UFR MATHÉMATIQUES
Université Clermont Auvergne

Master de mathématiques
première année

ALGÈBRE 1
Seconde partie : anneaux

Notes de cours de François DUMAS - année 2020-2021

Table des matières

version provisoire du 6 juillet 2020

Cette deuxième partie des notes, consacrée aux anneaux, est la suite des six chapitres sur les groupes. On renvoie donc à la note préliminaire de cette première partie pour en expliquer les objectifs, et pour quelques références d'ouvrages.

Sur les notions de base concernant les anneaux, on pourra se référer entre autres aux notes de cours de l'U.E. "anneaux et applications" de la troisième année de licence, citée dans le texte sous la forme [PolyL3].

Ces notes contiennent immanquablement des coquilles ou des erreurs. Merci de m'en faire part.

Francois.Dumas@uca.fr

Chapitre 7

Rappels et compléments sur les anneaux quotients

Tous les anneaux considérés ici sont supposés commutatifs et unitaires. On suppose connues les notions de sous-anneau, de morphisme d'anneaux, de groupe des éléments inversibles d'un anneau (ou groupe des unités), d'intégrité, de corps, d'idéal d'un anneau (voir par exemple [PolyL3] chapitres 1, 2 & 3). L'anneau $\mathbb{Z}$, les anneaux $\mathbb{Z}/n\mathbb{Z}$, les anneaux de polynômes, l'anneau des entiers de Gauss et ses variantes, figurent parmi les exemples de références à connaître.

7.1 Théorèmes d'isomorphisme

7.1.1 Rappel : quotient d'un anneau par un idéal

Soit A un anneau commutatif unitaire. Soit I un idéal de A.

(a) L'idéal I est en particulier un sous-groupe du groupe additif A, et il est trivialement normal puisque A est abélien. On peut considérer le groupe additif quotient A/I. Rappelons que, si l'on note $\overline{x}$ la classe dans A/I d'un élément x de A, on a par définition :

$$\overline{x} = \{y \in A\,;\, x - y \in I\} := x + I,$$

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

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{pour tous } x, y \in A.$$

En particulier, le groupe additif A/I est abélien, d'élément neutre additif $\overline{0} = I$, et la surjection canonique $\pi : A \to A/I$, qui à tout élément x de A associe sa classe $\overline{x}$, est un morphisme de groupes pour l'addition.

(b) On définit ensuite dans A/I une multiplication en posant :

$$\overline{x}.\overline{y} = \overline{xy} \quad \text{pour tous } x, y \in A,$$

1. Cette multiplication est bien définie, indépendamment des représentants choisis.

   En effet. Soient $x' \in \overline{x}$ et $y' \in \overline{y}$. Alors $x' - x \in I$ et $y' - y \in I$. On décompose : $x'y' - xy = (x' - x + x)(y' - y + y) - xy = (x' - x)(y' - y) + (x' - x)y + x(y' - y)$. Comme $x' - x \in I$ et que I est un idéal, on a $(x' - x)(y' - y) \in I$ et $(x' - x)y \in I$; de même $x(y' - y) \in I$ puisque $y' - y \in I$. On conclut que $x'y' - xy \in I$ comme somme de trois éléments de I, et donc $\overline{x'y'} = \overline{xy}$.

2. Cette multiplication est associative, commutative, distributive sur l'addition dans A/I, et admet $\overline{1}$ comme élément neutre.

   En effet. Quels que soient $x, y, z \in A$, on a $(\overline{x}\,\overline{y})\,\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\,(\overline{y}\,\overline{z})$, ce qui montre l'associativité. Les autres axiomes d'anneau se vérifient de même. □

3. La surjection canonique π vérifie $\pi(1) = \overline{1}$ et $\pi(xy) = \pi(x)\pi(y)$ pour tous $x, y \in A$.

   En effet. Par définition de π d'une part, et de la multiplication dans A/I d'autre part, on a $\pi(xy) = \overline{xy} = \overline{x}\,\overline{y} = \pi(x)\pi(y)$. □

On a ainsi démontré :

THÉORÈME (anneau quotient). *Soit A un anneau commutatif unitaire. Pour tout idéal I de A, le quotient A/I est un anneau commutatif unitaire, et la surjection canonique $\pi : A \to A/I$ est un morphisme d'anneaux unitaires.*

7.1.2 Propriété universelle de l'anneau quotient

LEMME (factorisation des morphismes). *Soient A un anneau commutatif unitaire, I un idéal de A, et π la surjection canonique $A \to A/I$. Soient A' un anneau commutatif unitaire, I' un idéal de A', et π' la surjection canonique $A' \to A'/I'$.*
Alors, pour tout morphisme d'anneaux unitaires $f : A \to A'$ vérifiant la condition $f(I) \subseteq I'$, il existe un unique morphisme $\varphi : A/I \to A'/I'$ tel que $\varphi \circ \pi = \pi' \circ f$.

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ A/I & \xrightarrow[\varphi]{} & A'/I' \end{array}$$

Preuve. Notons $\overline{x} = \pi(x)$ pour tout $x \in A$ et $\widehat{y} = \pi'(y)$ pour tout $y \in A'$. Posons $\varphi(\overline{x}) = \widehat{f(x)}$ pour tout $x \in A$. Il est facile de vérifier que l'hypothèse $f(I) \subseteq I'$ assure que φ est bien définie (c'est-à-dire que $\widehat{f(x)} = \widehat{f(x')}$ lorsque $\overline{x} = \overline{x}'$). On définit ainsi une application $\varphi : A/I \to A'/I'$, qui est clairement un morphisme d'anneaux unitaires puisque f, π, π' sont des morphismes d'anneaux unitaires. Par construction, φ vérifie $\varphi \circ \pi = \pi' \circ f$, et cette condition impose que ce choix de définition de φ est unique. □

THÉORÈME (propriété universelle de l'anneau quotient). *Soient A un anneau commutatif unitaire, I un idéal de A, et π la surjection canonique $A \to A/I$. Alors :*

(i) *Pour tout anneau commutatif unitaire A' et tout morphisme d'anneaux unitaires $f : A \to A'$ tel que $I \subseteq \operatorname{Ker} f$, il existe un unique morphisme d'anneaux unitaires $\varphi : A/I \to A'$ tel que $f = \varphi \circ \pi$;*

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\varphi} & \\ A/I & & \end{array}$$

(ii) *De plus : (f surjectif $\Rightarrow$ φ surjectif) et ($I = \operatorname{Ker} f$ $\Rightarrow$ φ injectif).*

Preuve. Le point (i) résulte de l'application immédiate du lemme précédent en prenant $I' = \{0_{A'}\}$, de sorte que la condtion $f(I) \subseteq I'$ se traduit par $I \subseteq \operatorname{Ker} f$. Les deux assertions du point (ii) se déduisent immédiatement du fait que $\varphi(\overline{x}) = f(x)$ pour tout $x \in A$. □

7.1.3 Premier et deuxième théorèmes d'isomorphisme

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

Preuve. On applique simplement le théorème 7.1.2 en prenant pour A' le sous-anneau $\operatorname{Im} f$ de B et pour I l'idéal $\operatorname{Ker} f$ de A, de sorte que φ est un isomorphisme. □

Ce résultat est un analogue pour les anneaux du théorème vu en 2.2.3 sur les groupes quotients. On a de même l'analogue suivant du dernier théorème de 2.2.5.

THÉORÈME (dit deuxième théorème d'isomorphisme). *Soit A un anneau commutatif unitaire. Soient B un sous-anneau unitaire de A et I un idéal de A . Alors :*

(i) *$B \cap I$ est un idéal de B ;*

(ii) *$B + I$ est un sous-anneau unitaire de A et I est un idéal de $B + I$;*

(iii) *on a l'isomorphisme d'anneaux $B/(B \cap I) \simeq (B + I)/I$.*

Preuve. Les deux premiers points découlent d'une vérification directe élémentaire laissée au lecteur. Pour le point (iii), on applique le lemme 7.1.2 à l'injection canonique $j : B \to B + I$, qui vérifie bien $j(B \cap I) \subseteq I$. Il existe donc un morphisme d'anneau unitaire φ tel que l'on ait le diagramme :

$$\begin{array}{ccc} B & \xrightarrow{\quad j \quad} & B+I \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ B/(B\cap I) & \xrightarrow[\quad\varphi\quad]{} & (B+I)/I \end{array} ,$$

avec $\varphi \circ \pi = \pi' \circ j$. On vérifie aisément que $\operatorname{Ker}(\pi' \circ j) = B \cap I$ d'où l'injectivité de φ. De même la surjectivité de $\pi' \circ j$ implique celle que φ. □

7.1.4 Idéaux d'un anneau quotient et troisième théorème d'isomorphisme

PROPOSITION ET NOTATION. *Soient A un anneau commutatif unitaire, I un idéal de A et π la surjection canonique $A \to A/I$.*

(i) *Pour tout idéal J de A, l'image $\pi(J)$ est un idéal de A/I ; on le note J/I.*

(ii) *Réciproquement, pour tout idéal K de A/I, il existe un unique idéal J de A contenant I tel que $K = J/I$.*

Preuve. Le point (i) résulte simplement du fait général que l'image d'un idéal par un morphisme d'anneaux surjectif est un idéal. Pour le point (ii), soit K un idéal de A/I. Posons $J = \pi^{-1}(K) = \{x \in A\,;\, \pi(x) \in K\}$. En tant qu'image réciproque d'un idéal par un morphisme d'anneaux, J est un idéal de A. Si $x \in I$, on a $\pi(x) = \overline{0}$, donc $\pi(x) \in K$, de sorte que $x \in \pi^{-1}(K)$, c'est-à-dire $x \in J$. Ceci montre que $I \subseteq J$. Par définition de J, on a $\pi(J) \subseteq K$. Réciproquement, soit $\overline{x} \in K$, avec $x \in A$; comme $\pi(x) = \overline{x} \in K$, on a clairement $x \in \pi^{-1}(K) = J$, et donc $\overline{x} = \pi(x) \in \pi(J)$. En résumé, $K = \pi(J)$, ce que l'on note $K = J/I$.

Montrons maintenant l'unicité. Soit donc J' un idéal de A contenant I tel que $\pi(J) = \pi(J')$. Soit $x \in J$ quelconque. On a $\overline{x} = \pi(x) \in \pi(J)$, donc $\overline{x} \in \pi(J')$. Il existe donc $y \in J'$ tel que $\overline{x} = \overline{y}$, c'est-à-dire $x - y \in I$. Mais $I \subseteq J'$, donc $x - y \in J'$ ce qui, comme $y \in J'$, implique que $x \in J'$. Ceci montre que J est inclus dans J'. L'inclusion réciproque s'obtient de même et l'on conclut que $J = J'$. □

On résume cette proposition en énonçant que :

> *il existe une bijection (à savoir $J \mapsto J/I$) entre l'ensemble des idéaux de A contenant I et l'ensemble des idéaux de l'anneau quotient A/I.*

Exemple d'application (idéaux de $\mathbb{Z}/n\mathbb{Z}$). Fixons un entier $n \geq 2$. Pour tout diviseur q de n, il existe un et un seul idéal de $\mathbb{Z}/n\mathbb{Z}$ d'ordre q, qui est $d\mathbb{Z}/n\mathbb{Z}$ où $n = dq$. Réciproquement tout idéal de $\mathbb{Z}/n\mathbb{Z}$ est de ce type.

> *Par exemple*, dans $\mathbb{Z}/12\mathbb{Z}$, les idéaux sont : $\{\overline{0}\} = 12\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{6}\} = 6\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{4}, \overline{8}\} = 4\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = 3\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} = 2\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$.

Théorème (dit troisième théorème d'isomorphisme). *Soient A un anneau commutatif unitaire et I un idéal de A. Pour tout idéal J/I de A/I, avec J idéal de A contenant I, on a l'isomorphisme d'anneaux $(A/I)/(J/I) \simeq A/J$.*

> *Preuve.* On applique le théorème 7.1.2 : comme $I \subseteq J$, la surjection canonique $\pi' : A \to A/J$, $x \mapsto \widehat{x}$ induit canoniquement un morphisme surjectif $\varphi : A/I \to A/J$, $\overline{x} \mapsto \widehat{x}$. Son noyau est formé des classes $\overline{x} \in A/I$ telles que $x \in J$, c'est-à-dire que $\operatorname{Ker}\varphi = J/I$. D'où le résultat en appliquant le premier théorème d'isomorphisme. □

7.2 Théorème des restes chinois

7.2.1 Somme et produit d'idéaux, idéaux comaximaux

Rappels (voir [PolyL3] chapitre 3). Soit A un anneau commutatif unitaire. Rappelons que :

1. Pour toute partie X non-vide de A, on appelle idéal engendré par X dans A l'intersection de tous les idéaux de A contenant X ; c'est le plus petit idéal de A contenant X. C'est l'ensemble des éléments qui peuvent s'écrire sous la forme de sommes finies $\sum_{j=1}^{k} x_j a_j$ avec $x_1, \ldots, x_k \in X$ et $a_1, \ldots, a_k \in A$.

