Licence de Mathématiques, 3ème année
U.E. 36MATS1

Cours d'algèbre : groupes et anneaux 2

François DUMAS

Chapitre 6

Anneaux de polynômes: rappels et compléments sur les polynômes en une indéterminée

Dans tout ce chapitre, le mot "anneau" désigne toujours un anneau commutatif unitaire.

1. Rappel de quelques notions générales.

1.1 Données et notations.

On fixe un anneau A. On note $A[X]$ l'anneau des polynômes en une indéterminée à coefficients dans A. Il contient A comme sous-anneau. Son neutre pour l'addition est 0_A. Son neutre pour la multiplication est 1_A. Pour tout élément non-nul P de $A[X]$, il existe un unique entier naturel n et un unique $(n+1)$-uplet $(a_0, a_1, \dots, a_n)$ d'éléments de A tels que:

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad \text{et} \quad a_n \neq 0.$$

L'entier n est appelé le degré de P, noté $\deg P$. L'élément non-nul a_n de A est appelé le coefficient dominant de P, noté $\mathrm{cd}(P)$. Par convention, on pose $\deg 0 = -\infty$. On vérifie aisément que, pour tous P et Q dans $A[X]$, on a:

$$\deg(P+Q) \leq \max(\deg P, \deg Q) \quad \text{et} \quad \deg(PQ) \leq \deg P + \deg Q.$$

1.2 Groupe des unités, intégrité, corps de fractions.

Définition et proposition. Soit A un anneau. Un élément $a \in A$ est dit inversible dans A s'il existe un élément b dans A tel que $ab = 1_A$. L'ensemble des éléments de A qui sont inversibles dans A est un groupe pour la multiplication, noté $U(A)$ ou A^* et appelé groupe des unités de l'anneau A.

Définition. Un anneau A est un corps lorsque tout élément non-nul de A est inversible dans A, c'est-à-dire lorsque $U(A) = A \setminus \{0\}$.

Définition. Un anneau A est intègre lorsque, pour tous $a, b \in A$, l'égalité $ab = 0$ implique $a = 0$ ou $b = 0$.

Proposition. Tout corps est un anneau intègre. La réciproque est fausse, mais, pour tout anneau intègre A, il existe un corps $K(A)$, appelé le corps de fractions de A qui est le plus petit corps contenant A (c'est-à-dire A est un sous-anneau de $K(A)$, et si F est un corps tel que A soit un sous-anneau de F, alors $K(A)$ est un sous-corps de F).

Exemples

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.
- L'anneau $\mathbb{Z}$ des entiers est intègre, vérifie $U(\mathbb{Z}) = \{-1, 1\}$, et donc n'est pas un corps. Son corps de fractions est $K(\mathbb{Z}) = \mathbb{Q}$.
- L'anneau $\mathbb{Z}[i]$ des entiers de Gauss est intègre, vérifie $U(\mathbb{Z}[i]) = \{-1, 1, i, -i\}$, et donc n'est pas un corps. Son corps de fractions est $K(\mathbb{Z}[i]) = \mathbb{Q}[i]$.
- L'anneau $\mathcal{F}$ des fonctions $\mathbb{R} \to \mathbb{R}$ n'est pas intègre (le produit de deux fonctions peut être la fonction nulle sans qu'aucune des deux ne soit la fonction nulle). Le groupe $U(\mathcal{F})$ est formé des fonctions qui ne s'annulent en aucun point de $\mathbb{R}$.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$, où n est un entier ≥ 2, est intègre si et seulement si n est un nombre premier, ce qui est encore équivalent au fait que $\mathbb{Z}/n\mathbb{Z}$ est un corps. Le groupe $U(\mathbb{Z}/n\mathbb{Z})$ est formé des éléments $\overline{x}$ tels que $0 \leq x \leq n-1$ soit premier avec n.

Lemme. *Si A est intègre, alors on a:* $\begin{cases} \deg(PQ) = \deg P + \deg Q & \text{pour tous } P, Q \in A[X], \\ \mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q) & \text{pour tous } P, Q \in A[X] \text{ non-nuls.} \end{cases}$

Preuve. L'égalité $\deg(PQ) = \deg P + \deg Q$ est trivialement vérifiée si P ou Q est nul. Supposons-les tous les deux non-nuls, et écrivons $P = a_n X^n + \cdots + a_1 X + a_0$ et $Q = b_m X^m + \cdots + b_1 X + b_0$, avec $\mathrm{cd}(P) = a_n \neq 0$ et $\mathrm{cd}(Q) = b_m \neq 0$. Alors:

$$PQ = a_n b_m X^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) X^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1) X + a_0 b_0.$$

L'intégrité de A impliquant $a_n b_m \neq 0$, le résultat voulu est établi. □

PROPOSITION. *$A[X]$ est intègre si et seulement si A est intègre.*

Preuve. Le fait que A intègre implique $A[X]$ intègre résulte immédiatement du lemme précédent. Récipoquement, si A n'est pas intègre, $A[X]$ ne peut pas l'être puisqu'il contient A comme sous-anneau. □

Remarque. En particulier, si K est un corps, alors $K[X]$ est intègre.

PROPOSITION. *Si A est intègre, on a: $U(A[X]) = U(A)$.*

Preuve. L'inclusion $U(A) \subset U(A[X])$ est claire. Pour la réciproque, considérons $P \in U(A[X])$. Il existe donc $Q \in A[X]$ tel que $PQ = 1$. Ces deux polynômes sont nécessairement non-nuls, donc il résulte du lemme ci-dessus que $\deg P + \deg Q = 0$. On en tire $\deg P = \deg Q = 0$, c'est-à-dire $P \in A$ et $Q \in A$, et donc l'égalité $PQ = 1$ implique $P \in U(A)$ et $Q \in U(A)$. □

Remarque. $A[X]$ n'est jamais un corps.

En effet, que A soit ou non intègre, l'élément X de $A[X]$ vérifie $\deg PX = \deg P + 1$ pour tout $P \in A[X]$, de sorte que l'on ne peut pas avoir $PX = 1$, ce qui montre que X n'est jamais inversible. □

PROPOSITION ET DÉFINITION. *Si A est intègre, le corps de fractions de $A[X]$ est égal au corps de fractions de l'anneau $K[X]$, où K désigne le corps de fractions de A; on l'appelle le corps des fractions rationnelles en une indéterminée à coefficients dans K, et on le note $K(X)$.*

Preuve. Evidente. □

1.3 Idéaux.

DÉFINITION. Soit A un anneau (commutatif). On appelle idéal de A tout sous-ensemble I de A vérifiant:
(1) I est un sous-groupe de A pour l'addition,
(2) pour tous $x \in I$ et $a \in A$, on a $ax \in I$.

EXEMPLES.
(1) A et $\{0\}$ sont toujours des idéaux de A. Rappelons les trois propriétés immédiates suivantes:
   - Un idéal I de A est égal à A si et seulement si $1_A \in I$.
   - Un idéal I de A est égal à A si et seulement s'il contient un élément de $U(A)$.
   - A et $\{0\}$ sont les seuls idéaux de A si et seulement si A est un corps

(2) Pour tout $a \in A$, l'ensemble $aA = \{ab\,;\, b \in A\}$ est un idéal de A. C'est le plus petit idéal de A contenant a, on l'appelle l'idéal principal engendré par a.
(3) Si f est un morphisme d'un anneau A dans un anneau B, le noyau $\operatorname{Ker} f = \{a \in A\,;\, f(a) = 0_B\}$ est un idéal de A.
(4) Si I et J sont deux idéaux de A, alors $I \cap J$ et $I + J = \{x + y\,;\, x \in I, y \in J\}$ sont des idéaux de A.

Un exemple intéressant. Montrons que, dans l'anneau $A = \mathbb{Z}[X]$, l'idéal $I = 2A + XA$ (qui n'est autre que l'idéal engendré par 2 et X) n'est pas un idéal principal.

Par l'absurde, supposons qu'il existe $P \in A$ tel que $I = PA$. Comme $2 \in I$, il existerait $Q \in A$ tel que $2 = PQ$, ce qui impliquerait par un raisonnement sur les degrés que $P \in \mathbb{Z}$. Comme de plus $X \in I$, il existerait $R \in A$ tel que $X = PR$, ce qui impliquerait $P = \pm 1$ (et $R = \pm X$). On aurait donc $1 = \pm P \in I$, de sorte qu'il existerait $S, T \in A$ tels que $1 = 2S + TX$, ce qui est clairement impossible dans $A = \mathbb{Z}[X]$, puisque le coefficient constant de $2S + TX$ est pair.

1.4 Anneaux quotients.

Soit I un idéal d'un anneau commutatif A. Comme I est un sous-groupe du groupe abélien A pour l'addition, on peut considérer le groupe additif quotient A/I. Rappelons que, si l'on note $\overline{a}$ la classe dans A/I d'un élément a de A, on a par définition:

$$\overline{a} = \{b \in A\,;\, a - b \in I\} := a + I,$$

et que l'addition dans A/I est définie par:

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{pour tous } a, b \in A,$$

d'où en particulier A/I abélien, de neutre additif $\overline{0} = I$. La surjection canonique $\pi : A \to A/I$, qui à tout élément a de A associe sa classe $\overline{a}$ est alors un morphisme de groupes pour l'addition.
Il est facile de vérifier que l'on peut munir A/I d'une multiplication, définie indépendamment des représentants choisis par:

$$\overline{a}.\overline{b} = \overline{ab} \quad \text{pour tous } a, b \in A,$$

et l'on montre alors que:

THÉORÈME. *A/I est un anneau commutatif, et $\pi : A \to A/I$ est un morphisme d'anneaux.*

On a pour les anneaux quotients des résultats de même nature que pour les groupes quotients, en particulier:

THÉORÈME (dit premier théorème d'isomorphisme). *Soient A et A' deux anneaux commutatifs, et $f : A \to A'$ un morphisme d'anneaux. Alors l'anneau quotient de A par l'idéal* $\operatorname{Ker} f$ *est isomorphe au sous-anneau* $\operatorname{Im} f = f(A)$ *de A'. On note:* $A/\operatorname{Ker} f \simeq \operatorname{Im} f$.

PROPOSITION (idéaux d'un anneau quotient). Soient A un anneau commutatif et I un idéal de A. Tout idéal de A/I est de la forme J/I pour J un idéal de A contenant I.

PROPOSITION. *Soient A un anneau et I un idéal de A. Dans $A[X]$, on pose $I[X]$ l'ensemble des éléments qui sont de la forme $\sum_{i=0}^{n} a_i X^i$ pour un entier $n \geq 0$ et des éléments $a_0, a_1, \ldots, a_n$ de I. Alors:*

(i) *$I[X]$ est un idéal de $A[X]$;* (ii) *les anneaux $(A/I)[X]$ et $A[X]/I[X]$ sont isomorphes.*

Preuve. Le point (i) est clair. Pour le (ii), considérons la surjection canonique $\pi : A \to A/I$ et son extension canonique en un morphisme d'anneaux $f : A[X] \to (A/I)[X]$, consistant à envoyer tout polynôme $P = \sum_{i=0}^{n} a_i X^i$ sur $f(P) = \sum_{i=0}^{n} \pi(a_i) X^i$. Il est clair que f est surjective et que son noyau est $\operatorname{Ker} f = I[X]$. L'isomorphisme $A[X]/\operatorname{Ker} f \simeq \operatorname{Im} f$ devient donc $A[X]/I[X] \simeq (A/I)[X]$. □

1.5 Idéaux premiers, idéaux maximaux.

DÉFINITION. Un idéal P d'un anneau commutatif A est dit premier si $P \neq A$ et s'il vérifie:
quels que soient deux éléments x et y de A, si $xy \in P$, alors $x \in P$ ou $y \in P$.

DÉFINITION. Un idéal M d'un anneau commutatif A est dit maximal si $M \neq A$ et s'il vérifie:
quel que soit I un idéal de A, si M est strictement inclus dans I, alors $I = A$.

