M1 algèbre 2023-2024 : Anneaux commutatifs

David Harari

Table des matières

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.
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*.

Exemple 1.2 a) L'anneau nul $\{0\}$.

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

c) Un corps K est par définition un anneau *commutatif*[1], distinct de $\{0\}$, tel que tout élément non nul ait un inverse pour la multiplication (autrement dit on demande que $K \setminus \{0\}$ soit un groupe commutatif).

d) Le produit direct $\prod_{i \in I} A_i$ d'une famille d'anneaux $(A_i)_{i \in I}$ est un anneau (pour les lois évidentes).

e) Si A est un anneau *commutatif*[2], on dispose de l'*anneau des polynômes en n indéterminées* $A[X_1, ..., X_n]$ qui est commutatif. Nous l'étudierons plus en détails dans la section 3.

f) 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^*.

On fera attention à ne pas noter de la même façon l'ensemble des éléments non nuls de A, qu'on notera plutôt $A \setminus \{0\}$.

Exemple 1.4 a) $(\mathbf{Z}/n\mathbf{Z})^*$ est l'ensemble des classes $\bar{m}$, avec m premier à n.

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

c) Si K est un corps, alors $K[X_1, ..., X_n]^*$ est l'ensemble des polynômes constants non nuls (qui est isomorphe au groupe multiplicatif K^*).

d) Si K est un corps, on a $M_n(K)^* = \mathrm{GL}_n(K)$.

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

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

1. D'après la convention déjà adoptée dans les autres parties du cours.

2. 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.

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

Définition 1.6 Une partie A de B est un *sous-anneau* si $(B, +, .)$ est un anneau *possédant le même élément unité que* A. Il est équivalent de dire que $1 \in B$, et que $(B, +)$ est un sous-groupe de $(A, +)$ qui est stable par multiplication interne.

On fera bien attention à la condition $1 \in B$, par exemple l'ensemble des $(x, 0)$ avec $x \in \mathbf{Z}$ n'est pas un sous-anneau de $\mathbf{Z} \times \mathbf{Z}$, et l'anneau nul n'est pas un sous-anneau d'un anneau non nul. Comme on va le voir, la notion de sous-anneau n'est souvent pas la plus intéressante, c'est celle d'idéal qui est la plus utile.

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 1.7 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 $ax \in I$.

On prendra garde de ne pas confondre cette notion avec celle de sous-anneau. En particulier un idéal de A contient 1 (ou encore un élément inversible de A) si et seulement s'il est égal à A.

Exemple 1.8 a) $\{0\}$ et A sont des idéaux de A. Ce sont les seuls si A est un corps.

b) Les idéaux de $\mathbf{Z}$ sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$.

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. Notons que si f n'est pas surjective, l'image directe d'un idéal de A par f n'est pas forcément un idéal de B (prendre pour f l'injection canonique de $\mathbf{Z}$ dans $\mathbf{Q}$). Par contre l'image $\operatorname{Im} f$ de f est un sous-anneau de B, dont $f(I)$ est un idéal pour tout idéal I de A.

d) Si E est une partie quelconque d'un anneau commutatif A, alors l'ensemble $(a_1, ..., a_n)$ des éléments de A de la forme $a_1x_1 + ... + a_nx_n$ avec $x_i \in E$ et $a_i \in A$ est un idéal, appelé *idéal engendré* par E ; c'est le plus petit idéal de A contenant E. On notera (a) ou aA l'idéal engendré par un élément a de A. Plus généralement, l'idéal engendré par une partie B de A est l'ensemble des combinaisons linéaires d'éléments de B à coefficients dans A.

Remarque 1.9 Contrairement à ce qui se passe pour les espaces vectoriels, un idéal J inclus dans un idéal I engendré par n éléments ne peut pas forcément être engendré par n éléments, par exemple l'idéal A est toujours engendré par 1 alors que certains idéaux peuvent ne pas être principaux (i.e. engendrés par un seul élément). En fait, il se peut même que J ne soit pas engendré par un nombre fini d'éléments. On verra toutefois que pour certains types d'anneaux particuliers (principaux, noethériens), ces problèmes disparaissent, au moins partiellement.

