Anneaux commutatifs

David Harari

M1 FES, Orsay, 2024-2025

Table des matières

1. Généralités sur les anneaux **1**
1.1. Définitions, premières propriétés 1
1.2. Idéaux, anneaux quotient 3
1.3. Anneaux intègres 5

2. Divisibilité dans les anneaux intègres **8**
2.1. Éléments irréductibles 8
2.2. Anneaux factoriels et noethériens 9

3. Factorialité d'un anneau de polynômes **14**

4. A-algèbres. Algèbres de polynômes **18**
4.1. Notion de A-algèbre 18
4.2. Algèbres de polynômes, propriété universelle 18
4.3. Polynômes symétriques 21

1. Généralités sur les anneaux

1.1. Définitions, premières propriétés

Définition 1.1 Un *anneau* $(A, +, .)$ est la donnée d'un ensemble A et de deux lois internes $+, .$ vérifiant :

1. $(A, +)$ est un groupe abélien (on notera comme d'habitude 0 le neutre pour $+$ et $-x$ l'opposé de $x \in A$).
2. La multiplication . est associative et possède un élément neutre (noté 1).

3. . est distributive par rapport à + : pour tous x, y, z dans A, on a $x(y+z) = xy + xz$ et $(y+z)x = yx + zx$.

Si la multiplication est commutative, on dit que l'anneau A est *commutatif*. Noter qu'on a dans tout anneau $0.x = x.0 = 0$ pour tout x, où 0 est le neutre pour l'addition.

Exemple 1.2 a) L'anneau nul $\{0\}$. Il est caractérisé par le fait que dans cet anneau, on a $0 = 1$.

b) $(\mathbf{Z}, +, .)$, $(\mathbf{Z}/n\mathbf{Z}, +, .)$ sont des anneaux commutatifs.

c) Un corps K est par définition un anneau *commutatif*, distinct de $\{0\}$, tel que tout élément non nul ait un inverse pour la multiplication. On peut aussi dire qu'un anneau commutatif K est un corps si et seulement si $K \setminus \{0\}$ est un groupe pour la multiplication.

d) Si A est un anneau *commutatif*[1], on dispose de l'*anneau des polynômes en n variables* $A[X_1, ..., X_n]$ qui est commutatif.

e) Pour tout corps K, $(M_n(K), +, .)$ est un anneau, non commutatif si $n \geq 2$.

Définition 1.3 On appelle ensemble des éléments *inversibles* d'un anneau A l'ensemble des $x \in A$ tels qu'il existe $y \in A$ avec $xy = yx = 1$. C'est un groupe pour la multiplication, noté en général A^*.

Exemple 1.4 a) $\mathbf{Z}^* = \{\pm 1\}$.

b) $(\mathbf{Z}/n\mathbf{Z})^*$ est l'ensemble des classes $\bar{m}$, avec m premier à n. Attention à ne pas parler d'élément de $\mathbf{Z}/n\mathbf{Z}$ premier avec n, ce qui n'a pas de sens en général (on ne peut parler de cette notion que dans un anneau intègre).

c) Dans un corps K, on a par définition $K^* = K \setminus \{0\}$.

d) Si K est un corps, alors $K[X_1, ..., X_n]^*$ est l'ensemble des polynômes constant non nul (qui est isomorphe au groupe multiplicatif K^*). Ceci reste vrai si on remplace K par un anneau *intègre* (voir plus loin) A, et K^* par son groupe des inversibles A^*.

e) Si K est un corps, on a $M_n(K)^* = \mathrm{GL}_n(K)$, qui est aussi l'ensemble des matrices de déterminant non nul. Si on remplace K par un anneau commutatif A, alors $M_n(A)^*$ est l'ensemble des matrices dont le déterminant est dans A^* (via l'identité de la comatrice).

1. On peut définir cet anneau de polynômes pour A non-commutatif, mais aucune des bonnes propriétés habituelles ne se conserve, donc on se limitera dans ce cours au cas commutatif.

Définition 1.5 Un *homomorphisme* (ou morphisme) d'anneaux $f : A \to B$ est une application entre deux anneaux vérifiant pour tous x, y de A :

1. $f(x+y) = f(x) + f(y)$.
2. $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

On notera que l'application nulle n'est pas un morphisme d'anneaux car elle ne vérifie pas 3.

1.2. Idéaux, anneaux quotient

On supposera désormais tous les anneaux commutatifs, sauf mention expresse du contraire (la théorie des anneaux non commutatifs est intéressante, mais très différente, et elle n'a pas les mêmes applications).

Définition 1.6 Soit A un anneau. Un *sous-anneau* de A est un sous-groupe B de $(A, +)$, *contenant* 1, et stable pour la multiplication. Autrement dit, cela signifie que B est un anneau pour les lois induites par A, avec le même neutre [2] pour la multiplication.

Cette notion est en pratique souvent moins utile que la suivante :

Définition 1.7 Une partie I d'un anneau commutatif A est un *idéal* de A si elle vérifie :

1. I est un sous-groupe de A pour $+$.
2. Pour tout x de I et tout a de A, on a $ax \in I$.

Remarque 1.8 a) En particulier un idéal de A contient 1 (ou encore contient un élément inversible de A) si et seulement s'il est égal à A.

b) Si A n'était pas commutatif, il faudrait parler d'idéal à gauche ou d'idéal à droite (voire d'idéal bilatère si I est stable par multiplication par un élément de A à droite et à gauche).

Noter aussi qu'un idéal de A n'est pas autre chose qu'un sous A-module de A.

2. Attention, l'ensemble des matrices $A = (a_{ij}) \in M_2(K)$ dont tous les coefficients autres que a_{11} sont nuls est un anneau pour les lois $+$ et $\times$, mais ce n'est pas un sous-anneau de $M_2(K)$, car le neutre pour $\times$ n'est pas le même. Plus simplement, $\{0\}$ n'est pas un sous-anneau d'un anneau non nul.

Exemple 1.9 a) $\{0\}$ et A sont des idéaux de A. Ce sont les seuls si A est un corps (et cette propriété caractérise les corps parmi les anneaux non nuls).

b) Les idéaux de $\mathbf{Z}$ sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$. Ceux de $\mathbf{Z}/n\mathbf{Z}$ sont les $d\mathbf{Z}/n\mathbf{Z}$, où d divise n.

c) Si $f : A \to B$ est un morphisme entre deux anneaux commutatifs, l'image réciproque d'un idéal de B par f est un idéal de A. En particulier le *noyau* $\ker f = f^{-1}(0)$ est un idéal de A. Ceci implique qu'un morphisme de corps (=morphisme entre les anneaux sous-jacents) est toujours injectif.

Remarque 1.10 On fera attention à ce que l'image directe d'un idéal par un morphisme d'anneaux n'est pas toujours un idéal si on ne suppose pas le morphisme surjectif. Par exemple l'image de $\mathbf{Z}$ par l'inclusion $\mathbf{Z} \to \mathbf{Q}$ est $\mathbf{Z}$, qui n'est pas un idéal de $\mathbf{Q}$. Par contre, l'image directe (resp. l'image réciproque) d'un sous-anneau par un morphisme d'anneaux est bien un sous-anneau. On vérifie facilement que l'image directe d'un idéal par un morphisme d'anneaux $f : A \to B$ est un idéal de $\operatorname{Im} f$.

Proposition 1.11 *Soient A un anneau commutatif et I un idéal de A. Alors le groupe quotient A/I muni de la multiplication $\bar{a}\bar{b} := \overline{ab}$ est un anneau, appelé anneau quotient de A par I. La surjection canonique $p : A \to A/I$ est un morphisme d'anneaux, et l'élément unité de A/I est $\bar{1}$.*

Vérification facile, comme dans le cas des espaces vectoriels quotients ou des groupes quotients.

On a alors immédiatement le théorème de factorisation habituel :

Theorème 1.12 *Soit $f : A \to B$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux $\tilde{f} : A/\ker f \to B$ tel que $f = \tilde{f} \circ p$, où $p : A \to A/\ker f$ est la surjection canonique. De plus $\tilde{f}$ est injectif d'image $\operatorname{Im} f$, i.e. on a un isomorphisme d'anneaux $A/\ker f \simeq \operatorname{Im} f$.*

Exemple 1.13 a) $\mathbf{Z}/n\mathbf{Z}$ est le quotient de $\mathbf{Z}$ par l'idéal $n\mathbf{Z}$.

b) L'application $P \mapsto P(i)$ est un morphisme d'anneaux surjectif de $\mathbf{R}[X]$ dans $\mathbf{C}$ dont le noyau est l'idéal (X^2+1) engendré par le polynôme X^2+1 (pour le voir effectuer la division euclidienne par X^2+1). On a donc un isomorphisme d'anneaux $\mathbf{R}[X]/(X^2+1) \simeq \mathbf{C}$ et $\mathbf{R}[X]/(X^2+1)$ est un corps (on peut prendre cela pour définition de $\mathbf{C}$!).

