Université Paris VII – Denis Diderot
UFR de Mathématiques

Février–Juin 2001

NOTES SUR LE COURS D'ALGÈBRE DE MAÎTRISE

Michel Broué

Université Paris VII – Denis Diderot **Février–Juin 2001**
UFR de Mathématiques

Notes sur le cours d'algèbre de maîtrise

Première partie : Anneaux et Polynômes

1. Définitions et conventions

Sauf mention du contraire, les anneaux A considérés

- possèdent un élément unité pour la multiplication, noté en général 1 ou 1_A,
- sont (sauf mention du contraire) commutatifs.

La multiplication est souvent notée $(a,b) \mapsto a \cdot b$ ou même $(a,b) \mapsto ab$.

Un morphisme d'anneaux (non nécessairement commutatifs) $\varphi\colon A \longrightarrow B$ est une application f de A vers B telle que

$$\begin{cases} f \text{ est un morphisme de groupes additifs de } A \text{ vers } B\,, \\ f(aa') = f(a)f(a') \text{ pour tous } a, a' \in A\,, \\ f(1_A) = 1_B\,. \end{cases}$$

Un sous–anneau d'un anneau A (non nécessairement commutatif) est un sous–ensemble B de A, qui est un sous–groupe pour la loi additive, qui est stable par multiplication ($bb' \in B$ pour tous $b, b' \in B$), et qui contient 1_A.

Un idéal à gauche (resp. à droite) $\mathfrak{a}$ d'un anneau (non nécessairement commutatif) A est un sous–groupe additif de A tel que pour tous $a \in A$ et $x \in \mathfrak{a}$, on a $ax \in \mathfrak{a}$ (resp. $xa \in \mathfrak{a}$). Un idéal bilatère est un sous–groupe qui est à la fois un idéal à gauche et un idéal à droite. Si A est commutatif, les notions d'idéal à gauche, à droite, bilatère coïncident, et on dit simplement "idéal".

1.A. Anneaux et morphismes fondamentaux.

1. Étant donné un anneau A, il existe un et un seul morphisme d'anneaux

$$\varphi_A\colon \mathbb{Z} \longrightarrow A\,.$$

En effet, il est facile de voir que tout morphisme $\varphi\colon \mathbb{Z} \longrightarrow A$ vérifie

$$\varphi(n) = \begin{cases} \underbrace{1_A + 1_A + \cdots + 1_A}_{n \text{ fois}} & \text{si } n \geq 0 \\ -(\underbrace{1_A + 1_A + \cdots + 1_A}_{-n \text{ fois}}) & \text{si } n < 0 \end{cases}$$

et que la formule précédente définit bien un morphisme d'anneaux.

2. Étant donnés un anneau A et un élément $x \in A$, il existe un et un seul morphisme d'anneaux

$$\varphi_{A,x}\colon \mathbb{Z}[X] \longrightarrow A \text{ tel que } \varphi_{A,x}(X) = x\,.$$

En effet, il est facile de voir que tout morphisme $\varphi\colon \mathbb{Z}[X] \longrightarrow A$ tel que $\varphi(X) = x$ vérifie

$$\varphi(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_01_A\,.$$

et que la formule précédente définit bien un morphisme d'anneaux.

Sous–anneaux engendrés.

Si A est un anneau, l'intersection d'une famille de sous–anneaux de A est un sous–anneau de A. Il en résulte que, pour tout sous–ensemble E de A, l'intersection de tous les sous–anneaux contenant E est le plus petit sous–anneau contenant E. On l'appelle l'anneau engendré par E.

- En considérant le cas où E est l'ensemble vide, on obtient le plus petit sous–anneau de A, appelé sous–anneau premier de A. Il est égal à l'image de $\mathbb{Z}$ dans A (par le morphisme φ_A).
- En considérant le cas où E est un singleton $\{a\}$, on obtient l'image du morphisme $\varphi_{A,a}$, constitué de l'ensemble des polynômes en a à coefficients dans le sous–anneau premier de A.

Exercice : Nombres décimaux. En prenant $A = \mathbb{Z}$ et $E = \{1/10\}$, ou encore $E = \{1/2, 1/5\}$, on obtient l'anneau des entiers décimaux.

1.B. Algèbres sur un corps.

Soit K un corps. Une K–algèbre commutative est un anneau (commutatif) A qui contient K comme sous–anneau.

Plus généralement, si A est un anneau non nécéssairement commutatif,

- le centre de A est le sous–anneau de A consistant en l'ensemble des éléments $z \in A$ tels que $az = za$ pour tout $a \in A$,
- on dit que A est une K–algèbre si K est un sous–anneau du centre de A.

Exemples.

1. Le corps K est une K–algèbre.
2. L'anneau $K[X]$ des polynômes en une indéterminée X est une K–algèbre (commutative).
3. L'anneau $\mathrm{Mat}_n(K)$ des matrices carrées $n \times n$ à coefficients dans K est une K–algèbre (non commutative si $n > 1$) : son élément unité est la matrice identité $n \times n$, et K est identifié à l'ensemble des matrices d'homothéties.

Morphismes fondamentaux.

Un morphisme de K–algèbres $f\colon A \longrightarrow B$ est un morphisme d'anneaux tel que $f(\lambda) = \lambda$ pour tout $\lambda \in K$.

Les résultats ci–dessous sont les analogues pour les K–algèbres de l'existence des morphismes fondamentaux introduits ci–dessus pour le cas des anneaux (qui doivent en fait être vus comme des $\mathbb{Z}$–algèbres – voir ci–dessous).

1. Soit A une K–algèbre. Il existe un unique morphisme de K–algèbres $\varphi\colon K \longrightarrow A$.

En effet, on a

$$\varphi(\lambda) = \lambda 1_A\,.$$

2. Étant donnés une K–algèbre A et un élément $x \in A$, il existe un et un seul morphisme d'algèbres

$$\varphi_{A,x}\colon K[X] \longrightarrow A \text{ tel que } \varphi_{A,x}(X) = x\,.$$

En effet, il est facile de voir que tout morphisme $\varphi\colon K[X] \longrightarrow A$ tel que $\varphi(X) = x$ vérifie

$$\varphi(a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 1_A\,.$$

et que la formule précédente définit bien un morphisme d'algèbres.

Sous–algèbres engendrées.

Une sous–algèbre d'une K–algèbre A est un sous–anneau de A qui contient K.

L'intersection d'une famille de sous–algèbres est une sous–algèbre. Il en résulte que, pour tout sous–ensemble E de A, l'intersection de toutes les sous–algèbres contenant E est la plus petite sous–algèbre contenant E. On l'appelle l'algèbre engendrée par E.

- En considérant le cas où E est l'ensemble vide, on obtient K.
- En considérant le cas où E est un singleton $\{x\}$, on obtient l'ensemble des polynômes en x à coefficients dans K, que l'on note $K[x]$.

Exemples.

1. Soit V un espace vectoriel sur K. L'anneau $\mathrm{End}(V)$ des endomorphismes de V est une K–algèbre : son élément unité est l'identité Id_V de V, et K est identifié à l'ensemble des homothéties $\lambda\mathrm{Id}_V$ pour $\lambda \in K$.

Si $f \in \mathrm{End}(V)$, la sous–algèbre $K[f]$ engendrée par f est l'ensemble des polynômes en f à coefficients dans K, *i.e.*, l'ensemble des éléments de la forme

$$a_m f^m + a_{m-1} f^{m-1} + \ldots a_1 f + a_0 \mathrm{Id}_V \,.$$

C'est l'image de $K[X]$ par le morphisme $K[X] \longrightarrow \mathrm{End}(V)$ qui envoie $\lambda \in K$ sur $\lambda\mathrm{Id}_V$ et X sur f.

2. La sous–$\mathbb{Q}$–algèbre $\mathbb{Q}[\sqrt{2}]$ de $\mathbb{R}$ engendrée par $\sqrt{2}$, ensemble des polynômes en $\sqrt{2}$ à coefficients rationnels, est aussi plus simplement égale à l'ensemble des nombres réels de la forme

$$\{\lambda + \mu\sqrt{2} \mid (\lambda, \mu \in \mathbb{Q})\}\,,$$

puisque pour tout entier $m \geq 0$ on a $\sqrt{2}^{2m+1} = 2^m\sqrt{2}$ et $\sqrt{2}^{2m} = 2^m$.

Cet anneau est en fait un corps, puisque si $\lambda + \mu\sqrt{2} \neq 0$ (*i.e.*, si λ et μ ne sont pas tous deux nuls), $\lambda + \mu\sqrt{2}$ est inversible. En effet, son inverse est

$$\frac{\lambda}{\lambda^2 - 2\mu^2} - \frac{\mu}{\lambda^2 - 2\mu^2}\sqrt{2}\,,$$

donc de la forme $\lambda' + \mu'\sqrt{2}$ avec $\lambda', \mu' \in \mathbb{Q}$.

3. Nous verrons plus loin que, par contre, la sous–algèbre $\mathbb{Q}[\pi]$ de $\mathbb{R}$ engendrée par π est isomorphe à l'algèbre des polynômes $\mathbb{Q}[X]$, donc en particulier n'est pas un corps.

Généralisation : algèbres sur un anneau.

Soit R un anneau (commutatif). Une R–algèbre (ou "algèbre sur R") est un couple (A, μ) où

- A est un anneau (non nécessairement commutatif),
- $\mu\colon R \longrightarrow ZA$ est un morphisme d'anneaux de R vers le centre ZA de A.

On omettra souvent le morphisme μ en mentionnant "la R–algèbre A".

Si (A, μ) et (B, ν) sont deux R–algèbres, un morphisme de R-algèbres de A vers B est un morphisme d'anneaux $f\colon A \longrightarrow B$ tel que $f \cdot \mu = \nu$.

Exemples.

- Tout anneau est (d'une manière unique) une algèbre sur $\mathbb{Z}$.
- L'anneau $\mathrm{Mat}_n(R)$ des matrices carrées $n \times n$ à coefficients dans R, muni du morphisme naturel de R vers l'ensemble des matrices d'homothéties, est une R–algèbre.
- Si A est un anneau commutatif, L'anneau $A[X]$ des polynômes à coefficients dans A est une A–algèbre.
- Si (A, μ) est une R–algèbre, le morphisme μ définit un morphisme de R–algèbres de R dans A.

Étant donnés une A–algèbre B, un morphisme $\alpha\colon A \longrightarrow B$, un élément $x \in B$, il existe un et un seul morphisme de R–algèbres

$$\widetilde{\alpha}\colon A[X] \longrightarrow B$$

qui prolonge α et envoie X sur x.

Le résultat suivant, que nous utiliserons souvent, est une conséquence de ce qui précède (pourquoi ?).

1.1. Proposition. *Soit $\alpha\colon A \longrightarrow B$ un morphisme d'anneaux (commutatifs). Alors il existe un et un seul morphisme*

$$\widetilde{\alpha}\colon A[X] \longrightarrow B[Y]$$

entre les anneaux de polynômes respectifs qui prolonge α et envoie l'indéterminée X sur l'indéterminée Y.

1.C. Idéaux et quotients.

Idéaux engendrés.

L'intersection d'une famille d'idéaux de A est un idéal de A. Il en résulte que, pour tout sous–ensemble E de A, l'intersection de tous les idéaux contenant E est le plus petit idéal contenant E. On l'appelle l'idéal engendré par E.

- En considérant le cas où E est l'ensemble vide, on obtient l'idéal trivial $\{0\}$.
- En considérant le cas où E est un singleton $\{x\}$, on obtient l'idéal de tous les éléments de la forme ax où $a \in A$. On l'appelle l'idéal principal engendré par x et on le note Ax, ou parfois (x).

Exemples. Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de A.

- On note $\mathfrak{a}+\mathfrak{b}$ l'idéal engendré par $\mathfrak{a} \cup \mathfrak{b}$. L'idéal $\mathfrak{a}+\mathfrak{b}$ est l'ensemble des éléments de la forme $x+y$ où $x \in \mathfrak{a}$ et $y \in \mathfrak{b}$.
- On note $\mathfrak{a}\mathfrak{b}$ l'idéal engendré par l'ensemble des produits xy où $x \in \mathfrak{a}$ et $y \in \mathfrak{b}$.

  ⓘ **Attention** ⓘ

  L'idéal $\mathfrak{a}\mathfrak{b}$ est l'ensemble des sommes finies d'éléments de la forme xy où $x \in \mathfrak{a}$ et $y \in \mathfrak{b}$.

Idéaux et morphismes.

Soit $f\colon A \longrightarrow B$ un morphisme d'anneaux. Le noyau $\ker(f)$ de f, ensemble des éléments $x \in A$ tels que $f(x) = 0$, est un idéal de A

Réciproquement, soit $\mathfrak{a}$ un idéal de l'anneau A. Il existe un couple (B, f), où

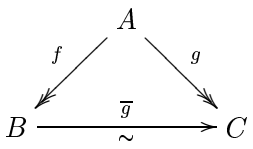
- B est un anneau et $f\colon A \longrightarrow B$ est un morphisme,
- f est surjectif et de noyau $\mathfrak{a}$.

En effet, on peut par exemple prendre $B = A/\mathfrak{a}$ et choisir pour f le morphisme surjectif canonique $\pi_{\mathfrak{a}}$ de A sur $A/\mathfrak{a}$.

Ainsi, les idéaux sont les noyaux des morphismes d'anneaux.

De plus, si $\mathfrak{a}$ est un idéal de A, un couple (B, f) comme ci–dessus est unique à unique isomorphisme près :

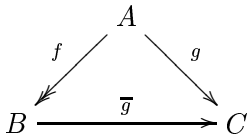
1.2. Proposition. *Soit (C, g) un couple où C est un anneau et $g\colon A \longrightarrow C$ est un morphisme surjectif de noyau $\mathfrak{a}$. Alors il existe un unique isomorphisme $\overline{g}$ de B sur C tel que le diagramme suivant est commutatif.*



Ainsi, le couple $(A/\mathfrak{a}, \pi_\mathfrak{a})$ est caractérisé (à unique isomorphisme près) par le fait que $A/\mathfrak{a}$ est un anneau et $\pi_\mathfrak{a}\colon A \twoheadrightarrow A/\mathfrak{a}$ est un morphisme surjectif de noyau $\mathfrak{a}$.

Plus généralement :

1.3. Proposition. *Soit (B, f) un couple où B est un anneau et $f\colon A \longrightarrow B$ est un morphisme surjectif de noyau $\mathfrak{a}$, et soit (C, g) un couple où C est un anneau et $g\colon A \longrightarrow C$ est un morphisme dont le noyau contient $\mathfrak{a}$. Alors il existe un unique morphisme $\overline{g}\colon B \longrightarrow C$ tel que le diagramme suivant est commutatif.*



De plus,

- *le noyau de $\overline{g}$ est $f(\ker(g))$, idéal de B isomorphe à $\ker(g)/\mathfrak{a}$, et $\overline{g}$ est injective si et seulement si $\ker(g) = \mathfrak{a}$,*
- *$\overline{g}$ est surjective si et seulement g est surjective.*

Exemple–Exercice.

Nous construisons un isomorphisme

$$\mathbb{Z}/6\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[i\sqrt{5}]/(1 + i\sqrt{5})\,.$$

1. Le sous–anneau $\mathbb{Z}[i\sqrt{5}]$ de $\mathbb{C}$ engendré par $i\sqrt{5}$ est égal à l'ensemble des nombres complexes de la forme $\lambda + \mu i\sqrt{5}$ où $\lambda, \mu \in \mathbb{Z}$.

Soit $\varphi\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[i\sqrt{5}]$ l'inclusion naturelle. On note $\overline{\varphi}\colon \mathbb{Z} \longrightarrow \mathbb{Z}[i\sqrt{5}]/(1 + i\sqrt{5})$ le composé de φ avec la surjection $\pi\colon \mathbb{Z}[i\sqrt{5}] \twoheadrightarrow \mathbb{Z}[i\sqrt{5}]/(1 + i\sqrt{5})$.

2. Le morphisme $\overline{\varphi}$ est surjectif. En effet, comme $\pi(1+i\sqrt{5}) = 0$, on a $\pi(i\sqrt{5}) = \pi(-1)$, donc $\pi(\lambda + \mu i\sqrt{5}) = \pi(\lambda - \mu) = \overline{\varphi}(\lambda - \mu)$, ce qui montre que tout élément de $\mathbb{Z}[i\sqrt{5}]/(x)$ appartient à l'image de $\overline{\varphi}$.

3. Le noyau de $\overline{\varphi}$ est $6\mathbb{Z}$. En effet, il est égal à l'ensemble des entiers n tels que $n \in (1+i\sqrt{5})$, *i.e.*, tels qu'il existe $\lambda, \mu \in \mathbb{Z}$ avec $n = (1 + i\sqrt{5})(\lambda + i\mu\sqrt{5})$, *i.e.*, $n = (\lambda - 5\mu) + i(\lambda + \mu)\sqrt{5}$, ou encore $\lambda = -\mu$ et $n = \lambda - 5\mu$, ce qui équivaut à $n \in 6\mathbb{Z}$.

Il résulte alors de la proposition que $\overline{\varphi}$ définit un isomorphisme de $\mathbb{Z}/6\mathbb{Z}$ sur $\mathbb{Z}[i\sqrt{5}]/(1+i\sqrt{5})$.

1.D. Le lemme chinois.

1.4. Proposition. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux d'un anneau A. On suppose que $\mathfrak{a} + \mathfrak{b} = A$. Alors l'application "diagonale"*

$$A \longrightarrow (A/\mathfrak{a}) \times (A/\mathfrak{b})\ ,\ a \mapsto (\pi_\mathfrak{a}(a), \pi_\mathfrak{b}(a))$$

définit par passage au quotient un isomorphisme

$$A/(\mathfrak{a} \cap \mathfrak{b}) \xrightarrow{\sim} (A/\mathfrak{a}) \times (A/\mathfrak{b})\,.$$

Démonstration. Il est clair que le noyau de l'application diagonale est $\mathfrak{a} \cap \mathfrak{b}$. Il suffit donc d'établir que cette application est surjective.

Soit $(\pi_\mathfrak{a}(x), \pi_\mathfrak{b}(y))$ un élément arbitraire de $(A/\mathfrak{a}) \times (A/\mathfrak{b})$. Par hypothèse, il existe $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$. Considérons l'élément $z := ay + bx$. Il est alors immédiat de vérifier que l'image de z par l'application diagonale est $(\pi_\mathfrak{a}(x), \pi_\mathfrak{b}(y))$. □

1.E. Les anneaux $\mathbb{Z}$ et $K[X]$ sont principaux.

Nous rappelons la propriété suivante :

1.5. Théorème. *Désignons par A un anneau égal, soit à $\mathbb{Z}$, soit à $K[X]$ où K est un corps. Alors tout idéal de A est principal.*

Applications.

- Si A est un anneau quelconque, son sous–anneau premier (image de $\mathbb{Z}$ par l'unique morphisme de $\mathbb{Z}$ dans A) est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain entier naturel n. Cet entier, appelé la caractéristique de A, est le plus petit (pour l'ordre naturel et pour la divisibilité) des entiers positifs m tels que $\underbrace{1_A + 1_A + \cdots + 1_A}_{m \text{ fois}} = 0$.
- Si A est une K–algèbre quelconque et x est un élément de A, la sous–algèbre $K[x]$ engendrée par x (image de $K[X]$ par l'unique morphisme d'algèbre de $K[X]$ dans A qui envoie X sur x) est isomorphe à $K[X]/(\mu(X))$ pour un certain élément $\mu(X) \in K[X]$, que l'on suppose unitaire s'il est non nul. Cet élément, appelé le polynôme minimal de x, est le plus petit (pour la divisibilité) des polynômes $P(X)$ tels que $P(x) = 0$.

Ⓘ **Attention** Ⓘ

Le sous–anneau engendré par x n'est pas nécessairement de la forme $\mathbb{Z}[X]/(\mu(X))$, car il y a des idéaux de $\mathbb{Z}[X]$ qui ne sont pas principaux.

Ainsi, l'idéal engendré dans $\mathbb{Z}[X]$ par $\{2, X\}$ (qui consiste en tous les polynômes à coefficients entiers dont le terme constant est pair) n'est pas principal, puisque les seuls polynômes qui divisent à la fois 2 et X sont les constantes 1 et -1.

1.F. Diviseurs de zéro, anneaux intègres.

Un élément a d'un anneau A est dit *diviseur de zéro* s'il est non nul et s'il existe un élément non nul $a' \in A$ tel que $aa' = 0$.

Un anneau est dit *intègre* s'il est non nul et s'il ne possède pas de diviseur de zéro.

Exemples d'anneaux non intègres.

- $A \times B$ si A et B sont des anneaux non nuls (en effet, on constate que $(a, 0_B)(0_A, b) = (O_A, O_B) = O_{A\times B}$).
- $\mathbb{Z}/n\mathbb{Z}$ si n est un entier non nul, non inversible et non premier, et $K[X]/(P(X))$ si $P(X)$ est un polynôme non nul, non inversible et non premier.
- $\mathbb{Z}[i\sqrt{5}]/(1 + i\sqrt{5})$.
- $A[X]$ si A est non intègre.
- L'anneau (non commutatif) des matrices 2×2 à coefficients dans un anneau commutatif non nul quelconque.

Exemples d'anneaux intègres.

- $\mathbb{Z}/p\mathbb{Z}$ si p est un nombre premier, et $K[X]/(P(X))$ si $P(X)$ est un polynôme irréductible.
- $A[X]$ si A est intègre.
- Tout sous–anneau d'un anneau intègre.
- Un corps – et donc tout sous–anneau d'un corps.

Remarque. Nous verrons plus loin (en construisant le corps des fractions d'un anneau intègre) que réciproquement, tout anneau intègre est isomorphe à un sous–anneau d'un corps.

Démontrons que $A[X]$ est intègre si A est intègre.

Cela résulte du lemme suivant, dont la démonstration est laissée au lecteur. On admet connue la notion de degré d'un polynôme à coefficients dans un anneau quelconque ... à ceci près qu'on convient ici que le degré du polynôme nul est $-\infty$.

1.6. Lemme. *Soient $P(X) = a_dX^d + \cdots + a_1X + a_0$ et $Q(X) = b_eX^e + \cdots + b_1X + b_0$ deux éléments non nuls de $A[X]$, de degré respectifs d et e. Alors $P(X)Q(X)$ est de degré au plus $d + e$, et il est exactement de degré $d + e$ si a_d ou b_e n'est pas diviseur de 0.*

En particulier si a_d ou b_e est inversible, ou si A est intègre, $P(X)Q(X)$ est exactement de degré $d+e$.

1.G. Caractéristique, polynôme minimal.

Caractéristique d'un anneau intègre.

Soit A un anneau (non nécessairement commutatif) intègre. Son sous–anneau premier est alors intègre. Or on sait que le sous–anneau premier est isomorphe, soit à $\mathbb{Z}$, soit à un $\mathbb{Z}/n\mathbb{Z}$ pour un certain entier non nul n. Dans ce dernier cas, l'entier n est nécessairement premier. Ainsi

1.7. Proposition. *Soit A un anneau (non nécessairement commutatif) intègre.*

- *Ou bien il n'existe pas d'entier m non nul tel que $\underbrace{1+1+\cdots+1}_{m \text{ fois}} = 0$ et le sous–anneau premier de A est isomorphe à $\mathbb{Z}$.*
- *Ou bien il existe un nombre premier p tel que $\underbrace{1+1+\cdots+1}_{m \text{ fois}} = 0$ si et seulement si p divise m, et alors le sous–anneau premier de A est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Dans le premier cas, on dit que A est de caractéristique nulle. Dans le deuxième cas, on dit que A est de caractéristique p.

Polynôme minimal d'un nombre algébrique.

Soit A une K–algèbre (non nécessairement commutative) intègre, et soit $x \in A$. La sous–algèbre $K[x]$ engendrée par x est alors intègre. Or on sait que cette sous–algèbre est isomorphe, soit à $K[X]$, soit à un $K[X]/(\mu(X))$ pour un certain polynôme non nul $\mu(X)$. Dans ce dernier cas, le polynôme $\mu(X)$ est nécessairement irréductible. Ainsi

1.8. Proposition. *Soit A une K–algèbre (non nécessairement commutative) intègre, et soit $x \in A$.*

- *Ou bien il n'existe pas de polynôme $P(X) \in K[X]$ non nul tel que $P(x) = 0$ et le sous–anneau $K[x]$ de A est isomorphe à $K[X]$.*
- *Ou bien il existe un polynôme irréductible $\mu(X) \in K[X]$ tel que $P(x) = 0$ si et seulement si $\mu(X)$ divise $P(X)$, et alors le sous–anneau $K[x]$ de A est isomorphe à $K[X]/(\mu(X))$. Noter que $\mu(X)$ est uniquement déterminé si on lui impose d'être unitaire.*

Dans le premier cas, on dit que x est transcendant sur K. Dans le deuxième cas, on dit que x est algébrique sur K et de polynôme minimal $\mu(X)$.

2. Idéaux premiers et idéaux maximaux

Définition.

• *Un idéal $\mathfrak{p}$ de A est dit premier si l'anneau $A/\mathfrak{p}$ est intègre. On note* $\mathrm{Spec}(A)$ *l'ensemble des idéaux premiers, appelé le spectre de A.*

• *Un idéal $\mathfrak{m}$ de A est dit maximal si l'anneau $A/\mathfrak{m}$ est un corps. On note* $\mathrm{Spec}_{\max}(A)$ *l'ensemble des idéaux maximaux, appelé le spectre maximal de A.*

Exemples.

- Comme un corps est un anneau intègre, tout idéal maximal est premier.
- $\{0\}$ est premier non maximal dans $\mathbb{Z}$,
- $2\mathbb{Z}[X]$ est premier non maximal dans $\mathbb{Z}[X]$.

