \xrightarrow{\cdot m} M \to M/Am \to 0$$

est scindée.

Elle est donc *a fortiori* scindée comme suite exacte courte de A-modules *i.e.*

$$M \simeq A/Ann_A(M) \oplus M/Am$$

comme A-module. Mais comme M est indécomposable (et non nul), on en déduit $M = Am \simeq A/Ann_A(M) = A/Aa_m$. On conclut par la factorialité de A, le Lemme des restes Chinois et l'indécomposabilité de M. □

Preuve du lemme **??** Soit $m_1, \dots, m_r$ un système de générateurs de M comme A-module. On a

$$Ann_A(M) = \bigcap_{1 \leq i \leq r} Ann_A(m_i).$$

Il suffit donc de montrer que pour tout $m_1, m_2 \in M$ il existe $m_3 \in M$ tel que

$$Ann_A(m_1) \cap Ann_A(m_2) = Ann_A(m_3).$$

Écrivons $Ann_A(m_i) = Aa_i$, $i = 1, 2$. Comme A est factoriel, en utilisant la décomposition en produit de facteurs irréductibles de a_1 et a_2, on peut écrire $a_1 = \alpha_1\beta_1$ et $a_2 = \alpha_2\beta_2$ avec α_1, α_2 premier entre eux de produit 'le' plus petit commun multiple de a_1 et a_2. Posons $m_3 := \beta_1 m_1 + \beta_2 m_2$ et vérifions que m_3 convient. On a clairement $Ann_A(m_1) \cap Ann_A(m_2) \subset Ann_A(m_3)$. Pour l'inclusion réciproque, soit $a \in Ann_A(m_3)$. On a $a\beta_1 m_1 = -a\beta_2 m_2$. Par Bézout, il existe $u, v \in A$ tels que $u\alpha_1 + v\alpha_2 = 1$. On a donc

$$a\beta_1 m_1 = (u\alpha_1 + v\alpha_2)a\beta_1 m_1 = au\underbrace{a_1 m_1}_{=0} + v\alpha_2 a\beta_1 m_1 = -av\underbrace{a_2 m_2}_{=0} = 0.$$

Donc $a\beta_1 \in Ann_A(m_1) = Aa_1$ et $a\beta_2 \in Ann_A(m_2) = Aa_2$ en particulier a est un multiple commun de α_1 et α_2 donc de $\alpha_1\alpha_2 = \text{ppcm}(a_1, a_2)$. Donc $a \in Ann_A(m_1) \cap Ann_A(m_2)$. □

Preuve du Lemme **??**.*2.* Introduisons l'ensemble $\mathcal{E}$ des couples (u, N) où $m \in N \subset M$ est un sous-B-module et $u : N \to B$ un morphisme de B-modules tel que $u(m) = 1$. On munit $\mathcal{E}$ de la relation d'ordre $\leq$ définie par $(u_1, N_1) \leq (u_2, N_2)$ si $N_1 \subset N_2$ et $u_2|_{N_1} = u_1$. $\mathcal{E}$ est non-vide : par définition $B = A/Ann_A gc(m)$ donc on a un isomorphisme $v : B \tilde{\to} Am$ et $(Am, v^{-1}) \in \mathcal{E}$. Par définition, $\mathcal{E}$ est un ensemble ordonné inductif donc admet un élément maximal (u, N) (en fait, ici, on peut invoquer le fait que M est noethérien, ce qui permet d'éviter le Lemme de Zorn). Montrons que $N = M$. Sinon, soit $\mu \in M \setminus N$ et montrons qu'on peut étendre $u : N \to B$ en $u_1 : N + B\mu \to B$. Pour cela, il faut 'deviner' la bonne valeur de $u_1(\mu)$. Introduisons l'idéal

$$\mathfrak{i} := \{b \in B \mid b\mu \in N\} \subset B.$$

Écrivons $Ann_A gc(M) = Aa$. Comme B est quotient de l'anneau principal A, $\mathfrak{i} = Ab/Aa$ avec $Aa \subset Ab$ *i.e.* $a = \alpha b$ pour un certain $\alpha \in A$. Notons $u(b\mu) = \overline{c}$ (on note $\overline{-}$ les classes modulo Aa). On a $u(a\mu) = 0 = \alpha\overline{c}$ donc $\alpha c = qa = q\alpha b$ dans A. Mais comme A est intègre $c = qb$. On a donc envie de poser $u_1(\mu) = \overline{q}$. Définissons $u_0 : N \oplus B \to B$ par $u_0(n \oplus \lambda) = u(n) + \lambda\overline{q}$. On a

$$\ker(N \oplus B \twoheadrightarrow N + B\mu, n \oplus \lambda \to n + \lambda\mu) = \{\beta b\mu \oplus -\beta b \mid \beta \in B\} \subset \ker(u_0)$$

En effet, $u_0(\beta b\mu \oplus -\beta b) = u(\beta b\mu) - \beta b\overline{q} = \beta u(b\mu) - \beta b\overline{q} = \beta\overline{c} - \beta b\overline{q} = 0$. Donc $u_0 : N \oplus B \to B$ passe au quotient en $u_1 : N + B\mu \to B$ avec $u_1|_N = u$. Cela contredit la maximalité de (u, N). □

Corollaire 12.3.0.1. *Soit M un A-module de type fini de torsion. Il existe une unique suite décroissante d'idéaux*

$$A \supsetneq I_1 \supset I_2 \supset \cdots \supset I_r \supsetneq 0$$

telle que

$$M \simeq A/I_1 \oplus \cdots \oplus A/I_r.$$

Démonstration. Comme M est artinien et noethérien, d'après le Théorème de Krull-Schmidt **??**, M se décompose de façon unique comme somme directe de modules indécomposables. D'après le Théorème **??**, cette décomposition s'écrit

$$M \simeq \bigoplus_{\mathfrak{p}} \bigoplus_{n \geq 0} A/\mathfrak{p}^{\alpha_{M,\mathfrak{p}}(n)},$$

où la première somme est indexée par l'ensemble $\text{Spec}(A)$ des idéaux premiers non nuls de A et

$$\alpha_{M,-} : \text{Spec}(A) \to \mathbb{Z}_{\geq 0}^{(\mathbb{Z}_{\geq 0})}$$

est une application à support fini telle que $\alpha_{M,\mathfrak{p}} = (\alpha_{M,\mathfrak{p}}(n))_{n \geq 0}$ est une suite décroissante dont les termes sont nuls pour à partir d'un certain rang. Pour chaque $\mathfrak{p} \in \text{Spec}(A)$ choisissons un générateur p de $\mathfrak{p}$ comme A-module. Soit $n \geq 0$ le plus grand des entiers tels qu'il existe $\mathfrak{p} \in \text{Spec}(A)$ pour lequel $\alpha_{M,\mathfrak{p}}(n) \neq 0$ et posons

$$a_{n+1-j} := \prod_{\mathfrak{p}} p^{\alpha_{M,\mathfrak{p}}(j)},\ j = 1, \ldots, n.$$

La suite d'idéaux $I_i := Aa_j$, $j = 1, \dots, n$ vérifie alors la propriété de l'énoncé. Leur unicité résulte de l'unicité dans le théorème de Krull-Schmidt. □

On dit que la suite $A \supsetneq I_1 \supset I_2 \supset \cdots \supset I_r \supsetneq 0$ est la *suite des invariants* du A-module M.

12.4 Applications

12.4.1 Classification des groupes abéliens de type fini

On peut appliquer la classification des A-modules de type fini sur un anneau principal à l'anneau $\mathbb{Z}$ pour obtenir le classique théorème de classification des groupes finis.

Corollaire 12.4.1.1. *Soit M un groupe abélien de type fini. Il existe un unique $r \in \mathbb{Z}_{\geq 0}$ et une unique suite d'entiers positifs $d_1|d_2|\dots|d_s$ tels que*

$$M \simeq \mathbb{Z}^r \oplus (\bigoplus_{1 \leq i \leq s} \mathbb{Z}/d_i).$$

Exercice 12.4.1.1. Donner la liste des groupes abéliens d'ordre 6, 18, 24 et 36.

12.4.2 Algèbre linéaire

On peut également appliquer la classification à l'anneau $k[T]$ des polynômes à une indéterminée sur le corps k pour obtenir la classification des classes de conjugaison des endomorphisme d'un k-espace vectoriel de dimension finie par les invariants de similitude. Plus précisément, si V est un k-espace vectoriel de dimension finie tout endomorphisme $u : V \to V$ définit une structure de $k[T]$ module V_u sur V par $P(T)v = P(u)(v)$, $P \in k[T]$, $v \in V$. Le $k[T]$-module V_u est évidemment de type fini et de torsion. Il existe donc une unique suite de polynômes $P_{u,1}|P_{u,2}|\cdots|P_{u,r_u}$ telle que

$$V_u \simeq k[T]/P_{u,1} \oplus \cdots \oplus k[T]/P_{u,r_u}.$$

On dit que la suite $P_{u,1}|P_{u,2}|\cdots|P_{u,r_u}$ est la suite des *invariants de similitude* de l'endomorphisme u.

Exercice 12.4.2.1 (Classification des classes de conjugaison par les invariants de similitude)**.**

1. Soit $u, u' : V \to V$ deux endomorphismes. Montrer qu'il existe $\phi \in \mathrm{Aut}_k(V)$ tel que $u = \phi \circ u' \circ \phi^{-1}$ si et seulement si u et u' ont mêmes invariants de similitude.
2. Calculer le polynôme minimal et le polynôme caractéristique de u en fonction de sa suite d'invariants de similitude. Montrer plus précisément qu'il existe une base du k-espace vectoriel V dans laquelle u a pour matrice la matrice diagonale par blocs dont les blocs diagonaux sont les matrices compagnons des $P_{u,i}$.

3. Calculer le nombre de classes de conjugaison (sous $\mathrm{GL}_n(\mathbb{F}_q)$) dans $M_n(\mathbb{F}_q)$, dans $\mathrm{GL}_n(\mathbb{F}_q)$.

Au lieu d'appliquer le Corollaire **??** sous la forme énoncée, on peut l'appliquer avec la décomposition donnée par Krull-Schmidt (*cf.* preuve) *i.e.* il existe une unique famille de polynômes irréductibles $P_1, \dots, P_s$ et des familles d'entiers $n_{i,1} \geq \cdots \geq n_{i,r_i} > 0$, $i = 1, \dots, s$ tels que

$$V_u \simeq \bigoplus_{1 \leq i \leq s} \bigoplus_{1 \leq j \leq r_i} k[T]/P_i^{n_j}.$$

On retrouve alors la décomposition de Jordan en concaténant les bases $X^j P_i^l$, $0 \leq j \leq d_i) - 1$, $0 \leq l \leq n_i - 1$ de $k[T]/P_i^{n_j}$, $i = 1, \dots, s$. Dans cette base, la matrice de u est diagonale par blocs avec s blocs $D_1, \dots, D_s$ et chaque bloc D_i de la forme

$$\begin{pmatrix} C(P_i) & 0 & \cdots & 0 & 0 \\ U & C(P_i) & & 0 & 0 \\ 0 & & \cdots & & \\ 0 & & & U & C(P_i) \end{pmatrix},$$

où U est ma matrice carrée de taille $d_i \times d_i$ avec $u_{1,d_i} = 1$ et $u_{i,j} = 0$ sinon.

12.4.3 Base adaptée

La forme suivante du théorème de structure est aussi très utile en pratique.

Théorème 12.4.3.1 (base adaptée)**.** *Soit A un anneau principal, M un A-module libre de rang r et $N \subset M$ un sous-A-module. Il existe un unique entier $0 \leq s \leq r$, une unique suite $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ d'idéaux de A et $m_1, \dots, m_r \in M$ tels que*

$$N \simeq \bigoplus_{1 \leq i \leq s} Ad_i m_i \subset \bigoplus_{1 \leq i \leq r} Am_i \simeq M.$$

Démonstration. L'unicité de s et de la suite $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ résulte du Corollaire **??** car $r - s$ est le rang de la partie libre de M/N et $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ est la suite des invariants de la partie de torsion de M/N. L'existence est un peu plus délicate. On procède par reccurence sur r. Si $r = 1$, c'est la traduction du fait que A est principal. Si $r \geq 1$, l'idée est de construire d_1, e_1 à partir de l'inclusion $N \hookrightarrow M$. Pour cela, on introduit l'ensemble $\mathcal{E}$ des idéaux de la forme $f(N) \subset A$, où $f : M \to A$ est un morphisme de A-module. Comme A est noethérien, $\mathcal{E}$ contient au moins un élément maximal $f(N) = Ad = Af(n)$.

1. En fait, pour tout $g : M \to A$ on a $g(N) \subset f(N)$. En effet, si δ est le pgcd de d et $g(n)$ il existe $u, v \in A$ tels que $ud + vg(n) = \delta$. Donc

$$f(N) = Ad \subset A\delta = A(uf + vg)(n) \subset (uf + vg)(N)$$

Par maximalité de $f(N)$, cela implique $f(N) = Ad = A\delta = (uf + vg)(N)$. En particulier, pour tout $n' \in N$, d divise $(uf + vg)(n')$. Mais $f(N) = Ad$, donc d divise aussi $f(n')$. On

en déduit que d divise $vg(n')$ et comme d est premier avec v, que d divise $g(n')$. *In fine*, on a $g(N) \subset Ad = f(N)$ comme annoncé.

2. Il existe $\mu \in M$ tel que $d\mu = n, \forall n \in N$. Choisissons une A-base quelconque $e_1, \dots, e_r$ de M et notons $p_i : M \twoheadrightarrow Am_i \simeq A$ la projection correspondante sur la i-ème coordonnée. On a, dans cette base, $n = \sum_{a \leq i \leq r} a_i e_i$ et en appliquant (1) aux p_i, on obtient que d divise a_i, $i = 1, \dots, r$. Donc en écrivant $a_i = db_i$ pour un certain $b_i \in A$, $i = a, \dots, r$, on peut prendre $\mu = \sum_{1 \leq i \leq r} b_i e_i$.

3. De $d\mu = m$, on déduit $f(d\mu) = df(\mu) = f(n) = d$, donc comme A est intègre, $f(\mu) = 1$. Cela donne une décomposition $M \simeq \ker(f) \oplus A\mu$ (car $m = (m - f(m)\mu) + f(m)\mu$) telle que $N = \ker(f) \cap N \oplus Ad\mu$. On peut donc appliquer l'hypothèse de recurrence à $\ker(f) \cap N \subset \ker(f)$ puisqu'on sait que $\ker(f)$ est un A-module libre de rang r (théorème du rang) pour obtenir une suite $A \supsetneq Ad_2 \supset \cdots \supset Ad_s \supsetneq 0$ d'idéaux de A et $m_2, \dots, m_r \in \ker(f)$ tels que
$$\ker(f) \cap N = \bigoplus_{2 \leq i \leq s} Ad_i m_i \subset \bigoplus_{2 \leq i \leq r} Am_i = \ker(f).$$
Enfin, en appliquant à nouveau (1) à la projection $M = A\mu \oplus \bigoplus_{2 \leq i \leq r} Am_i \twoheadrightarrow Am_2 \simeq A$, on voit que d divise d_2.

□

Théorème 12.4.3.2 (Classes d'équivalence)**.** *On considère l'action de* $\mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ *sur* $M_{n,m}(A)$ *donnée par* $(P, Q) \cdot M = PMQ^{-1}$*. L'ensemble des classes d'équivalence* $M_{n,m}(A)/\mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ *est canoniquement en bijection avec les suites* $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_n$ *d'idéaux de* A*.*

Démonstration. On suppose $m \geq n$. Notons $M := A^m$, $N := A^n$ et soit $f : M \to N \in \mathrm{Hom}_A(M, N)$. Par le théorème de la base adaptée pour $f(M) \subset N$ il existe un unique $0 \leq r \leq n$, une unique suite d'idéaux $A \supsetneq Ad_1 \supset Ad_2 \supset \cdots \supset Ad_r$ et des éléments $\nu_1, \dots, \nu_n \in N$ tels que
$$f(M) = \bigoplus_{1 \leq i \leq r} Ad_i \nu_i \subset \bigoplus_{1 \leq i \leq n} A\nu_i = N.$$
Comme $f(M)$ est un A-module libre, la suite exacte courte
$$0 \to \ker(f) \to M \xrightarrow{f} f(M) \to 0$$
est scindée. Notons $s : f(M) \to M$ un scindage. On a alors $M \simeq \ker(f) \oplus f(M)$. Comme A est principal et M est un A-module libre, $\ker(f) \subset M$ est encore un A-module libre. En concaténant une A-base de $\ker(f)$ et la A-base $s(\nu_1 d_1), \dots, s(\nu_n d_n)$ de $s(f(M)) = M$, on obtient une A-base $\mu_1, \dots, \mu_n$ de M. La matrice de f dans les bases $\mu_1, \dots, \mu_m$ et $\nu_1, \dots, \nu_n$ est de la forme
$$D(d_1, \dots, d_n) := \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 \\ 0 & d_2 & & 0 & 0 \\ 0 & & \cdots & & \\ 0 & & & d_n & 0 \end{pmatrix}.$$

On a donc montré que si $f, g : M \to N$ sont des morphismes de A-modules tels que $N/f(M) \simeq N/g(M)$ alors f, g sont équivalents. La réciproque est presque immédiate car s'il existe des automorphismes $\phi \in \mathrm{Aut}_A(M)$, $\psi \in \mathrm{Aut}_A(N)$ tels que $f \circ \phi = \psi \circ g$ alors $\psi : N \tilde{\to} N$ se restreint en un isomorphisme de A-modules $\psi : g(M) \tilde{\to} f(\phi(M)) = f(M)$ donc induit un isomorphisme de A-modules $\overline{\psi} : N/g(M) \tilde{\to} N/f(M)$. □

Remarque. Dans le cas où $A = k$ est un corps commutatif, on retrouve le thèorème de classification des classes d'équivalence par le rang de la matrice.

Démonstration. En effet, les seules suites possibles sont $k \supset \underset{r}{\cdots} \supset k \supset 0 \supset \underset{n-r}{\cdots} \supset 0$ On retrouve le théorème de classification des classes d'équivalence des matrices sur un corps par le rang. □

12.4.3.0.1 Exercice. Soit M un $\mathbb{Z}$-module libre de rang fini m et $\phi \in \mathrm{End}_{\mathbb{Z}}(M)$ tel que $\phi \otimes \mathbb{Q} \in \mathrm{Aut}_{\mathbb{Q}}(M \otimes \mathbb{Q})$ est inversible. Montrer que $\phi(M) \subset M$ est d'indice fini et calculer $[M : \Phi(M)$.

Chapitre 13

Produit tensoriel

13.1 Construction

Soient $M_1, \ldots, M_r$ une famille de A-modules et M un A-module. Notons

$$L_{r,A}(M_1 \times \cdots \times M_r, M)$$

l'ensemble des applications $f : M_1 \times \cdots \times M_r \to M$ qui sont r-A-multilinéaires *i.e.* telles que $f \circ \iota_i : M_i \to M$ est un morphisme de A-modules, $i = 1, \ldots, r$.

Notons

$$\Sigma := A^{(M_1 \times \cdots \times M_r)},$$

le A-module libre engendré par $M_1 \times \ldots \times M_r$, $(m_1, \ldots, m_r) \in M_0$ l'élément correspondant au terme avec des 0 partout sauf en l'indice $(m_1, \ldots, m_r)$ et $R \subset \Sigma$ le sous A-module engendré par les éléments de la forme

$$(m_1, \ldots, a_i m_i + a_i' m_i', \ldots, m_r) - a_i(m_1, \ldots, m_i, \ldots, m_r) - a_i'(m_1, \ldots, m_i', \ldots, m_r).$$

En posant $M_1 \otimes_A \cdots \otimes_A M_r := \Sigma / R$ et

$$\begin{array}{rccccc} p : & M_1 \times \cdots \times M_r & \to & A^{(M_1 \times \cdots \times M_r)} & \to & M_1 \otimes_A \cdots \otimes_A M_r \\ & (m_1, \ldots, m_r) & \mapsto & 1 \cdot (m_1, \ldots, m_r) & \mapsto & (m_1, \ldots, m_r) \bmod M_{00} =: m_1 \otimes \cdots \otimes m_r \end{array}$$

on vérifie facilement que $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ est une application A-r-linéaire. On prendra garde que $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ n'est pas surjective en général mais que, $M_1 \otimes_A \cdots \otimes_A M_r$ est engendré comme A-module par les éléments de la forme $m_1 \otimes \cdots \otimes m_r$.

Remarque 13.1.0.1. Les éléments de $M_1 \otimes_A \cdots \otimes_A M_r$ ne sont pas tous de la forme $m_1 \otimes \cdots \otimes m_r$ pour $(m_1, \ldots, m_r) \in M_1 \times \cdots \times M_r$ (*i.e.* p n'est en général pas surjective). En effet, il n'y a aucune raison pour que $a \cdot m_1 \otimes \cdots \otimes m_r + b \cdot n_1 \otimes \cdots \otimes n_r$ soit de la forme $\mu_1 \otimes \cdots \otimes \mu_r$. Par contre, $M_1 \otimes_A \cdots \otimes_A M_r$ est un quotient de $\Sigma := \bigoplus_{\underline{m} \in M_1 \times \cdots \times M_r} A e_{\underline{m}}$. Il est engendré, comme A-module, par les $m_1 \otimes \cdots \otimes m_r$

Définition 13.1.0.1 (tenseurs élémentaires)**.** On dit parfois que les éléments de la forme $m_1 \otimes \cdots \otimes m_r$ sont des tenseurs élémentaires.

Lemme 13.1.0.1 (propriété universelle du produit tensoriel)**.** *Pour toute famille $M_1, \dots, M_r$ de A-modules, il existe un A-module T et une application r-A-linéaire $p : M_1 \times \cdots \times M_r \to T$ tels que pour tout A-module M et pour toute application r-A-linéaire $f : M_1 \times \cdots \times M_r \to M$ il existe un unique morphisme de A-modules $\overline{f} : T \to M$ tel que $\overline{f} \circ p = f$.*

Remarque 13.1.0.2. Notons

$$L_{r,A}(M_1 \times \cdots \times M_r, M)$$

l'ensemble des applications $f : M_1 \times \cdots \times M_r \to M$ qui sont r-A-linéaires *i.e.* telles que $f \circ \iota_i : M_i \to M$ est un morphisme de A-modules, $i = 1, \dots, r$. La structure de A-module sur M induit une structure de A-module sur $L_{r,A}(M_1 \times \cdots \times M_r, M)$ et on vérifie immédiatement que

$$L_{r,A}(M_1 \times \cdots \times M_r, -) : Mod_{/A} \to Mod_{/A}$$

est un foncteur.

Démonstration. Vérifions que $T := M_1 \otimes_A \cdots \otimes_A M_r$ et l'application r-A-linéaire $\underline{p} : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ conviennent. Si $\overline{f} : M_1 \otimes \cdots \otimes M_r \to M$, la condition $p \circ \overline{f} = f$ impose $\overline{f}(m_1 \otimes \cdots \otimes m_r) = f(m_1, \dots, m_r)$. Comme $M_1 \otimes_A \cdots \otimes_A M_r$ est engendré, comme A-module, par les éléments de la forme $m_1 \otimes \cdots \otimes m_r$, cela montre l'unicité de $\overline{f}$ sous réserve de son existence. Par propriété universelle des $\iota_{\underline{m}} : A \hookrightarrow A^{(M_1 \times \cdots \times M_r)}$, $\underline{m} = (m_1, \dots, m_r) \in M_1 \times \cdots \times M_r$, il existe un unique morphisme de A-modules $F : M_0 = A^{(M_1 \times \cdots \times M_r)} \to M$ tel que $F \circ \iota_{\underline{m}} : A \to M$ est le morphisme qui envoie 1 sur $f(m_1, \dots, m_r)$. Comme $f : M_1 \times \cdots \times M_r \to M$ est r-A-linéaire, $M_{00} \subset \ker(F)$ donc $F : M_0 \to M$ se factorise en un morphisme de A-modules $\overline{f} : M_1 \otimes_A \cdots \otimes_A M_r \to M$ tel que $p \circ \overline{f} = F$; en particulier

$$p \circ \overline{f}(m_1, \dots, m_r) = F(m_1, \dots, m_r) = f(m_1, \dots, m_r),\ (m_1, \dots, m_r) \in M_1 \times \cdots \times M_r.$$

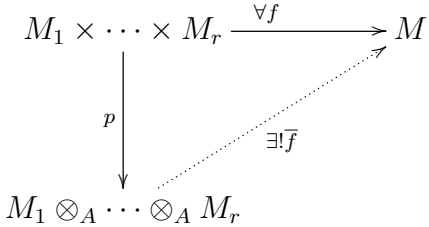
□

Comme d'habitude, $p : M_1 \times \cdots \times M_r \to M_1 \otimes_A \cdots \otimes_A M_r$ est unique à unique isomorphisme près.

On peut aussi réécrire **??** en disant que pour tout A-module M l'application canonique

$$\mathrm{Hom}_A(M_1 \times \cdots \times M_r, M) \to L_{r,A}(M_1 \times \cdots \times M_r, M),\ f \to p \circ f$$

est bijective ou encore, plus visuellement,



Si $f_i : M_i \to N_i$, $i = 1, \dots, r$ sont r morphismes de A-modules, l'application

$$\begin{array}{lccl} (f_1, \dots, f_r) & M_1 \times \cdots \times M_r & \to & N_1 \otimes_A \cdots \otimes_A N_r \\ & (m_1, \dots, m_r) & \to & f_1(m_1) \otimes \cdots \otimes f_r(m_r) \end{array}$$

est r-A-linéaire donc se factorise en un morphisme de A-modules $f_1 \otimes_A \cdots \otimes_A f_r : M_1 \otimes_A \cdots \otimes_A M_r \to N_1 \otimes_A \cdots \otimes_A N_r$ tel que $f_1 \otimes_A \cdots \otimes_A f_r(m_1 \otimes \dots m_r) = (f_1, \dots, f_r)(m_1, \dots, m_r) = f_1(m_1) \otimes \cdots \otimes f_r(m_r)$.