Proposition 1.14 *Soit I un idéal d'un anneau commutatif A.*

a) Les idéaux de A/I sont ses sous-groupes additifs de la forme J/I, où J est un idéal de A contenant I. L'anneau quotient de A/I par J/I est alors isomorphe à A/J.

b) Soit J_1 un idéal quelconque de A. Son image $p(J_1)$ par la surjection canonique $p : A \to A/I$ est l'idéal $(I + J_1)/I$ de A/I, qui est isomorphe en tant que A-module à $J_1/(I \cap J_1)$.

Démonstration : a) On sait déjà que les sous-groupes additifs de A/I sont les J/I, où J est un sous-groupe additif de A contenant J. Si de plus J/I est un idéal de A/I, alors son image réciproque par p (qui est J vu que $J \supset I$) est un idéal de A, et réciproquement si J est un idéal de A, son image J/I par la surjection canonique p est bien un idéal de A/I. Enfin, l'isomorphisme d'anneaux

$$(A/I)/(J/I) \simeq A/J$$

résulte du théorème de factorisation, comme dans le cas des groupes abéliens.

b) On a clairement $p(J_1) = p(J_1 + I) = (I + J_1)/I$. L'isomorphisme de groupes abéliens $(I + J_1)/I \simeq J_1/(I \cap J_1)$ (vu dans le cas des groupes) est clairement ici également un morphisme de A-modules (attention, morphisme d'"idéaux" n'a pas de sens, la notion d'idéal étant relative à l'anneau sous-jacent).

□

1.3. Anneaux intègres

Définition 1.15 Un anneau commutatif A est dit *intègre* s'il est non nul, et si pour tous a, b de A, la condition $ab = 0$ implique $a = 0$ ou $b = 0$.

Noter que la propriété analogue si l'anneau A n'est pas supposé commutatif s'appelle plutôt *anneau sans diviseur de zéro* ("domain" en anglais, tandis qu'anneau intègre se dit "integral domain" et corps se dit "field").

Exemples :

1. $\mathbf{Z}$ est intègre.
2. Pour $n \in \mathbf{N}^*$, $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est premier.
3. Tout corps est évidemment un anneau intègre (mais pas réciproquement, par exemple $\mathbf{Z}$ n'est pas un corps).
4. Tout sous-anneau d'un anneau intègre (par exemple d'un corps) est intègre.
5. Si A est intègre, les anneaux $A[X]$, $A[X_1, ..., X_n]$ sont intègres (et réciproquement), comme on le voit facilement par récurrence sur n.

On rappelle le résultat classique suivant :

Proposition 1.16 *Soit A un anneau intègre ; alors il existe un corps K et un homomorphisme injectif $i : A \to K$ tel que pour tout morphisme injectif f d'anneaux de A vers un corps K', il existe un unique morphisme de corps $j : K \to K'$ tel que $f = j \circ i$. K est unique à isomorphisme près, et s'appelle le corps des fractions de A. On le note* $\operatorname{Frac} A$.

Cela signifie donc que K est le "plus petit corps" contenant A, tout élément de K s'écrit x/y avec $x \in A$ et $y \in A$ non nul ; ainsi un anneau est intègre si et seulement s'il est sous-anneau d'un corps. Par exemple $\operatorname{Frac} \mathbf{Z} = \mathbf{Q}$, et $\operatorname{Frac}(K[X]) = K(X)$ (le corps des fractions rationnelles en une indéterminée). Noter que l'anneau nul n'a pas de corps des fractions (ce qui justifie qu'il ne soit pas intègre par convention). Pour construire $K = \operatorname{Frac} A$, on considère les couples (a, b) avec $a \in A$ et $b \in A \setminus \{0\}$, et on définit ensemblistement K comme le quotient de l'ensemble de ces couples par la relation d'équivalence : $(a, b) \sim (c, d)$ ssi $ad = bc$. On vérifie alors que K, muni des lois

$$(a, b)(c, d) := (ac, bd); \quad (a, b) + (c, d) = (ad + bc, bd),$$

est un corps (dans lequel (a, b) correspond à a/b) qui vérifie les propriétés voulues.

Définition 1.17 Un anneau commutatif A est dit *principal* s'il est intègre et si tous ses idéaux sont *principaux*, i.e. de la forme $(a) = aA$ avec $a \in A$.

En pratique, on vérifie souvent qu'un anneau est principal via la notion suivante.

Définition 1.18 Un anneau intègre A est dit *euclidien* s'il existe une application $v : A - \{0\} \to \mathbf{N}$ ("stathme euclidien") tel que si a, b sont dans A avec $b \neq 0$, alors il existe q, r dans A avec $a = bq + r$ et r vérifiant : $r = 0$ ou $v(r) < v(b)$.

Noter qu'on ne demande pas d'unicité dans cette "division euclidienne".

Exemple 1.19 a) L'anneau $\mathbf{Z}$ est euclidien avec $v(x) = |x|$.

b) Si K est un corps, l'anneau $K[X]$ est euclidien avec $v(P) = \deg P$.

c) On vérifiera que l'anneau $\mathbf{Z}[i]$ (constitué des nombres complexes de la forme $a + bi$ avec $a, b \in \mathbf{Z}$) est euclidien avec $v(x) = |x|^2$, sans qu'on ait unicité dans la division euclidienne.

Theorème 1.20 *Si A est euclidien, A est principal.*

Démonstration : Soit I un idéal non nul de A, on choisit b non nul dans I avec $v(b)$ minimal. Alors tout a de I s'écrit $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$. Mais le deuxième cas est impossible car $r \in I$ d'où $a \in (b)$. Finalement $I = (b)$.

□

Par exemple $\mathbf{Z}$ et $K[X]$ (quand K est un corps) sont principaux. Si $n \in \mathbf{N}^*$ n'est pas premier, alors $\mathbf{Z}/n\mathbf{Z}$ n'est pas un anneau principal (bien que tous ses idéaux soient principaux) car il n'est pas intègre. Un corps est trivialement un anneau principal.

Définition 1.21 Un idéal I de A est dit *premier* si A/I est intègre. De manière équivalente cela signifie : $A \neq I$, et la condition $ab \in I$ implique $a \in I$ ou $b \in I$.

Exemples :

1. Les idéaux premiers de $\mathbf{Z}$ sont $\{0\}$ et les $n\mathbf{Z}$ pour n premier.
2. Un anneau A est intègre si et seulement si $\{0\}$ est premier.
3. Les idéaux (X_1) et (X_1, X_2) sont tous deux premiers dans $K[X_1, X_2]$.

□

Définition 1.22 Un idéal I de A est dit *maximal* si $I \neq A$ et si tout idéal J contenant I est égal à A où à I.

Proposition 1.23 *Un idéal I est maximal si et seulement si A/I est un corps. En particulier, tout idéal maximal est premier.*

Démonstration : Si I est maximal et $\bar{x}$ est non nul dans A/I, alors $x \notin I$ donc l'idéal $I + xA$ contient strictement I ; par maximalité de I, on a $A = I + xA$ et 1 s'écrit $1 = i + xa$ avec $i \in I$ et $a \in A$ ce qui se traduit par $\bar{1} = \bar{x}\bar{a}$, d'où $\bar{x}$ inversible dans A/I. Comme $I \neq A$, l'anneau A/I n'est pas nul et ses éléments non nuls sont inversibles, i.e. A/I est un corps.

En sens inverse si A/I est un corps, alors $I \neq A$, et tout idéal J de A contenant strictement I contient un élément $x \notin I$. Alors $\bar{x}$ est inversible dans A/I, soit $\bar{1} = \bar{x}\bar{a}$ avec $a \in A$, ou encore $1 = xa + i$ avec $i \in I \subset J$ et $x \in J$. Ainsi $1 \in J$ et $J = A$.

□

Exemple 1.24 Tous les idéaux premiers non nuls de $\mathbf{Z}$ sont maximaux. Ce n'est plus le cas dans $K[X_1, X_2]$, où l'idéal premier (X_1) n'est pas maximal : il est strictement inclus dans l'idéal maximal (X_1, X_2) (on vérifie facilement que le quotient de $K[X_1, X_2]$ par (X_1, X_2) est isomorphe à K).

Le théorème suivant est utile pour les questions théoriques générales. [3]

Theorème 1.25 (Krull) *Dans un anneau commutatif*[4] *A, tout idéal $I \neq A$ est inclus dans un idéal maximal.*

Démonstration : L'ensemble des idéaux de A contenant I et distincts de A est non vide et inductif car si $(I_i)_{i\in I}$ est une famille totalement ordonnée d'idéaux de A distincts de A, la réunion est encore un idéal (parce que la famille est totalement ordonnée) distinct de A (parce qu'elle ne contient pas 1). On applique alors le lemme de Zorn.

□

2. Divisibilité dans les anneaux intègres

Dans tout cette section, A désigne un anneau commutatif, supposé intègre sauf mention explicite du contraire.