Vérifions en effet que $\mathbb{Z}[X]/2\mathbb{Z}[X] \simeq \mathbb{F}_2[X]$: Le morphisme $\mathbb{Z} \twoheadrightarrow \mathbb{F}_2$ induit un (unique) morphisme $\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_2[X]$ envoyant l'indéterminée sur l'indéterminée. Son noyau est manifestement $2\mathbb{Z}[X]$.

- $(1+i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$ est non premier dans $\mathbb{Z}[i\sqrt{5}]$ (on a déjà vérifié que $\mathbb{Z}[i\sqrt{5}]/(1+i\sqrt{5}) \simeq \mathbb{Z}/6\mathbb{Z}$).

Caractérisation.

• *Un idéal propre* $\mathfrak{p}$ *de* A *est premier si et seulement si, pour tous* $a, b \in A$ *avec* $a \notin \mathfrak{p}$ *et* $b \notin \mathfrak{p}$*, on a* $ab \notin \mathfrak{p}$*.*

• *Un idéal propre* $\mathfrak{m}$ *de* A *est maximal si et seulement si, pour tout idéal propre* $\mathfrak{a}$ *de* A *tel que* $\mathfrak{m} \subseteq \mathfrak{a}$*, on a* $\mathfrak{m} = \mathfrak{a}$*.*

On admettra le résultat suivant, dont la démonstration repose sur le lemme de Zorn.

2.1. Proposition. *Soit* $\mathfrak{a}$ *un idéal propre de* A*. Il existe un idéal maximal* $\mathfrak{m}$ *qui contient* $\mathfrak{a}$*.*

2.A. Éléments inversibles.

L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour la multiplication, appelé le groupe des éléments inversibles (ou "unités") de A.

Exemples.

• $(A \times B)^\times \simeq A^\times \times B^\times$,

• $A^\times = A \backslash \{0\}$ si et seulement si A est un corps,

• $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des classes modulo n des entiers premiers à n (ce groupe a pour cardinal $\varphi(n)$ où φ désigne la fonction d'Euler),

• $A[X]^\times = A^\times$ si A est intègre.

Remarque. Cette dernière égalité est fausse en général. Par exemple, si A possède un élément r tel que $r^n = 0$ pour un certain entier $n \geq 2$, le polynôme $1 - rX$ est inversible, puisque

$$(1 - rX)(1 + rX + r^2X^2 + \cdots + r^{n-1}X^{n-1}) = 1\,.$$

Concrètement, on peut par exemple considérer

$$A := \left\{ \begin{pmatrix} \lambda & \mu \\ 0 & \lambda \end{pmatrix} \mid (\lambda, \mu \in \mathbb{R}) \right\} = \mathbb{R}[r]$$

où $r := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

2.B. Idéaux premiers et anneaux de polynômes.

Soit $\mathfrak{a}$ un idéal de A. On note $\mathfrak{a}A[X]$ l'idéal de $A[X]$ engendré par $\mathfrak{a}$. Attention à la notation ! On a

$$\mathfrak{a}A[X] = \{a_0 + a_1X + \cdots + a_dX^d \mid (a_j \in \mathfrak{a})\}\,.$$

Le morphisme surjectif canonique $\pi_\mathfrak{a} \colon A \twoheadrightarrow A/\mathfrak{a}$ induit un unique morphisme

$$A[X] \twoheadrightarrow (A/\mathfrak{a})[X]$$

qui envoie l'indéterminée de $A[X]$ sur celle de $(A/\mathfrak{a})[X]$. On voit que le noyau de ce morphisme est l'idéal $\mathfrak{a}A[X]$, ce qui prouve que

$$A[X]/\mathfrak{a}A[X] \simeq (A/\mathfrak{a})[X]\,.$$

En particulier, on voit que

Si $\mathfrak{p}$ *est un idéal premier de* A*, l'idéal* $\mathfrak{p}A[X]$ *est premier dans* $A[X]$*.*

Inversément, soit $\mathfrak{A}$ un idéal de $A[X]$. Par le morphisme surjectif canonique $\pi_\mathfrak{A} \colon A[X] \twoheadrightarrow A[X]/\mathfrak{A}$, puisque le noyau de la restriction de $\pi_\mathfrak{A}$ à A est $\mathfrak{A} \cap A$, l'anneau A est envoyé sur un anneau isomorphe à $A/\mathfrak{A} \cap A$. On voit en particulier que

Si $\mathfrak{P}$ est un idéal premier de $A[X]$, l'idéal $\mathfrak{P} \cap A$ est premier dans A.

2.C. Idéaux maximaux dans $\mathbb{Z}[X]$.

Soit p un nombre premier, de sorte que $\mathbb{Z}/p\mathbb{Z}$ est le corps fini $\mathbb{F}_p$ à p éléments. Si $P(X) \in \mathbb{Z}[X]$, notons $\overline{P}(X)$ l'image de $P(X)$ dans $\mathbb{F}_p[X]$. Nous allons démontrer que si $\overline{P}(X)$ est irréductible dans $\mathbb{F}_p[X]$, l'idéal de $\mathbb{Z}[X]$ engendré par p et $P(X)$ est maximal.

L'idéal de $\mathbb{Z}[X]$ engendré par p et $P(X)$ est $p\mathbb{Z}[X] + P(X)\mathbb{Z}[X]$.

2.2. Lemme. *Soit $\mathfrak{a}$ un idéal de A et soit $\pi_\mathfrak{a}\colon A \twoheadrightarrow A/\mathfrak{a}$ le morphisme surjectif canonique. Soit $\mathfrak{b}$ un autre idéal de A.*

(1) On a $\pi_\mathfrak{a}(\mathfrak{b}) = (\mathfrak{a}+\mathfrak{b})/\mathfrak{a}$.

(2) Le morphisme surjectif canonique $A \twoheadrightarrow A/(\mathfrak{a}+\mathfrak{b})$ se factorise par $\pi_\mathfrak{a}\colon A \twoheadrightarrow A/\mathfrak{a}$ et induit un isomorphisme

$$(A/\mathfrak{a})/\pi_\mathfrak{a}(\mathfrak{b}) \xrightarrow{\sim} A/(\mathfrak{a}+\mathfrak{b})\,.$$

Soit $\pi_p\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ le morphisme canonique. D'après le lemme précédent, on a

$$\mathbb{Z}[X]/p\mathbb{Z}[X] + P(X)\mathbb{Z}[X] \simeq \mathbb{F}_p[X]/\overline{P}(X)\,,$$

ce qui montre bien que $p\mathbb{Z}[X] + P(X)\mathbb{Z}[X]$ est maximal.

2.D. Radical et Nilradical.

Le radical de A est défini par

$$\mathrm{Rad}A := \bigcap_{\mathfrak{m}\in \mathrm{Spec}_{\max}(A)} \mathfrak{m}\,.$$

Le nilradical de A est défini par

$$\mathrm{NilRad}A := \bigcap_{\mathfrak{p}\in \mathrm{Spec}(A)} \mathfrak{p}\,.$$

On voit que $\mathrm{NilRad}A \subseteq \mathrm{Rad}(A)$.

2.3. Proposition.

(1) On a

$$\mathrm{Rad}A = \{r \in A \mid (\forall x \in A)(1+rx \in A^\times)\}\,.$$

(2) On a

$$\mathrm{NilRad}A = \{r \in A \mid (1+rX \in A[X]^\times)\}\,.$$

Remarque. On voit bien ainsi que $\mathrm{NilRad}A \subset \mathrm{Rad}A$, puisque si $1+rX \in A[X]^\times$, il existe $P(X) \in A[X]$ tel que $(1+rX)P(X) = 1$, d'où $(1+rx)P(x) = 1$ et $1+rx \in A^\times$.

Démonstration.

(1) Démontrons tout d'abord un lemme.

2.4. Lemme. *On a $A\backslash A^\times = \bigcup_{\mathfrak{m}\in \mathrm{Spec}_{\max}(A)} \mathfrak{m}$.*

En effet,

• si $a \in A^\times$, a ne peut appartenir à aucun idéal propre donc $a \notin \bigcup_{\mathfrak{m}\in \mathrm{Spec}_{\max}(A)} \mathfrak{m}$,

• si $a \notin A^\times$, alors Aa est un idéal propre de A, donc est contenu dans un élément de $\mathrm{Spec}_{\max}(A)$ et $a \in \bigcup_{\mathfrak{m}\in \mathrm{Spec}_{\max}(A)} \mathfrak{m}$.

Nous pouvons maintenant démontrer (1).

• Si $r \in \mathrm{Rad}A$, pour tout $x \in A$ et pour tout $\mathfrak{m} \in \mathrm{Spec}_{\max}(A)$ on a $rx \in \mathfrak{m}$, donc $1+rx \notin \mathfrak{m}$, donc d'après le lemme ci–dessus $1+rx \in A^\times$.

• S'il existe $\mathfrak{m} \in \mathrm{Spec}_{\max}(A)$ tel que $r \notin \mathfrak{m}$, comme $A/\mathfrak{m}$ est un corps il existe $r' \in A$ tel que $rr' \equiv 1 \mod \mathfrak{m}$, *i.e.*, $1 - rr' \in \mathfrak{m}$, ce qui prouve qu'il existe $x \in A$ tel que $1+xr \notin A^\times$.

(2) Nous allons démontrer un résultat plus précis.

2.5. Proposition. *Soit $r \in A$. Les assertions suivantes sont équivalentes :*

(i) *r est nilpotent,*
(ii) $r \in \mathrm{NilRad}A$,
(iii) $(1 + rX) \in A[X]^\times$.

Démonstration.

(i) $\Rightarrow$ (ii) : Si r est nilpotent et si $\mathfrak{p}$ est un idéal premier, on a $r^d = 0$ donc $r^d \in \mathfrak{p}$, d'où $r \in \mathfrak{p}$.

(ii) $\Rightarrow$ (iii) : On a déjà vu que si r est nilpotent le polynôme $1+rX$ est inversible dans $A[X]$.

(iii) $\Rightarrow$ (i) : S'il existe $P(X) = a_0 + a_1X + \cdots + a_mX^m$ tel que $(1 + rX)P(X) = 1$, le calcul donne

$$a_0 = 1\,,\ a_0r + a_1 = 0\,,\ a_1r + a_2 = 0\,,\ \ldots a_{m-1}r + a_m = 0\,,\ ra_m = 0\,,$$

d'où on déduit

$$a_1 = -r\,,\ a_2 = r^2\,,\ \ldots\,,\ a_m = (-1)^m r^m \text{ et } r^{m+1} = 0\,.$$

□

3. Corps des fractions d'un anneau intègre

3.A. Corps des fractions d'un sous–anneau d'un corps.

Soit A un sous–anneau d'un corps K. Alors le sous–corps de K engendré par A est l'ensemble des éléments de K de la forme ab^{-1} (encore notés $\dfrac{a}{b}$) pour $a \in A$ et $b \in A\backslash\{0\}$. Il est clair que $(ab^{-1} = cd^{-1}) \Leftrightarrow (ad = bc)$. Ce sous–corps engendré par A est appelé, pour des raisons évidentes, le *corps des fractions de A*.

Exemples.

• Le corps de fractions de $\mathbb{Z}[\sqrt{2}]$ (dans $\mathbb{R}$) peut se décrire simplement. En effet, l'inverse d'un élément $m + n\sqrt{2}$ est $\dfrac{m - n\sqrt{2}}{m^2 - 2n^2}$, donc toute fraction d'éléments de $\mathbb{Z}[\sqrt{2}]$ est de la forme $\lambda + \mu\sqrt{2}$ où $\lambda\,,\ \mu \in \mathbb{Q}$.

On aurait aussi pu remarquer que le corps engendré par $\mathbb{Z}[\sqrt{2}]$ doit contenir $\mathbb{Q}$ (puisqu'il contient $\mathbb{Z}$), et contient $\sqrt{2}$, donc contient $\mathbb{Q}[\sqrt{2}]$, et comme $\mathbb{Q}[\sqrt{2}]$ est lui–même un corps puisque $\sqrt{2}$ est algébrique (voir cours précédents ou programme de licence), il lui est égal.

• Le corps des fractions de $\mathbb{Z}[\pi]$ dans $\mathbb{R}$ contient $\mathbb{Q}[\pi]$, mais ce dernier anneau n'est pas un corps (puisqu'il est isomorphe à $\mathbb{Q}[X]$). On n'a pas de description "plus simple" que celle décrivant ce corps des fractions comme l'ensemble des nombres de la forme $\dfrac{P(\pi)}{Q(\pi)}$ où $P(X)$ et $Q(X)$ sont des polynômes quelconques (et $Q(X) \neq 0$) de $\mathbb{Z}[X]$.

• Si un corps K est de caractéristique 0, il contient un sous–corps isomorphe à $\mathbb{Q}$: le corps des fractions de l'image de $\mathbb{Z}$ par le morphisme $n \mapsto n1_K$, dont on sait qu'elle est un anneau isomorphe à $\mathbb{Z}$. Noter que ce sous–corps est le plus petit sous–corps de K.

Si un corps K est de caractéristique $p > 0$, l'image de $\mathbb{Z}$ par le morphisme $n \mapsto n1_K$ est déjà un corps, isomorphe à $\mathbb{F}_p$ — c'est le plus petit sous–corps de K.

Propriété universelle.

3.1. Proposition. *Soit A un sous–anneau d'un corps, et soit F le corps de fractions de A. Si $\sigma\colon A \hookrightarrow K$ est un morphisme injectif de A dans un corps K, le morphisme σ s'étend de manière unique en un morphisme (injectif) $F \hookrightarrow K$.*

Démonstration de 3.1. En effet, un prolongement $\widetilde{\sigma}\colon F \longrightarrow K$ vérifie nécessairement la formule

$$\widetilde{\sigma}(ab^{-1}) = \widetilde{\sigma}(a)\widetilde{\sigma}(b)^{-1}\,,$$

et réciproquement la formule précédente définit bien un morphisme de F dans K. □

3.B. Corps de fractions d'un anneau intègre quelconque.

Si A est un sous–anneau d'un corps K, le sous–corps engendré par A est manifestement en bijection avec l'ensemble $\mathrm{Frac}(A)$ contruit de la façon suivante :

On pose $\mathrm{Frac}(A) := (A \times (A - \{0\}))/\sim$, où $\sim$ est la relation d'équivalence définie par

$$(a, b) \sim (c, d) \Leftrightarrow (ad = bc).$$

D'autre part, les lois d'addition et de multiplication dans K définissent sur $\mathrm{Frac}(A)$ les lois

$$\mathrm{cl}(a, b) + \mathrm{cl}(c, d) := \mathrm{cl}(ad + bc, bd)$$
$$\mathrm{cl}(a, b)\mathrm{cl}(c, d) := \mathrm{cl}(ac, bd).$$

Supposons maintenant que A est un anneau intègre quelconque (non *a priori* contenu dans un corps). On contruit alors le *corps des fractions* $\mathrm{Frac}(A)$ "abstraitement" comme ci–dessus, et on obtient un corps dont A s'identifie à un sous–anneau.

Ceci prouve en particulier que *tout anneau intègre est sous–anneau d'un corps.* C'est ainsi qu'on construit $\mathbb{Q}$ à partir de $\mathbb{Z}$, et $K(X)$ à partir de $K[X]$.

Exemple. Si A est un anneau intègre de corps des fractions F, le corps des fractions de $A[X]$ est isomorphe à $F(X)$.

4. Divisibilité et éléments irréductibles

Dorénavant l'anneau A est supposé *intègre*.

Deux éléments a et b d'un anneau A sont dits *associés* s'ils engendrent le même idéal, *i.e.*, s'il existe $u \in A^\times$ tel que $b = ua$.

On dit que b divise a s'il existe $q \in A$ tel que $a = bq$, *i.e.*, si $Aa \subseteq Ab$.

On dit que n éléments $a_1, a_2, \ldots, a_n$ sont premiers entre eux dans leur ensemble (ou, plus simplement, premiers entre eux) si leurs seuls diviseurs communs sont les éléments inversibles de A.

On dit que a est irréductible s'il est non nul, non inversible, et si les seuls diviseurs de a sont les éléments de $A^\times$ et les éléments de la forme ua pour $u \in A^\times$.

Si l'élément a est non nul et engendre un idéal premier, alors a est irréductible.

La réciproque est fausse en général, comme le montre l'exemple suivant.

Exemple. Les éléments 2 et $(1 + i\sqrt{5})$ sont irréductibles dans $\mathbb{Z}[i\sqrt{5}]$.

En effet, pour $m+ni\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$, on pose $N(m+ni\sqrt{5}) = (m+ni\sqrt{5})(m-ni\sqrt{5}) = m^2+5n^2$. On voit que si $N(u) = 1$, on a $u \in A^\times$.

Comme $N(2) = 4$, on voit que si 2 etait réductible il existerait $a \in \mathbb{Z}[i\sqrt{5}]$ tel que $N(a) = 2$, ce qui est impossible. Comme $N(1 + i\sqrt{5}) = 6$, le même raisonnement montre que $(1 + i\sqrt{5})$ est irréductible.

L'égalité $2.3 = (1+i\sqrt{5})(1-i\sqrt{5})$ montre que $(1+i\sqrt{5})(1-i\sqrt{5})$ appartient à l'idéal engendré par 2, alors que ni $(1+i\sqrt{5})$ ni $(1-i\sqrt{5})$ ne lui appartiennent, ce qui montre que l'idéal engendré par 2 n'est pas premier.

Définition. *On dit qu'un anneau (intègre) A est factoriel si*

1. *Tout élément de A est produit d'un nombre fini d'élément irréductibles.*
2. *Si $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ où les p_i et les q_j sont irréductibles, alors $r = s$ et, à une permutation près des indices, pour tout i, p_i et q_i sont associés.*

Remarquons tout de suite une propriété fondamentale des anneaux factoriels connue sous le nom de lemme de Gauß.

4.1. Lemme de Gauß. *Si A est factoriel, et si un élément irréductible p de A divise un produit ab, alors il divise a ou b. En d'autres termes, tout élement irréductible engendre un idéal premier.*

Contre–exemple. L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel, par exemple parce que l'élément 2, qui est irréductible, n'engendre pas un idéal premier. On peut aussi remarquer que l'élément $a = 2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ a deux décompositions différentes en éléments irréductibles.

4.2. Proposition. *Tout anneau (intègre) principal est factoriel.*

Démonstration.

(1) Démontrons d'abord que tout élément est produit d'irréductibles.

Appelons "décomposable" un élément qui est produit d'irréductibles. S'il existe un élément a non décomposable, un tel élément n'est pas irréductible, donc est produit d'un élément non décomposable a_1 par un élément b_1 non inversible. On recommence avec a_1 et on obtient $a_1 = a_2 b_2$ où a_2 est non décomposable et b_2 non inversible. Ainsi de suite, on construit une suite infinie a_n d'éléments non décomposables tels que la suite d'idéaux Aa_n soit strictement croissante.

Or il ne peut exister de suite infinie strictement croissante d'idéaux $\mathfrak{a}_n$ dans un anneau principal. En effet, l'idéal $\mathfrak{a} := \bigcup_n \mathfrak{a}_n$ est principal, donc engendré par un élément a. Il existe N tel que $a \in \mathfrak{a}_N$, donc $\mathfrak{a} = \mathfrak{a}_N$ et $\mathfrak{a}_{N+1} = \mathfrak{a}_N$, contradiction.

(2) Pour démontrer l'unicité de la décomposition, il suffit de démontrer que A satisfait au lemme de Gauß, *i.e.*, que si un élément irréductible p de A divise un produit ab, alors il divise a ou b.

Si p ne divise pas a, l'idéal engendré par a et p est égal à A tout entier (car il est de la forme Ad, où d divise a et divise p, donc ne peut qu'être inversible), et il existe donc α et $\lambda \in A$ tels que $\alpha a + \lambda p = 1$. Si p ne divise pas non plus b, il existe β et $\mu \in A$ tels que $\beta b + \mu p = 1$. On en déduit $1 = \alpha\beta ab + (\beta b\lambda + \alpha a\mu)p$, ce qui prouve que p ne peut diviser ab. □

4.A. Anneaux euclidiens.

Un anneau (intègre) A dit *euclidien* s'il existe une application $N\colon A \to \mathbb{N}$ avec les propriétés suivantes :

- Pour tout $a \in A$, on a $N(a) = 0 \Leftrightarrow a = 0$,
- Pour tout $a, b \in A\backslash\{0\}$, il existe q et r tels que $a = bq + r$ et $N(r) < N(b)$.

Exemples.

- $\mathbb{Z}$ est euclidien, avec $N(n) = |n|$.
- $K[X]$ est euclidien, avec $N(P(X)) = \deg(P(X)) + 1$ si $P(X) \neq 0$, et $N(0) = 0$.

Cela résulte du lemme plus général suivant.

4.3. Lemme. *Soit A un anneau intègre.*

(1) Soient $S(X)$ et $T(X)$ deux éléments de $A[X]$. On suppose $T(X) \neq 0$ et on suppose que le coefficient du terme de plus haut degré de $T(X)$ est inversible dans A :

$$T(X) = b_0 + b_1 X + \cdots + b_e X^e \quad \textit{avec } b_e \in A^\times .$$

Alors il existe deux éléments $Q(X)$ et $R(X)$ dans $A[X]$ uniques tels que

$$\begin{cases} S(X) = T(X)Q(X) + R(X), \\ R(X) = 0 \quad \textit{ou} \quad \deg R(X) < \deg T(X). \end{cases}$$

(2) En particulier, pour tout $a \in A$, il existe $Q(X) \in A[X]$ unique tel que

$$S(X) = (X - a)Q(X) + S(a),$$

et $S(a) = 0$ si et seulement si $X - a$ divise $S(X)$.

Démonstration de 4.3.

L'algorithme de la division de deux polynômes montre l'existence du quotient $Q(X)$ et du reste $R(X)$.

Démontrons l'unicité. Supposons donc $T(X)Q(X)+R(X) = 0$ avec $R(X) = 0$ ou $\deg R(X) < \deg T(X)$. Puisque $R(X) = -T(X)Q(X)$ on voit que nécessairement $R(X) = 0$, d'où $Q(X) = 0$. □

- L'anneau des entiers de Gauß $\mathbb{Z}[i]$ est euclidien, avec $N(m + ni) := m^2 + n^2$.

[Remarquons d'abord (faire un dessin) que pour tout nombre complexe z il existe un élément $q \in \mathbb{Z}[i]$ tel que $N(z - q) \leq 1/2$. Soient alors a et b dans $\mathbb{Z}[i]$ avec $b \neq 0$. Soit q tel que $N(a/b - q) \leq 1/2$, et soit $r := a - bq$. Il est clair que $N(r) \leq N(b)/2 < N(b)$.]

Remarques. Le quotient et le reste sont uniques dans le cas de $K[X]$. Ils ne le sont pas pour $\mathbb{Z}$ ni pour $\mathbb{Z}[i]$. En effet, notons que si $a = bq + r$, on a aussi $a = b(q + 1) + (r - q)$, et il peut se faire (donner des exemples !) que $N(r - q) < q$ sans que $r - q = q$.

4.4. Proposition. *Un anneau euclidien est principal.*

Contre–exemples.

- On a déjà vu que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Soit m un entier (positif ou négatif) non divisible par un carré. On appelle *anneau des entiers* (voir plus loin) du corps $\mathbb{Q}[\sqrt{m}]$ l'anneau $\mathbb{Z}[\omega_m]$ où

$$\omega_m := \begin{cases} \sqrt{m} & \text{si } m \equiv 2 \text{ ou } -1 \mod 4, \\ \dfrac{1+\sqrt{m}}{2} & \text{si } m \equiv 1 \mod 4. \end{cases}$$

Ainsi, l'anneau des entiers de $\mathbb{Q}[i\sqrt{5}]$ est $\mathbb{Z}[i\sqrt{5}]$, celui de $\mathbb{Q}[i\sqrt{3}]$ est $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, celui de $\mathbb{Q}[i\sqrt{19}]$ est $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$.

- L'anneau des entiers de $\mathbb{Q}[\sqrt{-d}]$ $(d > 0)$ est principal si et seulement si

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

- L'anneau des entiers de $\mathbb{Q}[\sqrt{m}]$ est euclidien si et seulement si

$$m \in \{-1, \pm 2, \pm 3, 5, 6, \pm 7, \pm 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Ainsi l'anneau $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ est principal mais non euclidien.

4.B. PGCD et PPCM.

1. *Dans les anneaux factoriels.*

Pour tout couple d'éléments a et b d'un anneau factoriel A, il existe

- un élément noté $a \wedge b$, appelé le pgcd de a et de b, caractérisé (à association près) par la condition suivante : un élément de A divise à la fois a et b si et seulement si il divise $a \wedge b$,
- un élément noté $a \vee b$, appelé le ppcm de a et de b, caractérisé (à association près) par la condition suivante : un élément de A est multiple à la fois de a et de b si et seulement si il est multiple de $a \wedge b$.

En effet, si

$$a = \prod_p p^{v_p(a)} \quad \text{et} \quad b = \prod_p p^{v_p(b)}\,,$$

on a

$$a \wedge b = \prod_p p^{\inf(v_p(a),v_p(b))} \quad \text{et} \quad a \vee b = \prod_p p^{\sup(v_p(a),v_p(b))}\,.$$

Remarquons que deux éléments a et b sont premiers entre eux si $a \wedge b = 1$.

Ⓘ **Attention** Ⓘ

Si les idéaux Aa et Ab sont étrangers (*i.e.*, $Aa + Ab = A$), alors a et b sont premiers entre eux. Par contre, la réciproque est fausse en général si l'anneau A n'est pas principal. C'est ainsi que les éléments 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$, alors que les idéaux qu'il engendrent respectivement ne sont pas étrangers.

Propriétés.

(1) On a $(a \wedge b)(a \vee b) = ab$.

(2) Posons $a = (a \wedge b)a_1$ *et* $b = (a \wedge b)b_1$. *Alors* a_1 *et* b_1 *sont premiers entre eux, et on a* $a \vee b = ab_1 = a_1 b$.