Proposition 1.10 *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 $\bar{1}$.*

Démonstration : Le seul point non trivial est que l'élément $\overline{ab}$ de A/I ne dépend pas du choix des représentants a, b. Or si $\bar{a} = \bar{a}'$ et $\bar{b} = \bar{b}'$, alors il existe i, j dans I avec $a' = a + i$, $b' = b + j$ d'où $a'b' = ab + (aj + ib + ij)$ avec $(aj + ib + ij) \in I$.

□

On a alors immédiatement le théorème de factorisation habituel :

Theorème 1.11 *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 1.12 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 $\mathbf{C}$!).

c) Si K est un corps, l'anneau $K[X]/(X^2)$ possède un élément ε non nul (la classe de X) tel que $\varepsilon^2 = 0$. On note cet anneau $K[\varepsilon]$ (en effet il est engendré en tant que K-algèbre par l'élément ε, cf. paragraphe 3.2.).

Remarque 1.13 On montre, comme dans l'étude des sous-groupes d'un groupe quotient, l'énoncé suivant : les idéaux de A/I sont les J/I (ce sont a priori des groupes abéliens, mais on voit tout de suite qu'ils sont des idéaux), où J est un idéal de A contenant I. De plus, l'anneau quotient de A/I par l'idéal J/I est isomorphe à A/J. Plus généralement, si B est un idéal de A, alors son image par la surjection canonique $A \to A/I$ est l'idéal $(B+I)/I$ de A/I. Un exemple simple est celui des idéaux de $\mathbf{Z}/n\mathbf{Z}$, qui sont les $d\mathbf{Z}/\mathbf{Z}$ avec d divisant n. On a également $(B+I)/I$ isomorphe à $B/(B \cap I)$ comme A-modules (la notion d'idéaux isomorphes n'a pas de sens, "idéal" étant une notion relative), cf. partie III du cours.

1.3. Anneaux intègres, corps, corps des fractions

Définition 1.14 Soit A un anneau commutatif. Soit a un élément non nul de A. On dit que a est un *diviseur de zéro* dans a s'il existe $b \in A$ non nul avec $ab = 0$.

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 $b = 0$.

Autrement dit un anneau intègre est un anneau commutatif non nul sans diviseurs de 0.

Exemple 1.16 a) Pour $n \in \mathbf{N}^*$, $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est premier.

b) Tout corps est un anneau intègre.

c) Tout sous-anneau d'un anneau intègre est intègre.

d) Si A est intègre, les anneaux $A[X]$, $A[X_1, ..., X_n]$ sont intègres. On vérifie facilement que dans ces deux exemples, le groupe des éléments inversibles est réduit aux constantes de A^*.

On rappelle le résultat classique suivant :

Proposition 1.17 *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 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 que K est le "plus petit corps" contenant A ; 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).

Démonstration (esquisse): 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, en prenant pour $i(a)$ la classe de $(a, 1)$.

□

Définition 1.18 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. L'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier.
4. Les idéaux (X_1) et (X_1, X_2) sont tous deux premiers dans $K[X_1, X_2]$.

Définition 1.19 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 1.20 *Un idéal I est maximal si et seulement si A/I est un corps.*

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 1.21 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).

Remarque 1.22 En général, l'image réciproque d'un idéal maximal par un morphisme d'anneaux n'est pas un idéal maximal, par exemple l'image réciproque de $\{0\}$ par l'injection canonique $\mathbf{Z} \to \mathbf{Q}$ est $\{0\}$, qui n'est pas un idéal maximal de $\mathbf{Z}$ (alors que c'en est un de $\mathbf{Q}$ vu que $\mathbf{Q}$ est un corps). C'est ce qui conduit à la nécessité en géométrie algébrique la nécessité de considérer l'ensemble des idéaux premiers d'un anneau commutatif plutôt que l'ensemble de ses idéaux maximaux qui est pourtant plus facile a priori à appréhender. [3]

Le théorème suivant est utile pour les questions théoriques générales. [4]

Theorème 1.23 (Krull) *Dans un anneau commutatif*[5] *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.

□

1.4. Anneaux principaux

Définition 1.24 Un anneau commutatif A est dit *principal* s'il est intègre et si tous ses idéaux sont principaux, c'est-à-dire de la forme $(a) = aA$ avec $a \in A$.