2.1. Éléments irréductibles

Définition 2.1 Soient a, b dans A. On dit que a *divise* b et on écrit $a|b$ s'il existe $c \in A$ tel que $b = ac$. En termes d'idéaux, c'est équivalent à $(a) \supset (b)$.

En particulier 0 ne divise que lui-même, et un élément de A^* divise tous les éléments de A.

Proposition 2.2 *Soient a, b dans A. Alors ($a|b$ et $b|a$) si et seulement s'il existe $u \in A^*$ tel que $a = ub$. On dit alors que a et b sont associés.*

Démonstration : On peut supposer a et b non nuls (sinon le résultat est trivial). Si $a = ub$ avec $u \in A^*$, alors $b|a$ et $b = u^{-1}a$ donc $a|b$. En sens inverse si $a = bc$ et $b = ad$ avec c, d dans A, alors $a = adc$ donc $dc = 1$ par intégrité de A, soit $c \in A^*$.

□

La relation "être associé" est d'équivalence sur A ou $A \setminus \{0\}$; en termes d'idéaux, a est associé à b si et seulement si $(a) = (b)$. La relation "divise"

3. En particulier quand on travaille avec des anneaux non noethériens, ce qui est souvent le cas en analyse.

4. On notera que l'existence d'un élément unité dans A est cruciale pour ce théorème. On a l'analogue dans un anneau non commutatif en remplaçant "idéal" par "idéal à gauche", "idéal à droite", ou "idéal bilatère".

est une relation d'ordre sur l'ensemble quotient de $A \setminus \{0\}$ par la relation d'association.

Définition 2.3 On dit qu'un élément p de $A \setminus \{0\}$ est *irréductible* s'il vérifie les deux propriétés suivantes :

1. p n'est *pas* inversible dans A.
2. La condition $p = ab$ avec a, b dans A implique que a ou b soit inversible.

La deuxième condition signifie que les seuls diviseurs de p sont ses associés et les inversibles de A. On fera bien attention au fait que par convention, les éléments de A^* ne sont pas irréductibles (tout comme 1 n'est pas un nombre premier).

Exemple 2.4 a) Les irréductibles de $\mathbf{Z}$ sont les $\pm p$ avec p nombre premier.

b) Les éléments irréductibles de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle. Les irréductibles de $\mathbf{C}[X]$ sont les polynômes de degré 1.

c) Un corps n'a pas d'éléments irréductibles.

2.2. Anneaux factoriels et noethériens

On suppose toujours que A est un anneau intègre.

Définition 2.5 On dit que deux éléments a et b de A sont *premiers entre eux* si leurs seuls diviseurs communs sont les éléments de A^*.

Définition 2.6 Soient $a, b \in A$. Un *pgcd* (plus grand commun diviseur) de a et b est un élément d de a qui divise a et b, et tel que tout diviseur commun de a et b divise d.

Noter que le pgcd, s'il existe, est bien défini à association près. Par exemple, a et b ont 1 comme pgcd si et seulement s'ils sont premiers entre eux. On observe aussi que le pgcd de a et 0 est a (on peut donc se limiter à des éléments non nuls pour parler de pgcd).

On a l'analogue du théorème de Bezout quand A est *principal* :

Proposition 2.7 *Soit A un anneau principal. Deux éléments a et b de A sont premiers entre eux si et seulement s'il existe u, v dans A tels que $ua + vb = 1$ (i.e. si $A = (a, b) = aA + bA$, idéal engendré par a et b). Plus généralement, deux éléments a et b ont pour pgcd d si et seulement si l'idéal $aA + bB$ est égal à dA.*

On verra que l'existence du pgcd s'étend à tout anneau factoriel, mais la définition via l'idéal (a, b) n'est plus valable dans ce cadre si l'anneau n'est pas principal.

Démonstration : Si $1 = ua + bv$, alors tout diviseur commun de a et b divise 1, donc est inversible (cette implication est vraie dans tout anneau commutatif). En sens inverse, si a et b sont premiers entre eux, alors l'idéal (a, b) s'écrit (d) avec $d \in A$ car A est principal. En particulier d divise a et b, donc est inversible donc $(d) = A$; ceci signifie exactement qu'il existe u, v dans A tels que $ua + vb = 1$.

Supposons maintenant que a et b vérifient $(a, b) = d$, alors d divise par définition a et b, et d s'écrit $d = sa + tb$ avec $s, t \in A$, donc tout diviseur commun de a et b divise aussi d, ce qui fait que d est bien le pgcd de a et b. □

Notons que dans l'anneau $A = K[X, Y]$ (où K désigne un corps), les polynômes X et Y sont premiers entre eux mais ne satisfont pas $A = (X, Y)$ (par exemple parce que tout polynôme de (X, Y) s'annule en $(0, 0)$). Ainsi $K[X, Y]$ n'est pas principal.

On aimerait quand même avoir une théorie de la divisibilité raisonnable pour des anneaux plus généraux que les anneaux principaux. C'est ce qui motive l'introduction de la notion d'anneau factoriel.

Définition 2.8 Un anneau commutatif A est dit *factoriel* s'il vérifie les trois propriétés suivantes :

1. A est intègre.
2. Tout élément non nul a de A s'écrit comme produit

$$a = up_1...p_r \tag{1}$$

   avec $u \in A^*$ et les p_i irréductibles [5].
3. Il y a unicité de cette décomposition au sens suivant : si $a = vq_1...q_s$ en est une autre (avec v inversible et les q_i irréductibles), alors $r = s$ et il existe une permutation σ de $\{1, ..., r\}$ telle que pour tout i de $\{1, ..., r\}$, les éléments p_i et $q_{\sigma(i)}$ soient associés.

Remarque 2.9 a) Comme pour principal, on n'oubliera pas la condition d'intégrité de A.

b) Une autre formulation, souvent plus commode, de l'unicité, est la suivante : fixons un *système de représentants irréductibles* $\mathcal{P}$ de A, i.e. un ensemble d'éléments irréductibles tels que tout irréductible de A soit associé à un et un seul élément de $\mathcal{P}$. Alors tout élément non nul a de A s'écrit d'une

5. Si a n'est pas inversible, le produit des p_i qui apparaît n'est pas un produit vide, et on peut remplacer up_1 par p_1, donc se passer de l'unité u dans la décomposition.

manière unique $a = u \prod_{p \in \mathcal{P}} p^{n_p}$ avec $u \in A^*$, et $(n_p)_{p \in \mathcal{P}}$ famille presque nulle d'entiers naturels. On note alors $n_p = v_p(a)$. Avec cette notation, on a : a divise b si et seulement si $v_p(a) \leq v_p(b)$ pour tout $p \in \mathcal{P}$. Noter qu'en général, l'existence d'un tel $\mathcal{P}$ résulte de l'axiome du choix.

Exemple 2.10 On verra un peu plus loin que tout anneau principal est factoriel. On peut déjà observer que :

a) L'anneau $\mathbf{Z}$ est factoriel, en prenant pour $\mathcal{P}$ l'ensemble des nombres premiers.

b) L'anneau $K[X]$ (où K est un corps) est factoriel en prenant pour $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires.

c) Un sous-anneau d'un anneau factoriel ne le reste pas forcément, puisque tout anneau intègre est un sous anneau de son corps des fractions, lequel est évidemment factoriel.

Il se trouve que la plupart des anneaux intègres que l'on rencontre en algèbre ont la propriété d'existence de la décomposition (la propriété forte est l'unicité). Plus précisément, ceci est lié à la notion suivante :

Proposition 2.11 *Soit A un anneau commutatif (pas forcément intègre). Les trois propriétés suivantes sont équivalentes :*

i) Pour tout idéal I de A, il existe un nombre fini $x_1, ..., x_n$ d'éléments de I tels que $I = \{\sum_{i=1}^{n} a_i x_i, a_i \in A\}$ (autrement dit : tout idéal de A est engendré par un nombre fini d'éléments).

ii) Toute suite croissante $I_1 \subset I_2 \subset ...I_n \subset ...$ d'idéaux est stationnaire (autrement dit : il existe un indice k tel que $I_n = I_k$ pour tout $n \geq k$).

iii) Toute famille non vide E d'idéaux de A possède un élément maximal pour l'inclusion (i.e. un élément I de E tel que si J est dans E et $J \supset I$, alors $J = I$).

On dit que A est noethérien s'il vérifie ces propriétés.

Démonstration : i) implique ii) : soit (I_n) une telle suite, alors la réunion I des I_n est encore un idéal car la famille (I_n) est totalement ordonnée pour l'inclusion (ainsi si x, y sont dans la réunion, il existe un même indice n tel que $x, y \in I_n$; il est alors clair que $x + y$ et ax sont dans I_n pour tout $a \in A$). Soient $x_1, ..., x_r$ des éléments de I qui l'engendrent, alors chaque x_i est dans l'un des I_n, donc il existe n_0 (le plus grand des indices correspondants) tel que I_{n_0} les contienne tous. Alors $I = I_{n_0}$ et la suite (I_n) stationne à I_{n_0}.

ii) implique iii) : si une famille non vide d'idéaux de A n'a pas d'élément maximal, on construit par récurrence une suite infinie strictement croissante d'idéaux de A, ce qui contredit ii).

iii) implique i) : soit I un idéal de A, alors la famille E des idéaux $J \subset I$ qui sont engendrés par un nombre fini d'éléments est non vide (elle contient $\{0\}$). Soit J_0 un élément maximal de E, alors pour tout x de I, l'idéal $J_0 + xA$ est aussi dans E, donc $J_0 + xA = J_0$ par maximalité. Ceci signifie que $x \in J_0$ Finalement $I = J_0$ et I est engendré par un nombre fini d'éléments.