2. *Si de plus l'anneau est principal.*

Le pgcd et le ppcm de deux éléments a et b sont caractérisés (à association près) par les conditions suivantes :

- $A(a \wedge b) = Aa + Ab$,
- $A(a \vee b) = Aa \cap Ab$.

Deux éléments a et b de A sont premiers entre eux si et seulement si ("propriété de Bézout") il existe $\lambda, \mu \in A$ tels que $1 = \lambda a + \mu b$.

3. *Si de plus l'anneau est euclidien.*

Algorithme d'Euclide. Décrivons comment calculer le pgcd de deux éléments a et b en effectuant un nombre fini de divisions euclidiennes successives.

On pose $x_0 := a$, $x_1 := b$. On désigne par x_2 le reste de la division euclidenne de x_0 par x_1. Puis on désigne par x_3 le reste de la division euclidenne de x_1 par x_2, par x_4 le reste de la division euclidenne de x_2 par x_3, et ainsi de suite. Soit N l'entier tel que $x_N \neq 0$ et $x_{N+1} = 0$. Alors x_N est un pgcd de a et de b.

En effet, il est immédiat que l'idéal engendré par (a, b) est égal à l'idéal engendré par (x_1, x_2), qui est égal à l'idéal engendré par (x_2, x_3), etc., donc égal à l'idéal engendré par x_N.

4.C. Étude de $\mathbb{Z}[i]$ et quelques applications.

On appelle anneau des entiers de Gauß l'anneau engendré par i, *i.e.*, l'anneau

$$\mathbb{Z}[i] = \{a + bi \;\mid\; (a, b \in \mathbb{Z})\}\,.$$

Pour $z = a + bi \in \mathbb{Z}[i]$, on pose $N(z) := z\overline{z} = (a + bi)(a - bi) = a^2 + b^2$, et on voit que N est une application de $\mathbb{Z}[i]$ dans $\mathbb{N}$ qui est multiplicative, *i.e.*, $N(zz') = N(z)N(z')$. Il en résulte que si un élément u de $\mathbb{Z}[i]$ est inversible (dans $\mathbb{Z}[i]$), alors $N(u)$ est inversible (dans $\mathbb{Z}$), donc $N(u) = 1$, et par suite $u \in \{1, -1, i, -i\}$. Comme réciproquement les éléments ± 1 et $\pm i$ sont manifestement inversibles, on a établi l'égalité

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}\,.$$

Remarque. Le groupe abélien fini (multiplicatif) $\mathbb{Z}[i]^\times$ est isomorphe au groupe additif $\mathbb{Z}/4\mathbb{Z}$.

Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}[i]$. L'inclusion naturelle $\varphi\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$, composée avec la surjection canonique $\mathbb{Z}[i] \twoheadrightarrow \mathbb{Z}[i]/\mathfrak{p}$, fournit un morphisme d'anneaux $\mathbb{Z} \longrightarrow \mathbb{Z}[i]/\mathfrak{p}$ de noyau $\mathfrak{p} \cap \mathbb{Z}$. Le sous–anneau premier de $\mathbb{Z}[i]/\mathfrak{p}$ est donc isomorphe à $\mathbb{Z}/\mathfrak{p} \cap \mathbb{Z}$.

Si $\mathfrak{p} \neq \{0\}$, on a $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$, car si z est un élément non nul de $\mathfrak{p}$, $N(z)$ est un élément non nul de $\mathfrak{p} \cap \mathbb{Z}$. Il en résulte que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ pour un certain nombre premier p.

4.5. Théorème. *Soit p un nombre premier. Les assertions suivantes sont équivalentes*

(i) *p est un élément réductible de $\mathbb{Z}[i]$.*
(ii) *Il existe deux entiers a et b tels que $p = a^2 + b^2$.*
(iii) *-1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.*
(iv) *$p = 2$ ou $p \equiv 1 \mod 4$.*

Si les assertions ci-dessus sont vraies, alors il existe un élément irréductible de $\pi \in \mathbb{Z}[i]$ tel que $p = \pi\overline{\pi}$ (où on désigne par $\overline{\pi}$ le complexe conjugué de π).

Démonstration.
(i)⇒(ii) : Supposons p réductible dans $\mathbb{Z}[i]$, *i.e.*, supposons qu'il existe deux éléments non inversibles z et z' de $\mathbb{Z}[i]$ tels que $p = zz'$. On a alors $p^2 = N(z)N(z')$ et comme ni $N(z)$ ni $N(z')$ n'est inversible, on en déduit $N(z) = N(z') = p$. Posant $z = a + bi$, on voit donc que $p = a^2 + b^2$.

(ii)⇒(iii) : Si $p = a^2 + b^2$, comme ni a ni b ne sont divisibles par p, a et b sont inversibles modulo p et on a donc dans $\mathbb{Z}/p\mathbb{Z}$ l'égalité $-1 = (ab^{-1})^2$.

(iii)⇔(i) : Les deux isomorphismes

$$\mathbb{Z}[X]/(x^2+1,p) \xrightarrow{\sim} \mathbb{Z}[i]/(p) \quad \text{et} \quad \mathbb{Z}[X]/(x^2+1,p) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$$

montrent que $\mathbb{Z}[i]/(p)$ est intègre si et seulement si $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ est intègre, donc en d'autres termes que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si X^2+1 est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

(iii)⇔(iv) : On peut supposer p impair.

Soit G un groupe cyclique d'ordre $2n$. Un élément $g \in G$ est le carré d'un autre élément de G si et seulement si $g^n = 1$. En appliquant ce résultat au groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$ et à l'élément -1, on voit que -1 est un carré modulo p si et seulement si $(-1)^{p-1/2} = 1$, *i.e.*, si et seulement si $p \equiv 1 \mod 4$.

Si p est réductible, on voit d'après ce qui précède qu'il existe $\pi \in \mathbb{Z}[i]$ tel que $N(\pi) = p$. Ainsi, on a $p = \pi\overline{\pi}$, et π est irréductible puisque sa norme est irréductible dans $\mathbb{Z}$. □

4.D. Critères d'irréductibilité dans $A[X]$.

Dans ce qui suit, on désigne par A un anneau intègre, de corps des fractions F.

Définition. Soit $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un élément non nul de $A[X]$. On dit que $P(X)$ est *primitif* si ses coefficients sont premiers entre eux dans leur ensemble.

On note $\mathrm{Prim}A[X]$ l'ensemble des polynômes primitifs de $A[X]$.

Primitifs et irréductibles.

Notons que les éléments irréductibles de A sont aussi irréductibles dans $A[X]$. En effet, un élément non nul a de A (un élément de degré 0 de $A[X]$) ne peut se décomposer dans $A[X]$ qu'en éléments de degré 0.

4.6. Proposition.
(1) Tout élément irréductible de degré au moins 1 de $A[X]$ est primitif.
(2) Si $P(X) \in \mathrm{Prim}A[X]$ et si $P(X)$ est irréductible dans $F[X]$, alors il est irréductible dans $A[X]$.

Ⓘ Attention Ⓘ

Noter que l'élément $2X$ est irréductible dans $F[X]$, mais qu'il n'est pas irréductible.

Démonstration de 4.6.

(1) Si $P(X)$ n'est pas primitif, il existe un élément non inversible $a \in A$ (donc non inversible dans $A[X]$) et un polynôme $Q(X) \in A[X]$ de degré au moins 1 (donc non inversible dans $A[X]$) tels que $P(X) = aQ(X)$. Ainsi, $P(X)$ n'est pas irréductible.

(2) Si $P(X)$ est primitif, et s'il est égal à un produit de deux éléments non inversibles de $A[X]$, ces deux éléments sont nécessairement tous deux de degrés non nuls – et $P(X)$ est alors réductible dans $F[X]$. □

On retiendra en particulier l'inclusion suivante :

$$\mathrm{Irr}A \bigcup (\mathrm{Prim}A[X] \cap \mathrm{Irr}F[X]) \subseteq \mathrm{Irr}A[X]\,.$$

Nous verrons plus loin que si A est factoriel cette inclusion est une égalité.

Réduction modulo un idéal premier.

4.7. Proposition. *Soit $P(X) \in \mathrm{Prim}A[X]$, et soit $\mathfrak{p}$ un idéal premier de A ne contenant pas le coefficient du terme de plus haut degré de $P(X)$. Alors si l'image de $P(X)$ dans $(A/\mathfrak{p})[X]$ est irréductible, $P(X)$ est irréductible.*

Démonstration de 4.7. Pour $Q(X) \in A[X]$, notons $\overline{Q}(X)$ son image dans $(A/\mathfrak{p})[X]$.

Supposons $P(X)$ réductible dans $A[X]$: on a $P(X) = Q(X)R(X)$, où $Q(X)$ et $R(X)$ sont deux éléments non inversibles de $A[X]$. On en déduit $\overline{P}(X) = \overline{Q}(X)\overline{R}(X)$; comme $\overline{P}(X)$ est irréductible, il en résulte que l'un des deux facteurs, par exemple $\overline{Q}(X)$, est inversible, donc est de degré zéro. On voit alors que $\overline{R}(X)$ a même degré que $\overline{P}(X)$, donc que $P(X)$, et par suite $R(X)$ a même degré que $P(X)$. Donc $Q(X)$ est de degré zéro, ce qui est impossible puisque $P(X)$ est primitif. □

4.E. Étude de $A[X]$ pour A factoriel.

Dans ce qui suit, on désigne par A un anneau factoriel, de corps des fractions F. Nous allons décrire les éléments irréductibles de $A[X]$, et démontrer que $A[X]$ est aussi factoriel.

(!) **Attention** (!)

Rappelons que $A[X]$ n'est en général pas principal (considérer le cas $A = \mathbb{Z}$).

4.8. Proposition ("Lemme de Gauß"). *Soit $P(X) \in A[X]$, de degré au moins 2. Supposons que $P(X)$ est réductible dans $F[X]$ et que $P(X) = Q(X)R(X)$ avec $Q(X), R(X) \in F[X]$, chacun de degré au moins 1. Alors il existe $\lambda, \mu \in F$ tels que*

- $\lambda Q(X), \mu R(X) \in A[X]$,
- $P(X) = (\lambda Q(X))(\mu R(X))$.

Ainsi, $P(X)$ est réductible dans $A[X]$.

Démonstration. En multipliant les deux membres de l'égalité $P(X) = Q(X)R(X)$ par le produit des dénominateurs de coefficients non nuls de $Q(X)$ et de $R(X)$, on obtient une égalité du type

$$(g) \qquad aP(X) = (bQ(X))(cR(X))$$

où $a \in A$ et $aP(X), bQ(X), cR(X) \in A[X]$.

Si a n'est pas inversible, choisissons un nombre premier p qui divise a, et posons $a = pa_1$. Par application du morphisme naturel $A[X] \twoheadrightarrow (A/pA)[X]$, l'agalité précédente devient alors

$$0 = \overline{bQ}(X)\overline{cR}(X)\,.$$

Comme $(A/pA)[X]$ est intègre, on voit que l'un des deux facteurs – par exemple $\overline{bQ}(X)$ – est nul. Ainsi p divise $bQ(X)$, qui s'écrit donc $bQ(X) = pb_1Q(X)$ avec $b_1Q(X) \in A[X]$.

Ainsi, on a pu remplacer l'égalité (g) par l'égalité

$$(g_1) \qquad a_1 P(X) = (b_1 Q(X))(cR(X))$$

où a_1 a un diviseur irréductible de moins que a_1.

En réitérant ce raisonnement, on voit que l'on se ramène au cas où a est inversible, ce qui établit le lemme de Gauß. □

Nous allons maintenant formaliser un peu plus le résultat précédent, que nous allons redémontrer en utilisant la notion de contenu et de polynôme primitif associé.

Contenu et polynôme primitif associé.

4.9. Proposition. *Soit $P(X) \in F[X]$. Il existe un couple $(c(P), \mathrm{pr}(P)(X))$, où $c(P) \in F$ et $\mathrm{pr}(P)(X) \in A[X]$, unique à multiplication près par (u, u^{-1}) où $u \in A^\times$, tel que*

$$P(X) = c(P)\mathrm{pr}(P)(X) \quad \textit{et} \quad \mathrm{pr}(P)(X) \textit{ est primitif.}$$

Le scalaire $c(P)$ (défini à multiplication près par un élément inversible de A) est appelé le *contenu* de $P(X)$. Le polynôme $\mathrm{pr}(P)(X)$ (défini à multiplication près par un élément inversible de A) est appelé le *polynôme entier primitif associé à* $P(X)$.

Démonstration de 4.9.
Existence. Il existe $\lambda \in A - \{0\}$ tel que $\lambda P(X) \in A[X]$. On note d un pgcd des coefficients de $\lambda P(X)$, et on définit $c(P) := d/\lambda$, puis $\mathrm{pr}(P)(X)$ par l'égalité $\lambda P(X) = d\mathrm{pr}(P)(X)$.
Unicité. Supposons $P(X) = \lambda Q(X) = \mu R(X)$, où $\lambda, \mu \in F$ et où $Q(X)$ et $R(X)$ sont des éléments primitifs de $A[X]$. Quitte à remplacer $P(X)$ par un multiple par un élément de A, on peut supposer que λ et μ appartiennent à A, et donc que $P(X) \in A[X]$. On voit alors que λ et μ sont des pgcd des coefficients de $P(X)$, donc sont associés. □

4.10. Proposition.
(1) Soit $P(X) \in F[X]$. On a les équivalences suivantes

$$P(X) \in A[X] \iff c(P) \in A$$
$$P(X) \in \mathrm{Prim}A[X] \iff c(P) \in A^\times .$$

(2) Soient $P(X), Q(X) \in F[X]$. On a

$$c(PQ) = c(P)c(Q) \quad \textit{et} \quad \mathrm{pr}(PQ)(X) = \mathrm{pr}(P)(X)\mathrm{pr}(Q)(X) .$$

4.11. Corollaire.
(1) Le produit de deux polynômes entiers primitifs est primitif.
(2) Si $P(X)$ est un polynôme entier primitif, factorisé en un produit de deux polynômes $P(X) = Q(X)R(X)$ de $F[X]$ de degrés respectifs d et e, alors $P(X) = \mathrm{pr}(Q)(X)\mathrm{pr}(R)(X)$. En particulier $P(X)$ est factorisé en un produit de deux polynômes de $A[X]$ de degrés respectifs d et e.

Démonstration de 4.10.
L'assertion (1) est triviale d'après l'unicité de $(c(P), \mathrm{pr}(P)(X))$.
Démontrons (2). On a $P(X) = c(P)\mathrm{pr}(P)(X)$ et $Q(X) = c(Q)\mathrm{pr}(Q)(X)$ d'où $P(X)Q(X) = c(P)c(Q)\mathrm{pr}(P)(X)\mathrm{pr}(Q)(X)$, et il suffit de démontrer que $\mathrm{pr}(P)(X)\mathrm{pr}(Q)(X)$ est primitif. Or s'il existe un nombre premier qui divise $\mathrm{pr}(P)(X)\mathrm{pr}(Q)(X)$, on voit (par passage dans $(A/pA)[X]$) que p doit diviser l'un des facteurs $\mathrm{pr}(P)(X)$ ou $\mathrm{pr}(Q)(X)$, ce qui est impossible. □

4.12. Théorème.
(1) $\mathrm{Irr}A[X] = \mathrm{Irr}A \bigcup (\mathrm{Prim}A[X] \cap \mathrm{Irr}F[X])$.
(2) $A[X]$ *est factoriel.*

Démonstration de 4.12. Soit $P(X) \in A[X]$. Comme $P(X) = c(P)\mathrm{pr}(P)(X)$ avec $c(P) \in A$ et $\mathrm{pr}(P)(X) \in \mathrm{Prim}A[X]$, en décomposant $c(P)$ en produit d'irréductibles de A et $\mathrm{pr}(P)(X)$ en produit d'éléments de $\mathrm{Prim}A[X] \cap \mathrm{Irr}F[X]$ (grâce au corollaire 4.11, (2)), on voit qu'un élément irréductible de $A[X]$ est nécessairement dans $\mathrm{Irr}A \bigcup (\mathrm{Prim}A[X] \cap \mathrm{Irr}F[X])$.

Comme on sait par ailleurs que tous les éléments de $\mathrm{Irr}A \bigcup (\mathrm{Prim}A[X] \cap \mathrm{Irr}F[X])$ sont irréductibles dans $A[X]$, on a bien établi la première assertion. De plus, on voit aussi que tout élément de $A[X]$ est produit d'éléménts irréductibles.

Reste à démontrer l'unicité de la décomposition en produits d'irréductibles : elle résulte de l'unicité de la décomposition $P(X) = c(P)\mathrm{pr}(P)(X)$, et de l'univité de la décomposition à la fois dans A et dans $F[X]$. □

Exemple–Exercice : les nombres décimaux.

Notons $\mathbb{D} := \mathbb{Z}[1/10]$ l'anneau des nombres décimaux.

4.13. Lemme. *Le morphisme* $\mathbb{Z}[X] \twoheadrightarrow \mathbb{D}$ *qui envoie* X *sur* $1/10$ *induit un isomorphisme*

$$\mathbb{Z}[X]/(10X - 1) \xrightarrow{\sim} \mathbb{D}.$$

Démonstration de 4.13. Il est clair que le noyau du morphisme $\mathbb{Z}[X] \twoheadrightarrow \mathbb{D}$ qui envoie X sur $1/10$ contient l'idéal engendré par $10X - 1$.

Démontrons que réciproquement si $P(X) \in \mathbb{Z}[X]$ est tel que $P(1/10) = 0$, alors $P(X)$ est divisible (dans $\mathbb{Z}[X]$) par $10X - 1$.

On sait, puisque $1/10$ est une racine de $P(X)$ dans $\mathbb{Q}$, que $P(X)$ est divisible (dans $\mathbb{Q}[X]$) par $X - 1/10$. D'après le lemme 4.11, (2), on voit que $P(X)$ est divisible dans $\mathbb{Z}[X]$ par $\mathrm{pr}(X - 1/10)$, qui est égal à $10X - 1$. □

Le critère d'Eisenstein.

4.14. Proposition. *Soit* A *un anneau factoriel de corps de fractions* F*, soit* $P(X) = a_d X^d + a_{d-1}X^{d-1} + \cdots + a_0$ *un élément de degré* d *de* $A[X]$*, et soit* p *un élément irréductible de* A *tel que*

- p *ne divise pas* a_d*,*
- p *divise* a_k *pour tout* $k < d$*,*
- p^2 *ne divise pas* a_0*.*

Alors $P(X)$ *est irréductible dans* $F[X]$*. De plus, si* $P(X)$ *est primitif, il est irréductible dans* $A[X]$.

Démonstration de 4.14. Si $P(X)$ est réductible dans $F[X]$, il est égal à un produit de deux polynômes de degrés respectifs e et f strictement supérieurs à 1, et on sait par le lemme de Gauß (4.8) que $P(X) = Q(X)R(X)$ où $Q(X)$ et $R(X)$ sont deux éléments de $A[X]$ de degrés respectifs e et f strictement supérieurs à 1. Par réduction modulo p, on obtient alors

$$\overline{a}_d X^d = \overline{Q}(X)\overline{R}(X)\,.$$

En regardant l'égalité précédente comme écrite dans l'anneau $L[X]$ où L désigne le corps des fractions de l'anneau intègre $(A/pA)[X]$, on voit (puisque cet anneau est factoriel) que $\overline{Q}(X) = X^e$ et $\overline{R}(X) = X^f$. Il en résulte que les termes constants $Q(0)$ et $R(0)$ sont divisibles par p, donc que $a_0 = P(0) = Q(0)R(0)$ est divisible par p^2, ce qui est contraire à l'hypothèse. □

Application. Pour tout entier d il y a une infinité de polynômes irréductibles de degré d dans $\mathbb{Q}[X]$.

En effet, pour tout entier d et tout nombre premier p, le polyôme $X^d - p$ satisfait aux hypothèses du critère d'Eisenstein.

Ⓘ **Attention** Ⓘ

Par contre, dans $\mathbb{R}[X]$, tout polynôme de degré au moins 3 est réductible. C'est ainsi que le polynôme $X^4 + 1$ est *réductible* dans $\mathbb{R}[X]$ – noter qu'il n'a pourtant pas de racines dans $\mathbb{R}$.

5. Anneaux de polynômes à plusieurs indéterminées

Propriété universelle, substitutions.

La propriété suivante ("propriété universelle de l'anneau des polynômes en n indéterminées sur A", est à la fois immédiate et fondamentale.

5.1. Théorème. *Soient A et B deux anneaux (commutatifs), soit $f\colon A \longrightarrow B$ un morphisme, et soient $x_1, x_2, \ldots, x_n$ n éléments de B. Alors il existe un et un seul morphisme*

$$A[X_1, X_2, \ldots, X_n] \longrightarrow B$$

qui induit f en restriction à A et qui, pour tout j $(1 \leq j \leq n)$, envoie X_j sur x_j.

Premier cas particulier.

Supposons donné un morphisme d'anneaux $f\colon A \longrightarrow B$, et soit $B[Y_1, Y_2, \ldots, Y_n]$ un anneau de polynômes à n indéterminées à coefficients dans B.

Le morphisme f définit aussi (par composition avec l'inclusion de B dans $B[Y_1, Y_2, \ldots, Y_n]$) un morphisme encore noté

$$f\colon A \longrightarrow B[Y_1, Y_2, \ldots, Y_n]\,.$$

On applique le théorème 5.1 en choisissant pour anneau cible l'anneau $B[Y_1, Y_2, \ldots, Y_n]$ et en posant $x_j := Y_j$. On obtient alors :

5.2. Corollaire. *Étant donné un morphisme d'anneaux $f\colon A \longrightarrow B$, il existe un et un seul morphisme*

$$A[X_1, X_2, \ldots, X_n] \longrightarrow B[Y_1, Y_2, \ldots, Y_n]$$

qui prolonge f et envoie X_j sur Y_j.

Deuxième cas particulier : fonction évaluation.

Prenons comme anneau B l'anneau $\mathrm{Fonc}(A^n, A)$ des fonctions de A^n vers A, où les lois d'addition et de multiplication sont définies comme l'addition et la multiplication point par point des fonctions.

On note $c\colon A \longrightarrow \mathrm{Fonc}(A^n, A)$ le morphisme qui, à l'élément $a \in A$, associe la fonction constante de valeur a.

On définit les éléments $\pi_1, \pi_2, \ldots, \pi_n$ de $\mathrm{Fonc}(A^n, A)$ par

$$\pi_j\colon A^n \longrightarrow A \quad , \quad (a_1, a_2, \ldots, a_n) \mapsto a_j\,.$$

Le morphisme

$$A[X_1, X_2, \ldots, X_n] \longrightarrow \mathrm{Fonc}(A^n, A) \quad , \quad X_j \mapsto \pi_j$$

qui prolonge c et envoie X_j sur π_j (voir le théorème 5.1) est appelé le morphisme d'évaluation. Il associe à un polynôme en n variables sur A la fonction polynomiale correspondante sur A^n.

Ainsi, à un polynôme $P(X_1, X_2, \ldots, X_n)$ on associe la *fonction polynôme* sur A^n définie par

$$(a_1, a_2, \ldots, a_n) \mapsto P(a_1, a_2, \ldots, a_n)\,.$$

Ⓘ Attention Ⓘ

Ce morphisme n'est pas nécessairement injectif : il peut arriver qu'un polynôme non nul définisse une fonction polynôme identiquement nulle. C'est ainsi que si q est une puissance d'un nombre premier et si $\mathbb{F}_q$ est un corps à q éléments (cf. plus loin dans le cours), le polynôme $X^q - X \in \mathbb{F}_q[X]$ est non nul (et de degré q) mais définit sur $\mathbb{F}_q$ la fonction nulle.

Remarque. Plus généralement, étant donné un morphisme d'anneaux $f\colon A \longrightarrow B$, on a un morphisme d'évaluation

$$A[X_1, X_2, \ldots, X_n] \longrightarrow \mathrm{Fonc}(B^n, B)$$

défini par la composition du morphisme d'évaluation défini ci–dessus, et du morphisme

$$A[X_1, X_2, \ldots, X_n] \longrightarrow B[Y_1, Y_2, \ldots, Y_n]$$

qui prolonge f.

Troisième cas particulier : substitution.

Donnons–nous des polynômes $\xi_1, \xi_2, \ldots, \xi_n \in A[X_1, X_2, \ldots, X_n]$.

Appliquant le théorème 5.1 en choisissant pour B l'anneau $A[X_1, X_2, \ldots, X_n]$, pour f l'injection naturelle de A dans B, et en posant $x_j := \xi_j$. On obtient alors :

5.3. *Étant donnés $\xi_1, \xi_2, \ldots, \xi_n \in A[X_1, X_2, \ldots, X_n]$, il existe un et un seul endomorphisme de $A[X_1, X_2, \ldots, X_n]$ qui induit l'identité sur A et envoie X_j sur ξ_j.*

Ce morphisme consiste à substituer, dans un polynôme $P(X_1, X_2, \ldots, X_n)$, le polynôme ξ_j à l'indéterminée X_j *i.e.*, :

$$P(X_1, X_2, \ldots, X_n) \mapsto P(\xi_1, \xi_2, \ldots, \xi_n)\,.$$

Quatrième cas particulier : spécialisation.

On constate facilement (par exemple grâce au théorème 5.1 – comment ?) qu'il y a un et un seul isomorphisme

$$A[X_1, X_2, \ldots, X_j, \ldots, X_n] \xrightarrow{\sim} A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n][X_j]$$

qui induit l'identité sur A et envoie X_k sur X_k pour tout k. Nous identifierons systématiquement $A[X_1, X_2, \ldots, X_j, \ldots, X_n]$ et $A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n][X_j]$ par cet isomorphisme.

Le résultat suivant est encore une conséquence du théorème 5.1 (pourquoi ?).