13.2 Propriétés élémentaires

13.2.1 Propriétés

Lemme 13.2.1.1 (« commutation » du produit tensoriel aux sommes directes)**.** *Soit M_i, $i \in I$ et M des A-modules. On a un isomorphisme canonique*

$$\begin{array}{ccc} M \otimes_A (\bigoplus_{i\in I} M_i) & \tilde{\to} & \bigoplus_{i\in I}(M \otimes_A M_i) \\ m \otimes (m_i)_{i\in I} & \to & (m \otimes m_i)_{i\in I} \end{array}$$

Démonstration. Vérifions d'abord que $\phi : M \otimes_A (\bigoplus_{i\in I} M_i) \to \bigoplus_{i\in I}(M \otimes_A M_i)$ est bien définie. L'application $\Phi : M \times \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I}(M \otimes_A M_i)$, $(m, (m_i)_{i\in I}) \to (m \otimes m_i)_{i\in I}$ est 2-A-linéaire donc par propriété universelle de $p : M \times (\bigoplus_{i\in I} M_i) \to M \otimes_A (\bigoplus_{i\in I} M_i)$ se factorise effectivement en un morphisme de A-module $\phi : M \otimes_A (\bigoplus_{i\in I} M_i) \to \bigoplus_{i\in I}(M \otimes_A M_i)$ tel que $p \circ \phi = \Phi$. Inversement, pour tout $i \in I$ l'application $\Psi_i : M \times M_i \to M \otimes_A (\bigoplus_{i\in I} M_i)$, $(m, m_i) \to m \otimes \iota_i(m_i)$ est 2-A-linéaire donc par propriété universelle de $p : M \times M_i \to M \otimes_A M_i$ se factorise en un morphisme de A-module $\psi_i : M \otimes_A M_i \to M \otimes_A (\bigoplus_{i\in I} M_i)$ tel que $p \circ \psi_i = \Psi_i$. Puis, par propriété universelle de $\iota_i : M \otimes_A M_i \to \bigoplus_{i\in I}(M \otimes_A M_i)$, $i \in I$ on obtient un unique morphisme de A-module $\psi : \bigoplus_{i\in I}(M \otimes_A M_i) \to M \otimes_A (\bigoplus_{i\in I} M_i)$ tel que $\psi \circ \iota_i = \Psi_i$, $i \in I$. On vérifie sur les constructions que ϕ, ψ sont inverses l'un de l'autre. □

Les preuves des lemmes suivant sont du même acabit *i.e.* purement formelles et laissées en exercice au lecteur.

Lemme 13.2.1.2 (commutativité et associativité)**.** *Soit L, M, N des A-modules. On a des isomorphismes (de A-modules) canoniques*

$$\begin{array}{ccc} L \otimes_A (M \otimes_A N) & \tilde{\to} & (L \otimes_A M) \otimes_A N \\ l \otimes (m \otimes n) & \mapsto & (l \otimes m) \otimes n \end{array}$$

$$\begin{array}{ccc} M \otimes_A N & \tilde{\to} & N \otimes_A M \\ m \otimes n & \mapsto & n \otimes m \end{array}$$

Lemme 13.2.1.3. *A est l'« unité » pour le produit tensoriel, c'est-à-dire que pour tout A-module M, on a un isomorphisme canonique*

$$\begin{array}{ccc} A \otimes_A M & \tilde{\to} & M \\ a \otimes m & \mapsto & am \end{array}$$

13.2.2 Espace dual

Soit I un ensemble. Pour $i \in I$ on rappelle qu'on note $e_i := (\delta_{i,j})_{j\in I} \in A^{(I)}$ le i-ème élément de la base canonique de $A^{(I)}$.

Lemme. *Soit $I_1, \dots, I_r$ des ensembles. On a un isomorphisme de A-modules canonique*

$$A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_r)} \tilde{\to} A^{(I_1\times\cdots\times I_r)}$$

qui envoie $e_{i_1} \otimes \cdots \otimes e_{i_r}$ sur $e_{(i_1,\dots,i_r)}$, $(i_1, \dots, i_r) \in I_1 \times \cdots \times I_r$.

Démonstration. On peut le déduire formellement des Lemmes **??**, **??**, **??** :

$$\begin{array}{ll} A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_r)} & (\tilde{\to} A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_{r-1})}) \otimes_A A^{(I_r)} \\ & \tilde{\to}((A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_{r-1})} \otimes_A A)^{(I_r)} \\ & \tilde{\to}(A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_{r-1})})^{(I_r)} \\ & \tilde{\to} \cdots \tilde{\to} A^{(I_1\times\cdots\times I_r)}. \end{array}$$

On peut aussi donner un argument direct. En effet, l'application $A^{(I_1)} \times \cdots \times A^{(I_r)} \tilde{\to} A^{(I_1\times\cdots\times I_r)}$, $((a_{i_1})_{i_1\in I_1}, \cdots, (a_{i_r})_{i_r\in I_r}) \to (a_{i_1} \cdots a_{i_r})_{(i_1,\dots,i_r)\in I_1\times\cdots\times I_r}$ est r-A-linéaire donc se factorise en un morphisme de A-modules $\phi : A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_r)} \to A^{(I_1\times\cdots\times I_r)}$ tel que $\phi((a_{i_1})_{i_1\in I_1} \otimes \cdots \otimes (a_{i_r})_{i_r\in I_r}) = (a_{i_1} \cdots a_{i_r})_{(i_1,\dots,i_r)\in I_1\times\cdots\times I_r}$). Inversement, pour chaque $(i_1, \dots, i_r) \in I_1 \times \cdots \times I_r$ on dispose du morphisme de A-modules $\psi_{(i_1,\dots,i_r)} : A \to A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_r)} \tilde{\to} A^{(I_1\times\cdots\times I_r)}$, $a \to ae_{i_1} \otimes \cdots \otimes e_{i_r}$ donc, par propriété universelle de la somme directe, d'un morphisme de A-modules $\psi = \oplus_{(i_1,\dots,i_r)\in I_1\times\cdots\times I_r}\psi_{(i_1,\dots,i_r)} : A^{(I_1\times\cdots\times I_r)} \to A^{(I_1)} \otimes_A \cdots \otimes_A A^{(I_r)}$ tel que $\psi \circ \iota_{(i_1,\dots,i_r)} = \psi_{(i_1,\dots,i_r)}$, $(i_1, \dots, i_r) \in I_1 \times \cdots \times I_r$. On vérifie sur les définitions que ϕ et ψ sont inverses l'une de l'autre. □

En particulier, si M_i est un A-module libre de rang fini d_i, $i = 1, \dots, r$, $M_1 \otimes_A \cdots \otimes_A M_r$ est un A-module libre de rang $d_1 \dots d_r$.

Définition 13.2.2.1. Soient M un A-module. On note $M^\vee := \mathrm{Hom}_A(M, A)$ qu'on appelle le dual de M.

Lemme 13.2.2.1. *Soit M, N des A-modules. On a des morphismes de A-modules canoniques*

$$\begin{array}{rcl|rcl} M^\vee \otimes_A N & \to & \mathrm{Hom}_A(M, N) \ , & M^\vee \otimes_A N^\vee & \to & (M \otimes_A N)^\vee \\ f \otimes n & \mapsto & f(-)n \ ; & f \otimes g & \mapsto & m \otimes n \to f(m)g(n). \end{array}$$

et

$$\begin{array}{rcl} \mathrm{End}_A(M) \otimes_A \mathrm{End}_A(N) & \to & \mathrm{End}_A(M \otimes_A N) \\ f \otimes g & \mapsto & m \otimes n \mapsto f(m) \otimes g(n) \ ; \end{array}$$

Si de plus M et N sont libres de rang fini, ces trois morphismes sont des isomorphismes.

Démonstration. Les morphismes se construisent en utilisant la propriété universelle du produit tensoriel. En général, il n'y a par contre pas de façon canonique de construire des inverses de ces morphismes (et d'ailleurs, ce ne sont pas toujours des isomorphismes). Mais si M et N sont libres de rang fini, on peut vérifier que ces trois morphismes envoient à chaque fois une base sur une base. □

13.3 Adjonctions

13.3.1 $- \otimes_A M$ versus $\mathrm{Hom}_A(M, -)$

Lemme 13.3.1.1 (adjonction 1)**.** *Soit L, M, N des A-modules. On a des isomorphismes (de A-modules) canoniques*

$$\begin{array}{ccccc} \mathrm{Hom}_A(L, \mathrm{Hom}_A(M,N)) & \tilde{\to} & L_{r,A}(L \times M, N) & \tilde{\to} & \mathrm{Hom}_A(L \otimes_A M, N) \\ f & \to & (l,m) \to f(l)(m) & & \\ l \to \beta(l,-) & \leftarrow & \beta & & \end{array}$$

(Le deuxième isomorphisme est simplement la propriété universelle du produit tensoriel).

Exercice 13.3.1.1. Soit M un A-module. Montrer que pour toute suite exacte courte de A-modules

$$0 \to N' \overset{u}{\to} N \overset{v}{\to} N'' \to 0$$

1. La suite
$$0 \to \mathrm{Hom}_A(M, N') \overset{u\circ}{\to} \mathrm{Hom}_A(M, N) \overset{v\circ}{\to} \mathrm{Hom}_A(M, N'')$$
est exacte.
2. La suite
$$M \otimes_A N' \overset{\mathrm{Id}\otimes u}{\to} M \otimes_A N \overset{\mathrm{Id}\otimes v}{\to} M \otimes_A N'' \to 0$$
est exacte.

13.3.2 Extension et restriction des scalaires

Soit $\phi : A \to B$ une A-algèbre. A tout B-module M on peut associer un A-module noté $M|_A$ (ou $\phi_* M$) dont le groupe abélien sous-jacent est encore M et dont la structure de A-module est définie par $a \cdot m = \phi(a)m$, $a \in A$, $m \in M$. Tout morphisme de B-modules $f : M \to N$ induit alors tautologiquement un morphisme de A-modules $f|_A : M|_A \to N|_A$. On voudrait, inversement, associer à tout A-module M un B-module $\phi^* M$ et à tout morphisme de A-modules $f : M \to N$ un morphisme de B-modules $\phi^* f : \phi^* M \to \phi^* N$.

Soit M un B-module et N un A-module. Pour tout $b_0 \in B$, l'application

$$\begin{array}{ccc} M \times N & \to & M \otimes_A N (:= (M|_A) \otimes_A N) \\ (m,n) & \to & (b_0 m) \otimes n \end{array}$$

est 2-A-linéaire donc se factorise en un morphisme de A-module

$$\begin{aligned} b_0 \cdot : M \otimes_A N &\to M \otimes_A N \\ m \otimes n &\mapsto b_0 \cdot (m \otimes n) := (b_0 m) \otimes n \end{aligned}$$

On vérifie que cela définit une structure de B-module sur $M \otimes_A N$. Tout morphisme de A-modules $f : N \to N'$ induit alors un morphisme de B-modules $\mathrm{Id}_M \otimes f : M \otimes_A N \to M \otimes_A N'$.

Si $M = B$ muni de la structure de A-module donnée par $\phi : A \to B$ ($a \cdot b = \phi(a)b$, $a \in A$, $b \in B$), on note parfois $\phi^* N := B \otimes_A N$ et $\phi^* f := \mathrm{Id}_B \otimes f : \phi^* N \to \phi^* N'$.

Les constructions ϕ_*, ϕ^* sont liées par le lemme suivant.

Lemme 13.3.2.1 (adjonction 2)**.** *Soit M un A-module et N un B-module. On a un isomorphisme canonique (de $\mathbb{Z}$-modules)*

$$\begin{array}{ccc} \mathrm{Hom}_A(M, N|_A) & \tilde{\to} & \mathrm{Hom}_B(B \otimes_A M, N) \\ f & \to & b \otimes m \to bf(m) \\ f(1 \otimes -) & \leftarrow & f \end{array}$$

Exercice 13.3.2.1 (Transitivité de l'extension des scalaires)**.**

1. Soit M, M' des B-modules et N un A-module. Montrer qu'on a un isomorphisme canonique de B-modules
$$M' \otimes_B (M \otimes_A N) \tilde{\to} (M' \otimes_B M) \otimes_A N.$$
En déduire qu'on a un isomorphisme canonique de B-modules $M \otimes_B (B \otimes_A N) \tilde{\to} M \otimes_A N$;
2. Soit $A \to B \to C$ des morphismes d'anneaux et M un A-module. Montrer qu'on a un isomorphisme canonique
$$C \otimes_B (B \otimes_A M) \tilde{\to} C \otimes_A N.$$

13.3.2.1 Extension des scalaires par un quotient

Soit M un A-module et $I \subset A$ un idéal. Notons $IM \subset M$ le sous-A-module engendré par les éléments de la forme am, $a \in I$, $m \in M$. Par propriété universelle du quotient, l'application

$$\begin{array}{ccc} A \times M/IM & \to & M/IM \\ (a, \overline{m}) & \to & a\overline{m} = \overline{am} \end{array}$$

donnée par la structure de A-module sur M/IM se factorise en une application $A/I \times M/IM \to M/IM$, qui fait de M/IM un A/I-module.

Lemme 13.3.2.2 (Propriété universelle de $M \to M/IM$)**.** *Pour tout A-module M et idéal $I \subset A$, il existe un A/I-module Q et un morphisme de A-modules $p : M \to (p_I)_* Q$ tel que pour tout A/I-module N et tout morphisme de A-module $\phi : M \to (p_I)_* N$ il existe un unique morphisme de A/I-module $\overline{\phi} : Q \to N$ tel que $\overline{\phi} \circ p = \phi$.*

Démonstration. On vérifie que $p_{IM} : M \to M/IM$ convient. Si $\overline{\phi} : M/IM \to N$ existe la condition $\overline{\phi} \circ p_{IM} = \phi$ impose $\overline{\phi}(\overline{m}) = \phi(m)$, $m \in M$, d'où l'unicité de $\overline{\phi}$ sous réserve de son existence. Par ailleurs, pour tout $a \in I$, $m \in M$, $\phi(am) = p_I(a)\phi(m) = 0$ donc $IM \subset \ker(\phi)$ et $\phi : M \to N$ se factorise en un morphisme de A-modules $\overline{\phi} : M/IM \to (p_I)_* M$ qui induit tautologiquement un morphisme $\overline{\phi} : M/IM \to N$ de A/I-modules. □

On peut réécrire le Lemme en disant que pour tout A/I-module N l'application canonique

$$\mathrm{Hom}_{A/I}(M/IM, N) \to \mathrm{Hom}_A(M, N),\ \phi \to (\phi \circ p_{IM})$$

est bijective. Or **??** dit que le morphisme de A-module $p : M \to A/I \otimes_A M$, $m \to \overline{1} \otimes m$ vérifie la même propriété. Par unicité des objets universels, on a donc un unique morphisme de A/I-modules $\phi : A/I \otimes M \to M/IM$ tel que $\phi \circ p = p_{IM}$. On peut aussi démontrer cela 'à la main', comme suit.

L'application canonique

$$\begin{array}{ccc} A \times M & \to & M/IM \\ (a, m) & \to & \overline{am} \end{array}$$

est 2-A-linéaire et passe au quotient en une application 2-A-linéaire $A/I \times M \to M/IM$ donc se factorise en un morphisme de A-modules $f : (A/I) \otimes_A M \to M/IM$. Inversement, l'application $M \to (A/I) \otimes_A M$, $m \to 1 \otimes m$ est un morphisme de A-modules dont le noyau contient IM donc se factorise en un morphisme de A-modules $M/IM \to (A/I) \otimes_A M$. Par construction, f et g sont inverses l'une de l'autre. On a donc montré qu'on avait un isomophisme de A-modules canoniques

$$(A/I) \otimes_A M \tilde{\to} M/IM.$$

Exemple 13.3.2.1. Soit A un anneau principal, $a, b \in A$ des éléments premiers entre eux et M un A-module tel que $aM = 0$. Par Bézout on a alors $bM = M$ donc $(A/b) \otimes_A M = 0$. Par exemple si $p \neq q$ sont deux nombres premiers, $\mathbb{Z}/p \otimes_{\mathbb{Z}} \mathbb{Z}/q = 0$.

13.3.2.2 Extension des scalaires par une localisation

Soit $S \subset A$ une partie multiplicative et M un A-module. Munissons le produit cartésien $S \times M$ de la relation $\sim$ définie par $(s, m) \sim (s', m')$ s'il existe $s'' \in S$ tel que $s''(s'm - sm') = 0$.

On vérifie que $\sim$ est une relation d'équivalence. On remarquera que si M est sans S-torsion, on peut, dans la définition de $\sim$, simplifier par s'' et la relation $\sim$ devient simplement $(s, m), (s', m') \in S \times M$, $(s, m) \sim (s', m')$ si $s'm - sm' = 0$. Mais on prendra garde que si S a de la S-torsion, la relation $(s, m) \sim (s', m')$ si $s'm - sm' = 0$ n'est pas transitive donc ne définit pas une relation d'équivalence.

On note $S^{-1}M := S \times M/\sim$ et

$$\begin{array}{rccc} -/- : & S \times M & \to & S^{-1}M \\ & (s, m) & \to & m/s \end{array}$$

la projection canonique.

On vérifie que les applications

$$\begin{array}{rccc} + : S^{-1}M \times S^{-1}M & \to & S^{-1}M \\ (m/s, n/t) & \to & (tm + sn)/(st) \end{array} \quad , \quad \begin{array}{rccc} \cdot : S^{-1}A \times S^{-1}M & \to & S^{-1}M \\ (a/s, n/t) & \to & (an)/(st) \end{array}$$

munissent $S^{-1}M$ d'une structure de $S^{-1}A$-module et que l'application canonique $\iota_S := -/1 : M \to (\iota_S)_* S^{-1}M$ est un morphisme de A-modules de noyau $\ker(\iota_S) = \{m \in M \mid \exists s \in S \text{ tel que } sm = 0\}$.

Lemme 13.3.2.3 (Propriété universelle de la localisation des A-modules)**.** *Pour toute partie multiplicative $S \subset A\backslash\{0\}$ et pour tout A-module M il existe un $S^{-1}A$-module L et un morphisme de A-modules $\iota_S : M \to (\iota_S)_*L$ tel que pour tout $S^{-1}A$-module N et pour tout morphisme de A-module $f : M \to N$, il existe un unique morphisme de $S^{-1}A$-modules $\tilde{f} : L \to N$ tel que $f = \tilde{f} \circ \iota_S$.*

Démonstration. On vérifie que $\iota_S := -/1 : M \to (\iota_S)_*S^{-1}M$ convient... □

En particulier, pour tout morphisme de A-modules $f : M \to N$, en appliquant la propriété universelle de $\iota_S : M \to S^{-1}M$ au morphisme de A-modules $M \xrightarrow{f} N \xrightarrow{\iota_S} S^{-1}N$ on obtient un morphisme de $S^{-1}A$-modules $S^{-1}f : S^{-1}M \to S^{-1}N$ donné explicitement par $f(m/s) = f(m)/s$, $s \in S$, $m \in M$.

On peut réécrire le Lemme en disant que pour tout $S^{-1}A$-module N l'application canonique

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}M, (\iota_S)_*N) \to \mathrm{Hom}_A(M, N),\ \phi \to (\phi \circ \iota_S)$$

est bijective. Or **??** dit que le morphisme de A-modules $\iota : M \to (\iota_S)_*(S^{-1}A \otimes_A M)$, $m \to 1/1 \otimes m$ vérifie la même propriété. Par unicité des objets universels, on a donc un unique morphisme de $S^{-1}A$-modules $\phi : S^{-1}A \otimes M \to S^{-1}M$ tel que $\phi \circ \iota = \iota_S$. Là encore, on peut aussi démontrer cela 'à la main'.

L'application canonique

$$\begin{array}{lll} S^{-1}A \times M & \to & S^{-1}M \\ (a/s, m) & \to & (am)/s (= a(m/s) \end{array}$$

est bien définie et 2-A-linéaire donc se factorise en un morphisme de A-modules $f : S^{-1}A \otimes_A M \to S^{-1}M$ qui est, automatiquement, un morphisme de $S^{-1}A$-modules. Inversement, l'application $S\times M \to S^{-1}A\otimes_A M$, $(s, m) \to (1/s)\otimes m$ se factorise en un morphisme de $S^{-1}A$-modules $g : S^{-1}M \to S^{-1}A \otimes_A M$. Par construction, f et g sont inverses l'une de l'autre. On a donc montré qu'on avait un isomophisme de $S^{-1}A$-modules canonique

$$S^{-1}A \otimes_A M \tilde{\to} S^{-1}M.$$

Exemple. Si pour tout $m \in M$ il existe $s \in S$ tel que $sm = 0$, $S^{-1}M = 0$. Si pour tout $s \in S$ l'application $s \cdot - : M \to M$ de multiplication par s est bijective, $\iota_S : M \to S^{-1}M$ est un isomorphisme de A-modules. En particulier, si A est un anneau principal de corps des fractions K et M est un A-module de type fini, $K \otimes_A M = K^{\oplus r}$ et pour tout $\mathfrak{p} \in \mathrm{Spec}(A) \setminus \{0\}$, $A_\mathfrak{p} \otimes_A M = A_\mathfrak{p}^{\oplus r} \oplus M(\mathfrak{p})$, où on a noté $M(\mathfrak{p})$ la $\mathfrak{p}$-partie de M et r le rang de M. Par exemple $\mathbb{Q} \otimes_\mathbb{Z} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = 0$, $\mathbb{Z}_{2\mathbb{Z}} \otimes_\mathbb{Z} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, $\mathbb{Z}_{3\mathbb{Z}} \otimes_\mathbb{Z} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = \mathbb{Z}/3 \times \mathbb{Z}/3$, $\mathbb{Z}_{p\mathbb{Z}} \otimes_\mathbb{Z} (\mathbb{Z}/12 \times \mathbb{Z}/6 \times \mathbb{Z}/3) = 0$ pour $p \neq 2, 3$.

13.4 Produit tensoriel de A-algèbres

Soit $\phi : A \to B$ et $\psi : A \to C$ deux A-algèbres. Les applications produits $B \times B \to B$ et $C \times C \to C$ sont 2-A-bilinéaires donc se factorisent en des morphismes de A-modules μ_B :

$B \otimes_A B \to B$ et $\mu_C : C \otimes_A C \to C$. On en déduit une application

$$(B \otimes_A C) \otimes_A (B \otimes_A C) \tilde{\to} (B \otimes_A B) \otimes_A (C \otimes_A C) \overset{\mu_B \otimes \mu_C}{\to} B \otimes_A C$$

dont on vérifie qu'elle munit le A-module $B \otimes_A C$ d'une structure de A-algèbre telle que les applications $\iota_B : B \to B \otimes_A C$, $b \to b \otimes 1$ et $\iota_C : C \to B \otimes_A C$, $c \to 1 \otimes c$ sont des morphismes de A-algèbres.

13.4.1

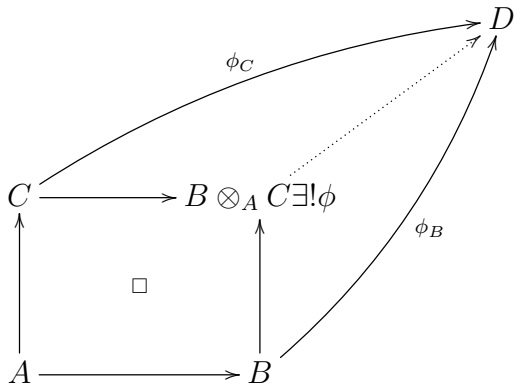
Lemme. (Propriété universelle du produit tensoriel de A-algèbres) *Pour toutes A-algèbres $A \to B$ et $A \to C$, il existe une A-algèbre T et des morphismes de A-algèbres $\iota_B : B \to T$, $\iota_C : C \to T$ tels que pour toute A-algèbre $A \to D$ et morphismes de A-algèbres $\phi_B : B \to D$, $\phi_C : C \to D$ il existe un unique morphisme de A-algèbres $\phi : T \to D$ tel que $\phi \circ \iota_B = \phi_B$ et $\phi \circ \iota_C = \phi_C$*

Démonstration. On vérifie comme d'habitude que $B \otimes_A C$ et $\iota_B : B \to B \otimes_A C$, $\iota_C : C \to B \otimes_A C$ conviennent. Si $\phi : B \otimes_A C \to D$ existe les conditions $\phi \circ \iota_B = \phi_B$ et $\phi \circ \iota_C = \phi_C$ forcent $\phi(b \otimes c) = \phi_B(b)\phi_C(c)$, d'où l'unicité de ϕ sous réserve de son existence. Considérons l'application $B \times C \to D$, $(b, c) \to \phi_B(b)\phi_C(c)$. Elle est 2-$A$-bilinéaire donc se factorise en un morphisme de A-modules $\phi : B \otimes_A C \to D$ tel que $\phi(b \otimes c) = \phi_B(b)\phi_C(c)$ et on vérifie sur la construction que c'est automatiquement un morphisme de A-algèbres. □

On peut aussi réécrire **??** en disant que pour toutes A-algèbres $A \to B$, $A \to C$ et $A \to C$ l'application canonique

$$\mathrm{Hom}_{Alg/_A}(B \otimes_A C, D) \to \mathrm{Hom}_{Alg/_A}(B, D) \times \mathrm{Hom}_{Alg/_A}(C, D),\ \phi \to (\phi \circ \iota_B, \phi \circ \iota_C)$$

est bijective ou encore, plus visuellement,



13.4.2

Exercice.

1. Soit $I, J \subset A$ deux idéaux. Montrer qu'on a un isomorphisme canonique de A-algèbres
$$(A/I) \otimes_A (A/J) \tilde{\to} A/(I+J).$$
Si A est un anneau principal et $a, b \in A$, calculer $(A/a) \otimes_A (A/b)$.
2. Montrer qu'on a un isomorphisme canonique de A-algèbres $A[X_1] \otimes_A \cdots \otimes_A A[X_n] \tilde{\to} A[X_1, \ldots, X_n]$.
3. Si $\varphi : A \to B$ est un morphisme d'anneaux et $P \in A[X]$, montrer qu'on a un isomorphisme canonique de B-algèbres
$$B \otimes_A (A[X]/P) \tilde{\to} B[X]/\varphi(P)$$
(on note encore $\varphi : A[X] \to B[X]$ le morphisme obtenu en appliquant φ aux coefficients). Calculer $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Est-ce un corps ? Même question avec $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$.

Remarque. On notera les similitudes suivantes au niveau des propriétés universelles.

	A-modules	A-algèbres
Objets libres de rang fini	$A^{\oplus n}$	$A[X_1, \ldots, X_n]$
Coproduits finis	$\oplus_{1 \leq i \leq n} M_i$	$A_1 \otimes_A \cdots \otimes_A A_n$
Produit	$\prod_{i \in I} M_i$	$\prod_{i \in I} A_i$

Troisième partie

Extensions de corps et théorie de Galois

Préliminaires

Dans cette partie du cours, sauf mention explicite du contraire, tous les anneaux considérés sont commutatifs. On rappelle qu'un corps (commutatif) est un anneau (commutatif) dont tous les éléments non nuls sont inversibles. On a vu dans les chapitres précédents un certain nombre de techniques pour construire des corps intéressants. Par exemple,

— Si A est un anneau intègre, $\mathrm{Frac}(A)$ est un corps.
Exemples : $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$, si k est un corps, $k(T_1, \dots, T_r) = \mathrm{Frac}(k[T_1, \dots, T_r])$, etc.