2. Si X est réduit à un singleton $\{x\}$ avec $x \in A$, l'idéal engendré par X est appelé l'idéal principal engendré x. On le note xA ; c'est l'ensemble des éléments de A qui peuvent s'écrire sous la forme xa avec $a \in A$:
$$xA = \{xa\,;\, a \in A\}.$$

3. Si I et J sont des idéaux de A, la réunion $I \cup J$ n'est en général pas un idéal de A. L'idéal engendré par $I \cup J$ est appelé l'idéal somme de I et J, noté $I + J$; c'est l'ensemble des éléments de A pouvant s'écrire comme somme d'un élément de I et d'un élément de J :
$$I + J = \{x + y\,;\, x \in I, y \in J\}.$$

4. En particulier, si x et y sont deux éléments de A, l'idéal de A engendré par x et y est la somme des deux idéaux principaux xA et yA :
$$xA + yA = \{xa + yb\,;\, a, b \in A\}.$$

5. Si I et J sont des idéaux de A, l'ensemble des produits d'un élément de I par un élément de J n'est en général pas un idéal de A. L'idéal engendré par cet ensemble est appelé l'idéal produit de I et J, noté IJ ; il vérifie $IJ \subset I \cap J$, et l'on a pour tout $x \in A$:
$$(\ x \in IJ\ ) \Leftrightarrow (\ \textit{il existe } n \in \mathbb{N}^*,\ y_1, \ldots, y_n \in I,\ z_1, \ldots, z_n \in J,\ \textit{tels que } x = \sum_{i=1}^{n} y_i z_i\ ).$$

EXERCICE. Montrer que, pour trois idéaux I, J, K d'un anneau commutatif unitaire A, on a :

$$I + (J + K) = (I + J) + K, \qquad I(JK) = (IJ)K, \qquad I(J + K) = IJ + IK.$$

DÉFINITION. Soit A un anneau commutatif unitaire. On dit que deux idéaux I et J de A sont *comaximaux* (ou encore *étrangers*) lorsque $I + J = A$.

PROPOSITION. *Soit A un anneau commutatif unitaire.*

(i) *Si I et J sont deux idéaux comaximaux de A, alors $IJ = I \cap J$*

(ii) *Si de plus A est un anneau principal, et si I et J sont deux idéaux non-nuls de A vérifiant $IJ = I \cap J$, alors ils sont comaximaux.*

Preuve. Montrons (i). On a toujours $IJ \subseteq I \cap J$. Réciproquement, soit $x \in I \cap J$ quelconque. L'hypothèse $A = I + J$ permet d'écrire $1 = a + b$ avec $a \in I$ et $b \in J$, donc $x = xa + xb$. Mais $xa \in IJ$ car $x \in J$ et $a \in I$, et $xb \in IJ$ car $x \in I$ et $b \in J$. Donc $x = xa + xb \in IJ$. On a ainsi montré que $IJ = I \cap J$.

Pour (ii), supposons maintenant que A est principal. Il existe donc $x, y \in A$ non-nuls tels que $I = xA$ et $J = yA$. Il est clair qu'on a alors $IJ = xyA$. Il existe aussi $d \in A$ tel que $I+J = dA$. Il s'agit de vérifier que d est inversible dans A, ce qui montrera bien que $dA = A$. L'inclusion $I \subseteq I + J$, ou encore $xA \subseteq dA$ se traduit par l'existence d'un élément $x' \in A$ tel que $x = dx'$. De même il existe $y' \in A$ tel que $y = dy'$. Considérons l'élément $m = dx'y' = xy' = x'y$. Il est clair que $m \in I \cap J$. Donc d'après l'hypothèse, $m \in xyA$. Il existe donc $k \in A$ tel que $dx'y' = m = kxy = kd^2x'y'$, ou encore $(kd - 1)dx'y' = 0$. L'intégrité de A implique alors $kd = 1$, ce qui achève la preuve.

REMARQUE. On aura reconnu (voir [PolyL3] chapitre 6) dans la preuve du point (ii) que d est le pgcd de x et y, qui est ici inversible, ce qui correspond au fait que x et y sont premiers entre eux, c'est-à-dire par le théorème de Bézout que $A = xA + yA$.

REMARQUE. Le point (ii) n'est plus vrai lorsqu'on ne suppose plus A principal ; il peut exister alors des idéaux non-nuls I, J qui vérifie $IJ = I \cap J$ mais ne sont pas comaximaux.
Contrexemple : prendre $A = K[X, Y]$ où K est un corps commutatif, $I = AX$ et $J = AY$. Il est clair que $I \cap J = AXY = IJ$, et pourtant $AX + AY \neq A$.

THÉORÈME (des restes chinois). *Soit A un anneau commutatif unitaire. Soient I et J deux idéaux comaximaux de A. Alors :*

$$IJ = I \cap J, \text{ et on a un isomorphisme d'anneaux } A/I \times A/J \simeq A/IJ.$$

Preuve. On a déjà remarqué à la proposition précédente que $IJ = I \cap J$. Introduisons l'application $f : A \to A/I \times A/J$ produit des deux surjections canoniques $\pi : A \to A/I$ et $\pi' : A \to A/J$; f est définie par $f(x) = (\overline{x}, \widehat{x})$, avec $\pi(x) = \overline{x}$ et $\pi'(x) = \widehat{x}$. Il est clair que f est un morphisme d'anneaux de noyau $\operatorname{Ker} f = I \cap J$. On va montrer que f est surjective. Pour cela, fixons un élément quelconque $(\overline{y}, \widehat{z})$ de $A/I \times A/J$. L'hypothèse $A = I + J$ permet d'écrire $1 = a + b$ avec $a \in I$ et $b \in J$. Posons $x = yb + za$. On a $yb \in J$ et $za \in I$, donc $\pi(x) = \pi(yb) = \pi(y - ya) = \pi(y) = \overline{y}$ et $\pi'(x) = \pi'(za) = \pi'(z - zb) = \pi'(z) = \widehat{z}$. On conclut que $f(x) = (\overline{y}, \widehat{z})$, ce qui montre la surjectivité de f. Il suffit d'appliquer alors le premier théorème d'isomorphisme à f pour conclure que $A/IJ = A/(I \cap J) = A/\operatorname{Ker} f \simeq \operatorname{Im} f = A/I \times A/J$. □

Le théorème dit des restes chinois en arithmétique élémentaire correspond au cas où $A = \mathbb{Z}$, $I = m\mathbb{Z}$ et $J = n\mathbb{Z}$ pour deux entiers m et n premiers entre eux.

7.2.2 Cas d'un nombre fini quelconque d'idéaux

DÉFINITIONS. Soit A un anneau commutatif unitaire. Si $I_1, I_2, \ldots, I_k$ sont des idéaux de A, on peut définir de façon naturelle l'idéal produit $I_1 I_2 \cdots I_k$ comme l'idéal engendré par l'ensemble tous les éléments de la forme $\prod_{j=1}^{k} x_j$ où $x_j \in I_j$ pour tout $1 \leq j \leq k$. Ses éléments sont donc toutes les sommes finies de produits de ce type.

PREMIER LEMME. *Soient A un anneau commutatif unitaire, et $I_1, I_2, \ldots, I_k$ des idéaux de A. Si un idéal I de A est comaximal avec chacun des I_j, $1 \leq j \leq k$, alors I est comaximal avec l'idéal produit $I_1 I_2 \cdots I_k$.*

> *Preuve.* Pour tout $1 \leq j \leq k$, on a par hypothèse $I + I_j = A$, donc il existe $x_j \in I$ et $y_j \in I_j$ tels que $x_j + y_j = 1$. Il en résulte que $\prod_{j=1}^{k}(x_j + y_j) = 1$. Or il est clair que ce produit se développe sous la forme $x + \prod_{j=1}^{k} y_j$, où x est une somme dont chaque terme contient en facteur au moins l'un des x_j, de sorte que $x \in I$. Comme par ailleurs $y = \prod_{j=1}^{k} y_j$ appartient à l'idéal produit $I_1 I_2 \cdots I_k$, l'égalité $x + y = 1$ prouve la propriété voulue. □

SECOND LEMME. *Soient A un anneau commutatif unitaire, et $I_1, I_2, \ldots, I_k$ des idéaux de A. Si les idéaux $I_1, I_2, \ldots, I_k$ sont deux à deux comaximaux, alors :*

$$I_1 I_2 \cdots I_k = I_1 \cap I_2 \cap \cdots \cap I_k.$$

> *Preuve.* On procède par récurrence sur k. Le cas $k = 2$ a été montré au point (i) de la proposition 7.2.1. Supposons le lemme vrai jusqu'à un rang k et considérons des idéaux $I_1, \ldots, I_k, I_{k+1}$ deux à deux comaximaux. Par hypothèse de récurrence, le produit $I = I_1 I_2 \cdots I_k$ est égal à l'intersection $I_1 \cap I_2 \cap \cdots \cap I_k$. Par ailleurs I et I_{k+1} sont comaximaux d'après le lemme précédent. Donc d'après le point (i) de la proposition 7.2.1, on a $I I_{k+1} = I \cap I_{k+1}$, c'est-à-dire $I_1 I_2 \cdots I_k I_{k+1} = I_1 \cap I_2 \cap \cdots \cap I_k \cap I_{k+1}$, ce qui achève la preuve. □

THÉORÈME (des restes chinois). *Soient A un anneau commutatif unitaire, et $I_1, I_2, \ldots, I_k$ des idéaux de A. Si les idéaux $I_1, I_2, \ldots, I_k$ sont deux à deux comaximaux, alors on a un isomorphisme d'anneaux :*

$$A/(I_1 I_2 \cdots I_k) \simeq A/I_1 \times A/I_2 \times \cdots \times A/I_k.$$

> *Preuve.* D'après le second lemme, on introduit l'idéal $P = I_1 I_2 \cdots I_k = I_1 \cap I_2 \cap \cdots \cap I_k$. Pour pouvoir distinguer les classes modulo les différents idéaux $P, I_1, \ldots, I_k$, on convient d'utiliser la notation additive des classes ; comme la classe $\overline{x}$ d'un élément x de A modulo P est l'ensemble des $y \in A$ tels que $y - x \in P$, on note $\overline{x} = x + P$. On note de même $x + I_\ell$ la classe de x modulo I_ℓ pour tout $1 \leq \ell \leq k$.
>
> Considérons l'application :
>
> $$\phi \ : \ A/P \longrightarrow A/I_1 \times A/I_2 \times \cdots \times A/I_k, \ x + P \longmapsto (x + I_1, x + I_2 \ldots, x + I_k)$$
>
> Il est clair que ϕ est bien définie car P est inclus dans chacun des I_ℓ, et donc deux éléments ayant la même classe modulo P ont la même classe modulo chacun des I_ℓ. Il est clair aussi que ϕ est un morphisme d'anneaux.
>
> Pour vérifier l'injectivité de ϕ prenons un élément $x \in A$ tel que $x + P$ appartienne à $\operatorname{Ker} \phi$. Cela signifie que, pour tout $1 \leq \ell \leq k$, la classe de $x + I_\ell$ est nulle dans A/I_ℓ, c'est-à-dire que $x \in I_\ell$ donc $x \in P$, ou encore $x + P$ nulle dans A/P. Le noyau de ϕ est donc trivial.
>
> Montrons la surjectivité de ϕ. Il s'agit de montrer que, quels que soient $x_1, \ldots, x_k \in A$, il existe $x \in A$ tel que $x - x_\ell \in I_\ell$ pour tout $1 \leq \ell \leq k$, de sorte que $x + P$ est un antécédent

de $(x_1 + I_1, \ldots, x_k + I_k)$ pour ϕ. Pour cela, introduisons pour tout $1 \leq r \leq k$, en utilisant le second lemme, l'idéal :

$$P_r := I_1 I_2 \ldots I_{r-1} I_{r+1} \ldots I_k = I_1 \cap I_2 \cap \cdots \cap I_{r-1} \cap I_{r+1} \cap \cdots \cap I_k$$

D'après le premier lemme, I_r et P_r sont comaximaux, et il existe donc $a_r \in I_r$ et $b_r \in P_r$ tels que $a_r + b_r = 1$. Remarquons que par définition même, on a :

$$\text{pour tout } 1 \leq r \leq k,\ b_r - 1 \in I_r, \text{ et } b_r \in I_\ell \text{ quel que soit } 1 \leq \ell \neq r \leq k.$$

Donnons-nous alors $x_1, \ldots, x_k \in A$ quelconque. Posons $x = \sum_{r=1}^{k} b_r x_r$. Pour tout $1 \leq \ell \leq k$, on a $x - x_\ell = (b_\ell - 1)x_\ell + \sum_{r=1, r\neq\ell}^{k} b_r x_r$. Le premier terme appartient à I_ℓ car $b_\ell - 1 \in I_\ell$, et la somme appartient à I_ℓ car dans chacun de ses termes $b_r \in I_\ell$. Ainsi $x - x_\ell \in I_\ell$ et ceci pour tout $1 \leq \ell \leq k$, ce qui achève la preuve. □

7.3 Théorème de Krull

7.3.1 Rappel : idéaux premiers et idéaux maximaux

Définitions. Soit A un anneau commutatif unitaire.

Un idéal P de A est dit *premier* lorsque $P \neq A$ et vérifie :

quels que soient deux éléments x et y de A, si $xy \in P$, alors $x \in P$ ou $y \in P$.

Un idéal M de A est dit *maximal* lorsque $M \neq A$ et vérifie :

quel que soit I un idéal de A, si M est strictement inclus dans I, alors $I = A$.

Remarques. Par définition, $\{0\}$ est premier si et seulement si A est intègre. Si A est un corps, l'idéal $\{0\}$ est l'unique idéal maximal de A, et si A n'est pas un corps, $\{0\}$ n'est pas maximal.