5.4. Proposition.

(1) Soit $a \in A$. Il existe un et un seul morphisme

$$A[X_1, X_2, \ldots, X_j, \ldots, X_n] \longrightarrow A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n]$$

qui induit l'identité sur $A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n]$ et envoie X_j sur a.

(2) Plus généralement, soit

$$\alpha(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n) \in A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n]\,.$$

Il existe un et un seul morphisme

$$A[X_1, X_2, \ldots, X_j, \ldots, X_n] \longrightarrow A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n]$$

qui induit l'identité sur $A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n]$ *et envoie*

$$X_j \quad \textit{sur} \quad \alpha(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n)\,.$$

Ces morphismes sont notés respectivement

$$P(X_1, X_2, \ldots, X_j, \ldots, X_n) \mapsto P(X_1, X_2, \ldots, a, \ldots, X_n)\,,$$

et

$$P([X_1, X_2, \ldots, X_j, \ldots, X_n) \mapsto P([X_1, X_2, \ldots, X_{j-1}, \alpha(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n), X_{j+1} \ldots, X_n)\,.$$

5.5. Proposition. *Soit* $\alpha(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n) \in A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n]$. *Les assertions suivantes sont équivalentes :*

(i) $P(X_1, X_2, \ldots, \alpha, \ldots, X_n) = 0\,,$

(ii) $P(X_1, X_2, \ldots, X_j, \ldots, X_n)$ *est divisible par* $X_j - \alpha$ *(dans* $A[X_1, X_2, \ldots, X_j, \ldots, X_n]$*).*

Démonstration de 5.5. Cela résulte de la propriété générale de division euclidienne dans les anneaux de polynômes (lemme 4.3).

On applique le lemme 4.3 en y remplaçant A par l'anneau de polynômes en $n-1$ indéterminées $A[X_1, X_2, \ldots, \widehat{X}_j, \ldots, X_n]$, et en choisissant $S(X) := P(X_1, X_2, \ldots, X_{j-1}, X, X_{j+1}, \ldots, X_n)$ et $T(X) := X - \alpha$. □

Propriétés de transfert.

Nous avons démontré plus haut qu'un certain nombre de propriétés se transfèrent de A à $A[X]$. Il en résulte que les mêmes propriétés se transfèrent de A à $A[X_1, X_2, \ldots, X_n]$.

5.6. Théorème.

(1) Si A *est intègre, alors* $A[X_1, X_2, \ldots, X_n]$ *est intègre, et* $A[X_1, X_2, \ldots, X_n]^\times = A^\times$.

(2) Si A *est factoriel, alors* $A[X_1, X_2, \ldots, X_n]$ *est factoriel. De plus, pour tout* j $(1 \leq j \leq n)$, *on a*

$$\operatorname{Irr} A[X_1, X_2, \ldots, X_n] = \begin{cases} \operatorname{Irr} A[X_1, X_2, \ldots, \widehat{X_j}, \ldots, X_n] \\ \bigcup \\ \operatorname{Prim} A[X_1, X_2, \ldots, \widehat{X_j}, \ldots, X_n][X_j] \ \cap \ \operatorname{Irr} F(X_1, X_2, \ldots, \widehat{X_j}, \ldots, X_n)[X_j] \end{cases}$$

Exemple 1.

Soit $P(X, Y) \in K[X, Y]$ un élément de la forme

$$P(X, Y) = a(X)Y + b(X)$$

où $a(X), b(X) \in K[X]$.

Alors l'élément $P(X, Y)$ est irréductible dans $K[X, Y]$ si et seulement si

- ou bien $a(X) = 0$ et $b(X)$ est irréductible dans $K[X]$,
- ou bien $a(X) \neq 0$ et alors $a(X) \wedge b(X) = 1$.

En effet, il suffit d'écrire que $P(X, Y)$ est irréductible dans $K[X, Y]$ si et seulement si

$$a(X)Y + b(X) \in \operatorname{Irr} K[X] \ \bigcup \ (\operatorname{Prim} K[X][Y] \cap \operatorname{Irr} K(X)[Y])$$

et de noter que, si $a(X) \neq 0$, le polynôme $a(X)Y + b(X)$ est irréductible (car de degré 1) dans $K(X)[Y]$.

Exemple 2 : Matrice générique.

Soit n un entier au moins égal à 1, et soit $M := (X_{i,j})$ la "matrice $n \times n$ générique", à coefficients dans l'anneau de polynômes à n^2 indéterminées $\mathbb{Z}[(X_{i,j})_{1 \leq i,j \leq n}]$. Désignons par $\chi_M(X) \in \mathbb{Z}[(X_{i,j}), X]$ son polynôme caractéristique.

5.7. Lemme. *Le polynôme $\chi_M(X)$ est irréductible dans $\mathbb{Q}((X_{i,j}))[X]$.*

Démonstration de 5.7. Puisque $\chi_M(X)$ est de degré en X au moins égal à 1, il suffit de vérifier que $\chi_M(X)$ est irréductible dans $\mathbb{Z}[(X_{i,j})][X]$.

Puisque le terme de plus haut degré de $\chi_M(X)$ est X^n, $\chi_M(X)$ est primitif dans $\mathbb{Z}[(X_{i,j})][X]$ et il suffit (cf. proposition 4.7) de trouver un idéal premier de $\mathfrak{p}$ de $\mathbb{Z}[(X_{i,j})]$ tel que la réduction de $\chi_M(X)$ modulo soit irréductible.

Considérons par exemple le morphisme surjectif

$$\mathbb{Z}[(X_{i,j})] \twoheadrightarrow \mathbb{Z}$$

qui envoie la matrice M sur la matrice $\begin{pmatrix} 0 & 0 & \cdots & 0 & p \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$. On voit alors que l'image de $\chi_M(X)$ est $X^n - p$, qui est irréductible d'après le critère d'Eisenstein. □

6. Polynômes symétriques

Definition et théorème fondamental.

Pour tout $\sigma \in \mathfrak{S}_n$, il y a un seul (endo-)morphisme d'algèbre de $A[X_1, X_2, \ldots, X_n]$ qui induit l'identité sur A et, pour tout j $(1 \leq j \leq n)$, envoie X_j sur $X_{\sigma(j)}$. On désigne encore cet endomorphisme par σ. Ainsi, on a

$$\begin{cases} \sigma \colon A[X_1, X_2, \ldots, X_n] \longrightarrow A[X_1, X_2, \ldots, X_n], \\ \sigma(P)(X_1, X_2, \ldots, X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}). \end{cases}$$

et

$$\begin{cases} \sigma(P+Q) = \sigma(P) + \sigma(Q), \\ \sigma(PQ) = \sigma(P)\sigma(Q) \end{cases}$$

pour tous $P, Q \in A[X_1, X_2, \ldots, X_n]$.

Exemple.

La transposition τ de $\mathfrak{S}_{\{X,Y\}}$ définit l'endomorphisme $P(X,Y) \mapsto P(Y,X)$ de $\mathbb{Z}[X,Y]$. Notons que le polynôme $X - Y$ n'est pas fixe par τ, tandis que le polynôme $X^2Y + XY^2$ l'est.

L'application qui à $\sigma \in \mathfrak{S}_n$ associe l'endomorphisme σ de $A[X_1, X_2, \ldots, X_n]$ définit une *opération* de $\mathfrak{S}_n$ sur $A[X_1, X_2, \ldots, X_n]$, *i.e.*, pour tous $\sigma, \sigma' \in \mathfrak{S}_n$ et $P \in A[X_1, X_2, \ldots, X_n]$, on a

$$\sigma(\sigma'(P)) = (\sigma\sigma')(P).$$

Il en résulte que les endomorphismes σ sont en fait des automorphismes.

Définition. On note $A[X_1, X_2, \ldots, X_n]^{\mathfrak{S}_n}$ l'ensemble des éléments de $A[X_1, X_2, \ldots, X_n]$ qui sont fixes par tous les éléments de $\mathfrak{S}_n$, et on appelle *polynômes symétriques* les éléments de $A[X_1, X_2, \ldots, X_n]^{\mathfrak{S}_n}$

Notons que $A[X_1, X_2, \ldots, X_n]^{\mathfrak{S}_n}$ est un sous–anneau de $A[X_1, X_2, \ldots, X_n]$.

Exemples.

Pour tout $P \in A[X_1, X_2, \ldots, X_n]$, les éléments

$$\sum_{\sigma \in \mathfrak{S}_n} \sigma(P) \quad \text{et} \quad \prod_{\sigma \in \mathfrak{S}_n} \sigma(P)$$

sont symétriques.

C'est ainsi que $\sum_{1 \leq j \leq n} X_j^2(X_j + 1)$ ou encore $\prod_{1 \leq j \leq n}(X_j^3 + 2X_j + 1)$ sont des polynômes symétriques.

Puisque le groupe $\mathfrak{S}_n$ opère sur l'anneau $A[X_1, X_2, \ldots, X_n]$, il opère aussi sur l'anneau de polynômes $A[X_1, X_2, \ldots, X_n][T]$.

Considérons le *polynôme générique*

$$P(T) := (T - X_1)(T - X_2) \cdots (T - X_n)\,.$$

Il est clair que $P(T)$ est fixe par $\mathfrak{S}_n$, *i.e.*,

$$P(T) \in A[X_1, X_2, \ldots, X_n]^{\mathfrak{S}_n}[T]\,.$$

Un calcul immédiat donne les formules suivantes.

$$P(T) = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^j \Sigma_j T^{n-j} + \cdots + (-1)^n \Sigma_n\,,$$

où

$$\begin{cases} \Sigma_1 = X_1 + X_2 + \cdots + X_n\,, \\ \Sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n\,, \\ \vdots \\ \Sigma_j = \displaystyle\sum_{i_1 < i_2 < \ldots i_j} X_{i_1} X_{i_2} \cdots X_{i_j}\,, \\ \vdots \\ \Sigma_1 = X_1 X_2 \cdots X_n\,, \end{cases}$$

6.1. Théorème. *Soient $Y_1, Y_2, \ldots, Y_n$ n indéterminées. Alors l'application*

$$\begin{cases} A[Y_1, , Y_2, \ldots, Y_n] \longrightarrow A[X_1, X_2, \ldots, X_n] \\ \textit{pour tout } j\,,\ Y_j \mapsto \Sigma_j \end{cases}$$

définit un isomorphisme d'anneaux

$$A[Y_1, , Y_2, \ldots, Y_n] \xrightarrow{\sim} A[X_1, X_2, \ldots, X_n]^{\mathfrak{S}_n}\,.$$

Les formules de Newton.

Posons

$$\Lambda(T) := T^n P(1/T) = (1 - X_1T)(1 - X_2T) \cdots (1 - X_nT)\,.$$

Ainsi, on a

$$\Lambda(T) = 1 - \Sigma_1 T + \cdots + (-1)^j \Sigma_j T^j + \cdots + (-1)^n \Sigma_n T^n\,.$$

Le calcul de la dérivée logarithmique de $\Lambda(T)$ donne

$$-\frac{\Lambda'(T)}{\Lambda(T)} \;=\; \sum_{j=1}^{j=n} \frac{X_j}{1 - X_jT} \;=\; \sum_{k=0}^{\infty} P_{k+1}(X_1, X_2, \ldots, X_n) T^k$$

où on note

$$P_k(X_1, X_2, \dots, X_n) := X_1^k +_2^k + \cdots + X_n^k .$$

En explicitant la formule

$$-\Lambda'(T) = \Lambda(T)\left(-\frac{\Lambda'(T)}{\Lambda(T)}\right),$$

on obtient

$$\Sigma_1 + \cdots + (-1)^{j+1} j \Sigma_j T^{j-1} + \cdots + (-1)^{n+1} n \Sigma_n T^{n-1} =$$
$$\left(1 - \Sigma_1 T + \cdots + (-1)^k \Sigma_k T^k + \cdots + (-1)^n \Sigma_n T^n\right)\left(\sum_{l=0}^{\infty} P_{l+1}(X_1, X_2, \dots, X_n) T^l\right).$$

La formule précédente fournit les égalités ("formules de Newton") :

$$\begin{cases} \text{Pour } m \geq n : \displaystyle\sum_{k+l=m} (-1)^k \, \Sigma_k(X_1, X_2, \dots, X_n) P_{l+1}(X_1, X_2, \dots, X_n) = 0 , \\ \text{Pour } m < n : \displaystyle\sum_{k+l=m} (-1)^k \, \Sigma_k(X_1, X_2, \dots, X_n) P_{l+1}(X_1, X_2, \dots, X_n) = (-1)^m (m+1) \Sigma_{m+1} . \end{cases}$$

Fractions rationnelles symétriques.

Soit F le corps des fractions de l'anneau intègre A.

Le groupe $\mathfrak{S}_n$ opère sur le corps des fractions rationnelles $F(X_1, X_2, \dots, X_n)$ par la formule

$$\sigma(P/Q) := \sigma(P)/\sigma(Q)$$

pour tous $\sigma \in \mathfrak{S}_n$, $P, Q \in A[X_1, X_2, \dots, X_n]$, $Q \neq 0$.

Les fractions rationnelles fixes par $\mathfrak{S}_n$ sont appelées les fractions rationnelles symétriques. L'ensemble des fractions rationnelles symétriques est un sous–corps de $F(X_1, X_2, \dots, X_n)$, que l'on note $F(X_1, X_2, \dots, X_n)^{\mathfrak{S}_n}$.

D'autre part, l'isomorphisme

$$A[Y_1, Y_2, \dots, Y_n] \xrightarrow{\sim} A[X_1, X_2, \dots, X_n]^{\mathfrak{S}_n} \quad , \quad P(Y_1, Y_2, \dots, Y_n) \mapsto P(\Sigma_1, \Sigma_2, \dots, \Sigma_n)$$

induit un isomorphisme

$$F(Y_1, Y_2, \dots, Y_n) \xrightarrow{\sim} F(\Sigma_1, \Sigma_2, \dots, \Sigma_n) .$$

6.2. Proposition. *On a*

$$F(X_1, X_2, \dots, X_n)^{\mathfrak{S}_n} = F(\Sigma_1, \Sigma_2, \dots, \Sigma_n) .$$

Démonstration de 6.2. Il est clair que $F(\Sigma_1, \Sigma_2, \dots, \Sigma_n)$ est contenu dans le corps des fractions rationnelles symétriques. Inversement, démontrons que toute fraction rationnelle symétrique appartient à $F(\Sigma_1, \Sigma_2, \dots, \Sigma_n)$.

Remarquons d'abord que tout élément de $F(X_1, X_2, \dots, X_n)$ peut s'écrire P/Q où Q est un polynôme symétrique. En effet, si R/T est une fraction quelconque, on a

$$\frac{R}{T} = \frac{R \prod_{\sigma \neq 1} \sigma(T)}{\prod_\sigma \sigma(T)} .$$

Pour une telle fraction P/Q on voit alors qu'elle est symétrique si et seulement si P est symétrique. □

Polynômes antisymétriques.

On définit l'élément $\delta(X_1, X_2, \ldots, X_n) \in A[X_1, X_2, \ldots, X_n]$ par la formule

$$\delta(X_1, X_2, \ldots, X_n) := \prod_{1 \leq i < j \leq n} (X_j - X_i)\,.$$

6.3. Lemme. *Pour tout $\sigma \in \mathfrak{S}_n$, on a*

$$\sigma(\delta) = \mathrm{sgn}(\sigma)\delta$$

où

$$\mathrm{sgn}\colon \mathfrak{S}_n \twoheadrightarrow \{\pm 1\}$$

est le morphisme signature.

Démonstration de 6.3. Il est clair qu'il existe une fonction $\varepsilon\colon \mathfrak{S}_n \longrightarrow \{\pm 1\}$ telle que $\sigma(\delta) = \varepsilon(\sigma)\delta$. Comme cette fonction ε est manifestement un morphisme de groupes et qu'elle prend la valeur -1 sur toute transposition, elle est égale à la signature. □

Un polynôme $P(X_1, X_2, \ldots, X_n)$ est dit *antisymétrique* s'il vérifie la condition

$$\sigma(P)(X_1, X_2, \ldots, X_n) = \mathrm{sgn}(\sigma)P(X_1, X_2, \ldots, X_n)$$

pour tout $\sigma \in \mathfrak{S}_n$.

6.4. Proposition. *Supposons A factoriel et de caractéristique différente de 2.*
Un polynôme $P(X_1, X_2, \ldots, X_n)$ est antisymétrique si et seulement si il est de la forme

$$P(X_1, X_2, \ldots, X_n) = \delta(X_1, X_2, \ldots, X_n)P_0(X_1, X_2, \ldots, X_n)$$

où $P_0(X_1, X_2, \ldots, X_n)$ est un polynôme symétrique.

Démonstration de 6.4. Si P est antisymétrique, pour tous i et j tels que $i < j$ on a

$$P(X_1, X_2, \ldots, X_n)_{|X_i = X_j} = 0\,,$$

et par conséquent (appliquer la proposition 5.5 avec $\alpha = X_i$) on voit que $P(X_1, X_2, \ldots, X_n)$ est divisible par $X_j - X_i$. Comme les $X_j - X_i$ sont irréductibles (pourquoi ?) et que l'anneau $A[X_1, X_2, \ldots, X_n]$ est factoriel, on voit que $P(X_1, X_2, \ldots, X_n)$ est divisible par leur produit, *i.e.*, est divisible par δ. Il est alors clair que le quotient est symétrique. □

7. Résultant et discriminant

7.A. Résultant de deux polynômes.

Convention. Pour tout système de vecteurs $(v_1, v_2, \ldots, v_n)$ dans un espace vectoriel, combinaisons linéaires des éléments $(e_1, e_2, \ldots, e_n)$ d'un autre système de vecteurs :

$$\left\{\begin{array}{ccccc} v_1 = & a_{1,1}e_1 + a_{1,2}e_2 & + \cdots + & a_{1,n}e_n \\ v_2 = & a_{2,1}e_1 + a_{2,2}e_2 & + \cdots + & a_{2,n}e_n \\ \vdots & \vdots & \vdots & \vdots \\ v_n = & a_{n,1}e_1 + a_{n,2}e_2 & + \cdots + & a_{n,n}e_n\,, \end{array}\right.$$

on appelle *matrice du système $(v_1, v_2, \ldots, v_n)$ sur $(e_1, e_2, \ldots, e_n)$* la matrice $(a_{i,j})_{1 \leq i,j \leq n}$, et on appelle *déterminant du système $(v_1, v_2, \ldots, v_n)$ sur $(e_1, e_2, \ldots, e_n)$* le déterminant de cette matrice $(a_{i,j})_{1 \leq i,j \leq n}$.

Si φ est un endomorphisme d'un espace vectoriel de base $(e_1, e_2, \ldots, e_n)$, la matrice Φ de φ sur cette base est par définition *la transposée* de la matrice du système $(\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n))$ sur $(e_1, e_2, \ldots, e_n)$ (en d'autres termes, les *colonnes* de la matrice Φ sont les coordonnées des vecteurs $\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n)$).

Soit A un anneau intègre, soient m et n deux entiers positifs, et soient $P(X)$ et $Q(X)$ deux éléments de $A[X]$, de degrés respectifs au plus m et n.

Définition. Le résultant $\mathrm{Res}_{m,n}(P,Q)$ est par définition le déterminant, sur la base

$$\{X^{m+n-1}, X^{m+n-2}, \dots, X, 1\}$$

du système

$$\{X^{n-1}P(X), X^{n-2}P(X), \dots, P(X), X^{m-1}Q(X), X^{m-2}Q(X), \dots, Q(X)\}\,.$$

En d'autres termes, si

$$\begin{aligned} P(X) &:= p_m X^m + p_{m-1}X^{m-1} + \cdots + p_1 X + p_0 \\ Q(X) &:= q_n X^n + q_{n-1}X^{n-1} + \cdots + q_1 X + q_0\,, \end{aligned}$$

on a $\mathrm{Res}_{m,n}(P,Q) = \det \mathrm{Mat}_{m,n}(P,Q)$ où

$$\mathrm{Mat}_{m,n}(P,Q) = \begin{pmatrix} p_m & p_{m-1} & \cdots & \cdots & \cdots & p_0 & 0 & \cdots & 0 \\ 0 & p_m & \cdots & \cdots & \cdots & p_1 & p_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & p_m & \cdots & \cdots & \cdots & \cdots & p_0 \\ q_n & q_{n-1} & \cdots & \cdots & q_0 & \cdots & 0 & \cdots & 0 \\ 0 & q_n & \cdots & \cdots & q_1 & q_0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & q_n & \cdots & q_0 \end{pmatrix}$$

est une matrice carrée à $m+n$ lignes et $m+n$ colonnes, dont les n premières lignes contiennent les coefficients de $P(X)$ (et des zéros), et les m dernières lignes contiennent les coefficients de $Q(X)$ (et des zéros).

Premiers exemples.

1. Choisissons $P(X) = X - a$ et $Q(X) = X - b$. On a :

$$\mathrm{Res}_{1,1}(P,Q) = \begin{vmatrix} 1 & -a \\ 1 & -b \end{vmatrix} = a - b = -P(b) = Q(a)\,.$$

2. Choisissons $P(X) = aX^2 + bX + c$ et $Q(X) = X - d$. Désignons par α_1 et α_2 les racines de $P(X)$. On a :

$$\mathrm{Res}_{2,1}(P,Q) = \begin{vmatrix} a & b & c \\ 1 & -d & 0 \\ 0 & 1 & -d \end{vmatrix} = ad^2 + bd + c = P(d) = aQ(\alpha_1)Q(\alpha_2)\,.$$

Nous allons voir comment les propriétés constatées ci–dessus se généralisent.

Premières propriétés.

1. Si $p_m = q_n = 0$, on a $\mathrm{Res}_{m,n}(P,Q) = 0$.
2. On a la *formule de réciprocité* :

$$\mathrm{Res}_{m,n}(P,Q) = (-1)^{mn}\mathrm{Res}_{n,m}(Q,P)\,.$$

3. Pour tout entier naturel n, désignons par $A[X]_n$ le sous–groupe – en fait, le sous–A–module (cf. plus loin dans le cours) des éléments de $A[X]$ de degré inférieur ou égal à n.

7.1. Lemme. *Les deux assertions suivantes sont équivalentes :*

(i) $\mathrm{Res}_{m,n}(P,Q)=0$.

(ii) *Il existe* $U(X)\in A[X]_{m-1}$ *et* $V(X)\in A[X]_{n-1}$ *tels que*

$$U(X)Q(X)+V(X)P(X)=0\,.$$

Démonstration de 7.1. On écrit que le déterminant du système

$$\{X^{n-1}P(X),X^{n-2}P(X),\dots,P(X),X^{m-1}Q(X),X^{m-2}Q(X),\dots,Q(X)\}$$

sur la base $\{X^{m+n-1},X^{m+n-2},\dots,X,1\}$ est nul si et seulement si il existe une combinaison linéaire de ces vecteurs qui est nulle. □

7.2. Corollaire. *Supposons A factoriel, de corps des fractions F, et supposons $p_m q_n\neq 0$. Les deux assertions suivantes sont équivalentes :*

(i) $\mathrm{Res}_{m,n}(P,Q)=0$.

(ii) $P(X)$ *et* $Q(X)$ *ne sont pas premiers entre eux dans* $F[X]$.

Démonstration de 7.2.

(i) ⇒ (ii) : On sait qu'il existe $U(X)\in A[X]_{m-1}$ et $V(X)\in A[X]_{n-1}$ tels que $U(X)Q(X)=-V(X)P(X)$. Si $P(X)$ et $Q(X)$ étaient premiers entre eux, par le lemme de Gauß on obtiendrait que $P(X)$ divise $U(X)$ ce qui est impossible pour des raisons de degré.

(ii) ⇒ (i) : Supposons qu'il existe $D(X)$, de degré au moins 1, tel que $P(X)=D(X)P_1(X)$ et $Q(X)=D(X)Q_1(X)$. On voit alors que $P_1(X)Q(X)-Q_1(X)P(X)=0$. □

4. Généralisons la propriété précédente. Considérons l'application linéaire

$$\mathrm{R}_{m,n}\colon\begin{cases}A[X]_{m-1}\times A[X]_{n-1}\longrightarrow A[X]_{m+n-1}\\ (U(X),V(X))\mapsto U(X)Q(X)+V(X)P(X)\,.\end{cases}$$

Alors la matrice de cette application sur les bases

$$\{(0,X^{n-1}),(0,X^{n-2}),\dots,(0,1),(X^{m-1},0),(X^{m-2},0),\dots,(1,0),\}$$

et

$$\{X^{m+n-1},X^{m+n-2},\dots,X,1\}$$

est la matrice ${}^t\mathrm{Mat}_{m,n}(P,Q)$.

Soit ${}_{\mathrm{Mat}}\mathbf{Com}_{m,n}(P,Q)$ la comatrice de $\mathrm{Mat}_{m,n}(P,Q)$. Comme on a

$${}^t\mathrm{Mat}_{m,n}(P,Q)\,{}_{\mathrm{Mat}}\mathbf{Com}_{m,n}(P,Q)\;=\;\det\mathrm{Mat}_{m,n}(P,Q)\,\mathrm{Id}_{m+n}=\mathrm{Res}_{m,n}(P,Q)\,\mathrm{Id}_{m+n}\,,$$

on voit que l'image de l'application $\mathrm{R}_{m,n}$ contient $\mathrm{Res}_{m,n}(P,Q)\,A[X]_{m+n}$. On a donc démontré :

7.3. Proposition. *Il existe* $U(X)\in A[X]_{m-1}$ *et* $V(X)\in A[X]_{n-1}$ *tels que*

$$U(X)Q(X)+V(X)P(X)=\mathrm{Res}_{m,n}(P,Q)\,.$$

Résultant et racines.

Supposons $P(X) = p_m X^m + p_{m-1}X^{m-1} + \cdots + p_1 X + p_0$ de degré m, *i.e.*, $p_m \neq 0$. Alors le quotient $F[X]/(P(X))$ est un espace vectoriel sur F de dimension m.