— Si k est un corps muni d'une valeur absolue *i.e.* d'une application $|-| : k \to \mathbb{R}_{\geq 0}$ vérifiant :
  — $|x| = 0$ si et seulement si $x = 0$,
  — $|xy| = |x||y|$,
  — $|x + y| \leq |x| + l|y|$,

  alors l'ensemble $\mathrm{Cau}(k) \subset k^{\mathbb{N}}$ des suites de Cauchy de $(k, |-|)$ est une sous-k-algèbre et on vérifie facilement que le sous-ensemble $\mathrm{Cau}_0(k) \subset \mathrm{Cau}(k)$ des suites de Cauchy qui convergent vers 0 est un idéal maximal. On dit que $\widehat{k} := \widehat{k^{|-|}} := Cau(k)/Cau_0(k)$ est le complété de k par rapport à la valeur absolue $|-|$. Par exemple, sur $\mathbb{Q}$, on peut considérer
  — la valeur absolue usuelle $|x| = x$ si $x \geq 0$, $|x| = -x$ si $x < 0$. On obtient ainsi le corps des réels $\mathbb{R} = \widehat{\mathbb{Q}^{|-|}}$;
  — pour chaque nombre premier $p > 0$, la valeur absolue p-adique $|x|_p = p^{-v_p(x)}$. On obtient ainsi le corps des nombres p-adiques $\mathbb{Q}_p = \widehat{\mathbb{Q}^{|-|_p}}$;

— Si $\mathfrak{m} \subset A$ est un idéal maximal, $A/\mathfrak{m}$ est un corps.
Exemple : si A est un anneau principal et p un élément irréductible, A/p est un corps : $\mathbb{F}_p = \mathbb{Z}/p$, $\mathbb{C} = \mathbb{R}[T]/(T^2 + 1)$, $\mathbb{Q}[T]/(T^p + T^{p-1} + \cdots + 1)$, p premier, etc.

— Si $\mathfrak{p} \subset A$ est un idéal premier, $A_{\mathfrak{p}}$ est un anneau local d'unique idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$ donc $\kappa(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ est un corps, etc.

Chapitre 14

Extensions algébriques, extensions transcendantes

Définition 14.0.0.1. Soient k, K deux corps. On dit que K est une extension de k (ou une k-extension, ou encore que k est un sous-corps de K) si K est une k-algèbre *i.e.* s'il existe un morphisme d'anneaux $\phi : k \to K$

Remarque 14.0.0.1. Ce morphisme est alors automatiquement injectif, ce qui justifie la terminologie « extension / sous-corps » et le fait que, dans la suite, on notera presque toujours $k \subset K$ ou K/k au lieu de $\phi : k \to K$, identifiant implicitement k et son image $\phi(k) \subset K$.
Un morphisme de k-extensions $K/k \to K'/k$ est, par définition, un morphisme de k-algèbres. Un morphisme de k-extensions est automatiquement injectif et on dit parfois que c'est un k-plongement.

14.1 Degré d'une extension

Définition 14.1.0.1. Si K/k est une extension de corps, on appelle degré de K/k, et l'on note $[K : k]$ la dimension de K comme espace vectoriel sur k (avec la convention que si K n'est pas de dimension finie sur k, $[K : k] = +\infty$).

Avec la convention $+\infty \cdot +\infty = +\infty$, on a

Lemme 14.1.0.1. *Si K_3/K_2 et K_2/K_1 sont des extensions de corps, $[K_3 : K_1] = [K_3 : K_2][K_2 : K_1]$.*

Démonstration. Il suffit d'observer que si e_i^3, $i \in I_3$ est une K_2-base de K_3 et e_i^2, $i \in I_2$ est une K_1-base de K_2 alors $e_{i_2}^3 e_{i_3}^2$, $i_2 \in I_2$, $i_3 \in I_3$ est une K_1-base de K_3. □

14.2 Éléments algébriques, éléments transcendants

Soit $k \subset K$ un sous-corps. On rappelle que si $\mathscr{S} \subset K$ est un sous-ensemble, on a noté $k[\mathscr{S}] \subset K$ la plus petite sous-k-algèbre de K contenant $\mathscr{S}$ et que c'est aussi l'image de l'unique

morphisme de k-algèbre $k[T_x,\ x \in \mathscr{S}] \to K$, $T_x \mapsto x$.

14.2.1 Sous-corps engendré par une partie

Si $k \subset K_i \subset K$, $i \in I$ sont des sous-corps contenant k, on vérifie immédiatement que $k \subset \cap_{i\in I} K_i \subset K$ est encore un sous-corps contenant k. Il existe donc une unique sous-corps $k \subset k(\mathscr{S}) \subset K$ contenant k, $\mathscr{S}$ et minimal pour l'inclusion.

Définition 14.2.1.1. On dit que $k \subset k(\mathscr{S}) \subset K$ est la sous-k-extension de $k \subset K$ engendrée par $\mathscr{S}$. Explicitement, $k(\mathscr{S})$ est l'intersection de toutes les sous-corps $k \subset K' \subset K$ tels que $\mathscr{S} \subset K'$.
Si $K = k(\mathscr{S})$ on dit que $\mathscr{S}$ est un système de générateurs de K comme extension de corps de k (ou que K est engendré par $\mathscr{S}$ comme extension de corps de k). Si on peut prendre $\mathscr{S}$ fini, on dit que K est une extension de corps de type fini de k.

Comme $k[\mathscr{S}] \subset k(\mathscr{S})$ et $k(\mathscr{S})$ est un corps, la propriété universelle du corps des fractions d'un anneau intègre montre qu'on a $k \subset k[\mathscr{S}] \subset \mathrm{Frac}(k[\mathscr{S}]) \subset k(\mathscr{S}) \subset K$ et, comme $\mathscr{S} \subset \mathrm{Frac}(k[\mathscr{S}])$, la minimalité de $k(\mathscr{S})$ assure que $\mathrm{Frac}(k[\mathscr{S}]) = k(\mathscr{S})$.

14.2.2 Alternative algébrique/transcendant

Soit K/k une extension de corps, $x \in K$ et $\mathrm{ev}_x : k[X] \twoheadrightarrow k[x]$ l'unique morphisme de k-algèbres tel que $\mathrm{ev}_x(X) = x$

Lemme 14.2.2.1. *On a l'alternative suivante.*
1. *Soit* $\mathrm{ev}_x : k[X] \xrightarrow{\sim} k[x]$ *est un isomorphisme de k-algèbres et le morphisme*

$$k[X] \xrightarrow{ev_x}_{\sim} k[x] \hookrightarrow k(x)$$

   se localise en un isomorphisme de corps $k(X) \xrightarrow{\sim} k(x)$. En particulier $k[x]$ (donc a fortiori $k(x)$) est de dimension infinie sur k.
2. *Soit il existe un unique polynôme irréductible unitaire $P_x \in k[X]$ tel que* $\ker(ev_x) = k[X]P_x$ *et le morphisme de k-algèbres* $\mathrm{ev}_x : k[X] \twoheadrightarrow k[x]$ *se factorise en un isomorphisme $k[X]/(P_x) \xrightarrow{\sim} k[x]$. En particulier $k[x] = k(x)$ et $k(x)$ est de dimension finie sur k, égale au degré de P_x.*

Définition 14.2.2.1. Dans le cas (1), on dit que $x \in K$ est *transcendant sur k* et dans le cas (2) que $x \in K$ est *algébrique* sur k de degré $[k(x) : k] = \deg(P_x)$ et que P_x est le polynôme irréductible (unitaire) de x sur k.

Démonstration. Si $\ker(\mathrm{ev}_x) = 0$ on est dans le cas (1) et les assertions sont immédiates.
Si $\ker(\mathrm{ev}_x) \neq 0$, comme $k[X]$ est principal, il existe un unique polynôme unitaire P_x tel que

$\ker(\mathrm{ev}_x) = k[X]P_x$ et le morphisme de k-algèbres $\mathrm{ev}_x : k[X] \twoheadrightarrow k[x]$ se factorise en un isomorphisme $k[X]/P_x \tilde{\to} k[x]$. Comme $k[x] \subset K$ est un sous-anneau d'un corps, il est intègre donc P_x est premier. Comme $k[X]$ est principal, tout idéal premier est maximal, donc $k[x] \subset K$ est un sous-corps de K. Comme $k[x]$ contient k et x, c'est nécessairement $k(x)$. Il reste à voir que $k[X]/P_x$ est de dimension le degré d de P_x sur k. Mais en utilisant la division euclidienne de $k[X]$, on voit immédiatement que les classes de $1, X, \ldots, X^{d-1}$ forment une k-base de $k[X]/P_x$. □

Remarque 14.2.2.1. On retiendra en particulier que si $x \in K$

$$\begin{array}{rcccl} x \text{ est algébrique sur } k & \Leftrightarrow & [k(x):k] < +\infty & \Leftrightarrow & k[x] = k(x)\,; \\ x \text{ est transcendant sur } k & \Leftrightarrow & [k(x):k] = +\infty & \Leftrightarrow & k[x] \subsetneq k(x)\,; \end{array}$$

Exemple 14.2.2.1. Considérons l'extension $\mathbb{C}/\mathbb{Q}$. Les nombres $i, \sqrt{2}$ *etc* sont algébriques par définition.

- Si $a \in \mathbb{C}$ est algébrique, $\exp(a)$ est transcendant (Lindemann, $\sim$ 1880) ; en particulier, e ($a = 1$) et π ($a = i\pi$) sont transcendants sur $\mathbb{Q}$.
- Si $a, b \in \mathbb{C}$ sont algébriques sur $\mathbb{Q}$ et $a \neq 0, 1$, $b \notin \mathbb{Q}$, $a^b = \exp(b \log a)$ est transcendant sur $\mathbb{Q}$ (septième problème de Hilbert, Gelfond, $\sim$ 1930) ; en particulier, e^π ($a = e^\pi$, $b = i$) est transcendant sur $\mathbb{Q}$.
- On ne sait pas si $e+\pi$ est transcendant. Il est par contre possible que d'ici la fin de l'année (2020), on sache que si $a, b \in \mathbb{C}$ sont algébriques sur $\mathbb{Q}$, $\exp(a)\log(b)$ soit transcendant sur $\mathbb{Q}$.

En fait, sauf cas très particulier, on ne sait pas dire si un nombre complexe pris « au hasard » est transcendant sur $\mathbb{Q}$ alors que moralement, « presque tous » les nombres complexes sont transcendants sur $\mathbb{Q}$ puisque $\mathbb{Q}$ est dénombrable alors que $\mathbb{R}$ (donc $\mathbb{C}$) n'est pas dénombrable.

14.2.3 Indépendance algébrique

Définition 14.2.3.1. Soit K/k une extension de corps.
On dit que les éléments $a_i \in K$, $i \in I$ sont algébriquement indépendants sur k si pour tout sous-ensemble fini $J \subset I$, l'unique morphisme de k-algèbre $\psi : k[X_j,\ j \in J] \to K$ tel que $psi(X_j) = a_j$, $j \in J$ est injectif. Dans le cas contraire, on dit que les $a_i \in K$, $i \in I$ sont algébriquement liés sur k.

Remarque 14.2.3.1. Pour $|I| = 1$, on retrouve la notion d'élément transcendant sur k.

Exemple 14.2.3.1. Considérons encore l'extension $\mathbb{C}/\mathbb{Q}$. On en sait encore moins sur l'indépendance algébrique que sur l'alternative algébrique/transcendant. Le seul résultat un peu général dont on dispose est que si $a_1, \ldots, a_n \in \mathbb{C}$ sont algébriques et linéairement indépendants sur $\mathbb{Q}$, les $\exp(a_1), \ldots, \exp(a_n)$ sont algébriquement indépendants sur $\mathbb{Q}$ (Lindeman-Weierstrass, $\sim$ 1885).

Définition 14.2.3.2. On dit qu'une extension de corps K/k est *transcendante pure* s'il existe $a_i \in K$, $i \in I$ algébriquement indépendants sur k tels que $K = k(a_i,\ i \in I)$.

Le lemme suivant résulte immédiatement de la définition.

Lemme 14.2.3.1. *Soit K_3/K_2 et K_2/K_1 des extensions de corps. Si K_3/K_2 et K_2/K_1 sont transcendantes pures alors K_3/K_1 est transcendante pure.*

Remarque 14.2.3.2. La réciproque n'est pas vraie en général mais ce n'est pas évident. En fait, toute sous-extension de $k(X)/k$ est encore transcendante pure (Luroth $\sim$ 1875). Si k est de caractéristique 0, toute sous-extension de $k(X_1, X_2/k$ est encore transcendante pure (Castelnuovo $\sim$ 1940) mais ce n'est plus vrai si k est de caractéristique $p > 0$ (Zariski $\sim$ 1958) ou si $n \geq 3$ (Clemens-Griffith $\sim$ 1972).

Exemple 14.2.3.2. L'extension $k(T)[X]/\langle X^2 - T\rangle/k$ est transcendante pure par contre, l'extension $k[X, Y]/\langle Y^2 - X^3 - X - 1\rangle/k$ ne l'est pas.

Définition 14.2.3.3. On dit qu'une extension de corps K/k est *finie* si $[K : k] < +\infty$ et que K/k est algébrique si tout $a \in K$ est algébrique sur k.

Lemme 14.2.3.2. *Soit K/k une extension de corps. Alors K/k est finie si et seulement si K/k est algébrique et de type fini.*

Démonstration. L'implication $\Rightarrow$ est immédiate. Pour l'implication $\Leftarrow$, écrivons $K = k(a_1, \ldots, a_n)$. Pour chaque $i = 1, \ldots, n$, $a_i \in K$ est algébrique sur k donc a fortiori sur $k(a_1, \ldots, a_{i-1})$; en particulier, $[k(a_1, \ldots, a_{i-1})(a_i) : k(a_1, \ldots, a_{i-1}] < +\infty$. Et donc, par **??** on a

$$[K : k] = \prod_{1 \leq i \leq n} [k(a_1, \ldots, a_i) : k(a_1, \ldots, a_{i-1})] < +\infty.$$

□

14.2.3.0.1 Lemme. *Soit K_3/K_2 et K_2/K_1 des extensions de corps.*
1. *K_3/K_1 est finie si et seulement si K_2/K_1 et K_1/K_3 sont finies, auquel cas on a $[K_3 : K_1] = [K_3 : K_2][K_2 : K_1]$.*
2. *K_3/K_1 est algébrique si et seulement si K_2/K_1 et K_1/K_3 sont algébriques.*

Démonstration. Les implications $\Rightarrow$ sont immédiates. L'implication $\Leftarrow$ de (1) résulte de **??**. Pour l'implication $\Leftarrow$ de (2), fixons $a \in K_3$ et montrons que a est algébrique sur K_1. Comme a est algébrique sur K_2, en écrivant son polynôme minimal sous la forme $P_a = T^d + \sum_{0 \leq i \leq d-1} a_i T^i \in K_2[T]$, on voit que a est aussi algébrique sur le sous-corps $K_1(a_0, \ldots, a_d)$ de K_2 *i.e* $[K_1(a_0, \ldots, a_d, a) : K_1(a_0, \ldots, a_d)] < +\infty$. Mais comme $K_1(a_0, \ldots, a_d)/K_1$ est algébrique de type fini, elle est finie par **??** donc

$$[K_1(a) : K_1] \leq [K_1(a_0, \ldots, a_d, a) : K_1] = [K_1(a_0, \ldots, a_d, a) : K_1(a_0, \ldots, a_d)][K_1(a_0, \ldots, a_d) : K_1] < +\infty.$$

□

Corollaire. *Soit K/k une extension de corps. Alors l'ensemble $\overline{k^K} \subset K$ des $a \in K$ algébrique sur k est un sous-corps de K contenant k.*

Démonstration. La partie non triviale de l'énoncé est l'affirmation que $\overline{k^K} \subset K$ est un sous-corps. Soit donc $a \in \overline{k^K}$, $0 \neq b \in \overline{k^K}$. On a $a-b, ab^{-1} \in k(a,b) \subset K$ donc

$$[k(a-b):k], [k(ab^{-1}):k] \leq [k(a,b):k] \leq [k(a)(b):k(a)][k(a):k] \leq [k(b):k][k(a):k] < +\infty$$

i.e. $a-b, ab^{-1} \in \overline{k} \cap K$ (de degré sur $k \leq [k(b):k][k(a):k]$). □

Exercice. Notons $\overline{\mathbb{Q}} := \overline{\mathbb{Q}^{\mathbb{C}}} \subset \mathbb{C}$. Montrer que $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$ et que tout élément de $\mathbb{C} \setminus \overline{\mathbb{Q}}$ est transcendant sur $\overline{\mathbb{Q}}$ mais que $\overline{\mathbb{Q}} \subset \mathbb{C}$ n'est pas une extension transcendante pure.

D'après **??**, une extension de corps est finie si et seulement si elle est algébrique et de type fini. Si $k \subset K$ est finie et si $a_1, \ldots, a_n K = k(a_1, \ldots, a_n)$ est un système de générateurs de K comme extension de corps de k, **??** montre que $K = k(a_1, \ldots, a_n) = k(a_1) \cdots (a_n) = k[a_1] \cdots [a_n] = k[a_1, \ldots, a_n]$ donc K est aussi une k-algèbre de type fini. Cette dernière propriété suffit en fait à caractériser les extensions finies ; c'est le Théorème des zéros de Hilbert ou Nullstellensatz.

14.3 Nullstellensatz

14.3.1

Proposition. (Nullstellensatz) *Soit K/k une extension de corps. Si K est une k-algèbre de type fini alors K est une extension finie de k.*

Démonstration. Commençons par observer que le corps des fractions $k(X)$ de l'anneau des polynômes à une indéterminée sur k n'est pas une k-algèbre de type fini. Sinon, on aurait $k(X) = k[a_1, \ldots, a_n]$ où $a_i = P_i/Q_i$ avec $0 \neq P_i, Q_i \in k[X]$, $i = 1, \ldots, n$. Posons $Q := Q_1, \ldots Q_n \in k[X]$. Par construction $k(X) \subset k[X]_Q$. Mais si $P \in k[X]$ est premier avec Q, $1/P \notin k[X]_Q$: contradiction.

On procède par récurrence sur le nombre n de générateurs de K comme k-algèbre. Plus précisément, pour tout $n \geq 0$ considérons l'assertion suivante

H(n) Pour tout corps k, toute k-algèbre $K = k[a_1, \ldots, a_n]$ qui est un corps est une extension finie de k

— H(0) est trivialement vraie.
— Supposons maintenant $n \geq 2$ et soit $K = k[a_1, \ldots, a_n]$ un corps. Comme K est un corps, on a $K = k[a_1, \ldots, a_n] = k(a_1)[a_2, \ldots, a_n]$ et H(n-1) assure que $[K : k(a_1)] < +\infty$. Il suffit donc de montrer que $[k(a_1) : k] < +\infty$ *i.e.* **??** que $a_1 \in K$ est algébrique sur k. Choisissons une $k(a_1)$-base $b_1, \ldots, b_r$ de K. Écrivons $a_i = \sum_{1 \leq j \leq r} x_{i,j} b_j$ avec $x_{i,j} \in k(a_1)$, $1 \leq i \leq n$, $1 \leq j \leq r$, $b_i b_j = \sum_{1 \leq k \leq r} x_{i,j,k} b_k$ avec $x_{i,j,k} \in k(a_1)$, $1 \leq i, j, k \leq r$ et introduisons la sous-k-algèbre

$$A := k[x_{i,j}, 1 \leq i \leq n,\ 1 \leq j \leq r, x_{i,j,k},\ 1 \leq i, j, k \leq r] \subset K.$$

Comme $K = k[a_1, \ldots, a_n]$ on a $K = \oplus_{1 \leq i \leq r} Ab_i$ donc

$$K = \oplus_{1 \leq i \leq r} k(a_1)b_i \subset \oplus_{1 \leq i \leq r} Ab_i \subset \oplus_{1 \leq i \leq r} k(a_1)b_i,$$

ce qui impose $k(a_1) = A$ et contredit notre observation préliminaire.

□

14.3.2

Corollaire. *Soit A une k-algèbre de type fini. Pour tout $\mathfrak{m} \in \mathrm{spm}(A)$, $A/\mathfrak{m}$ est une extension finie de k.*

Exemple. En particulier, si $k = \mathbb{C}$, **??**.3 (3) montre que pour tout $\mathfrak{m} \in \mathrm{spm}(A)$, $A/\mathfrak{m} = \mathbb{C}$. Rappelons qu'une sous-variété algébrique affine de $\mathbb{C}^n$ est par définition un sous-ensemble V de $\mathbb{C}^n$ de la forme

$$V = V(I) = \{\underline{x} \in \mathbb{C}^n \mid P(\underline{x}) = 0,\ P \in I\}.$$

Notons $\mathbb{C}[V] := C[X_1, \ldots, X_n]/I$. Les propriétés universelles de la $\mathbb{C}$-algèbre des polynômes à n indéterminées et du quotient donnent une bijection canonique

$$V \tilde{\to} \mathrm{Hom}_{Alg/\mathbb{C}}(\mathbb{C}[V], \mathbb{C})$$

et le Corollaire **??**, une bijection canonique

$$\mathrm{Hom}_{Alg/\mathbb{C}}(\mathbb{C}[V], \mathbb{C}) \tilde{\to} \mathrm{spm}(\mathbb{C}[V]).$$

La composée $V \tilde{\to} \mathrm{spm}(\mathbb{C}[V])$ est donnée explicitement par $\underline{x} \to \ker(ev_{\underline{x}} : \mathbb{C}[X_1, \ldots, X_n] \to \mathbb{C})/I$. En particulier, comme $\mathbb{C}[V]$ est noethérien, $\mathrm{spm}(\mathbb{C}[V]) \neq \varnothing$. Cela montre qu'une sous-variété algébrique affine de $\mathbb{C}^n$ a toujours un point. En particulier, les idéaux maximaux de $\mathbb{C}[X_1, \ldots, X_n]$ sont exactement les $\sum_{1 \leq i \leq n} \mathbb{C}[X_1, \ldots, X_n](X_i - x_i)$, $\underline{x} \in \mathbb{C}^n$.

14.3.3

Corollaire. *Soit A une k-algèbre de type fini. Alors pour tout idéal $I \subset A$, $\sqrt{I} = \bigcap_{\mathfrak{m} \in \mathrm{spm}(A),\ I \subset \mathfrak{m}} \mathfrak{m}$.*

Démonstration. On peut réécrire le lemme sous la forme $\sqrt{\{0\}} = \mathcal{J}_{A/I}$. Il suffit donc de montrer que si A est une k-algèbre de type fini alors $\mathcal{J}_A \subset \sqrt{\{0\}}$ ou encore $A \setminus \sqrt{\{0\}} \subset A \setminus \mathcal{J}_A$. Soit donc $a \in \setminus\sqrt{\{0\}}$. Il faut montrer qu'il existe un idéal maximal de A qui ne contient pas a. Un tel idéal induit un idéal premier $\mathfrak{m}A_a$. Cela amène naturellement à considérer le morphisme de localisation $c_a : A \to A_a$.

— **Lemme 1.** *A_a est une k-algèbre de type fini.*

Démonstration. Par la propriété universelle de $A \to A[T]$, on a un unique morphisme de A-algèbres $ev_{1/a} : A[T] \to A_a$ tel que $ev_{1/a}(T) = 1/a$. Par construction, $(Ta - 1)A[T] \subset \ker(ev_{1/a})$, d'où une factorisation $\phi := \overline{ev}_{1/a} : A[T]/(Ta - 1) \to A_a$. Inversement, par la

propriété universelle de $A \to A_a$, le morphisme canonique $A \xrightarrow{\iota_A} A[T] \twoheadrightarrow A[T]/(Ta-1)$ se factorise en un morphisme $\psi : A_a \to A[T]/(Ta-1)$ et on vérifie sur les constructions que $\phi : A[T]/(Ta-1) \to A_a$, $\psi : A_a \to A[T]/(Ta-1)$ sont inverses l'un de l'autre. □

— **Lemme 2.** *Toute k-agèbre intègre de k-dimension finie est un corps.*

Démonstration. Soit A une k-agèbre intègre de k-dimension finie et $0 \neq a \in A$. La multiplication par a induit un morphisme $\mu_a : A \to A$ de k-espaces vectoriels qui est est injectif puisque A est intègre donc bijectif puisque A est de k-dimension finie. En particulier, il existe $b \in A$ tel que $ab = \mu_a(b) = 1$. □

— Fin de la preuve. D'après le Lemme 1, A_a est encore une k-algèbre de type fini. Soit $\mathfrak{m} \in \mathrm{spm}(A_a)$. Alors $\mathfrak{p} := c_a^{-1}(\mathfrak{m}) \in \mathrm{Spec}(A)$ et $a \notin \mathfrak{p}$. De plus, on a des morphismes d'anneaux injectifs $k \hookrightarrow A/\mathfrak{p} \hookrightarrow A_a/\mathfrak{m}$. Par **??**, $A_a/\mathfrak{m}$ est une extension finie de k. Donc par le Lemme 2, $A/\mathfrak{p}$ est un corps *i.e.* $\mathfrak{p} \in \mathrm{spm}(A)$.

□

Exemple. Reprenons les notations de l'Exemple **??**. Considérons le morphisme de $\mathbb{C}$-algèbres canonique $-|_V : \mathbb{C}[X_1, \ldots, X_n] \to \mathbb{C}^V$ qui envoie $P \in \mathbb{C}[X_1, \ldots, X_n]$ sur l'application $ev_-(P)|_V : V \to \mathbb{C}$, $\underline{x} \to ev_{\underline{x}}(P) = P(\underline{x})$. On a clairement $I \subset I(V) := \ker(-|_V)$ et le Corollaire **??** montre qu'en fait $I = \ker(-|_V)$ (rappelons qu'on a supposé $I = \sqrt{I}$). Le morphisme de $\mathbb{C}$-algèbre $-|_V : \mathbb{C}[X_1, \ldots, X_n] \to \mathbb{C}^V$ se factorise donc en un morphisme injectif $\mathbb{C}[V] \hookrightarrow \mathbb{C}^V$; on dit que $\mathbb{C}[V]$ est la $\mathbb{C}$-algèbre des applications polynômiales sur V. On en déduit aussi que les applications $I \to V(I)$ et $V \to I(V)$ sont des bijections inverses l'une de l'autres entre l'ensemble des idéaux radiciels de $\mathbb{C}[X_1, \ldots, X_n]$ et les sous-variétés algébriques affines de $\mathbb{C}^n$.

14.4 Bases de transcendance, degré de transcendance

Soit K/k une extension de corps. Une *base de transcendance* de K/k est une famille $a_i \in K$, $i \in I$ d'éléments algébriquement indépendants sur k tels que $K/k(a_i, i \in I)$ est algébrique.

14.4.1

[Utilise le Lemme de Zorn] **Proposition.** *Les bases de transcendance existent et ont même cardinal.*

On rappelle que deux ensembles A, B ont même cardinal (notation : $|A| = |B|$) s'il existe une application bijective $A \tilde{\to} B$. On note $|A| \leq |B|$ s'il existe une application injective $A \hookrightarrow B$ et $|A| < |B|$ si $|A| \leq |B|$ et $|A| \neq |B|$. En utilisant l'axiome du choix, on peut montrer que si A et B sont deux ensembles alors on a toujours $|A| \leq |B|$ ou $|B| \leq |A|$. En fait on a même soit $|A| < |B|$ ou $|A| = |B|$ ou $|B| < |A|$ (trichotomie). Cela résulte de ce qu'on vient de dire combiné au lemme de Schröder-Bernstein.