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

3. Le *théorème des zéros de Hilbert* assure par exemple que les idéaux maximaux de $\mathbf{C}[X_1, ..., X_n]$ correspondent bijectivent aux $a \in \mathbf{C}^n$ via l'application qui envoie un tel a sur l'ensemble des polynômes qui l'annulent, voir TD.

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

5. 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".

Définition 1.25 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 1.26 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 1.27 *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 $I = (b)$.

□

La réciproque est fausse mais les contre-exemples classiques ne sont pas évidents ($\mathbf{Z}[\frac{1+i\sqrt{19}}{2}]$, $\mathbf{R}[X, Y]/(X^2 + Y^2 + 1)$; voir TD et [1], chapitre II, §5).

Exemple 1.28 a) Les anneaux $\mathbf{Z}$ et $K[X]$ (où K est un corps) sont euclidiens, donc principaux.

b) L'anneau $\mathbf{Z}/4\mathbf{Z}$ n'est pas principal (bien que tous ses idéaux soient principaux), car il n'est pas intègre !

c) Attention, A principal n'implique pas du tout $A[X]$ principal (ce n'est vrai que si A est un corps en fait). On vérifiera par exemple que dans $K[X_1, X_2]$ (où K est un corps), l'idéal I engendré par X_1 et X_2 n'est par principal (s'il l'était, un générateur de I devrait diviser X_1 et X_2, donc être un polynôme constant, donc on aurait $I = A$; or $1 \notin I$).

2. Divisibilité dans les anneaux intègres

2.1. Éléments irréductibles, éléments associés

Dans tout ce paragraphe, A désigne un anneau commutatif intègre.

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 $(a) \supset (b)$ ("diviser c'est contenir").

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 : 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 $A \setminus \{0\}$.

Définition 2.3 On dit qu'un élément p de A 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 ; en particulier un corps n'a pas d'élément irréductible.

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

b) Si K est un corps, les polynômes de degré 1 ainsi que ceux de degré 2 ou 3 sans racine, sont irréductibles dans $K[X]$ (mais la réciproque est fausse dans $\mathbf{Q}[X]$ par exemple).

c) Les irréductibles de $\mathbf{C}[X]$ sont les polynômes de degré 1, ceux de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle. On verra dans le cours sur les corps que dans $\mathbf{Q}[X]$ ou $F[X]$ avec F corps fini, il y a des polynômes irréductibles de tout degré.

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^*.

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

Proposition 2.6 *Soit A un anneau principal. Deux éléments a et b de A sont premiers entre eux si et seulement s'il existe des éléments u, v de A tels que $ua + vb = 1$ (i.e. si $A = (a, b)$, idéal engendré par a et b).*

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 $(d) = A$.

□

Notons que dans l'anneau $A = K[X, Y]$, 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.

2.2. Anneaux factoriels

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 2.7 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

$$a = up_1...p_r$$

avec $u \in A^*$ et les p_i irréductibles [6].

3. Il y a unicité de cette décomposition au sens suivant : si $a = vq_1...q_s$ en est une autre, 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.

Remarques : 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 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 $n_p = v_p(a)$, et on obtient que a divise b si et

6. 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.

seulement si $v_p(a) \leq v_p(b)$ pour tout p de $\mathcal{P}$. Noter qu'en général, l'existence de $\mathcal{P}$ dépend de l'axiome du choix.

c) La plupart des anneaux intègres (notamment ceux qui sont noethériens, voir plus loin) que l'on rencontre en algèbre ont la propriété d'existence de la décomposition en irréductibles [7], la propriété forte est l'unicité.

Exemple 2.8 a) $\mathbf{Z}$ est factoriel (prendre pour $\mathcal{P}$ l'ensemble des nombres premiers).

b) $K[X]$ est factoriel (on peut prendre pour $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires).

c) On verra que plus généralement tout anneau principal est factoriel, mais que la réciproque est fausse par exemple pour $K[X_1, ..., X_n]$.