L'opération

$$\mu_X \colon F[X] \longrightarrow F[X] \quad , \quad R(X) \mapsto XR(X)$$

définit par passage au quotient un endomorphisme de l'espace vectoriel $F[X]/(P(X))$ encore désigné par μ_X. Plus généralement, si $Q(X) \in F[X]$, l'endomorphisme $Q(\mu_X)$ est induit par l'opération de multiplication par $Q(X)$. On note alors $\left(\frac{Q(X)}{P(X)}\right)$ le déterminant de cette opération de multiplication par $Q(X)$ dans l'espace vectoriel $F[X]/(P(X))$.

Exemple. Pour $P(X) = X^2 + bX + c$, on a

$$\left(\frac{X-d}{P(X)}\right) = \det{}_{\{1,X\}}(X-d, X^2 - dX) = \begin{vmatrix} -d & -c \\ 1 & -b-d \end{vmatrix} = d^2 + bd + c\,.$$

7.4. Lemme. *Supposons $P(X) = p_m X^m + p_{m-1}X^{m-1} + \cdots + p_1 X + p_0$ avec $p_m \neq 0$, et $Q(X)$ de degré au plus n. On a alors*

$$\mathrm{Res}_{m,n}(P,Q) = p_m^n \left(\frac{Q(X)}{P(X)}\right)$$

Démonstration de 7.4. Pour tout polynôme $T(X) \in F[X]$, désignons par $R_P(T)$ le reste de la division euclidienne de $T(X)$ par $P(X)$.

Pour tout entier $j < m$, on a $X^j Q(X) = S(X)P(X) + R_P(X^j Q(X))$ où $S(X)$ est un polynôme de degré au plus $n-1$.

Il en résulte que $\mathrm{Res}_{m,n}(P,Q)$ est le déterminant, sur la base $\{X^{m+n-1}, X^{m+n-2}, \ldots, X, 1\}$ du système

$$\{X^{n-1}P(X), X^{n-2}P(X), \ldots, P(X), R_P(X^{m-1}Q(X)), R_P(X^{m-2}Q(X)), \ldots, R_P(Q(X))\}\,.$$

Ainsi, $\mathrm{Res}_{m,n}(P,Q)$ est le déterminant d'une matrice $(m+n)\times(m+n)$ de la forme $\begin{pmatrix} T & T' \\ 0 & M \end{pmatrix}$ où T est une matrice $n \times n$ triangulaire supérieure de la forme

$$T = \begin{pmatrix} p_m & \cdots & \cdots & \cdots \\ 0 & p_m & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_m \end{pmatrix}$$

et où M est la matrice de $\mu_{Q(X)}$. □

Remarque. Supposons $P(X)$ et $Q(X)$ unitaires et de degrés respectifs m et n. On a alors la formule de réciprocité suivante (qui peut être à rapprocher de la formule de réciprocité quadratique de Gauß) :

$$\left(\frac{Q(X)}{P(X)}\right) = (-1)^{mn}\left(\frac{P(X)}{Q(X)}\right)\,.$$

7.5. Proposition.
(1) Supposons $p_m \neq 0$ et $P(X) = p_m(X-a_1)(X-a_2)\cdots(X-a_m)$. Alors

$$\mathrm{Res}_{m,n}(P,Q) = p_m^n Q(a_1)Q(a_2)\cdots Q(a_m)\,.$$

(2) Supposons de plus $q_n \neq 0$ et $Q(X) = q_n(X-b_1)(X-b_2)\cdots(X-b_n)$. Alors

$$\mathrm{Res}_{m,n}(P,Q) = p_m^n q_n^m \prod_{i,j}(a_i - b_j)\,.$$

Démonstration de 7.5. Il suffit de remarquer que l'endomorphisme μ_X de l'espace vectoriel $F[X]/(P(X))$ a pour polynôme minimal (et donc caractéristique) $P(X)$, donc est trigonalisable avec pour valeurs propres $a_1, a_2, \ldots, a_m$. L'assertion (1) résulte alors du lemme 7.4. L'assertion (2) est immédiate à partir de (1). □

7.6. Corollaire. *Soit φ un endomorphisme d'un espace vectoriel de dimension finie m sur un corps F, et soit $\chi_\varphi(X)$ son polynôme caractéristique. Soit $Q(X)$ un élément de degré au plus n de $F[X]$. On a*

$$\det Q(\varphi) = \mathrm{Res}_{m,n}(\chi_\varphi, Q)\,.$$

Démonstration de 7.6. Quitte à augmenter le corps de base, on peut supposer que $\chi_\varphi(X)$ est totalement décomposé (*i.e.*, produit de facteurs de degré 1). L'endomorphisme φ est alors trigonalisable. Si $a_1, a_2, \ldots, a_m$ sont ses valeurs propres, on a alors $\det Q(\varphi) = Q(a_1)Q(a_2)\cdots Q(a_m)$, d'où la formule annoncée. □

Une application géométrique.

Soient $P(X,Y,Z)$ et $Q(X,Y,Z)$ deux éléments de $\mathbb{C}[X,Y,Z]$, définissant deux surfaces algébriques S_P et S_Q dans $\mathbb{C}^3$ par

$$S_P := \{(x,y,z) \in \mathbb{C}^3 \mid (P(x,y,z) = 0)\}\,,$$
$$S_Q := \{(x,y,z) \in \mathbb{C}^3 \mid (Q(x,y,z) = 0)\}\,.$$

Regardons les polynômes $P(X,Y,Z)$ et $Q(X,Y,Z)$ comme éléments de $\mathbb{C}[X,Y][Z]$:

$$P(X,Y,Z) := p_m(X,Y)Z^m + \cdots + p_1(X,Y)Z + p_0(X,Y)\,,$$
$$Q(X,Y,Z) := q_n(X,Y)Z^n + \cdots + q_1(X,Y)Z + q_0(X,Y)\,,$$

et désignons par $\mathrm{Res}^{(Z)}_{m,n}(P,Q)(X,Y)$ leur résultant, élément de $\mathbb{C}[X,Y]$.

On note C_{p_m} et C_{q_n} les courbes de $\mathbb{C}^2$ définies respectivement par les équations

$$C_{p_m} := \{(x,y) \in \mathbb{C}^2 \mid (p_m(x,y) = 0)\} \quad \text{et} \quad C_{q_n} := \{(x,y) \in \mathbb{C}^2 \mid (q_n(x,y) = 0)\}\,.$$

Désignons par $\mathrm{pr}_{x,y}\colon \mathbb{C}^3 \twoheadrightarrow \mathbb{C}^2$ la projection définie par $(x,y,z) \mapsto (x,y)$.

7.7. Proposition. *L'ensemble $S^{(Z)}_{P,Q}$ des points de $\mathbb{C}^2$ défini par*

$$S^{(Z)}_{P,Q} := \{(x,y) \in \mathbb{C}^2 \mid (\mathrm{Res}^{(Z)}_{m,n}(P,Q)(x,y) = 0)\}$$

est égal à

$$(C_{p_m} \cap C_{q_n}) \bigcup \mathrm{pr}_{x,y}(S_P \cap S_Q)\,.$$

Discriminant.

Définition. Soit $P(X) = p_m(X - a_1)(X - a_2)\cdots(X - a_m)$. On appelle discriminant de $P(X)$ et on note $\mathrm{Discr}\, P(X)$ l'élément défini par

$$\mathrm{Discr}\, P(X) := p_m^{2m-2} \left(\prod_{1 \leq i < j \leq m} (a_i - a_j) \right)^2 .$$

Notons qu'ainsi par définition $\mathrm{Discr}\, P(X)$ est le carré des éléments

$$\pm\, p_m^{m-1} \prod_{1 \leq i < j \leq m} (a_i - a_j) .$$

On voit aussi que

$$\mathrm{Discr}\, P(X) := p_m^{2m-2} (-1)^{m(m-1)/2} \prod_{1 \leq i \neq j \leq m} (a_i - a_j) .$$

Exemple. Si $P(X) = aX^2 + bX + c$, on vérifie que $\mathrm{Discr}\, P(X) = b^2 - 4ac$.

Supposons dorénavant $P(X)$ unitaire, *i.e.*, $p_m = 1$.

Comme

$$P'(X) = \sum_{i=0}^{i=m} (X - a_1)(X - a_2) \cdot \cdots \cdot \widehat{(X - a_i)} (X - a_m) ,$$

on voit alors que

$$\mathrm{Discr}\, P(X) = (-1)^{m(m-1)/2} \prod_{1 \leq i \leq m} P'(a_i) = (-1)^{m(m-1)/2} \mathrm{Res}_{m,m-1}(P, P')$$

d'où

$$\mathrm{Discr}\, P(X) = (-1)^{m(m-1)/2} \left(\frac{P'(X)}{P(X)} \right) .$$

Exemple.

Soit $P(X) = X^3 + pX + q$.

On a $m = 3$, donc $m(m-1)/2 = 3$, et $P'(X) = 3X^2 + p$. On voit donc que

$$\mathrm{Discr}\, P(X) = -\mathrm{Res}_{3,2}(P, P') = -\mathrm{Res}_{2,3}(P', P) = -3^3 \left(\frac{X^3 + pX + q}{3X^2 + p} \right)$$

$$= -27 \begin{vmatrix} q & -2p^2/9 \\ 2p/3 & q \end{vmatrix} = -4p^3 - 27q^2 .$$

Remarque. Pour que les calculs indiqués ci–dessus soient corrects, il faut supposer que le corps F est de caractéristique différente de 3. On laisse la lectrice et lecteur mener à bien le calcul dans le cas où F est de caractéristique 3.

Donnons une application géométrique de cette formule.

Considérons la surface définie par

$$S := \{(p, q, x) \in \mathbb{C}^3 \mid (x^3 + px + q = 0)\} .$$

[Dessin]

Alors la courbe C définie par

$$X := \{(p, q) \in \mathbb{C}^2 \mid (4p^3 + 27q^2 = 0)\}$$

est le contour apparent de S "vu depuis le plan (p, q)".

Deuxième partie : Modules

8. Définitions et conventions

Dans tout ce qui suit, A désigne un anneau commutatif unitaire. Si de plus A est supposé intègre, on note F son corps des fractions.

Un A–module M est un groupe additif muni d'une multiplication

$$A \times M \longrightarrow M \quad , \quad (\lambda, m) \mapsto \lambda m$$

vérifiant les propriétés suivantes (pour tous $m, n \in M$, $\lambda, \mu \in A$) :

- elle est bilinéaire, *i.e.*, $(\lambda + \mu)m = \lambda m + \mu m \quad$ et $\quad \lambda(m + n) = \lambda m + \lambda n$,
- $1_A\, m = m$,
- $(\lambda\mu)m = \lambda(\mu m)$.

Il en résulte que

$$\begin{cases} 0_A\, m = 0_M \\ (-\lambda)m = -(\lambda m)\,. \end{cases}$$

8.1. Lemme.
(1) Un groupe abélien M muni d'une application

$$A \times M \longrightarrow M \quad , \quad (\lambda, m) \mapsto \lambda m$$

est un A–module si et seulement si l'application

$$A \longrightarrow \mathrm{End}(M) \quad , \quad \lambda \mapsto (m \mapsto \lambda m)$$

est un morphisme d'anneau.
(2) Si M est un groupe abélien muni d'un morphisme d'anneaux $\varphi\colon A \longrightarrow \mathrm{End}(M)$, alors la multiplication externe définie par

$$A \times M \longrightarrow M \ , \ (\lambda, m) \mapsto \varphi(\lambda)(m)$$

définit sur M une structure de A–module.

Si M et N sont deux A–modules, un morphisme de A–modules $\varphi\colon M \longrightarrow N$ est un morphisme de groupes abéliens tel que $\varphi(\lambda m) = \lambda\varphi(m)$ pour tous $\lambda \in A$ et $m \in M$.

Quelques exemples.

1. Tout groupe abélien est muni d'une et d'une seule structure de $\mathbb{Z}$–module, parfois appelée la "structure naturelle" de $\mathbb{Z}$–module.
Les morphismes de groupes abéliens sont les morphismes de $\mathbb{Z}$–modules.

2. Les F–modules sont les espaces vectoriels sur F et les morphismes de F–modules sont les applications linéaires.

3. Si $\mathfrak{a}$ est un idéal de A, $\mathfrak{a}$ et $A/\mathfrak{a}$ sont naturellement munis de structures de A–modules. L'injection naturelle $\mathfrak{a} \hookrightarrow A$ et la surjection naturelle $A \twoheadrightarrow A/\mathfrak{a}$ sont des morphismes de A–modules.

4. Soit $\mathfrak{a}$ un idéal de A et soit M un $A/\mathfrak{a}$–module. La composition du morphisme de structure $A/\mathfrak{a} \longrightarrow \mathrm{End}(M)$ avec la surjection canonique $A \twoheadrightarrow A/\mathfrak{a}$ définit sur M une structure de A–module, qu'on appelle parfois "M vu comme A–module".

5. Soit M un A–module et soit $\mathfrak{a}$ un idéal de A tel que $am = 0$ pour tous $a \in \mathfrak{a}$ et $m \in M$. Alors M est naturellement muni d'une structure de $A/\mathfrak{a}$–module.

En effet, par hypothèse le morphisme $A \longrightarrow \mathrm{End}(M)$ qui définit la structure de A–module se factorise par $A/\mathfrak{a}$.

6. Si I est un ensemble, on note $A^{(I)}$ l'ensemble des familles $(a_i)_{i\in I}$ telles que $a_i = 0$ pour presque tout $i \in I$ (*i.e.*, pour tous les i sauf un nombre fini). On munit $A^{(I)}$ de la structure évidente de A–module. On appelle $A^{(I)}$ le *A–module type sur I*.

Notons que, si I est fini, on a $A^{(I)} = A^I$.

On note $\mathbf{e}_i$ l'élément de $A^{(I)}$ dont toutes les coordonnées sont nulles, sauf la i–ième qui est égale à 1. On voit alors que tout élément $\mathbf{a} = (a_i)_{i\in I}$ s'écrit

$$\mathbf{a} = \sum_{i\in I} a_i \mathbf{e}_i \,,$$

la somme ayant un sens puisque presque tous les coefficients sont nuls.

7. Soit E une algèbre non nécessairement commutative sur un corps K, et soit $x \in E$. La multiplication

$$K[X] \times E \longrightarrow E \quad , \quad (P(X), e) \mapsto P(x)e$$

définit sur E une structure de $K[X]$–module, parfois alors noté E_x.

Si $z \in E$ commute à x, la multiplication par z dans E est alors un endomorphisme du $K[X]$–module E_x.

8. Soit V un K–espace vectoriel. Soit $\varphi \in \mathrm{End}(V)$. Alors le morphisme naturel

$$K[X] \longrightarrow \mathrm{End}(V) \quad , \quad P(X) \mapsto P(\varphi)$$

muni V d'une structure de $K[X]$–module noté V_φ.

Les endomophismes du $K[X]$–module V_φ sont les endomorphismes du K–espace vectoriel V qui commutent à φ.

Sous–modules, sommes, quotients.

On laisse au lecteur le soin de définir la notion de sous–module, de vérifier que l'intersection d'une famille de sous–modules est un sous–module, et donc de définir la notion de sous–module engendré par un sous–ensemble.

Somme de deux sous–modules, somme directe.

Si M_1 et M_2 sont deux sous–modules d'un A–module M, on note $M_1 + M_2$ le sous–module engendré par $M_1 \cup M_2$. Il est clair que

$$M_1 + M_2 = \{m_1 + m_2 \mid (m_1 \in M_1)(m_2 \in M_2)\} \,.$$

On dit que la somme $M_1 + M_2$ est directe et on écrit alors $M_1 + M_2 = M_1 \oplus M_2$ si $M_1 \cap M_2 = \{0\}$. On a $M_1 + M_2 = M_1 \oplus M_2$ si et seulement si, pour tous $m_1, m_1' \in M_1$, $m_2, m_2' \in M_2$, on a

$$(m_1 + m_2 = m_1' + m_2') \;\Leftrightarrow\; (m_1 = m_1') \text{ et } (m_2 = m_2') \,.$$

Plus généralement, si $(M_i)_{i\in I}$ est une famille de sous–modules de M, on note $\sum_{i\in I} M_i$ le sous–module de M engendré par $\bigcup_{i\in I} M_i$. On dit que la somme est directe et on écrit

$$\sum_{i\in I} M_i = \bigoplus_{i\in I} M_i$$

si tout élément de $\sum_{i\in I} M_i$ s'écrit de façon unique $\sum_{i\in I} m_i$ avec, pour tout $i \in I$, $m_i \in M_i$ (et $m_i = 0$ pour presque tout i).

Somme directe "externe".

Soient M_1 et M_2 sont deux A–modules. On note alors

$$M_1 \sqcup M_2 := \{(m_1, m_2) \mid (m_1 \in M_1)(m_2 \in M_2)\}\,.$$

Il est clair que

- $M_1 \sqcup M_2$ est naturellement muni d'une structure de A–module,
- Les applications
$$M_1 \longrightarrow M_1 \sqcup M_2\ ,\ m_1 \mapsto (m_1, 0)$$
$$M_2 \longrightarrow M_1 \sqcup M_2\ ,\ m_2 \mapsto (0, m_2)$$
sont des morphismes injectifs de A–modules, qui identifient M_1 et M_2 respectivement à des sous–modules $\widetilde{M_1}$ et $\widetilde{M_2}$ de $M_1 \sqcup M_2$ tels que
$$M_1 \sqcup M_2 = \widetilde{M_1} \oplus \widetilde{M_2}\,.$$

Le module $M_1 \sqcup M_2$ est appelé (parfois) la somme directe externe de M_1 et M_2. Il arrive (très souvent) de poser, par abus de notation :

$$M_1 \sqcup M_2 = M_1 \oplus M_2\,.$$

Quotients.

Si N est un sous–module du A–module M, il existe une et une seule structure de A–module sur le groupe quotient M/N telle que la surjection naturelle

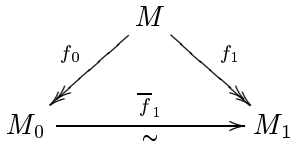
$$\pi_N \colon M \twoheadrightarrow M/N$$

est un morphisme de A–modules. Notons que le noyau de π_N est N.

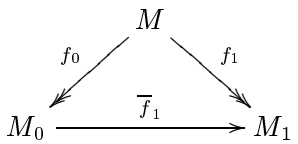
Le couple $(M/N, \pi_N)$ est caractérisé (à unique isomorphisme près) par le fait que M/N est un A–module et $\pi_N \colon M \twoheadrightarrow M/N$ est un morphisme surjectif de noyau N, grâce aux propriétés universelles suivantes.

8.2. Proposition.
Soit (M_0, f_0) un couple où M_0 est un A–module et $f_0 \colon M \longrightarrow M_0$ est un morphisme surjectif de noyau N

(1) Soit (M_1, f_1) un (autre) couple où M_1 est un A–module et $f_1 \colon M \longrightarrow M_1$ est un morphisme surjectif de noyau N. Alors il existe un unique isomorphisme $\overline{f}_1$ de M_0 sur M_1 tel que le diagramme suivant est commutatif



(2) Plus généralement, soit (M_1, f_1) un couple où M_1 est un A–module et $f_1 \colon M \longrightarrow M_1$ est un morphisme dont le noyau contient N. Alors il existe un unique morphisme $\overline{f}_1 \colon M_0 \longrightarrow M_1$ tel que le diagramme suivant est commutatif



De plus, le noyau de $\overline{f}_1$ *est* $f_0(\ker(f_1))$*, sous–module de* M_0 *isomorphe à* $\ker(f_0)/N$.

Exemples–Exercices.

(1) Soient M_1 et M_2 deux sous–modules d'un A–module M. Alors l'injection naturelle de M_1 dans $M_1 + M_2$ induit un isomophisme

$$M_1/(M_1 \cap M_2) \xrightarrow{\sim} (M_1 + M_2)/M_2 \,.$$

(2) Soient M' et N deux sous–modules d'un A–module M tels que $N \subseteq M'$. Alors la surjection naturelle $M/N \twoheadrightarrow M/M'$ induit un isomorphisme

$$(M/N)/(M'/N) \xrightarrow{\sim} M/M' \,.$$

Modules et idéaux.

Soient M un A–module et $\mathfrak{a}$ un idéal de A. On désigne par $\mathfrak{a}M$ le sous–module de M engendré par les éléments de la forme am pour $a \in \mathfrak{a}$ et $m \in M$. Ainsi, $\mathfrak{a}M$ est l'ensemble des sommes finies d'éléments de la forme am pour $a \in \mathfrak{a}$ et $m \in M$.

Les propriétés suivantes seront souvent utilisées.

- Le module $M/\mathfrak{a}M$ est naturellement muni d'une structure de $A/\mathfrak{a}$–module (cf. ci–dessus).
- Si $\varphi\colon M \longrightarrow N$ est un morphisme de A–modules, on a $\varphi(\mathfrak{a}M) \subseteq \mathfrak{a}N$ et φ induit donc un morphisme de $A/\mathfrak{a}$–modules $M/\mathfrak{a}M \longrightarrow N/\mathfrak{a}N$.
- Si $M = M_1 \oplus M_2$, alors $M/\mathfrak{a}M = (M_1/\mathfrak{a}M_1) \oplus (M_2/\mathfrak{a}M_2)$.
- En particulier, si I est un ensemble, on a $A^{(I)}/\mathfrak{a}A^{(I)} = (A/\mathfrak{a})^{(I)}$.

Éléments et sous–module de torsion.

Soit M un A–module et soit $m \in M$. Alors l'ensemble

$$\mathrm{Ann}_A(m) := \{a \in A \mid (am = 0)\}$$

est un idéal de A appelé l'annulateur de m. Plus généralement, si E est un sous–ensemble de M, on appelle annulateur de E et on note $\mathrm{Ann}_A(E)$ l'idéal défini par

$$\mathrm{Ann}_A(E) := \bigcap_{m \in E} \mathrm{Ann}_A(m) \,.$$

On dit qu'un élément $m \in M$ est *de torsion* s'il est non nul et si $\mathrm{Ann}_A(m) \neq \{0\}$.

Exemples.

- Le $\mathbb{Z}$–module $\mathbb{Q}$ n'a aucun élément de torsion.
- Si A est intègre, le A–module $A^{(I)}$ n'a aucun élément de torsion.
- Si $\mathfrak{a}$ est un idéal non nul de A, tout élément non nul du A–module $A/\mathfrak{a}$ est de torsion.
- Plus généralement, si $\mathfrak{a}$ est un idéal non nul de A, et si M est un $A/\mathfrak{a}$–module, tout élément non nul de M vu comme A–module est de torsion.

La démonstration du lemme suivant est immédiate.

8.3. Lemme. *Soit* M *un* A*–module et soit* $x \in M$*. L'application*

$$A \longrightarrow M \quad , \quad a \mapsto ax$$

définit un isomorphisme

$$A/\mathrm{Ann}_A(x) \xrightarrow{\sim} Ax \,.$$

Si A est intègre, le sous–ensemble de M défini par

$$\mathrm{Tor}(M) := \{m \in M \mid (\mathrm{Ann}_A(m) \neq \{0\})\} \,,$$

constitué de 0 et de l'ensemble des éléments de torsion de M, est un sous–module de M.

Définition.
Si A est intègre, le sous–module $\mathrm{Tor}(M)$ est appelé sous–module de torsion de M.
On dit que M est un "module de torsion" si $M = \mathrm{Tor}(M)$.

8.4. Proposition. *On suppose A intègre.*
(1) $\mathrm{Tor}(\mathrm{Tor}(M)) = \mathrm{Tor}(M)$.
(2) On a $\mathrm{Tor}(M/\mathrm{Tor}(M)) = \{0\}$.

Démonstration de 8.4. La première assertion est triviale. Démontrons la seconde. Soit $m \in M$ tel que son image dans $M/\mathrm{Tor}(M)$ est annulée par un élément non nul $a \in A$. Ainsi, on a $am \in \mathrm{Tor}(M)$. Donc il existe un élément non nul $a' \in A$ tel que $a'am = 0$. Comme A est intègre, on voit que $a'a \neq 0$ et donc que $m \in \mathrm{Tor}(M)$. □

Exemples.
(1) Soit K un corps. Regardons son groupe multiplicatif $K^\times$ comme muni de son unique structure de $\mathbb{Z}$–module. Alors

$$\mathrm{Tor}(K^\times) = \boldsymbol{\mu}(K)\,,$$

le groupe de toutes les racines de l'unité de K.
C'est ainsi que

$$\mathrm{Tor}(\mathbb{R}^\times) = \mathrm{Tor}(\mathbb{Q}^\times) = \{\pm 1\}\ ,\ \mathrm{Tor}(\mathbb{Q}(i)) = \{\pm 1, \pm i\}\ ,\ \mathrm{Tor}(\mathbb{F}_p) = \mathbb{F}_p^\times\ ,$$

et

$$\mathrm{Tor}(\mathbb{C}^\times) = \{e^{2\pi ik/n} \mid (k, n \in \mathbb{Z})\} \simeq \mathbb{Q}/\mathbb{Z}\,.$$

(2) On a

$$\mathrm{Tor}(\mathbb{Q}) = \{0\}\ ,\ \mathrm{Tor}((\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z}) \times \{0\}$$

et $\mathbb{Q}/\mathbb{Z}$ est de torsion.

Systèmes libres, Systèmes générateurs, Modules libres.

Soit I un ensemble et soit $(x_i)_{i\in I}$ une famille indexée par I d'éléments du A–module M.
Le sous–module engendré par $(x_i)_{i\in I}$ est noté $\sum_{i\in I} Ax_i$.
On définit un morphisme de A–modules d'image $\sum_{i\in I} Ax_i$ par la formule

$$\varphi\colon A^{(I)} \longrightarrow M\ ,\ (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i x_i\,.$$

Définition. On dit que le système $(x_i)_{i\in I}$ est respectivement libre, générateur, une base, si et seulement si le morphisme φ est respectivement injectif, surjectif, un isomorphisme.