□

Exemple 2.12 a) Via la propriété i), tout anneau principal est noethérien.

b) Si A est noethérien, le quotient A/I de A par un idéal I est noethérien (via la propriété i) et la proposition 1.14).

c) Si A est noethérien, on a aussi $A[X]$ noethérien (cf. [1], partie II, théorème 2.3) et donc par récurrence $A[X_1, ..., X_n]$ noethérien, ce qui implique que la plupart des anneaux qu'on rencontre (qui apparaissent comme quotients d'un anneau de polynômes sur un corps ou sur $\mathbf{Z}$) sont noethériens.

d) L'anneau l'anneau $K[(X_n)_{n \in \mathbf{N}^*}]$ est intègre (donc sous-anneau de son corps des fractions, qui est évidemment noethérien) mais n'est pas noethérien, via la suite strictement croissante d'idéaux

$$(X_1) \subset (X_1, X_2) \subset ... \subset (X_1, ..., X_n) \subset ...$$

Proposition 2.13 *Soit A un anneau intègre noethérien. Alors tout élément non nul a de A admet une décomposition en produit d'irréductibles.* [6]

Démonstration : Soit F l'ensemble des idéaux de A de la forme xA avec x ne s'écrivant pas comme produit d'irréductibles (en particulier, un tel x n'est pas inversible). Si F n'était pas vide, il admettrait un élément maximal $(a) = aA$. En particulier a n'est alors pas irréductible, donc comme il n'est pas inversible il s'écrit $a = bc$ avec b, c dans A non associés à a. Mais alors les idéaux (b) et (c) contiennent strictement (a), donc par maximalité b et c se décomposent en produit d'irréductibles, ce qui contredit le fait que a ne s'écrit pas comme produit d'irréductibles.

□

La proposition suivante donne un critère pour qu'un anneau soit factoriel quand on connaît déjà l'existence de la décomposition en irréductibles.

Proposition 2.14 *Soit A un anneau intègre tel que tout élément non nul de A admette une décomposition en produit d'irréductibles, par exemple un anneau noethérien. Alors les propriétés suivantes sont équivalentes :*

6. C'est ici un léger abus de langage pour dire que tout élément non nul admet une décomposition du type (1), i.e. est produit d'un inversible par un produit d'irréductibles.

1. *A est factoriel.*
2. *Si $p \in A$ est irréductible, alors l'idéal (p) est premier.*
3. *Soient a, b, c dans $A \setminus \{0\}$. Si a divise bc et est premier avec b, alors a divise c ("lemme de Gauss").*

Démonstration : 3. implique 2. : déjà $(p) \neq A$ car p n'est pas inversible puisqu'irréductible. Si maintenant p divise ab et ne divise pas a, alors p est premier avec a puisque p est irréductible (donc un diviseur commun non inversible de a et p serait associé à p, et p diviserait a), d'où p divise b d'après 3. Ainsi (p) est premier.

2. implique 1. : Soit $\mathcal{P}$ un système de représentants irréductibles. Si $u \prod_{p\in\mathcal{P}} p^{m_p} = v \prod_{p\in\mathcal{P}} p^{n_p}$ sont deux décompositions, alors la condition $m_q > n_q$ pour un certain q de $\mathcal{P}$ impliquerait que q divise $\prod_{p\in\mathcal{P}, p\neq q} p^{n_p}$, donc l'un des facteurs d'après 2. Mais q ne peut diviser p pour $p \in \mathcal{P}$ distinct de q car $\mathcal{P}$ est un système de représentants irréductibles. Ainsi $m_p = n_p$ pour tout $p \in \mathcal{P}$, puis $u = v$ par intégrité de A.

1. implique 3. : on décompose a, b, c comme ci-dessus (il y a unicité de la décomposition puisque A est supposé factoriel). Alors pour tout p de $\mathcal{P}$, $v_p(a) \leq v_p(b) + v_p(c)$ (car a divise bc) et $v_p(b) > 0$ implique $v_p(a) = 0$ (car a est premier avec b). Finalement on a $v_p(a) \leq v_p(c)$ aussi bien quand $v_p(b) = 0$ que quand $v_p(b) > 0$. Ainsi a divise c.

□

Exemple 2.15 L'anneau $A = \mathbf{Z}[i\sqrt{5}] = \mathbf{Z}[T]/(T^2 + 5)$, qui est aussi le sous-anneau de $\mathbf{C}$ constitué des $a + bi\sqrt{5}$ avec $a, b \in \mathbf{Z}$, est intègre. Si $z = a+bi\sqrt{5} \in A$, posons $N(z) = |z|^2 = a^2+5b^2$. On observe que $N(z) \in \mathbf{N}$ et que $N(zz') = N(z)N(z')$. En particulier, si $z \in A^*$, alors l'égalité $N(z)N(z') = 1$ implique $N(z) = 1$, ce qui implique que $z = 1$ ou $z = -1$ puisque $N(z) = a^2 + 5b^2$. Comme 1 et -1 sont évidemment inversibles, on a $A^* = \{\pm 1\}$. Un exemple d'irréductible de A est 3, car si $3 = zz'$ avec z, z' dans A, alors $9 = N(3) = N(z)N(z')$, ce qui implique que $N(z) = 1$ vu que $N(z)$ divise 9 et ne peut pas valoir 3 (parce que l'équation $a^2+5b^2 = 3$ n'a pas de solutions avec a, b entiers) ; or $N(z) = 1$ implique comme on l'a vu que $z \in \{\pm 1\}$. On vérifie de même que $2 - i\sqrt{5}$ et $2 + i\sqrt{5}$ sont irréductibles, et aucun des deux n'est associé à 3 puisque $A^* = \{\pm 1\}$. Ainsi, 9 a deux décompositions différentes en produit d'irréductibles : $9 = 3 \times 3 = (2 - i\sqrt{5})(2 + i\sqrt{5})$. Ceci montre que A (qui est nothérien comme quotient d'un anneau noethérien) est un anneau intègre qui n'est pas factoriel.

Theorème 2.16 *Tout anneau principal A est factoriel.*

Démonstration : Comme A est noethérien, on connaît déjà l'existence de la décomposition en irréductibles par la proposition 2.13. Il suffit donc de montrer (en utilisant la caractérisation 2. de la proposition 2.14) que si $p \in A$ est irréductible, alors l'idéal (p) est premier. On va en fait montrer que (p) (qui n'est pas égal à A vu que p n'est pas inversible) est un idéal maximal de A. Soit en effet I un idéal de A contenant strictement A. Soit x un élément de I qui n'est pas dans (p), alors x est premier avec p parce que p est irréductible et ne divise pas x. Du coup, comme A est principal, on peut trouver u, v dans A tels que $ux + vp = 1$, ce qui montre que $1 \in I$ et donc $I = A$.

□

Proposition 2.17 *Si A est un anneau factoriel, alors deux éléments non nuls a et b de A (et plus généralement toute famille d'éléments de $A \setminus \{0\}$) ont un pgcd, bien défini à association près.*

La proposition est immédiate en décomposant a et b suivant un système de représentants $\mathcal{P}$, un pgcd étant $\prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$ (et de même pour une famille quelconque d'éléments de $A \setminus \{0\}$). On étend immédiatement ceci a une famille d'éléments de A, le pgcd étant alors le même que celui de la famille à laquelle on a éventuellement enlevé 0 (le pgcd de la famille vide, ou encore de la famille réduite à 0, est 0). Notons que deux éléments de A sont premiers entre eux si et seulement si leur pgcd est 1.

On a de même un ppcm de a et b (plus petit commun multiple) en prenant $\prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))}$, notion qu'on peut étendre à une famille *finie* d'éléments de $A \setminus \{0\}$.

3. Factorialité d'un anneau de polynômes

Dans ce paragraphe, A désigne un anneau factoriel. On pourra dans une première lecture supposer $A = \mathbf{Z}$ (et donc $\operatorname{Frac} A = \mathbf{Q}$) pour se familiariser avec les notions introduites et les preuves.

Définition 3.1 Le *contenu* (noté $c(P)$) d'un polynôme $P \in A[X]$ est le p.g.c.d. de ses coefficients. P est dit *primitif* si $c(P) = 1$.

On notera que le contenu est défini à multiplication par un inversible de A près, par contre l'idéal qu'il engendre est bien défini. D'autre part, on a immédiatement $c(aP) = a.c(P)$ (mod. A^*) pour tout $a \in A$, ce qui fait que $P/c(P)$ est primitif pour tout polynôme non nul P de $A[X]$.