Théorème. *Soit I un idéal d'un anneau commutatif unitaire A. On a :*

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

Preuve. Supposons que M est un idéal maximal de A. Comme $M \neq A$, l'anneau A/M est non-nul. Considérons un idéal quelconque K de A/M. D'après la proposition 7.1.4, il existe un idéal J de A tel que $M \subseteq J$ et $K = J/M$. Mais, par maximalité de M, l'inclusion $M \subseteq J$ implique que $J = M$ ou $J = A$, c'est-à-dire $J/M = \{\overline{0}\}$ ou $J/M = A/M$. Ceci prouve que les seuls idéaux de A/M sont $\{\overline{0}\}$ et A/M. On sait (voir [PolyL3] que cela traduit que A/M est un corps. L'implication réciproque découle des mêmes calculs. L'équivalence de la première ligne est donc vérifiée.

Supposons que P est un idéal premier de A. Comme $P \neq A$, l'anneau A/P est non-nul. Considérons $\overline{x}, \overline{y} \in A/P$ tels que $\overline{x}\ \overline{y} = \overline{0}$. On a $\overline{xy} = \overline{0}$, c'est-à-dire $xy \in P$. Comme P est premier, on a $x \in P$ ou $y \in P$, c'est-à-dire $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Donc A/P est intègre. L'implication réciproque découle des mêmes calculs. L'équivalence de la seconde ligne est vérifiée. Il suffit de rappeler que tout corps est un anneau intègre pour achever la preuve. □

Corollaire (idéaux premiers et maximaux d'un anneau quotient) *Soient A un anneau commutatif unitaire et I un idéal de A. La bijection $J \mapsto J/I$ entre l'ensemble des idéaux de A*

contenant I et l'ensemble des idéaux de A/I induit par restriction une bijection entre l'ensemble des idéaux premiers (respectivement maximaux) de A contenant I et l'ensemble des idéaux premiers (respectivement maximaux) de A/I.

> *Preuve.* Soit K un idéal de A/I et J l'unique idéal de A contenant I tel que $K = J/I$ (voir proposition 7.1.4). D'après le théorème 7.1.4, on a l'isomorphisme d'anneaux $(A/I)/K \simeq A/J$. Dès lors, J est premier (resp. maximal) dans A si et seulement si A/J est intègre (resp. est un corps), c'est-à-dire si et seulement si $(A/I)/K$ est intègre (resp. est un corps), ce qui est équivaut à dire que K est un idéal premier (resp. maximal) de A/I. □

PROPOSITION. *Dans un anneau principal, tout idéal premier non-nul est maximal (et donc, pour les idéaux non-nuls, les notions de premier et de maximal coïncident).*

> *Preuve.* Soit I un idéal premier non-nul de A. Il existe donc $a \in A$, $a \neq 0$, tel que $I = aA$. Soit J un idéal de A tel que $I \subset J$. Il existe $b \in A$, $b \neq 0$, tel que $J = bA$. Comme $a \in I$, on a $a \in J$ donc il existe $x \in A$ tel que $a = bx$. Supposons que $I \neq J$, c'est-à-dire que $b \notin I$. Ainsi $a = bx \in I$ avec $b \notin I$, donc le fait que I soit premier implique que $x \in I$. Donc il existe $y \in A$ tel que $x = ay$. On déduit que $a = bx = bay$, ou encore $a(1 - by) = 0$. L'intégrité de A implique que $1 - by = 0$, d'où $by = 1$, ce qui prouve que $b \in U(A)$, c'est-à-dire $J = A$. Ainsi, pour tout idéal J de A tel que $I \subset J$ et $J \neq I$, on a $J = A$. Donc I est un idéal maximal. □

REMARQUE. La proposition ci-dessus n'est plus vraie si l'on ne suppose plus que A est principal : il existe des anneaux commutatifs unitaires A possédant des idéaux premiers non-nuls qui ne sont pas maximaux.

> *Exemple.* Prenons $A = \mathbb{Z}[X]$ et $I = XA$ l'idéal principal engendré par X. Soit $f : A \to \mathbb{Z}$ l'application qui à tout polynôme $P = a_m X^m + \cdots + a_1 X + a_0$, avec les $a_i \in \mathbb{Z}$, associe le terme constant a_0. Il est facile de vérifier que f est un morphisme d'anneaux unitaires, qu'il est surjectif, et que son noyau est $I = XA$. D'après le premier théorème d'isomorphisme, on a alors $A/I \simeq \mathbb{Z}$. Comme $\mathbb{Z}$ est intègre sans être un corps, l'idéal I est premier sans être maximal. □

L'exemple ci-dessus montre que, bien que $\mathbb{Z}$ soit un anneau principal, l'anneau $\mathbb{Z}[X]$ n'est pas un anneau principal.

> *Remarque.* A titre d'exercice, on peut aussi le montrer de façon élémentaire en vérifiant que, par exemple, l'idéal $I = 2A + XA$ 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 $2 = PQ$, d'où 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. □

On verra plus loin en 8.2.3 qu'en fait un anneau de polynômes $A[X]$ est principal si et seulement si A est un corps (voir aussi [PolyL3]).

Le théorème de Krull qui fait l'objet du paragraphe 7.3.3 est un résultat important et non trivial qui démontre l'existence d'idéaux maximaux dans tout anneau unitaire commutatif. Sa preuve utilise des arguments d'algèbre générale sur les structures ordonnées, dont le lemme de Zorn, que l'on rappelle ci-dessous.

7.3.2 Rappels et compléments : ensembles ordonnés et lemme de Zorn

DÉFINITIONS. Soit E un ensemble. On appelle *ordre* sur E ou *relation d'ordre* sur E une relation binaire $\preceq$ qui est à la fois réflexive, antisymétrique et transitive ; rappelons que cela signifie respectivement :

- pour tout $x \in E$, on a $x \preceq x$,
- pour tous $x, y \in E$, si $x \preceq y$ et $y \preceq x$, alors $x = y$,
- pour tous $x, y, z \in E$, si $x \preceq y$ et $y \preceq z$, alors $x \preceq z$.

On dit que $(E, \preceq)$ est un *ensemble ordonné*. Il est clair que tout sous-ensemble d'un ensemble ordonné est un ensemble ordonné (si $\preceq$ est une relation d'ordre sur E, elle est une relation d'ordre sur tout sous-ensemble de E).

DÉFINITIONS. Soit $(E, \preceq)$ un ensemble ordonné. Deux cas sont possibles :

- si, quels que soient deux éléments $x, y \in E$, on a $x \preceq y$ ou $y \preceq x$, on dit que $\preceq$ est un *ordre total*, et que $(E, \preceq)$ est un ensemble *totalement ordonné*.
- sinon, l'ordre est dit *partiel* et $(E, \preceq)$ est un ensemble *partiellement ordonné*.

Concrètement, tous les éléments d'un ensemble totalement ordonné sont deux à deux comparables par la relation d'ordre, et ce n'est pas le cas dans un ensemble partiellement ordonné.

DÉFINITIONS. Soit $(E, \preceq)$ un ensemble ordonné.

1. On appelle *élément maximal* dans E tout un élément $x \in E$ tel que :
$$\text{pour tout } y \in E, \text{ si } x \preceq y, \text{ alors } x = y.$$
2. Pour tout sous-ensemble F de E, on appelle *majorant* de F dans E tout élément $m \in E$ tel que $x \preceq m$ pour tout $x \in F$.
3. On dit que l'ensemble ordonné $(E, \preceq)$ est *inductif* lorsque tout sous-ensemble non-vide totalement ordonné de E admet un majorant dans E.

LEMME DE ZORN. *Si $(E, \preceq)$ est un ensemble ordonné inductif non-vide, alors il admet (au moins) un élément maximal.*

> *Preuve.* Voir ouvrage de référence ; elle pourra être exposée en cours si le temps le permet. □

C'est cet argument qui permet par exemple de démontrer en toute généralité l'existence d'une base dans un espace vectoriel, ou de démontrer le théorème de Hahn-Banach. Dans le cadre de ce cours, on va l'appliquer à l'ensemble des idéaux d'un anneau commutatif unitaire, partiellement ordonné par l'inclusion.

7.3.3 Existence d'idéaux maximaux

THÉORÈME (de Krull). *Tout anneau commutatif unitaire non-nul admet un moins un idéal maximal.*

> *Preuve.* Soit A un anneau commutatif unitaire. Soit E l'ensemble de tous les idéaux de A distincts de A. Il est non vide, car contient au moins $\{0\}$. L'inclusion définit une relation d'ordre dans E. Ce n'est pas un ordre total, mais seulement un ordre partiel (si $I, J \in E$ quelconques, on n'a pas forcément $I \subseteq J$ ou $J \subseteq I$).

Soit $F = \{I_k\}_{k\in X}$ une famille d'éléments de E totalement ordonnée par l'inclusion, c'est-à-dire que, quels que soient $k, \ell \in X$, on a $I_k \subseteq I_\ell$ ou $I_\ell \subseteq I_k$. On introduit la réunion $I := \bigcup_{k\in X} I_k$. En général une réunion d'idéaux n'est pas un idéal (car cette réunion n'est pas stable par addition), mais du fait que les idéaux I_k sont ici supposés totalement ordonnés, il est facile de vérifier que I est un idéal de A.

Si l'on avait $I = A$, on aurait $1 \in I$, donc il existerait $k \in X$ tel que $1 \in I_k$, d'où $I_k = A$, ce qui contredirait $I_k \in E$. C'est donc que $I \neq A$, c'est-à-dire que $I \in E$. Enfin il est clair que tout $I_k \in F$ vérifie $I_k \subseteq I$, de sorte que I est un majorant de F dans E. En résumé, on a montré que E ordonné par l'inclusion est un ensemble partiellement ordonné inductif.

Par application du lemme de Zorn, E admet (au moins) un élément maximal M. Cela signifie que $M \neq A$ et que, quel que soit un idéal J de A tel que $J \neq A$ et $M \subseteq J$, on a $J = M$. On conclut que M est un idéal maximal de A au sens de la définition de 7.3.1. □

COROLLAIRE (forme pratique d'application du théorème de Krull). *Soit A un anneau commutatif unitaire.*

(i) *Tout idéal de A distinct de A est contenu dans un idéal maximal de A.*

(ii) *Tout élément de A non inversible dans A est contenu dans un idéal maximal de A.*

Preuve. Soit I un idéal de A tel que $I \neq A$. D'après le théorème de Krull, l'anneau A/I admet un idéal maximal N. D'après le corollaire 7.3.1, il existe un unique idéal maximal M de A contenant I tel que $N = M/I$, ce qui prouve le point (i). La seconde assertion en découle immédiatement en considérant pour tout $x \in A$ non-inversible dans A l'idéal principal xA qui est alors distinct de A. □

Chapitre 8

Arithmétique dans les anneaux principaux

8.1 Rappels généraux sur la divisibilité

Le but de cette section est de rappeler comment, dans un anneau commutatif unitaire A, les principales notions sur la divisibilité s'interprètent en termes d'idéaux principaux. Rappelons que, pour tout $x \in A$, on note $xA = \{xy\,;\, y \in A\}$ l'idéal principal de A engendré par x.

8.1.1 Multiples, diviseurs, éléments associés

Définitions. Soit A un anneau commutatif unitaire. Soient x et y deux éléments de A. On dit que x est un *diviseur* de y dans A, ou encore que x *divise* y dans A, ou encore que y est un *multiple* de x dans A, lorsqu'il existe $a \in A$ tel que $y = xa$. On note alors : $x|y$.

Proposition. *Soit A un anneau commutatif unitaire. Pour tous $x, y \in A$, on a :*

$$(\ x|y\ ) \Leftrightarrow (\ y \in xA\ ) \Leftrightarrow (\ yA \subseteq xA\ ).$$

Preuve. Supposons que $x|y$. Il existe $a \in A$ tel que $y = xa$. Donc $y \in xA$. De plus, tout élément de yA est de la forme yb avec $b \in A$, donc de la forme xab, et donc appartient à xA, ce qui montre que $yA \subseteq xA$. La réciproque est claire. □

Remarques. On déduit immédiatement que :

- Pour tous $x, y, z \in A$, $(\ x|y$ et $y|z)\ \Rightarrow\ (\ x|z\ )$.
- Pour tout $u \in A$, $(\ u \in U(A)\ ) \Leftrightarrow (\ uA = A\ ) \Leftrightarrow (\ u|y$ quel que soit $y \in A\ )$.
- Pour tous $x, u \in A$, $(\ u \in U(A)$ et $x|u\ ) \Rightarrow (\ x \in U(A)\ )$.

Définition. Soit A un anneau commutatif unitaire *intègre*. Soient x et y deux éléments de A. On dit que x et y sont *associés* lorsqu'on a à la fois $x|y$ et $y|x$. On note alors $x \sim y$.

Proposition. *Soit A un anneau commutatif unitaire intègre. Pour tous $x, y \in A$, on a :*

$$(\ x \sim y\ ) \Leftrightarrow (\ x|y \text{ et } y|x\ ) \Leftrightarrow (\ xA = yA\ ) \Leftrightarrow (\ \textit{il existe } u \in U(A) \textit{ tel que } x = uy).$$

Preuve. La première équivalence est vraie par définition, la seconde découle de 8.1.1. Pour la dernière, supposons que $x \sim y$. Il existe $u, v \in A$ tels que $x = uy$ et $y = vx$, donc $x = uvx$. Si $x = 0$, alors $y = 0$, et on a $x = uy$ pour tout $u \in U(A)$. Si $x \neq 0$, on écrit

$x(1-uv)=0$; l'intégrité de A implique que $uv=1$, d'où $u \in U(A)$, ce qui montre le résultat voulu. Réciproquement, supposons $x=uy$ avec $u \in U(A)$; on a $y|x$ et, puisque $y=u^{-1}x$ avec $u^{-1} \in A$, on a aussi $x|y$. On conclut que $x \sim y$. □

EXEMPLES.