Exercice. (Schröder-Bernstein) *Montrer que si $|A| \leq |B|$ et $|B| \leq |A|$ alors $|A| = |B|$.*

Démonstration. Montrons d'abord que si $\mathcal{L} \subset K$ est algébriquement indépendant sur k et $\mathcal{G} \subset K$ est un système de générateurs de $k \subset K$ tel que $\mathcal{L} \subset \mathcal{G} \subset K$, il existe une base de transcendance $\mathcal{L} \subset \mathcal{B} \subset \mathcal{G}$. En effet, l'ensemble $\mathcal{E}$ des sous-ensembles $\mathcal{L} \subset \mathcal{U} \subset \mathcal{G}$, algébriquement indépendants sur k est non vide (il contient $\mathcal{L}$) et ordonné inductif pour $\subset$. Par le Lemme de Zorn, il admet donc un élément $\mathcal{B}$ maximal pour $\subset$. La maximalité de $\mathcal{B}$ impose que $K/k(\mathcal{B})$ est algébrique. En effet, s'il existait $x \in K$ transcendant sur $k(\mathcal{B})$, en écrivant $x = y/z$ avec $y, z \in k[\mathcal{G}]$, on voit qu'il existerait forcément un élément $g \in \mathcal{G}$ transcendant sur $k(\mathcal{B})$ donc tel que $\mathcal{B} \cup \{g\} \in \mathcal{E}$: contradiction.
Soit maintenant $\mathcal{B}, \mathcal{B}'$ deux bases de transcendance. Supposons $|\mathcal{B}'| \leq |\mathcal{B}|$. Pour chaque $b' \in \mathcal{B}'$ il existe une sous-ensemble fini $\mathcal{B}_{b'} \subset \mathcal{B}$ tel que b' est algébrique sur $k(\mathcal{B}_{b'})$. Notons

$$\mathcal{B}'' := \bigcup_{b' \in \mathcal{B}'} \mathcal{B}_{b'} \subset \mathcal{B}.$$

On a en fait $\mathcal{B}'' = \mathcal{B}$. En effet, s'il existait $b \in \mathcal{B} \setminus \mathcal{B}''$, comme b est algébrique sur $k(\mathcal{B}')$ et $k(\mathcal{B}')$ est algébrique sur $k(\mathcal{B}'')$, b est algébrique sur $k(\mathcal{B}'')$ **??** (2) : contradiction. Cela montre déjà que $\mathcal{B}'$ est fini si et seulement si $\mathcal{B}$ est fini. Supposons d'abord $\mathcal{B}, \mathcal{B}'$ infinis. On a alors $|\mathcal{B}| \leq |\mathcal{B}'|$ (quitte à remplacer $\mathcal{B}'$ et les $\mathcal{B}_{b'}$ par des sous-ensembles, on peut supposer que les $\mathcal{B}_{b'}$ sont tous disjoints et l'assertion est alors immédiate) et la conclusion résulte de Schröder-Bernstein. Supposons donc $\mathcal{B}, \mathcal{B}'$ finis et procédons par réccurence sur $m := |\mathcal{B}'| \leq n := |\mathcal{B}|$. Si $m = 0$, $k \subset K$ est algébrique donc $n = 0$. Si $m > 0$, écrivons $\mathcal{B}' = \{b'_1, \ldots, b'_m\}$, $\mathcal{B} = \{b_1, \ldots, b_n\}$. Comme b'_1 est algébrique sur $k(\mathcal{B})$ et transcendant sur k, il existe $P \in k[X, Y_1, \ldots, Y_n]$ irréductible et vérifiant $P(b'_1, b_1, \ldots, b_n) = 0$ avec X et au moins l'un des Y_i - disons Y_1 - qui apparaissent dans l'expression de P ; en particulier, b_1 est algébrique sur $k(b'_1, b_2, \ldots, b_n)$. Considérons $\mathcal{B}'' := \{b'_1, b_2, \ldots, b_n\}$ (on a échangé b_1 et b'_1) et montrons que c'est encore une base de transcendance de $k \subset K$. En effet, d'une part $K/k(\mathcal{B}'', b_1)$ et $k(\mathcal{B}'', b_1)/k(\mathcal{B}'')$ sont algébrique donc $K/k(\mathcal{B}'')$ est algébrique **??** (2). D'autre par, s'il existait $P \in k[X, Y_2, \ldots, Y_n]$ irréductible tel que $P(b'_1, b_2, \ldots, b_n) = 0$, comme $b_2, \ldots, b_n$ sont algébriquement indépendants sur k, X apparait dans l'expression de P donc b'_1 est algébrique sur $k(b_2, \ldots, b_n)$ et donc b_1 aussi : contradiction. On a donc deux bases de transcendance $\mathcal{B}'$ et $\mathcal{B}''$ de $k \subset K$ qui contiennent b'_1 ; on vérifie immédiatement sur la définition que $\mathcal{B}' \setminus \{b'_1\}$, $\mathcal{B}'' \setminus \{b'_1\}$ sont alors des bases de transcendance de $k(b'_1) \subset K$. Par hypothèse de récurrence, $m - 1 = n - 1$. □

On dit que le cardinal d'une base de transcendance est le *degré de transcendance* de $k \subset K$; on le notera $trdeg_k(K)$.

Exemples.

1. La première partie de la preuve montre que si $k \subset K$ est de type fini alors $trdeg_k(K)$ est fini et $\leq$ au nombre minimal de générateurs de $k \subset K$. Dans ce cas, si on note $n := trdeg_k(K)$ on a $X_1, \ldots, X_n \in K$ algébriquement indépendants sur k tels que $K/k(X_1, \ldots, X_n)$ est algébrique. Mais comme K/k est de type fini, $K/k(X_1, \ldots, X_n)$ l'est *a fortiori* donc, en fait, $K/k(X_1, \ldots, X_n)$ est même finie.
2. Comme $\mathbb{Q}(X_1, \ldots, X_n)$ est dénombrable et $\mathbb{C}$ ne l'est pas, on voit par contre que $\mathbb{C}/\mathbb{Q}$ est de degré de transcendance infini.
3. On dit qu'une variété algébrique affine $V = V(I) \subset \mathbb{C}^n$ est irréductible si $\mathbb{C}[V] := \mathbb{C}[X_1, \ldots, X_n]/\sqrt{I}$ est intègre. Dans ce cas, on peut introduire le corps des fractions $\mathbb{C}(V)$ de $\mathbb{C}[V]$ et définir

la dimension de la variété algébrique affine V comme étant le degré de transcendance de $\mathbb{C}(V)$ sur $\mathbb{C}$. Par exemple, l'extension de corps $\mathbb{C}[X,Y]/\langle Y^2-X^3-X-1\rangle/k$ est de degré de transcendance 1 - donc $V(Y^2-X^3-X-1)\subset\mathbb{C}^2$ est une courbe - mais ce n'est pas une extension transcendante pure, ce qui se traduit par le fait qu'on ne peut pas donner une paramétrisation rationnelle de $V(Y^2-X^3-X-1)$.

14.4.2

Lemme. *Soit $K_1\subset K_2\subset K_3$ des extensions de corps. On a*

$$trdeg_{K_1}(K_3)=trdeg_{K_1}(K_2)+trdeg_{K_2}(K_3).$$

Démonstration. Si $\mathcal{E}_1$ est une base de transcendance de $K_1\subset K_2$ et $\mathcal{E}_2$ est une base de transcendance de $K_2\subset K_3$, il faut vérifier que $\mathcal{E}:=\mathcal{E}_1\cup\mathcal{E}_2$ est une base de transcendance de $K_1\subset K_3$. Les éléments de $\mathcal{E}$ sont clairement algébriquement indépendants sur K_1. Soit $x\in K_3$. Comme $\mathcal{E}_2$ est une base de transcendance de $K_2\subset K_3$, il existe un sous-ensemble fini $\mathcal{E}_{2,x}\subset\mathcal{E}_2$ et $P_x=T^d+\sum_{0\leq i\leq d-1}a_iT^i\in K_2(\mathcal{E}_{2,x})[T]$ tel que $\mathrm{ev}_x(P)=0$. En écrivant $a_i=\frac{b_i}{c_i}$ avec $b_i,c_i\in K_2[\mathcal{E}_{2,x}]$, on voit qu'il existe un sous-ensemble fini $A_i\subset K_2$ tel que $a_i\in K_1(A_i)(\mathcal{E}_{2,x})$, $i=0,\dots,d-1$. On a donc

$$[K_1(A_0,\dots,A_{d-1},\mathcal{E}_{2,x})(x):K_1(A_0,\dots,A_{d-1},\mathcal{E}_{2,x})]<+\infty.$$

Comme $\mathcal{E}_1$ est une base de transcendance de $K_1\subset K_2$, on a $[K_1(\mathcal{E}_1)(A_0,\dots,A_{d-1}):K_1(\mathcal{E}_1)]<+\infty$. On en déduit

$$\begin{aligned}
&[K_1(\mathcal{E}_1,\mathcal{E}_{2,x})(x):K_1(\mathcal{E}_1,\mathcal{E}_{2,x})]\\
&\leq[K_1(\mathcal{E}_1,A_0,\dots,A_{d-1},\mathcal{E}_{2,x})(x):K_1(\mathcal{E}_1,\mathcal{E}_{2,x})]\\
&=[K_1(\mathcal{E}_1,A_0,\dots,A_{d-1},\mathcal{E}_{2,x})(x):K_1(\mathcal{E}_1,A_0,\dots,A_{d-1},\mathcal{E}_{2,x})][K_1(\mathcal{E}_1,A_0,\dots,A_{d-1},\mathcal{E}_{2,x}):K_1(\mathcal{E}_1,\mathcal{E}_{2,x})]\\
&=[K_1(\mathcal{E}_1,A_0,\dots,A_{d-1},\mathcal{E}_{2,x})(x):K_1(\mathcal{E}_1,A_0,\dots,A_{d-1},\mathcal{E}_{2,x})][K_1(\mathcal{E}_{2,x},\mathcal{E}_1)(A_0,\dots,A_{d-1}):K_1(\mathcal{E}_{2,x},\mathcal{E}_1)]<+\infty
\end{aligned}$$

□

14.4.3

Lemme. *Soit K/k une extension de corps. Si K est de type fini sur k alors $[\overline{k}^K:k]<+\infty$.*

Démonstration. Si $\mathcal{B}=\{b_1,\dots,b_n\}$ est une base de transcendance de K/k, $K/k(\mathcal{B})$ est algébrique de type fini donc finie. Pour toute sous-extension $k\subset k'\subset K$ finie sur k on a $[k':k]=[k'(\mathcal{B}):k(\mathcal{B})]\leq[K:k(\mathcal{B})]<+\infty$. □

On peut donc toujours décomposer une extension de corps K/k en trois parties

$$k\subset\overline{k}^K\subset\overline{k}^K(\mathcal{B})\subset K$$

avec $\overline{k}^K/k$ algébrique, $\overline{k}^K(\mathcal{B})/\overline{k}^K$ transcendante pure et $K/\overline{k}^K(\mathcal{B})$ algébrique. Si, de plus, K/k est de type fini alors $\overline{k}^K/k$ et $K/\overline{k}^K(\mathcal{B})$ sont finies et $\overline{k}^K(\mathcal{B})/\overline{k}^K$ est de degré de transcendance

finie. Les extensions de corps de type fini apparaissent naturellement en (et leur étude est motivée par) géométrie algébrique comme dans l'Exemple (3) de **??**. Il s'agit d'un sujet très vaste et encore largement ouvert.

Dans la suite du cours, nous allons nous intéresser au cas de degré de transcendance 0, qui est déjà très riche dès lors que le corps de base k est suffisamment 'compliqué' (on verra ce que compliqué veut dire plus loin...). Il s'agit donc de comprendre les variétés algébriques de dimension 0 sur un corps k *i.e.* les solutions d'une equation polynômiale à une indéterminée et à coefficients dans k. Ce problème concret remonte au 19ème siècle. A cette époque, on savait déjà depuis longtemps résoudre par radicaux (*i.e.* en n'utilisant que les opérations $+, -, \times, -/-, \sqrt[n]{-}$) des équations de degré ≤ 4 (les formules de Cardan en degré 3 et Ferrari en degré 4 remontent au milieu du 16ème siècle) mais pas au-delà. Ruffini et Abel, au tout début du 19ème siècle, ont annoncé qu'il 'n'existait pas de formule universelle pour résoudre une équation de degré donné ≥ 5'. Mais c'est Galois, dans son *Mémoire sur les conditions de résolubilité des équations par radicaux* (écrit en 1831 ; Galois avait 20 ans et devait mourir tué en duel l'année d'après), qui a eu l'intuition prodigieuse pour l'époque de relier le problème de la résolubilité d'une équation polynomiale aux symétries de ses zéros. Plus précisément, si $P \in \mathbb{Q}[T]$ est de degré n et se factorise en n facteurs de degré 1 distincts (ce que l'on appelera un polynôme séparable) dans $\mathbb{C}$

$$P = a_n \prod_{1 \leq i \leq n} (T - \alpha_i) \in \mathbb{C}[T]$$

on peut considérer le groupe $\mathcal{S}_n$ des permutations de $\{\alpha_1, \ldots, \alpha_n\}$. On peut alors attacher à P un sous-groupe $G_P \subset \mathcal{S}_n$ qui reflète les symétries de P (et qu'on appelle maintenant le groupe de Galois de P). Plus ce groupe est compliqué, plus les racines de P seront difficiles à calculer. Par exemple, l'introduction du groupe G_P permet de résoudre de façon limpide le problème de la résolution par radicaux : 'l'équation $P(x) = 0$ est résoluble par radicaux dans $\mathbb{C}$ si et seulement si le groupe G_P est résoluble (*i.e.* si $D^n G_P = 1$ pour $n \gg 0$ où les $D^n G_P$ sont les sous-groupes de G_P définis inductivement par $D^0 G_P = G_P$, $D^1 G_P = [G_P, G_P]$, $D^{n+1} G_P = [D^n G_P, D^n G_P]$)'. En particulier, puisque les groupes $\mathcal{S}_n$ ne sont pas résolubles pour $n \geq 5$ (et qu'il existe des polynômes $P \in \mathbb{Q}[T]$ de degré n tels que $G_P = \mathcal{S}_n$ - c'est en fait le cas 'générique'), il n'y a en effet aucune chance de trouver un formule universelle de résolution par radicaux des équations polynômiales de degrés ≥ 5.

Mais encore faut-il pouvoir calculer ces groupes G_P. Sur des exemples simples, on peut deviner intuitivement ce à quoi ressemble ces groupes. Par exemple, les solutions de $P = (T^2 + 1)(T^2 - 2) = 0$ sont $\pm i$, $\pm\sqrt{2}$ et si on peut échanger i avec $-i$ (ce sont les racines de T^2+1) et $\sqrt{2}$ avec $-\sqrt{2}$ (ce sont les racines de T^2-2), on ne peut pas échanger i et $\sqrt{2}$. Dans ce cas, G_P est le sous-groupe de $\mathcal{S}_4$ engendré par les transpositions $(1, 2)$ et $(3, 4)$ *i.e.* $\mathbb{Z}/2 \times \mathbb{Z}/2$. Cependant, très vite cette approche empirique ne suffit plus. La résolution conceptuelle du problème est donnée par ce qu'on appelle maintenant la correspondance de Galois. Dans le cas particulier considéré ici - $P \in \mathbb{Q}[T]$ est de degré n et a n zéros distincts $\alpha_1, \ldots, \alpha_n$ dans $\mathbb{C}$ - G_P est isomorphe au groupe § $\mathrm{Aut}(K_P/\mathbb{Q})$ des $\mathbb{Q}$-automorphismes de l'extension de corps $K_P := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q}$ et les sous-groupes $H \subset \mathrm{Aut}(K_P/\mathbb{Q})$ correspondent bijectivement aux sous-extensions $\mathbb{Q} \subset L \subset K_P$ par $H \to K_P^H := \{x \in K_P \mid \sigma(x) = x;\ \sigma \in H\}$ et

$L \to \mathrm{Aut}(K_P/L)$. Par exemple,

— Pour $P = X^5 + 10X^3 - 10X^2 + 35X - 18$, $G_P = \mathcal{A}_5$;

— Pour $P = X^5 + 10X^3 - 15$, $G_P = \mathcal{S}_5$.

Chapitre 15

Extensions algébriques

On rappelle que si K/k est une extension de corps et $x \in K$, on note $\mathrm{ev}_x : k[X] \to K$ l'unique morphisme de k-algèbres qui envoie X sur x et qu'on écrit en général $\mathrm{ev}_x(P) =: P(x)$, $P \in k[X]$.

15.1 Corps algébriquement clos, clôture algébrique

Pour tout $P \in k[X]$ on dit que $x \in K$ est une *racine* de P si $P(x) = 0$ (*i.e.* $P \in \ker(\mathrm{ev}_x) = k[X](X-1)$).

15.1.1

Lemme/définition. *Soit k un corps. Les propriétés suivantes sont équivalentes.*

1. *Tout $P \in k[X] \setminus k$ admet une racine sur k ;*
2. *Les éléments irréductibles de $k[X]$ sont de degré 1 ;*
3. *La seule extension algébrique $k \subset K$ est $k = K$.*

Un corps k qui vérifie les propriétés équivalentes du Lemme **??** est dit *algébriquement clos*.

Exemple.

1. $\mathbb{C}$ est algébriquement clos.

   Utilisons la caractérisation (1). Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$. Dire que P a une racine dans $\mathbb{C}$ revient à dire que la fonction continue $x \to |P(x)|$ atteint son minimum sur $\mathbb{C}$ et que celui-ci vaut 0. Observons déjà qu'elle atteint bien son minimum. En effet, puisque $\lim_{|x|\to+\infty} |P(x)| = +\infty$, il existe $R > 0$ tel que $|x| > r$ implique $|P(x)| > |a_0| = |P(0)|$ donc la fonction continue $x \to |P(x)|$ atteint son minimum sur le compact $B(0,R) := \{x \in \mathbb{C} \mid |x| \leq R\}$ (et ce minimum est $\leq |a_0|$). Quitte à faire un changement de variable de la forme $X \to X - x$, on peut supposer que $x \to |P(x)|$ atteint

son minimum en 0 donc que ce minimum vaut $|a_0|$. Si $a_0 = 0$, on a gagné. Sinon, quitte à remplacer P par $a_0^{-1}P$, on peut supposer que $a_0 = 1$. Soit v le plus petit entier ≥ 1 tel que $a_v \neq 0$. Écrivons $a_v = -|a_v| \exp(-iv\theta)$. On a alors $P(r\exp(i\theta)) = 1 - |a_v|r^v + O_0(r^{v+1})$ donc, lorsque $x \to 0$, on a $|P(0)| \leq 1 - |a_v|r^v + O_0(r^{v+1}) < 1$: contradiction.

2. Soit K/k une extension de corps avec K algébriquement clos. Alors $\overline{k}^K \subset K$ est un corps algébriquement clos. En effet, on sait déjà que $\overline{k}^K$ un corps. De plus, comme K est algébriquement clos, tout $P \in \overline{k}[T] \setminus k (\subset K[T] \setminus K)$ admet une racine $x \in K$. Mais par construction x est algébrique sur $\overline{k}^K$ et comme $\overline{k}^K$ est par définition algébrique sur k, x est algébrique sur k *i.e.* $x \in \overline{k}^K$.

15.1.2

Soit k un corps, une *clôture algébrique* de k est une extension algébrique $\overline{k}/k$ avec $\overline{k}$ algébriquement clos. Il résulte immédiatement de la définition que si $\overline{k}/k$ est une clôture algébrique alors pour toute sous extension K/k de $\overline{k}/k$, $\overline{k}/K$ est une côture algébrique de K.

Exemple.

1. $\mathbb{R} \subset \mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

2. Soit K/k une extension de corps avec K algébriquement clos. Alors $\overline{k}^K/k$ est une clôture algébrique de k. Par exemple, $\overline{\mathbb{Q}}^{\mathbb{C}}/\mathbb{Q}$ est une clôture algébrique de $\mathbb{Q}$.

L'objectif des deux paragraphes suivants est de démontrer la

15.1.3

Proposition. *Tout corps k possède une clôture algébrique $\overline{k}/k$, qui est unique à isomorphisme (non unique !) près.*

15.1.4

Unicité à isomorphisme près de la clôture algébrique.

15.1.4.0.1 Si K/k est une extension de corps et $P \in k[X]$, on notera

$$Z_K(P) := \{x \in K \mid P(x) = 0\} \subset K$$

l'ensemble des racines de P dans K. Supposons de plus que P est irréductible sur k. Pour tout $x \in Z_K(P)$, $\mathrm{ev}_x : k[T] \to K$ induit un k-plongement $\overline{ev}_x : k[T]/P \to K$. Inversement, pour tout k-pongement $\phi : k[T]/P \to K$, $x := \phi(\overline{T}) \in Z_K(P)$ et $\phi = \overline{ev}_x$. On a donc montré

Lemme. *Soit k un corps et $P \in k[X]$ un polynôme irréductible. Pour toute extension K/k l'application $\phi \to \phi(\overline{T})$ induit une bijection*

$$\mathrm{Hom}_{Alg/k}(k[T]/P, K) \tilde{\to} Z_K(P)$$

d'inverse $x \to \overline{ev}_x$.

Autrement dit, et c'est là l'idée clef de la théorie de Galois, les racines distinctes d'un polynôme irréductible $P \in k[T]$ dans une extension K/k correspondent bijectivement aux k-plongement $k[T]/P \to K$.

15.1.4.0.2 [Utilise le Lemme de Zorn] **Lemme.** *Soit k un corps et $\overline{k}/k$ une clôture algébrique de k. Alors pour toute extension algébrique K/k il existe un k-plongement $K \to \overline{k}$.*

Démonstration. Considérons l'ensemble $\mathcal{E}$ des couples (K', ϕ), où $k \subset K' \subset K$ est une sous-extension et $\phi : K' \to \overline{k}$ un k-plongement. On munit $\mathcal{E}$ de la relation d'ordre partiel $(K'_1, \phi_1) \leq (K'_2, \phi_2))$ si $K'_1 \subset K'_2$ et $\phi_2|_{K'_1} = \phi_1$. L'ensemble $\mathcal{E}$ est non vide puisqu'il contient $(k, k \subset \overline{k})$ et $(\mathcal{E}, \leq)$ est ordonné inductif. Par le Lemme de Zorn, il contient donc un élément maximal (K', ϕ). Mais si $K' \subsetneq K$, en appliquant **??** à l'extension $\phi : K' \to \overline{k}$ (qui est une clôture algébrique de K') et à $x \in K \setminus K'$, on construit un K'-plongement $\iota : K'(x) \to \overline{k}$. Par construction $(K', \phi) \leq (K'(x), \iota \circ \phi)$, ce qui contredit la maximalité de (K', ϕ). □

15.1.4.0.3 **Lemme.** *Soit K_1/k, K_2/k deux clôtures algébriques de k. Alors $Hom_{Alg/k}(K_1, K_2) = \mathrm{Aut}_{Alg/k}(K_1, K_2)$*

Démonstration. Soit $\phi : K_1/k \to K_2/k$ un k-plongement ; il faut montrer qu'il est surjectif. Mais d'une part $\phi(K_1)$ est algébriquement clos et, d'autre part, $K_2/\phi(K_1)$ est une extension algébrique puisque c'est une sous-extension de K_2/k. Donc on a forcément $\phi(K_1) = K_2$. □

Corollaire. *Les clôtures algébriques de k sont toutes k-isomorphes.*

Démonstration. Soit K_1/k, K_2/k deux clôtures algébriques de k. Par **??**, il existe un k-plongement $\phi : K_1 \to K_2$. Par le lemme précédent, c'est un isomorphisme. □

15.1.5

Existence de la clôture algébrique.

15.1.5.0.1 **Lemme.** (Limite inductive de corps) *Soit $k_0 \overset{\phi_0}{\to} k_1 \overset{\phi_1}{\to} k_2 \overset{\phi_2}{\to} \cdots$ une suite de morphismes de corps. Il existe un corps k_∞ et une suite de morphismes de corps $i_n : k_n \to k_\infty$, $n \geq 0$ tels que $i_{n+1} \circ \phi_n = i_n$, $n \geq 0$ pour tout corps K et toute suite de morphismes de corps $j_n : k_n \to K$, $n \geq 0$ tels que $j_{n+1} \circ \phi_n = j_n$, $n \geq 0$ on a un unique morphisme de corps $j : k_\infty \to K$ tel que $j \circ i_n = j_n$, $n \geq 0$.*

Démonstration. On commence par faire la construction en oubliant les structures de produit. Considérons donc la somme directe $\iota_n : k_n \to \Sigma := \oplus_{n\geq 0} k_n$ des k_0-modules k_n, $n \geq 0$ et le sous-k_0-module R engendré par les éléments de la forme

$$\iota_{n+1} \circ \phi_n(x_n) - \iota_n(x_n),\ x_n \in k_n,\ n \geq 0.$$

Posons $k_\infty := \Sigma/R$ et

$$i_n : k_n \xrightarrow{\iota_n} \Sigma \overset{p_R}{\twoheadrightarrow} k_\infty,\ n \geq 0.$$

Observons que

1. $k_\infty = \cup_{n\geq 0} i_n(k_n)$: cela résulte des relations $\iota_n(x_n) = \iota_{n+1}\circ\phi_n(x_n) + \iota_n(x_n) - \iota_{n+1}\circ\phi_n(x_n) \in \iota_{n+1} \circ \phi_n(x_n) + R$, qui montrent que $i_n(k_n) \subset i_{n+1}(k_{n+1})$, $n \geq 0$.
2. Pour tout $n \geq 0$, $\ker(i_n) = \{0\}$: Tout $0 \neq x \in R$ s'écrit sous la forme

$$x = \sum_{1\leq i\leq r} \iota_{n_i+1} \circ \phi_{n_i}(x_{n_i}) - \iota_{n_i}(x_{n_i})$$

   avec $0 \neq x_{n_i} \in k_{n_i}$, $i = 1, \ldots, r$ et $n_1 < n_2 < \cdots < n_r$. En particulier, la n_1-ième composant de x vaut $-x_{n_1}$ et la $n_r + 1$-ième vaut $-\phi_{n_r}(x_{n_r})$. Comme ϕ_{n_r} est injective, on en déduit que x a au moins deux composantes non nulles. En particulier, $\iota_n(k_n) \cap R = 0$.
3. Produit sur k_∞ : On a donc des carrés commutatifs

$$\begin{array}{ccc} k_{n+1} & \xrightarrow[i_{n+1}]{\simeq} & i_{n+1}(k_{n+1}) \\ \uparrow{\scriptstyle \phi_n} & & \uparrow{\scriptstyle \cup} \\ k_n & \xrightarrow[i_n]{\simeq} & i_n(k_n) \end{array}$$

   ar (1), pour tout $x, y \in k_\infty$, on peut choisir $n \geq 0$ tel que $x, y \in i_n(k_n)$ et par (2), $xy = i_n(i_n^{-1}(x)i_n^{-1}(y))$. Cette définition est indépendante du choix de n car la commutativité du diagramme ci-dessus et le fait que $\phi_n : k_n \to k_{n+1}$ est un morphisme de corps montrent que

$$i_{n+1}(i_{n+1}^{-1}(x)i_{n+1}^{-1}(y)) = i_{n+1}(\phi_n(i_n^{-1}(x))\phi_n(i_n^{-1}(x))) = i_{n+1}(\phi_n(i_n^{-1}(x)i_n^{-1}(x))) = i_n(i_n^{-1}(x)i_n^{-1}(y)).$$

   Enfin, on vérifie facilement qu'avec cette loi, k_∞ est un corps et que $i_n : k_n \to k_\infty$ est un morphisme de corps, $n \geq 0$.