d) L'anneau $A = \mathbf{Z}[i\sqrt{5}] \simeq \mathbf{Z}[T]/(T^2+5)$, qui est le sous-anneau de $\mathbf{C}$ constitué des $a + bi\sqrt{5}$ avec $a, b \in \mathbf{Z}$, est intègre mais n'est pas factoriel. Posons en effet, pour tout $z = a + ib$ de A :

$$N(z) = z\bar{z} = a^2 + 5b^2,$$

qu'on appelle *norme* de z. Alors, on a $N(z) \in \mathbf{N}$, ce qui implique que tout $z \in A^*$ vérifie $N(z) = 1$ et donc $z \in \{\pm 1\}$ (réciproquement 1 et -1 sont bien dans A^*). Maintenant, les éléments 3, $2 - i\sqrt{5}$, et $2 + i\sqrt{5}$ sont irréductibles car de norme 9, et A n'a pas d'élément de norme 3, ce qui fait que si un élément z de norme 9 s'écrit $z = z_1 z_2$, alors $9 = N(z_1)N(z_2)$ d'où $N(z_1) = 1$ ou $N(z_2) = 1$, ce qui implique z_1 ou z_2 inversible.

Pourtant $9 = 3 \times 3 = (2 - i\sqrt{5})(2 + i\sqrt{5})$ dans A, ce qui constitue bien deux décompositions différentes vu que 3 n'est associé ni à $2 - i\sqrt{5}$ ni à $2 + i\sqrt{5}$.

On voit au passage qu'un quotient d'un anneau factoriel par un idéal premier ne reste pas toujours factoriel (on verra au chapitre suivant que $\mathbf{Z}[X]$ est factoriel) ; cela ne marche pas non plus pour un sous-anneau, vu que tout anneau intègre est un sous-anneau d'un corps, lequel est évidemment un anneau factoriel.

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

Proposition 2.9 *Soit A un anneau intègre tel que tout élément non nul de A ait une décomposition en irréductibles. Alors les propriétés suivantes sont équivalentes :*

7. Il est commode d'employer l'expression "décomposition en irréductibles" pour "décomposition en produit d'un inversible et 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 en utilisant l'écriture unique

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad , u \in A^*$$

et de même pour b et c. 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) donc $v_p(a) \leq v_p(c)$ dans tous les cas. Ainsi a divise c.

□

Proposition 2.10 *Si A est un anneau factoriel, alors deux éléments non nuls a et b de A ont un pgcd, bien défini à association près.*

Rappelons qu'un pgcd (plus grand commun diviseur) de a et b est un diviseur commun d de a et b, tel que tout autre diviseur commun divise d ; "grand" fait réference à la relation d'ordre partiel "divise" sur l'ensemble quotient de $A \setminus \{0\}$ par la relation d'association.

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 non vide d'éléments de $A \setminus \{0\}$; le produit est bien fini puisque si on choisit un élément non nul a dans la famille, alors $v_p(a) = 0$ pour presque tout $p \in \mathcal{P}$). 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. D'autre part, si A est principal, on peut prendre comme pgcd de a et b tout générateur de l'idéal $(a,b) = aA + bA$ (et cela s'étend immédiatement à une famille quelconque d'éléments de A).

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*[8] d'éléments de $A \setminus \{0\}$. Si A est principal, le ppcm de (a,b) s'obtient en prenant un générateur de l'idéal engendré $aA \cap bA$ (et de même pour une famille finie d'éléments de A).

Pour ce qui est de l'existence de la décomposition, on a besoin d'une propriété de finitude qui est à l'origine de la notion d'anneau noethérien. Historiquement, cette notion a été introduite pour généraliser une propriété des anneaux de polynômes, anneaux que nous allons maintenant étudier en détails.

3. Anneaux de polynômes

On désigne toujours par A un anneau commutatif. Rappelons qu'une famille d'éléments de A est dite *presque nulle* si tous les éléments de la famille sont nuls à l'exception d'un nombre fini d'entre eux. Si I est un ensemble. On note $A^{(I)}$ l'ensemble des familles presque nulles d'élements de A indexées par I.

3.1. Rappels sur les polynômes en plusieurs indéterminées

Pour tout entier $n \geq 2$, on définit l'anneau $A[X_1, ..., X_n]$ par récurrence via la formule

$$A[X_1, ..., X_n] := (A[X_1, ..., X_{n-1}])[X_n].$$

Autrement dit $A[X_1, ..., X_n]$ est l'anneau des polynômes en une indéterminée (notée X_n) sur l'anneau commutatif $A[X_1, ..., X_{n-1}]$. Les éléments de $A[X_1, ..., X_n]$ sont appelés *polynômes en n indéterminées* (à coefficient dans A).