THÉORÈME. *Soit I un idéal d'un anneau commutatif A. On a les implications suivantes:*

$$\begin{array}{ccc} I \text{ maximal} & \Longleftrightarrow & A/I \text{ corps} \\ \Downarrow & & \Downarrow \\ I \text{ premier} & \Longleftrightarrow & A/I \text{ intègre} \end{array}$$

PROPOSITION (idéaux premiers ou maximaux d'un quotient). *Soit A un anneau commutatif et I un idéal de A, distinct de A. Les idéaux premiers de A/I sont de la forme P/I où P est un idéal premier de A contenant I. Les idéaux maximaux de A/I sont de la forme M/I où M est un idéal maximal de A contenant I.*

PROPOSITION. *Soient A un anneau et I un idéal de A. Alors $I[X]$ est un idéal premier de $A[X]$ si et seulement si I est un idéal premier de A.*

Preuve. I est premier si et seulement si A/I est intègre, ce qui équivaut d'après 1.2 à $(A/I)[X]$ intègre, c'est-à-dire $A[X]/I[X]$ intègre d'après la proposition de 1.4, ce qui équivaut à dire que $I[X]$ est premier dans $A[X]$. □

1.6 Euclidianité.

LEMME (division euclidienne des polynômes). *Soit K un corps. Quels que soient des polynômes P et S dans $K[X]$ tels que $S \neq 0$, il existe Q et R uniques dans $K[X]$ tels que:*

$$P = SQ + R \quad \text{et} \quad \deg R < \deg S.$$

Preuve. Supposée connue; à réviser. □

DÉFINITION. Un anneau A est dit euclidien lorsqu'il est intègre et qu'il existe une application $\delta : A\backslash\{0\} \to \mathbb{N}$ vérifiant les deux conditions:

(i) quels que soient a, b non-nuls dans A, si a divise b, alors $\delta(a) \leq \delta(b)$,

(ii) quels que soient $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que: $a = bq + r$, avec $r = 0$ ou $\delta(r) < \delta(b)$.

L'application δ est appelé stathme euclidien.

Exemples

- L'anneau $\mathbb{Z}$ des entiers est euclidien, pour le stathme $\delta : \mathbb{Z}^* \to \mathbb{N}$ défini par $\delta(x) = |x|$.
- L'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien, pour le stathme $\delta : \mathbb{Z}[i]^* \to \mathbb{N}$ défini par $\delta(x + iy) = x^2 + y^2$.

COROLLAIRE. *Si K est un corps, l'anneau $K[X]$ est euclidien, pour le stathme défini par le degré.*

1.7 Principalité.

DÉFINITION. Un anneau intègre A est dit principal lorsque tout idéal de A est principal, c'est-à-dire de la forme aA pour un élément a de A.

THÉORÈME. *Tout anneau euclidien est principal.*

Exemples. En particulier, $\mathbb{Z}$ et $\mathbb{Z}[i]$ sont principaux.

Remarque. La réciproque du théorème est fausse. Il existe des anneaux principaux non euclidiens. Un des exemples classiques, élémentaire mais non immédiat, est $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$.

PROPOSITION. *Dans un anneau principal, tout idéal premier non-nul est maximal (et donc les notions d'idéal premier non-nul et d'idéal maximal coïncident).*

COROLLAIRE. *Si K est un corps, l'anneau $K[X]$ est principal.*

Remarque fondamentale. On a vu en 1.3 un exemple d'idéal de $\mathbb{Z}[X]$ qui n'est pas principal. Ceci prouve que l'anneau $\mathbb{Z}[X]$ n'est pas principal (et donc a fortiori non euclidien), bien que l'anneau $\mathbb{Z}$ des coefficients soit euclidien (et donc a fortiori principal). On retiendra que:

$$(\ A \text{ euclidien} \not\Rightarrow A[X] \text{ euclidien}\ ) \text{ et } (\ A \text{ principal} \not\Rightarrow A[X] \text{ principal}\ ).$$

Le théorème suivant précise cette observation.

THÉORÈME. *Soit A un anneau. Les conditions suivantes sont équivalentes.*

(i) *A est un corps.* (ii) *$A[X]$ est euclidien;* (iii) *$A[X]$ est principal.*

Preuve. On a déja vu que (i) ⇒ (ii) ⇒ (iii). Supposons donc maintenant $A[X]$ principal. En particulier, $A[X]$ est intègre, et donc (voir 1.2), A est intègre. Considérons l'application $f : A[X] \to A$ qui, à tout polynôme $P = \sum_{i=0}^{n} a_i X^i$, associe le coefficient a_0. Il est facile de voir que f est un morphisme d'anneaux, qui est clairement surjectif. Donc le premier théorème d'isomorphisme conduit à $A[X]/\operatorname{Ker} f \simeq A$. L'intégrité de A implique que $A[X]/\operatorname{Ker} f$ est intègre, donc $\operatorname{Ker} f$ est un idéal premier de $A[X]$. Mais comme $A[X]$ est supposé principal, $\operatorname{Ker} f$ est alors un idéal maximal de $A[X]$, donc $A[X]/\operatorname{Ker} f$ est un corps; on conclut via l'isomorphisme $A[X]/\operatorname{Ker} f \simeq A$ que A est un corps. □

2. Factorialité des anneaux de polynômes

2.1 Divisibilité

Définitions. Soient a et b deux éléments d'un anneau intègre A.
On dit que b divise a lorsqu'il existe un élément c de A tel que $a = bc$. On note $b|a$.
On dit que b est associé à a lorsqu'il existe un élément u de $U(A)$ tel que $a = bu$. On note $b \sim a$.

Proposition (traduction en terme d'idéaux principaux). *Soient a et b deux éléments d'un anneau A.*
(1) $b|a \Leftrightarrow a \in bA \Leftrightarrow aA \subseteq bA$.
(2) $b \sim a \Leftrightarrow a \sim b \Leftrightarrow (b|a \text{ et } a|b) \Leftrightarrow aA = bA$.

Exemple. Dans le cas où $A = \mathbb{Z}$, on retrouve la notion de diviseur de l'arithmétique élémentaire.

Application. Pour tout anneau intègre A, deux polynômes P et Q de $A[X]$ sont associés si et seulement s'il existe $c \in U(A)$ tel que $P = cQ$ (et alors $Q = c^{-1}P$). En particulier, si K est un corps, deux polynômes P et Q de $K[X]$ sont associés si et seulement s'il existe $c \in K^*$ tel que $P = cQ$.

Définition. Un polynôme de $A[X]$ est dit unitaire lorsque son coefficient dominant est égal à 1.

Remarque. Si K est un corps, tout polynôme non-nul est associé à un polynôme unitaire.

Définition. Soient a et b deux éléments non-nuls d'un anneau A. On dit qu'un élément non-nul d de A est un pgcd de a et b lorsque: $d|a$, $d|b$ et tout élément de A qui divise a et b divise aussi d.

Remarque. Deux pgcd de a et b sont nécessairement associés.

Définition. Deux éléments non-nuls a et b de A sont dits premiers entre eux lorsque leurs seuls diviseurs communs sont les inversibles de A, ce qui équivaut à dire que 1 est un pgcd de a et b.

Proposition. *Soient a et b deux éléments non-nuls d'un anneau A admettant un pgcd d. Alors il existe deux éléments non-nuls a' et b' de A tels que $a = da'$, $b = db'$, et a' et b' sont premiers entre eux.*

Question. Pour quels types d'anneaux deux éléments quelconques a et b non-nuls dans A admettent-ils toujours des pgcd ? Le théorème suivant montre que c'est le cas pour les anneaux principaux. On verra plus loin que c'est aussi le cas plus généralement pour les anneaux factoriels.

Théorème. *Soit A un anneau principal. Soient a et b deux éléments non-nuls de A. Alors:*
(i) *l'idéal $aA + bA$ est principal et tout générateur de $aA + bA$ est un pgcd de a et b;*
(ii) *pour tout $d \in A$, on a: (d est un pgcd de a et b) $\Rightarrow$ (il existe $u, v \in A$ tels que $d = au + bv$);*
(iii) *(a et b sont premiers entre eux) $\Leftrightarrow$ (il existe $u, v \in A$ tels que $au + bv = 1$).*

Remarques.
(1) La propriété (iii) est connue sous le nom de théorème de Bézout dans un anneau principal (elle est donc vraie en particulier dans $\mathbb{Z}$).
(2) Dans le cas particulier d'un anneau euclidien (en particulier dans $\mathbb{Z}$), on dispose pour calculer les pgcd d'un moyen algorithmique basé sur la division euclidienne, l'algorithme d'Euclide (à réviser).
(3) On généralise sans difficultés les notions de pgcd et d'éléments premiers entre eux rappelées ci-dessus pour deux éléments à un nombre fini quelconque d'éléments de A.

Application. Si K un corps, $A = K[X]$ est euclidien et donc principal, et tout ce qui précède s'applique (pgcd de polynômes, polynômes premiers entre eux, théorème de Bézout, algorithme d'Euclide,...)

Contre-exemple. Dans l'anneau $A = \mathbb{Z}[X]$, il est facile de vérifier que les éléments 2 et X sont premiers entre eux, mais que $1 \notin 2A + XA$; donc la propriété de Bézout n'est pas vérifiée dans $\mathbb{Z}[X]$ (ce qui donne une autre preuve du fait que $\mathbb{Z}[X]$ n'est pas principal).

Exercice. Soit K un corps de caractéristique nulle. Soient m, n, d trois entiers strictement positifs. Montrer:
(1) d divise m dans $\mathbb{Z}$ si et seulement si $X^d - 1$ divise $X^m - 1$ dans $K[X]$;
(2) d est un pgcd de m et n dans $\mathbb{Z}$ si et seulement si $X^d - 1$ est un pgcd de $X^m - 1$ et $X^n - 1$ dans $K[X]$.

2.2 Irréductibité

DÉFINITION. Un élément r d'un anneau intègre A est dit irréductible dans A lorsqu'il n'est pas inversible dans A et vérifie la condition:

si $r = ab$ avec $a, b \in A$, alors $a \in U(A)$ ou $b \in U(A)$.

Remarques.

(1) r irréductible dans $A \Leftrightarrow rA$ maximal dans l'ensemble des idéaux principaux propres de A.
(2) Tout élément de A associé à un élément irréductible est encore irréductible.
(3) 0 n'est pas irréductible dans A.
(4) Un élément de A peut être irréductible dans A mais ne plus l'être dans un anneau contenant A. Par exemple, 3 est irréductible dans $\mathbb{Z}$, mais ne l'est pas dans $\mathbb{Q}$ puisqu'il est inversible dans $\mathbb{Q}$.

DÉFINITION. Un élément p d'un anneau intègre A est dit premier dans A lorsqu'il est non nul, non inversible dans A, et vérifie la condition:

si p divise ab avec $a, b \in A$, alors p divise a ou p divise b.

Remarques.

(1) p premier dans $A \Leftrightarrow pA$ idéal premier non-nul de $A \Leftrightarrow pA \neq (0)$ et A/pA intègre.
(2) Tout élément de A associé à un élément premier est encore premier.

PROPOSITION. *Tout élément premier dans A est irréductible dans A.*

Remarque. La réciproque est fausse en général. Par exemple, il est facile de montrer que, dans $A = \mathbb{Z}[i\sqrt{5}]$, l'élément 3 est irréductible, mais il n'est pas premier car il divise $9 = (2+i\sqrt{5})(2-i\sqrt{5})$ sans diviser $(2+i\sqrt{5})$ ni $(2-i\sqrt{5})$. Néanmoins, on a le théorème suivant:

THÉORÈME. *Si A est un anneau principal, tout élément irréductible est premier, et donc les notions d'élément premier et d'élément irréductible coïncident dans ce cas.*

Exemple. Dans $\mathbb{Z}$, les éléments premiers (ou irréductibles) sont les nombres premiers et leurs opposés.