(a) Dans $\mathbb{Z}$, deux entiers m et n sont associés si et seulement si $m = \pm n$.

(b) 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 l'on a alors $Q = c^{-1}P$.

(c) 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 $P = cQ$.

REMARQUE. Deux éléments associés ont les mêmes multiples et les mêmes diviseurs dans A.

En effet. Supposons $x \sim y$. On a $xA = yA$. Soit z un diviseur de y ; alors $yA \subseteq zA$, d'où $xA \subseteq zA$, c'est-à-dire que z divise x. □

8.1.2 Eléments irréductibles, éléments premiers.

DÉFINITIONS. Soit A un anneau commutatif unitaire *intègre*. Soit x un élément de A.

(a) x est dit *irréductible* dans A lorsqu'il n'est pas inversible dans A, et vérifie :

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

(b) x est dit *premier* dans A lorsqu'il est non-nul et non inversible dans A, et vérifie :

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

EXEMPLES.

1. Dans $\mathbb{Z}$, les éléments premiers et les éléments irréductibles sont les mêmes : ce sont les nombres premiers et leurs opposés.
2. Pour tout corps K, les polynômes de degré un sont toujours irréductibles dans $K[X]$. Si $K = \mathbb{C}$, les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un. 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 négatif.

REMARQUES.

- 0 n'est pas irréductible dans A.
- Dans la définition (a), le "ou" est exclusif. En d'autres termes, si x est irréductible dans A et s'écrit $x = ab$, alors un seul des deux éléments a, b appartient à $U(A)$.
- 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 pas dans $\mathbb{Q}$ puisqu'il est inversible dans $\mathbb{Q}$.

PROPOSITION (caractérisation en termes d'idéaux principaux). *Soit A un anneau commutatif unitaire intègre. Pour tout $x \in A$, on a :*

(i) *(x irréductible dans A) $\Leftrightarrow$ (xA maximal parmi les idéaux principaux de A distincts de A).*

(ii) *(x premier dans A) $\Leftrightarrow$ (xA idéal premier non-nul de A).*

Preuve. Supposons x irréducible. L'idéal principal $M = xA$ est distinct de A car $x \notin U(A)$. Soit $J = aA$ un idéal principal de A distinct de A, c'est-à-dire tel que $a \notin U(A)$, et supposons que $M \subseteq J$. Alors en particulier $x \in J$, donc il existe $b \in A$ tel que $x = ab$. Puisque $a \notin U(A)$, l'irréductibilité de x implique que $b \in U(A)$. Donc $x \sim a$, d'où $M = J$. Ceci prouve que M est maximal parmi les idéaux principaux distincts de A.

Réciproquement soit $x \in A$ tel que xA soit maximal parmi les idéaux principaux distincts de A. Soient $a, b \in A$ tels que $x = ab$. Alors $x \in aA$, et donc $xA \subseteq aA$. Si $a \in U(A)$, alors $aA = A$. Sinon, $aA \neq A$ et la maximalité de xA implique alors que $xA = aA$, donc $x \sim a$, d'où l'existence de $u \in U(A)$ tel que $x = ua$. Mais $x = ua = ba$ implique par intégrité de A que $b = u$, et donc $b \in U(A)$. L'assertion (i) est ainsi établie.

L'équivalence (ii) est quant à elle évidente par définition même d'un idéal premier (cf. 7.3.1) et par la proposition 8.1.1. □

Corollaire. *Soit A un anneau commutatif unitaire intègre.*

(i) *Tout élément de A associé à un élément irréductible dans A est irréductible dans A.*

(ii) *Tout élément de A associé à un élément premier dans A est premier dans A.*

Preuve. Découle de la proposition précédente puisque deux éléments associés engendrent le même idéal principal. □

Proposition. *Soit A un anneau commutatif unitaire intègre. Tout élément premier dans A est irréductible dans A.*

Preuve. Soit $x \in A$ premier dans A. On a $x \notin U(A)$. Supposons que $x = ab$ avec $a, b \in A$. En particulier $x|ab$, donc puisque x est premier, $x|a$ ou $x|b$. Supposons que $x|a$. Il existe $y \in A$ tel que $a = xy$, d'où $x = xyb$, ou encore $x(1 - yb) = 0$. A est intègre et x est non-nul car premier, donc $yb = 1$, d'où $b \in U(A)$. On prouve de même que $a \in U(A)$ si $x|b$. □

Remarque. On verra plus loin que la réciproque est fausse en général (voit 8.2.4), mais vraie pour les anneaux principaux (voir 8.2.1).

8.1.3 Pgcd, ppcm, éléments premiers entre eux

Définition. Soit A un anneau commutatif unitaire intègre. Soient $x_1, \ldots, x_n$ des éléments de A. On dit qu'ils sont *premiers entre eux*, ou *étrangers*, lorsque les seuls éléments de A qui divisent x_i pour tout $1 \leq i \leq n$ sont les éléments de $U(A)$.

Proposition. *Tout élément irréductible est premier avec tout élément qu'il ne divise pas.*

Preuve. Soit x irréductible dans A. Soit $y \in A$ tel que x ne divise pas y. Par l'absurde, supposons que u soit un diviseur commun de x et y non inversible dans A. On aurait alors $x = ua$ et $y = ub$ avec $a, b \in A$. Comme $x = ua$ et $u \notin U(A)$, l'irréductibilité de x impliquerait que $a \in U(A)$. On obtiendrait $u = xa^{-1}$ avec $a^{-1} \in A$, de sorte que $y = xa^{-1}b$, ce qui contredit le fait que x ne divise pas y.

Définitions. Soient $x_1, \ldots, x_n$ des éléments d'un anneau commutatif unitaire intègre A.

1. On dit qu'un élément $a \in A$ est un *diviseur commun* de $x_1, \ldots, x_n$ dans A lorsque a divise x_i pour tout $1 \leq i \leq n$.

2. On dit qu'un élément $a \in A$ est un *multiple commun* de $x_1, \ldots, x_n$ dans A lorsque x_i divise a pour tout $1 \leq i \leq n$.

3. On suppose que les x_i ne sont pas tous nuls. On dit que $x_1, \ldots, x_n$ *admettent un plus grand commun diviseur* dans A lorsqu'il existe un élément $d \in A$ tel que d est un diviseur commun de $x_1, \ldots, x_n$ et tel que tout diviseur commun de $x_1, \ldots, x_n$ divise d. On dit alors que d est *un pgcd* de $x_1, \ldots, x_n$.

4. On suppose que les x_i sont tous non-nuls. On dit que $x_1, \ldots, x_n$ *admettent un plus petit commun multiple* dans A lorsqu'il existe un élément $m \in A$ tel que m est un multiple commun de $x_1, \ldots, x_n$ et tel que tout multiple commun de $x_1, \ldots, x_n$ est un multiple de m. On dit alors que m est *un ppcm* de $x_1, \ldots, x_n$.

Remarques.

► Parce que deux éléments associés dans A ont les mêmes multiples et les mêmes diviseurs dans A, il est clair dans le point 3 ci-dessus qu'un élément $d' \in A$ est un pgcd de $x_1, \ldots, x_n$ si et seulement s'il est associé à d ; de même pour le ppcm dans le point 4. On dit que le pgcd et le ppcm, lorsqu'ils existent, sont définis *à l'association près*. On note alors :

$$d \sim \text{pgcd}(x_1, \ldots, x_n) \quad \text{et} \quad m \sim \text{ppcm}(x_1, \ldots, x_n).$$

► Soient $x_1, \ldots, x_n$ des éléments non-tous nuls de A. Il est clair que :

$$x_1, \ldots, x_n \text{ sont premiers entre eux dans } A \text{ si et seulement si } \text{pgcd}(x_1, \ldots, x_n) \sim 1,$$

ce qui traduit encore que $U(A)$ est l'ensemble des pgcd de $x_1, \ldots, x_n$.

Dans le cas de deux éléments, on a un lien important entre pgcd et ppcm :

Proposition. *Soit A un anneau commutatif unitaire intègre. Si deux élément non-nuls $x, y \in A$ admettent un ppcm dans A, alors ils admettent un pgcd dans A, et on alors la relation :*

$$xy \sim \text{pgcd}(x, y) \times \text{ppcm}(x, y).$$

Preuve. Supposons que x et y admettent un ppcm m. Comme m est un multiple de x et de y, il existe $x', y' \in A$ tel que $m = xx' = yy'$. Le produit xy est aussi un multiple de x et de y donc de m, donc il existe $d \in A$ tel que $xy = md$. Ainsi $xy = xx'd$, donc par intégrité de A, $y = x'd$. De méme $x = y'd$, ce qui prouve que d est un diviseur commun de x et y.

Suposons maintenant que e est un diviseur commun de x et de y. Il existe $x'', y'' \in A$ tels que $x = ex''$ et $y = ey''$. L'élément $n = ex''y'' = xy'' = x''y$ apparaît comme un multiple commun de x et y. C'est donc un mutiple de m par définition du ppcm. Il existe $k \in A$ tel que $n = km$. Donc $kme = ne = e^2x''y'' = xy = md$ d'où $ke = d$ par intégrité de A, c'est-à-dire que e divise d. On conclut que d est un pgcd de a et y. □

Attention.

- On peut dans certains anneaux trouver deux éléments qui n'admettent pas de pgcd, ou qui admettent un pgcd mais pas de ppcm (voir plus loin 8.2.4).

- Même dans les anneaux les plus simples, la relation entre pgcd, ppcm et produit peut ne plus être vraie si l'on considère plus que deux éléments :

$$\text{par exemple dans } \mathbb{Z},\ \text{pgcd}(2,3,4) \times \text{ppcm}(2,3,4) = 1 \times 12 \neq 2 \times 3 \times 4.$$

8.2 Cas des anneaux principaux.

8.2.1 Eléments irréductibles dans un anneau principal

Rappelons qu'on appelle *anneau principal* un anneau commutatif unitaire qui est intègre et dans lequel tout idéal est principal (c'est-à-dire que, quel que soit I un idéal de A, il existe $x \in A$ tel que $I = xA$). On a déjà vu en 7.3.1 que la réciproque du fait que tout idéal maximal est premier est vrai dans le cas des anneaux principaux :

> *Dans un anneau principal, tout idéal premier non-nul est maximal (et donc, pour les idéaux non-nuls, les notions de premier et de maximal coïncident).*

On a aussi dans ce cas la réciproque suivante de la seconde proposition de 8.1.2 :

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

> *Preuve.* Soit x un élément irréductible de A. Il est non-inversible (par définition), non-nul (voir remarque 8.1.2), et l'idéal $M = xA$ est maximal parmi les idéaux principaux de A distincts de A (voir première proposition de 8.1.2). Mais ici tout idéal de A est par hypothèse principal. Donc M est tout simplement un idéal maximal de A. Donc M est un idéal premier de A (voir 7.3.1), et comme il est non-nul, on déduit de la première proposition de 8.1.2 que x est un élément premier dans A. □

8.2.2 Pgcd et ppcm dans un anneau principal

THÉORÈME. *Soit A un anneau principal.*

Toute famille $x_1, \dots, x_n$ d'éléments non tous nuls de A admet des pgcd dans A, qui sont les générateurs de l'idéal $x_1A + \cdots + x_nA$:

$$(\ d \text{ est un pgcd de } x_1, \dots, x_n\ ) \Leftrightarrow (\ x_1A + \cdots + x_nA = dA\ )$$

Toute famille $x_1, \dots, x_n$ d'éléments tous non nuls de A admet des ppcm dans A, qui sont les générateurs de l'idéal $x_1A \cap \cdots \cap x_nA$:

$$(\ m \text{ est un ppcm de } x_1, \dots, x_n\ ) \Leftrightarrow (\ x_1A \cap \cdots \cap x_nA = dA\ )$$

> *Preuve.* Comme A est un anneau principal, l'idéal $x_1A+\cdots+x_nA$ est principal. Il existe donc $d \in A$ tel que $x_1A + \cdots + x_nA = dA$. Montrons que d est un pgcd de $x_1, \dots, x_n$. Pour tout $1 \leq i \leq n$, on a $x_iA \subseteq x_1A + \cdots + x_nA$, donc $x_iA \subseteq dA$, donc $d|x_i$. Soit maintenant $c \in A$ tel que $c|x_i$ pour tout $1 \leq i \leq n$. Alors $x_iA \subseteq cA$ pour tout $1 \leq i \leq n$, donc, puisque cA est stable par addition, $x_1A+\cdots+x_nA \subseteq cA$, c'est-à-dire $dA \subseteq cA$, et donc $c|d$. Ceci prouve que d est un pgcd de $x_1, \dots, x_n$. Réciproquement, soit d' un pgcd de $x_1, \dots, x_n$. D'après 8.1.3, on a $d' \sim d$, donc $dA = d'A$, c'est-à-dire $d'A = x_1A + \cdots + x_nA$.
>
> De même, l'idéal $x_1A \cap \cdots \cap x_nA$ est principal. Il existe $m \in A$ tel que $x_1A \cap \cdots \cap x_nA = mA$. Montrons que m est un ppcm de $x_1, \dots, x_n$. Pour tout $1 \leq i \leq n$, on a $x_iA \supseteq x_1A \cap \cdots \cap x_nA$ donc $x_iA \supseteq mA$, donc $x_i|m$. Soit maintenant $c \in A$ tel que $x_i|c$ pour tout $1 \leq i \leq n$. Alors $x_iA \supseteq cA$ pour tout $1 \leq i \leq n$, donc $x_1A \cap \cdots \cap x_nA \supseteq cA$, c'est-à-dire $mA \supseteq cA$, et donc $m|c$. Ceci prouve que m est un ppcm de . Réciproquement, soit m' un ppcm de $x_1, \dots, x_n$. D'après 8.1.3, on a $m' \sim m$, donc $mA = m'A$, c'est-à-dire $m'A = x_1A \cap \cdots \cap x_nA$. □

COROLLAIRE (propriété de Bézout). *Soit A un anneau principal. Soient $x_1, \dots, x_n$ des éléments non tous nuls de A. Alors $x_1, \dots, x_n$ sont premiers entre eux dans A si et seulement s'il existe $u_1, \dots, u_n \in A$ tels que $x_1u_1 + \cdots + x_nu_n = 1$.*

Preuve. Conséquence immédiate de la première assertion du théorème précédent. □

Les coefficients $u_1, \ldots, u_n$ dans la propriété de Bézout ne sont pas uniques (voir par exemple [PolyL3] pour leur détermination dans le cas $n = 2$).