Lemme 3.2 (Gauss) *Pour tous P, Q de $A[X]$, on a $c(PQ) = c(P)c(Q)$ (toujours modulo A^*).*

Démonstration : Supposons d'abord P et Q primitifs et montrons que PQ est primitif. Sinon il existe un irréductible p de A qui divise tous les coefficients de PQ. Comme P et Q sont primitifs, chacun a au moins un coefficient non divisible par p. Soit a_{i_0} (resp. b_{j_0}) le coefficient de P (resp. Q) d'indice minimal non divisible par p. Alors le coefficient d'indice $i_0 + j_0$ de PQ est somme de termes divisibles par p et de $a_{i_0}b_{j_0}$ donc il n'est pas divisible par p car (p) est premier vu que A est factoriel. Ceci contredit le fait que tous les coefficients de PQ soient divisibles par p.

On se ramène à P, Q primitifs en appliquant le résultat précédent à $P/c(P)$, $Q/c(Q)$.

□

On en déduit l'important résultat suivant :

Theorème 3.3 *Soit A un anneau factoriel de corps des fractions K. Alors les irréductibles de $A[X]$ sont de deux types :*

i) Les polynômes $P = p$ constants avec p irréductible dans A.

ii) Les polynômes primitifs de degré ≥ 1 qui sont irréductibles dans $K[X]$.

En particulier, pour un polynôme primitif de $A[X]$, il revient au même d'être irréductible dans $A[X]$ et dans l'anneau principal $K[X]$ (ce qui n'est pas du tout évident vu qu'il y a a priori plus de décompositions possibles dans $K[X]$). On fera attention avec les polynômes non primitifs : 2 est irréductible dans $\mathbf{Z}[X]$ mais pas dans $\mathbf{Q}[X]$ (il y est inversible) tandis que $2X$ est irréductible dans $\mathbf{Q}[X]$ mais pas dans $\mathbf{Z}[X]$.

Démonstration : Comme on a $A[X]^* = A^*$, il est clair qu'un polynôme constant $P = p$ est irréductible si et seulement si p est irréductible dans A (en effet si un polynôme constant non nul se décompose en produit de deux polynômes de $A[X]$, ces polynômes doivent être constants pour raison de degré).

Si d'autre part P est un polynôme primitif de degré ≥ 1 de $A[X]$ qui est irréductible dans $K[X]$, alors une écriture $P = QR$ avec Q, R dans $A[X]$ implique que Q ou R est constant, par exemple $Q = a \in A$. Alors, a divise le contenu de P, donc $a \in A^*$, c'est-à-dire que Q est inversible dans $A[X]$. Ainsi P est bien irréductible dans $A[X]$ (il n'est pas inversible car de degré au moins 1).

Il reste à montrer qu'un polynôme P de degré ≥ 1 qui est irréductible dans $A[X]$ est primitif, et irréductible dans $K[X]$. Le fait que P soit primitif résulte de ce que $c(P)$ divise P dans $A[X]$ et ne lui est pas associé pour raison de degré. Il reste à montrer que P (qui n'est pas inversible dans $K[X]$)

est irréductible dans $K[X]$. Or si $P = QR$ dans $K[X]$, on peut (vu que $K = \mathrm{Frac}\, A$) écrire $Q = Q_1/q$ et $R = R_1/r$ avec q, r dans A et Q_1, R_1 dans $A[X]$. Alors en posant $a = qr$, on obtient $aP = Q_1 R_1$, et en passant aux contenus : $a = c(Q_1)c(R_1)$ (modulo A^*). Ainsi $P = u\frac{Q_1}{C(Q_1)}\frac{R_1}{C(R_1)}$ avec $u \in A^*$. Comme P est irréductible dans $A[X]$, l'un des polynômes $\frac{P_1}{C(P_1)}$, $\frac{Q_1}{C(Q_1)}$ de $A[X]$ est inversible, donc constant, et l'un des polynômes Q, R est constant ce qui achève la preuve.

□

On en déduit enfin

Theorème 3.4 *Si A est factoriel, $A[X]$ est factoriel.*

Démonstration : On doit d'abord démontrer qu'on a l'existence de la décomposition [7]. Quitte à écrire $P = c(P)P_1$ et à décomposer $c(P)$ en produit d'irréductibles dans A, on se ramène à P primitif. On décompose alors P (qu'on peut supposer non constant) dans l'anneau principal $K[X]$, soit $P = P_1...P_r$, ou encore $aP = Q_1...Q_r$ avec $Q_i \in A[X]$, $a \in A$, et Q_i irréductible dans $K[X]$. En passant aux contenus, on obtient $a = c(Q_1)...c(Q_r)$ (mod. A^*) et d'après le théorème précédent $P = u.\prod_{i=1}^{r} \frac{Q_i}{c(Q_i)}$ (avec $u \in A^*$) est une décomposition de P en produits d'irréductibles de $A[X]$, puisque chaque $\frac{Q_i}{c(Q_i)}$ est un polynôme primitif de $A[X]$ qui est irréductible dans $K[X]$ (il est le produit de Q_i par une constante de K^*).

Il suffit donc d'après la proposition 2.14 de montrer que si $P \in A[X]$ est irréductible, alors (P) est premier. Si $P = p$ est une constante irréductible de $A[X]$, alors p n'est pas inversible et si p divise un produit QR de deux polynômes de $A[X]$, alors il divise aussi le contenu $c(QR) = c(Q)c(R)$, donc il divise $c(Q)$ ou $c(R)$ vu que (p) est premier dans A (puisque A est factoriel). Ainsi la constante p divise bien Q ou R dans $A[X]$ (on aurait pu aussi remarquer que $A[X]/(p)$ est isomorphe à $(A/(p))[X]$, qui est intègre vu que (p) est premier dans A).

Supposons donc P primitif de degré au moins 1, et donc irréductible dans $K[X]$ d'après le théorème précédent. Alors si P divise le produit QR de deux polynômes de $A[X]$, il divise Q ou R dans $K[X]$ vu que $K[X]$ est principal, par exemple Q. Il existe donc a dans A tel que $aQ = SP$ avec $S \in A[X]$. Alors $ac(Q) = c(S)$ (mod. A^*) car P est primitif, et a divise $c(S)$. En particulier $Q = (S/a)P$ avec S/a dans $A[X]$, i.e. P divise Q dans $A[X]$. C'est ce qu'on voulait montrer.

□

7. Noter que A n'est pas forcément noethérien

Corollaire 3.5 *Si A est factoriel, $A[X_1, ..., X_n]$ est factoriel.*[8] *Ceci s'applique en particulier si A est un corps.*

Il est commode d'avoir un critère pratique d'irréductibilité dans les anneaux factoriels. Le résultat suivant est souvent utile :

Theorème 3.6 (Critère d'Eisenstein) *Soient A un anneau factoriel, P un polynôme non constant de $A[X]$, p irréductible dans A. On pose $P = \sum_{k=0}^{n} a_k X^k$ et on suppose :*

1. *p ne divise pas a_n.*
2. *p divise a_k pour $0 \leq k \leq n-1$.*
3. *p^2 ne divise pas a_0.*

Alors P est irréductible dans $K[X]$ (donc aussi dans $A[X]$ s'il est primitif).

Démonstration : Notons que $P/c(P)$ vérifie les mêmes hypothèse que P vu que $c(P)$ n'est pas divisible par p via 1. On peut donc supposer P primitif et $\deg P \geq 2$. Si P n'était pas irréductible, il s'écrirait (d'après le théorème 3.3) $P = QR$ avec Q, R non constants dans $A[X]$. Posons $Q = b_r X^r + ... + b_0$, $R = c_s X^s + ... + c_0$. L'anneau $B = A/(p)$ est intègre, et $A[X]/pA[X]$ est isomorphe à $B[X]$. Dans $A[X]/pA[X]$, on a $\overline{P} = \overline{QR}$, soit $\bar{a}_n X^n = \overline{Q}.\overline{R}$ dans $B[X]$. On a $\bar{a}_n \neq 0$ dans B, donc $\bar{b}_r$ et $\bar{c}_s$ sont aussi non nuls. Ainsi $\overline{Q}$ et $\overline{R}$ ne sont pas constants et l'égalité $\bar{a}_n X^n = \overline{Q}.\overline{R}$ dans l'anneau principal (donc factoriel) $(\mathrm{Frac}\, B)[X]$ implique alors (comme X est irréductible dans cet anneau) que $\overline{Q}$ et $\overline{R}$ sont divisibles par X dans $(\mathrm{Frac}\, B)[X]$. Cela signifie que p divise b_0 et c_0, ce qui contredit le fait que a_0 n'est pas divisible par p^2.