PROPOSITION. *Soit K un corps.*

(i) *Les polynômes de degré un sont irréductibles dans $K[X]$.*
(ii) *Si $K = \mathbb{C}$, les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.*
(iii) *Si $K = \mathbb{R}$, les éléments irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un, et les polynômes de degré deux de discriminant strictement négatifs.*

Preuve. Le point (i) est évident en raisonnant sur le degré. Les points (ii) et (iii) ont été vus précédemment (à réviser). □

2.3 Factorialité

DÉFINITION. Un anneau intègre A est dit factoriel lorsque tout élément non-nul et non-inversible se décompose en un produit d'un nombre fini d'éléments irréductibles dans A, de façon unique, à l'ordre et au produit par un élément inversible près.

Explicitement, cela signifie que:

(F1) tout élément $a \in A$, $a \neq 0$, $a \notin U(A)$, s'écrit $a = r_1 r_2 \dots r_n$, avec $r_1, r_2, \dots, r_n$ irréductibles dans A;
(F2) si $r_1 r_2 \dots r_n = s_1 s_2 \dots s_m$, avec $r_1, \dots, r_n, s_1, \dots, s_m$ irréductibles dans A, alors $m = n$, et il existe une permutation $\sigma \in S_n$ telle que $s_i \sim r_{\sigma(i)}$ pour tout $1 \leq i \leq n$.

On parlera de *la* décomposition de a en produit de facteurs irréductibles, bien que l'unicité s'entende à la relation d'association près.

Exemple. $\mathbb{Z}$ est factoriel (la décomposition ci-dessus n'étant autre que la classique décomposition en produit de facteurs premiers). Plus généralement, on a:

THÉORÈME. *Tout anneau principal est factoriel.*

Remarque. La réciproque est fausse. On verra plus loin que $A[X]$ est factoriel dès lors que A est factoriel, donc par exemple $\mathbb{Z}[X]$ est factoriel, alors qu'il n'est pas principal comme on l'a vu plus haut. Ainsi, les anneaux factoriels forment une classe d'anneaux plus vaste que celle des anneaux principaux, importante pour les applications (car stable par passage aux polynômes, voir plus loin), et dans laquelle on peut facilement faire de l'arithmétique, en particulier grâce aux résultats résumés dans le théorème suivant.

THÉORÈME. *Soit A un anneau factoriel.*

(i) *Les diviseurs d'un élément a non-nul de A sont tous les produits par un élément de $U(A)$ de certains des éléments irréductibles apparaissant dans une décomposition de a.*

(ii) *Deux éléments non-nuls quelconques a et b admettent toujours des pgcd dans A, dont on obtient la décomposition en facteurs irréductibles en prenant les facteurs irréductibles apparaissant à la fois dans la décomposition de a et celle de b.*

(iii) *Quels que soient a, b, c non-nuls dans A, on a:*
$$(a \text{ divise } bc) \text{ et } (a \text{ et } b \text{ premiers entre eux}) \Rightarrow (a \text{ divise } c)$$

Remarque. La propriété (iii) est connue sous le nom de théorème de Gauss.

THÉORÈME. *Si A est un anneau factoriel, tout élément irréductible est premier, et donc les notions d'élément premier et d'élément irréductible coïncident dans ce cas.*

2.4 Irréductibilité des polynômes à coefficients dans un anneau factoriel

DÉFINITION. Soit A un anneau factoriel. Soit P un élément de $A[X]$ tel que $P \notin A$. On appelle contenu de P, noté $c(P)$, un pgcd dans A des coefficients de P.

Remarque. La notion de contenu n'est définie qu'au produit par un inversible de A près. Lorsque l'on écrit $c(P) = a$, on a aussi $c(P) = ua$ pour tout $u \in U(A)$.

DÉFINITION. Soit A un anneau factoriel. Un polynôme P dans $A[X]$ est dit primitif lorsque $\deg P \geq 1$ et lorsque ses coefficients sont premiers entre eux, c'est-à-dire lorsque $c(P) = 1$ (ou encore, d'après la remarque précédente, lorsque $c(P) \in U(A)$).

Remarques.

(1) Tout polynôme unitaire est primitif.

(2) Tout polynôme $P \in A[X]$ tel que $P \notin A$ s'écrit $P = c(P)P_1$ avec P_1 primitif.

LEMME 1. *Soit A un anneau factoriel. Soient P_1 et P_2 primitifs dans $A[X]$. Soient a_1 et a_2 non-nuls dans A. Si $a_1P_1 = a_2P_2$, alors a_1 et a_2 sont associés dans A, et P_1 et P_2 sont associés dans $A[X]$.*

Preuve. Comme P_1 est primitif, ont a $c(a_1P_1) = a_1$. De même $c(a_2P_2) = a_2$. Donc a_1 et a_2 sont deux pgcd des coefficients du polynôme $a_1P_1 = a_2P_2$. Ils sont donc associés dans A: il existe $u \in U(A)$ tel que $a_2 = ua_1$. On a alors $a_1P_1 = ua_1P_2$, ce qui par intégrité de $A[X]$ (puisque A est intègre) implique que $P_1 = uP_2$. Comme u est un élément inversible de $A[X]$, on conclut que P_1 et P_2 sont associés. □

LEMME 2. (GAUSS) *Soit A un anneau factoriel. Soient P et Q deux éléments de $A[X]$. D'une part P et Q sont primitifs si et seulement si PQ est primitif. D'autre part $c(PQ) = c(P)c(Q)$.*

Preuve. Supposons que P et Q soient primitifs et que PQ ne le soit pas. Comme $c(PQ)$ n'est pas inversible dans l'anneau factoriel A, il est divisible par au moins un élément p irréductible et donc premier. Considérons l'anneau intègre $B = A/pA$. La surjection canonique $\pi : A \to B$ se prolonge canoniquement en un morphisme d'anneaux $\hat{\pi} : A[X] \to B[X]$ défini par $\hat{\pi}(\sum a_i X^i) = \sum \pi(a_i) X^i$. Comme $c(P) = 1$, l'élément p ne divise pas tous les coefficients de P, donc $\hat{\pi}(P) \neq 0$. De même, $\hat{\pi}(Q) \neq 0$. L'intégrité de B impliquant celle de $B[X]$, on en déduit que $\hat{\pi}(P)\hat{\pi}(Q) \neq 0$, c'est-à-dire $\hat{\pi}(PQ) \neq 0$. Or, p divise $c(PQ)$, donc tous les coefficients de PQ, donc $\hat{\pi}(PQ) = 0$. D'où une contradiction. On a ainsi montré que P et Q primitifs implique PQ primitif.

Réciproquement, supposons PQ primitif. On peut toujours écrire P et Q sous la forme $P = c(P)P_1$ et $Q = c(Q)Q_1$ avec P_1 et Q_1 primitifs. Alors P_1Q_1 est primitif d'après ce qui précède, et l'égalité $PQ = c(P)c(Q)P_1Q_1$ implique avec le lemme 1 que $c(P)c(Q)$ est associé à 1 dans A, c'est-à-dire inversible dans A. D'où $c(P) \in U(A)$ et $c(Q) \in U(A)$, de sorte que P et Q sont primitifs.

Enfin, plus généralement, en notant $P = c(P)P_1$, $Q = c(Q)Q_1$ et $PQ = c(PQ)S_1$ avec P_1, Q_1, S_1 primitifs, l'égalité $c(PQ)S_1 = c(P)c(Q)P_1Q_1$ implique, puisque P_1Q_1 est primitif d'après le début de la preuve, que $c(PQ)$ est associé à $c(P)c(Q)$ dans A, ce que l'on a convenu d'écrire aux élément inversibles près $c(PQ) = c(P)c(Q)$. □

LEMME 3. *Soient A un anneau factoriel et K son corps de fractions. Tout polynôme $P \in K[X]$ tel que $P \notin K$ peut s'écrire $P = qP_1$ où $q \in K^*$ et $P_1 \in A[X]$ est primitif dans $A[X]$.*

Preuve. Notons $P = \sum_{i=0}^{n} \frac{a_i}{s_i} X^i$ avec $n \geq 1$, $a_i \in A$, s_i non-nuls dans A, et $a_n \neq 0$. Quitte à multiplier le numérateur et le dénominateur de chaque fraction $\frac{a_i}{s_i}$ par un même élément non-nul de A, on peut écrire toutes les fractions $\frac{a_i}{s_i}$ avec un même dénominateur s (par exemple un ppcm des s_i puisque cette notion existe dans l'anneau factoriel A, ou encore simplement le produit de s_i), sous la forme $\frac{a_i}{s_i} = \frac{a'_i}{s}$, avec $a'_i \in A$. Donc $P = \frac{1}{s} \sum_{i=0}^{n} a'_i X^i$. En désignant par d un pgcd des a'_i, et en écrivant $a'_i = db_i$, les b_i sont premiers entre eux dans A, de sorte que $P = \frac{d}{s} P_1$ avec $P_1 = \sum_{i=0}^{n} b_i X^i$ primitif. □

THÉORÈME. *Soient A un anneau factoriel et K son corps de fractions. Soit R un élément non-nul de $A[X]$.*

(i) *Ou bien $R \in A$; alors R est irréductible dans $A[X]$ si et seulement si R est irréductible dans A.*

(ii) *Ou bien $R \notin A$; alors R est irréductible dans $A[X]$ si et seulement si R est primitif dans $A[X]$ et irréductible dans $K[X]$.*

Preuve. Rappelons d'abord que $U(A[X]) = U(A)$ puisque A est intègre.

(i) Supposons $R \in A$. Notons alors $R = r$. Supposons d'abord r irréductible dans A. En particulier $r \notin U(A)$ donc $r \notin U(A[X])$. Si P et Q dans $A[X]$ sont tels que $r = PQ$, on a $0 = \deg r = \deg P + \deg Q$ donc $P \in A$ et $Q \in A$, de sorte que l'irréductibilité de r dans A implique $P \in U(A)$ ou $Q \in U(A)$, c'est-à-dire $P \in U(A[X])$ ou $Q \in U(A[X])$, ce qui prouve que r est irréductible en tant qu'élément de $A[X]$. Supposons maintenant que r est irréductible dans $A[X]$. En particulier $r \notin U(A[X])$ donc $r \notin U(A)$. Si $a, b \in A$ sont tels que $r = ab$, alors cette égalité dans $A[X]$ implique $a \in U(A[X])$ ou $b \in U(A[X])$, c'est-à-dire $a \in U(A)$ ou $b \in U(A)$, ce qui prouve que r est irréductible en tant qu'élément de A.

(ii) Supposons R de degré non-nul dans $A[X]$ primitif dans $A[X]$ et irréductible dans $K[X]$. Si P et Q dans $A[X]$ sont tels que $R = PQ$, comme R est irréductible dans $K[X]$, on a P ou Q dans $U(K[X]) = K \setminus \{0\}$. Mais P et Q étant à coefficients dans A, cela signifie que P ou Q appartient à $A \setminus \{0\}$. Considérons le cas où $P \in A$, $P \neq 0$. Dans $A[X]$, on peut toujours écrire $Q = c(Q)Q_1$ avec Q_1 primitif. On a l'égalité $R = Pc(Q)Q_1$ avec $Pc(Q) \in A$, Q_1 primitif dans $A[X]$ et R primitif dans $A[X]$. On en déduit avec le lemme 1 que $Pc(Q) \in U(A)$. D'où a fortiori $P \in U(A)$, ou encore $P \in U(A[X])$. De même $Q \in A$, $Q \neq 0$, implique $Q \in U(A[X])$. On a ainsi montré que R est irréductible dans $A[X]$.

