Préface. VOYAGE AU PAYS DES POLYNÔMES

Martin Debaisieux

Contenu

Cette préface à la géométrie algébrique revisite partiellement la hiérarchie des anneaux commutatifs en adoptant le point de vue des anneaux de polynômes. Divers résultats préparatoires à la suite des chapitres figurent également dans ce document.

1 Les anneaux intègres

Rappel 1.1. Un anneau *intègre* est un anneau commutatif non nul dans lequel le produit de deux éléments non nuls quelconques est non nul.

Nota Bene 1.2. Un anneau commutatif est intègre si et seulement si son idéal nul est premier.

Exemple 1.3. Si A est un anneau intègre alors $A[X]$ l'est aussi ; par induction l'anneau $A[X_1, \dots, X_n]$ est alors également intègre. En particulier, si K est un corps alors $K[X_1, \dots, X_n]$ est intègre.

Remarque 1.4. Noter que si A n'est pas intègre, alors $A[X]$ non plus (puisqu'il contient A) : l'anneau $(\mathbf{Z}/6\mathbf{Z})[X]$ n'est pas intègre étant donné que $(2X)(3X) = 0X^2 = 0$ bien que ni $2X$, ni $3X$ soit nul.

Stabilité 1.5. Tout sous-anneau d'un anneau intègre est clairement intègre. En revanche, le quotient d'un anneau intègre par un idéal (quelconque) n'est en général pas intègre : l'anneau $\mathbf{R}[X]$ est intègre et pourtant $\mathbf{R}[X]/(X^2-1) \simeq \mathbf{R}[X]/(X-1) \times \mathbf{R}[X]/(X+1) \simeq \mathbf{R} \times \mathbf{R}$ ne l'est pas. Pour que le quotient d'un anneau intègre par un idéal reste intègre, il faut et il suffit de considérer un idéal premier.

Lemme 1.6. *Soit K un corps infini ; si $f \in K[X_1, \dots, X_n]$ s'annule en tout point de K^n, alors f est le polynôme nul (i.e. tous ses coefficients sont nuls).*

Preuve. Par induction sur n. Si $n = 1$ alors $f = f(X) \in K[X]$ et l'assertion est vérifiée puisque un polynôme non nul à une indéterminée admet un nombre fini de racines (borné par son degré). Si $n \geq 2$, considérons $f_a = f(X_1, \dots, X_{n-1}, a) \in K[X_1, \dots, X_{n-1}]$ pour tout $a \in K$. Si f_a s'annule sur K^{n-1}, alors $X_n - a$ divise f et donc, à nouveau par un argument de degré, il ne peut y avoir qu'un nombre fini de tels $a \in K$. $\square$

Remarque 1.7. L'hypothèse d'infinitude de K est cruciale : considérons $p \in \mathbf{Z}$ un nombre premier, alors $X^p + Y^p - X - Y \in \mathbf{F}_p[X, Y]$ s'annule en tout point et admet pourtant des coefficients non nuls.

2 Les anneaux factoriels

Rappel 2.1. Un anneau *factoriel* est un anneau intègre dans lequel tout élément non nul se décompose de façon unique en un produit fini d'irréductibles, à inversible près et à ordre des facteurs près.

Remarque 2.2. Cette notion est plus restrictive que l'intégrité : si K est un corps, l'anneau $K[X^2, X^3]$ est intègre mais n'est pas factoriel car $X^6 = (X^2)^3 = (X^3)^2$ et ces deux factorisations sont données par des irréductibles non associés.

Théorème 2.3 (Gauss)**.** *Soit A un anneau factoriel ; alors $A[X]$ est factoriel. En particulier, l'anneau $A[X_1, \ldots, X_n]$ est factoriel dès que A l'est.*

Preuve. Détaillée dans [Woo20]. □

Lemme 2.4. *Soient A un anneau factoriel et K son corps des fractions ; si f, $g \in A[X]$ sont copremiers dans $A[X]$, ils le sont aussi dans $K[X]$ et donc il existe a, $b \in A[X]$ et un $d \in A - \{0\}$ tels que $af + bg = d$.*