□

Exemple 3.7 a) Le polynôme $X^{18} - 4X^7 - 2$ est irréductible dans $\mathbf{Q}[X]$ et $\mathbf{Z}[X]$.

b) Le polynôme $X^5 - XY^3 - Y$ est irréductible dans $\mathbf{C}[X, Y]$ (prendre $A = \mathbf{C}[Y]$ et $p = Y$).

c) Il existe des polynômes irréductibles de tout degré dans $\mathbf{Q}[X]$ (ou $\mathbf{Z}[X]$), en prenant par exemple $X^d + pX + p$ pour $d \in \mathbf{N}^*$ et p premier.

8. On a l'analogue avec une infinité d'indéterminées, c'est immédiat à partir du cas fini.

d) Si p est un nombre premier, alors $R := 1 + X + ... + X^{p-1} = \frac{X^p-1}{X-1}$ est irréductible dans $\mathbf{Q}[X]$ ou $\mathbf{Z}[X]$: on applique le critère d'Eisenstein au polynôme

$$R(X+1) = \frac{(X+1)^p - 1}{X} = p + C_p^2 X + ... + X^{p-1}.$$

4. A-algèbres. Algèbres de polynômes

4.1. Notion de A-algèbre

Définition 4.1 Une *A-algèbre* est un anneau commutatif[9] B équipé d'un morphisme d'anneaux (pas forcément injectif) $\varphi : A \to B$.

Notons que B est alors munie d'une loi externe (qui en fait un A-module) définie par $a.b = \varphi(a)b$ pour tous $a \in A, b \in B$. On peut alors poser :

Définition 4.2 Un *morphisme de A-algèbres* $f : B \to C$ est un morphisme d'anneaux qui vérifie de plus $f(a.b) = a.f(b)$ pour tous $a \in A, b \in B$. Une sous-A-algèbre de B est un sous-anneau C de B qui vérifie de plus $a.c \in C$ pour tous $a \in A, c \in C$.

Noter que l'image d'un morphisme $f : B \to C$ de A-algèbres est une sous A-algèbre de B, et le noyau $\ker f$ est un idéal de l'anneau B. Le théorème de factorisation s'étend immédiatement aux morphismes de A-algèbres.

Exemple 4.3 a) Tout anneau commutatif B est ipso facto une $\mathbf{Z}$-algèbre via le morphisme $n \mapsto n.1$ de $\mathbf{Z}$ dans B.

b) L'anneau $A[X_1, ...X_n]$ est une A-algèbre via l'injection canonique $A \to A[X_1, ...X_n]$.

c) L'anneau produit A^n est une A-algèbre via l'application diagonal $a \mapsto (a, a, ..., a)$ de A dans A^n.

4.2. Algèbres de polynômes, propriété universelle

Rappelons qu'un élément P de l'anneau commutatif $A[X_1, ..., X_n]$ s'écrit de manière unique :

9. On peut définir la même notion en ne supposant pas l'anneau B commutatif, ou même en demandant juste que B soit un A-module équipé d'une forme A-bilinéaire, mais dans ce cours nous n'aurons à considérer que des A-algèbres qui sont des anneaux commutatifs.

$$P = \sum_{(i_1,...,i_n)\in\mathbf{N}^n} a_{i_1,...,i_n} X_1^{i_1} ... X_n^{i_n}, \tag{2}$$

où $(a_{i_1,...,i_n})_{(i_1,...,i_n)\in\mathbf{N}^n}$ est une famille presque nulle d'éléments de A indexée par $\mathbf{N}^n$ (avec la convention $X_i^0 = 1$). Cela permet pour chaque $r \in \{1, ..., n\}$ de voir aussi les éléments de $A[X_1, ..., X_n]$ comme des éléments de $(A[X_1, ..., \widehat{X_r}, ..., X_n])[X_r]$ (la notation $A[X_1, ..., \widehat{X_r}, ..., X_n]$ signifie qu'on omet le terme X_r).

Définition 4.4 On dit qu'un polynôme P de $A[X_1, ..., X_n]$ est *homogène de degré d* si dans l'écriture (2) ci-dessus, tous les $a_{i_1,...,i_n}$ non nuls correspondent à des multi-indices (appelés aussi *exposants*) $(i_1, ..., i_n)$ tels que $\sum_{k=1}^n i_k = d$.

Tout polynôme $F \in A[X_1, ..., X_n]$ s'écrit ainsi de façon unique $P = \sum_{d\geq 0} F_d$ avec F_d homogène de degré d et la famille des F_d presque nulle

Proposition 4.5 (Propriété universelle des algèbres de polynômes) *Soit B un anneau commutatif. Soit $\varphi : A \to B$ un morphisme d'anneaux. Soient $b_1, ..., b_n$ des éléments de B. Alors, il existe un unique morphisme d'anneaux $f : A[X_1, ..., X_n] \to B$ vérifiant :*

1. Pour tout polynôme constant a de $A[X_1, ..., X_n]$, on a $f(a) = \varphi(a)$.

2. On a $f(X_i) = b_i$ pour tout $i \in \{1, ..., n\}$.

Autrement dit, si on considère B comme une A-algèbre via φ, il existe un unique morphisme de A-algèbres $f : A[X_1, ..., X_n] \to B$ envoyant X_i sur b_i.

Une fois fixé le morphisme φ (i.e. la structure de A-algèbre de B), on peut noter (pour tout polynôme P de $A[X_1, ..., X_n]$) $P(b_1, ..., b_n)$ l'élément de B obtenu en prenant l'image de P par le morphisme f du théorème. Il s'obtient en "substituant" $b_1, ..., b_n$ aux indéterminées $X_1, ..., X_n$, puis en utilisant la structure de A-algèbre de B.

Démonstration : On démontre la proposition par récurrence sur $n \geq 1$. Supposons d'abord $n = 1$. Alors, le morphisme $f : A[X_1] \to B$ doit nécessairement être défini par la formule

$$f(\sum_{n\in\mathbf{N}} \alpha_n X_1^n) = \sum_{n\in\mathbf{N}} \varphi(\alpha_n) b_1^n.$$

Réciproquement, il est immédiat que f vérifie alors $f(1) = 1$ et $f(P + Q) = f(P) + f(Q)$ pour tous polynômes P, Q de $A[X_1]$. Si $P = \sum_n \alpha_n X_1^n$ et

$Q = \sum_n \beta_n X_1^n$ sont deux polynômes, alors $PQ = \sum_n \gamma_n X_1^n$ avec $\gamma_n = \sum_{p+q=n} \alpha_p \beta_q$, d'où

$$f(PQ) = \sum_n \varphi(\gamma_n) b_1^n = \sum_n \sum_{p+q=n} \varphi(\alpha_p)\varphi(\beta_q) b_1^p b_1^q =$$

$$\sum_n \sum_{p+q=n} (\varphi(\alpha_p) b_1^p)(\varphi(\beta_q) b_1^q) = \sum_{p,q} (\varphi(\alpha_p) b_1^p)(\varphi(\beta_q) b_1^q) =$$

$$(\sum_n \varphi(\alpha_n) b_1^n))(\sum_n \varphi(\beta_n) b_1^n)) = f(P) f(Q),$$

ce qui montre que f est bien un morphisme d'anneaux. Ceci conclut le cas $n = 1$.

Supposons maintenant le résultat acquis pour $n-1$ et montrons-le pour n. Par hypothèse de récurrence, on a un unique morphisme d'anneaux $\psi : A[X_1, ..., X_{n-1}] \to B$ tel que $\psi(X_i) = b_i$ pour $1 \leq i \leq n-1$ et ψ coïncide avec φ sur les polynômes constants. D'après le cas $n = 1$ (appliqué aux polynômes en une indéterminée à coefficients dans l'anneau $A[X_1, ..., X_{n-1}]$), on a alors un unique morphisme d'anneaux $f : A[X_1, ..., X_n] \to B$ qui coïncide avec ψ sur les polynômes de $A[X_1, ..., X_{n-1}]$ et vérifie $f(X_n) = b_n$. Il est alors évident que f convient et est l'unique solution du problème.

□

Exemple 4.6 Soient F, G deux polynômes de $A[X]$. Alors le polynôme $F \circ G$ est défini en "substituant" G à la place de X dans F, c'est-à-dire que $F \circ G$ est l'image de F par l'unique morphisme de A-algèbres de $A[X]$ dans lui-même qui envoie X sur G.

Définition 4.7 Soit B une A-algèbre. Soit S une partie de B. La sous-A-algèbre de B *engendrée par* S est l'ensemble C des $P(x_1, ..., x_n)$ avec $n \in \mathbf{N}^*$ quelconque, $x_1, ..., x_n \in S$ et $P \in A[X_1, ..., X_n]$. C'est la plus petite sous-A-algèbre de B contenant S.

Proposition 4.8 *Soit B une A-algèbre. Alors il existe une partie finie $S = \{b_1, ..., b_n\}$ de B engendrant B si et seulement si B est isomorphe au quotient de $A[X_1, ..., X_n]$ par un idéal I. On dit alors que la A-algèbre B est engendrée par une partie finie.* [10]

10. On peut aussi dire "de type fini", mais il y a alors une ambiguïté entre être de type fini comme A-algèbre et comme A-module. Typiquement, si par exemple K est un corps, $K[X]$ est de type fini comme K-algèbre mais pas comme K-espace vectoriel.