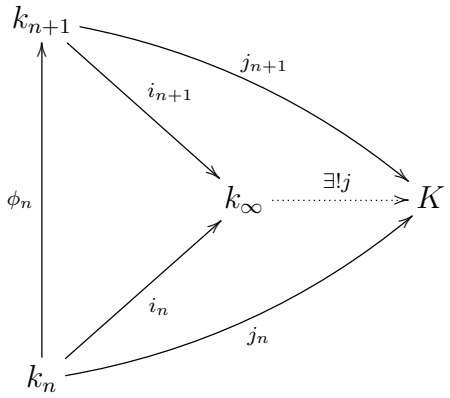
Il reste à vérifier que les morphismes de corps $i_n : k_n \to k_\infty$, $n \geq 0$ ainsi construits vérifient bien la propriété universelle de l'énoncé. Si $j : k_\infty \to K$ existe, les conditions $j \circ i_n = j_n$, $n \geq 0$ impose que $j(\overline{(x_n)}_{n\geq 0}) = \sum_{n\geq 0} j_n(x_n)$, d'où l'unicité de $j : k_\infty \to K$ sous réserve de son existence. Par propriété universelle de la somme directe, il existe un unique morphisme de k_0-modules $\Sigma \to K$, $(x_n)_{n\geq 0} \to \sum_{n\geq 0} j_n(x_n)$ et les conditions $j_{n+1} \circ \phi_n = j_n$, $n \geq 0$ montrent que R est contenu dans le noyau de ce morphisme donc qu'il passe au quotient en un morphisme de k_0-module $j : k_\infty \to K$ tel que $j(\overline{(x_n)}_{n\geq 0}) = \sum_{n\geq 0} j_n(x_n)$. Par construction, $j \circ i_n(x_n) = j_n(x_n)$, $n \geq 0$ et on vérifie sur les définitions que $j : k_\infty \to K$ est bien un morphisme de corps. □

Comme d'habitude les $i_n : k_n \to k_\infty (=: \varinjlim k_n)$, $n \geq 0$ sont uniques à unique isomorphisme près et on dit que c'est la limite inductive (ou la limite directe ou simplement la limite) des $k_0 \overset{\phi_0}{\to} k_1 \overset{\phi_1}{\to} k_2 \overset{\phi_2}{\to} \cdots$.

On peut réécrire **??** en disant que l'application canonique

$$\mathrm{Hom}(k_\infty, K) \to \{(j_n)_{n\geq 0} \in \prod_{n\geq 0} \mathrm{Hom}(k_n, K) \mid j_{n+1} \circ \phi_n = j_n,\ n \geq 0\},\ j \to (j \circ i_n)_{n\geq 0}$$

est bijective ou encore, plus visuellement,



15.1.5.0.2 **Lemme.** *Avec les notations de* **??**, *supposons de plus que pour tout* $n \geq 0$ *et* $P_n \in k_n[X] \setminus k_n$, $\phi_n(P_n) \in k_{n+1}[X]$ *a une racine dans* k_{n+1}. *Alors* k_∞ *est algébriquement clos.*

Démonstration. Soit $P \in k_\infty[X] \setminus k_\infty$. Comme $k_\infty = \cup_{n\geq 0} i_n(k_n)$ il existe $n \geq 0$ tel que $P \in i_n(k_n)[X] \setminus k_n$. Mais par hypothèse $\phi_n \circ i_n^{-1}(P) \in k_{n+1}[X]$ a une racine $x_{n+1} \in k_{n+1}$ donc $i_{n+1}(x_{n+1}) \in i_{n+1}(k_{n+1}) \subset k_\infty$ est une racine de $i_{n+1} \circ \phi_n \circ i_n^{-1}(P) = P$. □

15.1.5.0.3 [Utilise le Lemme de Zorn] **Lemme.** *Pour tout corps* k *il existe une extension algébrique* K/k *telle que tout* $P \in k[X] \setminus k$ *possède une racine dans* K.

Démonstration. Observons d'abord que si $P \in k[T] \setminus k$, il existe toujours une extension finie K_P/k telle que P possède une racine dans K. En effet, il suffit de considérer l'extension $k \to K_P := k[X]/Q$ pour $Q \in k[X]$ un diviseur irréductible unitaire de P. En appliquant inductivement ce procédé, pour tout $P_1, \ldots, P_r \in k[X] \setminus k$, on peut toujours construire une extension finie $K_{P_1,\ldots,P_r}/k$ telle que P_i possède une racine dans $K_{P_1,\ldots,P_r}$, $i = 1, \ldots, r$. En utilisant **??**, on peut encore étendre cette construction à une suite $(P_n)_{n\geq 0}$ éléments de $k[X] \setminus k$. Mais $k[X] \setminus k$ n'est en général pas dénombrable et il faut un peu adapter ces observations.Considérons la k-algèbre de polynômes $k \to k[X_P,\ P \in k[X] \setminus k]$ et l'idéal $I \subset k[X_P,\ P \in k[X] \setminus k]$ engendré par les $P(X_P)$, $P \in \mathcal{P}$. Vérifions d'abord que $I \subsetneq k[X_P,\ P \in k[X] \setminus k]$. Sinon on pourrait écrire

$$(*)\ \ 1 = \sum_{1\leq i\leq r} F_i P_i(X_{P_i})$$

avec $F_i \in k[X_P,\ P \in k[X] \setminus k]$, $i = 1, \dots, r$. Chaque F_i ne fait intervenir qu'un sous-ensemble fini $\mathcal{F} \subset k[X] \setminus k$ et quitte à agrandir $\mathcal{F}$, on peut supposer que $P_1, \dots, P_r \in \mathcal{F}$. On peut donc réécrire la relation précédente sous la forme

$$(*)\ \ 1 = \sum_{P \in \mathcal{F}} F_P P(X_P)$$

avec $F_P \in k[X_Q,\ Q \in \mathcal{F}]$, $P \in \mathcal{F}$. D'après nos observations préliminaires, il existe une extension finie $K_{\mathcal{F}}/k$ tel que P possède une racine $x_p \in K_{\mathcal{F}}$, $P \in \mathcal{F}$. En évaluant $(*)$ en les x_P, $P \in \mathcal{F}$, on obtient donc $1 = 0$. Cela montre que $I \subsetneq k[X_P,\ P \in k[X] \setminus k]$ donc est contenu dans un idéal maximal $\mathfrak{m} \subset k[X_P,\ P \in k[X] \setminus k]$. Cela nous donne une extension $k \to k[X_P,\ P \in k[X] \setminus k]/\mathfrak{m} := \Omega$ tel que tout $P \in k[X] \setminus k$ a une racine $x_P \in \Omega$. De plus, Ω est engendrée comme extension de k par les x_P, $P \in k[X] \setminus k$ donc est algébrique sur k. □

15.1.5.0.4 Proposition. *Tout corps k admet une clôture algébrique.*

Démonstration. Notons $k_0 := k$. D'après **??**, il existe une extension k_1/k algébrique sur k et tel que tout $P \in k_0[T] \setminus k_0$ possède une racine dans k_0. En itérant le procédé, on construit une suite de morphisme corps $k_0 \xrightarrow{\phi_0} k_1 \xrightarrow{\phi_1} k_2 \xrightarrow{\phi_2} \cdots$ telle que pour tout $n \geq 0$ et $P_n \in k_n[X] \setminus k_n$, $\phi_n(P_n) \in k_{n+1}[X]$ a une racine dans k_{n+1}. Par **??** et **??**, k_∞/k est algébriquement clos. On peut donc prendre $\overline{k} := \overline{k}^{k_\infty}$ (*cf.* **??**). □

15.2 Automorphismes, Corps de décomposition, extensions normales

15.2.1

Pour une extension de corps K/k on notera $\mathrm{Aut}(K/k) := \mathrm{Aut}_{Alg/k}(K)$ le groupe des automorphismes de la k-algèbre $k \to K$. Si K_1/k, K_2/k sont deux extensions de corps tout k-isomorphisme $\phi : K_1 \tilde{\to} K_2$ induit un isomorphisme de groupes

$$\mathrm{Aut}_{Alg/k}(K_1) \tilde{\to} \mathrm{Aut}_{Alg/k}(K_2),\ \sigma \to \phi \circ \sigma \circ \phi^{-1}.$$

En particulier, si $\overline{k}/k$, $\overline{k}'/k$ sont deux clôtures algébriques de k, on sait qu'il existe toujours un k-isomorphisme $\phi : \overline{k} \tilde{\to} \overline{k}'$ donc que $\mathrm{Aut}(\overline{k}/k)$ ne dépend pas - à isomorphisme près - du choix de la clôture algébrique $\overline{k}/k$.

Exemple. $\mathbb{C} = \mathbb{R}[T]/T^2+1$. Notons $\overline{T} := i$. On a $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \mathrm{Hom}_{Alg/\mathbb{R}}(\mathbb{R}[T]/T^2+1, \mathbb{C}) = \{\overline{ev}_i = \mathrm{Id}, \overline{ev}_{-i} = \overline{\ \ }\}$.

Si $\phi : K_1 \tilde{\to} K_2$ est un isomorphisme de corps, la propriété universelle de $c_1 : K_1 \to K_1[T]$ appliquée à la K_1-algèbre $K_1 \xrightarrow{\phi} K_2 \xrightarrow{c_2} K_2[T]$ donne un unique isomorphisme de K-algèbres

$\phi : K_1[T] \to K_2[T]$ tel que $\phi \circ c_1 = c_2 \circ \phi$ (ici, $c_i : K_i \to K_i[T]$, $i = 1, 2$ sont les morphismes canoniques). Explicitement $\phi(\sum_{n\geq 0} a_n T^n) = \sum_{n\geq 0} \phi(a_n) T^n$. Par construction, pour tout $x_1 \in K_1$ on a

$$\phi \circ ev_{x_1} = ev_{\phi(x_1)} \circ \phi : K_1[T] \to K_2[T].$$

En particulier, $\phi : K_1 \tilde{\to} K_2$ se restreint en une bijection

$$\phi : Z_{K_1}(P) \tilde{\to} Z_{K_2}(\phi(P)).$$

Dans le cas particulier où $K_1 = K_2 = K/k$, $\phi \in \mathrm{Aut}(K/k)$ et $P \in k[T]$, $\phi P = P$, $\phi \in \mathrm{Aut}(K/k)$ induit une perm utation $\phi : Z_K(P) \tilde{\to} Z_K(P)$. En d'autres termes, $\mathrm{Aut}(K/k)$ agit sur $Z_K(P)$ *i.e.* on a un morphisme de groupes

$$\mathrm{Aut}(K/k) \to \mathcal{S}(Z_K(P)).$$

On peut notamment appliquer cette observation à $K/k = \overline{k}/k$ une clôture algébrique de k.

15.2.2

Sous-extensions normales de $\overline{k}/k$.

15.2.2.0.1 Lemme. *Soit K/k une extension algébrique et $\phi_1, \phi_2 : K \to \overline{k}$ deux k-plongements. Il existe $\sigma \in \mathrm{Aut}(\overline{k}/k)$ tel que $\sigma \circ \phi_1 = \phi_2$.*

Démonstration. C'est un cas particulier de **??**. En effet, comme $\phi_1 : K \to \overline{k}$ est une extension algébrique et $\phi_2 : K \to \overline{k}$ est une clôture algébrique de K, il existe un K-plongement $\sigma : \overline{k} \to \overline{k}$, qui est automatiquement un K-automorphisme. Comme à gauche l'extension $\overline{k}/K$ est donnée par $\phi_1 : K \to \overline{k}$ et à droite est donnée par $\phi_2 : K \to \overline{k}$, dire que $\sigma : \overline{k} \to \overline{k}$ est un k-plongement signifie bien que $\sigma \circ \phi_1 = \phi_2$. □

15.2.2.0.2 On rappelle que si $x \in \overline{k}$, on note $P_x \in k[T]$ le polynôme minimal de x sur k.

Lemme. *Pour tout $x, y \in \overline{k}$ les propriétés suivantes sont équivalentes.*

1. *Il existe $\sigma \in \mathrm{Aut}(\overline{k}/k)$ tel que $\sigma(x) = y$;*
2. *$P_x = P_y$.*

Démonstration. (1) $\Rightarrow$ (2) D'après **??**, $y = \sigma(x) \in Z_{\overline{k}}(P_x)$ donc $P_y | P_x$ dans $k[T]$. Mais comme P_x est irréductible sur k on a nécessairement $P_x = P_y$.
(2) $\Rightarrow$ (1) Notons $P := P_x = P_y \in k[T]$. On dispose de deux k-plongements $\overline{ev}_x : k[T]/P \to \overline{k}$, $\overline{T} \to x$, $\overline{ev}_y : k[T]/P \to \overline{k}$, $\overline{T} \to y$ donc, d'après **??**, il existe $\sigma \in \mathrm{Aut}(\overline{k}/k)$ tel que $\sigma \circ \overline{ev}_x = \overline{ev}_y$. En particulier $\sigma(x) = \sigma(\overline{ev}_x(\overline{T})) = \overline{ev}_y(\overline{T}) = y$. □

On dit que deux éléments $x, y \in \overline{k}$ qui vérifient les propriétés équivalentes du lemme **??** sont conjugués sur k. Si $x \in \overline{k}$ les conjugués de x sur k sont donc les éléments de

$$(*)\ \ \mathcal{C}_k(x) := \{\sigma(x) \mid \sigma \in \mathrm{Aut}(\overline{k}/k)\} = Z_{\overline{k}}(P_x).$$

Exemple.

1. $\mathbb{C}/\mathbb{R}$: les conjugués sur $\mathbb{R}$ de $z \in \mathbb{C}$ sont z et $\overline{z}$.

2. $\overline{\mathbb{Q}}/\mathbb{Q}$: les conjugués sur Q de $\sqrt[3]{5}$ sont $\sqrt[3]{5}$, $j\sqrt[3]{5}$, $j^2\sqrt[3]{5}$ (où j est une racine de T^2+T+1 *i.e.* une racine primitive 3ième de l'unité).

15.2.2.0.3 Lemme. *Soit $k \subset K \subset \overline{k}$ une sous-extension. Les propriétés suivantes sont équivalentes.*

1. *Pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, $\sigma(K) \subset K$*
2. *Pour tout $x \in K$, $Z_K(P_x) = Z_{\overline{k}}(P_x)$ (i.e. toutes les racines de P_x dans $\overline{k}$ sont contenues dans K).*

Démonstration. (1) $\Rightarrow$ (2) Cela résulte immédiatement de $(*)$. (2) $\Rightarrow$ (1) Toujours d'après $(*)$, pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$ et tout $x \in K$, $\sigma(x) \in Z_{\overline{k}}(P_x)$ or, par (2) $Z_{\overline{k}}(P_x) = Z_K(P_x) \subset K$. □

On dit qu'une sous-extension $k \subset K \subset \overline{k}$ qui vérifie les propriétés équivalentes du lemme **??** est une *sous-extension normale* de $\overline{k}/k$.

15.2.2.0.4 Corollaire. *Soit $k \subset K \subset \overline{k}$ une sous-extension normale de $\overline{k}/k$. Le morphisme de restriction*

$$\mathrm{Aut}(\overline{k}/k) \to \mathrm{Aut}(K/k),\ \sigma \to \sigma|_K$$

est un morphisme de groupes bien défini, surjectif et de noyaux $\mathrm{Aut}(\overline{k}/K)$.

Démonstration. Le fait que $\sigma \to \sigma|_K$ est bien défini résulte de **??** ; c'est alors automatiquement un morphisme de groupes. Soit $\sigma \in \mathrm{Aut}(K/k)$ et notons $\phi : K \to \overline{k}$ le k-plongement définissant $\overline{k}/K$. On dispose donc de deux k-plongements $\phi, \phi \circ \sigma : K \to \overline{k}$ donc, d'après **??**, il existe $\tilde{\sigma} \in \mathrm{Aut}(\overline{k}/k)$ tel que $\tilde{\sigma} \circ \phi = \phi \circ \sigma$. Cela montre la surjectivité. On a immédiatement $\mathrm{Aut}(\overline{k}/K) = \ker(\sigma \to \sigma|_K)$. □

La terminologie 'normale' vient du fait que le sous-groupe $\mathrm{Aut}(\overline{k}/k) \subset \mathrm{Aut}(\overline{k}/k)$ est normal.

Exemple.

— Toute sous-extension $k \subset K \subset \overline{k}$ de degré 2 est normale.

— La sous-extension $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ de $\overline{\mathbb{Q}}/\mathbb{Q}$ (de degré 3) n'est pas normale puisqu'elle ne contient pas $j\sqrt[3]{5}$, $j^2\sqrt[3]{5}$. Par contre la sous-extension $\mathbb{Q}(\sqrt[3]{5}, j\sqrt[3]{5})/\mathbb{Q} = \mathbb{Q}(\sqrt[3]{5}, j)/\mathbb{Q}$ de $\overline{\mathbb{Q}}/\mathbb{Q}$ (de degré 6) est normale.

15.2.3

Extensions normales, corps de décomposition.

15.2.3.0.1 Si k est un corps et K/k une extension de corps, on dit qu'un polynôme $P \in k[T]$ est totalement décomposé sur K si tous ses facteurs irréductibles dans $K[T]$ sont de degré 1 *i.e.* P s'écrit sous la forme

$$P = a \prod_{1 \leq i \leq n} (T - \alpha_i)$$

avec $a \in k$, $\alpha_1, \ldots, \alpha_n \in k$.

Observons que si $P \in k[T]$ est totalement décomposé sur K, pour toute extension de corps K'/k et k-plongement $\phi : K \to K'$, $P \in k[T]$ est encore totalement décomposé sur K' puisque, en utilisant que $\phi : K[T] \tilde{\to} K[T]$ est un automorphisme de k-algèbre,

$$\phi P = P = \phi(a \prod_{1 \leq i \leq n} (T - \alpha_i)) = a \prod_{1 \leq i \leq n} (T - \phi(\alpha_i)).$$

En particulie, on a $\phi(Z_K(P)) = Z_{\phi(K)}(P) = Z_{K'}(P)$.

Lemme. *Soit K/k une extension algébrique. Les propriétés suivantes sont équivalentes.*

1. *Pour tout $x \in K$, $P_x \in k[T]$ est totalement décomposé sur K ;*
2. *Si $\overline{k}/k$ est une clôture algébrique et $\phi_1, \phi_2 : K \to \overline{k}$ sont deux k-plongements, $\phi_1(K) = \phi_2(K)$;*
3. *Si $\overline{k}/k$ est une clôture algébrique et $\phi : K \to \overline{k}$ un k-plongement, $k \subset \phi(K) \subset \overline{k}$ est une sous-extension normale de $\overline{k}/k$.*

Démonstration. (1) $\Rightarrow$ (2) D'après l'observation ci-dessus appliquée à un k-plongement $\phi : K \to \overline{k}$, pour tout $x \in K$, $\phi(x) \in \phi_i(Z_K(P_x)) = Z_{\overline{k}}(P_x) = Z_{\phi(K)}(P_x) \subset \phi(K)$. Autrement dit

$$\phi(K) = \cup_{x \in K} Z_{\overline{k}}(P_x)$$

est indépendant du k-plongement $\phi : K \to \overline{k}$. (2) $\Rightarrow$ (3) Pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, $\sigma \circ \phi : K \to \overline{k}$ est un autre k-plongement donc par (2) $\sigma(\phi(K)) = \phi(K)$ et on utilise la caractérisation (1) de **??**.
(3) $\Rightarrow$ (1) Par **??**, il existe un k-plongement $\phi : K \to \overline{k}$. Par (3) et **??** (2), pour tout $x \in K$, $P_{\phi(x)} = \phi(P_x) = P_x \in k[T]$ est totalement décomposé sur $\phi(K)$ donc P_x est totalement décomposé sur K. □

On dit qu'une extension K/k qui vérifie les propriétés équivalentes du lemme **??** est une *extension normale*.

Remarque. On peut reformuler (1) en (1)' pour tout $P \in k[T]$ irréductible si P a une racine dans K alors P est totalement décomposé sur K et (2) en (2)' Si $\phi : K \to K'$ est un k-plongement alors $\phi(K) \subset K'$ est la sous-extension de K'/k engendrée par les $Z_{K'}(P_x)$, $x \in K$ (et est, en particulier, indépendante du k-plongement $\phi : K \to K'$).

Exemple.

— Toute extension K/k de degré 2 est normale.

— L'extension $\mathbb{Q}(\sqrt[3]{5}) \simeq \mathbb{Q}[T]/T^3-5/\mathbb{Q}$ (de degré 3) n'est pas normale. Par contre $\mathbb{Q}(\sqrt[3]{5}, j\sqrt[3]{5})/\mathbb{Q} \simeq \mathbb{Q}(\sqrt[3]{5})[T]/\langle T^2+T+1\rangle \simeq \mathbb{Q}[X,T]/\langle X^3-5, T^2+T+1\rangle/\mathbb{Q}$ (de degré 6) est normale.

Contre-exemple. On prendra garde que la propriété d'être normale se comporte mal par transitivié. Plus précisément, si K_3/K_2 et K_2/K_1 sont deux extensions de corps,

— il n'est pas vrai en général que si K_3/K_2 et K_2/K_1 sont normales alors K_3/K_1 est normale (contre-exemple : $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sont normales mais $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ne l'est pas) ;

— il n'est pas vrai non plus en général que si K_3/K_1 est normale alors K_2/K_1 est normale (contre-exemple : $\mathbb{Q}(\sqrt[3]{5}, j)/\mathbb{Q}$ est normale mais $\mathbb{Q}(3\sqrt{5})/\mathbb{Q}$ ne l'est pas) ;

— par contre si K_3/K_1 est normale alors K_3/K_2 l'est aussi. En effet, pour tout $x \in K_3$ si on note $P_{x,1} \in K_1[T]$ et $P_{x,2} \in K_2[T]$ les polynômes minimaux de x sur K_1 et K_2 respectivement alors $P_{x,2}|P_{x,1}$ dans $K_2[T]$ donc, comme $P_{x,1}$ est totalement décomposé sur K_3, $P_{x,2}$ l'est aussi.

15.2.3.0.2 Soit $P \in k[T]$. On dit qu'une extension K/k est un *corps de décomposition* de $P \in k[T]$ sur k si P est totalement décomposé sur k et si $K = k(Z_K(P))/k$.

Lemme. *Tout polynôme $P \in k[T]$ admet un corps de décomposition sur k, qui est unique à k-isomorphisme (non-unique) près et est une extension normale de k.*

Démonstration. Soit $\overline{k}/k$ une clôture algébrique de k alors $K_0 = k(Z_{\overline{k}}(P))/k$ est un corps de décomposition de P sur k. Soit K/k un corps de décomposition de P sur k. Par **??**, il existe un k-plongement $\phi : K \to \overline{k}$. Or par $(*)$ et comme P est totalement décomposé sur K donc sur $\phi(K) \subset \overline{k}$, $\phi(K) = \phi(k(Z_K(P))) = k(Z_{\overline{k}}(P)) = K_0$. En particulier, $\phi : K \to \overline{k}$ induit un k-isomorphisme $\phi : K = k(Z_K(P)) \tilde{\to} k(\phi(Z_K(P))) = k(Z_{\overline{k}}(P)) = K_0$. Enfin, pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, $\sigma_{K_0} : K_0 \to \overline{k}$ est un k-plongement et l'argument qui précède appliqué avec $K = K_0$ montre que $\sigma(K_0) = K_0$. Donc K_0/k est une sous-extension normale de $\overline{k}/k$ donc une extension normale. □

Si K/k est un corps de décomposition de P, on a une action naturelle $\mathrm{Aut}(K/k) \times Z_K(P) \to Z_K(P)$ qui est fidèle puisque $K = k(Z_K(P))$ d'où un morphisme de groupes injectif $\mathrm{Aut}(K/k) \hookrightarrow \mathcal{S}(Z_K(P))$. C'est essentiellement ce groupe $\mathrm{Aut}(K/k)$ qui va reflèter les 'symétries' des racines de P.

Remarque. Le Lemme **??** montre qu'une extension K/k finie est normale si et seulement si c'est le corps de décomposition d'un polynôme $P \in k[T]$ sur k.

Exemple. Le corps de décomposition de $X^3 - 5 \in \mathbb{Q}[T]$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{5}, j)/\mathbb{Q}$. En considérant l'extension intermédiaire $\mathbb{Q} \subset \mathbb{Q}(j) \subset \mathbb{Q}(j)(\sqrt[3]{5})$ et en observant que $\mathbb{Q}(j)/\mathbb{Q}$ est le corps de décomposition de $X^2 + X + 1 \in \mathbb{Q}[T]$ sur $\mathbb{Q}$, on obtient une suite exacte courte de groupes

$$1 \to \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5}, j)/\mathbb{Q}(j)) \to \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5}, j)/\mathbb{Q}) \to \mathrm{Aut}(\mathbb{Q}(j)/\mathbb{Q}) \to 1.$$

Or la bijection $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5},j)/\mathbb{Q}(j))\tilde{\to}Z_{\mathbb{Q}(\sqrt[3]{5},j)}(X^3-5)$ montre que $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5},j)/\mathbb{Q}(j))$ est d'ordre 3 donc cyclique et engendré par $\mathbb{Q}(\sqrt[3]{5},j)=\mathbb{Q}(j)[T]/T^3-5\tilde{\to}\mathbb{Q}(\sqrt[3]{5},j)$, $\overline{T}=^3\sqrt{5}\to j\,\sqrt[3]{5}$. De même, la bijection $\mathrm{Aut}(\mathbb{Q}(j)/\mathbb{Q})\tilde{\to}Z_{\mathbb{Q}(j)}(X^2+X+1)$ montre que $\mathrm{Aut}(\mathbb{Q}(j)/\mathbb{Q})$ est d'ordre 2 donc cyclique et engendré par $\mathbb{Q}(j)=\mathbb{Q}[T]/T^2+T+1\tilde{\to}\mathbb{Q}(j)$, $\overline{T}=J\to j^2$. Donc $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5},j)/\mathbb{Q})$ est un sous-groupe d'ordre 6 de $\mathcal{S}_3$; c'est $\mathcal{S}_3$... On verra bientôt comment mener de façon plus systématique ce type de calculs.