Récipoquement, supposons R de degré non-nul irréductible dans $A[X]$. Ecrivons-le sous la forme $R = c(R)R_1$ avec R_1 primitif dans $A[X]$, de même degré que R; l'irréductibilité de R implique alors R_1 ou $c(R)$ inversible dans $A[X]$. Comme $\deg R_1 = \deg R \geq 1$, le premier cas est exclu, donc $c(R) \in U(A[X])$, c'est-à-dire $c(R) \in U(A)$, et donc R est primitif dans $A[X]$. Pour montrer maintenant que R est irréductible dans $K[X]$, considérons P et Q dans $K[X]$ tels que $R = PQ$. Raisonnons par l'absurde en supposant que P et Q ne sont pas dans K; ils sont d'après le lemme 3 de la forme $P = \frac{a}{b} P_1$ et $Q = \frac{c}{d} Q_1$ avec a, b, c, d non-nuls dans A, et P_1, Q_1 primitifs dans $A[X]$, de mêmes degrés strictement positifs que P et Q respectivement. L'égalité $R = PQ$ devient $bdR = acP_1Q_1$. Or R est primitif dans $A[X]$ comme on vient de le voir, et P_1Q_1 l'est aussi d'après le lemme 2. En appliquant le lemme 1, on déduit que R est associé à P_1Q_1 dans $A[X]$. Il existe donc $u \in U(A[X]) = U(A)$ tel que $R = uP_1Q_1$. Comme R est supposé irréductible dans $A[X]$, il en résulte que P_1 ou Q_1 appartient à $U(A[X]) = U(A)$, ce qui contredit l'hypothèse faite selon laquelle P et Q sont de degrés strictement positifs. C'est donc que P ou Q appartient à $U(K[X]) = K^*$, ce qui achève de prouver que R est irréductible dans $K[X]$. □

2.5 Première application: critère d'irréductibilité d'Eisenstein

THÉORÈME. *Soit A un anneau factoriel. Soit $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un élément de $A[X]$ de degré $n \geq 1$. On suppose qu'il existe dans A un élément p, premier dans A, et satisfaisant les trois conditions suivantes:*

$$p \text{ divise } a_0, a_1, \ldots, a_{n-1}, \qquad p \text{ ne divise pas } a_n, \qquad p^2 \text{ ne divise pas } a_0.$$

(i) *Alors P est irréductible dans $K[X]$, où K désigne le corps de fractions de A.*

(ii) *Si de plus P est primitif dans $A[X]$ (en particulier s'il est unitaire dans $A[X]$), alors P est irréductible dans $A[X]$.*

Preuve. On montre d'abord le point (ii). Supposons donc P primitif. Par l'absurde, supposons P non irréductible dans $A[X]$: il existe donc $Q, R \in A[X]$ tels que $P = QR$, avec $0 < \deg Q < \deg P$ et $0 < \deg R < \deg P$. Comme P est primitif, le lemme 2 implique que Q et R le sont. Posons $Q = \sum_{i=0}^{q} b_i X^i$ et $R = \sum_{i=0}^{r} c_i X^i$, avec $b_i, c_i \in A$, et $0 < q < n$ et $0 < r < n$. On a $a_n = b_q c_r \neq 0$, et l'hypothèse p ne divise pas a_n implique que p ne divise pas b_q et ne divise pas c_r. On a aussi $a_0 = b_0 c_0$, et donc par hypothèse p divise $b_0 c_0$ mais p^2 ne divise pas $b_0 c_0$, ce qui implique que p ne divise pas b_0 ou

p ne divise pas c_0. Si l'on est dans le cas où p ne divise pas b_0, alors p divise c_0 en utilisant le fait que p est premier dans A. On a vu que p ne divise pas c_r, et on peut donc considérer le plus petit entier $k \in \{1, \dots, r\}$ tel que p ne divise pas c_k. Par construction, p ne divise pas $b_0 c_k$, et p divise $b_i c_{k-i}$ pour tout $i \in \{1, \dots, k\}$. Il en résulte que p ne divise pas $a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0$. Comme $1 \leq k \leq r < n$, ceci est contraire aux hypothèses faites au départ sur P. C'est donc que P est irréductible dans $A[X]$.

On ne suppose plus maintenant que P est primitif. Notons $P = c(P)P_1$ avec P_1 primitif. Comme $c(P)$ est un pgcd des a_i (pour $0 \leq i \leq n$), il existe $a'_0, a'_1, \dots, a'_n$ premiers entre eux dans leur ensemble tels que $a_i = c(P)a'_i$ pour tout $0 \leq i \leq n$. Donc $P_1 = a'_n X^n + \cdots + a'_1 X + a'_0$. On a clairement p qui ne divise pas a'_n (sinon il diviserait $a_n = c(P)a'_n$) et p^2 qui ne divise pas a'_0 (par le même argument). Pour $0 \leq i \leq n-1$, p divise $a_i = c(P)a'_i$ avec p qui ne divise pas $c(P)$ (car sinon p diviserait en particulier a_n, ce qui est exclu). Les coefficients a'_i du polynôme primitif P_1 vérifiant donc les conditions du critère, on peut appliquer à P_1 la première étape, et conclure que P_1 est irréductible dans $A[X]$. D'après le point (ii) du théorème de 2.4, il s'ensuit que P_1 est irréductible dans $K[X]$. En multipliant par $c(P) \in K^* = U(K[X])$, il en est de même de $c(P)P_1 = P$. □

EXEMPLE: $P = X^5 + 4X^3 + 12X + 2$ est unitaire donc primitif dans $\mathbb{Z}[X]$, et il est irréductible dans $\mathbb{Z}[X]$ par application du critère d'Eisenstein.

2.6 Seconde application: factorialité de l'anneau des polynômes sur un anneau factoriel

On commence par prouver le lemme général suivant, qui donne une autre définition équivalente de la notion d'anneau factoriel, et dont un sens a déjà été cité à la fin du rappel du 2.3.

LEMME (Une définition équivalente de la factorialité). *Un anneau intègre A est factoriel si et seulement s'il vérifie la condition* (F1) *de la définition et la condition suivante:*

(F2') *tout élément irréductible dans A est premier dans A.*

Preuve. Montrons d'abord que (F1) et (F2) impliquent (F2'). Soit r un élément iréductible de A; en particulier $r \neq 0$ et $r \notin U(A)$. Supposons que r divise dans A un produit ab, avec $a, b \in A$ non-nuls. Il s'agit de montrer que r divise a ou b. Soit $x \in A$ tel que $ab = rx$. Si $a \in U(A)$, on a alors r divise b. De même $b \in U(A)$ implique que r divise a. On suppose donc maintenant que $a \notin U(A)$ et $b \notin U(A)$. D'après la condition (F1), on a des décompositions en produits d'éléments irréductibles: $a = a_1 \dots a_n$, $b = b_1 \dots b_m$ et $x = x_1 \dots x_k$. D'où $a_1 \dots a_n b_1 \dots b_m = r x_1 \dots x_k$. Comme r est irréductible, le condition (F2) implique qu'ou bien il existe $1 \leq i \leq n$ tel que $r \sim a_i$, auquel cas r divise a, ou bien il existe $1 \leq j \leq m$ tel que $r \sim b_j$, auquel cas r divise b. On a ainsi prouvé que r est premier dans A.

Montrons maintenant que (F2') implique (F2). On suppose donc que tout irréductible est premier dans A. Supposons que $r_1 r_2 \dots r_n = s_1 s_2 \dots s_m$ avec r_i et s_j irréductibles dans A pour tous $1 \leq i \leq n$ et $1 \leq j \leq m$. L'élément r_1 est premier car irréductible, et comme il divise $s_1 s_2 \dots s_m$, il existe $1 \leq j \leq m$ tel que r_1 divise s_j. On a donc $s_j = a r_1$ pour un certain $a \in A$. Comme s_j est irréductible et que $r_1 \notin U(A)$, on a $a \in U(A)$, c'est-à-dire $r_1 \sim s_j$. Par intégrité, on simplifie par r_1 pour obtenir $r_2 \dots r_n \sim s_1 \dots s_{j-1} s_{j+1} \dots s_m$. On réitère, et le résultat voulu s'en déduit par récurrence. □

THÉORÈME. *Si A est un anneau factoriel, alors l'anneau $A[X]$ est factoriel.*

Preuve. Montrons que $A[X]$ vérifie (F1). Soit $P \in A[X]$, non-nul et non inversible. Si $\deg P = 0$, alors $P \in A$. Comme A est factoriel, P s'écrit comme un produit d'éléments de A irréductibles dans A, donc irréductibles dans $A[X]$ d'après le point (i) du théorème 2.4. On supposera dans la suite que $n = \deg P$ est strictement positif. On peut sans restriction supposer que P est primitif (car sinon $P = c(P)P_1$ avec P_1 primitif, et $c(P)$ se décomposant d'après ce qui précède en produit d'éléments irréductibles dans A donc dans $A[X]$, il suffit de trouver une décomposition en irréductibles de P_1 pour en déduire une décomposition de P). On raisonne par récurrence sur n. Si $n = 1$, on écrit $P = u(X - a)$ avec $u \in U(A)$ et $a \in A$. Il est clair que $X - a$ est irréductible dans $A[X]$, donc il en est de même pour P. Prenons maintenant $n > 1$ et supposons (H.R.) la condition (F1) vérifiée par tout polynôme primitif de degré $< n$. Si P est irréductible, c'est fini. Sinon, il s'écrit $P = QR$ avec $0 < \deg Q < \deg P$ et $0 < \deg R < \deg P$. D'après le lemme 2 de 2.4, Q et R sont primitifs, donc par application de l'hypothèse de récurrence, ils se décomposent en produits d'éléments irréductibles de $A[X]$, d'où $P = QR$ aussi.

Montrons que $A[X]$ vérifie (F2'). Soit R un élément irréductible de $A[X]$; montrons qu'il est premier. Si $\deg R = 0$, alors R est irréductible dans A (point (i) du théorème 2.4), donc premier dans A puisque A est factoriel (lemme ci-dessus). Il s'agit de montrer que l'élément R de A est premier dans $A[X]$. Pour

cela, supposons que R divise PQ dans $A[X]$. Alors R divise $c(PQ) = c(P)c(Q)$, donc divise $c(P)$ ou $c(Q)$ dans A puisque R est premier dans A, donc a fortiori divise $c(P)$ ou $c(Q)$ dans $A[X]$, et finalement R divise P ou Q dans $A[X]$.

Considérons maintenant le cas non trivial où $\deg R > 0$. D'après le point (ii) du théorème 2.4, R est primitif dans $A[X]$ et irréductible dans $K[X]$, où K est le corps de fractions de A. Mais comme K est un corps, $K[X]$ est principal donc factoriel, de sorte que d'après le lemme ci-dessus, l'irréductibilité de R dans $K[X]$ implique que R est premier dans $K[X]$. Il s'agit de montrer que R est premier dans $A[X]$. Pour cela, supposons que R divise PQ dans $A[X]$. On a a fortiori que R divise PQ dans $K[X]$, et comme R est premier dans $K[X]$, on déduit que R divise P ou Q dans $K[X]$. Supposons pour fixer les idées que R divise P dans $K[X]$. Il existe $S \in K[X]$ tel que $P = RS$.

Supposons d'abord $S \notin K$. D'une part $P = c(P)P_1$ avec P_1 primitif dans $A[X]$. D'autre part, d'après le lemme 3 de 2.4, on a $S = \frac{d}{s}S_1$ avec $d, s \in A$ non-nuls et S_1 primitif dans $A[X]$. D'où $sc(P)P_1 = dRS_1$ dans $A[X]$, avec P_1 primitif et et RS_1 primitif (comme produit de deux polynômes primitifs, voir lemme 2 de 2.4). On en déduit avec le lemme 1 de 2.4 que d et $sc(P)$ sont associés dans A. Il existe $u \in U(A)$ tel que $d = usc(P)$, donc s divise d dans A, donc $\frac{d}{s} \in A$, et finalement $S \in A[X]$. On conclut que R divise P dans $A[X]$. Si maintenant $S \in K$, on raisonne comme ci-dessus, mais en prenant $S_1 = 1$.

Ceci achève de prouver que R est premier dans $A[X]$. On a ainsi montré que $A[X]$ vérifie les conditions (F1) et (F2'); on conclut que $A[X]$ est factoriel. □

EXEMPLE: $\mathbb{Z}[X]$ est factoriel (rappelons qu'il n'est pas principal).

EXEMPLE: Si A est factoriel, alors $A[X, Y]$ est factoriel car isomorphe à $A[X][Y]$ avec $A[X]$ factoriel. Plus généralement on obtient ainsi (voir au chapitre suivant) la factorialité de l'anneau des polynômes en n indéterminées à coefficients dans un anneau factoriel A.