Une conséquence de la propriété de Bézout est le résultat suivant bien connu et très utile en arithmétique élémentaire des anneaux principaux.

COROLLAIRE (lemme de Gauss). *Soit A un anneau principal. Pour tous a, b, c dans A, on a :*

$$(\ a \text{ divise } bc, \text{ et } a \text{ premier avec } b\ ) \Rightarrow (\ a \text{ divise } c\ )$$

Preuve. Comme a et b sont premiers entre eux, il existe d'après la propriété de Bézout $u, v \in A$ tels que $au + bv = 1$. Donc $c = cau + cbv$. Comme a divise bc, on a $bc \in aA$, donc $bcv \in aA$. Par ailleurs il est clair que $acu \in aA$. Par stabilité de l'idéal aA pour l'addition, on conclut que $c = acu + bcv \in aA$. □

8.2.3 Cas particulier des anneaux euclidiens

Rappelons tout d'abord la définition suivante :

DÉFINITION. On appelle *anneau euclidien* un anneau commutatif unitaire qui est intègre, et pour lequel il existe une application $\delta : A^* \to \mathbb{N}$ vérifiant les deux conditions suivantes :

1. pour tous $a, b \in A^*$, $(\ a|b\ ) \Rightarrow (\ \delta(a) \leq \delta(b)\ )$;
2. pour tout $a \in A$ et $b \in A^*$, il existe $q, r \in A$ tels que :
$$(\ a = bq + r\ ) \quad \text{et} \quad (\ r = 0 \ \text{ ou } \ \delta(r) < \delta(b)\ ).$$

Une application δ vérifiant ces deux conditions s'appelle un *stathme* euclidien. Dans la condition 2, on dit que q est un *quotient* et r un *reste* dans la *division euclidienne* de a par b.

Remarquons que la définition d'un stathme n'impose pas de conditions d'unicité de q et r dans la seconde condition.

EXEMPLES FONDAMENTAUX (voir par exemple [PolyL3] pour les preuves).

(a) L'anneau $\mathbb{Z}$ est euclidien, pour le stathme défini par $\delta(x) = |x|$ pour tout $x \in \mathbb{Z}^*$.

(b) Si K est un corps, l'anneau $K[X]$ est euclidien, pour le stathme défini par $\delta(F) = \deg F$ pour tout $F \in K[X]$ non-nul.

(c) L'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien, pour le stathme défini par $\delta(z) = z\,\overline{z}$ pour tout $z \in \mathbb{Z}[i]$ non-nul.

THÉORÈME. *Tout anneau euclidien est principal.*

Preuve. Soit A un anneau euclidien, de stathme δ. Il est intègre, et il s'agit donc de montrer que tout idéal I de A est principal. C'est clair si $I = \{0\}$ (alors $I = 0A$) ou si $I = A$ (alors $I = 1A$). On suppose donc $I \neq \{0\}$ et $I \neq A$. On considère $E = \{\delta(x)\,;\, x \in I, x \neq 0\}$. C'est une partie non-vide de $\mathbb{N}$, elle admet donc un plus petit élément n. Il existe $x \in I$, $x \neq 0$ tel que $n = \delta(x)$. Soit alors $a \in I$ quelconque ; par division euclidienne de a par x, il existe $q, r \in A$ tels que $a = xq + r$ avec $r = 0$ ou $\delta(r) < \delta(x) = n$. Or $r = a - xq$ avec $a \in I$ et $x \in I$, donc $r \in I$ par définition d'un idéal. Par minimalité de n, on ne peut donc pas avoir $\delta(r) < n$, et donc nécessairement $r = 0$, d'où $a = xq$. Ceci prouve que tout $a \in I$ appartient à xA. On conclut que $I \subseteq xA$, et donc $I = xA$. □

Exemples, contre-exemples, remarques.

(a) On retrouve que : $\mathbb{Z}$, $\mathbb{Z}[i]$, et $K[X]$ lorsque K est un corps, sont des anneaux principaux.

(b) La réciproque du théorème est fausse. Il existe des anneaux principaux qui ne sont pas euclidiens. C'est par exemple un exercice classique que de montrer que :

l'anneau $\mathbb{Z}[\omega] = \{a + \omega b\,;\, a, b \in \mathbb{Z}\}$ *pour* $\omega = \frac{1+i\sqrt{19}}{2}$ *est principal et non euclidien.*

(c) On a déjà observé précédemment que l'anneau $\mathbb{Z}[X]$ n'est pas principal. Ceci montre que, pour un anneau commutatif unitaire intègre A :

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

On a en fait le résultat général suivant :

Proposition (cas des anneaux de polynômes). *Soit A un anneau commutatif unitaire. Les trois 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) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Supposons donc maintenant $A[X]$ principal. En particulier, $A[X]$ est intègre, donc A est intègre (en tant que sous-anneau d'un anneau 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 d'après 7.3.1, $\operatorname{Ker} f$ est un idéal premier non-nul de $A[X]$. Mais comme $A[X]$ est supposé principal, $\operatorname{Ker} f$ est alors, d'après la seconde proposition de 8.2.1, un idéal maximal de $A[X]$. Donc $A[X]/\operatorname{Ker} f$ est un corps en réappliquant 7.3.1. On conclut via l'isomorphisme $A[X]/\operatorname{Ker} f \simeq A$ que A est un corps. □

Remarque (pgcd dans les anneaux euclidiens). Il résulte du théorème ci-dessus que toutes les propriétés arithmétique vraies dans les anneaux principaux s'appliquent en particulier aux anneaux euclidiens. Ces derniers possèdent de plus des spécificités propres, en particulier le lemme suivant :

Lemme (fondamental de l'algorithme d'Euclide). *Soit A un anneau euclidien. Soient $a, b \in A$ tels que $b \neq 0$. Alors, pour tout reste r d'une division euclidienne de a par b, tout pgcd de a et b est associé à tout pgcd de b et r. En d'autres termes, en notant δ le stathme de A :*

$$(\ a = bq + r,\ \text{avec } r = 0 \ \text{ ou } \ \delta(r) < \delta(b)\ ) \ \Rightarrow\ (\ \operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(b, r)\ ).$$

Preuve. Il résulte de l'égalité $a = bq + r$ que $a \in bA + rA$; comme $bA + rA$ est un idéal, on en déduit que $ax \in bA + rA$ pour tout $x \in A$, c'est-à-dire $aA \subset bA + rA$. Comme par ailleurs $bA \subset bA + rA$, la stabilité de $bA + rA$ pour l'addition implique alors $aA + bA \subset bA + rA$. En écrivant ensuite $r = a - bq$, on montre de même que $bA + rA \subset aA + bA$. Finalement $aA + bA = bA + rA$. Donc, en notant d un pgcd de a et b, et d' un pgcd de b et r, on a $dA = d'A$, c'est-à-dire $d \sim d'$. □

L'application itérative de ce résultat est à la base de l'algorithme d'Euclide, méthode puissante de calcul dans les anneaux euclidiens (voir [PolyL3] ou autres ouvrages de référence pour des exemples de mise en œuvre et d'applications).

8.2.4 Contre-exemples

On considère dans $\mathbb{C}$ le sous-ensemble :

$$A = \mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b\,;\, a, b \in \mathbb{Z}\} \;\subset\; \mathbb{C}.$$

Il est facile de vérifier que A est un anneau commutatif unitaire intègre, qui contient $\mathbb{Z}$ comme sous-anneau, et que l'application $N : A \to \mathbb{Z}$ définie par :

$$N(x) = |x|^2 = a^2 + 5b^2 \text{ pour tout } x = a + ib\sqrt{5}$$

est multiplicative. On en déduit en particulier que :

$$U(A) = \{x \in A\,;\, N(x) = 1\} = \{-1; +1\}.$$

► L'élément 3 est irréductible mais non premier dans A.

En effet. Montrons que 3 n'est pas premier dans A. Observons d'abord que 3 ne divise pas $2 + i\sqrt{5}$ dans A (en effet, on aurait sinon $(2 + i\sqrt{5}) = 3(a + ib\sqrt{5})$ avec $a, b \in \mathbb{Z}$, d'où $3a = 2$ et $1 = 3b$, ce qui est impossible). De même 3 ne divise pas $2 - i\sqrt{5}$. Et pourtant 3 divise $9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ dans A. On conclut que 3 n'est pas premier dans A.

Montrons maintenant que 3 est irréductible dans A. Il est clair que 3 n'est pas inversible dans A. Supposons que $3 = xy$ avec $x = a + ib\sqrt{5}$ et $y = c + id\sqrt{5}$, où $a, b, c, d \in \mathbb{Z}$. On a $N(x)N(y) = N(xy) = 9$ dans $\mathbb{N}^*$, donc trois cas seulement sont possibles : $N(x) = N(y) = 3$, ou $N(x) = 1$ et $N(y) = 9$, ou $N(x) = 9$ et $N(y) = 1$. Or le premier cas est impossible (car $a^2 + 5b^2 = 3$ n'a pas de solutions entières), le second implique que $x \in U(A)$, et le troisième implique de même que $y \in U(A)$. On conclut que 3 est irréductible dans A. □

► Les éléments $x = 3$ et $y = 2 + i\sqrt{5}$ admettent un pgcd dans A mais n'admettent pas de ppcm dans A.

En effet. Puisque 3 est irréductible dans A, les seuls diviseurs de x dans A sont ± 3 et ± 1. On a vu que ± 3 ne divisent pas y, on en déduit que x et y admettent ± 1 comme pgcd. Si x et y admettaient un ppcm, il résulte de la proposition précédente que ce dernier serait $m = \pm xy = \pm 3(2 + i\sqrt{5})$. Or comme $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ est un multiple commun de x et de y, ce serait un mutiple de leur ppcm $m = 3(2 + i\sqrt{5})$, et donc 3 serait un multiple de $2 + i\sqrt{5}$, ce qui est clairement impossible dans A. □

► Les éléments $x = 9$ et $y = 6 + 3i\sqrt{5}$ n'admettent pas de pgcd dans A.

En effet. En écrivant $x = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ et $y = 3(2 + i\sqrt{5})$, il apparaît que 3 et $2 + i\sqrt{5}$ dont des diviseurs communs de x et y. Supposons que x et y admettent un pgcd d. Ce dernier serait divisible par 3 et par $2 + i\sqrt{5}$. Il existerait $a, b \in A$ tel que $d = 3a$ et $d = b(2 + i\sqrt{5})$. Mais d'autre part il existerait $x', y' \in A$ tels que $9 = dx'$ et $6 + 3i\sqrt{5} = dy'$. D'où en particulier $9 = 3ax'$ donc a diviserait 3 dans A, c'est-à-dire $a = \pm 3$ ou $a = \pm 1$. Le cas $a = \pm 3$ est impossible car $d = \pm 9$ ne divise pas $y = 6 + 3i\sqrt{5}$. Le cas $a = \pm 1$ est aussi impossible car on aurait $d = \pm 3 = b(2 + i\sqrt{5})$ qui n'a pas de solution dans A. □

D'après les résultats de 8.2.1 et 8.2.2, chacune de ces trois assertions suffit à prouver que cet anneau A n'est pas principal.

On va introduire dans le chapitre suivant une classe d'anneaux plus générale, englobant strictement les anneaux principaux, dans lesquels on peut faire de l'arithmétique : tout couple d'éléments y admet des pgcd et des ppcm, la propriété de Bézout n'y est plus toujours vérifiée, mais le lemme de Gauss y reste vrai.

Chapitre 9

Arithmétique dans les anneaux factoriels

9.1 Notion d'anneau factoriel.

9.1.1 Décomposition en facteurs irréductibles

DÉFINITION. On appelle anneau *factoriel* un anneau commutatif unitaire qui est intègre, et dans lequel 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 près et au produit par un élément inversible près.

Explicitement, cela signifie que A est intègre et que l'on a :

(F1) tout élément $a \in A$ tel que $a \neq 0$ et $a \notin U(A)$ 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 <u>la</u> 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. Ce n'est qu'un cas particulier du théorème 9.1.2 ci-dessous.