On vérifie immédiatement par récurrence sur n qu'un élément P de l'anneau commutatif $A[X_1, ..., X_n]$ s'écrit de manière unique :

8. ou même quelconque si on accepte que 0 soit le ppcm d'une famille n'ayant pas de multiple commun non nul.

$$P = \sum_{(i_1,...,i_n)\in\mathbf{N}^n} a_{i_1,...,i_n} X_1^{i_1}...X_n^{i_n}, \qquad (1)$$

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 3.1 Appelons *exposants* les éléments de $\mathbf{N}^n$. On dit qu'un exposant $(i_1, ..., i_n)$ *apparaît dans* P si dans l'écriture (1), le coefficient $a_{i_1,...,i_n}$ est non nul. Si $\alpha = (\alpha_1, ..., \alpha_n)$ est un exposant, on pose $|\alpha| = \sum_{i=1}^n \alpha_i$. On dit que P est *homogène de degré* d si tous les exposants α qui apparaissent dans P vérifient $|\alpha| = d$.

Remarque 3.2 Via l'écriture (1), tout polynôme F en n indéterminées s'écrit 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.

La proposition suivante se démontre facilement à partir du cas $n = 1$:

Proposition 3.3 *a) Soit $P \in A[X_1, ..., X_n]$ non nul. On suppose qu'il existe $i \in \{1, ..., n\}$ tel que le terme de plus grand degré de P vu comme polynôme dans $(A[X_1, ..., \widehat{X_i}, ..., X_n])[X_i]$ soit de la forme $aX_1^{i_1}...X_r^{i_r}$ avec a non diviseur de zéro dans A. Alors P n'est pas diviseur de zéro dans $A[X_1, ..., X_n]$.*

b) L'anneau $A[X_1, ..., X_n]$ est intègre si et seulement si A est intègre.

c) Si A est intègre, le groupe des inversibles de $A[X_1, ..., X_n]$ est le groupe A^* des polynômes constants inversibles dans A.

Noter que le c) est faux sans hypothèse d'intégrité de A : par exemple, si A contient un élément non nul ε tel que $\varepsilon^2 = 0$, alors $1 - \varepsilon X$ est inversible dans $A[X]$ d'inverse $1 + \varepsilon X$. C'est le cas de l'anneau $A = K[Y]/(Y^2)$, en prenant pour ε la classe de Y. On verra en TD comment déterminer $A[X]^*$ pour A commutatif quelconque.

3.2. Notion de A-algèbre

Définition 3.4 Une *A-algèbre* est un anneau commutatif[9] B équipé d'un morphisme d'anneaux (pas forcément injectif) $\varphi : A \to B$.

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.

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 3.5 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 1.11 s'étend immédiatement aux morphismes de A-algèbres.

Exemple 3.6 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) Si $r \in \mathbf{N}^*$, l'anneau produit A^r est une A-algèbre via le morphisme $a \mapsto (a, a, ..., a)$ de A dans A^r.

Proposition 3.7 (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 $i \in \{1, ..., n\}$.*

Si on considère B comme une A-algèbre via φ, une formulation équivalente consiste à dire qu'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, 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 3.8 Soient $P, Q_1, ..., Q_n \in A[X_1, .., X_n]$. On dispose du polynôme $R = P(Q_1, ..., Q_n)$ obtenu en substituant Q_i à l'indéterminée X_i. Plus précisément, le polynôme R est l'image de P par l'unique morphisme de A-algèbres qui envoie X_i sur Q_i. En particulier, on a $P = P(X_1, ...X_n)$ par définition (ce qui justifie l'emploi des deux notations !). Quand $n = 1$, on note souvent $P \circ Q$ le polynôme de $A[X]$ défini par $(P \circ Q)(X) = P(Q(X))$.

Définition 3.9 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 $P \in A[X_1, ..., X_n]$.

Il est immédiat que C est la plus petite sous-A-algèbre de B contenant S.

Proposition 3.10 *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

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 3.7 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.