A ce stade, on aimerait poser, pour un polynôme $P\in k[T]$, $G_P:=\mathrm{Aut}(K/k)$, où K est un corps de décomposition de P sur k et étudier les racines $\alpha_1,\dots,\alpha_n$ de P dans K - ou plutôt les sous-corps $k(\alpha_i)$, $i=1,\dots,n$ de K engendrés par les racines *via* la structure du groupe G_P en montrant qu'on a une correspondance bijective entre les sous-groupes $H\subset G_P$ et les sous-corps $k\subset L\subset K$ donnée par $H\to K^H$, $L\to\mathrm{Aut}(K/L)$. Cependant, ce n'est pas toujours vrai que les applications $H\to K^H$, $L\to\mathrm{Aut}(K/L)$ sont bijectives comme le montre l'exemple suivant. Prenons $k:=\mathbb{F}_p(X)$, $P=T^{p^2}-X\in k[T]$ et notons $K/\mathbb{F}_p(X)$ un corps de décomposition. Soit $\alpha\in K$ une racine de P. On a alors $P=(T-\alpha)^{p^2}$ sur $K[T]$. En particulier, $K=k(\alpha)=k[T]/P$. Mais comme P n'a qu'une seule racine sur k, $\mathrm{Aut}(K/k)=1$ alors que K/k contient est non triviale (et même contient une sous-extension stricte : $k\subsetneq k(\alpha^p)\subsetneq k(\alpha)=K$). Pour faire marcher cette approche, il va falloir imposer une condition supplémentaire sur P, celle d'être séparable.

15.3 Extensions séparables

15.3.1

Dérivations. Soit A une k-algèbre. Une *k-dérivation sur A* est un endomorphisme de k-module $\partial:A\to A$ tel que

$$\partial(ab)=a\partial b+(\partial a)b,\ a,b\in A.$$

Une récurrence facile montre que $\partial(a^n)=na^{n-1}\partial a$, $a\in A$, $n\geq 1$. En particulier, $\partial 1=\partial(1^2)=2\partial 1$ donc $\partial 1=0$ et par k-linéarité, $k\subset\ker(\partial)$.

Sur $A=k[T]$ une dérivation est donc uniquement déterminée par sa valeur en T. Considérons la dérivation $\partial:k[T]\to k[T]$, $T\to 1$ *i.e.*

$$\partial(\sum_{n\geq 0}a_nT^n)=\sum_{n\geq 1}na_nT^{n-1}.$$

On note en général $P':=\partial P$, $P\in k[T]$ et on dit que P' est le polynôme dérivé de P.

Remarques.

1. Pour tout morphisme de corps $\phi:k\to k'$ on vérifie immédiatement que $\phi(P)'=\phi(P')$, $P\in k[T]$.
2. Notons p la caractéristique de k. Soit $P\in k[T]$ tel que $P'=0$.

— Si $p = 0$, $P \in k$.

— Si $p > 0$, il existe - un unique polynôme $Q \in k[T]$ tel que $P = Q_1(T^p)$. Par récurrence il existe donc un unique $r \in \mathbb{Z}_{\geq 1}$ et un unique polynôme $Q_r \in k[T]$ tels que $Q_r' \neq 0$ et $P = Q_r(T^{p^r})$

Écrivons $P = \sum_{n\geq 0} a_n T^n$ donc $P' = \sum_{n\geq 1} n a_n T^{n-1} = 0$ si et seulement si $na_n = 0$, $n \geq 1$. Si $p = 0$, cela impose $a_n = 0$, $n \geq 1$ donc $P = a_0$. Si $p > 0$, cela impose $a_n = 0$, $n \geq 1$, $p \nmid n$ donc $P = \sum_{n\geq 0} a_{np} T^{np} = \sum_{n\geq 0} a_{np}(T^p)^n = Q(T^p)$ avec $Q_1 = \sum_{n\geq 0} a_{np} T^n$.

15.3.2

Lemme. *Pour $P \in k[T]$ les propriétés suivantes sont équivalentes.*

1. *P et P' sont premiers entre eux dans $k[T]$;*
2. *Pour toute clôture algébrique $\overline{k}/k$, P et P' sont premiers entre eux dans $\overline{k}[T]$;*
3. *Pour toute clôture algébrique $\overline{k}/k$, $|Z_{\overline{k}}(P)| = \deg(P)$;*
4. *Pour toute clôture algébrique $\overline{k}/k$, $\overline{k}[T]/P$ est réduite.*

Démonstration. (1) $\Rightarrow$ (2) résulte de Bézout : P et P' sont premiers entre eux dans $k[T]$ si et seulement si $k[T] = k[T]P + k[T]P'$ *i.e.* il existe $U, V \in k[T]$ tels que $UP + VP' = 1$. Mais cette relation est *a fortiori* vraie dans $\overline{k}[T]$ donc la conclusion résulte de Bézout dans $\overline{k}[T]$. (2) $\Rightarrow$ (1) Par la contraposé, si P et P' ont un diviseur irréductible commun Q dans $k[T]$, celui-ci est *a fortiori* un diviseur commun (non constant...) de P et P' dans $\overline{k}[T]$. (2) $\Rightarrow$ (3) Par la contraposée, si $|Z_{\overline{k}}(P)| < \deg(P)$ cela signifie que P a au moins une racine double α dans $\overline{k}$ *i.e.* $(T-\alpha)^2 | P$ dans $\overline{k}[T]$. En écrivant $P = (T-\alpha)^2 Q$ dans $\overline{k}[T]$ et en dérivant on obtient $P' = 2(T-\alpha)Q + tT - \alpha)^2 Q'$ donc $(T-\alpha)|P'$ dans $\overline{k}[T]$. (3) $\Rightarrow$ (2) Par la contraposée, si P, P' ont un diviseur irréductible commun $T - \alpha$ dans $\overline{k}[T]$, on peut écrire $P = (T-\alpha)Q$ dans $\overline{k}[T]$ donc $P' = (T-\alpha)Q' + Q$. Comme $(T-\alpha)|P'$ on a forcément $(T-\alpha)|Q$ donc $(T-\alpha)^2|P$ donc $|Z_{\overline{k}}(P)| \leq \deg(P) - 1$. (3) $\Leftrightarrow$ (4) En écrivant $P = a\prod_{1\leq i\leq n}(T-\alpha_i)^{\nu_i}$ dans $\overline{k}[T]$ avec $0 \neq a \in k$ et $\alpha_1, \ldots, \alpha_n \in \overline{k}$ deux à deux distincts, le Lemme des restes chinois nous donne un isomorphisme canonique de $\overline{k}$-algèbres

$$\overline{k}[T]/P \tilde{\to} \prod_{1\leq i\leq n} \overline{k}[T]/(T-\alpha_i)^{\nu_i}.$$

En particulier $\overline{k}[T]/P$ est réduit si et seulement si $\overline{k}[T]/(T-\alpha_i)^{\nu_i}$ est réduit, $i = 1, \ldots, n$ si et seulement si $\nu_1 = \cdots = \nu_n = 1$. □

On dit qu'un polynôme $P \in k[T]$ qui vérifie les propriétés équivalentes du Lemme **??** est *séparable*.

Exemple. Si k est de caractéristique 0 tout polynôme $P \in k[T]$ irréductible est séparable sur k. Ce n'est plus vrai si k est de caractéristique $p > 0$: le polynôme $P = T^p - X \in \mathbb{F}_p(X)[T]$ est irréductible sur $\mathbb{F}_p(X)$ mais pas séparable.

15.3.3

D'après **??** on a

P	arbitraire	séparable
$\lvert Z_{\overline{k}}(P)\rvert$	$\leq \deg(P)$	$= \deg(P)$

Si $P \in k[T]$ est irréductible, puisque pour toute clôture algébrique $\overline{k}/k$, $|\operatorname{Hom}_{Alg/k}(k[T]/P, \overline{k})| = |Z_{\overline{k}}(P)|$ et $\deg(P) = [k[T]/P : k]$ on peut réécrire le tableau précédent sous la forme

P	arbitraire	séparable
$\lvert \operatorname{Hom}_{Alg/k}(k[T]/P, \overline{k})\rvert$	$\leq [k[T]/P : k]$	$= [k[T]/P : k]$

Lemme. *Soit k un corps algébriquement clos et A une k-algèbre de dimension finie sur k. Le morphisme de k-algèbres*

$$A \to k^{\operatorname{Hom}_{Alg_{/k}}(A,k)},\ a \to (\sigma(a))_{\sigma \in \operatorname{Hom}_{Alg_{/k}}(A,k)}$$

est surjectif de noyau le nilradical de A. En particulier, $\dim_k(A) \geq |\operatorname{Hom}_{Alg/k}(A, k)|$.

Démonstration. Il s'agit de la combinaison d'un cas facile du Nullstellensatz et du Lemme des restes chinois. Plus précisément, comme A est de k-dimension finie - donc en particulier de type fini comme k-algèbre - et que k est algébriquement clos, le Nullstellensatz nous donne une bijection canonique

$$\operatorname{Hom}_{Alg/k}(A, k) \tilde{\to} \operatorname{spm}(A),\ (\phi : A \to k) \to \ker(\phi)$$

(d'inverse $\mathfrak{m} \to (A \to A/\mathfrak{m}) = k$). On a vu qu'il résultait aussi du Nullstellensatz que le radical de Jacobson et le nilradical de A coincident, d'où l'assertion sur le noyau. La surjectivité résultera du Lemme des restes chinois si l'on sait que A n'a qu'un nombre fini d'idéaux maximaux. Mais en notant $n := \dim_k A$, A a au plus n idéaux maximaux deux à deux distincts. En effet, si on avait $n+1$ idéaux maximaux $\mathfrak{m}_1, \ldots, \mathfrak{m}_{n+1}$ deux à deux distincts, le Lemme des restes chinois nous donnerait un morphisme surjectif de k-algèbres (donc de k-espaces vectoriels)

$$A \twoheadrightarrow A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_{n+1} = k^{n+1}.$$

□

Le corollaire suivant généralise la première colonne du tableau à une extension finie arbitraire.

Corollaire. *Si K/k est une extension finie et $\overline{k}/k$ une clôture algébrique, $|\operatorname{Hom}_{Alg/k}(K, \overline{k})|$ est indépendant de $\overline{k}/k$ et $\leq [K : k]$.*

Démonstration. L'indépendance de la clôture algébrique vient du fait que si $\overline{k}'/k$ est une autre clôture algébrique tout k-isomorphisme $\phi : \overline{k} \tilde{\to} \overline{k}'$ induit une bijection $\phi \circ - : \operatorname{Hom}_{Alg/k}(K, \overline{k}) \tilde{\to} \operatorname{Hom}_{Alg/k}(K,$
Par la propriété universelle du produit tensoriel de k-algèbres on a une bijection canonique

$$\operatorname{Hom}_{Alg/k}(K, \overline{k}) \tilde{\to} \operatorname{Hom}_{Alg/\overline{k}}(\overline{k} \otimes_k K, \overline{k})$$

Et comme $[K : k] = \dim_{\overline{k}} \overline{k} \otimes_k K$, l'assertion résulte immédiatement du lemme ci-dessous. □

15.3.4

Soit K/k une extension de corps. On dit que $x \in K$ est *séparable sur* k si le polynôme minimal $P_x \in k[T]$ de x sur k est séparable. Le corollaire suivant décrit qu'elle est la bonne généralisation - en termes d'extensions de corps - de la notion de polynômes séparables.

Corollaire. *Soit K/k une extension algébrique. Les propriétés suivantes sont équivalentes.*

1. *Tout élément de K est séparable sur k ;*
2. *Pour toute clôture algébrique $\overline{k}/k$, $\overline{k} \otimes_k K$ est une $\overline{k}$-algèbre réduite.*

Si, de plus, K/k est finie, ces propriétés sont aussi équivalentes à

3. *Pour toute clôture algébrique $\overline{k}/k$, $|\operatorname{Hom}_{Alg/k}(K, \overline{k})| = [K : k]$.*

Démonstration. Montrons d'abord (1) $\Rightarrow$ (3) $\Leftrightarrow$ (2) lorsque K/k est finie. On a déjà observé que $\operatorname{Hom}_{Alg/k}(K, \overline{k}) \tilde{\to} \operatorname{Hom}_{Alg/\overline{k}}(\overline{k} \otimes_k K, \overline{k})$ et que $[K : k] = \dim_{\overline{k}}(\overline{k} \otimes_k K)$ donc (2) $\Leftrightarrow$ (3) résulte du Lemme **??**. Pour (1) $\Rightarrow$ (3) rappelons que si $k \subset K' \subset K$ est une sous-k-extension, le morphisme de restriction

$$\operatorname{Hom}_{Alg/k}(K, \overline{k}) \to \operatorname{Hom}_{Alg/k}(K', \overline{k}),\ \phi \to \phi|_{K'}$$

est surjectif et la fibre au-dessus de $\phi : K' \to \overline{k}$ est l'ensemble $\operatorname{Hom}_{Alg/K',\phi}(K, \overline{k})$ des k-plongements avec $\overline{k}$ muni de la structure de K'-algèbre donnée par $\phi : K' \to \overline{k}$. Donc

$$(*)\quad |\operatorname{Hom}_{Alg/k}(K, \overline{k})| = \sum_{\phi \in \operatorname{Hom}_{Alg/k}(K', \overline{k})} |\operatorname{Hom}_{Alg/K',\phi}(K, \overline{k})|.$$

Cette observation permet de faire un raisonnement par récurrence sur le nombre minimal n de générateurs de K/k comme k-extension. Si $n = 1$, $K = k(x) = k[T]/P_x$ et on a vu que dans ce cas

$$|\operatorname{Hom}_{Alg/k}(K, \overline{k})| = |Z_{\overline{k}}(P_x)|.$$

Or comme $P_x \in k[T]$ est séparable, $|Z_{\overline{k}}(P_x)| = \deg(P_x)(= [k(x) : k])$. Si le nombre minimal de générateurs de K/k comme k-extension est n, on peut écrire $K = k(x_1, \ldots, x_n) = k(x_1, \ldots, x_{n-1})(x_n)$. Puisque $K' = k(x_1, \ldots, x_{n-1})/k$ est engendrée par $\leq n - 1$ générateurs comme k-extension et vérifie (1), l'hypothèse de récurrence montre que $|\operatorname{Hom}_{Alg/k}(K', \overline{k})| = [K' : K]$ alors que par le cas $n = 1$, pour tout k-plongement $\phi : K' \to \overline{k}$, on a $|\operatorname{Hom}_{Alg/K',\phi}(K, \overline{k})| = [K : K']$. De $(*)$ on déduit

$$|\operatorname{Hom}_{Alg/k}(K, \overline{k})| = \sum_{\phi \in \operatorname{Hom}_{Alg/k}(K', \overline{k})} [K : K'] = [K' : k][K : K'] = [K : k].$$

Pour (2) $\Rightarrow$ (1), on n'a pas besoin de supposer K/k finie. En effet, observons que si $k \subset K' \subset K$ est une sous-k-extension, le morphisme de $\overline{k}$-algèbres $\overline{k} \otimes_k K' \to \overline{k} \otimes_k K$ est injectif. En effet, il suffit pour cela de choisir une k-base e_i, $i \in I$ de K telle que e_i, $i \in I'$ soit une k-base de K' pour un certain sous-ensemble $I' \subset I$ et d'observer que $1 \otimes e_i$, $i \in I$ est encore une $\overline{k}$-base de $\overline{k} \otimes K$ (le produit tensoriel commute aux sommes directes). Or, d'après **??**, $x \in K$ est séparable sur k si et seulement si $\overline{k} \otimes_k k(x)$ est réduite. Comme on vient de voir que $\overline{k} \otimes_k k(x)$ est une

sous-$\overline{k}$-algèbre de, cela montre (2) $\Rightarrow$ (1). Enfin, on sait déjà que (1) $\Rightarrow$ (2) lorsque K/k est finie. Pour le cas général, tout élément de $\overline{k} \otimes_k K$ s'écrit comme combinaison k-linéaire finie d'éléments de la forme $\lambda \otimes x$, $\lambda \in \overline{k}$, $x \in K$ donc il est contenu dans une sous-$\overline{k}$-algèbre de la forme $\overline{k} \otimes_k k(x_1, \ldots, x_n)$, où $x_1, \ldots, x_n \in K$. Comme les $x_1, \ldots, x_n$ sont algébriques sur k, $[k(x_1, \ldots, x_n) : k]$ est fini et $k(x_1, \ldots, x_n)/k$ vérifie (1) donc l'assertion résulte de (1) $\Rightarrow$ (2) dans le cas où K/k est finie. □

On dit qu'une extension algébrique K/k qui vérifie les propriétés équivalentes du Corollaire ci-dessus est *séparable*. L'équivalence (1) $\Rightarrow$ (3) lorsque K/k est finie montre en particulier que $x \in K$ est séparable sur k si et seulement si $k(x) = k[T]/P_x/k$ est une extension séparable puisque

$$|\operatorname{Hom}_{Alg/k}(k[T]/P_x, \overline{k})| = |Z_{\overline{k}}(P_x)| \leq \deg(P_x) = [k(x) : k]$$

avec égalité si et seulement si $P_x \in k[T]$ est séparable.

Exemple. Si k est de caractéristique 0, toute extension algébrique de k est séparable (par la caractérisation (1) de **??**). L'extension $\mathbb{F}_p(X)[T]/T^p - X/\mathbb{F}_p(X)$ n'est pas séparable.

15.3.5

Corollaire. *Soit K_3/K_2 et K_2/K_1 des extensions algébriques. Alors K_3/K_1 est séparable si et seulement si K_3/K_2 et K_2/K_1 sont séparables.*

Démonstration. Si K_3/K_1 est séparable, la caractérisation (1) de la séparabilité montre immédiatement que K_2/K_1 est séparable et, puisque le polynôme minimal P_{x,K_2} d'un élément $x \in K_3$ sur K_2 divise dans $K_2[T]$ le polynôme minimal P_{x,K_1} de x sur K_1, que K_3/K_2 est aussi séparable. Réciproquement, si K_3/K_1 est finie, $(*)$ dans la preuve du Corollaire de **??** montre que

$$|\operatorname{Hom}_{Alg/K_1}(K_3, \overline{k})| = \sum_{\phi \in \operatorname{Hom}_{Alg/K_1}(K_2, \overline{k})} |\operatorname{Hom}_{Alg/K_2,\phi}(K_3, \overline{k})| = [K_3 : K_2][K_2 : K_1] = [K_3 : K_1].$$

Si K_3/K_1 n'est pas finie, soit $x \in K_3$. Par hypothèse son polynôme minimal sur K_2 s'écrit $P_{x,K_2} = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in K_2[T]$ et est séparable donc x est séparable sur $K_2' = K_1(a_{n-1}, \ldots, a_0)$ (puisque son polynôme minimal sur K_2' est encore P_{x,K_2}) *i.e.* $K_2'(x)/K_2'$ est séparable ; $K_2'(x)/K_2'$ et K_2'/K_1 sont donc finies (car algébriques de type fini) et séparables donc $K_2'(x)/K_1$ est séparable par transitivité. □

15.3.6

Corollaire. (Élément primitif) *Toute extension K/k séparable finie est monogène i.e. de la forme $K = k(x)/k$ pour un certain $x \in K$.*

Démonstration. Supposons d'abord que k est *infini*. Pour tout $x \in K$, on a vu que l'application de restriction

$$-|_{k(x)} : \operatorname{Hom}_{Alg/k}(K, \overline{k}) \to \operatorname{Hom}_{Alg/k}(k(x), \overline{k})$$

était toujours surjective. De plus, puisque K/k est séparable finie, on a $|\operatorname{Hom}_{Alg/k}(K,\overline{k})| = [K:k]$ et $|\operatorname{Hom}_{Alg/k}(k(x),\overline{k})| = [k(x):k]$. Donc

$$K = k(x) \Leftrightarrow [K:k] = [k(x):k] \Leftrightarrow -|_{k(x)} : \operatorname{Hom}_{Alg/k}(K,\overline{k}) \to \operatorname{Hom}_{Alg/k}(k(x),\overline{k}) \text{ est injective}$$

Mais comme l'évaluation en x, $\operatorname{Hom}_{Alg/k}(k(x),\overline{k}) \to \overline{k}$, $\phi \to \phi(x)$ est injective, $-|_{k(x)} : \operatorname{Hom}_{Alg/k}(K,\overline{k}) \to \operatorname{Hom}_{Alg/k}(k(x),\overline{k})$ est injective si et seulement si l'évaluation en x $\operatorname{Hom}_{Alg/k}(K,\overline{k}) \to \overline{k}$, $\phi \to \phi(x)$ est injective autrement dit, si et seulement si $x \notin \ker(\phi_1 - \phi_2)$, $\phi_1 \neq \phi_2 \in \operatorname{Hom}_{Alg/k}(K,\overline{k})$. Comme $\operatorname{Hom}_{Alg/k}(K,\overline{k})$ est fini et que les $\ker(\phi_1 - \phi_2) \subsetneq K$ sont des sous-k-espace vectoriels stricts, la conclusion résulte du Lemme 1 ci-dessous.

Supposons maintenant que k est fini. Le corps K est donc également fini (de cardinal $|k|^{[K:k]}$) et, d'après le Lemme 2 ci-dessous, le groupe multiplicatif $K^\times$ est cyclique. Tout générateur x du groupe $K^\times$ vérifie $K = k(x)$. □

Lemme 1. *Soit k un corps infini et V un k-espace vectoriel de dimension finie. Si $W_1, \dots, W_r \subsetneq V$ sont des sous-k-espaces vectoriels stricts, $V \setminus \cup_{1\leq i\leq r} V_i \neq \varnothing$.*

Démonstration. On procède par récurrence sur la k-dimension n de V. Si $n = 1$, c'est immédiat. Si $n \geq 1$, il suffit de montrer l'énoncé dans le cas où les W_i, $i = 1, \dots, r$ sont des hyperplans deux à deux distincts. Comme $W_1 \cap W_i \subsetneq W_1$, par hypothèse de récurrence il existe $w \in W_1 \setminus \cup_{2\leq i\leq r} W_1 \cap W_i$. Fixons également $v \in V \setminus W_1$ et notons $D := v + kw \subset V$. Puisque $v \in V \setminus W_1$, $D \cap W_1 = \varnothing$ et, pour $i = 1, \dots, r$, $D \cap W_i$ contient au plus un élément car si $v + aw, v + bw \in W_i$, $(a-b)w \in W_i$ donc, puisque $w \in V \setminus W_i$, $a = b$. Cela montre que $D \cap \cup_{1\leq i\leq r} W_i$ est fini et on conclut en utilisant que D est infini puisque k l'est. □

Lemme 2. *Soit k un corps. Tout sous-groupe fini G du groupe multiplicatif $k^\times$ est cyclique.*

Démonstration. Notons $n = |G|$ et m le ppcm des ordres des éléments de G. Comme G est un groupe abélien fini, il contient un élément d'ordre m (penser au théorème de structure... ou le vérifier à la main). Il suffit donc de montrer que $m = n$. Mais par définition de m, $G \subset Z_k(T^m - 1)$. Or $|Z_k(T^m - 1)| \leq \deg(T^m - 1) = m$. Donc $n = |G| \leq |Z_k(T^m - 1)| = m \leq n$ montre bien que $m = n$. □

Exemples.

— Une extension finie non séparable n'est en général pas monogène. Par exemple $K := \mathbb{F}_p(X,Y)/k := \mathbb{F}_p(X^p, Y^p))$ est finie, de $\mathbb{F}_p(X^p, Y^p)$-base X^iY^j, $0 \leq i, j \leq p-1$ mais elle n'est pas monogène car tout $x \in K$ vérifie $x^p \in k$ donc son polynôme minimal sur k divise $T^p - x^p$ et est donc de degré $\leq p$.

— La preuve de **??** n'est pas constructive. On verra plus loin comment en trouver. Par exemple, on verra que $[\mathbb{Q}(\sqrt[3]{5} + j) : \mathbb{Q}] = 6$ et donc que $\mathbb{Q}(\sqrt[2]{5}, j) = \mathbb{Q}(\sqrt[3]{5} + j)$.

15.4 Corps finis

Soit k un corps et $c_k : \mathbb{Z} \to k$ le morphisme caractéristique de k et p la caractéristique de k. Comme k est intègre,

— soit $p = 0$, auquel cas, par propriété universelle de l'anneau des fractions, $c_k : \mathbb{Z} \to k$ se factorise en un morphisme de corps $c_k : \mathbb{Q} \hookrightarrow k$;

— soit $p = 0$, auquel cas, par propriété universelle du quotient, $c_k : \mathbb{Z} \to k$ se factorise en un morphisme de corps $c_k : \mathbb{F}_p \hookrightarrow k$;

Si $p = 0$ (resp. $p > 0$) on dit que $\mathbb{Q}$ (resp. $\mathbb{F}_p$) est le sous-corps premier de k (c'est le plus petit sous-corps de k).

En particulier, un corps fini $\mathbb{F}$ est nécessairement de caractéristique $p > 0$ et c'est un $\mathbb{F}_p$-espace vectoriel de dimension finie. On doit donc avoir $|\mathbb{F}| = p^{[\mathbb{F}:\mathbb{F}_p]}$.

L'une des spécificités fondamentales des corps de caractéristique $p > 0$ est l'existence du Frobenius.

15.4.1

Lemme. (Frobenius) *Soit k un corps de caractéristique $p > 0$. L'application $F_k : k \to k$, $x \to x^p$ est un endomorphisme de $\mathbb{F}_p$-algèbre.*

Démonstration. La seule chose à vérifier est l'additivité. Cela résulte de la formule du binôme de Newton. Pour tout $a, b \in k$

$$F_k(a+b) = (a+b)^p = \sum_{0 \leq i \leq p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

puisque $p | \binom{p}{i}$, $i = 1, \ldots, p-1$. □

Remarque. On prendra garde que si le Frobenius est toujours injectif (puisque c'est un morphisme de corps), il n'est pas toujours surjectif. Par exemple, m'image du Frobenius sur $\mathbb{F}_p(T)$ est le sous-corps strict $\mathbb{F}_p(T^p) \subsetneq \mathbb{F}_p(T)$. Le Frobenius est cependant toujours surjectif sur un corps $\mathbb{F}$ fini (injectif entre deux ensembles de mêmes cardinal) ou algébriquement clos (puisque les polynômes $T^p - x$ ont tous une racine dans $\mathbb{F}$). La surjectivité du Frobenius est lié à la notion de corps parfait.