Démonstration : Il est immédiat que la A-algèbre $A[X_1, ..., X_n]/I$ est engendrée par les images de $X_1, ..., X_n$ via la surjection canonique, qui constituent donc une partie finie l'engendrant. En sens inverse, si B est une A-algèbre engendrée par $S = \{b_1, ..., b_n\}$, il existe d'après la proposition 4.5 un (unique) morphisme de A-algèbres $f : A[X_1, ..., X_n] \to B$ envoyant X_i sur b_i. L'image de f contient les b_i, donc est égale à B (qui est engendrée par les b_i). On conclut avec le théorème de factorisation.

□

4.3. Polynômes symétriques

Soit A un anneau commutatif. Soit $\sigma \in \mathcal{S}_n$. D'après la proposition 4.5, il existe un unique morphisme de A-algèbres $\varphi_\sigma : A[X_1, ..., X_n] \to A[X_1, ..., X_n]$ qui envoie chaque X_i sur $X_{\sigma(i)}$. On vérifie tout de suite que pour σ, τ dans $\mathcal{S}_n$, on a $\varphi_{\sigma\tau} = \varphi_\sigma \circ \varphi_\tau$. Autrement dit, on a :

Proposition 4.9 *La formule $\sigma.P := \varphi_\sigma(P)$ définit une opération du groupe symétrique $\mathcal{S}_n$ sur $A[X_1, ..., X_n]$.*

Il s'agit d'une opération par automorphismes de A-algèbres, la réciproque de φ_σ étant $\varphi_{\sigma^{-1}}$. Explicitement, on a

$$(\sigma.P)(X_1, ..., X_n) = P(X_{\sigma(1)}, ...X_{\sigma(n)}).$$

Définition 4.10 On dit qu'un polynôme $P \in A[X_1, ..., X_n]$ est *symétrique* si on a $\sigma.P = P$ pour tout $\sigma \in \mathcal{S}_n$. On note $A[X_1, ..., X_n]^{\mathcal{S}_n}$ la sous-A-algèbre de $A[X_1, ..., X_n]$ constituée des polynômes symétriques.

Proposition 4.11 *Soit K un corps. Notons $K(X_1, ..., X_n)^{\mathcal{S}_n}$ le sous-corps de $K(X_1, ..., X_n) = \mathrm{Frac}\,(K[X_1, ...X_n])$ constitué des fractions rationnelles symétriques (i.e. fixes pour l'action de $\mathcal{S}_n$). Alors*

$$K(X_1, ..., X_n)^{\mathcal{S}_n} = \mathrm{Frac}\,(K[X_1, ..., X_n]^{\mathcal{S}_n}).$$

Démonstration : Il est immédiat que le quotient de deux polynômes symétriques est une fraction rationnelle symétrique, d'où $\supset$. En sens inverse, soit $R = P/Q$ une fraction rationnelle symétrique avec P, Q dans $K[X_1, ..., X_n]$ et Q non nul. On peut supposer $R \neq 0$. On note alors que

$$R = \frac{\prod_{\sigma \in \mathcal{S}_n} \sigma.P}{(\prod_{\sigma \in (\mathcal{S}_n \setminus \mathrm{Id})} P)Q}$$

est une écriture de R comme quotient de deux polynômes symétriques. C'est clair pour le numérateur P_1, et pour le dénominateur Q_1 cela résulte de ce que $Q_1 = P_1/R_1$, où P_1 et R_1 sont des fractions rationnelles symétriques.

□

Définition 4.12 Soit $k \in \{1, ..., n\}$ un entier. On définit le k-ième *polynôme symétrique élémentaire en n indéterminées* par

$$\sigma_k := \sum_{I \subset \{1,...,n\}, \#I=k} \prod_{i \in I} X_i.$$

En particulier, on a $\sigma_1 = X_1 + ... + X_n$ et $\sigma_n = X_1...X_n$. On remarque que dans l'anneau $A[X_1, ..., X_n][X]$, on a aussi

$$\prod_{i=1}^{n}(X - X_i) = \sum_{k=0}^{n}(-1)^k \sigma_k X^{n-k},$$

en convenant que $\sigma_0 = 1$. Le polynôme σ_k est homogène de degré k.

Le principal résultat sur les polynômes symétriques est le théorème de structure suivant :

Theorème 4.13 *Soit $\Phi : A[X_1, ...X_n] \to A[X_1, ...X_n]$ le morphisme de A-algèbres qui envoie chaque X_k sur le polynôme symétrique élémentaire σ_k. Alors Φ induit un isomorphisme de $A[X_1, ...X_n]$ sur $A[X_1, ...X_n]^{\mathcal{S}_n}$.*

Autrement dit : pour tout polynôme symétrique en n indéterminées R, il existe un unique polynôme en n indéterminées P tel que $R = P(\sigma_1, ..., \sigma_n)$, où les σ_i sont les polynômes symétriques élémentaires. Noter que du coup, les A-algèbres $A[X_1, ...X_n]$ et $A[X_1, ...X_n]^{\mathcal{S}_n}$ sont isomorphes, bien que la deuxième soit strictement incluse dans la première !

Démonstration : a) Surjectivité. Soit $F \in A[X_1, ..., X_n]$ symétrique, on veut montrer qu'il est dans l'image de Φ. On peut supposer F non nul, on peut alors écrire $F = \sum_{d=0}^{r} F_d$ avec $r \in \mathbf{N}$ et chaque F_d homogène de degré d (avec de plus $F_d \neq 0$). Pour tout $\tau \in \mathcal{S}_n$, on a alors

$$\tau.F = \sum_{d=0}^{r} \tau.F_d = F = \sum_{d=0}^{r} F_d,$$

avec $\tau.F_d$ et F_d homogènes de degré d, ce qui implique immédiatement $\tau.F_d = F_d$ pour tout d, autrement dit chaque F_d est symétrique. On se ramène ainsi

au cas où le polynôme symétrique F est homogène de degré $d \geq 0$. On procède alors par récurrence sur $n + d$.

Si $n = 1$ ou $d = 0$, il n'y a rien à démontrer et si $d = 1$, le polynôme F est un multiple de σ_1. Supposons donc d et n au moins égaux à 2. Montrons un lemme :

Lemme 4.14 *Soit $G = G(X_1, ..., X_n)$ un polynôme symétrique tel que*

$$G(X_1, ..., X_{n-1}, 0) = 0.$$

Alors G s'écrit $G = \sigma_n H$, avec H symétrique.

Preuve du lemme : En utilisant l'écriture[11] usuelle d'un polynôme en n indéterminéees, on voit que G s'écrit $G = X_n G_1$ avec $G_1 \in A[X_1, ..., X_n]$. Comme G est symétrique, il vérifie aussi

$$G(X_1, ..., X_{i-1}, 0, X_{i+1}, ..., X_n) = 0$$

pour tout i, en particulier $G_1(X_1, ..., 0, X_n) = 0$ vu que X_n n'est pas diviseur de zéro dans $A[X_1, ..., X_n]$. Le même raisonnement montre alors que $G_1 = X_{n-1} G_2$ avec $G_2 \in A[X_1, ..., X_n]$, et on recommence jusqu'à obtenir

$$G = (X_n X_{n-1} ... X_1) H = \sigma_n H$$

avec $H \in A[X_1, ..., X_n]$. De plus H est symétrique car pour toute permutation $\tau \in \mathcal{S}_n$, on a $\tau.G = G = \sigma_n H = \sigma_n(\tau.H)$, d'où $\tau.H = H$ vu que σ_n n'est pas diviseur de 0 dans $A[X_1, ..., X_n]$.

□

Reprenons la preuve de la surjectivité de Φ. Posons $F_1(X_1, ..., X_{n-1}) = F(X_1, ..., X_{n-1}, 0)$, c'est un polynôme symétrique en $n-1$ indéterminées (les permutations de $\{1, ..., n-1\}$ s'identifiant aux permutations de $\{1, ..., n\}$ qui laissent fixe n). Supposons d'abord que $F_1 = 0$, on peut alors appliquer le lemme à F, ce qui permet d'écrire $F = \sigma_n H$ avec H symétrique homogène de degré $d - n$ (en n indéterminées). Il suffit alors d'appliquer l'hypothèse de récurrence à H (car $n + (d - n) = d < n + d$), ce qui donne le résultat.