□

Remarque 3.11 Si I est un ensemble quelconque (pas forcément fini), on peut encore définir l'anneau $A[(X_i)_{i\in I}]$ en considérant les polynômes P dont l'écriture est de la forme (1) pour des multi-indices $(i_1, ..., i_n)$ dans I^n, mais où n est un entier quelconque (qui dépend du polynôme P), l'addition et la multiplication de deux polynômes étant définies en utilisant le fait qu'il existe une partie finie J de I telle que les deux polynômes soient dans $A[(X_j)_{j\in J}]$. L'anneau $A[(X_i)_{i\in I}]$ est en quelque sorte la réunion [11] des $A[(X_j)_{j\in J}]$ pour J finie. On peut aussi définir $A[(X_i)_{i\in I}]$ comme l'ensemble des familles presque nulles d'éléments de A indexées par $\mathbf{N}^{(I)}$ avec l'addition usuelle et la multiplication induite par celles des polynômes de $A[(X_j)_{j\in J}]$ pour J partie finie de I, ceux-ci étant vus comme des familles presque nulles d'éléments de A indexées par $\mathbf{N}^J$. La propriété universelle 3.7 reste vraie pour $A[(X_i)_{i\in I}]$ avec I infini, en définissant f sur chaque $A[(X_j)_{j\in J}]$ pour J finie.

3.3. Anneaux noethériens

Proposition 3.12 *Soit A un anneau commutatif. Alors les trois propriétés suivantes sont équivalentes :*

1. *Tout idéal de A est engendré par un nombre fini d'éléments.*
2. *Toute suite croissante (pour l'inclusion) $(I_n)_{n\in\mathbf{N}^*}$ d'idéaux est stationnaire.*
3. *Toute famille non vide d'idéaux de A possède un élément maximal pour l'inclusion.*

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

fini comme A-algèbre et comme A-module (notion qui sera vue dans le chapitre sur les modules). Typiquement, si par exemple K est un corps, $K[X]$ est de type fini comme K-algèbre mais pas comme K-espace vectoriel.

11. Plus précisément, il s'agit de leur *limite inductive* ou *colimite*.

Démonstration : 1. implique 2. : 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. 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}.

2. implique 3. : 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 2.

3. implique 1. : 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 3.13 a) Tout anneau principal est noethérien via la caractérisation 1.

b) Si A est noethérien, tout quotient de A l'est encore via la la caractérisation 1, vu que les idéaux de A/I sont les J/I, où J est un idéal de A contenant I (si J est un idéal engendré par $a_1, ..., a_r$, alors J/I est engendré par les images de $a_1, ..., a_r$ via la surjection canonique).

c) L'anneau $K[(X_n)_{n\in\mathbf{N}^*}]$ (où K est un corps) n'est pas noethérien car $(X_1) \subset (X_1, X_2) \subset ...(X_1, ..., X_n) \subset ...$ forme une suite infinie strictement croissante d'idéaux. Noter que cet anneau est factoriel : ceci se déduit aisément du fait, que l'on prouvera plus tard, que $K[X_1, ..., X_n]$ est factoriel, car un élément *fixé* de $K[(X_n)_{n\in\mathbf{N}^*}]$ est dans $K[X_1, ..., X_n]$ pour un certain n. Les anneaux de fonctions qui apparaissent en analyse sont également souvent non noethériens.

d) Un sous-anneau d'un anneau noethérien ne le reste pas forcément (prendre un anneau intègre non noethérien comme $K[(X_n)_{n\in\mathbf{N}^*}]$, qui est un sous-anneau de son corps de fractions ; or, un corps est évidemment un anneau noethérien).

La plupart des anneaux avec lesquels on travaille en algèbre sont noethériens, via le théorème suivant :

Theorème 3.14 (Hilbert) *Soit A un anneau noethérien. Alors $A[X]$ est noethérien.*

Démonstration : Soient I un idéal de $A[X]$ et $n \in \mathbf{N}$; on note $d_n(I)$ le sous-ensemble de A constitué de 0 et des coefficients dominants des éléments de degré n de I. Il est immédiat que $d_n(I)$ est un idéal de A, et que l'inclusion $I \subset J$ implique $d_n(I) \subset d_n(J)$. On a d'autre part :

Lemme 3.15 *i) Si $k \in \mathbf{N}$, alors $d_k(I) \subset d_{k+1}(I)$.*

ii) Si $I \subset J$ et si $d_k(I) = d_k(J)$ pour tout $k \in \mathbf{N}$, alors $I = J$.