Chapitre 7

Anneaux de polynômes: polynômes en plusieurs indéterminées

Dans tout ce chapitre, le mot "anneau" désigne toujours un anneau commutatif unitaire.

1. Quelques notions générales.

1.1 Données, notations, définitions.

• On fixe un anneau A, et un entier naturel $n \geq 1$. Considérons une application f:

$$\begin{array}{ccc} \mathbb{N}^n & \to & A \\ (i_1, i_2, \ldots, i_n) & \mapsto & a_{i_1,i_2,\ldots,i_n} \end{array}$$

que l'on notera sous forme de suite (indexée sur $\mathbb{N}^n$), c'est-à-dire $(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n}$. On dit que f est à support fini lorsque $a_{i_1,i_2,\ldots,i_n} = 0$ sauf pour un nombre fini d'éléments $(i_1, i_2, \ldots, i_n)$ de $\mathbb{N}^n$. On note $\mathcal{R}_n(A)$ l'ensemble de toutes les suites f de ce type qui sont à support fini.

• Il est technique mais élémentaire de vérifier que $\mathcal{R}_n(A)$ est un anneau commutatif pour la somme et le produit définis par

$$(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} + (b_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} = (a_{i_1,i_2,\ldots,i_n} + b_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n},$$

$$(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} \times (b_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} = (c_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n},$$

avec

$$c_{i_1,i_2,\ldots,i_n} = \sum_{r=1}^{n} \sum_{j_r+k_r=i_r} a_{j_1,j_2,\ldots,j_n} b_{k_1,k_2,\ldots,k_n}.$$

Pour tout $a \in A$, on note encore a la suite $(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n}$ dont tous les termes $a_{i_1,i_2,\ldots,i_n}$ sont nuls, sauf $a_{0,0,\ldots,0} = a$. La définition du produit dans $\mathcal{R}_n(A)$ permet de vérifier que:

$$a \times (b_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} = (ab_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n},$$

de sorte que A peut être identifié à un sous-anneau de $\mathcal{R}_n(A)$. En particulier, le neutre additif et le neutre multiplicatif de l'anneau $\mathcal{R}_n(A)$ sont (via l'identification ci-dessus) le zéro et le un de l'anneau A.

• Pour tout $(j_1, j_2, \ldots, j_n) \in \mathbb{N}^n$, on note $X_1^{j_1} X_2^{j_2} \ldots X_n^{j_n}$ la suite $(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n}$ dont tous les termes sont nuls, sauf $a_{j_1,j_2,\ldots,j_n} = 1$. La définition du produit dans $\mathcal{R}_n(A)$ permet de vérifier que:

$$(X_1^{j_1} X_2^{j_2} \ldots X_n^{j_n})(X_1^{k_1} X_2^{k_2} \ldots X_n^{k_n}) = X_1^{j_1+k_1} X_2^{j_2+k_2} \ldots X_n^{j_n+k_n}.$$

En particulier, $X_1^0 X_2^0 \ldots X_n^0 = 1$ et tout élément de l'anneau $\mathcal{R}_n(A)$ s'écrit comme une somme finie:

$$(a_{i_1,i_2,\ldots,i_n})_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} = \sum_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,i_2,\ldots,i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}.$$

Définition. L'anneau $\mathcal{R}_n(A)$ est appelé l'anneau des polynômes en n indéterminées à coefficients dans A. On le note $A[X_1, X_2, \ldots, X_n]$.

Définitions. Un polynôme de la forme $aX_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$, avec $a \in A$, est appelé un monôme. Si $a \neq 0$, l'entier $i_1 + i_2 + \cdots + i_n$ est appelé le degré total de ce monôme. Tout polynôme est une somme de monômes, et on appelle degré total d'un polynôme non-nul le maximum des degrés totaux des monômes dont il est la somme. Par convention, le degré total du polynôme nul est strictement inférieur au degré total de tout polynôme non-nul; on le note $-\infty$.

Définitions. Un polynôme non-nul de $A[X_1, X_2, \ldots, X_n]$ est dit homogène de degré d (où d est un entier naturel) s'il est une somme de monômes qui sont tous de même degré total d. Pour tout polynôme P non-nul de $A[X_1, X_2, \ldots, X_n]$ et tout entier naturel d, on appelle composante homogène de degré d de P la somme des monômes de P de degré total d.

• Si $n = 1$, on note $X = X_1$ et on retrouve l'anneau $A[X]$ bien connu, étudié au chapitre précédent. Le degré total est le degré usuel.

• Si $n = 2$, on note souvent $X = X_1$ et $Y = X_2$; un élément de $A[X, Y]$ est une somme finie:

$$P = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j} X^i Y^j, \quad \text{avec } a_{i,j} \in A.$$

EXEMPLE. Considérons par exemple dans $\mathbb{Z}[X, Y]$ les polynômes:

$$P = 3X^3Y + 5X^3 - 2XY + 7 \quad \text{et} \quad Q = XY + 5X - 6Y + 1.$$

Le degré total de P est 4, celui de Q est 2. Dans Q, la composante homogène de degré 2 est XY, la composante homogène de degré 1 est $5X - 6Y$, la composante homogène de degré 0 est 1. On calcule:

$$PQ = \underbrace{3X^4Y^2}_{6} + \underbrace{20X^4Y - 18X^3Y^2}_{5} + \underbrace{25X^4 - 27X^3Y - 2X^2Y^2}_{4} + \underbrace{5X^3 - 10X^2Y + 12XY^2}_{3} + \underbrace{5XY}_{2} + \underbrace{35X - 42Y}_{1} + \underbrace{7}_{0}.$$

• Si $n = 3$, on note souvent $X = X_1$, $Y = X_2$ et $Z = X_3$; un élément de $A[X, Y, Z]$ est une somme finie:

$$P = \sum_{(i,j,k)\in\mathbb{N}^3} a_{i,j,k} X^i Y^j Z^k, \quad \text{avec } a_{i,j,k} \in A.$$

EXEMPLE. Considérons par exemple dans $\mathbb{Z}[X, Y, Z]$ les polynômes:

$$P = X^3 + XYZ + X^2Z \quad \text{et} \quad Q = X + Y - Z.$$

P est homogène de degré 3 et Q est homogène de degré 1.

Leur produit $PQ = X^4 + X^3Y + 2X^2YZ - X^2Z^2 + XY^2Z - XYZ^2$ est homogène de degré 4.

1.2 Premières propriétés de l'anneau $A[X_1, X_2, \ldots, X_n]$.

LEMME (propriété universelle des anneaux de polynômes). *Soient A et B deux anneaux et φ un morphisme d'anneaux $A \to B$. Alors, quels que soient un entier $n \geq 1$ et des éléments $b_1, b_2, \ldots, b_n$ de B, il existe un unique morphisme d'anneaux $\Phi : A[X_1, X_2, \ldots, X_n] \to B$ qui prolonge φ (c'est-à-dire $\Phi(a) = \varphi(a)$ pour tout $a \in A$), et tel que $\Phi(X_i) = b_i$ pour tout $1 \leq i \leq n$.*

Preuve. Si Φ existe, il est nécessairement défini par:

$$\Phi\big(\sum a_{i_1,i_2,\ldots,i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}\big) = \sum \varphi(a_{i_1,i_2,\ldots,i_n}) b_1^{i_1} b_2^{i_2} \ldots b_n^{i_n},$$

ce qui réciproquement définit bien un morphisme d'anneaux $A[X_1, X_2, \ldots, X_n] \to B$. □

PROPOSITION (fondamentale). *Soit A un anneau.*

(i) *Pour tout entier $n \geq 2$, il existe dans $A[X_1, X_2, \ldots, X_n]$ un sous-anneau isomorphe à $A[X_1, X_2, \ldots, X_{n-1}]$, et l'on a alors $A[X_1, X_2, \ldots, X_n] \simeq A[X_1, X_2, \ldots, X_{n-1}][X_n]$.*

(i) *En particulier, $A[X, Y] \simeq A[X][Y]$, et $A[X, Y, Z] \simeq A[X, Y][Z] \simeq A[X][Y][Z]$.*

Preuve. Dans $B = A[X_1, X_2, \ldots, X_n]$, considérons l'ensemble C des polynômes $P = \sum a_{i_1,i_2,\ldots,i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$ tels que $a_{i_1,i_2,\ldots,i_n} = 0$ pour tout multi-indice $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$ tel que $i_n \neq 0$. Il est clair que C est un sous-anneau de A isomorphe à $A[X_1, X_2, \ldots, X_{n-1}]$. D'après le lemme précédent (appliqué avec $n = 1$), l'injection canonique $\varphi : C \to B$ se prolonge en un unique morphisme d'anneaux $\Phi : C[X] \to B$ tel que $\Phi(P) = \varphi(P) = P$ pour tout $P \in C$ et $\Phi(X) = X_n$, qui réalise de façon évidente un isomorphisme $C[X] \simeq B$, d'où le résultat en revenant aux notations de l'énoncé. □

THÉORÈME. *Soit A un anneau. Soit n un entier naturel non-nul.*

(i) *Si A est intègre, alors $A[X_1, X_2, \ldots, X_n]$ est intègre.*

(ii) *Si A est factoriel, alors $A[X_1, X_2, \ldots, X_n]$ est factoriel.*

Preuve. On raisonne par récurrence grâce à la proposition précédente, en utilisant la proposition d'intégrité du paragraphe 1.2 du chapitre 6 pour le point (i), et le théorème 2.6 du chapitre 6 pour le point (ii). □

Remarque. On n'a pas de propriétés analogues pour les notions d'anneau principal ou euclidien. Même si K est un corps, $K[X, Y] \simeq K[X][Y]$ n'est pas principal (d'après le théorème 1.7 du chapitre 6).

2. Polynômes symétriques.

Dans toute cette partie, on fixe un entier $n \geq 2$ et un anneau A intègre, et on se place dans l'anneau de polynômes $A[X_1, X_2, \ldots, X_n]$.

2.1 Action canonique du groupe symétrique sur l'anneau des polynômes.

• *Notations.* Pour tout polynôme $P \in A[X_1, X_2, \ldots, X_n]$ et toute permutation $\sigma \in S_n$, on note P_σ le polynôme de $A[X_1, X_2, \ldots, X_n]$ obtenu en permutant les indéterminées $X_1, X_2, \ldots, X_n$ suivant σ, c'est-à-dire:

$$P_\sigma(X_1, X_2, \ldots, X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}).$$

• *Exemple.* $n = 3$, $\sigma = (1, 3, 2)$, $P(X, Y, Z) = X^2 + YZ - 3XY$, alors $P_\sigma(X, Y, Z) = Z^2 + XY - 3ZX$.

• *Remarque.* Si P est constant (c'est-à-dire de degré nul), alors $P = P_\sigma$ pour toute $\sigma \in S_n$.

• Proposition.

(i) *Le groupe S_n opère sur $A[X_1, X_2, \ldots, X_n]$ par l'action:*

$$\begin{array}{ccc} S_n \times A[X_1, X_2, \ldots, X_n] & \to & A[X_1, X_2, \ldots, X_n] \\ (\sigma, P) & \mapsto & P_\sigma \end{array}.$$

(ii) *Quelle que soit $\sigma \in S_n$, l'application:*

$$\begin{array}{ccc} A[X_1, X_2, \ldots, X_n] & \to & A[X_1, X_2, \ldots, X_n] \\ P & \mapsto & P_\sigma \end{array}$$

est un automorphisme de l'anneau $A[X_1, X_2, \ldots, X_n]$.

Preuve. Simple vérification, sans aucune difficulté. □

2.2 Notion de polynôme symétrique.

Définition. Un polynôme $P \in A[X_1, X_2, \ldots, X_n]$ est dit symétrique si $P_\sigma = P$ pour toute $\sigma \in S_n$.

Remarque. L'ensemble des polynômes symétriques n'est autre que l'ensemble des points fixes pour l'action du groupe S_n sur l'ensemble $A[X_1, X_2, \ldots, X_n]$.