Preuve. Puisque $K[X]$ est principal, il existe a', $b' \in K[X]$ tels que $a'f + b'g = 1$ par Bézout. Comme A est factoriel, il existe un $d \in A - \{0\}$ tel que $a := da'$ et $b := db'$ sont deux éléments de $A[X]$. □

Critère 2.5 (Eisenstein)**.** *Soit A un anneau factoriel et $f(X) = a_n X^n + \cdots + a_0 \in A[X]$ de degré au moins 1 ; si un irréductible $\pi \in A$ divise chaque a_i pour $0 \leq i < n$, ne divise pas a_n et est tel que son carré ne divise pas a_0, alors f est irréductible dans $A[X]$.*

Exemple 2.6. Soit K un corps et soit $A = K[Y]$; dès lors $A[X] \simeq K[X, Y]$:

— $f(X, Y) = X^2 + Y^2 + 1$ est irréductible dans $\mathbf{R}[X, Y]$ par le critère d'Eisenstein en $Y^2 + 1$ (mais aussi par le critère de réduction). Il est également irréductible dans $\mathbf{C}[X, Y]$ par le critère d'Eisenstein en $Y + i$ (ou $Y - i$) puisque $X^2 + Y^2 + 1 = X^2 + (Y + i)(Y - i)$.

— $f(X, Y) = X^2 + Y^2 - 1$ est irréductible dans $K[X, Y]$ si et seulement si K n'est pas de caractéristique 2 : en effet, si K est de caractéristique 2 alors $f(X, Y) = (X+Y+1)^2$ et est donc réductible ; sinon $Y + 1 \neq Y - 1$, donc $f(X, Y) = X^2 + (Y - 1)(Y + 1)$ et ainsi le critère d'Eisenstein en $Y + 1$ (ou $Y - 1$) peut être appliqué.

Critère 2.7 (réduction)**.** *Soient A un anneau factoriel et $\mathfrak{p}$ un idéal premier de A ; alors $A \twoheadrightarrow A/\mathfrak{p}$ induit un épimorphisme canonique $A[X] \twoheadrightarrow (A/\mathfrak{p})[X] \colon f(X) \mapsto \bar{f}(X)$. Soit $f \in A[X]$ non nul tel que* $\deg f = \deg \bar{f}$ *; si $\bar{f}$ est irréductible dans* $\mathrm{Frac}(A/\mathfrak{p})[X]$ *alors f est irréductible dans* $\mathrm{Frac}(A)[X]$*. De plus, si le coefficient dominant de f est inversible dans A alors f est irréductible dans $A[X]$.*

Exemple 2.8. Soit K un corps. Considérons $A = K[Y]$ et $\mathfrak{p} = (Y)$; alors $K[Y]/(Y) \simeq K$ par factorisation de l'épimorphisme $K[Y] \twoheadrightarrow K$ d'évaluation en $Y = 0$ et donc

$$\begin{array}{rcl} K[X, Y] \simeq (K[Y])[X] & \twoheadrightarrow & (K[Y]/(Y))[X] \simeq K[X] \\ f(X, Y) & \longmapsto & f(X, 0). \end{array}$$

Si $\deg_X f(X, Y) = \deg_X f(X, 0) \neq -\infty$ et si $f(X, 0)$ est irréductible dans $K[X]$, alors $f(X, Y)$ est irréductible dans $K[X, Y]$. Bien entendu, il est possible de remplacer (Y) par n'importe quel idéal de $K[Y]$ engendré par un polynôme irréductible. Ainsi $X + Y^2 + 1$, $X^2 + Y + 1$, $X^2 - Y$ sont irréductibles dans $K[X, Y]$.

Remarque 2.9. Attention, ce critère n'est pas une condition nécessaire : $XY - 1$ est irréductible dans $K[X, Y]$ et pourtant ne satisfait pas les hypothèses du critère. Également, le polynôme $X^2 + Y^2$ est irréductible dans $\mathbf{R}[X]$ mais est réductible dans $\mathbf{C}[X, Y]$. C'est en général un problème difficile de déterminer l'irréductibilité d'un polynôme à plusieurs indéterminées.