15.4.2

Lemme. *Soit k un corps de caractéristique $p > 0$. Pour tout $r \in \mathbb{Z}_{\geq 1}$, le sous-ensemble $\mathbb{F}_p \subset Z_k(T^{p^r} - T) \subset k$ est un sous-corps fini, de cardinal p^s avec $s | r$.*

Démonstration. Puisque $\mathbb{F} := Z_k(T^{p^r} - T)$ est l'égalisateur de deux endomorphismes de $\mathbb{F}_p$-algèbres : $F_k^{p^r}, \mathrm{Id} : k \to k$, c'est une sous-$\mathbb{F}_p$-algèbre (donc un sous-corps) de k. Explicitement, $\mathbb{F} = \ker(F_k^{p^r} - \mathrm{Id}) \subset k$ est un sous-$\mathbb{F}_p$-espace vectoriel, $1 \in \mathbb{F}$ et pour tout $a, 0 \neq b \in \mathbb{F}$, $(ab^{-1})^{p^r} = a^{p^r}(b^{-1})^{p^r} = ab^{-1}$ donc $ab^{-1} \in \mathbb{F}$. Comme $|\mathbb{F}| < +\infty$, $\mathbb{F}$ est un $\mathbb{F}_p$-espace vectoriel de dimension finie - disons s - donc de cardinal p^s. Soit $x \in \mathbb{F}^\times$ un générateur de $\mathbb{F}^\times$. On a donc $\mathbb{F} \subset Z_k(T^{p^s} - T)$. Or $p^s = |\mathbb{F}| \leq |Z_k(T^{p^s} - T)| \leq p^s$ donc $\mathbb{F} = Z_k(T^{p^s} - T)$ et $T^{p^s} - T$ est totalement décomposé sur $\mathbb{F}$. Autrement dit, $\mathbb{F}$ est un corps de décomposition de $T^{p^s} - T$ sur $\mathbb{F}_p$. Comme $T^{p^s} - T | T^{p^r} - T$ dans $\overline{\mathbb{F}}_p[T] \subset \overline{k}[T]$ donc dans $\mathbb{F}_p[T]$, on a

$$\mathbb{F}_p \subset \mathbb{F} = Z_k(T^{p^s} - T) = Z_{\overline{k}}(T^{p^s} - T) \subset Z_{\overline{k}}(T^{p^r} - T) =: \mathbb{F}_{\overline{k}}$$

Comme $T^{p^r} - T \in \mathbb{F}_p[T]$ est séparable, $|\mathbb{F}_{\overline{k}}| = p^r$. On doit donc avoir

$$r = [\mathbb{F}_{\overline{k}} : \mathbb{F}_p] = [\mathbb{F}_{\overline{k}} : \mathbb{F}][\mathbb{F} : \mathbb{F}_p] = [\mathbb{F}_{\overline{k}} : \mathbb{F}]s$$

donc $s|r$. □

15.4.3

Corollaire. (Corps finis) *Pour tout premier $p > 0$ et tout $r \in \mathbb{Z}_{\geq 1}$, il existe un corps fini $\mathbb{F}_{p^r}$ à $\mathbb{F}_{p^r}$-éléments, unique à isomorphisme (non-unique près) ; c'est le corps de décomposition de $T^{p^r} - T \in \mathbb{F}_p[T]$ sur $\mathbb{F}_p$. De plus,*

1. *pour tout $r, s \in \mathbb{Z}_{\geq 1}$, $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^r}$ si et seulement si $s|r$;*
2. *toute extension algébrique $K/\mathbb{F}_p$ est réunion de ses sous-corps finis. En particulier, $\overline{\mathbb{F}}_p = \cup_{r \geq 1} \overline{\mathbb{F}}_{p^r}$.*

Démonstration. Soit $\overline{\mathbb{F}}_p/\mathbb{F}_p$ une clôture algébrique et $\mathbb{F}_p \subset \mathbb{F}_{p^r} := \mathbb{F}_p(Z_{\overline{\mathbb{F}}_p}(T^{p^r} - T)) \subset \overline{\mathbb{F}}_p$ le corps de décomposition correspondant de $T ? p^r - T$ sur $\mathbb{F}_p$. D'après **??**, $Z_{\overline{\mathbb{F}}_p}(T^{p^r} - T)$ est une extension algébrique de $\mathbb{F}_p$ vérifiant tautologiquement $Z_{\overline{\mathbb{F}}_p}(T^{p^r} - T) = \mathbb{F}_p(Z_{\overline{\mathbb{F}}_p}(T^{p^r} - T))$; donc $\mathbb{F}_{p^r} = Z_{\overline{\mathbb{F}}_p}(T^{p^r} - T)$. De plus, comme $T^{p^r} - T \in \mathbb{F}_p[T]$ est séparable et totalement décomposé sur $\overline{\mathbb{F}}_p$, $|\mathbb{F}_{p^r}| = |Z_{\overline{\mathbb{F}}_p}(T^{p^r} - T)| = p^r$. Cela montre l'existence de $\mathbb{F}_{p^r}$. Pour l'uncité, soit $\mathbb{F}$ est un corps fini à p^r éléments ; c'est une extension finie donc algébrique de $\mathbb{F}_p$ donc on peut le plonger dans $\overline{\mathbb{F}}_p$. Comme $|\mathbb{F}^\times| = p^{r-1}$, tout $0 \neq x \in \mathbb{F}$ vérifie $x^{p^r - 1} = 1$ donc $\mathbb{F} \subset Z_{\overline{\mathbb{F}}_p}(T^{p^r} - T)$. Par cardinalité, $\mathbb{F} = Z_{\overline{\mathbb{F}}_p}(T^{p^r} - T)$. La condition nécessaire de (1) résulte de

$$r = [\mathbb{F}_{p^r} : \mathbb{F}_p] = [\mathbb{F}_{p^r} : \mathbb{F}_{p^s}][\mathbb{F}_{p^s} : \mathbb{F}_p] = [\mathbb{F}_{p^r} : \mathbb{F}_{p^s}]s.$$

Pour la condition suffisante, si $s|r$, on a $p^s - 1 | p^r - 1$ car

$$p^r - 1 = (p^s)^{r/s} - 1 = (p^s - 1) \sum_{0 \leq i \leq r/s - 1} p^{si}.$$

Or $0 \neq x \in \mathbb{F}_{p^s} \Rightarrow x^{p^s - 1} = 1 \Rightarrow x^{p^r - 1} = (x^{p^s - 1})^{(p^r - 1)/(p^s - 1)} = 1 \Rightarrow x \in \mathbb{F}_{p^r}$. (2) est immédiat. □

15.5 Polynôme caractéristique, trace et norme

15.5.1

Soit A une k-algèbre de dimension finie. A tout $a \in K$ on peut associer l'automorphisme de k-espace vectoriel $L_a : A \to A$, $b \to ab$. On note

$$\chi_{A/k}(a) := det(L_a - T\,\mathrm{Id}\,|A) \in k[T]$$

son *polynôme caractéristique*, $tr_{A/k}(a) := tr_k(L_a : A \to A) \in k$ sa *trace* et $N_{A/k} := det(L_a) \in k$ son déterminant - appelé *norme*. On dispose en particulier d'une forme linéaire $tr_{A/k} : A \to k$ et d'un morphisme de groupes $N_{A/k} : A^\times \to k^\times$.

15.5.2

Lemme. *Soit K/k une extension finie. Pour tout $x \in K$, on a $\chi_{K/k}(x) = P_x^{[K:k(x)]}$ où $P_x \in k[T]$ est le polynôme minimal de x sur k. En particulier, $tr_{K/k}(x) = [K : k(x)]tr_{k(x)/k}(x)$ et $N_{K/k}(x) = N_{k(x)/k}(x)^{[K:k(x)]}$.*

Démonstration. Notons $n := [K : k]$, $q_x := [K : k(x)]$, $n_x := [k(x) : k]$. Fixons une $k(x)$-base $y_1, \ldots, y_{q_x}$ de K. On a une décomposition $K = \oplus_{1\leq i\leq q_x} k(x)y_i$ en k-espaces vectoriels $k(x)y_i \subset K$ L_x-stables et pour chaque $i = 1, \ldots, q_x$, la matrice de $L_x : k(x)y_i \to k(x)y_i$ dans la k-base $x^j y_i$, $j = 0, \ldots, n_x - 1$ est la matrice compagnon $C(P_x)$ de P_x. Donc la matrice de $L_x : K \to K$ dans la k-base $y_i x^j$, $1 \leq i \leq q_x$, $0 \leq j \leq n_x - 1$ de K est la matrice diagonale par blocs de taille $n \times n$ dont tous les blocs diagonaux valent $C(P_x)$. On conclut en utilisant que le polynôme minimal et le polynôme caractéristique d'une matrice compagnon $C(P)$ coïncident et sont égaux à P. □

15.5.3

Lemme. *Soit K_3/K_2 et K_2/K_1 des extensions finies. Alors $tr_{K_2/K_1} \circ tr_{K_3/K_2} = tr_{K_3/K_1}$.*

Démonstration. Notons $n_3 := [K_3 : K_2]$, $n_2 := [K_2 : K_1]$. Soit $e_{3,i}$, $i = 1, \ldots, n_3$ une K_2-base de K_3 et $e_{2,i}$, $i = 1, \ldots, n_2$ une K_1-base de K_2. Soit $x \in K_3$. Notons $A_3 := (a_{3,i,j})_{1\leq i,j\leq n_3} \in M_{n_3}(K_2)$ la matrice du K_2-endomorphisme $L_x : K_3 \to K_3$ dans $e_{3,i}$, $i = 1, \ldots, n_3$ et pour chaque $a_{3,i,j}$, notons $A_{2,i,j} := (a_{2,i,j,r,s})_{1\leq r,s\leq n_2} \in M_{n_2}(K_1)$ la matrice du K_1-endomorphisme $L_{a_{3,i,j}} : K_2 \to K_2$ dans $e_{2,i}$, $i = 1, \ldots, n_2$. Dans la K_1-base $e_{3,i}e_{2,j}$, $1 \leq i \leq n_3, 1 \leq j \leq n_2$ de K_3, la matrice du K_1-endomorphisme $L_x : K_3 \to K_3$ est la matrice par blocs $(A_{2,i,j})_{1\leq i,j\leq n_3} \in M_{n_2 n_3}(K_1)$. En particulier

$$tr_{K_2/K_1}(tr_{K_3/K_2}(x)) = \sum_{1\leq i\leq n_3} tr_{K_2/K_1}(a_{3,i,i}) = \sum_{1\leq i\leq n_3}\sum_{1\leq j\leq n_2} a_{2,i,i,j,j} = tr_{K_3/K_1}(x).$$

□

Remarque. On peut aussi montrer que $N_{K_2/K_1} \circ N_{K_3/K_2} = N_{K_3/K_1}$ mais c'est un peu plus délicat.

15.5.4

Proposition *Une extension finie K/k est séparable si et seulement si $tr_{K/k} : K \to k$ est non nulle (i.e. surjective).*

Démonstration. En prenant des bases adaptées, on vérifie facilement que si $k \subset K' \subset K$ est une sous-extension, $tr_{K/k} = tr_{K'/k} \circ tr_{K/K'}$. En particulier, pour tout $x \in K$, $tr_{K/k} = tr_{k(x)/k} \circ tr_{K/k(x)}$. Si K/k est séparable, on sait qu'il existe $x \in K$ tel que $K = k(x)$. Il suffit donc de montrer que $x \in K$ est séparable sur k si et seulement si $tr_{k(x)/k} : k(x) \to k$ est surjective. De plus, la suite exacte courte de k-espaces vectoriels

$$0 \to \ker(tr_{K/k}) \to K \overset{tr_{K/k}}{\to} \operatorname{im}(tr_{K/k}) \to 0$$

reste exacte après $\overline{k} \otimes_k -$

$$0 \to \overline{k} \otimes_k \ker(tr_{K/k}) \to \overline{k} \otimes_k K \overset{\mathrm{Id} \otimes tr_{K/k}}{\to} \overline{k} \otimes_k \operatorname{im}(tr_{K/k}) \to 0$$

Autrement dit, $\overline{k} \otimes_k \ker(tr_{K/k}) = \ker(\mathrm{Id} \otimes tr_{K/k} tr_{K/k})$, $\overline{k} \otimes_k \operatorname{im}(tr_{K/k}) = \operatorname{im}(\mathrm{Id} \otimes tr_{K/k} tr_{K/k})$. Il suffit donc de montrer que $x \in K$ est séparable si et seulement si $\mathrm{Id} \otimes tr_{K/k} tr_{K/k} : \overline{k} \otimes_k K \to \overline{k}$ est non nulle. P en écrivant $P_x = \prod_{1 \leq i \leq r} (T - x_i)^{n_i}$ dans $\overline{k}[T]$ avec les $x_1, \ldots, x_n \in \overline{k}$ deux à deux distincts, le lemme des restes Chinois nous donne un isomorphisme de $\overline{k}$-algèbres explicite

$$\overline{k} \otimes_k K = \overline{k} \otimes_k k[T]/P_x = \overline{k}[T]/P_x \tilde{\to} \prod_{1 \leq i \leq r} \overline{k}[T]/(T - x_i)^{n_i}$$

et en prenant une $\overline{k}$-base adaptée à cette décomposition, on obtient $tr_{\overline{k} \otimes_k K/\overline{k}} = \sum_{1 \leq i \leq r} tr_{A_i/\overline{k}}$, où $A_i := \overline{k}[T]/(T - x_i)^{n_i}$, $i = 1, \ldots, r$.

— Si x est séparable sur k, $n_1 = \cdots = n_r = 1$ donc $A_i = \overline{k}$ donc t $tr_{A_i/\overline{k}} = \mathrm{Id}$, $i = 1, \ldots, n$ et $tr_{\overline{k} \otimes_k K/\overline{k}} : \overline{k}^n \to \overline{k}$, $(a_1, \ldots, a_n) \to a_1 + \cdots + a_n$ est clairement surjective.

— Si x n'est pas séparable sur k, k est de caractéristique $p > 0$ et $P_x = P(T^{p^s})$ avec $P \in k[T]$ séparable et $r \geq 1$ (*cf.* **??**). En écrivant $P = \prod_{1 \leq i \leq r} (T - \alpha_i)$ et $\alpha_i = x_i^{p^s}$, $i = 1, \ldots, r$ dans $\overline{k}$, on en déduit

$$P_x(T) = \prod_{1 \leq i \leq r} (T^{p^s} - x_i^{p^s}) = \prod_{1 \leq i \leq r} (T - x_i)^{p^s},$$

autrement dit $n_1 = \cdots = n_r = p^s$. Or tout élément $a \in A_i$ s'écrit sous la forme $a = a_0 + \nu$ avec $a_0 \in \overline{k}$ et $\nu \in A_i$ nilpotent. Donc $tr_{A_i/\overline{k}}(a) = tr_{A_i/\overline{k}}(a_0) + tr_{A_i/\overline{k}}(\nu) = p^s a_0 = 0$.

□

Chapitre 16

Correspondance de Galois

16.1 Extensions galoisiennes

16.1.1

Lemme *Soit K/k une extension finie. Les propriétés suivantes sont équivalentes.*

1. *K/k est normale et séparable ;*
2. *K/k est le corps de décomposition d'un polynôme séparable sur k ;*
3. *$|\operatorname{Aut}(K/k)| = [K : k]$;*
4. *$k = K^{\operatorname{Aut}(K/k)}$;*
5. *Pour tout $x \in K$, son polynôme minimal $P_x \in k[T]$ sur k se décompose comme $P_x = \prod_{y \in \operatorname{Aut}(K/k)\cdot x}(T - y)$ dans $K[T]$;*

Démonstration. On se fixe une clôture algébrique $\overline{k}/k$. Pour $x \in K$ on note $P_x \in k[T]$ son polynôme minimal sur k. On va montrer que (1) $\Leftrightarrow$ (i), $i = 2, 3, 4$ et (4) $\Leftrightarrow$ (5)

— (1) $\Rightarrow$ (2) résulte de l'élément primitif **??** et de la définition d'une extension normale. (2) $\Rightarrow$ (1) Si K est le corps de décomposition d'un polynôme $P \in k[T]$ séparable, K/k est normale. Mais par **??**, K/k est aussi séparable puisque si on note $Z_K(P) = \{x_1, \ldots, x_n\}$, $K = k(x_1, \ldots, x_n)/k$ $K = k(x_1, \ldots, x_n)/k$ et chacune des extensions $k(x_1, \ldots, x_i)/k(x_1, \ldots, x_{i-1})$ est séparable (monogène engendrée par un élément séparable *cf.* caractérisation (3) de **??**).

— (1) $\Leftrightarrow$ (3) Pour toute clôture algébrique $k \subset K \subset \overline{k}$ on a toujours $\operatorname{Aut}(K/k) \hookrightarrow \operatorname{Hom}_{Alg/k}(K, \overline{k})$ et $|\operatorname{Hom}_{Alg/k}(K, \overline{k})| \leq [K : k]$. Donc $|\operatorname{Aut}(K/k)| = [K : k]$ si et seulement si $\operatorname{Aut}(K/k) \tilde{\to} \operatorname{Hom}_{Alg/k}(K, \overline{k}$ (*i.e.* K/k est normale) et $|\operatorname{Hom}_{Alg/k}(K, \overline{k})| = |K : k]$ (*i.e.* K/k est séparable).

— (1) $\Rightarrow$ (5) Comme K/k est séparable, pour tout $x \in K$, son polynôme minimal $P_x \in k[T]$ sur k se décompose comme $P_x = \prod_{y \in Z_{\overline{k}}(P_x)}(T - y)$ dans $\overline{k}[T]$. Mais comme K/k est normale,

$$Z_{\overline{k}}(P_x) = \{\sigma(x) \mid \sigma \in \operatorname{Hom}_{Alg/k}(K, \overline{k})\} = \operatorname{Aut}(K/k) \cdot x.$$

(5) $\Rightarrow$ (1) Pour tout $x \in K$, la décomposition $P_x = \prod_{y \in \mathrm{Aut}(K/k)\cdot x}(T-y)$ dans $K[T]$ montre que P_x est séparable (donc que K/k est séparable) et est totalement décomposé sur K (donc que K/k est normale).

— (5) $\Rightarrow$ (4) Si $x \in K \setminus k$, son polynôme minimal $P_x \in k[T]$ sur k est de degré ≥ 2. Or, par hypothèse $P_x = \prod_{y \in \mathrm{Aut}(K/k)\cdot x}(T-y)$ donc il existe $\sigma \in \mathrm{Aut}(K/k)$ tel que $\sigma(x) \neq x$. Autrement dit $x \in K \setminus K^{\mathrm{Aut}(K/k)}$. (4) $\Rightarrow$ (5) Pour tout $x \in K$ notons $\widetilde{P}_x := \prod_{y \in \mathrm{Aut}(K/k)\cdot x}(T-y) \in K[T]$. Dans $\overline{k}[T]$ on a

$$\prod_{y \in Z_{\overline{k}}(P_x)} (T-y) = \prod_{y \in \mathrm{Aut}(\overline{k}/k)\cdot x} (T-y) | P_x.$$

Et comme pour tout $\sigma \in \mathrm{Aut}(K/k)$ il existe $\widetilde{\sigma} \in \mathrm{Aut}(\overline{k}/k)$ tel que le diagramme suivant commute (**??**)

$$\begin{array}{ccc} \overline{k} & \xrightarrow[\simeq]{\widetilde{\sigma}} & \overline{k} \\ \uparrow & & \uparrow \\ K & \xrightarrow[\simeq]{\sigma} & K, \end{array}$$

on a $\mathrm{Aut}(K/k)\cdot x \subset \mathrm{Aut}(\overline{k}/k)\cdot x$ donc $\widetilde{P}_x | P_x$(dans $\overline{k}[T]$ donc) dans $K[T]$. Par ailleurs, $\widetilde{P}_x(x) = 0$ et pour tout $\sigma \in \mathrm{Aut}(K/k)$ $\sigma\widetilde{P}_x = \widetilde{P}_x$ donc $\widetilde{P}_x \in K^{\mathrm{Aut}(K/k)}[T] = k[T]$. Cela impose $P_x | \widetilde{P}_x$ donc $P_x = \widetilde{P}_x$.

□

On dit qu'une extension finie K/k qui vérifie les propriétés équivalentes du Lemme **??** est *galoisienne*. Lorsque K/k est galoisienne, on note $\mathrm{Gal}(K/k) := \mathrm{Aut}(K/k)$ et on dit que c'est le *groupe de Galois* de K/k.

Exemple. On a vu que $\mathbb{Q}(\sqrt[3]{5}, j)/\mathbb{Q}$ était galoisienne et que $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{5}, j)/\mathbb{Q}) = \mathcal{S}_3$.

16.2

Exemples classiques. Si k est corps on note $\mu_n(k) := Z_k(T^n - 1) \subset k^\times$; c'est un sous-groupe fini donc cyclique (Lemme 2 de la preuve de **??**) de $k^\times$.

16.2.1

Corps finis. Pour tout $r \in \mathbb{Z}_{\geq 1}$, $\mathbb{F}_{p^r}/\mathbb{F}_p$ est galoisienne puisque c'est le corps de décomposition du polynôme séparable $T^{p^r} - T \in \mathbb{F}_p[T]$ sur $\mathbb{F}_p$. En outre, $F : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$, $x \to x^p \in \mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$. De plus, si $x \in \mathbb{F}_{p^r}^\times$ est un générateur, les éléments $x, F(x), \ldots, F^{r-1}(x)$ sont tous distincts donc F est d'ordre $\geq r$. Mais par la caractérisation (3) d'une extension galoisienne $|\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)| = [\mathbb{F}_{p^r} : \mathbb{F}_p] = r$. Donc $F : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ est d'ordre exactement r et

$$\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) = \langle F \rangle \simeq \mathbb{Z}/r.$$

16.2.2

Extensions cyclotomiques. Pour tout corps k et $n \in \mathbb{Z}_{\geq 1}$, la n-ième *extension cyclotomique* k_n/k de k est par définition le corps de décomposition de $T^n - 1 \in k[T]$ sur k. Si on note p la caractéristique de k et si $p > 0$ on a, en écrivant $n = p^r m$, $p \nmid m$

$$T^n - 1 = (T^m - 1)^{p^r}$$

donc $k_n = k_m$. On peut par conséquent supposer que $p \nmid n$ donc que $T^n - 1 \in k[T]$ est séparable et k_n/k galoisienne. Fixons une clôture algébrique $\overline{k}/k$. Puisque $T^n - 1$ est séparable $\mu_n := \mu_n(\overline{k}) = Z_{\overline{k}}(T^n - 1) \subset \overline{k}^\times$ est (cyclique) d'ordre n. De plus, pour tout $\sigma \in \mathrm{Gal}(k_n/k)$ et $\zeta, \zeta' \in \mu_n$ on a $\sigma(\zeta\zeta') = \sigma(\zeta)\sigma(\zeta')$ puisque σ est un morphisme de corps. Donc la restriction à $\mu_n \subset k_n$ induit un morphisme de groupes

$$\chi_k : \mathrm{Gal}(k_n/k) \to \mathrm{Aut}_{Grp}(\mu_n)$$

qui est injectif puisque $k_n = k(\mu_n)$. Le choix d'un générateur ζ_n de μ_n définit un isomorphisme de groupes (non canonique) $\mathbb{Z}/n\tilde{\to}\mu_n$ et donc un isomorphisme de groupes $\mathrm{Aut}_{Grp}(\mu_n)\tilde{\to}\mathrm{Aut}_{Grp}(\mathbb{Z}/n) = \mathbb{Z}/n^\times$. Modulo ces isomorphismes, on a

$$\sigma(\zeta_n) = \zeta_n^{\chi_k(\sigma)},\ \sigma \in \mathrm{Gal}(k_n/k).$$

L'image de $\mathrm{Gal}(k_n/k)$ dans $(\mathbb{Z}/n)^\times$ dépend de l'arithmétique du corps. Voici un exemple.

Proposition. $\chi_{\mathbb{Q}} : \mathrm{Gal}(\mathbb{Q}_n/Q) \to \mathbb{Z}/n^\times$ *est un isomorphisme de groupes.*

Démonstration. On sait déjà que $\chi_{\mathbb{Q}} : \mathrm{Gal}(\mathbb{Q}_n/Q) \to (\mathbb{Z}/n)^\times$ est injectif. Il suffit donc de montrer que $[\mathbb{Q}_n : \mathbb{Q}](= |\mathrm{Gal}(\mathbb{Q}_n/Q)|) = |\mathbb{Z}/n^\times| =: \varphi(n)$. Mais $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)/\mathbb{Q}$. Il suffit donc de montrer que le polynôme minimal $P_{\zeta_n} \in \mathbb{Q}[T]$ de ζ_n sur $\mathbb{Q}$ est irréductible. Pour cela, notons $\mathfrak{u}_n \subset \mu_n$ le sous-ensemble des générateurs de μ_n (les racines primitives n-ièmes de 1). Par construction $\mathfrak{u}_n$ est $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$-stable donc le polynôme $\Phi_n = \prod_{u\in\mathfrak{u}_n}(T-u)$ est dans $\mathbb{Q}[T]$ (par la caractérisation (4) de **??**) et il a ζ_n pour racine. Donc $P_{\zeta_n}|\Phi_n$. Comme $\deg(\Phi_n) = |\mathfrak{u}_n| = |\mathbb{Z}/n^\times|$, la conclusion résulte du Lemme ci-dessous. □

Lemme. $\Phi_n \in \mathbb{Q}[T]$ *est irréductible sur* $\mathbb{Q}[T]$.

Démonstration. On procède en plusieurs étapes.

1. $\Phi_n \in \mathbb{Z}[T]$. En effet $T^n - 1 = \prod_{d|n} \Phi_d$ dans $\mathbb{Q}[T]$. Comme $\mathbb{Z}$ est factoriel, on a en particulier $1 = C_{\mathbb{Z}}(T^n - 1) = \prod_{d|n} C_{\mathbb{Z}}(\Phi_d)$. Mais comme Φ_d est unitaire , on a $C_{\mathbb{Z}}(\Phi_d) = \frac{1}{a_d}$ pour un certain $a_d \in \mathbb{Z}_{\geq 1}$, $d|n$. Cela impose $C_{\mathbb{Z}}(\Phi_d) = 1$ *i.e.* $\Phi_d \in \mathbb{Z}[T]$, $d|n$.
2. Soit $\zeta \in \mathfrak{u}_n$ et notons P le polynôme minimal de ζ sur $\mathbb{Q}$. On veut montrer que $P = \Phi_n$. Comme les éléments de $\mathfrak{u}_n$ sont tous de la forme ζ^m pour un certain $m \in \mathbb{Z}_{\geq 1}$, $gcd(m, n) = 1$, il suffit de prouver que si p est un nombre premier $\nmid n$, ζ^p est aussi une racine de P. Sinon, notons Q le polynôme minimal de ζ^p sur $\mathbb{Q}$. Comme $P \neq Q$ et $P, Q|\Phi_n$ dans $\mathbb{Q}[T]$, $PQ|\Phi_n$ dans $\mathbb{Q}[T]$. On peut donc écrire $\Phi_n = PQR$ dans $\mathbb{Q}[T]$. Comme $\Phi_n \in \mathbb{Z}[T]$ et P, Q, R sont unitaires, le même argument de contenu qu'en (1) montre que $P, Q, R \in \mathbb{Z}[T]$.

3. Puisque $Q(\zeta^p)=0$, $P|Q(T^p)$ dans $\mathbb{Q}[T]$ donc - toujours par l'argument de contenu - dans $\mathbb{Z}[T]$. Notons $F\to\overline{F}$ le morphisme de réduction modulo p, $\mathbb{Z}[T]\to\mathbb{Z}/p[T]$. On a donc $\overline{P}|\overline{Q}(T^p)=\overline{Q}(T)^p$ dans $\mathbb{F}_p[T]$. Mais puisque $\mathbb{F}_p[T]$ est factoriel, tout diviseur irréductible de $\overline{P}$ est en particulier un diviseur irréductible de $\overline{Q}$. Fixons $\Pi\in\mathbb{F}_p[T]$ un diviseur irréductible de $\overline{P}$ donc de $\overline{Q}$. On a donc
$$\Pi^2|\overline{PQ}|\overline{\Phi}_n|T^n-\overline{1}$$
dans $\mathbb{F}_p[T]$. On peut donc écrire $T^n-\overline{1}=\Pi^2\Xi$ dans $\mathbb{F}_p[T]$. En particulier, $nT^{n-1}=2\Pi\Pi'\Xi+\Pi^2\Xi'$ donc $\Pi|T^n$ dans $\mathbb{F}_p[T]$ donc $\Pi|(T^n-\overline{1})-T^n=\overline{1}$ dans $\mathbb{F}_p[T]$: contradiction.