PROPOSITION (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 irréductible 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. □

9.1.2 Cas des anneaux principaux

THÉORÈME. *Tout anneau principal est factoriel.*

Preuve. Soit A un anneau principal. En particulier, il est intègre (par définition) et il vérifie la condition (F2') comme on l'a montré en 8.2.1. Il suffit donc de montrer que A vérifie la condition (F1). Pour cela, raisonnons par l'absurde, en supposant que A ne vérifie pas (F1). Cela signifie que l'ensemble :

$$R = \{a \in A,\ a \neq 0,\ a \notin U(A),\ a \text{ n'est pas produit d'éléments irréductibles}\}$$

est non-vide. Il en résulte que l'ensemble $E = \{aA\ ;\ a \in R\}$ des idéaux principaux de A engendrés par les éléments de R est également non-vide. On montre que E est inductif (voir 7.3.2) pour l'inclusion. Pour cela, considérons $F = (I_k)_{k \in X}$ une famille d'éléments de E totalement ordonnée par l'inclusion. Pour tout $k \in X$, considérons un élément $a_k \in R$ tel que $I_k = a_k A$. La réunion $I = \bigcup_{k \in X} I_k$ est un idéal non-nul de A. Comme A est principal, il existe $b \in A$, $b \neq 0$, tel que $I = bA$. Puisque $b \in I$, il existe $a_k \in R$ tel que $b \in a_k A$, et donc $bA \subseteq a_k A$. Comme par ailleurs $a_k A \subseteq I = bA$, on conclut que $I = a_k A$, et donc $I \in E$. En résumé, toute famille d'éléments de E totalement ordonnée admet un plus grand élément. On conclut que E est inductif.

D'après le lemme de Zorn, E admet (au moins) un élément maximal ; notons-le cA, avec $c \in R$. Parce que $c \in R$, il est non-nul, non-inversible, et non-irréductible. Donc il existe $x, y \in A$ tel que $c = xy$ avec $x \notin U(A)$ et $y \notin U(A)$. Il en résulte que $cA \subset xA$ avec $cA \neq xA$, et $cA \subset yA$ avec $cA \neq yA$. De plus, il est clair que $x \in R$ ou $y \in R$ (en effet, sinon, x et y seraient produits d'irréductibles, et donc $c = xy$ aussi), d'où $xA \in E$ ou $yA \in E$. Dans l'un ou l'autre cas, il y a contradiction avec la maximalité de cA dans E. □

EXEMPLES ET REMARQUES.

(a) Les anneaux $\mathbb{Z}$, $K[X]$ pour K un corps, et $\mathbb{Z}[i]$, sont factoriels, car principaux.

(b) La réciproque du théorème ci-dessus est fausse : il existe des anneaux factoriels qui ne sont pas principaux. En effet, on verra plus loin en 9.2.4 que, si A est factoriel, alors $A[X]$ est factoriel ; ainsi $\mathbb{Z}[X]$ est factoriel, alors qu'il n'est pas principal comme on l'a vu en 7.3.1.

(c) Il existe des anneaux intègres non factoriels. Par exemple l'anneau $\mathbb{Z}[i\sqrt{5}]$ étudié en 8.1.2 possède des éléments irréductibles non premiers, et ne vérifie donc pas la condition (F2').

(d) L'anneau quotient A/I d'un anneau factoriel A par un idéal I peut ne pas être factoriel, même lorsqu'il est intègre (c'est-à-dire lorsque I est premier). Considérons par exemple l'anneau $A = \mathbb{Z}[X]$ qui est factoriel (voir ci-dessus). Si l'on prend $I = (X^2+1)A$, l'anneau $A/I \simeq \mathbb{Z}[i]$ des entiers de Gauss est euclidien, donc principal, donc factoriel. Mais pour $I = (X^2+5)A$, l'anneau $A/I \simeq \mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel, comme on vient de le voir.

9.1.3 Divisibilité dans les anneaux factoriels, lemme de Gauss.

Commentaire. Le but de ce paragraphe est d'établir pour les anneaux factoriels certaines propriétés arithmétiques que nous avons déjà démontrées pour les anneaux principaux (existence de pgcd, lemme de Gauss). Sur le plan strictement logique, il est donc suffisant de les montrer comme ci-dessous dans le cadre plus général des anneaux factoriels. Il n'est néanmoins pas inutile de connaître les preuves directes que nous avons données dans le cas particulier des anneaux principaux, ne serait-ce que pour différencier les arguments généraux de ceux spécifiques au cas principal, comme le théorème de Bézout.

Remarques préliminaires sur les notations. Soit A un anneau factoriel.

(a) Dans l'ensemble des éléments irréductibles de A, l'association définit d'après 8.1.2 une relation d'équivalence. En choisissant un représentant dans chaque classe d'équivalence, on définit un *système de représentants* $\mathscr{R}$ des éléments irréductibles. Tout élément irréductible de A est alors équivalent à un unique élément irréductible de la famille $\mathscr{R}$.

quel que soit r irréductible dans A, il existe $r' \in \mathscr{R}$ et $u \in U(A)$ uniques tels que $r = ur'$.

Exemples :

1. Dans l'anneau $\mathbb{Z}$, on choisit généralement comme système de représentants des éléments irréductibles l'ensemble $\mathscr{P}$ des nombres premiers positifs. Tout élément irréductible de $\mathbb{Z}$ est de la forme εp avec $p \in \mathscr{P}$ et $\varepsilon \in U(\mathbb{Z}) = \{-1, +1\}$.
2. Dans l'anneau $\mathbb{C}[X]$, on choisit généralement comme système de représentants des éléments irréductibles l'ensemble $\mathscr{R}$ les polynômes de degré 1 unitaires (c'est-à-dire de coefficient dominant égal à 1). Tout élément irréductible est de la forme $\alpha(X - \beta)$ avec $X - \beta \in \mathscr{R}$ et $\alpha \in U(\mathbb{C}[X]) = \mathbb{C}^*$.

(b) Soit $\mathscr{R}$ un système de représentants des éléments irréductibles dans A. Soit $a \in A$ non-nul et non-inversible. Il résulte de la condition (F1) que a s'écrit de façon unique :

$$a = u\, r_1^{n_1} r_2^{n_2} \dots r_s^{n_s}, \quad \text{avec } u \in U(A),\ r_i \in \mathscr{R} \text{ et } n_i \in \mathbb{N}^* \text{ pour tout } 1 \leq i \leq s.$$

Exemples :

1. Dans $\mathbb{Z}$, tout élément a non-nul et distinct de ± 1 s'écrit de façon unique $a = \varepsilon\, p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, avec $\varepsilon = \pm 1$, et $n_i \in \mathbb{N}^*$ et $p_i \in \mathscr{P}$ pour tout $1 \leq i \leq s$.
2. Dans $\mathbb{C}[X]$, tout polynôme $P(X)$ de degré ≥ 1 s'écrit de façon unique :
$$P(X) = \alpha(X - \beta_1)^{n_1}(X - \beta_2)^{n_2} \dots (X - \beta_s)^{n_s},$$
avec $\alpha \in \mathbb{C}^*$, et $n_i \in \mathbb{N}^*$ et $\beta_i \in \mathbb{C}$ pour tout $1 \leq i \leq s$.

(c) Soit $\mathscr{R}$ un système de représentants des éléments irréductibles dans A. Soient $a, b \in A$ non-nuls et non-inversibles. En réunissant les facteurs irréductibles intervenant dans l'écriture ci-dessus de a et dans celle de b, et en autorisant alors des exposants nuls dans l'une des décompositions, a et b s'écrivent de façon unique :

$$a = u\, r_1^{n_1} r_2^{n_2} \dots r_q^{n_q} \quad \text{et} \quad b = v\, r_1^{m_1} r_2^{m_2} \dots r_q^{m_q}, \quad \text{avec } u, v \in U(A),$$
$$r_i \in \mathscr{R},\ \ n_i \in \mathbb{N},\ \ m_i \in \mathbb{N},\ \ (n_i, m_i) \neq (0, 0) \ \text{ pour tout } 1 \leq i \leq q.$$

Lemme (diviseurs d'un élément dans un anneau factoriel). *Soit A un anneau factoriel. Soit $a \in A$, non-nul et non-inversible. Avec la notation* (b) *ci-dessus, les diviseurs de a dans A sont tous les éléments de la forme :*

$$w r_1^{p_1} r_2^{p_2} \dots r_s^{p_s}, \quad 0 \leq p_i \leq n_i \text{ pour tout } 1 \leq i \leq s,\ \ w \in U(A).$$

Preuve. Soit b un diviseur de a. Si $b \in U(A)$, le résultat est clair avec $b = w$ et $p_1 = p_2 = \cdots = p_s = 0$. Supposons donc maintenant que $b \notin U(A)$. Soit r un des facteurs irréductibles intervenant dans la décomposition de b. Comme $b|a$, on a $r|a$, c'est-à-dire que r divise $r_1^{n_1} r_2^{n_2} \dots r_s^{n_s}$. Puisque r est premier (car irréductible dans un anneau factoriel, voir 9.1.1), on en tire que r est associé à l'un des r_i. Ceci prouve que b est de la forme $b = w\, r_1^{p_1} r_2^{p_2} \dots r_s^{p_s}$, avec $w \in U(A)$ et $p_i \geq 0$ pour tout $1 \leq i \leq s$. Pour montrer ensuite que $p_i \leq n_i$ pour tout $1 \leq i \leq s$, raisonnons par l'absurde. Supposons par exemple (pour fixer les idées) que $p_1 > n_1$. En notant $a = xb$ avec $x \in A$, on aurait donc : $u\, r_2^{n_2} \dots r_s^{n_s} = xw\, r_1^{p_1 - n_1} r_2^{p_2} \dots r_s^{p_s}$, avec $p_1 - n_1 > 0$, ce que contredirait la condition (F2). Ce qui achève la preuve. □

PROPOSITION (pgcd et ppcm dans un anneau factoriel). *Soit A un anneau factoriel.*

(i) *Deux éléments quelconques admettent toujours un pgcd, et un ppcm dans A.*

(ii) *Plus précisément, si a et b sont deux éléments de A non-nuls et non-inversibles, on a avec les notations* (c) *:*

$$\mathrm{pgcd}(a,b) \sim r_1^{h_1} r_2^{h_2} \dots r_q^{h_q} \quad \text{et} \quad \mathrm{ppcm}(a,b) \sim r_1^{\ell_1} r_2^{\ell_2} \dots r_q^{\ell_q},$$

avec $h_i = \min(n_i, m_i)$ et $\ell_i = \max(n_i, m_i)$ pour tout $1 \leq i \leq q$.

Preuve. Soient $a, b \in A$. Si $a = 0$, on a $\mathrm{pgcd}(a,b) \sim b$. Si $a \in U(A)$, on a $\mathrm{pgcd}(a,b) \sim a \sim 1$. De même si $b = 0$ ou $b \in U(A)$. Sinon, a et b sont non-nuls et non-inversibles : le point (ii) résulte alors de la proposition précédente et la définition des pgcd et ppcm (voir 8.1.3). □

THÉORÈME (dit lemme de Gauss). *Soit A un anneau factoriel. Soient a, b, c trois éléments de A. Si a divise bc et si a est premier avec b, alors a divise c. En d'autres termes :*

$$(\ a|bc \quad et \quad \mathrm{pgcd}(a,b) \sim 1\ ) \quad \Rightarrow \quad (\ a|c\ )$$

Preuve. On peut sans restriction supposer que a, b, c sont non-nuls et non inversibles. Avec la notation (c), on pose :

$$a = u\, r_1^{n_1} r_2^{n_2} \dots r_q^{n_q}, \quad b = v\, r_1^{m_1} r_2^{m_2} \dots r_q^{m_q}, \quad c = w\, r_1^{p_1} r_2^{p_2} \dots r_q^{p_q}, \quad \text{avec } u, v, w \in U(A).$$

On suppose $a|bc$, donc $n_i \leq m_i + p_i$ pour tout $1 \leq i \leq q$. Par contraposée, supposons que a ne divise pas c, c'est-à-dire qu'il existe un indice j tel que $n_j > p_j$. Alors $m_j \geq n_j - p_j > 0$. Ainsi $n_j > 0$ et $m_j > 0$, donc r_j divise à la fois a et b, ce qui contredit $\mathrm{pgcd}(a,b) \sim 1$. □

REMARQUE. En revanche, la propriété de Bézout n'est plus forcément vraie dans un anneau qui n'est pas principal (même s'il est factoriel). Par exemple, dans $\mathbb{Z}[X]$, les éléments 2 et X sont clairement premiers entre eux, mais pourtant il n'existe pas de polynômes $S, T \in \mathbb{Z}[X]$ tels que $2S + XT = 1$, comme on l'a déja observé en 8.2.1.

9.2 Polynômes à coefficients dans un anneau factoriel

9.2.1 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'à l'association près, c'est-à-dire au produit par un inversible de A près. Lorsque l'on écrit $c(P) = a$, on a aussi $c(P) = ua$ pour tout $u \in U(A)$. On peut aussi écrire $c(P) \sim a$.

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.

$$(\ P \text{ primitif }) \ \Leftrightarrow\ (\ \deg P \geq 1 \ \text{ et } \ c(P) = 1\ ) \ \Leftrightarrow\ (\ \deg P \geq 1 \ \text{ et } \ c(P) \in U(A)\ ).$$

Remarques.

(1) Tout polynôme unitaire non constant 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 deux éléments primitifs dans $A[X]$. Soient a_1 et a_2 deux éléments 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, on 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 implique que $P_1 = uP_2$ car $A[X]$ est intègre (rappelons que $A[X]$ est intègre si et seulement si A l'est ; voir cours de L3). Puisque 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 non constants de $A[X]$. On a l'égalité $c(PQ) = c(P)c(Q)$. En particulier, P et Q sont primitifs si et seulement si PQ est primitif.*

Preuve. On montre d'abord la seconde assertion. 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 $\hat{\pi}(\sum a_iX^i) = \sum \pi(a_i)X^i$. 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 précédent 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. On a ainsi démontré l'équivalence de la seconde assertion.