Exemple 2.10. Soit K un corps. Le polynôme $Y^2 - X^3$ est irréductible dans $K[X, Y]$ bien qu'aucun des critères précédents ne peut s'appliquer. Un moyen d'y parvenir est de montrer que $(Y^2 - X^3)$ est le noyau du morphisme

$$\begin{array}{rcl} K[X, Y] & \longrightarrow & K[X] \\ f(X, Y) & \longmapsto & f(X^2, X^3). \end{array}$$

Stabilité 2.11. En général, un sous-anneau d'un anneau factoriel n'est pas factoriel : si K est un corps, $K[X^2, X^3]$ n'est pas factoriel mais est pourtant un sous-anneau de $K[X]$. Cela ne se passe pas bien non plus au niveau des quotients : $\mathfrak{p} = (Y^2 - X^3)$ est un idéal premier de $K[X, Y]$ car il est engendré par un irréductible et $K[X, Y]/\mathfrak{p} \simeq K[x, y]$ où $x = X \bmod \mathfrak{p}$ et $y = Y \bmod \mathfrak{p}$ sont tels que x et y sont irréductibles et pourtant $x^3 = y^2$.

3 Les anneaux intégralement clos

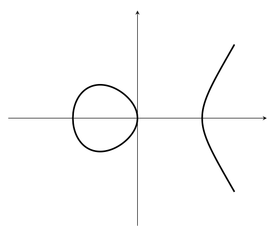
Rappel 3.1. Un anneau *intégralement clos* est un anneau intègre étant sa propre clôture intégrale dans son corps des fractions.

Exemple 3.2. Tout anneau factoriel est intégralement clos ; ainsi, quand A est un anneau factoriel, $A[X_1, \ldots, X_n]$ est intégralement clos. En particulier, $K[X_1, \ldots, X_n]$ est intégralement clos si K est un corps. Noter que la réciproque est fausse : $\mathbf{Z}[i\sqrt{5}]$ est intégralement clos mais n'est pas factoriel.

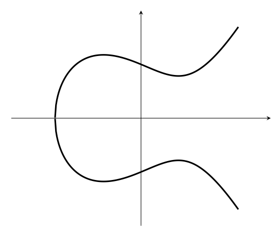
Exemple 3.3. Soit K un corps et posons $A = K[X, Y]/(Y^2 - X^3 - X^2)$. Nous montrons que ce quotient n'est pas intégralement clos (et donc que cette notion n'est pas stable par quotient). Comme $Y^2 - X^3 - X^2 = Y^2 - X^2(X + 1)$ est irréductible (par Eisenstein en $(X + 1)$), A est intègre. De plus, $A = \{f(x) + yg(x) \mid f, g \in K[X]\}$ avec x et y les images de X et Y dans le quotient. Noter que $y^2 = x^3 + x^2 = x^2(x + 1)$ et que $x \notin A^\times$. Soit $y/x \in \operatorname{Frac} A$; alors $(y/x)^2 - x + 1 = 0$ et donc y/x est entier sur A mais n'est pas un élément de A.

Remarque 3.4. En posant $f(X) = X^3 + X^2$; alors f admet une racine double en 0 (autrement dit $(f, f') \neq 1$). Soient a, $b \in K$ tels que $f(X) = X^3 + aX + b$ (tout polynôme monique de degré 3 se ramène à un tel polynôme par $X \mapsto X + \alpha$ avec $\alpha \in K$ bien choisi (ici $\alpha = -1/3$)). Le discriminant de f est $\Delta(f) = -27b^2 - 4a^3$, et $(f, f') = 1$ si et seulement si $\Delta(f) \neq 0$ (*i.e.* f n'a que des racines simples dans K^{alg}). Le fait que $\Delta(f) \neq 0$ implique que $A = K[X, Y]/(Y^2 - f(X))$ soit intégralement clos (admis).

Schématiquement (pour $K = \mathbf{R}$), les deux situations suivantes surviennent (suivant que toutes les racines sont réelles ou que deux racines sont complexes conjuguées) :



Lorsque $\Delta(f) \neq 0$.



Lorsque $\Delta(f) = 0$.