Proposition. *L'ensemble des polynômes symétriques est un sous-anneau de l'anneau $A[X_1, X_2, \ldots, X_n]$.*

Preuve. Simple vérification, sans aucune difficulté, utilisant le point (ii) de la proposition précédente. □

Exemples avec $n = 2$. Les polynômes suivants sont des polynômes symétriques dans $A[X, Y]$:

(1) $S_1 = X + Y$, $S_2 = X^2 + Y^2$, $S_3 = X^3 + Y^3$, $\ldots$

(2) $W_1 = X + Y$, $W_2 = X^2 + XY + Y^2$, $W_3 = X^3 + X^2Y + XY^2 + Y^3$, $\ldots$

(3) $D = (X - Y)^2$.

(4) $\Sigma_1 = X + Y$, $\Sigma_2 = XY$.

Exemples avec $n = 3$. Les polynômes suivants sont des polynômes symétriques dans $A[X, Y, Z]$:

(1) $S_1 = X + Y + Z$, $S_2 = X^2 + Y^2 + Z^2$, $S_3 = X^3 + Y^3 + Z^3$, $\ldots$

(2) $W_1 = X + Y + Z$, $W_2 = X^2 + XY + XZ + Y^2 + YZ + Z^2$,
$W_3 = X^3 + Y^3 + Z^3 + X^2Y + XY^2 + X^2Z + XZ^2 + Y^2Z + YZ^2 + XYZ$, $\ldots$

(3) $D = (X - Y)^2(X - Z)^2(Y - Z)^2$.

(4) $\Sigma_1 = X + Y + Z$, $\Sigma_2 = XY + XZ + YZ$, $\Sigma_3 = XYZ$.

Ces exemples sont des cas particuliers des exemples classiques suivants.

EXEMPLES avec n quelconque. Les polynômes suivants sont des polynômes symétriques dans $A[X_1, X_2, \ldots, X_n]$:

(1) les sommes de Newton: $\boxed{S_k = X_1^k + X_2^k + \cdots + X_n^k}$ pour tout $k \in \mathbb{N}$;

(2) les polynômes de Wronski: $\boxed{W_k = \sum_{i_1+i_2+\cdots+i_n=k} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}}$ pour tout $k \in \mathbb{N}$;

(3) le discriminant des indéterminées: $\boxed{D = \prod_{1\leq i<j\leq n} (X_i - X_j)^2}$;

(4) les polynômes symétriques élémentaires:

$\Sigma_1 = X_1 + X_2 + \cdots + X_n$,

$\Sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_2X_n + \cdots + X_{n-1}X_n$,

$\ldots$

$\boxed{\Sigma_k = \sum_{1\leq i_1<i_2<\cdots<i_k\leq n} X_{i_1}X_{i_2}\ldots X_{i_k}}$ pour tout $1 \leq k \leq n$, (somme de C_n^k termes),

$\ldots$

$\Sigma_n = X_1X_2\ldots X_n$.

REMARQUE. Dans l'anneau $A[X_1, X_2, \ldots, X_n][Z]$, le polynôme $P(Z) = (Z - X_1)(Z - X_2)\ldots(Z - X_n)$ vérifie:

$$P(Z) = Z^n - \Sigma_1 Z^{n-1} + \Sigma_2 Z^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}Z + (-1)^n\Sigma_n.$$

2.3 Le théorème fondamental.

On reprend toutes les notations et hypothèses de 2.1 et 2.2. En particulier, on note $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ les polynômes symétriques élémentaires.

• *Premier exemple introductif.*

Considérons dans $\mathbb{Z}[X, Y, Z]$ le polynôme symétrique: $P(X, Y, Z) = X^2Y+XY^2+Y^2Z+YZ^2+Z^2X+ZX^2$.

On calcule:

$\Sigma_1\Sigma_2 = (X+Y+Z)(XY+YZ+ZX) = X^2Y+XYZ+X^2Z+XY^2+Y^2Z+XYZ+XYZ+YZ^2+Z^2X$
$= P(X, Y, Z) + 3XYZ = P(X, Y, Z) + 3\Sigma_3$.

On conclut que: $P(X, Y, Z) = \Sigma_1\Sigma_2 - 3\Sigma_3$,

ou encore: $P(X, Y, Z) = F(\Sigma_1, \Sigma_2, \Sigma_3)$, avec $F = XY - 3Z \in \mathbb{Z}[X, Y, Z]$.

• *Second exemple introductif.*

Considérons dans $\mathbb{Z}[X, Y, Z]$ le polynôme symétrique: $P(X, Y, Z) = (2X-Y-Z)(2Y-Z-X)(2Z-X-Y)$.

On calcule:

$P(X, Y, Z) = (3X - \Sigma_1)(3Y - \Sigma_1)(3Z - \Sigma_1)$
$= (9XY - 3X\Sigma_1 - 3Y\Sigma_1 + \Sigma_1^2)(3Z - \Sigma_1)$.
$= 27XYZ - 9XY\Sigma_1 - 9XZ\Sigma_1 + 3X\Sigma_1^2 - 9YZ\Sigma_1 + 3Y\Sigma_1^2 + 3Z\Sigma_1^2 - \Sigma_1^3$
$= 27XYZ - 9(XY + XZ + YZ)\Sigma_1 + 3(X + Y + Z)\Sigma_1^2 - \Sigma_1^3$.

On conclut que: $P(X, Y, Z) = 27\Sigma_3 - 9\Sigma_2\Sigma_1 + 2\Sigma_1^3$,

ou encore: $P(X, Y, Z) = F(\Sigma_1, \Sigma_2, \Sigma_3)$, avec $F = 27Z - 9XY + 2X^3 \in \mathbb{Z}[X, Y, Z]$.

THÉORÈME. *Soit $n \geq 2$ un entier. Soit A un anneau intègre. Pour tout polynôme symétrique $P \in A[X_1, X_2, \ldots, X_n]$, il existe un unique polynôme $F \in A[X_1, X_2, \ldots, X_n]$ tel que:*

$$P(X_1, X_2, \ldots, X_n) = F(\Sigma_1, \Sigma_2, \ldots, \Sigma_n),$$

où $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ sont les polynômes symétriques élémentaires en les X_i, $1 \leq i \leq n$.

La preuve de ce théorème est relativement longue et technique. On la donnera en détail plus loin dans le chapitre. Auparavant, on développe quelques applications des polynômes symétriques à des questions concrètes d'algèbre.

2.4 Formules de Newton.

On reprend toutes les notations et hypothèses de 2.1 et 2.2. En particulier, on note $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ les polynômes symétriques élémentaires, et $S_1, S_2, \ldots$ les sommes de Newton.

THÉORÈME. *Soit $n \geq 2$ un entier. Soit A un anneau intègre. On a dans l'anneau $A[X_1, X_2, \ldots, X_n]$ les relations suivantes:*

(i) $S_k - \Sigma_1 S_{k-1} + \Sigma_2 S_{k-2} - \cdots + (-1)^{k-1}\Sigma_{k-1}S_1 + (-1)^k k\Sigma_k = 0$, *pour tout* $1 \leq k \leq n$,

(ii) $S_\ell - \Sigma_1 S_{\ell-1} + \Sigma_2 S_{\ell-2} + \cdots + (-1)^n \Sigma_n S_{\ell-n} = 0$, *pour tout* $\ell > n$.

Preuve. Considérons dans l'anneau $A[X_1, X_2, \ldots, X_n][Z]$ le polynôme $P(Z) = (Z - X_1)(Z - X_2)\ldots(Z - X_n)$. Comme on l'a vu à la fin de 2.2, on a:

$$P(Z) = Z^n - \Sigma_1 Z^{n-1} + \Sigma_2 Z^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}Z + (-1)^n\Sigma_n.$$

• Par définition de P, on a $P(X_i) = 0$ pour tout $1 \leq i \leq n$, et donc:

$$X_i^n - \Sigma_1 X_i^{n-1} + \Sigma_2 X_i^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}X_i + (-1)^n\Sigma_n = 0.$$

On fait la somme membre à membre de ces n égalités pour $1 \leq i \leq n$; il vient:

$$S_n - \Sigma_1 S_{n-1} + \Sigma_2 S_{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}S_1 + (-1)^n n\Sigma_n = 0,$$

ce qui est l'assertion (i) pour $k = n$.

• Pour $\ell > n$, on considère dans $A[X_1, X_2, \ldots, X_n][Z]$ le polynôme $Z^{\ell-n}P(Z)$. Pour tout $1 \leq i \leq n$, il vérifie $X_i^{\ell-n}P(X_i) = 0$, donc:

$$X_i^{\ell-n}\big(X_i^n - \Sigma_1 X_i^{n-1} + \Sigma_2 X_i^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}X_i + (-1)^n\Sigma_n\big) = 0,$$

ou encore:

$$X_i^\ell - \Sigma_1 X_i^{\ell-1} + \Sigma_2 X_i^{\ell-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}X_i^{\ell-n+1} + (-1)^n\Sigma_n X_i^{\ell-n} = 0.$$

On fait la somme membre à membre de ces n égalités pour $1 \leq i \leq n$; on obtient exactement l'assertion (ii).

• Pour $k = 1$, la formule (i) est triviale, puisque $S_1 = \Sigma_1$.

• Il reste à prouver (i) pour $1 < k < n$. On raisonne pour cela par récurrence sur le nombre n d'indéterminées. C'est clair pour $n = 3$, car alors $k = 2$ et l'on a bien: $S_2 - \Sigma_1 S_1 + 2\Sigma_2 = 0$. On suppose maintenant la relation (i) vraie dans $A[X_1, X_2, \ldots, X_{n-1}]$, et on fixe $1 < k < n$.

On considère dans $A[X_1, X_2, \ldots, X_n]$ le polynôme $S_k - \Sigma_1 S_{k-1} + \Sigma_2 S_{k-2} - \cdots + (-1)^{k-1}\Sigma_{k-1}S_1 + (-1)^k k\Sigma_k$. Notons-le $Q(X_1, X_2, \ldots, X_{n-1}, X_n)$. Il est clairement homogène de degré k.

Introduisons enfin dans $A[X_1, X_2, \ldots, X_{n-1}]$ le polynôme $Q_0(X_1, \ldots, X_{n-1}) = Q(X_1, \ldots, X_{n-1}, 0)$.

Il est clair que, pour tout $1 \leq i \leq n-1$, on a: $\Sigma_i(X_1, \ldots, X_{n-1}, 0) = \Sigma_i(X_1, \ldots, X_{n-1})$, le i-ième polynôme symétrique élémentaire dans $A[X_1, X_2, \ldots, X_{n-1}]$. Et de même $S_i(X_1, \ldots, X_{n-1}, 0) = S_i(X_1, \ldots, X_{n-1})$. L'hypothèse de récurrence se traduit donc par: $Q_0(X_1, \ldots, X_{n-1}) = 0$ dans $A[X_1, X_2, \ldots, X_{n-1}]$.

En d'autres termes, $Q(X_1, \ldots, X_{n-1}, 0) = 0$ dans $A[X_1, X_2, \ldots, X_{n-1}, X_n]$. On en déduit que Q est divisible par X_n dans $A[X_1, X_2, \ldots, X_{n-1}, X_n]$. Comme Q est symétrique, cela implique que Q est aussi divisible par X_i pour tout $1 \leq i \leq n-1$. Finalement Q est divisible par le produit $X_1 X_2 \ldots X_n$. Comme Q est homogène de degré $k < n$, ce n'est possible que si $Q = 0$, ce qui prouve le résultat voulu, et achève la preuve. □

APPLICATION 1 (*expression des sommes de Newton en fonction des polynômes symétriques élémentaires*). Soit $n \geq 2$ un entier. Soit A un anneau intègre. On a dans l'anneau $A[X_1, X_2, \ldots, X_n]$ les relations suivantes:

$$S_1 = \Sigma_1, \qquad S_2 = S_1\Sigma_1 - 2\Sigma_2 = \Sigma_1^2 - 2\Sigma_2, \qquad S_3 = S_2\Sigma_1 - S_1\Sigma_2 + 3\Sigma_3 = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3, \quad \cdots$$

et ainsi, de proche en proche, l'expression de tous les S_i comme des polynômes en les Σ_j.