Déduisons-en plus généralement la première. 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 éléments 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 $P = qP_1$, avec $q \in K^*$ et $P_1 \in A[X]$ 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 a_i/s_i par un même élément non-nul de A, on peut écrire toutes les fractions a_i/s_i avec un même dénominateur s (par exemple un ppcm des s_i, ou encore simplement le produit de s_i), sous la forme $a_i/s_i = a'_i/s$, avec $a'_i \in A$. Donc $P = \frac{1}{s}\sum_{i=0}^{n} a'_iX^i$. 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 $P_1 = \sum_{i=0}^{n} b_iX^i$ primitif. □

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

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

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

Preuve. Rappelons que $U(A[X]) = U(A)$ puisque A est intègre (voir par exemple [PolyL3]).

(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 $U(K[X]) = K^*$. Mais P et Q étant à coefficients dans A, cela signifie que P ou Q appartient à A^*. 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 ci-dessus 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 $K[X]$. □

REMARQUE. On a en particulier montré dans la preuve ci-dessus le résultat souvent utile suivant :

Soient A un anneau factoriel et K son corps de fractions. Soit R un élément de $A[X]$. Si R est le produit de deux éléments de $K[X]$ de degré ≥ 1, alors R est le produit de deux éléments de $A[X]$ de degré ≥ 1.

On termine ce chapitre en développant trois applications classiques de ce théorème, relatives à l'irréductibilité des polynômes à coefficients dans un anneau factoriel.

9.2.2 Première application : réduction modulo p

NOTATIONS. Soit A un anneau factoriel, de corps de fractions K. Soit I un idéal premier de A et L le corps de fractions de l'anneau intègre $B = A/I$. A tout polynôme R dans $A[X]$, on associe sa réduction modulo I, qui est le polynôme $\overline{R}$ dans $B[X]$ défini par :

$$\text{si } R = \sum_{i=0}^{n} a_i X^i \text{ avec } a_i \in A, \text{ alors } \overline{R} = \sum_{i=0}^{n} \overline{a}_i X^i, \text{ avec } \overline{a}_i \in B.$$

Il est facile de vérifier que l'application $R \mapsto \overline{R}$ définit un morphisme d'anneaux $A[X] \to B[X]$.

PROPOSITION. *Avec les notations précédentes, soit $R = \sum_{i=0}^{n} a_i X^i \in A[X]$ tel que $a_n \notin I$. Si $\overline{R}$ est irréductible dans $B[X]$ ou $L[X]$, alors R est irréductible dans $K[X]$.*

> *Preuve.* Supposons que R ne soit pas irréductible dans $K[X]$. Il s'écrirait donc comme produit de deux polynômes de $K[X]$ de degré ≥ 1. Donc, en appliquant la dernière remarque de 9.2.1, il existerait dans $A[X]$ un polynôme $P = \sum_{i=0}^{p} b_i X^i$ de degré $p \geq 1$ et un polynôme $Q = \sum_{i=0}^{q} c_i X^i$ de degré $q \geq 1$ tels que $R = PQ$. On aurait alors $b_p c_q = a_n \notin I$, donc $b_p \notin I$ et $c_q \notin I$, d'où $\deg \overline{P} = p$ et $\deg \overline{Q} = q$. Mais par ailleurs $\overline{R} = \overline{P}\,\overline{Q}$ et l'irréductibilité de $\overline{R}$ dans $B[X]$ ou $L[X]$ impliquerait que $\deg \overline{P} = 0$ ou $\deg \overline{Q} = 0$, d'où une contradiction. □

On applique souvent ce principe pour le cas où $A = \mathbb{Z}$ et en prenant pour I l'idéal principal engendré par un nombre premier p, de sorte que $B = L = \mathbb{Z}/p\mathbb{Z}$ est un corps. En rappelant la notation classique $\mathbb{F}_p$ pour désigner le corps $\mathbb{Z}/p\mathbb{Z}$, la réduction modulo p d'un polynôme de $\mathbb{Z}[X]$ est son image par le morphisme d'anneaux :

$$\mathbb{Z}[X] \to \mathbb{F}_p[X],\ R = \sum_{i=0}^{n} a_i X^i \mapsto \overline{R} = \sum_{i=0}^{n} \overline{a}_i X^i.$$

On a alors par exemple :

COROLLAIRE. *Soit R un polynôme unitaire dans $\mathbb{Z}[X]$. S'il existe un nombre premier p tel que la réduction de R modulo p soit irréductible dans $\mathbb{F}_p[X]$, alors R est irréductible dans $\mathbb{Q}[X]$ (et donc dans $\mathbb{Z}[X]$ puisqu'il est primitif).*

> EXEMPLE. Soit $R = X^5 - 2X^4 - 4X^3 + 3X^2 + 6X + 5 \in \mathbb{Z}[X]$. Sa réduction modulo 2 est $\overline{R} = X^5 + X^2 + \overline{1}$ dans $\mathbb{F}_2[X]$. Il est facile de vérifier par identification que $\overline{R}$ ne peut s'exprimer dans $\mathbb{F}_2[X]$ ni comme le produit d'un polynôme de degré 1 par un polynôme de degré 4, ni comme le produit d'un polynôme de degré 2 par un polynôme de degré 3 ; $\overline{R}$ est donc irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$, et donc R est irréductible dans $\mathbb{Z}[X]$.
>
> EXEMPLE. Soit $R = X^4 + 4X^3 + 3X^2 + 7X - 4 \in \mathbb{Z}[X]$. Sa réduction modulo 2 est $\overline{R} = X^4 + X^2 + X = X(X^3 + X + \overline{1}) \in \mathbb{F}_2[X]$, qui n'est donc pas irréductible dans $\mathbb{F}_2[X]$. Sa réduction modulo 3 est $\widetilde{R} = X^4 + X^3 + X - \widetilde{1} = (X^2 + \widetilde{1})(X^2 + X - \widetilde{1}) \in \mathbb{F}_3[X]$, qui n'est donc pas irréductible dans $\mathbb{F}_3[X]$. Sa réduction modulo 5 est $\widehat{R} = X^4 - X^3 - \widehat{2}X^2 + \widehat{2}X + \widehat{1} = (X - \widehat{2})(X^3 + X^2 + \widehat{2}) \in \mathbb{F}_5[X]$, qui n'est donc pas irréductible dans $\mathbb{F}_5[X]$. Sa réduction modulo 7 est $\check{R} = X^4 - \check{3}X^3 + \check{3}X^2 + \check{3} = (X - \check{2})(X^3 - X^2 + X + \check{2}) \in \mathbb{F}_7[X]$, qui n'est donc pas irréductible dans $\mathbb{F}_7[X]$... Faute de pouvoir appliquer le corollaire directement, on modifie un peu le raisonnement. Si R admettait un zéro dans $\mathbb{Z}$, alors $\widetilde{R}$ admettrait un zéro dans $\mathbb{F}_3$; il est facile à partir de la décomposition de $\widetilde{R}$ de vérifier que $\widetilde{R}$ n'admet pas de zéro dans $\mathbb{F}_3$, et donc R n'admet pas de zéro dans $\mathbb{Z}$. Si R était produit de deux polynômes de degré 2 dans $\mathbb{Z}[X]$, alors $\overline{R}$ serait produit de deux polynômes de degré 2 dans $\mathbb{F}_2[X]$, ce qui n'est pas le cas. On conclut que R est irréductible dans $\mathbb{Z}[X]$.
>
> REMARQUE. Ce corollaire de réduction modulo p donne seulement une condition suffisante d'irréductibilité. Il est très loin d'être applicable en toutes circonstance : il existe des polynômes irréductibles dans $\mathbb{Z}[X]$ dont la réduction modulo p est non irréductible dans $\mathbb{F}_p[X]$ quel que soit le nombre premier p.

9.2.3 Deuxième 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 de 9.2.1 implique que Q et R le sont. Posons $Q = \sum_{i=0}^{q} b_iX^i$ et $R = \sum_{i=0}^{r} c_iX^i$, avec $b_i, c_i \in A$, et $0 < q < n$ et $0 < r < n$. On a $a_n = b_qc_r \neq 0$, 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 $a_0 = b_0c_0$, et donc par hypothèse p divise b_0c_0 mais p^2 ne divise pas b_0c_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 $k \in \{1, \ldots, r\}$ tel que p ne divise pas c_k. Par construction, p ne divise pas b_0c_k, et p divise b_ic_{k-i} pour tout $i \in \{1, \ldots, k\}$. Il en résulte que p ne divise pas $a_k = b_0c_k + b_1c_{k-1} + \cdots + b_kc_0$. 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 $a'_0, a'_1, \ldots, a'_n$ premiers entre eux dans leur ensemble tels que $a_i = c(P)a'_i$ pour tout $0 \leq i \leq n$. Donc $P_1 = a'_nX^n + \cdots + a'_1X + a'_0$. 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), et donc p divise a'_i. 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 9.2.1, 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 $c(P)P_1 = P$. □

EXEMPLES : $P = X^5 + 4X^3 + 12X + 2$ est unitaire donc primitif dans $\mathbb{Z}[X]$, et il est irréductible dans $\mathbb{Z}[X]$ par application du critère d'Eisenstein. Pour tout $n \in \mathbb{N}^*$, $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$, ce qui prouve qu'il existe dans $\mathbb{Q}[X]$ des polynômes irréductibles de tout degré.

Exercice (polynômes cyclotomiques). Soit $P(X) = X^{p-1} + \cdots + X + 1 \in \mathbb{Z}[X]$, où p est un nombre premier. Montrer que le polynôme $T(X) = P(X+1)$ vérifie $T(X) = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$. Utiliser le critère d'Eisenstein pour vérifier que $T(X)$ est irréductible dans $\mathbb{Q}[X]$. En déduire que que $P(X)$ est irréductible dans $\mathbb{Q}[X]$.

9.2.4 Troisième application : factorialité des anneaux de polynômes

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 9.2.1.

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 produit d'éléments irréductibles de P_1 pour en déduire une décomposition de P). On raisonne par récurrence sur n. Si $n = 1$, on écrit $P = aX + b$ avec $a, b \in A$ premiers entre eux. Il est clair que P est irréductible dans $A[X]$. 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 9.2.1, 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 9.2.1), donc premier dans A puisque A est factoriel (voir 9.1.1). 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 9.2.1, 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 9.1.1, 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 9.2.1, 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 9.2.1). On en déduit avec le lemme 1 de 9.2.1 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 avec 9.1.1 que $A[X]$ est factoriel. □

Exemples.

(a) $\mathbb{Z}[X]$ est factoriel (rappelons une fois encore qu'il n'est pas principal).

(b) Pour tout anneau A, on définit l'anneau des polynômes en deux indéterminées $A[X, Y]$ à coefficients dans A, qui n'est autre à isomorphisme près que $A[X][Y]$. Si A est factoriel, $A[X]$ est factoriel d'après le théorème précédent, et en le réappliquant, on déduit que $A[X][Y]$ est factoriel. En résumé :

$$(\ A \text{ factoriel }) \ \Rightarrow \ (\ A[X, Y] \text{ factoriel }).$$

(c) Plus généralement, en définissant par récurrence $A[X_1, X_2, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$, l'application itérée n fois du théorème ci-dessus montre que :

$$(\ A \text{ factoriel }) \ \Rightarrow \ (\ A[X_1, X_2, \ldots, X_n] \text{ factoriel }).$$

Les anneaux de polynômes en n indéterminées fontl'objet du chapitre suivant.

Chapitre 10

Polynômes en plusieurs indéterminées

10.1 Anneaux de polynômes en plusieurs indéterminées

10.1.1 Construction formelle

On fixe un anneau commutatif unitaire A. On rappelle ici pour mémoire comment sont construits et définis formellement les anneaux de polynômes à coefficients dans A.

a) Retour sur le cas des polynômes en une indéterminée.

On fixe un anneau commutatif unitaire A. Notons (provisoirement) $B = A^{(\mathbb{N})}$ l'ensemble des suites d'éléments de A qui sont "à support fini" c'est-à-dire dont tous les termes sont nuls sauf un nombre fini d'entre eux. On note $0_B = (0_A, 0_A, \ldots)$. Pour tout $f = (a_n)_{n\in\mathbb{N}} \in B$ distinct de 0_B, on appelle degré de f le plus grand des entiers $n \in \mathbb{N}$ tels que $a_n \neq 0$. On définit une addition et une multiplication dans B en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$ et $g = (b_n)_{n\in\mathbb{N}}$ dans B,

$$f + g = (a_n + b_n)_{n\in\mathbb{N}} \quad \text{et} \quad fg = (c_n)_{n\in\mathbb{N}}, \text{ avec } c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

► On peut montrer (vérification technique et fastidieuse, mais élémentaire) que, pour ces opérations, B est un anneau commutatif unitaire, avec $0_B = (0_A, 0_A, \ldots)$ et $1_B = (1_A, 0_A, 0_A, \ldots)$. On l'appelle l'anneau des polynômes en une indéterminée à coefficients dans A.

► On définit aussi le produit externe d'un élément $\alpha \in A$ par un élément $f = (a_n)_{n\in\mathbb{N}} \in B$ en posant $\alpha f = (\alpha a_n)_{n\in\mathbb{N}}$. A noter que le produit externe $\alpha.f$ n'est autre que le produit interne de f par $(\alpha, 0_A, 0_A, \ldots)$. C'est pourquoi on convient de noter encore α l'élément $(\alpha, 0_A, 0_A, \ldots)$ de B. En particulier $0_B = 0_A$ et $1_B = 1_A$.