□

16.2.3

Extensions radicielles. Soit k un corps de caractéristique $p\geq 0$ et $n\in\mathbb{Z}_{\geq 1}$ tel que $|\mu_n:=\mu_n(k)|=n$ *i.e.* si $p>0$, $p\nmid n$ et k contient toutes les racines n-ièmes de 1. Fixons $a\in k$ et notons $k_{n,a}/k$ un corps de décomposition de T^n-a ; puisque $T^n-a\in k[T]$ est séparable, $k_{n,a}/k$ est galoisienne. Si $\alpha\in Z_k(T^n-a)$ on a $Z_{\overline{k}}(T^n-a)=Z_k(T^n-a)=\{\zeta\alpha\mid\alpha\in\mu_n\}$. Donc $k_{n,a}=k(\alpha)$ et on dispose d'un morphisme de groupes injectif
$$\begin{array}{ccc} Gal(k_{n,a}/k) & \hookrightarrow & \mu_n \\ \sigma & \to & \frac{\sigma(\alpha)}{\alpha}\end{array}$$
d'image l'unique sous-groupe d'ordre $n_a:=[k_{n,a}:k]|n$ *i.e.* μ_{n_a}. En particulier
$$\prod_{\zeta\in\mu_{n_a}}(T-\zeta\alpha)=\alpha^{n_a}((\alpha^{-1}T)-\zeta)=T^{n_a}-\alpha^{n_a}\in k[T]$$
donc $\alpha^{n_a}\in k$. Cela montre que n_a est aussi le plus petit $m\in\mathbb{Z}_{\geq 1}$ tel que $\alpha^m\in k$ ou, encore (puisque $|Z_k(T^n-1)|=n$), tel que $a^m\in k^{\times n}$. Autrement dit, $[k_{n,a}:k]=n_a$ est l'ordre de l'image de a dans $k^\times/k^{\times n}$. On a donc montré la première partie de la proposition suivante.

16.2.3.0.1 Proposition. *$k_{n,a}/k$ est Galoisienne de degré l'ordre n_a de a dans $k^\times/k^{\times n}$ et on a un isomorphisme de groupes*
$$\begin{array}{ccc} Gal(k_{n,a}/k) & \tilde{\to} & \mu_{n_a} \\ \sigma & \to & \frac{\sigma(\alpha)}{\alpha}\end{array}$$
Réciproquement, toute extension K/k galoisienne cyclique de degré n est le corps de décomposition d'un polynôme irréductible de la forme $T^n-a\in k[T]$.

Démonstration. Il reste a démontrer la réciproque. Soit donc K/k une extension galoisienne de groupe de Galois $Gal(K/k)\simeq\mathbb{Z}/n$ et $\sigma\in Gal(K/k)$ un générateur. On cherche à construire $\alpha\in K$ tel que $\sigma(\alpha)=\zeta\alpha$ pour $\zeta\in\mathfrak{u}_n$. Tout élément non nul de la forme
$$\alpha=\sum_{0\leq i\leq n-1}\zeta^{-i}\sigma^i(x)$$
conviendrait. Il faut donc s'assurer que le k-endomorphisme $\sum_{0\leq i\leq n-1}\zeta^{-i}\sigma^i:K\to K$ est non nul. Cela résulte du classique Lemme **??**. □

16.2.3.0.2 Lemme. *Soit K, L deux corps. Tout sous-ensemble fini de* $\mathrm{Hom}(K, L)$ *est L-libre.*

Démonstration. Soit $\phi_1, \dots, \phi_n : K \to L$ n morphismes de corps deux à deux distincts. On raisonne par induction sur n. Si $n = 1$, l'assertion est claire. Si $n \geq 2$ et si $\phi_1, \dots, \phi_n : K \to L$ ne sont pas L-libre, il existe $x_1, \dots, x_n \in L$, tous non nuls par hypothèses de récurrence, tels que

$$x_1\phi_1 + \cdots + x_n\phi_n = 0.$$

On a alors pour tout $x, y \in K$

$$(x_1\phi_1 + \cdots + x_n\phi_n)(xy) = x_1\phi_1(x)\phi_1(y) + \cdots + x_n\phi_n(x)\phi_n(y) = 0.$$

En particulier, pour tout $x \in K$ on a

$$(*) \quad x_1\phi_1(x)\phi_1 + \cdots + x_n\phi_n(x)\phi_n = 0.$$

Mais on a aussi,

$$(**) \quad \phi_1(x)(x_1\phi_1 + \cdots + x_n\phi_n) = x_1\phi_1(x)\phi_1 + \cdots + x_n\phi_1(x)\phi_n = 0.$$

Comme $\phi_1 \neq \phi_2$, il existe $x \in K$ tel que $\phi_1(x) \neq \phi_2(x)$, ce qui en faisant $(**) - (*)$, implique

$$x_2(\phi_1(x) - \phi_2(x))\phi_2 + \cdots + x_n(\phi_1(x) - \phi_n(x))\phi_n = 0$$

avec $x_2(\phi_1(x) - \phi_2(x)) \neq 0$, ce qui contredit l'hypothèse de récurrence. □

16.2.3.0.3 Corollaire. *Soit K/k une extension finie engendrée par des éléments $\alpha_1, \dots, \alpha_r \in \overline{K}$ tels que $\alpha_i^n \in k$. Alors K/k est galoisienne de groupe $Gal(K/k)$ abélien.*

Démonstration. L'extension K/k est galoisienne puisque c'est le corps de décomposition du polynôme séparable $(T^n - \alpha_1^n) \cdots (T^n - \alpha_r^n) \in k[T]$ sur k. De plus, puisque $K = k(\alpha_1, \dots, \alpha_r)$ le morphisme de groupes

$$Gal(K/k) \to \prod_{1 \leq i \leq r} Gal(k(\alpha_i/k)), \quad \sigma \to (\sigma|_{k(\alpha_i)})_{1 \leq i \leq r}$$

est injectif ; la conclusion résulte donc de la première partie de **??**. □

16.3

Lemme. *Soit K un corps et $G \subset \mathrm{Aut}(K)$ un sous-groupe fini. Alors K/K^G est galoisienne et $Gal(K/K^G) = G$.*

Démonstration. Pour tout $x \in K$ le polynôme $\Pi_x := \prod_{y \in G \cdot x}(T - y)$ est par construction séparable, dans $K^G[T]$ et $P_x(x) = 0$. En particulier x est algébrique sur K^G et son polynôme minimal $P_x \in K^G[T]$ sur K^G divise Π_x donc est de degré $\leq |G \cdot x| \leq |G|$. Cela montre que K/K^G est algébrique séparable. Elle est de plus de degré fini $\leq |G|$ sinon il existerait une sous-extension séparable finie $K^G \subset L \subset K$ de degré $[L : K^G] > |G|$. Mais par **??**, $L = K^G(x)$: contradiction. Par ailleurs, puisque $G \subset \mathrm{Aut}(K/K^G)$, on a $|G| \leq |\mathrm{Aut}(K/K^G)| \leq [K : K^G] \leq |G|$ donc $|G| = |\mathrm{Aut}(K/K^G)| = [K : K^G]$, K/K^G est galoisienne et $Gal(K/K^G) = \mathrm{Aut}(K/K^G) = G$. □

16.4

Corollaire. *Pour tout groupe fini G il existe une extension galoisienne K/k de groupe $Gal(K/k) = G$.*

Démonstration. D'après **??**, il suffit de montrer qu'il existe un corps K tel que G est un sous-groupe de $\mathrm{Aut}(K)$. Or on peut toujours plonger G dans un groupe de permutations $\mathcal{S}_n$ (*e.g* en faisant agir G sur lui-même par translation et en prenant $n = |G|$). Or pour n'importe quel corps k, $\mathcal{S}_n$ l'action de $\mathcal{S}_n$ par permutation des coordonnées induit un k-plongement canonique $\mathcal{S}_n \hookrightarrow \mathrm{Aut}(k(X_1, \ldots, X_n)/k)$. □

Remarque. Un problème beaucoup plus difficile est de savoir si, étant donné un corps k, tout groupe fini G est le groupe de Galois d'une extension galoisienne K/k ou, de façon équivalente, est un quotient de $\mathrm{Aut}(\overline{k}/k)$; c'est ce qu'on appelle le problème de Galois inverse pour k. Il y a des corps k pour lesquels on sait que la réponse est non (les corps algébriquement clos, les corps finis, $\mathbb{R}$, les extensions finies de $\mathbb{Q}_p$ etc.) car le groupe $\mathrm{Aut}(\overline{k}/k)$ est trop simple. En fait, la complexité du groupe $\mathrm{Aut}(\overline{k}/k)$ est une bonne mesure de la complexité arithmétique de k (plus $\mathrm{Aut}(\overline{k}/k)$ a de quotients finis, plus il y a de possibilités pour les groupes de Galois des polynômes à coefficients dans k et donc plus c'est difficile de résoudre une équation à coeffiicients dans k). Par exemple, on ne sait pas résoudre le problème de GAlois inverse pour $\mathbb{Q}$ ou les extensions de type fini de $\mathbb{Q}$ - par exemple $\mathbb{Q}(T)$ (en fait, si on savait le résoudre pour $\mathbb{Q}(T)$ on saurait le résoudre pour $\mathbb{Q}$; c'est une conséquence du théorème d'irréductibilité de Hilbert). On sait par contre le résoudre - par des méthodes géométriques - pour des corps comme $\mathbb{C}(T)$, $\overline{\mathbb{Q}}(T)$, $\mathbb{Q}_p(T)$.

16.5

Proposition *Soit K/k une extension galoisienne et $k \subset L \subset K$ une sous-extension.*

1. *K/L est galoisienne et $L = K^{Gal(K/L)}$;*
2. *Pour tout $\sigma \in Gal(K/k)$, $\sigma Gal(K/L)\sigma^{-1} = Gal(K/\sigma(L))$*
3. *L/k est galoisienne (de façon équivalente normale) si et seulement si $Gal(K/L)$ est normal dans $Gal(K/k)$, auquel cas, le morphisme de restriction $Gal(K/k) \to Gal(L/k)$, $\sigma \to \sigma|_K$ est bien défini et induit une suite exacte courte de groupes*

$$1 \to Gal(K/L) \to Gal(K/k) \to Gal(L/k) \to 1.$$

Démonstration. (1) K/L est galoisienne puisque normale et séparable (**??** - Contre-Exemple, **??**) et l'égalité $L = K^{Gal(K/L)}$ résulte alors de la caractérisation (5) de **??**. (2) Pour tout $\sigma \in Gal(K/k)$, $\tau \in Gal(K/L)$ et $x \in L$ on a $\sigma\tau\sigma^{-1}(\sigma(x)) = \sigma\tau(x) = \sigma(x)$ donc $\sigma Gal(K/L)\sigma^{-1} \subset Gal(K/\sigma(L))$. Par symétrie, $\sigma^{-1}Gal(K/\sigma(L))\sigma \subset Gal(K/L)$. (3) La deuxième partie de l'assertion et la condition nécessaire de la première partie résulte de **??**. Pour la condition suffisante, si $Gal(K/L)$ est normal dans $Gal(K/k)$, d'après (2), pour tout $\sigma \in Gal(K/k)$ on a $Gal(K/L) = Gal(K/\sigma(L)) =: H$. Mais par (1) on a alors $L = K^H = \sigma(L)$. Comme par ailleurs K/k est galoisienne, si $K \subset \overline{k}$ est une clôture algébrique, tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$ se restreint en $\sigma|_K \in Gal(K/k)$ donc, en fait, on a bien que pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, $\sigma(L) = L$ *i.e.* L/k est normale. Enfin L/k est séparable par **??**. □

16.6

Soit K/k une extension galoisienne. Notons $\mathcal{S}(K/k)$ l'ensemble des sous-extensions de K/k et $\mathcal{S}(Gal(K/k))$ l'ensemble des sous-groupes de $Gal(K/k)$.

16.6.1

Corollaire (Correspondance de Galois) *Les applications*

$$\begin{array}{ccc} \mathcal{S}(Gal(K/k)) & \to & \mathcal{S}(K/k) \\ H & \to & K^H := \{x \in K \mid \sigma(x) = x,\ \sigma \in H\} \end{array} \quad , \quad \begin{array}{ccc} \mathcal{S}(K/k) & \to & \mathcal{S}(Gal(K/k)) \\ L & \to & Gal(K/L) \end{array}$$

induisent des bijections inverses l'une de l'autre, décroissantes pour $\subset$ et telles que les sous-extensions galoisiennes (de façon équivalente normales) de K/k correspondent aux sous-groupes normaux de $Gal(K/k)$.

Démonstration. Résulte de **??** et **??**. □

16.7

Exemples.

16.7.1 Extensions de Kummer de $\mathbb{Q}$

Soit $n \in \mathbb{Z}_{\geq 1}$, $\zeta \in \overline{\mathbb{Q}}$ une racine primitive n-ième de l'unité et $a \in \mathbb{Q}$ dont l'image dans $\mathbb{Q}^\times/(\mathbb{Q}^\times)^n$ est d'ordre n. On a vu que

- (**??**) le polynôme $T^n - a \in \mathbb{Q}(\zeta)[T]$ est irréductible sur $\mathbb{Q}(\zeta)$ et que l'extension $\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\zeta)$ est galoisienne de groupe $Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\zeta)) \tilde{\to} \mu_n$, $\sigma \to \sigma(\sqrt[n]{a})/\sqrt[n]{a}$;
- (**??**) le polynôme $\Phi_n \in \mathbb{Q}[T]$ est irréductible sur $\mathbb{Q}$ et que l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de groupe $\chi_{\mathbb{Q}} : Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \tilde{\to} (\mathbb{Z}/n)^\times$.

L'extension $\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}$ est galoisienne puisque c'est un corps de décomposition du polynôme séparable $T^n - a \in \mathbb{Q}[T]$ sur $\mathbb{Q}$ et on a, d'après **??** une suite exacte courte de groupes

$$1 \to Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\zeta)) \to Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}) \to Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \to 1.$$

Cette suite exacte se scinde. En effet, considérons le sous-groupe $Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\sqrt[n]{a})) \subset Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q})$. En effet, on a clairement

$$Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\sqrt[n]{a})) \cap Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\zeta)) = 1$$

donc un morphisme de groupe injectif $Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\sqrt[n]{a})) \hookrightarrow Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. Mais puisque $\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\sqrt[n]{a})$ est galoisienne, on a aussi

$$|Gal(\mathbb{Q}(\zeta, \sqrt[n]{a})/\mathbb{Q}(\sqrt[n]{a}))| = [\mathbb{Q}(\zeta, \sqrt[n]{a}) : \mathbb{Q}(\zeta)] = \frac{[\mathbb{Q}(\zeta, \sqrt[n]{a} : \mathbb{Q}]}{[\mathbb{Q}(\sqrt[n]{a}) : \mathbb{Q}]} = \frac{n\phi(n)}{n} = \phi(n) = |Gal(\mathbb{Q}(\zeta)/\mathbb{Q})|$$

d'où, en fait, un isomorphisme de groupes $Gal(\mathbb{Q}(\zeta,\sqrt[n]{a})/\mathbb{Q}(\sqrt[n]{a}))\tilde{\to}Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. On peut même calculer facilement l'action par conjugaison de $Gal(\mathbb{Q}(\zeta,\sqrt[n]{a})/\mathbb{Q}(\sqrt[n]{a}))$ sur $Gal(\mathbb{Q}(\zeta,\sqrt[n]{a})/\mathbb{Q}(\zeta))$: soit $\sigma \in Gal(\mathbb{Q}(\zeta,\sqrt[n]{a})/\mathbb{Q}(\sqrt[n]{a}))$, $\tau \in Gal(\mathbb{Q}(\zeta,\sqrt[n]{a})/\mathbb{Q}(\zeta))$ alors

$$\frac{\sigma\tau\sigma^{-1}(\sqrt[n]{a})}{\sqrt[n]{a}} = \sigma(\frac{\tau(\sigma^{-1}(\sqrt[n]{a}))}{\sigma^{-1}(\sqrt[n]{a})}) = \sigma(\frac{\tau(\sqrt[n]{a})}{\sqrt[n]{a}}) = (\frac{\tau(\sqrt[n]{a})}{\sqrt[n]{a}})^{\chi_{\mathbb{Q}}(\sigma)} = \frac{\tau^{\chi_{\mathbb{Q}}(\sigma)}(\sqrt[n]{a})}{\sqrt[n]{a}}$$

i.e. $\sigma\tau\sigma^{-1} = \tau^{\chi_{\mathbb{Q}}(\sigma)}$. On a donc un isomorphisme de groupes

$$Gal(\mathbb{Q}(\zeta,\sqrt[n]{a})/\mathbb{Q})\tilde{\to}\mathbb{Z}/n \rtimes (\mathbb{Z}/n)^\times, \;\; \sigma \to (\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}, \sigma|_{\mu_n})$$

avec, à gauche, la structure de produit direct 'tautologique' (donnée par l'action naturelle de $\mathbb{Z}/n^\times$ sur μ_n par $u \cdot \zeta = \zeta^u$).

16.8

Clôture normale. Soit K/k une extension algébrique, $\overline{k}$ une clôture algébrique (contenant K) et K_i/k, $i \in I$ des sous-extensions normales de $\overline{k}/k$ contenant K. Alors $\cap_{i\in I}K_i/k$ est encore une extension normale contenant K puisque pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, $\sigma(K_i) = K_i$ et $\sigma(\cap_{i\in I}K_i) = \cap_{i\in I}\sigma(K_i)$. Il existe donc une plus petit sous-extension normale $\widehat{K}/k$ de $\overline{k}/k$ contenant K appelé *clôture normale* de K/k dans $\overline{k}/k$.

Lemme. *Soit $\widetilde{K}/K$ une extension algébrique. Les propriétés suivantes sont équivalentes.*

1. *$\widetilde{K}$ est K-isomorphe à $\widehat{K}$;*
2. *$\widetilde{K}/k$ est normale et engendrée, comme k-extension de corps par les $\sigma(K)$, $\sigma \in \mathrm{Hom}_k(K,\widetilde{K})$.*

On dit qu'une extension$\widetilde{K}/k$ vérifiant les propriétés équivalentes du lemme ci-dessus est une clôture normale de K/k. La propriété (1) montre qu'elle est unique à isomorphisme (non unique) près.

Démonstration. Si $\overline{k}'/k$ est une autre clôture algébrique contenant K et $\sigma : \overline{k}\tilde{\to}\overline{k}'$ un k-isomorphisme, $\sigma(\widehat{K})/k$ est la clôture normale de $\sigma(K)/k$ dans $\overline{k}'/k$. On peut donc supposer que $\widehat{K}, \widetilde{K} \subset \overline{k}$. Comme $\widetilde{K}/k$ est normale, $\widehat{K} \subset \widetilde{K}$. En outre, $\widetilde{K}/k$ est aussi la sous-k-extension de $\overline{k}/k$ engendrée comme k-extension par les $\sigma(K)$, $\sigma \in \mathrm{Hom}_k(K,\overline{k})$. Or tout $\sigma \in \mathrm{Hom}_k(K,\overline{k})$ s'étend en un k-plongement $\widehat{\sigma} \in \mathrm{Hom}_k(\widehat{K},\overline{k})$ qui, comme $\widehat{K}/k$ est normale, vérifie $\widehat{\sigma}(\widehat{K}) = \widehat{K}$ Donc $\widetilde{K} \subset \widehat{K}$. □

Exemple. Si K/k est une extension séparable fini, par **??** il existe $x \in K$ tel que $K = k(x)/k$. Si $P_x \in k[T]$ est le polynôme minimal de x sur k, les clôtures normales de K/k sont les corps de décomposition de P_x sur k. En particulier, la clôture normale $\widehat{K}/k$ de K/k est alors galoisienne finie (de degré divisant $[K : k]!$) et on dit plutôt que $\widehat{K}/k$ est la *clôture galoisienne* de K/k. Par exemple, $\mathbb{Q}(\sqrt[3]{5}, j)/\mathbb{Q}$ est la clôture galoisienne de $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$.

16.9

Résolubilité par radicaux. Étant donné un polynôme séparable $P \in k[T]$, notons K_P/k un corps de décomposition de P sur k et $G_P := Gal(K_P/k)$. Si P est de degré n et $Z_K(P) = \{x_1, \dots, x_n\}$, la restriction induit un morphisme de groupes injectifs

$$Gal(K_P/k) \hookrightarrow \mathcal{S}(\{x_1, \dots, x_n\}) \simeq \mathcal{S}_n.$$

16.9.1

Lemme. *$P \in k[T]$ est irréductible sur k si et seulement si l'action de G_P sur $Z_K(P)$ est transitive.*

Démonstration. Si $x \in Z_K(P)$, $P \in k[T]$ est irréductible sur k si et seulement si c'est le polynôme minimal de P_x de x sur k *i.e.* (caractérisation (5) de **??**) si et seulement si $P = \prod_{y \in Gal(K_P/k)}(T - y)$. □

A l'opposé, si P se factorise en produit de polynômes irréductibles $P = P_1 \cdots P_r$ dans $k[T]$, les sous-extensions K_{P_i}/k de K_P/k étant galoisiennes, on a des suites exactes courtes

$$1 \to Gal(K/K_i) \to G_P \overset{-|_{K_{P_i}}}{\to} G_{P_i}) \to 1,\ i = 1, \dots, r$$

et un morphisme $G_P \hookrightarrow \prod_{1 \le i \le r} G_{P_i}$ induit par le produit des $-|_{K_{P_i}} : G_P \twoheadrightarrow G_{P_i}$ est injectif puisque $K_P = k(Z_K(P_1) \cup \cdots \cup Z_K(P_r))$.

Exemple. Soit ζ une racine primitive 5ème de 1. L'extension $\mathbb{Q}(\sqrt[3]{5}, j, \zeta)/\mathbb{Q}$ est galoisienne puisque c'est le corps de décomposition du polynôme séparable $P = (T^3 - 5)\Phi_5$. En posant $P_1 := T^3 - 5$, $P_2 = \Phi_5$, on a donc un morphisme de groupes injectif $G_P \hookrightarrow G_{P_1} \times G_{P_2} = \mathcal{S}_3 \times (\mathbb{Z}/5)^\times$. De plus $T^3 - 5$ est irréductible sur $\mathbb{Q}(\zeta)$...

16.9.2

On dit qu'un polynôme $P \in k[T]$ est *résoluble par radicaux sur k* si ses racines peuvent s'exprimer à partir des éléments de k en appliquant successivement les opérations $+, -, /, \sqrt[n]{-}$. Autrement dit, cela signifie qu'on a une suite de sous-extensions

$$K_P = K_{n+1} \supset K_n \supset \cdots \supset K_1 \supset K_0 = k$$

telles que $K_{i+1} = K_i(x_i)$ et $x_i^{n_i} \in K_i$, $i = 0, \dots, n$.

On dit qu'un groupe G est *résoluble* s'il existe une suite de sous-groupes

$$G =: G_0 \supset G_1 \supset \cdots \supset G_n \supset G_{n+1} = 1$$

tels que G_{i+1} est normal dans G_i et G_i/G_{i+1} est abélien, $i = 0, \dots, n$. (Il n'est pas difficile de vérifier que cette définition est équivalente à celle donnée précédemment à savoir que $D^n G = 1$,

$n \gg 0$).

Exercice. Montrer que tout sous-groupe et tout quotient d'un groupe résoluble est résoluble et que toute extension de groupes résolubles est résoluble.

16.9.3

Théorème. *Un polynôme séparable $P \in k[T]$ est résoluble par radicaux sur k si et seulement si G_P est résoluble.*

Démonstration. Notons $p \geq 0$ la caractéristique de k. Supposons d'abord $P \in k[T]$ résoluble par radicaux sur k et soit

$$K_P = n+1 \supset K_n \supset \cdots \supset K_1 \supset K_0 = k$$

une suite de sous-extensions telles que $K_{i+1} = K_i(x_i)$ et $x_i^{n_i} \in K_i$, $i = 0, \ldots, n$. On peut supposer que $p \nmid n_i$ et que $T^{n_i} - x_i^{n_i} \in K_i[T]$ est irréductible sur K_i, $i = 0, \ldots, n$. Comme K_P/K_i est galoisienne et contient x_i, K_P contient les racines $n_i$ième de 1. Donc, en posant $n = pgcm(n_0, \ldots, n_n)$, K_P contient les racines $n$ième de 1. On peut donc supposer que $K_1 = k(\zeta)$ pour $\zeta \in K_P$ une racine primitive $n$ième de 1. Chacune des extensions K_{i+1}/K_i est alors galoisienne de groupe $Gal(K_{i+1}/K_i)$ abélien. Mais K_i/k n'a aucune raison d'être galoisienne pour $n \geq 2$. Remplaçons donc les K_i/k par leur clôture galoisienne. Comme K_{n+1}/k est galoisienne et par minimalité de la clôture galoisienne on a des inclusions

$$\begin{array}{ccccccccc}
K_{n+1} & \supset & K_n & \supset & \cdots & \supset & K_2 & \supset \\
\| & & \downarrow & & & & \downarrow & \\
K_{n+1} & \supset & \widehat{K}_n & \supset & \cdots & \supset & \widehat{K}_2 & \supset
\end{array}$$

Il reste à voir que $Gal(\widehat{K}_{i+1}/\widehat{K}_i)$ est abélien, $i = 0, \ldots, n$. Mais $\widehat{K}_{i+1}$ est engendrée comme k-extension par les $x_{i+1}, \sigma := \sigma(x_{i+1})$, $\sigma \in Gal(K_{n+1}/k)$. Or $\sigma(x_{i+1})^{n_i} = \sigma(x_{i+1}^{n_i}) \in \sigma(K_i) \subset \widehat{K}_i$; la conclusion résulte donc de **??**. Inversement, supposons G_P résoluble. Notons $n := [K_P : k]$ et $\widetilde{K}_P/K_P$ un corps de décomposition de $T^n - 1 \in k[T] \subset K_P[T]$ sur K_P. L'extension $\widetilde{K}_P/k$ est encore galoisienne car c'est le corps de décomposition du polynôme séparable $P(T^n - 1)/\operatorname{pgcd}(P, T^n - 1) \in k[T]$ sur k. En particulier, on a une suite exacte courte de groupes finis

$$1 \to Gal(\widetilde{K}_P/K_P) \to Gal(\widetilde{K}_P/k) \to G_P = Gal(K_P/k) \to 1,$$

ce qui montre que $Gal(\widetilde{K}_P/k)$ est extension d'un groupe résoluble par un groupe abélien donc est résoluble. □

16.10

Spécialisation. Si le degré de P est ≥ 5, on ne dispose pas de formule universelle pour calculer les racines de P et déterminer G_P est en général une question difficile. Le critère de spécialisation que nous allons voir permet souvent de réduire la question au problème de la factorisation des polynômes sur les corps finis, problème qu'on sait résoudre algorithmiquement.

* * *

anna.cadoret@imj-prg.fr
IMJ-PRG, Sorbonne Université
Paris, FRANCE