APPLICATION 2 (*expression des polynômes symétriques élémentaires en fonction des sommes de Newton; cas d'un corps de caractéristique zéro*). Soit $n \geq 2$ un entier. Soit K un corps de caractéristique zéro. On a dans l'anneau $K[X_1, X_2, \ldots, X_n]$ les relations suivantes:

$$\Sigma_1 = S_1, \qquad \Sigma_2 = \tfrac{1}{2}S_1^2 - \tfrac{1}{2}S_2, \qquad \Sigma_3 = \tfrac{1}{6}S_1^3 - \tfrac{1}{2}S_1S_2 + \tfrac{1}{3}S_3, \quad \cdots$$

et, de proche en proche, l'expression de tous les Σ_j comme des polynômes en les S_i, à coefficients dans K.

COROLLAIRE (une autre forme du théorème fondamental; cas d'un corps de caractéristique zéro). *Soit $n \geq 2$ un entier. Soit A un anneau intègre de caractéristique nulle. Soit K son corps de fractions. Pour tout polynôme symétrique $P \in A[X_1, X_2, \ldots, X_n]$, il existe un unique polynôme $G \in K[X_1, X_2, \ldots, X_n]$ tel que:*

$$P(X_1, X_2, \ldots, X_n) = G(S_1, S_2, \ldots, S_n),$$

où $S_1, S_2, \ldots, S_n$ sont les n premières sommes de Newton en les X_i, $1 \leq i \leq n$.

Preuve. Il suffit de combiner la seconde remarque ci-dessus avec le théorème fondamental de 2.3. □

2.5 Application aux relations entre coefficients et zéros d'un polynôme de $K[X]$.

On fixe un corps K algébriquement clos. Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme de $K[X]$, de degré $n \geq 1$. Il a alors n zéros dans K, que l'on notera $\alpha_1, \alpha_2, \ldots, \alpha_n$, et se factorise en:

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_n \prod_{j=1}^{n} (X - \alpha_j), \quad \text{avec } a_n \neq 0.$$

Pour tout $1 \leq k \leq n$, notons $\Sigma_k = \Sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ le k-ième polynôme symétrique élémentaire en les α_i. On a alors (voir remarque finale de 2.2):

$$\prod_{j=1}^{n} (X - \alpha_i) = X^n - \Sigma_1 X^{n-1} + \Sigma_2 X^{n-2} - \cdots + (-1)^{n-1} \Sigma_{n-1} X + (-1)^n \Sigma_n.$$

On en déduit par identification que:

$$a_{n-1} = -a_n \Sigma_1, \quad a_{n-2} = a_n \Sigma_2, \quad \ldots, \quad a_1 = (-1)^{n-1} a_n \Sigma_{n-1}, \quad a_0 = (-1)^n a_n \Sigma_n.$$

On a ainsi établi:

PROPOSITION. *Si K est un corps algébriquement clos, alors pour tout polynôme $P(X) = \sum_{i=0}^{n} a_i X^i$ de degré $n \geq 1$, les n zéros $\alpha_1, \alpha_2, \ldots, \alpha_n$ de P vérifient:*

$$\Sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}, \quad \text{pour tout } 1 \leq k \leq n.$$

COROLLAIRE. *Soit K un corps. Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ des éléments quelconques de K. Pour tout $1 \leq i \leq n$, posons $\lambda_i = \Sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Alors $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les zéros du polynôme:*

$$X^n - \lambda_1 X^{n-1} + \lambda_2 X^{n-2} - \cdots + (-1)^n \lambda_n.$$

Exemple 1. Pour $P(X) = aX^2 + bX + c \in \mathbb{C}[X]$, avec $a \neq 0$, on retrouve le résultat bien connu:

$$\Sigma_1 = \alpha_1 + \alpha_2 = -\frac{b}{a} \quad \text{et} \quad \Sigma_2 = \alpha_1 \alpha_2 = \frac{c}{a}.$$

Exemple 2. Pour $P(X) = X^3 + pX + q \in \mathbb{C}[X]$, on retrouve le résultat bien connu:

$$\Sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \Sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \quad \text{et} \quad \Sigma_3 = \alpha_1\alpha_2\alpha_3 = -q.$$

3. RÉSULTANT ET DISCRIMINANT

3.1. Position du problème.

DONNÉES, QUESTION, REMARQUES. Dans toute cette partie, K est un corps algébriquement clos. On cherche à résoudre la question suivante:

> étant donnés deux polynômes P et Q de degré ≥ 1 dans $K[X]$, distincts, trouver une condition nécessaire et suffisante pour qu'ils admettent au moins un zéro commun.

Dire que P et Q admettent un zéro commun $\alpha \in K$ équivaut à dire que le polynôme $X - \alpha$ divise à la fois P et Q dans $K[X]$, ce qui équivaut à dire que leur pgcd dans l'anneau $K[X]$ est de degré ≥ 1.

PROPOSITION. *Soit K un corps algébriquement clos. Soient P et Q deux polynômes dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Ils admettent un zéro commun dans K si et seulement s'il existe des polynômes R et S dans $K[X]$ tels que:*

$$\deg R \leq m - 1, \qquad \deg S \leq n - 1, \qquad RQ = SP.$$

Preuve. Supposons les trois conditions de la proposition vérifiées. Appelons $\alpha_1, \alpha_2, \ldots, \alpha_m$ les zéros (non nécessairement distincts) de P dans K. Alors, pour tout $1 \leq i \leq m$, le polynôme $X - \alpha_i$ divise P, donc divise RQ, dans $K[X]$. Puisque $X - \alpha_i$ est premier (car irréductible dans l'anneau principal $K[X]$), on a donc $X - \alpha_i$ divise R ou $X - \alpha_i$ divise Q, et ceci quel que soit $1 \leq i \leq m$. Comme $\deg R < m$, on ne peut pas avoir R divisible par $(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_m)$. C'est donc qu'il existe au moins un indice $1 \leq i_0 \leq m$ tel que $X - \alpha_{i_0}$ divise Q. Ainsi α_{i_0} est un zéro commun à P et Q dans K.

Réciproquement, supposons que P et Q aient un zéro commun $\alpha \in K$. Si D est un pgcd de P et Q dans $K[X]$, on a donc $\deg D \geq 1$, et il existe des polynômes non-nuls R et S dans $K[X]$ tels que $P = RD$ et $Q = SD$, avec $\deg R < \deg P$ et $\deg S < \deg Q$. On a alors l'égalité $RQ = RSD = SP$. □

3.2 Notion de résultant de deux polynômes.

DÉFINITION. Soit K un corps algébriquement clos. Soient P et Q deux polynômes non-nuls dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Notons:

$$P = \sum_{i=0}^{m} a_i X^i \quad \text{et} \quad Q = \sum_{i=0}^{n} b_i X^i, \qquad a_i, b_i \in K, \;\; a_m \neq 0, \;\; b_n \neq 0.$$

On appelle résultant de P et Q le déterminant d'ordre $m+n$ suivant:

$$R(P,Q) = \begin{vmatrix}
a_m & 0 & . & 0 & 0 & b_n & 0 & . & 0 & 0 \\
a_{m-1} & a_m & . & . & . & b_{n-1} & b_n & . & . & . \\
a_{m-2} & a_{m-1} & . & . & . & b_{n-2} & b_{n-1} & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & a_m & 0 & . & . & . & . & . \\
a_{m-n+1} & a_{m-n+2} & . & a_{m-1} & a_m & b_1 & . & . & . & . \\
a_{m-n} & a_{m-n+1} & . & a_{m-2} & a_{m-1} & b_0 & b_1 & . & . & . \\
a_{m-n-1} & a_{m-n} & . & . & a_{m-2} & 0 & b_0 & . & . & . \\
. & . & . & . & . & 0 & 0 & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 0 & . \\
a_2 & a_3 & . & a_n & a_{n+1} & 0 & . & . & b_n & 0 \\
a_1 & a_2 & . & a_{n-1} & a_n & 0 & . & . & b_{n-1} & b_n \\
a_0 & a_1 & . & a_{n-2} & a_{n-1} & 0 & . & . & b_{n-2} & b_{n-1} \\
0 & a_0 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & a_0 & a_1 & . & . & . & b_0 & b_1 \\
0 & 0 & . & 0 & a_0 & 0 & 0 & . & 0 & b_0
\end{vmatrix}$$

$\leftarrow 1$, $\leftarrow 2$, $\leftarrow 3$, $\leftarrow n$, $\leftarrow n+1$, $\leftarrow n+2$, $\leftarrow m-1$, $\leftarrow m$, $\leftarrow m+1$, $\leftarrow m+n$

(n colonnes de gauche, m colonnes de droite)

Remarque. On a ci-dessus, pour fixer clairement l'écriture du déterminant, supposé que $m > n$. Mutatis mutandis, l'analogue pour $m \leq n$ s'en déduit de façon évidente.

THÉORÈME. *Soit K un corps algébriquement clos. Deux polynômes de $K[X]$ non-nuls et non constants ont au moins un zéro commun dans K si et seulement si leur résultant est nul.*

Preuve. Soient $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ dans $K[X]$, de degrés respectifs $m \geq 1$ et $n \geq 1$. D'après la proposition de 3.1, l'existence d'un zéro commun à P et Q équivaut à l'existence de deux polynômes non-nuls $R = \sum_{i=0}^{m-1} \lambda_i X^i$, de degré $\leq m-1$, et $S = \sum_{i=0}^{n-1} \mu_i X^i$, de degré $\leq n-1$, tels que $RQ = SP$. Par identification, cette égalité équivaut aux relations:

$$\begin{cases}
a_m\mu_{n-1} & & = & b_n\lambda_{m-1} & \\
a_{m-1}\mu_{n-1} + a_m\mu_{n-2} & & = & b_{n-1}\lambda_{m-1} + b_n\lambda_{m-2} & \\
a_{m-2}\mu_{n-1} + a_{m-1}\mu_{n-2} + a_m\mu_{n-3} & & = & b_{n-2}\lambda_{m-1} + b_{n-1}\lambda_{m-2} + b_n\lambda_{m-3} & \\
\cdots & & \cdots & \cdots & \\
 & a_0\mu_1 + a_1\mu_0 & = & & b_0\lambda_1 + b_1\lambda_0 \\
 & a_0\mu_0 & = & & b_0\lambda_0
\end{cases}$$

En faisant "tout passer" dans le premier membre, on obtient un système linéaire homogène, de $m+n$ équations à $m+n$ inconnues, ces inconnues étant $\mu_{n-1}, \mu_{n-2}, \ldots, \mu_0, -\lambda_{m-1}, -\lambda_{m-2}, \ldots, -\lambda_0$. Il admet une solution non-nulle si et seulement si son déterminant est nul. Or ce dernier n'est autre que le résultant $R(P,Q)$, d'où le résultat. □

COROLLAIRE. *Soit K un corps algébriquement clos. Deux polynômes de $K[X]$ non-nuls et non constants sont premiers entre eux dans $K[X]$ si et seulement si leur résultant est non-nul.*

Preuve. On a déjà observé en 3.1 que l'existence d'un zéro commun à P et Q équivaut au fait que leur pgcd est de degré ≥ 1, c'est-à-dire que P et Q ne sont pas premiers entre eux. D'où le résultat d'après le théorème précédent. □

Exemples en petits degrés.

- Si $P = aX + b$ et $Q = cX + d$, alors $R(P,Q) = ad - bc$.
- Si $P = aX^2 + bX + c$ et $Q = pX + q$, alors $R(P,Q) = p^2c + q^2a - pqb$.
- Si $P = aX^2 + bX + c$ et $Q = pX^2 + qX + r$, alors $R(P,Q) = (ar - cp)^2 - (aq - bp)(br - cq)$.