(!) **Attention** (!)
Un singleton (x) (famille à un seul élément) est libre si et seulement si $\mathrm{Ann}_A(x) = \{0\}$.
Si $(x_i)_{i\in I}$ est libre, alors chaque sous–famille $(x_i)_{i\in J}$ $(J \subset I)$ est libre, et on a

$$\sum_{i\in I} Ax_i = \bigoplus_{i\in I} Ax_i\,.$$

Si $(x_i)_{i\in I}$ est une base de M, on dit alors que M est libre de base $(x_i)_{i\in I}$.
(!) **Attention** (!)
On peut avoir

$$M = \bigoplus_{i\in I} Ax_i$$

sans que $(x_i)_{i\in I}$ soit une base de M.

Une propriété des modules libres.

8.5. Lemme. *Soit L un module libre de base $(x_i)_{i\in I}$. Pour tout A–module M, l'application*

$$\varphi \mapsto \varphi_I \quad \text{où} \quad \varphi_I : i \mapsto \varphi(x_i)$$

de l'ensemble $\mathrm{Hom}_A(L,M)$ *des morphismes de L dans M, vers l'ensemble* $\mathrm{Fonc}(I,M)$ *des fonctions de I dans M, est une bijection.*

Démonstration de 8.5. C'est évident. □

8.6. Proposition. *Soit L un A–module libre. Soient M un A–module et $\varphi\colon M \twoheadrightarrow L$ un morphisme surjectif.*

(1) Il existe un morphisme $\psi\colon L \longrightarrow M$ tel que $\varphi\cdot\psi = \mathrm{Id}_L$.

(2) ψ induit un isomorphisme de L sur son image, et on a

$$M = \ker(\varphi) \oplus \psi(L)\,.$$

Démonstration de 8.6.

(1) Soit $(x_i)_{i\in I}$ une base de L. Pour tout $i \in I$, soit m_i un élément de M tel que $\varphi(m_i) = x_i$. On définit alors ψ (grâce au lemme 8.5) par la formule $\psi(x_i) := m_i$.

(2) Il est clair que ψ est injectif. Pour $m \in M$, on a $m = \psi(\varphi(m)) + (m - \psi(\varphi(m)))$. Comme $m - \psi(\varphi(m)) \in \ker(\psi)$, ceci prouve que

$$M = \ker(\varphi) + \psi(L)\,.$$

La somme est directe puisque $\ker(\varphi) \cap \psi(L) = \{0\}$. □

Modules de type fini.

On dit que M est de type fini s'il admet un système générateur fini. En d'autres termes, M est de type fini s'il existe un entier naturel n et un morphisme surjectif

$$A^n \twoheadrightarrow M\,.$$

Exemples.

1. $\mathbb{Q}$ n'est par un $\mathbb{Z}$–module de type fini.

   En effet, soit $N := \sum_{1\le i\le n} \mathbb{Z}(a_i/b_i)$ un sous–module de type fini de $\mathbb{Q}$. Posons $k := b_1 b_2 \cdots b_n$. On voit que $kN \subset \mathbb{Z}$. Or il existe un nombre premier p qui ne divise pas k, ce qui implique que $1/p \notin N$.

2. Si V est un espace vectoriel sur K de dimension finie et si φ est un endomorphisme de V, le $K[X]$–module V_φ est de type fini.

8.7. Théorème. *Soit M un A–module libre admettant une base de cardinal m.*

(1) Tout système générateur de M a au moins m éléments, et tout système générateur de M de cardinal m est une base.

(2) Toute base de M a pour cardinal m.

Démonstration de 8.7. Elle résulte du lemme suivant.

8.8. Lemme. *Soit M un A–module libre de base $(e_i)_{1\le i\le m}$. Soit $(f_j)_{1\le j\le n}$ un système générateur de M. Alors $m \le n$.*

Démonstration de 8.8. Notons P et Q les matrices à coefficients dans A définies par les égalités

$$\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} = P \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} = Q \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}\,.$$

On en déduit

$$\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} = PQ \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} \quad \text{et donc} \quad PQ = \mathrm{Id}_m \,.$$

Supposons $m \geq n$. Nous allons démontrer que $m = n$, ce qui établira le lemme 8.8.

La matrice P est une matrice à m lignes et n colonnes. Complétons–la en une matrice carrée $m \times m$, notée $\widetilde{P}$, en la faisant précéder de $m - n$ colonnes nulles. De même, complétons la matrice Q en une matrice carrée $m \times m$, notée $\widetilde{Q}$, en la faisant précéder de $m - n$ lignes nulles.

On voit que

$$\widetilde{P}\widetilde{Q} = \mathrm{Id}_m \,.$$

On sait qu'alors on a

$$\widetilde{Q}\widetilde{P} = \mathrm{Id}_m \,,$$

ce qui prouve que $m = n$. □

Rappelons pourquoi si P et Q sont deux matrices carrées $m \times m$ telles que $PQ = \mathrm{Id}_m$, alors $QP = \mathrm{Id}_m$. Si $PQ = \mathrm{Id}_m$, on voit en effet que $\det(P)$ est inversible. Comme ${}^t\mathrm{C}om(P)P = P\,{}^t\mathrm{C}om(P) = \det(P)\mathrm{Id}_m$, on voit en particulier que $(1/\det(P))\,{}^t\mathrm{C}om(P)P = \mathrm{Id}_m$. En multipliant à gauche les deux membres de l'égalité $PQ = \mathrm{Id}_m$ par $(1/\det(P))\,{}^t\mathrm{C}om(P)$, on en déduit $Q = (1/\det(P))\,{}^t\mathrm{C}om(P)$, puis $QP = \mathrm{Id}_m$.

□

Définition. Si un A–module M a une base de cardinal fini, le cardinal commun à toutes les bases de M est appelé le *rang* de M.

Remarquons que pour qu'un A–module M soit libre de rang m, il faut et il suffit qu'il soit isomorphe à A^m.

Ⓘ **Attention** Ⓘ

- Un système générateur minimal d'un module libre n'est pas nécessairement une base (c'est ainsi que le système à deux éléments $\{2, 3\}$ est un système générateur minimal de $\mathbb{Z}$ mais n'en est pas une base).
- Un système libre maximal d'un module libre n'est pas nécessairement une base (c'est ainsi que le système à un élément $\{2\}$ est un système libre de $\mathbb{Z}$ mais n'en est pas une base).
- Un système libre de cardinal m d'un module libre de rang m n'est pas nécessairement une base (c'est ainsi que le système à un élément $\{2\}$ est un système libre de $\mathbb{Z}$ mais n'en est pas une base).

Rang : une autre démonstration.

Pour démontrer que deux bases finies d'un module M ont même cardinal, il suffit de démontrer que si A^m est isomorphe à A^n, alors $m = n$.

Supposons donc $A^m \simeq A^n$. Soit $\mathfrak{m}$ un idéal maximal de A. On a alors

$$A^m/\mathfrak{m}A^m \simeq A^n/\mathfrak{m}A^n \quad \text{donc} \quad (A/\mathfrak{m})^m \simeq (A/\mathfrak{m})^n \,.$$

Comme $A/\mathfrak{m}$ est un corps, on en déduit $m = n$.

Remarque. Un module libre M ne contient aucun élément de torsion : si M est libre et si $x \in M$, $x \neq 0$, alors $\mathrm{Ann}_A(x) = \{0\}$.

Modules monogènes.

Définition. Un A–module M est dit monogène (ou cyclique) s'il admet un système générateur à 1 élément.

8.9. Lemme. *Soit M un A–module monogène. Alors M est isomorphe à $A/\mathrm{Ann}_A(M)$. Réciproquement, si $\mathfrak{a}$ est un idéal de A, le module $A/\mathfrak{a}$ est monogène et engendré par n'importe quel élément inversible de l'anneau $A/\mathfrak{a}$.*

Démonstration de 8.9. Le lemme 8.9 résulte immédiatement du lemme 8.3. □

Le dual d'un A–module.

Soit M un A–module. Le dual de M est le A–module noté M^* et défini par

$$M^* := \mathrm{Hom}_A(M, A) \quad \text{avec} \quad (a\varphi)(m) := \varphi(am) = a\varphi(m) \text{ pour } a \in A\,,\ m \in M\,,\ \varphi \in M^*\,.$$

Si $f\colon M \longrightarrow N$ est un morphisme de A–module, le dual (ou transposé) f^* de f est le morphisme $f^*\colon N^* \longrightarrow M^*$ défini par

$$f^*(\varphi) := \varphi \cdot f \quad \text{pour tous } \varphi \in N^*\,.$$

Ⓘ **Attention** Ⓘ

- Si A est intègre, on a $\mathrm{Tor}(M^*) = \{0\}$.
- Si M est annulé par un idéal $\mathfrak{a}$ de A (*i.e.*, si M est en fait un $A/\mathfrak{a}$–module), alors il en est de même de M^*. Si de plus A est intègre et $\mathfrak{a}$ non nul, on a alors $M^* = \{0\}$. C'est ainsi que $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = \{0\}$.

Sur le dual d'un module libre.

8.10. Proposition.
(1) Si M est libre et de rang m, il en est de même de M^*.
(2) Si M est de type fini à m générateurs, M^* est isomorphe à un sous–module de A^m.

Démonstration de 8.10.
(1) Il est immédiat de vérifier que si M est libre de base $(e_i)_{1\leq i\leq m}$, alors le système $(e_i^*)_{1\leq i\leq m}$ défini par

$$e_i^*(e_j) := \delta_{i,j}$$

est une base de M^* (appelée la base duale de la base $(e_i)_{1\leq i\leq m}$).
(2) Dire que M est de type fini à m générateurs est dire qu'il existe un morphisme surjectif $\pi\colon A^m \twoheadrightarrow M$. Le morphisme transposé $\pi^*\colon M^* \longrightarrow (A^m)^*$ est alors injectif, puisque $\pi^*(\varphi) = 0$ si et seulement si $\varphi \cdot \pi = 0$, *i.e.*, si et seulement si $\varphi = 0$. □

Pour tout $x \in M$, l'ensemble

$$M^*(x) := \{\varphi(x) \mid (\varphi \in M^*)\}$$

est un idéal de A.

8.11. Lemme. *Soit M un A–module libre de base $(e_i)_{1\leq i\leq m}$. Soit $x = a_1e_1 + a_2e_2 + \cdots + a_me_m$ un élément de M. Alors on a*

$$M^*(x) = Aa_1 + Aa_2 + \cdots + Aa_m\,.$$

Démonstration de 8.11. Soit $(e_i^*)_{1\leq i\leq m}$ la base duale de $(e_i)_{1\leq i\leq m}$. Puisque $M^*(x)$ est engendré par $(e_i^*(x))_{1\leq i\leq m}$, et puisque $e_i^*(x) = a_i$, le lemme est immédiat. □

8.12. Proposition. *Supposons A intègre. Soit M un A–module libre de base $(e_i)_{1\leq i\leq m}$ et soit $x = a_1e_1 + a_2e_2 + \cdots + a_me_m$ un élément non nul de M. Les propriétés suivantes sont équivalentes.*

(i) $M^*(x) = A$.
(ii) $\sum_{i=1}^{i=m} Aa_i = A$.
(iii) *Il existe* $\varphi \in M^*$ *tel que* $\varphi(x) = 1$.
(iv) *Il existe un sous–module* M_1 *de* M *tel que* $M = Ax \oplus M_1$.

Démonstration de 8.12.

(i)$\Leftrightarrow$(ii) : résulte du lemme 8.11.

(ii)$\Longrightarrow$(iii) : Si (ii) est vérifié, il existe $u_1, u_2, \ldots, u_m \in A$ tels que $u_1a_1+u_2a_2+\cdots+u_ma_m = 1$. Posant $\varphi := u_1e_1^* + u_2e_2^* + \cdots + u_me_m^*$, on voit alors que $\varphi(x) = 1$.

(iii)$\Longrightarrow$(iv) : Soit $M_1 := \ker(\varphi)$. Puisque $\varphi(x) = 1$, on a, pour tout $y \in M$:

$$y = \varphi(y)x + (y - \varphi(y)x$$

et on constate que $\varphi(y)x \in Ax$ et $(y-\varphi(y)x \in M_1$. D'autre part, il est clair que $Ax \cap M_1 = \{0\}$.

(iv)$\Longrightarrow$(i) : Comme x est sans torsion (puisque M est libre et A intègre), l'application

$$A \longrightarrow Ax\ ,\ a \mapsto ax$$

est un isomorphisme. Son inverse est une forme linéaire sur Ax qui envoie x sur 1. En la composant avec le morphisme défini par la composition

$$M \twoheadrightarrow M/M_1 \xrightarrow{\sim} Ax\,,$$

on obtient une forme linéaire sur M qui prend la valeur 1 sur x. Ainsi, l'idéal $M^*(x)$ contient 1, donc est égal à A. □

La proposition suivante est immédiate à partir du lemme 8.11.

8.13. Proposition.

Soit M un A–module libre de base $(e_i)_{1\leq i\leq m}$ et soit $x = a_1e_1+a_2e_2+\cdots+a_me_m$ un élément de M. Soit $d \in A$. Les propriétés suivantes sont équivalentes.

(i) $M^*(x) \subseteq Ad$.
(ii) $\sum_{i=1}^{i=m} Aa_i \subseteq Ad$.
(iii) *Il existe* $y \in M$ *tel que* $x = dy$.

En particulier, on a

$$M^*(x) = Ad \quad \Leftrightarrow \quad \sum_{i=1}^{i=m} Aa_i = Ad\,.$$

9. Modules de type fini sur un anneau principal

Soit A un anneau principal.

Nous allons démontrer la série de résultats suivant.

9.1. Théorème.

(1) Tout sous–module d'un A–module libre de rang fini m est libre de rang $\leq m$.
(2) Tout sous–module d'un A–module de type fini est de type fini.
(3) Tout A–module de type fini sans torsion est libre.

Décomposition en somme directe de modules monogènes.

Nous allons démontrer que tout A–module de type fini M est somme directe d'un nombre fini de sous–modules monogènes :

$$M = \bigoplus_{i=1}^{i=m} Ax_i \,.$$

Ceci résultera d'une série de propriétés plus précises.

9.2. Proposition. *Tout A–module de type fini M est somme directe de son module de torsion $\mathrm{Tor}(M)$ et d'un sous–module libre.*

Décompositions remarquables d'un module de torsion et de type fini.

9.3. Théorème (Composantes p–primaires). *Pour tout A–module M de torsion et de type fini, et pour tout élément irréductible p de A, soit M_p la composante p–primaire de M définie par*

$$M_p := \{x \in M \mid (\exists k \in \mathbb{N})(\mathrm{Ann}_A(x) = Ap^k)\} \,.$$

On a alors

$$M = \bigoplus_{m} M_p \,.$$

9.4. Théorème (Décomposition de Jordan).

(1) Un A–module de type fini et de torsion M est indécomposable (i.e., n'est pas somme directe de deux sous–modules non triviaux) si et seulement si il est monogène et d'annulateur de la forme Ap^n où $p \in \mathrm{Irr}(A)$.

(2) Tout A–module de type fini et de torsion M est somme directe d'un nombre fini de sous–modules indécomposables :

$$M = \bigoplus_{i=1}^{i=m} Ax_i$$

(où, pour chaque i $(1 \leq i \leq m)$ il existe un élément irréductible p_i de A et un entier naturel $n_i \geq 1$ tel que l'application $A \twoheadrightarrow Ax_i$, $a \mapsto ax_i$ induit un isomorphisme $A/(p_i^{n_i}) \xrightarrow{\sim} Ax_i$).

Une autre décomposition en somme directe de sous–modules monogènes (non nécessairement indécomposables) est donnée par le résultat suivant.

9.5. Théorème (invariants de similitude). *Soit M un A–module de type fini et de torsion. Il existe une unique (à association près) famille d'éléments de A, notée $a_1, a_2, \ldots, a_m$ telle que*

(a) *a_1 est non inversible, et $a_1 \mid a_2 \mid \cdots \mid a_m$,*
(b) *il existe une famille $x_1, x_2, \ldots, x_m$ d'éléments de M telle que*

- *pour tout i, on a $\mathrm{Ann}_A(x_i) = Aa_i$,*
- *$M = \bigoplus_{i=1}^{i=m} Ax_i$.*

9.6. Corollaire. *Soit M un A–module de type fini et de torsion, d'annulateur $\mathrm{Ann}_A(M) = Aa$. Il existe un élément $x \in M$ d'annulateur Aa, et un sous–module M_1 de M tels que $M = Ax \oplus M_1$.*

"Bases adaptées".

L'ensemble des propriétés des modules de type fini énoncées ci–dessus résulte du théorème suivant, appelé parfois "théorème de la base adaptée".

9.7. Théorème fondamental. *Soit M un A–module libre de rang m et soit N un sous–module de M. Il existe une unique (à association près) famille $a_1, a_2, \ldots, a_m$ d'éléments de A telle que*

(a) $a_1 \mid a_2 \mid \cdots \mid a_m$,

(b) *il existe une base $e_1, e_2, \ldots, e_m$ de M telle que la famille $(a_i e_i \mid (a_i \neq 0))$ est une base de N.*

Définition. Avec les notations du théorème précédent, les éléments $a_1, a_2, \ldots, a_m$ s'appellent les facteurs invariants de N dans M.

Démonstrations.

Démonstration du théorème 9.1.

(1) Nous devons démontrer que tout sous–module M du A–module libre A^m est libre et de rang $\leq m$. Nous le démontrons par récurrence sur m.

• Le cas $m = 1$ exprime précisément le fait que A est principal, puisque les sous–modules de A sont ses idéaux.

• Supposons maintenant la propriété démontrée pour le rang $m - 1$.

Soit

$$\pi \colon A^m \twoheadrightarrow A \quad , \quad (a_1, a_2, \ldots, a_m) \mapsto a_m$$

la projection sur le dernier facteur, dont le noyau est

$$\ker(\pi) = \{((a_1, a_2, \ldots, 0)\} \simeq A^{m-1} .$$

La restriction de π au sous–module M de A^m a pour image $\pi(M)$, sous–module de A (donc libre de rang ≤ 1), et pour noyau $\ker(\pi) \cap M$, isomorphe à un sous–module de A^{m-1} (libre de rang $\leq m - 1$ par hypothèse de récurrence). D'après la proposition 8.6, on a

$$M \xrightarrow{\sim} \pi(M) \oplus (\ker(\pi) \cap M) ,$$

donc M est libre et de rang $\leq m$.

(2) Si M est de type fini, il existe un entier naturel m et un morphisme surjectif $\pi \colon A^m \twoheadrightarrow M$. Si N est un sous–module de M, son image réciproque $\pi^{-1}(N)$ est un sous–module de A^m, donc est libre de rang au plus m d'après ce qui précède. Comme π induit un morphisme surjectif $\pi^{-1}(N) \twoheadrightarrow N$, on voit que N est de type fini (et engendré par un système d'au plus m éléments).

(3) Soit M un A–module de type fini, engendré par $(e_1, e_2, \ldots, e_n)$. Quitte à renuméroter les éléments $e_1, e_2, \ldots, e_n$, on peut supposer (ce que nous faisons dorénavant) que $(e_1, e_2, \ldots, e_m)$ $(m \leq n)$ en est un sous–système libre maximal. Soit M' le sous–module de M engendré par $(e_1, e_2, \ldots, e_m)$. Le sous–module M' est libre et de base $(e_1, e_2, \ldots, e_m)$.

Puisque $(e_1, e_2, \ldots, e_m)$ $(m \leq n)$ est un sous–système libre maximal, on voit que pour tout i $(1 \leq i \leq n)$, il existe $a_i \neq 0$ tel que $a_i e_i \in M'$. Posons $a := a_1 a_2 \cdots a_n$. On voit alors que $a \neq 0$ (puisque A est intègre) et que $aM \subset M'$. Il s'ensuit que aM est libre.

Or l'application

$$M \twoheadrightarrow aM \quad , \quad x \mapsto ax$$

est un isomorphisme puisque M est sans torsion. Donc M est libre. □

Ⓘ **Attention** Ⓘ

Soit A un anneau intègre. Tout système d'éléments de A de cardinal au moins 2 est lié.

Donc un sous–module (*i.e.*, un idéal) de A est libre si et seulement si il est principal.

Ⓘ **Attention** Ⓘ

- Le $\mathbb{Z}$–module (*i.e.*, groupe abélien) $\mathbb{Q}$ est sans torsion.
- Le $\mathbb{Z}$–module $\mathbb{Q}$ n'est pas libre. En effet, tout système de cardinal au moins 2 d'éléments de $\mathbb{Q}$ est lié, et si $\mathbb{Q}$ était libre il serait de rang 1. Or on sait que $\mathbb{Q}$ n'est pas de type fini.

Démonstration de la proposition 9.2. Puisque $M/\mathrm{Tor}(M)$ est sans torsion (8.4), la proposition 9.2 est une application immédiate du lemme 8.6 et de la seconde assertion du théorème 9.1. □

Ⓘ **Attention** Ⓘ

La décomposition d'un module de type fini M sous la forme

$$M = \mathrm{Tor}(M) \oplus L$$

(où L est libre) n'est pas unique. Considérons en effet la somme directe

$$M := \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\,.$$

On vérifie que

$$\mathrm{Tor}(M) = \mathbb{Z}/2\mathbb{Z}$$

(identifié au sous–module $\{(0,a) \mid (a \in \mathbb{Z}/2\mathbb{Z})\}$ de M) et que le sous–module $\mathbb{Z}$ (identifié au sous–module $\{(n,0) \mid (n \in \mathbb{Z})\}$ de M) est libre. Posons

$$L := \{(n,\overline{n} \mid (n \in \mathbb{Z})\}\,,$$

où on désigne par $\overline{n}$ l'image de n modulo 2. On a aussi

$$M = \mathrm{Tor}(M) \oplus L\,.$$

Démonstration du théorème 9.7.

1. **Existence.**

a. Toute famille d'idéaux de A a un élément maximal.

En effet, pour tout idéal $\mathfrak{a} = Aa$ de A, notons $\nu(\mathfrak{a})$ le nombre de diviseurs irréductibles d'un générateur a de $\mathfrak{a}$. Alors dans toute famille d'idéaux de A, un élément $\mathfrak{a}$ tel que $\nu(\mathfrak{a})$ est minimal est maximal dans la famille.

b. Soit $f_1 \in N$ tel que l'idéal $M^*(f_1)$ soit maximal dans la famille des idéaux de la forme $M^*(y)$ pour $y \in N$. Choisissons $a_1 \in A$ (unique à association près) et $\varepsilon_1 \in M^*$ tels que

$$M^*(f_1) = Aa_1 \quad \text{et} \quad a_1 = \varepsilon_1(f_1)\,.$$

On sait (cf. proposition 8.13) qu'il existe un élément $e_1 \in M$ tel que $f_1 = a_1 e_1$. Notons que $\varepsilon_1(e_1) = 1$, donc que

$$M = Ae_1 \oplus \ker(\varepsilon_1)\,.$$

c. Démontrons que l'idéal

$$\varepsilon_1(N) := \{\varepsilon_1(y) \mid (y \in N)\}$$

est égal à Aa_1.

En effet, soit $y \in N$. Notons $d := \varepsilon_1(y) \wedge \varepsilon_1(f_1)$. Il existe $u_1, v \in A$ tels que $d = u_1\varepsilon_1(f_1) + v\varepsilon_1(y)$, d'où $d = \varepsilon_1(u_1 f_1 + vy)$. Ainsi on voit que

$$M^*(f_1) \subseteq Ad \subseteq M^*(u_1 f_1 + vy)$$

et par maximalité de $M^*(f_1)$ on en déduit $M^*(f_1) = Ad$ donc que $\varepsilon_1(y)$ est multiple de $\varepsilon_1(f_1)$, ce qui établit bien que $\varepsilon_1(N) = Aa_1$.

On définit donc une forme linéaire φ_1 sur N par la formule

$$\varepsilon_1(y) = a_1\varphi_1(y) \quad (\forall y \in N)\,.$$

Notons que $\varphi_1(f_1) = 1$ et donc que

$$N = Af_1 \oplus \ker(\varphi_1)\,.$$

Comme il est clair que

$$\ker(\varphi_1) = N \cap \ker(\varepsilon_1)\,,$$

on voit qu'on a les deux décompositions suivantes

$$\begin{cases} M = & Ae_1 & \oplus & \ker(\varepsilon_1) \\ N = & Aa_1e_1 & \oplus & (\ker(\varepsilon_1) \cap N) \end{cases}$$

d. On démontre l'existence par récurrence sur m. L'assertion est vraie par définition d'un anneau principal si $m = 1$. En supposant l'assertion vraie pour le rang $m-1$, on voit d'après ce qui précède qu'il existe des éléments $a_2, \ldots, a_m$ de A et une base $(e_2, \ldots, e_m)$ de $\ker(\varepsilon_1)$ tels que

$$a_2 \mid a_3 \mid \cdots \mid a_m \quad \text{et} \quad \ker(\varepsilon_1) \cap N = Aa_2e_2 \oplus \cdots \oplus Aa_me_m\,.$$

Il reste à vérifier que $a_1 \mid a_2$. Or on a

$$M^*(a_1e_1 + a_2e_2) = Aa_1 + Aa_2 \supseteq Aa_1\,,$$

d'où il résulte, par maximalité de Aa_1, que $Aa_2 \subseteq Aa_1$, donc $a_1 \mid a_2$. □

2. **Unicité.**

• Soit $n \leq m$ l'entier tel que $a_i \neq 0$ si et seulement si $i \leq n$. On voit alors que n est le rang de N.