Supposons maintenant $F_1 \neq 0$, c'est un polynôme homogène de degré d en $n - 1$ indéterminées et on peut donc lui appliquer l'hypothèse de récurrence, ce qui permet d'écrire

$$F_1 = Q(\sigma'_1, ..., \sigma'_{n-1}),$$

11. Attention, A n'est pas supposé intègre, donc des raisonnements à base de divisibilité n'ont pas de sens stricto sensu.

où $Q \in A[X_1, ..., X_{n-1}]$ et $\sigma'_k = \sigma_k(X_1, ..., X_{n-1}, 0)$ est le k-ième polynôme symétrique élémentaire en $n-1$ indéterminées. Posons alors

$$G = F(X_1, ..., X_n) - Q(\sigma_1, ..., \sigma_{n-1}).$$

Alors, G est symétrique en n indéterminées et vérifie $G(X_1, ..., X_{n-1}, 0) = 0$, donc d'après ce qu'on a vu précédemment G est dans l'image de Φ. Comme $Q(\sigma_1, ..., \sigma_{n-1})$ est de manière évidente aussi dans cette image, on en conclut bien que $F \in \operatorname{Im} \Phi$.

b) Injectivité de Φ. Soit $Q \in A[X_1, ..., X_n]$ tel que $Q(\sigma_1, ..., \sigma_n) = 0$, il s'agit de démontrer que Q est nul. On procède par récurrence sur n. Pour $n = 1$ c'est clair vu que $\sigma_1 = X_1$. Supposons le résultat vrai pour $n-1$. En regardant Q comme un polynôme de $A[X_1, ..., X_{n-1}][X_n]$, on peut écrire :

$$Q = \sum_{k \in \mathbf{N}} Q_k X_n^k,$$

avec $Q_k \in A[X_1, ..., X_{n-1}]$. Raisonnons par l'absurde en supposant $Q \neq 0$, alors il existe un plus petit entier l tel que $Q_l \neq 0$, et alors

$$0 = Q(\sigma_1, ..., \sigma_n) = \sigma_n^l \sum_{k \geq l} Q_k(\sigma_1, ..., \sigma_{n-1}) \sigma_n^{k-l}.$$

Comme σ_n n'est pas diviseur de zéro dans $A[X_1, ..., X_n]$, on obtient

$$\sum_{k \geq l} Q_k(\sigma_1, ..., \sigma_{n-1}) \sigma_n^{k-l} = 0,$$

et en substituant 0 à X_n, cela donne

$$Q_l(\sigma'_1, ..., \sigma'_{n-1}) = 0,$$

ce qui entraîne $Q_l = 0$ par hypothèse de récurrence, contradiction.

□

Corollaire 4.15 *Soit K un corps. Alors $K(X_1, ...X_n)$ et $K(X_1, ..., X_n)^{\mathcal{S}_n}$ sont isomorphes (en tant que corps et aussi en tant que K-algèbres).*

Démonstration : Cela résulte du théorème 4.13 et de la proposition 4.11.

□

Remarque 4.16 (culturelle) Soit G un sous-groupe de $\mathcal{S}_n$. On peut se demander si le corollaire précédent vaut encore si on remplace $K(X_1, ..., X_n)^{\mathcal{S}_n}$

par le sous-corps de $K(X_1, ..., X_n)$ constitué des fractions rationnelles invariantes pour l'action de G. C'est en fait : faux en général (par exemple pour $K = \mathbf{Q}$, $n = 8$, et G le groupe engendré par un 8-cycle, Swan 1969), vrai si $K = \mathbf{C}$ et G est abélien (Fisher, 1915), et à nouveau faux si $K = \mathbf{C}$ et G n'est pas abélien (Saltman, 1984). Pour $K = \mathbf{C}$ et $G = \mathcal{A}_n$, la question est encore ouverte ! Pour ce qui est de la question analogue concernant l'anneau $K[X_1, ..., X_n]^G$, elle a été résolue par Chevalley (1955), qui a donné une condition sur G pour que cette K-algèbre soit isomorphe à $K[X_1, ..., X_n]$.

D'autres polynômes symétriques intéressants sont les sommes de Newton :

Définition 4.17 Pour tout entier $k \geq 1$, on définit les *sommes de Newton* (en n indéterminées)

$$s_k = \sum_{i=1}^{n} X_i^k$$

Ce sont des polynômes symétriques, homogènes de degré k.

L'énoncé suivant fait le lien entre polynômes symétriques élémentaires et sommes de Newton dans l'anneau $A[X_1, ..., X_n]$.

Theorème 4.18 (Formules de Newton) *a) Supposons $k \geq n$. Alors*

$$s_k - \sigma_1 s_{k-1} + ... + (-1)^n \sigma_n s_{k-n} = 0.$$

(pour $k = n$, on convient que $s_0 = k = n$).

b) Supposons $1 \leq k \leq n$. Alors

$$s_k - \sigma_1 s_{k-1} + ... + (-1)^{k-1} \sigma_{k-1} s_1 + (-1)^k k \sigma_k = 0.$$

On fera attention au dernier terme dans le cas b), qui n'est pas $(-1)^k \sigma_k s_0$ (lequel donnerait plutôt $(-1)^k n \sigma_k$, ce qui est erroné).

Démonstration : a) Soit

$$Q = \prod_{i=1}^{n} (X - X_i) = X^n - \sigma_1 X^{n-1} + ... + (-1)^n \sigma_n.$$

En évaluant en $X = X_i$, on obtient (dans l'anneau $A[X_1, ..., X_n]$) :

$$X_i^n - \sigma_1 X_i^{n-1} + ... + (-1)^n \sigma_n = 0.$$

Pour $k \geq n$, en multipliant par X_i^{k-n}, on trouve

$$X_i^k - \sigma_1 X_i^{k-1} + ... + (-1)^n \sigma_n X_i^{k-n} = 0,$$

d'où on tire la formule en sommant de $i = 1$ à $i = n$.

b) Pour $k = n$, la formule a déjà été démontrée en a), supposons donc $k < n$. Posons

$$S = s_k - \sigma_1 s_{k-1} + ... + (-1)^k k\sigma_k,$$

le polynôme S est homogène de degré k. On observe que

$$S(X_1, ..., X_k, 0, ..., 0) = 0,$$

car cette identité correspond précisément au cas a) de la formule de Newton en degré k dans $A[X_1, ..., X_k]$ (c'est pour cela que c'est bien le terme $(-1)^k k\sigma_k$ qui apparaît à la fin et non $(-1)^k n\sigma_k$) : en effet, pour $r = 1, ..., k$, le polynôme $\sigma_r(X_1, ..., X_k, 0, ..., 0)$ est le r-ième polynôme symétrique en k indéterminées et $s_r(X_1, ..., X_k, 0, ..., 0)$ est la r-ième somme de Newton en k indéterminées. Écrivons maintenant S sous la forme (2) :

$$S = \sum_{(\alpha_1,...,\alpha_n) \in \mathbf{N}^n} a_{\alpha_1,...,\alpha_n} X_1^{\alpha_1} ... X_n^{\alpha_n}.$$

L'égalité $S(X_1, ..., X_k, 0, ..., 0) = 0$ donne alors que tous les coefficients du type $a_{\alpha_1,...,\alpha_k,0,...,0}$ sont nuls. Par ailleurs tous les exposants $\alpha = (\alpha_1, ..., \alpha_n)$ qui apparaissent dans S vérifient $|\alpha| = k$, et en particulier comportent au plus k entiers non nuls parmi les α_i. Comme S est de plus symétrique, on obtient finalement que tous les $a_{\alpha_1,...,\alpha_n}$ sont nuls, d'où $S = 0$.

□

Remarque 4.19 Quand A est un corps de caractéristique zéro (ou plus généralement un anneau contenant un corps de caractéristique zéro comme sous-anneau, ce qui correspond au fait que pour tout entier $n > 0$, l'élément $n.1$ est inversible dans A), les formules de Newton (cas b) permettent de calculer les σ_k en fonction des s_k en résolvant un système linéaire de Cramer triangulaire :

$$\sigma_1 = s_1; \quad 2\sigma_2 = \sigma_1 s_1 - s_2; \quad 3\sigma_3 = \sigma_2 s_1 - \sigma_1 s_2 + s_3 \quad ...$$

Il en résulte que dans ce cas, tout polynôme symétrique de $A[X_1, ..., X_n]$ s'écrit aussi de manière unique comme un polynôme en les s_k.

Comme application de la remarque précédente, on a l'exercice classique : si une matrice $A \in M_n(\mathbf{C})$ vérifie $\mathrm{Tr}\,(A^k) = 0$ pour $1 \leq k \leq n$, alors A est nilpotente. En effet, si $\lambda_1, ..., \lambda_n$ sont les valeurs propres de A, on obtient $s_k(\lambda_1, ..., \lambda_n) = 0$ pour $1 \leq k \leq n$, et donc $\sigma_k(\lambda_1, ..., \lambda_n) = 0$ pour $1 \leq k \leq n$; on en déduit que le polynôme caractéristique Q de A est $\prod_{i=1}^{n}(X - \lambda_i) = X^n$, d'où le résultat (par exemple avec le théorème de Cayley-Hamilton). Ceci vaut plus généralement si on remplace $\mathbf{C}$ par un corps K de caractéristique zéro (à condition de savoir qu'il existe une extension $L \supset K$ sur laquelle Q est scindé).

Références

[1] D. Perrin : *Cours d'algèbre*, Ellipses 1996.