Exercice. Soit $a \in K$ un paramètre quelconque. Montrer qu'il existe au plus 7 valeurs de a pour lesquelles les polynômes $P = X^4 + X^3 + X + a + 1$ et $Q = aX^3 + X + a$ ont un zéro commun. (Indication: vérifier que $R(P,Q) = a^7 + 2a^4 + 3a^3 + a^2 + a + 1$.)

3.3 Expression du résultant en fonction des zéros.

THÉORÈME. *Soit K un corps algébriquement clos. Soient P et Q deux polynômes non-nuls dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Notons:*

$$P = \sum_{i=0}^{m} a_i X^i = a_m \prod_{j=1}^{m} (X - \alpha_j) \quad \text{et} \quad Q = \sum_{i=0}^{n} b_i X^i = b_n \prod_{j=1}^{n} (X - \beta_j),$$

où les a_i $(0 \leq i \leq m)$ et les b_i $(0 \leq i \leq n)$ sont les coefficients dans K de P et Q respectivement, avec $a_m \neq 0$ et $b_n \neq 0$, et où les α_j $(1 \leq j \leq m)$ et les β_j $(1 \leq j \leq n)$ sont les zéros dans K de P et Q respectivement.

Alors le résultant $R(P,Q)$ est donné par:

$$R(P,Q) = a_m^n b_n^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (\alpha_i - \beta_j).$$

Preuve. On raisonne en plusieurs étapes.
Première étape. Soient P_1 et Q_1 les polynômes unitaires dans $K[X]$ définis par $P = a_m P_1$ et $Q = b_n Q_1$. On a:

$$P_1 = \prod_{j=1}^{m} (X - \alpha_j) \qquad \text{et} \qquad Q_1 = \prod_{j=1}^{n} (X - \beta_j).$$

Notons $\Sigma_1, \ldots, \Sigma_m$ les fonctions symétriques élémentaires en les zéros $\alpha_1, \ldots, \alpha_m$ de P, et $\Sigma'_1, \ldots, \Sigma'_n$ les fonctions symétriques élémentaires en les zéros $\beta_1, \ldots, \beta_n$ de Q. D'après les résultats de 2.5, on a:

$$\Sigma_1 = -\frac{a_{m-1}}{a_m}, \quad \Sigma_2 = \frac{a_{m-2}}{a_m}, \quad \ldots, \quad \Sigma_m = (-1)^m \frac{a_0}{a_m}, \quad \Sigma'_1 = -\frac{b_{n-1}}{b_n}, \quad \Sigma'_2 = \frac{b_{n-2}}{b_n}, \quad \ldots, \quad \Sigma'_n = (-1)^n \frac{b_0}{b_n},$$

et donc:

$$P_1 = X^m - \Sigma_1 X^{m-1} + \Sigma_2 X^{m-2} - \ldots + (-1)^{m-1} \Sigma_{m-1} X + (-1)^m \Sigma_m,$$
$$Q_1 = X^n - \Sigma'_1 X^{n-1} + \Sigma'_2 X^{n-2} - \ldots + (-1)^{n-1} \Sigma'_{n-1} X + (-1)^n \Sigma'_n.$$

Deuxième étape. Reprenons maintenant les expressions développées $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$.
L'expression du déterminant $R(P,Q)$ vu en 3.2 permet de voir $R(P,Q)$ comme un polynôme en les $n + m + 2$ indéterminées $a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n$. Plus précisément, la forme du déterminant permet d'observer que ce polynôme est homogène de degré n en les indéterminées $a_0, a_1, \ldots, a_m$ et homogène de degré m en les indéterminées $b_0, b_1, \ldots, b_n$. Dans l'anneau $K[a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n]$, notons:

$$R(P,Q) = F(a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n).$$

D'après les observations précédentes:

$$R(P,Q) = a_m^n b_n^m F(\frac{a_0}{a_m}, \frac{a_1}{a_m}, \ldots, \frac{a_{m-1}}{a_m}, 1, \frac{b_0}{b_n}, \frac{b_1}{b_n}, \ldots, \frac{b_{n-1}}{b_n}, 1).$$

Cette relation appliquée aux polynômes P_1 et Q_1 développés comme à la fin de la première étape s'écrit:

$$R(P_1, Q_1) = F\big((-1)^m \Sigma_m,\ (-1)^{m-1} \Sigma_{m-1},\ \ldots,\ -\Sigma_1,\ 1,\ (-1)^n \Sigma'_n,\ (-1)^{n-1} \Sigma'_{n-1},\ \ldots,\ -\Sigma'_1,\ 1 \big).$$

On en déduit d'abord que $R(P_1, Q_1)$ est un polynôme symétrique en $\alpha_1, \alpha_2, \ldots, \alpha_m$ d'une part, et en $\beta_1, \beta_2, \ldots, \beta_n$ d'autre part (c'est le sens évident du théorème 2.3).

On en déduit d'autre part que $R(P,Q) = a_m^n b_n^m R(P_1,Q_1)$, d'où $R(P_1,Q_1) = 0$ si et seulement si $R(P,Q) = 0$, c'est-à-dire d'après le théorème 3.2 si et seulement s'il existe un couple (i,j) avec $1 \leq i \leq m$ et $1 \leq j \leq n$ tel que $\alpha_i = \beta_j$.

Ces deux remarques impliquent que, dans $K[\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n]$, le polynôme $R(P_1,Q_1)$ est divisible par $(\alpha_i - \beta_j)$ pour tous $1 \leq i \leq m$ et $1 \leq j \leq n$, et donc par le produit $\Pi = \prod_{1\leq i\leq m, 1\leq j\leq n}(\alpha_i - \beta_j)$. En comparant pour chacun des polynômes $R(P_1,Q_1)$ et Π les degrés en $\alpha_1,\alpha_2,\ldots,\alpha_m$ et en $\beta_1,\beta_2,\ldots,\beta_n$, ainsi que le coefficient de $(\alpha_1\alpha_2\cdots\alpha_m)^n$, on conclut finalement que $R(P_1,Q_1) = \Pi$.

On en tire que $R(P,Q) = a_m^n b_n^m \Pi$, ce qui achève la preuve. □

Remarque. On a donc du résultant les expressions suivantes:

$$R(P,Q) = a_m^n b_n^m \prod_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} (\alpha_i - \beta_j) = a_m^n \prod_{1\leq i\leq m} Q(\alpha_i) = (-1)^{mn} b_n^m \prod_{1\leq j\leq n} P(\beta_j).$$

qui rendent explicite la conclusion du théorème 3.2.

3.4 Discriminant d'un polynôme.

Définition. Soit K un corps algébriquement clos. On appelle discriminant d'un polynôme P de degré au moins égal à 2 dans $K[X]$ le résultant de P et de son polynôme dérivé P'. On note:

$$\Delta(P) = R(P,P').$$

Théorème. *Soit K un corps algébriquement clos. Soient P un polynôme de degré au moins égal à 2 dans $K[X]$ et P' son polynôme dérivé. Les conditions suivantes sont équivalentes.*

(i) *Le polynôme P a au moins un zéro multiple dans K.*

(ii) *Les polynômes P et P' ne sont pas premiers entre eux.*

(iii) *Les polynômes P et P' ont au moins un zéro commun dans K.*

(iv) *Le discriminant $\Delta(P)$ du polynôme P est nul.*

Preuve. L'équivalence de (ii) et (iii) résulte de la remarque préliminaire de 3.1. Par définition même du discriminant, l'équivalence de (iii) et (iv) est une conséquence du théorème 3.2. Il suffit donc de montrer l'équivalence de (i) et (ii).

Supposons d'abord que P a un zéro multiple α. Alors il existe un polynôme Q de degré $n-2$, où n désigne le degré de P, tel que $P(X) = (X-\alpha)^2 Q(X)$. On a alors $P'(X) = 2(X-\alpha)Q(X) + (X-\alpha)^2 Q'(X)$, de sorte que $X - \alpha$ est un diviseur commun de P et P' de degré non-nul. Donc P et P' ne sont pas premiers entre eux.

Supposons réciproquement que P et P' ne sont pas premiers entre eux. Leur pgcd D est de degré strictement positif. Comme K est algébriquement clos, il admet au moins un zéro $\alpha \in K$. Le polynôme $X - \alpha$ divise D, donc divise P et P'. Il existe en particulier un polynôme Q de degré $n-1$, où n désigne le degré de P, tel que $P(X) = (X-\alpha)Q(X)$. On a alors $P'(X) = Q(X) + (X-\alpha)Q'(X)$. Mais comme $X - \alpha$ divise aussi P', on en déduit qu'il divise Q. Et donc P est divisible par $(X-\alpha)^2$, ce qui achève la preuve. □

Corollaire. *Soit K un corps algébriquement clos. Un polynôme P de degré au moins égal à 2 dans $K[X]$ n'admet que des zéros simples dans K si et seulement si son discriminant est non-nul.*

Exemple 1. Dans $\mathbb{C}[X]$, considérons $P(X) = aX^2 + bX + c$, avec $a \neq 0$. On a $P'(X) = 2aX + b$, et donc:

$$\Delta(P) = R(P,P') = \begin{vmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{vmatrix} = a(4ac - b^2).$$

L'application du corollaire ci-dessus montre que P n'a que des zéros simples si et seulement si $b^2 - 4ac \neq 0$, résultat bien connu !

Exemple 2. Dans $\mathbb{C}[X]$, considérons $P(X) = X^3 + pX + q$. On a $P'(X) = 3X^2 + p$, et donc:

$$\Delta(P) = R(P,P') = \begin{vmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ p & 0 & p & 0 & 3 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{vmatrix} = 4p^3 + 27q^2.$$

Supposons que $\Delta(P) = 0$, et notons α le zéro multiple de P dans K (il est forcément unique puisque P est de degré 3). Comme α est alors aussi zéro de P', on a $\alpha^2 = -\frac{p}{3}$.

Si $p = 0$, alors la nullité de $\Delta(P) = 4p^3 + 27q^2$ implique que l'on a aussi $q = 0$, donc $P(X) = X^3$, qui admet 0 comme zéro triple.

Si $p \neq 0$, alors la nullité de $\Delta(P) = 4p^3 + 27q^2$ implique que l'on a $p = -\frac{27q^2}{4p^2}$, d'où $\alpha^2 = -\frac{p}{3} = \frac{9q^2}{4p^2}$. On vérifie que seul $\alpha = -\frac{3q}{2p}$ est zéro de P, et c'est un zéro double.

PROPOSITION (expression du discriminant en fonction des zéros). *Soit K un corps algébriquement clos. Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de degré $n \geq 2$ dans $K[X]$. Soient $\alpha_1, \ldots, \alpha_n$ les zéros de P dans K. Alors le discriminant de P est donné par:*

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Preuve. On a: $P(X) = a_n \prod_{1 \leq k \leq n} (X - \alpha_k)$, donc: $P'(X) = a_n \sum_{1 \leq j \leq n} \Big(\prod_{1 \leq k \leq n, k \neq j} (X - \alpha_k) \Big)$

d'où, pour tout $1 \leq i \leq n$, l'égalité: $P'(\alpha_i) = a_n(\alpha_i - \alpha_1)(\alpha_i - \alpha_2) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n)$.

On calcule alors en utilisant les expressions de la remarque suivant le théorème 3.3:

$$\begin{aligned}
\Delta(P) = R(P, P') &= a_n^{n-1} \prod_{1 \leq i \leq n} P'(\alpha_i) \\
&= a_n^{n-1} \prod_{1 \leq i \leq n} a_n(\alpha_i - \alpha_1)(\alpha_i - \alpha_2) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n) \\
&= a_n^{2n-1} \prod_{1 \leq i \leq n} (\alpha_i - \alpha_1)(\alpha_i - \alpha_2) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n) \\
&= a_n^{2n-1} \prod_{1 \leq i \leq n} (-1)^{i-1} (\alpha_1 - \alpha_i)(\alpha_2 - \alpha_i) \ldots (\alpha_{i-1} - \alpha_i)(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n) \\
&= a_n^{2n-1} (-1)^{n(n-1)/2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.
\end{aligned}$$

□

Remarque. Cette relation justifie le nom de discriminant des indéterminées donné à l'exemple (3) du paragraphe 2.2.