• Soit $r \leq n$ l'entier tel que a_i est inversible si et seulement si $i \leq r$. On voit alors que

$$M/N \simeq A/Aa_{r+1} \oplus \ldots A/Aa_n \oplus A^{m-n}\,.$$

Il est facile de vérifier que

$$\mathrm{Tor}(M/N) \simeq A/Aa_{r+1} \oplus \ldots A/Aa_n\,.$$

Pour démontrer l'unicité d'une famille telle que $a_1, a_2, \ldots, a_m$, on se ramène donc à démontrer que si T est un A–module de torsion tel que

$$T \simeq A/Aa_1 \oplus \cdots A/Aa_m \simeq A/Ab_1 \oplus \cdots A/Ab_n$$

avec a_1 et b_1 non inversibles, et

$$a_1 \mid a_2 \mid \cdots \mid a_m \quad \text{et} \quad b_1 \mid b_2 \mid \cdots \mid b_n\,,$$

(et a_m et b_n non nuls puisque T est de torsion) alors $m = n$ et (à association près) $a_i = b_i$ pour tout i $(1 \leq i \leq m)$.

Remarquons que

$$\mathrm{Ann}_A(T) = Aa_m = Ab_n$$

donc en particulier que a_m et b_n sont associés. Raisonnons par récurrence sur le nombre $\nu(\mathrm{Ann}_A(T))$ de facteurs irréductibles d'une décomposition de a_m.

L'assertion est évidente si $\nu(\mathrm{Ann}_A(T)) = 0$. Supposons donc $\nu(\mathrm{Ann}_A(T)) \geq 1$, et l'assertion vérifiée pour tout module T' tel que $\nu(\mathrm{Ann}_A(T')) < \nu(\mathrm{Ann}_A(T))$.

La démonstration du lemme suivant est laissée au lecteur (resp. à la lectrice).

9.8. Lemme. *Soient $a \in A$ et $p \in \mathrm{Irr}(A)$. On a*

$$p(A/Aa) \simeq \begin{cases} A/Aa & si\ p \nmid a\,, \\ A/Aa' & si\ a = pa'\,, \end{cases} \quad et \quad (A/Aa)/p(A/Aa) \simeq \begin{cases} \{0\} & si\ p \nmid a\,, \\ A/Ap & si\ p \mid a\,. \end{cases}$$

Soit alors p un diviseur irréductible de a_1. D'après le lemme précédent, on voit que T/pT est un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$

- d'une part de dimension m,
- d'autre part de dimension égale au nombre d'indices j tel que $p \mid b_j$.

Il en résulte que $m \leq n$.

Un raisonnement analogue à partir d'un diviseur irréductible de b_1 montre que $n \leq m$. On en déduit que $m = n$ et que a_1 et b_1 ont les mêmes diviseurs irréductibles.

Soit p un tel diviseur irréductible. Pour tous i $(1 \leq i \leq m)$ et j $(1 \leq j \leq n)$, posons $a_i = pa'_i$ et $b_j = pb'_j$. On voit (grâce au lemme 9.8 ci–dessus) que

$$pT \simeq A/Aa'_1 \oplus A/Aa'_2 \oplus \cdots \oplus A/Aa'_m \simeq A/Ab'_1 \oplus A/Ab'_2 \oplus \cdots \oplus A/Ab'_n\,.$$

L'hypothèse de récurrence montre alors que $m = n$ et que, à association près, $a'_i = b'_i$ d'où $a_i = b_i$ pour tout i $(1 \leq i \leq m)$. □

Exemple. Considérons le $\mathbb{Z}$–module libre $M := \mathbb{Z}[i]$, de base canonique $\{1, i\}$, et son sous–module N engendré par $\{1+i, 1-i\}$. Alors M a aussi pour base $\{1+i, i\}$ et N a pour base $\{1+i, 2i\}$. En particulier les facteurs invariants de N dans M sont $\{1, 2\}$.

Démonstration du théorème 9.5.

1. *Existence.* Soit M un A–module de type fini et de torsion. Il existe un entier m et un morphisme surjectif

$$\pi\colon A^m \twoheadrightarrow M\,,\ \text{d'où}\ M \simeq A^m/\ker(\pi)\,.$$

Si $a_1, a_2, \ldots, a_m$ sont les facteurs invariants de $\ker(\pi)$ dans A^m, on voit donc que

$$M \simeq A/Aa_{r+1} \oplus \ldots A/Aa_m$$

où $r \leq m$ désigne l'entier tel que a_i est inversible si et seulement si $i \leq r$.

2. *Unicité.* Elle a été démontrée dans le cours de la démonstration d'unicité dans le théorème 9.7 ci–dessus. □

Démonstration du théorème 9.4.

1. *Existence.* Si $a \in A$, rappelons que l'on note $a = \prod_p p^{v_p(a)}$ "la" décomposition de a en facteurs irréductibles (où l'on convient que les différents p ne sont pas associés). Le lemme chinois montre alors que

$$A/Aa \simeq \bigoplus_p \left(A/Ap^{v_p(a)}\right)\,.$$

L'existence d'une décomposition de Jordan de tout module de type fini résulte alors de la décomposition donnée par le théorème 9.5.

Ceci démontre aussi que les modules indécomposables sont nécessairement de la forme A/Ap^α.

Réciproquement, démontrons qu'un module isomorphe à A/Ap^k est indécomposable. Supposons $A/Ap^k = M_1 \oplus M_2$. Comme $\mathrm{Ann}_A(M_i) \subseteq Ap^k$ pour $i = 1, 2$, on voit que les invariants de similitude de M_i $(i = 1, 2)$ sont de la forme p^l pour $l \leq k$. En réunissant les invariants de similitude de M_1 et M_2, et en ordonnant leurs exposants, on voit qu'on obtient des invariants

de similitude pour A/Ap^k. L'unicité des invariants de similitude permet de conclure que M_1 ou M_2 est nul.

2. *Unicité.* Supposons donné un isomorphisme

$$M \xrightarrow{\sim} \bigoplus_p \bigoplus_{i=1}^{i=m_p} A/Ap^{k_{p,i}}\,,$$

où, pour tout p, on a

$$k_{p,1} \leq k_{p,2} \leq \cdots \leq k_{p,m_p}\,.$$

Soit $m := \max\{m_p \mid (p \in \mathrm{Irr}(A))\}$. Quitte à rajouter un certain nombre de zéros en tête de la liste des entiers $k_{p,i}$, et à les renuméroter, on peut supposer que, pour tout p, on a $m_p = m$, avec

$$k_{p,1} \leq k_{p,2} \leq \cdots \leq k_{p,m}\,.$$

Pour tout i $(1 \leq i \leq m)$, on pose alors

$$a_i := \prod_p p^{k_{p,i}}\,.$$

Il est clair que

$$a_1 \mid a_2 \mid \cdots \mid a_m\,.$$

D'autre part, grâce au lemme chinois, on a

$$\bigoplus_p A/Ap^{k_{p,i}} \simeq A/Aa_i\,,$$

d'où on déduit

$$M \simeq \bigoplus_{i=1}^{i=m} A/Aa_i\,.$$

Ainsi, les éléments $a_1, a_2, \ldots, a_m$ sont les invariants de similitude de M. L'unicité des invariants de similitude montre alors que la suite ordonnée des entiers $k_{p,i}$ est uniquement déterminée par M. □

Exemple.

Soit

$$M = (\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z})^4 \oplus (\mathbb{Z}/5\mathbb{Z}) \oplus (\mathbb{Z}/5^2\mathbb{Z})\,.$$

Avec les notations de la démonstration précédente, on voit que $m = 4$, d'où la liste des entiers $k_{p,i}$:

$$\begin{array}{lllll} p=2: & k_{2,1}=0, & k_{2,2}=1, & k_{2,3}=1, & k_{2,4}=1, \\ p=3: & k_{3,1}=1, & k_{3,2}=1, & k_{3,3}=1, & k_{3,4}=1, \\ p=5: & k_{5,1}=0, & k_{5,2}=0, & k_{5,3}=1, & k_{5,4}=2, \end{array}$$

d'où

$$a_1 = 3\,,\ a_2 = 6\,,\ a_3 = 30\,,\ a_4 = 150\,,$$

et

$$M \simeq (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/30\mathbb{Z}) \oplus (\mathbb{Z}/150\mathbb{Z})\,.$$

Démonstration du théorème 9.3. Le théorème 9.3 résulte immédiatement (la démonstration en est laissée à la lectrice – resp. le lecteur) du théorème sur la décomposition de Jordan.

Nous en donnons ici une démonstration directe. Le lemme suivant peut être vu comme une généralisation aux modules du lemme chinois pour les anneaux principaux.

9.9. Lemme. *Soit M un A–module de type fini et de torsion, annulé par un produit ab où a et b sont premiers entre eux. Posons*

$$M_a := \{x \in M \mid (ax = 0)\} \quad et \quad M_b := \{x \in M \mid (bx = 0)\}.$$

On a

(1) $M_a = bM$ *et* $M_b = aM$,
(2) $M = M_a \oplus M_b$.

Démonstration du lemme 9.9. D'après la relation de Bézout, il existe $u, v \in A$ tels que $ua+vb = 1$.

Il est clair que $bM \subseteq M_a$ et $aM \subseteq M_b$. Démontrons que réciproquement $M_a \subseteq bM$.

Pour $x \in M$, on a $x = uax + vbx$, donc si $x \in M_a$ on a $x = bvx \in bM$. Ainsi $M_a = bM$ et $M_b = aM$.

La même relation de Bézout montre que $M = aM + bM$ et que $M_a \cap M_b = \{0\}$. □

L'application répétée du lemme 9.9 démontre le théorème 9.3. □

Troisème partie : Introduction aux extensions de corps

10. Éléments algébriques sur un corps

Soit L/K une extension de corps, et soit $x \in L$.

Rappelons (cf. première partie) les deux séries (équivalentes) d'équivalences définissant les notions d'élément algébrique et transcendant.

10.1. *L'élément x est dit algébrique sur K si les assertions équivalentes suivantes sont vérifiées.*

(i) *Il existe un polynôme $P(X) \in K[X]$, $P(X) \neq 0$, tel que $P(x) = 0$.*
(ii) *On a $K[x] = K(x)$.*
(iii) *$[K(x) : K]$ est fini.*
(iv) *$[K[x] : K]$ est fini.*

L'élément x est dit transcendant sur K si les assertions équivalentes suivantes sont vérifiées.

(i) *Il n'existe aucun polynôme $P(X) \in K[X]$, $P(X) \neq 0$, tel que $P(x) = 0$.*
(ii) *On a $K[x] \neq K(x)$.*
(iii) *$[K(x) : K]$ est infini.*
(iv) *$[K[x] : K]$ est infini.*

On en déduit le théorème suivant.

10.2. Théorème. *Notons L_{alg} l'ensemble des éléments de L qui sont algébriques sur K.*

(1) L_{alg} est un sous–corps de L.

(2) L_{alg} est "algébriquement clos dans L", i.e., les seuls éléments de L qui sont algébriques sur L_{alg} sont ceux de L.

Remarque. L'assertion (2) ci–dessus montre en particulier que si L est algébriquement clos, il en est de même de L_{alg}.

On voit ainsi que l'ensemble $\overline{\mathbb{Q}}$ des nombres complexes algébriques sur $\mathbb{Q}$ est un corps algébriquement clos strictement contenu dans $\mathbb{C}$.

Démonstration de 10.2. Elle repose sur le lemme suivant, connu sous le nom de "lemme de la base télescopique".

10.3. Lemme. *Soient $K \subseteq L \subseteq M$ trois corps emboîtés.*

(1) Soit $(l_i)_{i \in I}$ une base de L comme espace vectoriel sur K, et soit $(m_j)_{j \in J}$ une base de M comme espace vectoriel sur L. Alors $(l_i m_j)_{(i,j) \in I \times J}$ est une base de M comme espace vectoriel sur K.

(2) En particulier (en posant des conventions évidentes pour la multuplication des entiers naturels par $+\infty$), on a

$$[M : K] = [M : L][L : K] .$$

Démonstration de 10.3.

□

Démontrons maintenant le théorème 10.2.

(1) Pour démontrer que L_{alg} est un sous–corps de L, il suffit de démontrer que, si x et y sont deux éléments quelconques de L_{alg}, alors l'extension $K(x, y)$ de K qu'ils engendrent avec K est contenu dans L_{alg}.

Pour cela, il suffit de démontrer que $[K(x, y) : K]$ est fini. En effet, si z est un élément quelconque de $K(x, y)$, le lemme de la base téléscopique montre que

$$[K(x, y) : K] = [K(x, y) : K(z)][K(z) : K] ,$$

d'où il résulte que, si $[K(x, y) : K]$ est fini, $[K(z) : K]$ est fini et $z \in L_{\text{alg}}$.

Or on a $[K(x,y):K] = [K(x,y):K(x)][K(x):K]$. Comme x est algébrique sur K, le degré $[K(x):K]$ est fini. Comme y est algébrique sur K, donc sur $K(x)$, le degré $[K(x,y):K(x)] = [K(x)(y):K(x)]$ est aussi fini, ce qui montre que $[K(x,y):K]$ est fini.

(2) Soit $P(X) = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ un élément de $L_{\mathrm{alg}}[X]$. Nous allons démontrer que toute racine de $P(X)$ dans L appartient en fait à L_{alg}.

Soit $\alpha \in L$ et tel que $P(\alpha) = 0$. Ainsi, α est algébrique sur le corps $K(a_1, a_2, \ldots, a_d)$ et par conséquent on a $[K(a_1, a_2, \ldots, a_d, \alpha) : K(a_1, a_2, \ldots, a_d)] < \infty$. Or chaque a_j est algébrique sur K, donc *a fortiori* algébrique sur $K(a_1, a_1, \ldots, a_{j-1})$. Comme (posant $a_{-1} := 1$)

$$[K(a_1, a_2, \ldots, a_d) : K] = \prod_{j=0}^{j=d} [K(a_1, a_2, \ldots, a_j) : K(a_1, a_2, \ldots, a_{j-1})],$$

il en résulte que $[K(a_1, a_2, \ldots, a_d) : K] < \infty$. Une autre application du lemme de la base télescopique montre alors que $[K(a_1, a_2, \ldots, a_d, \alpha) : K] < \infty$, d'où $[K(\alpha) : K] < \infty$, et $\alpha \in L_{\mathrm{alg}}$. □

11. Corps de rupture et corps des racines

11. A. Corps de rupture d'un polynôme irréductible.

Soit $P(X) \in \operatorname{Irr} K[X]$. Soit L un surcorps de K. Un *corps de rupture de $P(X)$ dans L* est un sous–corps de L de la forme $K(a)$ où a est une racine de $P(X)$ dans L.

On omettra souvent de mentionner le "corps ambiant" L en parlant simplement de "corps de rupture" de $P(X)$.

Exemples. Prenons $K := \mathbb{Q}$ et $L = \mathbb{C}$.

(1) Considérons $P(X) := X^3 - 2$. Désignons par ρ l'unique nombre réel tel que $\rho^3 = 2$, et posons $\omega := e^{2i\pi/3}$. Alors les racines de $P(X)$ dans $\mathbb{C}$ sont $\rho, \omega\rho, \omega^2\rho$.

Si a désigne l'une quelconque des trois racines de $P(X)$, on peut vérifier qu'aucune des deux autres racines ωa et $\omega^2 a$ n'appartient au corps de rupture $\mathbb{Q}(a)$, et donc $P(X)$ a *trois* corps de rupture distincts dans $\mathbb{C}$, à savoir les corps $\mathbb{Q}(\rho)$, $\mathbb{Q}(\rho\omega)$, $\mathbb{Q}(\rho\omega^2)$. La décomposition de $P(X)$ en facteurs irréductibles sur le corps de rupture $\mathbb{Q}(a)$ est

$$P(X) = (X - a)(X^2 + aX + a^2).$$

(2) Considérons maintenant $P(X) := \dfrac{X^5 - 1}{X - 1}$. Posons $\zeta := \varepsilon^{2i\pi/5}$. Alors les racines de $P(X)$ sont $\zeta, \zeta^2, \zeta^3, \zeta^4$, et comme ζ est une puissance de chacune d'entre elles, tous les corps de ruptures correspondant sont égaux. Ainsi, $P(X)$ a *un seul* corps de rupture dans $\mathbb{C}$, à savoir le corps $\mathbb{Q}(\zeta)$. Le polynôme $P(X)$ est est décomposé en facteurs du premier degré.

Remarque. Les exemples précédents montrent qu'il peut y avoir *plusieurs* corps de rupture d'un même polynôme irréductible de $K[X]$ dans une extension donnée de K.

Rappelons que, étant donné un polynôme irréductible $P(X) \in K[X]$, il existe une extension de K dans laquelle $P(X)$ admet une racine : l'injection naturelle de K dans $K[X]$ induit un morphisme (injectif) $K \hookrightarrow K[X]/(P(X))$ qui permet d'identifier le corps $K[X]/(P(X))$ à une extension de K. L'image x de X dans $K[X]/(P(X))$ par le morphisme canonique est alors une racine de $P(X)$ dans $K[X]/(P(X))$. On voit que ce dernier corps est engendré par x, *i.e.*, est égal à $K(x)$. Ainsi, c'est un corps de rupture de $P(X)$ (dans lui–même).

Si $K(a)$ est un autre corps de rupture de $P(X)$, on sait qu'il y a un isomorphisme et un seul

$$K[X]/(P(X)) \xrightarrow{\sim} K(a)$$

qui induit l'identité sur K et envoie x sur a.

En particulier, tous les corps de rupture d'un même polynôme irréductible sont isomorphes entre eux. Le résultat suivant donne un résultat plus précis.

11.1. Proposition. *Soit $P(X) \in \operatorname{Irr} K[X]$, et soit $K(a)$ un corps de rupture de $P(X)$.*

Soit $\iota\colon K \xrightarrow{\sim} \widetilde{K}$ un isomorphisme de corps, et soit $\widetilde{L}$ une extension de $\widetilde{K}$. On pose $\widetilde{P}(X) := \iota(P(X))$.

Alors l'application

$$\sigma \mapsto \sigma(a)$$

est une bijection

- *de l'ensemble des morphismes de corps $\sigma\colon K(a) \longrightarrow \widetilde{L}$ qui prolongent ι*
- *sur l'ensemble des racines de $\widetilde{P}(X)$ dans $\widetilde{L}$.*

Démonstration de 11.1. Il est clair que (avec les notations de l'énoncé de la proposition) $\sigma(a)$ est une racine de $\widetilde{P}(X)$, et que de plus l'application $\sigma \mapsto \sigma(a)$ est injective. Vérifions que cette application est surjective.

Soit b une racine de $\widetilde{P}(X)$ dans $\widetilde{L}$: nous allons construire un morphisme σ comme dans l'énoncé tel que $\sigma(a) = b$.

On sait que

- notant x l'image de X dans $K[X]/(P(X))$ (par la surjection canonique), il existe un (et un seul) isomorphisme

  $$K[X]/(P(X)) \xrightarrow{\sim} K(a) \quad , \quad x \mapsto a$$

  induisant l'identité sur K,
- notant y l'image de X dans $\widetilde{K}[X]/(\widetilde{P}(X))$ (par la surjection canonique), il existe un (et un seul) isomorphisme

  $$\widetilde{K}[X]/(\widetilde{P}(X)) \xrightarrow{\sim} \widetilde{K}(b) \quad , \quad y \mapsto b$$

  induisant l'identité sur $\widetilde{K}$,

Comme ι induit un isomorphisme

$$K[X]/(P(X)) \xrightarrow{\sim} \widetilde{K}[X]/(\widetilde{P}(X)) \quad , \quad x \mapsto y\,,$$

qui prolonge $\iota\colon K \longrightarrow \widetilde{K}$, on en déduit bien l'existence d'un isomorphisme

$$\sigma\colon K(a) \xrightarrow{\sim} \widetilde{K}(b) \quad , \quad a \mapsto b$$

qui prolonge ι. □

Définition. Si L/K est une extension de corps, on appelle *groupe de Galois de L/K* et on note $\operatorname{Gal}(L/K)$ l'ensemble des automorphismes de L qui induisent l'identité sur K.

Exemples. La proposition 11.1 montre que, si L est un corps de rupture de $P(X) \in \operatorname{Irr} K[X]$, le groupe de Galois $\operatorname{Gal}(L/K)$ a pour ordre le nombre de racines de $P(X)$ dans L. En particulier,

- $|\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$,
- $|\operatorname{Gal}(\mathbb{Q}(e^{2i\pi/5})/\mathbb{Q})| = 4$.

11. B. Corps des racines d'un polynôme.

Préliminaire : racines multiples.

Soit $P(X) \in K[X]$. Soit L une extension de K, soit $a \in L$, et soit m un entier. On dit que a est *racine avec multiplicité m de $P(X)$* si $(X-a)^m$ divise $P(X)$ (dans le corps $K(a)$) mais $X-a)^{m+1}$ ne divise pas $P(X)$.

On dit que a est *racine multiple* de $P(X)$ si a est racine de $P(X)$ avec multiplicité au moins 2. Une *racine simple* est une racine qui n'est pas racine multiple.

Le lemme suivant est bien connu.

11.2. Lemme. *Soit $P(X) \in K[X]$ et soit m un entier.*

(1) Un élément a est racine de $P(X)$ avec multiplicité m si et seulement si a est racine de $P(X)$ et racine de $P'(X)$ avec multiplicité $m-1$.

(2) $P(X)$ admet une racine multiple (dans une extension de K) si et seulement si $P(X)$ n'est pas premier avec son polynôme dérivé $P'(X)$.

Démonstration de 11.2. . Nous démontrons l'assertion (2).

Si $P(X)$ et $P'(X)$ ne sont pas premiers entre eux, ils ont un diviseur irréductible $Q(X)$ commun. Ce diviseur a une racine (dans une extension convenable), qui est une racine commune à $P(X)$ et $P'(X)$, donc racine multiple de $P(X)$.

Si $P(X)$ et $P'(X)$ sont premiers entre eux, par le critère de Bézout il existe $U(X), V(X) \in K[X]$ tels que $U(X)P(X) + V(X)P'(X) = 1$, donc $P(X)$ et $P'(X)$ ne peuvent avoir de racine commune dans une extension de K et $P(X)$ n'a pas de racine multiple. □

11.3. Proposition. *Soit $P(X) \in \operatorname{Irr} K[X]$.*

(1) Si $P(X)$ a une racine multiple, alors K est de caractéristique $p > 0$, et il existe un polynôme $P_1(X) \in K[X]$ tel que $P(X) = P_1(X^p)$.

(2) Si K est de caractéristique nulle, ou est un corps fini, $P(X)$ n'a que des racines simples.

Démonstration de 11.3.

(1) Si $P(X)$ admet une racine multiple, il n'est pas premier avec son polynôme dérivé $P'(X)$, donc il le divise. Or ce polynôme dérivé, s'il est non nul, est de degré strictement inférieur au degré de $P(X)$. Donc on a $P'(X) = 0$. Si $P(X) = a_d X^d + \cdots + a_1 X + a_0$, on a $P'(X) = da_d X^{d-1} + \cdots + a_1$, d'où on déduit que, pour tout k, on a $ka_k = 0$. Ainsi, si $a_k \neq 0$, k est multiple de p, ce qui démontre (1).

(2) Supposons que K est un corps fini de caractéritique p. Nous allons démontrer, en utilisant le lemme ci–dessous, que pour tout $P_1(X) \in K[X]$, $P_1(X^p)$ ne peut être irréductible dans $K[X]$.

11.4. Lemme.

(1) Si A est un anneau intègre de caractéristique p, l'application

$$F_A \colon A \longrightarrow A \ , \ a \mapsto a^p$$

est un endomorphisme de A.

(2) Si K est un corps fini de caractéristique p, l'endomorphisme F_K est un automorphisme.

Démonstration de 11.4.

(1) Pour démontrer que l'application F est un morphisme, il suffit de vérifier que $(a+b)^p = a^p + b^p$, *i.e.*, que pour tout $k < p$, $\binom{p}{k}$ est divisible par p. Or on a

$$k!(p-k)! \binom{p}{k} = p! \, ,$$

donc p divise $k!(p-k)!\binom{p}{k}$. Comme p est premier avec $k!$ et avec $(p-k)!$, il résulte du lemme de Gauß que p divise $\binom{p}{k}$.

(2) Pour vérifier que F est bijective, il suffit alors de vérifier que son noyau est $\{0\}$, ce qui est évident. □

Soit alors $P_1(X) \in K[X]$. Posons $P_1(X) = b_e X^e + \cdots + b_1 X + b_0$. Pour tout k, il existe $c_k \in K$ tel que $b_k = c_k^p$. Ainsi, on a $P_1(X^p) = c_e^p X^{ep} + \cdots + c_1^p X^p + c_0^p = (c_e X^e + \cdots + \cdots + c_1 X + c_0)^p$. Ainsi il existe $Q(X) \in K[X]$ tel que $P_1(X^p) = Q(X)^p$, et donc $P_1(X^p)$ ne peut être irréductible dans $K[X]$. □

Remarque. Considérons le corps $K := \mathbb{F}_p(T)$, corps des fractions rationnelles en une indéterminée T sur le corps premier $\mathbb{F}_p$: K est un corps infini de caractéristique p.

Le polynôme $P(X) := X^p - T$ est alors irréductible dans $K[X]$ (puisqu'il est irréductible dans $\mathbb{F}_p[T, X]$, car il est primitif dans $\mathbb{F}_p[X][T]$ et irréductible dans $\mathbb{F}_p(X)[T]$).

Si a est une racine de $P(X)$ (par exemple dans l'extension $K[X]/(P(X))$, on a $P(X) = (X - a)^p$.

Corps des racines d'un polynôme.

Nous supposons dorénavant que *les corps considérés sont finis ou de caractéristique zéro*, de sorte que tous les polynômes irréductibles considérés n'ont que des racines simples.

Si $P(X)$ est un polynôme quelconque à coefficients dans K, il existe toujours une extension de degré fini de$K$ dans lequel $P(X)$ est décomposé en facteurs du premier degré (on dit alors que $P(X)$ "a toutes ses racines dans L").