Le premier point du lemme vient de ce que si $P \in I$, alors $XP \in I$. Pour le deuxième, on observe que si J contient strictement I, on choisit un polynôme P dans $J \setminus I$ de degré r minimal ; comme $d_r(I) = d_r(J)$, I contient un polynôme Q de degré r qui a même coefficient dominant que P, mais alors $P - Q$ est dans $J \setminus I$ et est de degré $< r$, contradiction.

□

Reprenons la preuve du théorème. Soit $(I_n)_{n \in \mathbf{N}^*}$ une suite croissante d'idéaux de $A[X]$. Comme A est noethérien, la famille des $d_k(I_n)$ pour $k \in \mathbf{N}$ et $n \in \mathbf{N}^*$ admet un élément maximal, mettons $d_l(I_m)$. D'autre part pour chaque $k \leq l$, la suite d'idéaux $(d_k(I_n))_{n \in \mathbf{N}^*}$ est croissante, donc elle est stationnaire, c'est-à-dire qu'il existe n_k tel que pour $n \geq n_k$, on ait $d_k(I_n) = d_k(I_{n_k})$. Soit alors N le plus grand des entiers $m, n_0, n_1, ..., n_l$, nous allons montrer que pour tout $n \geq N$, on a $d_k(I_n) = d_k(I_N)$ pour tout $k \in \mathbf{N}$, ce qui suffira à conclure via la propriété ii) du lemme. On distingue deux cas :

a) Si $k \leq l$, alors $d_k(I_N) = d_k(I_{n_k}) = d_k(I_n)$ par définition de n_k puisque n et N sont tous deux $\geq n_k$.

b) Si $k \geq l$, alors $d_k(I_N)$ et $d_k(I_n)$ contiennent tous deux $d_k(I_m)$, donc aussi $d_l(I_m)$ d'après la propriété i) du lemme ; par maximalité de $d_l(I_m)$, on a alors $d_k(I_N) = d_l(I_m)$ et $d_k(I_n) = d_l(I_m)$. Ainsi $d_k(I_N) = d_k(I_n)$.

□

Corollaire 3.16
1. *Si A est noethérien, alors l'anneau $A[X_1, ..., X_n]$ est noethérien.*
2. *Si A est noethérien, tout anneau B qui est une A-algèbre engendrée par une partie finie est noethérien.*

Démonstration : 1. résulte du théorème précédent par récurrence sur n.

2. résulte de 1. et de la proposition 3.10, en utilisant le fait qu'un quotient d'anneau noethérien est noethérien.

□

On s'intéresse maintenant à l'existence de la décomposition en produit d'irréductibles dans un anneau intègre noethérien.

Proposition 3.17 *Soit A un anneau intègre noethérien. Alors tout élément x non nul de A s'écrit : $x = up_1...p_r$ avec $u \in A^*$ et les p_i irréductibles.*

Démonstration : Soit $\mathcal{F}$ l'ensemble des idéaux de A de la forme xA avec x non inversible ne s'écrivant pas comme produit d'irréductibles. Si $\mathcal{F}$ 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.

□

Remarque : Il n'y a pas d'implication entre noethérien et factoriel. Si K est un corps, $K[X_n]_{n\in\mathbf{N}^*}$ est factoriel mais pas noethérien. D'autre part $\mathbf{Z}[X]/(X^2+5)$ est noethérien via le théorème 3.14, et on a déjà vu qu'il n'était pas factoriel.

Corollaire 3.18 *Si A est principal, A est factoriel.*

Démonstration : On vient de voir l'existence de la décomposition en irréductibles. D'autre part si $p \in A$ est irréductible, alors l'idéal (p) (qui est différent de A car $p \notin A^*$) est maximal car si $I = (a)$ contient (p), alors a divise p, ce qui implique que a est inversible ou associé à p, i.e. $(a) = (p)$ ou $(a) = A$. En particulier (p) est premier et on conclut avec la proposition 2.9. [12]

□

3.4. Factorialité des anneaux de polynômes

On a vu que A principal n'impliquait pas du tout $A[X]$ principal (ceci n'est vrai que si A est un corps). On va voir par contre que la propriété analogue est vraie pour factoriel. On commence par une définition :

Définition 3.19 Soit A un anneau factoriel. Le *contenu* (noté $c(P)$) d'un polynôme P est le pgcd de ses coefficients. P est dit *primitif* si $c(P) = 1$.