► En posant $e_i = (0_A, 0_A, \ldots, 0_A, 1_A, 0_A, 0_A, \ldots)$, avec le 1_A en $i+1$-ième position, pour tout $i \in \mathbb{N}$, tout élément de B s'écrit de façon unique $f = \sum_{n\in\mathbb{N}} a_n e_n$ avec les $a_n \in A$ nuls sauf un nombre fini d'entre eux (de sorte que la somme est finie). Il est clair que $e_n e_m = e_{n+m}$ pour tous $n, m \in \mathbb{N}$, et donc $e_n = e_1^n$ pour tout $n \in \mathbb{N}$. On note traditionnellement $X = e_1$ et $B = A[X]$, et l'on retrouve les notations usuellement utilisées pour désigner les polynômes.

b) Généralisation au cas des polynômes en plusieurs indéterminées.

On fixe un anneau commutatif untaire A et un entier naturel $n \geq 1$. Considérons une application :

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

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 $\mathscr{R}_n(A)$ l'ensemble de toutes les suites f de ce type qui sont à support fini.

► Il est technique mais élémentaire de vérifier que $\mathscr{R}_n(A)$ 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 $\mathscr{R}_n(A)$ montre 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 $\mathscr{R}_n(A)$. En particulier, le neutre additif et le neutre multiplicatif de l'anneau $\mathscr{R}_n(A)$ 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 $\mathscr{R}_n(A)$ 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 $\mathscr{R}_n(A)$ s'écrit comme une somme finie :

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

c) Définitions et exemples.

Définition. L'anneau $\mathscr{R}_n(A)$ ci-dessus 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.

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

10.1.2 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 vérifie nécessairement :

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

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 le sous-ensemble C formé des polynômes $P = \sum a_{i_1,i_2,\ldots,i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$ vérifiant $a_{i_1,i_2,\ldots,i_n} = 0$ pour tout $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$ 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 sur n grâce à la proposition précédente, en utilisant le fait déjà plusieurs fois souligné qu'un anneau de polynômes à coefficients dans un anneau intègre est intègre, et le théorème 9.2.4 pour la factorialité. □

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 jamais principal (d'après le second théorème de 8.2.3).

10.2 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 $A[X_1, X_2, \ldots, X_n]$.

10.2.1 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. Pour $n = 3$ et $\sigma = (1, 3, 2)$, si $P(X, Y, Z) = X^2 + YZ - 3XY$, alors $P_\sigma(X, Y, Z) = Z^2 + XY - 3ZX$.

Remarque. Quel que soit $n \geq 1$, 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 :*

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

(ii) *Quelle que soit $\sigma \in S_n$, l'application : $P \mapsto P_\sigma$ est un automorphisme de l'anneau $A[X_1, X_2, \ldots, X_n]$.*

Preuve. Simple vérification, sans aucune difficulté. □

10.2.2 Sous anneau des polynômes symétriques

DÉFINITION. Un polynôme $P \in A[X_1, X_2, \ldots, X_n]$ est dit *symétrique* si $P_\sigma = P$ pour toute $\sigma \in S_n$. En d'autres termes, 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 dans $A[X_1, X_2, \ldots, X_n]$ est un sous-anneau de $A[X_1, X_2, \ldots, X_n]$.*

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

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

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

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

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

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

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

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

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

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

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

Ces exemples sont des cas particuliers des exemples classiques suivants.

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

(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 : $\boxed{W_k = \sum_{i_1+i_2+\cdots+i_n=k} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}}$ pour tout $k \in \mathbb{N}^*$;

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

(4) les polynômes symétriques élémentaires :

$\Sigma_1 = X_1 + X_2 + \cdots + X_n,$
$\Sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_2X_n + \cdots + X_{n-1}X_n,$
$\dots$
$\boxed{\Sigma_k = \sum_{1\le i_1<i_2<\cdots<i_k\le n} X_{i_1}X_{i_2} \dots X_{i_k}}$ pour tout $1 \le k \le n$, (somme de $\binom{n}{k}$ termes),
$\dots$
$\Sigma_n = X_1X_2 \dots X_n.$

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

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

10.2.3 Théorème de structure de l'anneau des polynômes symétriques

On reprend toutes les notations et hypothèses du paragraphe précédent. 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 :

$$\begin{aligned}\Sigma_1\Sigma_2 &= (X+Y+Z)(XY+YZ+ZX)\\ &= X^2Y + XYZ + X^2Z + XY^2 + Y^2Z + XYZ + XYZ + YZ^2 + Z^2X\\ &= P(X,Y,Z) + 3XYZ = P(X,Y,Z) + 3\Sigma_3.\end{aligned}$$

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 :

$$\begin{aligned}P(X,Y,Z) &= (3X - \Sigma_1)(3Y - \Sigma_1)(3Z - \Sigma_1)\\ &= (9XY - 3X\Sigma_1 - 3Y\Sigma_1 + \Sigma_1^2)(3Z - \Sigma_1).\\ &= 27XYZ - 9XY\Sigma_1 - 9XZ\Sigma_1 + 3X\Sigma_1^2 - 9YZ\Sigma_1 + 3Y\Sigma_1^2 + 3Z\Sigma_1^2 - \Sigma_1^3\\ &= 27XYZ - 9(XY + XZ + YZ)\Sigma_1 + 3(X+Y+Z)\Sigma_1^2 - \Sigma_1^3.\end{aligned}$$

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. *On suppose que A est intègre. Soit $n \geq 2$ un entier. 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. Elle pourra être détaillée en cours si le temps le permet. On ne la reprend pas dans ces notes, et renvoyons aux divers ouvrages de référence. On développe en revanche ci-dessous quelques applications des polynômes symétriques à des questions concrètes d'algèbre.

10.2.4 Formules de Newton

On reprend toutes les notations et hypothèses des paragraphes précédents. 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. *On suppose que A est intègre. Soit $n \geq 2$ un entier. On a les relations suivantes dans l'anneau $A[X_1, X_2, \ldots, X_n]$:*

(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 le polynôme $P(Z) = (Z - X_1)(Z - X_2)\dots(Z - X_n)$ dans l'anneau $A[X_1, X_2, \dots, X_n][Z]$. Comme on l'a vu à la fin de 10.2.2, 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 $A[X_1, X_2, \dots, X_n][Z]$ 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 $A[X_1, X_2, \dots, X_{n-1}]$, et on fixe $1 < k < n$.

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

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

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

En d'autres termes, $Q(X_1, \dots, X_{n-1}, 0) = 0$ dans $A[X_1, X_2, \dots, X_{n-1}, X_n]$. On en déduit que Q est divisible par X_n dans $A[X_1, X_2, \dots, X_{n-1}, X_n]$. 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 $X_1X_2\dots X_n$. 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*). On suppose que A est intègre. Soit $n \geq 2$ un entier. On a les relations suivantes dans l'anneau $A[X_1, X_2, \dots, X_n]$:

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

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 $K[X_1, X_2, \dots, X_n]$ 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.

COROLLAIRE (une autre forme du théorème fondamental ; cas d'un corps de caractéristique zéro). *Soit $n \geq 2$ un entier. On suppose que A est anneau intègre et 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 remarque ci-dessus avec le théorème fondamental 10.2.3. □

10.2.5 Relations entre coefficients et zéros d'un polynôme en une indéterminée.

DÉFINITION. Un corps K est dit *algébriquement clos* si tout polynôme de $K[X]$ de degré non-nul admet (au moins) un zéro dans K.

Remarque. Si K est algébriquement clos ; tout polynôme de degré $n \geq 1$ dans $K[X]$ se décompose en un produit de n facteur de degré un, et a donc n zéros dans K (compt{e avec leur ordre de multiplicite).

Exemples et contre-exemples. Le corps $\mathbb{C}$ est algébriquement clos (théorème de d'Alembert-Gauss). Les corps $\mathbb{R}$ et $\mathbb{Q}$ ne sont pas algébriquement clos. Un corps fini F n'est jamais algébriquement clos (car le polynôme $P(X) = \prod_{a \in F}(X - a) + 1$ n'a pas de zéros dans F puisqu'il prend la valuer 1 en tout point de F).

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 :*

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

Preuve. Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme de $K[X]$, de degré $n \geq 1$. Comme K est algébriquement clos, P admet n zéros $\alpha_1, \alpha_2, \ldots, \alpha_n$ dans K, et se factorise en :

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

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 évalué en les α_i. On a alors d'après la dernière remarque de 10.2.2 :

$$\textstyle\prod_{j=1}^{n}(X - \alpha_i) = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdots + (-1)^{n-1}\sigma_{n-1} X + (-1)^n \sigma_n.$$

On en déduit par identification que : $a_{n-1} = -a_n\sigma_1$, $a_{n-2} = a_n\sigma_2$, ..., jusqu'à $a_1 = (-1)^{n-1} a_n \sigma_{n-1}$, $a_0 = (-1)^n a_n \sigma_n$. □

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 $\sigma_i = \Sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Alors $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les zéros du polynôme :*

$$X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdots + (-1)^n \sigma_n.$$

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 :

$$\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \quad \text{et} \quad \sigma_3 = \alpha_1\alpha_2\alpha_3 = -q.$$

10.3 Résultant et discriminant

10.3.1 Notion de résultant de deux polynômes.

COMMENTAIRE. Dans toute cette partie, K est un corps algébriquement clos. On cherche à résoudre la question suivante : étant donnés deux polynômes distincts P et Q de degré ≥ 1 dans $K[X]$, 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.

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 :

$$R(P,Q) = \begin{vmatrix}
a_m & 0 & . & 0 & 0 & b_n & 0 & . & 0 & 0 \\
a_{m-1} & a_m & . & . & . & b_{n-1} & b_n & . & . & . \\
a_{m-2} & a_{m-1} & . & . & . & b_{n-2} & b_{n-1} & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & a_m & 0 & . & . & . & . & . \\
a_{m-n+1} & a_{m-n+2} & . & a_{m-1} & a_m & b_1 & . & . & . & . \\
a_{m-n} & a_{m-n+1} & . & a_{m-2} & a_{m-1} & b_0 & b_1 & . & . & . \\
a_{m-n-1} & a_{m-n} & . & . & a_{m-2} & 0 & b_0 & . & . & . \\
. & . & . & . & . & 0 & 0 & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 0 & . \\
a_2 & a_3 & . & a_n & a_{n+1} & 0 & . & . & b_n & 0 \\
a_1 & a_2 & . & a_{n-1} & a_n & 0 & . & . & b_{n-1} & b_n \\
a_0 & a_1 & . & a_{n-2} & a_{n-1} & 0 & . & . & b_{n-2} & b_{n-1} \\
0 & a_0 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & a_0 & a_1 & . & . & . & b_0 & b_1 \\
0 & 0 & . & 0 & a_0 & 0 & 0 & . & 0 & b_0
\end{vmatrix}
\begin{matrix}
\leftarrow 1 \\ \leftarrow 2 \\ \leftarrow 3 \\ \\ \\ \leftarrow n \\ \leftarrow n+1 \\ \leftarrow n+2 \\ \\ \\ \\ \leftarrow m-1 \\ \leftarrow m \\ \leftarrow m+1 \\ \\ \\ \\ \leftarrow m+n
\end{matrix}$$

$\underbrace{\qquad\qquad}_{n}$ $\underbrace{\qquad\qquad}_{m}$

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

LEMME. *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 :*

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

Preuve. Supposons les trois conditions du lemme 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 $X-\alpha_i$ qui divise R ou $X-\alpha_i$ qui divise Q, et ceci quel que soit $1 \leq i \leq m$. Comme $\deg R < m$, on ne peut pas avoir R divisible par $(X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_m)$. 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 $\deg D \geq 1$, 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 $RQ = RSD = SP$. □

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 le lemme, 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 :

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

En faisant "tout passer" dans le premier membre, on obtient un système linéaire homogène, de $m+n$ équations à $m+n$ inconnues, qui sont $\mu_{n-1}, \mu_{n-2}, \dots, \mu_0, -\lambda_{m-1}, -\lambda_{m-2}, \dots, -\lambda_0$. 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 au début du paragraphe 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 $R(P,Q) = a^7 + 2a^4 + 3a^3 + a^2 + a + 1$.)

10.3.2 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 :*

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

Alors le résultant 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. Les a_i pour $1 \leq i \leq m$ et les b_j pour $1 \leq j \leq n$*sont les coefficients dans K de P et Q respectivement, avec donc $a_m \neq 0$ et $b_n \neq 0$. Les α_i pour $1 \leq i \leq m$ et les β_j pour $1 \leq j \leq n$*sont les zéros dans K de P et Q respectivement, comptés avec leur ordre de multiplicité. 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 :

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

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 10.2.5, on a :

$$\sigma_1 = -\frac{a_{m-1}}{a_m}, \quad \cdots \quad \sigma_m = (-1)^m \frac{a_0}{a_m}, \quad \sigma'_1 = -\frac{b_{n-1}}{b_n}, \quad \cdots \quad \sigma'_n = (-1)^n \frac{b_0}{b_n},$$

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 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 10.3.2 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 :

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

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 10.2.3).

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 10.3.1 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 en tire que $R(P_1,Q_1) = \Pi$. On conclut $R(P,Q) = a_m^n b_n^m \Pi$, ce qui achève la preuve. □

REMARQUE. On a donc les expressions suivantes du résultant :

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

qui rendent explicite la conclusion du théorème 10.3.1

10.3.3 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) est claire. Par définition du discriminant, l'équivalence de (iii) et (iv) est une conséquence du théorème 10.3.1. 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 $P = a_nX^n + \cdots + a_1X + a_0$ 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 finale de 10.3.2 :

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

□

Remarque. Cette relation justifie le nom de discriminant des indéterminées donné à l'exemple (3) du paragraphe 10.2.2.