En effet, raisonnons par récurrence sur le degré de $P(X)$.

- Si $P(X)$ est de degré 1, on peut choisir $L := K$.
- Soit $P(X)$ de degré au moins 2. Par hypothèse de récurrence, on sait que pour tout corps M et tout polynôme $R(X) \in M[X]$ de degré $\deg R(X) < \deg P(X)$, il existe une extension de M dans lequel $R(X)$ a toutes ses racines.

  Soit $Q(X)$ un facteur irréductible de $P(X)$. On sait qu'il existe une extension $K(a)$ de K engendré par une racine a de $Q(X)$. Il existe donc $P_a(X) \in K(a)[X]$ tel que $P(X) = (X - a)P_a(X)$. Appliquant l'hypothèse de récurrence au couple $(K(a), P_a(X))$, on voit qu'il existe une extension L de $K(a)$ où $P_a(X)$ a toutes ses racines. Le corps L est alors aussi une extension de K où $P(X)$ a toutes ses racines.

Définition. Soit $P(X) \in K[X]$ et soit L une extension de K dans laquelle $P(X)$ a toutes ses racines. Le *corps des racines de $P(X)$ dans L* est l'extension de K engendrée par toutes les racines de $P(X)$ dans L.

Exemples.

- Le corps des racines de $X^3 - 2$ dans $\mathbb{C}$ est $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.
- Le corps des racines de $\dfrac{X^5 - 1}{X - 1}$ dans $\mathbb{C}$ est $\mathbb{Q}(e^{2i\pi/5})$.

Remarque. Contrairement au corps de rupture d'un polynôme irréductible, il n'y a qu'un seul corps des racines de $P(X) \in K[X]$ dans une extension donnée (et assez grande) de K.

Le résultat suivant permet en particulier de démontrer que deux corps des racines d'un même polynôme (dans des extensions différentes de K) sont toujours isomorphes.

11.5. Théorème. *Soit $P(X) \in K[X]$, et soit L le corps des racines de $P(X)$ dans une extension de K où $P(X)$ a toutes ses racines. On note* $\mathrm{Rac}(P(X), L)$ *l'ensemble de ces racines.*

Soit $\iota\colon K \xrightarrow{\sim} \widetilde{K}$ un isomorphisme de corps. On pose $\widetilde{P}(X) := \iota(P(X))$. Soit $\widetilde{M}$ une extension de $\widetilde{K}$ dans laquelle $\widetilde{P}(X)$ a toutes ses racines. On note $\mathrm{Rac}(\widetilde{P}(X), \widetilde{M})$ *l'ensemble de ces racines.*

Soit $\mathrm{Mor}_\iota(L, \widetilde{M})$ *l'ensemble des morphismes de L dans $\widetilde{M}$ qui prolongent ι.*

(1) $\mathrm{Mor}_\iota(L, \widetilde{M})$ *est de cardinal* $[L : K]$.

(2) L'application

$$\sigma \mapsto \sigma_{|\mathrm{Rac}(P(X),L)}$$

(qui à un élément $\sigma \in \mathrm{Mor}_\iota(L, \widetilde{M})$ associe sa restriction à $\mathrm{Rac}(P(X), L)$*) est une injection de* $\mathrm{Mor}_\iota(L, \widetilde{M})$ *dans l'ensemble des bijections*

$$\mathrm{Rac}(P(X), L) \xrightarrow{\sim} \mathrm{Rac}(\widetilde{P}(X), \widetilde{M}).$$

Le théorème précédent permet de démontrer le premier résultat fondamental de la théorie de Galois.

11.6. Théorème. *Soit $P(X) \in K[X]$, et soit L le corps des racines de $P(X)$ dans une extension de K où $P(X)$ a toutes ses racines. On note R l'ensemble des racines de $P(X)$ dans L.*

(1) Le groupe de Galois $\mathrm{Gal}(L/K)$ *est d'ordre* $[L : K]$.

(2) L'application $\sigma \mapsto \sigma_{|R}$ est un morphisme de groupes injectif

$$\mathrm{Gal}(L/K) \hookrightarrow \mathfrak{S}_R\,.$$

(3) Les orbites de $\mathrm{Gal}(L/K)$ *dans son action sur R sont les ensembles de racines des divers facteurs irréductibles de $P(X)$ dans $K[X]$.*

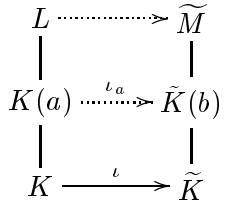
Remarque. Le groupe $\mathrm{Gal}(L/K)$ est souvent appelé *le groupe de Galois du polynôme $P(X)$.*

Si une extension de M de K dans laquelle $P(X)$ a toutes ses racines est donnée (par exemple, si $K = \mathbb{Q}$, on condidère implicitement que $\mathbb{Q}$ est plongé dans le corps des complexes $\mathbb{C}$), cette terminologie est justifiée : le polynôme $P(X)$ a *un* corps des racines bien défini (le sous–corps de M engendré par les racines de $P(X)$), et le groupe de Galois de $P(X)$ est le groupe de Galois de cette extension. Par contre, si la seule donnée de départ est celle du corps K, les corps de racines de $P(X)$ que l'on peut construire sont certes tous isomorphes entre eux, mais pas en général par un isomorphisme unique. "Le groupe de Galois de $P(X)$" n'est donc pas, à proprement parler, défini – seule est définie une classe d'isomorphismes de groupes.

Démonstration de 11.5.

Nous démontrons l'assertion (1) par récurrence sur le degré $[L : K]$. Notons que cette assertion est évidente si $[L : K] = 1$.

Supposons donc $[L : K] > 1$. Ainsi, il existe une racine a de $P(X)$ dans L qui n'appartient pas K, donc telle que $[K(a) : K] > 1$. Soit $\mu_a(X)$ le polynôme minimal de cette racine.



Grâce au théorème 11.1, on sait qu'il existe exactement m_a prolongements de ι à un morphisme de $K(a)$ dans $\widetilde{M}$, où m_a désigne le nombre de racines de $\widetilde{\mu}_a(X)$ dans $\widetilde{M}$. Or $\widetilde{\mu}_a(X)$ est complètement décomposé dans $\widetilde{M}$ et n'y a que des racines simples puisque les corps considérés sont finis ou de caractéristique nulle. On a donc $m_a = \deg \mu_a(X) = [K(a) : K]$.

Pour chacun de ces prolongements ι_a, l'élément $b := \iota_a(a)$ est une racine de $\widetilde{\mu}_a(X)$ et ι_a est un isomorphisme de $K(a)$ sur $\widetilde{K}(b)$.

Or L est corps des racines de $P(X)$ sur $K(a)$. Comme $[L : K(a)] < [L : K]$, on peut appliquer l'hypothèse de récurrence et en déduire qu'il y a exactement $[L : K(a)]$ prolongements de ι_a à un morphisme de L dans $\widetilde{M}$.

Il en résulte qu'il y a bien exactement $[L : K(a)][K(a) : K] = [L : K]$ prolongements de ι à un morphisme de L dans $\widetilde{M}$.

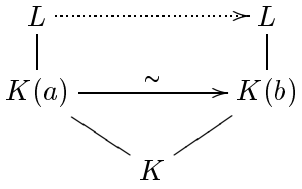
L'assertion (2) est évidente. □

Démonstration de 11.6. Les assertions (1) et (2) ne sont que des reformulations des assertions (1) et (2) du théorème 11.5 dans le cas particulier ou $\widetilde{K} = K$, $\iota = \mathrm{Id}_K$, $\widetilde{M} = L$. Démontrons l'assertion (3).

Il est clair que si $\sigma \in \mathrm{Gal}(L/K)$ et si $Q(X) \in \mathrm{Irr}\, K[X]$ est un facteur de $P(X)$, alors σ envoie une racine de $Q(X)$ dans L sur une racine de $Q(X)$ dans L. Il reste à démontrer que, si a et

b sont deux racines quelconques de $Q(X)$ dans L, il existe un élément $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(a) = b$.

Or on sait par 11.1 qu'il existe un isomorphisme de $K(a)$ sur $K(b)$ qui induit l'identité sur K.



Il résulte alors du théorème 11.5 que cet isomorphisme se prolonge (d'ailleurs, de $[L : K(a)]$ façons différentes, mais une nous suffit) à un automorphisme de L. □

Extensions galoisiennes.

Le résultat suivant permet de caractériser les extensions de K qui sont corps des racines sur K d'un polynôme de $K[X]$.

11.7. Proposition. *Soit L/K une extension de degré fini. Les propriétés suivantes sont équivalentes.*

(i) *Il existe $P(X) \in K[X]$ tel que L est corps des racines de $P(X)$.*
(ii) *Si $Q(X)$ est un élément irréductible de $K[X]$ qui a une racine dans L, alors $Q(X)$ a toutes ses racines dans L.*

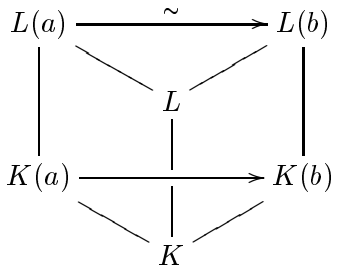
Démonstration de 11.7.

(i)⇒(ii) . Nous démontrons un résultat un peu plus général

11.8. Lemme. *Supposons que L est corps des racines sur K de $P(X) \in K[X]$. Soit $Q(X) \in \mathrm{Irr}\, K[X]$ et soient a et b deux racines de $Q(X)$. Alors*

$$[L(a) : L] = [L(b) : L]\,.$$

Démonstration de 11.8. On sait (cf. 11.1) qu'il existe un isomorphisme de $K(a)$ sur $K(b)$ qui induit l'identité sur K. Comme $L(a)$ (resp. $L(b)$) est corps des racines de $P(X)$ sur $K(a)$ (resp. sur $K(b)$), on voit grâce à 11.5 qu'un tel isomorphisme se prolonge en un isomorphisme de $L(a)$ sur $L(b)$.



On voit que $[L(a) : K] = [L(b) : K]$. Comme $[L(a) : K] = [L(a) : L][L : K]$ et $[L(b) : K] = [L(b) : L][L : K]$, on en déduit bien $[L(a) : L] = [L(b) : L]$. □

(ii)⇒(i) . Supposons $L = K(a_1, a_2, \ldots, a_n)$. Si $\mu_a(X)$ désigne le polynôme minimal sur K de $a \in L$, on pose alors $P(X) := \mu_{a_1}(X)\mu_{a_2}(X)\cdots\mu_{a_n}(X)$, et on constate que L est corps des racines de $P(X)$ sur K. □

Définition. Une extension L/K qui possède les propriétés (i) et (ii) de la proposition 11.7 est appélée une *extension galoisienne*.

La propriété suivante des extensions galoisiennes est immédiate d'après l'assertion (i) de 11.7.

11.9. Proposition. *Supposons $K \subseteq L \subseteq M$, et supposons l'extension M/K galoisienne. Alors l'extension M/L est galoisienne.*

Ⓘ Attention Ⓘ

Par contre, avec les notations de la proposition précédente, il est faux en général que L/K soit galoisienne. Considérons par exemple $K = \mathbb{Q}$, $L := \mathbb{Q}(\sqrt[3]{2})$, et $M := \mathbb{Q}(\sqrt[3]{2}, \omega)$. On sait que M/K est galoisienne. Mais L/K n'est pas galoisienne, puisque $X^3 - 2$ n'a qu'une racine dans L.

La proposition suivante donne une condition nécessaire et suffisante pour qu'une sous–extension d'une extension galoisienne soit galoisienne.

11.10. Proposition. *Supposons $K \subseteq L \subseteq M$, et supposons l'extension M/K galoisienne. Les propriétés suivantes sont équivalentes.*

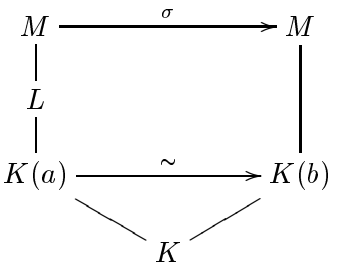
(i) *L'extension L/K est galoisienne.*
(ii) *Pour tout $\sigma \in \mathrm{Gal}(M/K)$, on a $\sigma(L) = L$.*

Démonstration de 11.10.
(i)⇒(ii). Soit $\sigma \in \mathrm{Gal}(M/K)$ et soit $a \in L$. Nous allons démontrer que $\sigma(a) \in L$.

Soit $P(X)$ le polynôme minimal de a sur K. L'élément $\sigma(a)$ est une racine de $P(X)$ dans M. Or $P(X)$ a une racine dans L, donc les y a toutes. Par suite, on a bien $\sigma(a) \in L$.

(ii)⇒(i). Soit $P(X) \in \mathrm{Irr}\, K[X]$. On suppose que L contient une racine a de $P(X)$, et on va démontrer que $P(X)$ a toutes ses racines dans L.

Comme M/K est galoisienne, $P(X)$ a toutes ses racines dans M. Soit b l'une d'entre elles. On sait (cf. 11.1) qu'il y a un isomorphisme de $K(a)$ sur $K(b)$ induisant l'identité sur K et envoyant a sur b. On sait d'autre part (cf. 11.5) qu'un tel isomorphisme se prolonge en un automorphisme de M, *i.e.*, en un élément $\sigma \in \mathrm{Gal}(M/K)$:



Puisque par hypothèse σ envoie L dans lui–même, on voit bien que $b \in L$. □

Clôture galoisienne d'une extension.

Soit M/K une extension de corps. Si L_1/K et L_2/K sont deux sous–extensions galoisiennes de M/K, alors $(L_1 \cap L_2)/K$ est aussi une extension galoisienne.

En effet, si $P(X) \in \mathrm{Irr}\, K[X]$ a une racine dans $L_1 \cap L_2$, il a toutes ses racines dans L_1 et dans L_2, donc dans $L_1 \cap L_2$.

On peut donc définir la notion d'"extension galoisienne engendrée" :

Soit $K \subseteq L \subseteq M$ une "tour" d'extensions, où l'on suppose M/K galoisienne. Alors l'intersection des sous–corps de M, contenant L et galoisiens sur K est une extension galoisienne de K, appelée *la clôture galoisienne de L/K*.

Il est facile de vérifier que la clôture galoisienne de L/K est définie de la manière suivante.
(11.11) Supposons $L = K(a_1, a_2, \ldots, a_r)$. Pour tout i, notons $\mu_{a_i}(X)$ le polynôme minimal de a_i. Alors la clôture galoisienne de L/K est le corps des racines dans M du polynôme $P(X) := \mu_{a_1}(X) \cdots \mu_{a_i}(X) \cdots \mu_{a_r}(X)$.

Considérons maintenant la situation "abstraite" où le point de départ est une extension (de degré fini) L/K pour laquelle on n'a pas choisi d'extension galoisienne M/K la contenant.

La construction 11.11 ci–dessus nous fournit une construction d'une extension galoisienne minimale de L contenant L. La démonstration de la proposition suivante est laissée en exercice.

11.12. Proposition. *Si L_1/K et L_2/K sont deux extensions galoisiennes minimales contenant L/K, il existe un isomorphisme de L_1 sur L_2 induisant l'identité sur K.*

12. Corps finis

12.A. Existence et unicité.

Soit $\mathbb{F}$ un corps fini. Sa caractéristique ne peut pas être nulle (car son sous–corps premier serait alors $\mathbb{Q}$) ; elle est donc un nombre premier p et le sous–corps premier de $\mathbb{F}$ est $\mathbb{F}_p$. Soit $n := [\mathbb{F} : \mathbb{F}_p]$; on a alors $|\mathbb{F}| = p^n$. Le résultat suivant montre qu'un corps fini est déterminé, à isomorphisme (non unique en général) près, par son cardinal.

12.1. Théorème. *Soit p un nombre premier, soit n un entier, et soit $q := p^n$.*

(1) Si $\mathbb{F}$ est un corps fini de cardinal q, $\mathbb{F}$ est corps des racines sur $\mathbb{F}_p$ de $X^q - X$.

(2) Réciproquement, tout corps de racines de $X^q - X$ sur $\mathbb{F}_p$ est de cardinal q.

Démonstration de 12.1.

(1) Puisque $\mathbb{F}^\times$ est d'ordre $q-1$, pour tout $x \in \mathbb{F}^timesimes$ on a $x^{q-1} = 1$, d'où il résulte que $x^q = x$ pour tout $x \in \mathbb{F}$. Ainsi, $\mathbb{F}$ est formé de racines du polynôme $X^q - X$. Comme ce polynôme a au plus q racines et que $\mathbb{F}$ est de cardinal q, on voit que $\mathbb{F}$ *est l'ensemble des racines* de $X^q - X$, donc *a fortiori* est corps de racines de ce polynôme.

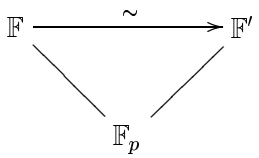
(2) Notons maintenant $\mathbb{F}$ un corps de racines de $X^q - X$. L'ensemble des racines de $X^q - X$ est un sous–ensemble de cardinal q de $\mathbb{F}$ (en effet, $X^q - X$ n'a pas de racine double car il est premier avec son polynôme dérivé -1).

L'ensemble des racines de $X^q - X$ est l'ensemble des points fixes de $\mathbb{F}$ par l'automorphisme (cf. 11.4) $F_n : \mathbb{F} \longrightarrow \mathbb{F}$, $x \mapsto x^q$, donc est un sous–corps de $\mathbb{F}$.

Il en résulte que $\mathbb{F}$, engendré par ces racines, coïncide avec cet ensemble de racines, et donc en particulier est de cardinal q. □

Le corollaire suivant est une conséquence immédiate de 11.5.

12.2. Corollaire. *Soient $\mathbb{F}$ et $\mathbb{F}'$ deux corps de cardinal $q = p^n$. Il existe exactement n isomorphismes de $\mathbb{F}$ sur $\mathbb{F}'$ (qui induisent l'identité sur le sous–corps premier $\mathbb{F}_p$).*



12.B. Théorie de Galois des corps finis.

12.3. Proposition. *Soit $\mathbb{F}$ un corps fini de cardinal $q = p^n$.*

- *Tout sous–corps de $\mathbb{F}$ est de cardinal p^d où d divise n.*
- *Pour tout diviseur d de n il existe un et un seul sous–corps $\mathbb{F}_{p^d}$ de $\mathbb{F}$ de cardinal p^d.*

Ainsi l'application $d \mapsto \mathbb{F}_{p^d}$ est une bijection de l'ensemble de diviseurs de n sur l'ensemble des sous–corps de $\mathbb{F}$.

Démonstration de 12.3.

Si $\mathbb{F}'$ est un sous–corps de $\mathbb{F}$, $\mathbb{F}'$ contient le sous–corps premier $\mathbb{F}_p$ de $\mathbb{F}$ donc est de cardinal p^d pour un certain d. D'autre part $\mathbb{F}$ est un espace vectoriel de dimension finie sur $\mathbb{F}'$, donc son cardinal p^n est une puissance du cardinal p^d de $\mathbb{F}'$, ce qui montre que d divise n.

Supposons que d divise n. Toute racine du polynôme $X^{p^d} - X$ est aussi racine de $X^{p^n} - X$, donc $X^{p^d} - X$ est totalement décomposé en facteurs du premier degré dans $\mathbb{F}$ puisque tel est le cas pour $X^{p^n} - X$. Le corps des racines de $X^{p^d} - X$ (qui coïncide ici avec *l'ensemble* des racines) est alors *le* sous–corps de cardinal p^d de $\mathbb{F}$. □

Nous allons réinterpréter ce résultat en utilisant les opérations du groupe de Galois.

Désignons par $F\colon \mathbb{F} \xrightarrow{\sim} \mathbb{F}$ l'automorphisme de $\mathbb{F}$ défini par $\mathbb{F}(x) := x^q$.

12.4. Théorème.

(1) $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ *est le groupe cyclique (d'ordre* n*) engendré par* F*.*

(2) L'application

$$H \mapsto \mathbb{F}^H ,$$

qui à un sous–groupe H *de* $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ *associe le corps des points fixes de* H *dans* $\mathbb{F}$*, est une bijection décroissante de l'ensemble des sous–groupes de* $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ *sur l'ensemble des sous–corps de* $\mathbb{F}$*.*

Démonstration de 12.4.

(1) On sait que $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ est d'ordre n et contient le sous–groupe engendré par F. Il suffit donc de vérifier que F est d'ordre n. Or pour tout d divisant n, on a $F^d(x) = x^{p^d}$. On voit que $F^n = \mathrm{Id}$. D'autre part, on sait que le groupe $\mathbb{F}^\times$ est cyclique d'ordre n. Donc il existe un élément $\xi \in \mathbb{F}$ tel que $\xi^{p^d} \neq \xi$ pour tout $d < n$, ce qui prouve bien que F est d'ordre n.

(2) Comme $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ est cyclique d'ordre n et engendré par F, l'application qui à un diviseur d de n associe le sous–groupe de $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ engendré par $F^{n/d}$ est une bijection de l'ensemble des diviseurs de n sur l'ensemble des sous–groupes de $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$.

D'autre part le sous–corps des points fixes par $F^{n/d}$ est manifestement l'ensemble des racines de $X^{n/d} - X$, *i.e.*, le sous–corps $\mathbb{F}_{p^{n/d}}$ de $\mathbb{F}$. L'assertion à démontrer résulte alors immédiatement de 12.3. □

Terminons ce paragraphe par une mise en garde et une remarque.

Ⓘ **Attention** Ⓘ

$\mathbb{F}_4$ n'est pas un sous–corps de $\mathbb{F}_8$.

Remarque. Toute extension $\mathbb{F}$ d'un corps fini $\mathbb{F}'$ est galoisienne. En particulier, si $P(X) \in \mathrm{Irr}\,\mathbb{F}'[X]$ admet une racine dans $\mathbb{F}$, il y est totalement décomposé en facteurs du premier degré.

13. Théorie de Galois

Dans tout ce qui suit, on suppose dorénavant K de caractéristique zéro.

13.1. Théorème. *Soit* M/K *une extension galoisienne. On pose* $G := \mathrm{Gal}(M/K)$*.*

(1) L'application $H \mapsto M^H$ *, qui à un sous–groupe* H *de* G *associe le sous–corps des points fixes de* M *par* H*, est une bijection décroissante de l'ensemble des sous–groupes de* G *sur l'ensemble des sous–corps de* M *contenant* K*.*

(2) La bijection réciproque est l'application $L \mapsto \mathrm{Gal}(M/L)$*, qui à un sous–corps* L *de* M *contenant* K *associe le groupe de Galois de* M/L*.*

(3) Si L *est un sous–corps de* M *contenant* K*, l'extension* L/K *est galoisienne si et seulement si le sous–groupe* $\mathrm{Gal}(M/L)$ *est normal dans* G*.*

Dans ce cas, la restriction à L*, notée* $\sigma \mapsto \sigma_{|L}$ *définit un isomorphisme*

$$\mathrm{Gal}(M/K)/\mathrm{Gal}(M/L) \xrightarrow{\sim} \mathrm{Gal}(L/K) .$$

Démonstration de 13.1.
(1) et (2). Il est clair que

$$H \subseteq \mathrm{Gal}(M/M^H) \quad \text{et} \quad L \subseteq M^{\mathrm{Gal}(M/L)}.$$

• Remarquons qu'il suffit de démontrer que

$$|H| \leq [M : M^H].$$

En effet, puisque $L \leq M^{\mathrm{Gal}(M/L)}$ on a alors

$$|\mathrm{Gal}(M/L)| \leq [M : M^{\mathrm{Gal}(M/L)}] \leq [M : L].$$

Comme $|\mathrm{Gal}(M/L)| = [M : L]$, on en déduit

$$H = \mathrm{Gal}(M/M^H) \quad \text{et} \quad L = M^{\mathrm{Gal}(M/L)}.$$

• Pour la démonstration de l'inégalité $|H| \leq [M : M^H]$, on renvoie la lectrice et le lecteur au polycopié de Bruguières.

(3) Il est facile de vérifier que, pour tout $\sigma \in \mathrm{Gal}(M/K)$, on a

$$\sigma \mathrm{Gal}(M/L)\sigma^{-1} = \mathrm{Gal}(M/\sigma(L)).$$

L'assertion (3) résulte alors de $\square$

Discriminant et groupe de Galois.

Soit $P(X) \in \mathrm{Irr}\, K[X]$, et soit R l'ensemble de ses racines dans un corps de racines L. D'après 11.6, le groupe de Galois de $P(X)$ (*i.e.*, le groupe $\mathrm{Gal}(L/K)$) s'identifie à un sous–groupe transitif du groupe symétrique $\mathfrak{S}_R$ de R.

13.2. Proposition. *Le groupe de Galois de $P(X)$ est contenu dans le groupe alterné $\mathfrak{A}_R$ si et seulement si le discriminant* $\mathrm{Discr}(P(X))$ *est un carré dans K.*

Démonstration de 13.2. Posons $R := \{a_1, a_2, \ldots, a_d\}$. Rappelons que

$$\mathrm{Discr}(P(X)) = \left(\prod_{i<j} (a_j - a_i) \right)^2,$$

et que $\mathrm{Discr}(P(X)) \neq 0$ puisque K est fini ou de caractéristique nulle. Ainsi $\mathrm{Discr}(P(X))$ est un carré dans K si et seulement si $\prod_{i<j}(a_j - a_i) \in K$.

Or pour $\sigma \in \mathfrak{S}_R$, on a

$$\prod_{i<j} (\sigma(a_j) - \sigma(a_i)) = \mathrm{sgn}(\sigma) \prod_{i<j} (a_j - a_i).$$

Puisqu'un élément de L est dans K si et seulement si il est fixe par $\mathrm{Gal}(L/K)$, on voit que $\prod_{i<j}(a_j - a_i) \in K$ si et seulement si $\mathrm{sgn}(\sigma) = +1$ pour tout $\sigma \in \mathrm{Gal}(L/K)$. $\square$