12. On dit qu'un anneau intègre est *de dimension 1* si tout idéal premier non nul est maximal. On vient de voir qu'un anneau principal est de dimension 1. Par contre $\mathbf{Z}[i\sqrt{5}]$ est de dimension 1 (résultat classique, qu'on voit souvent dans les cours de théorie des nombres de M2) sans être principal (ni même factoriel), et $K[X_1, X_2]$ est factoriel sans être de dimension 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. De plus, pour tout polynôme non nul $P \in A[X]$, on a $\frac{P}{c(P)}$ primitif.

Lemme 3.20 (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 3.21 *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 $A[X]^* = A^*$, il est immédiat qu'un polynôme constant $P = p$ est irréductible si et seulement si p est irréductible dans A. 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 $c(Q)$ et $c(R)$ soient dans A^*, car ils divisent tous les coefficients de P. Comme d'autre part l'un des polynômes Q, R est constant (parce que P est irréductible dans $K[X]$), c'est une constante inversible dans A.

Finalement 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 écrire $Q = Q_1/q$ et $R = R_1/r$ avec q, r dans $A \setminus \{0\}$ et Q_1, R_1 dans $A[X]$. Alors en posant $a = qr$, on obtient $aP = Q_1R_1$, 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 $\frac{Q_1}{C(Q_1)}$, $\frac{R_1}{C(R_1)}$ 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 3.22 *Si A est factoriel, $A[X]$ est factoriel.*

Démonstration : On doit d'abord démontrer qu'on a l'existence de la décomposition (qui est claire via le théorème 3.14 et la proposition 3.17 si A est de plus supposé noethérien). 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^*) soit $P = u\prod_{i=1}^r \frac{Q_i}{c(Q_i)}$ avec $u \in A^*$. D'après le théorème précédent, c'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 2.9 de montrer que si $P \in A[X]$ est irréductible, alors (P) est premier. Si $P = p$ est une constante irréductible de $A[X]$, on remarque que $A[X]/(p)$ est isomorphe à $(A/(p))[X]$ (le morphisme de A-algèbres de $A[X]$ dans $(A/(p))[X]$ qui envoie X sur la classe de X est par définition surjectif, et son noyau est constitué des polynômes dont tous les coefficients sont divisibles par p, i.e. des polynômes divisibles par p). Or, cet anneau est intègre car (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 $ac(Q) = c(S)$ 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.

□

Corollaire 3.23 *Si A est factoriel, $A[X_1, ..., X_n]$ est factoriel.*

Remarque 3.24 On a l'analogue avec une infinité d'indéterminées, c'est immédiat à partir du cas fini.

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

Theorème 3.25 (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 3.21) $P = QR$ 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 3.26 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.

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

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

Nous verrons plus tard (dans le chapitre sur les extensions de corps) d'autres exemples de polynômes irréductibles, notamment les *polynômes cyclotomiques* sur $\mathbf{Q}$ et nous montrerons aussi que si F est un corps fini, il y a des polynômes irréductibles de tout degré > 0 sur F.

3.5. Polynômes symétriques

Soit A un anneau commutatif. Soit $\sigma \in \mathcal{S}_n$. D'après la proposition 3.7, 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 3.27 *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 3.28 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.

On a l'analogue pour les fractions rationnelles, avec le lien suivant quand A est un corps :

Proposition 3.29 *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 clair 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.

□

Exemple 3.30 a) 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.

b) Pour tout entier $k \geq 1$, les *sommes de Newton* (en n indéterminées)

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

sont des polynômes symétriques, homogènes de degré k.

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

Theorème 3.31 *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 (cf. remarque 3.2) $\tau.F_d = F_d$ 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 3.32 *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 [13] (1), 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 $A[X_1, ..., X_n]$ via la proposition 3.3, a). 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 $A[X_1, ..., X_n]$ par la proposition 3.3, a).

□

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

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

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

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

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 3.33 *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 3.31 et de la proposition 3.29. □

Remarque 3.34 (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 $K[X_1, ..., X_n]$.

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

Theorème 3.35 (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 (1) :

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

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 $S = 0$.

□

Références

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