Exemple 3.5. Soit K un corps ; l'anneau $K[X, Y]/(Y^2 - X^3)$ n'est pas intégralement clos : si nous notons x et y les images respectives de X et Y dans ce quotient alors $y^2 = x^3$ et donc $(y/x)^2 - x = 0$.

Stabilité 3.6. La théorie algébrique des nombres nous apprend dès le début qu'un sous-anneau d'un anneau intégralement clos ne l'est pas nécessairement : $\mathbf{Z}[(1 + i\sqrt{3})/2]$ est l'anneau des entiers de $\mathbf{Q}(i\sqrt{3})$ et pourtant contient l'anneau $\mathbf{Z}[i\sqrt{3}]$ qui n'est pas intégralement clos. Un argument similaire montre que $(\mathbf{Z}[i\sqrt{3}])[X]$ n'est pas non plus intégralement clos.

4 Les anneaux principaux

Rappel 4.1. Un anneau *principal* est un anneau intègre dont tous ses idéaux sont principaux.

Remarque 4.2. Tout anneau principal est factoriel. L'idée repose sur le fait qu'un anneau principal est noethérien et que la condition de chaîne ascendante sur les idéaux principaux implique l'existence d'une factorisation des éléments non nuls en irréductibles (existence) ; d'un autre côté, le lemme de Bézout est valable dans un anneau principal, permettant de montrer que tout irréductible est premier et donc que deux factorisations en irréductibles d'un même élément sont égales à l'ordre et à associé près (unicité). La réciproque est fausse : $\mathbf{Z}[X]$ n'est pas principal mais est factoriel.

Proposition 4.3. *Soit A un anneau commutatif ; $A[X]$ est principal si et seulement si A est un corps.*

Preuve. Si $A[X]$ est principal : soit $a \in A$ non nul ; l'idéal (a, X) de $A[X]$ est principal et donc $a \in A^\times$.

Si A est un corps : soit $\mathfrak{a}$ un idéal non nul (trivial sinon) de $A[X]$. Soit $f \in \mathfrak{a}$ un polynôme non nul de degré minimal ; nous montrons que $\mathfrak{a} = (f)$. Soit $g \in \mathfrak{a}$, par l'algorithme de division, il existe des polynômes q et r tels que $g = qf + r$ avec $\deg(r) < \deg(f)$. Alors $r = g - qf \in \mathfrak{a}$ et puisque f est supposé minimal, $r = 0$. Donc $g = qf \in (f)$. □

Exemple 4.4. Soit K est un corps ; l'anneau $K[X_1, \ldots, X_n]$ est principal à la seule et unique condition que $n \in \{0, 1\}$ (avec pour convention qu'en $n = 0$ il s'agit de K).

Stabilité 4.5. Un sous-anneau d'un anneau principal n'est pas nécessairement principal : $\mathbf{Z}[X]$ est un sous-anneau de $\mathbf{Q}[X]$ n'étant pas principal. En revanche, le quotient d'un anneau principal par un idéal premier reste principal : si A est principal alors $\mathfrak{p} \in \operatorname{Spec} A$ implique que $\mathfrak{p} = (a)$ où $a \in A$ est nul ou irréductible et donc $\mathfrak{p}$ est nul ou maximal ; ainsi $A/\mathfrak{p} \simeq A$ ou est un corps.

5 Les corps

Rappel 5.1. Un *corps* est un anneau intègre K vérifiant $K^\times = K - \{0\}$.

Remarque 5.2. Tout corps est principal puisque les seuls idéaux d'un corps sont l'idéal nul et le corps lui même. La réciproque est fausse : si K est un corps, $K[X]$ est principal mais n'est pas un corps car $K[X]^\times = K^\times$.

Lemme 5.3. *Tout corps algébriquement clos est infini.*

Preuve. Soit K est un corps algébriquement clos. Si K est de caractéristique 0 alors $\mathbf{Q} \rightarrowtail K$ et donc il est infini. Sinon, $\mathbf{F}_p \rightarrowtail K$ pour un certain nombre premier $p \in \mathbf{Z}$ et K est algébriquement clos, donc $\mathbf{F}_p^{\mathrm{alg}} \rightarrowtail K$; il est ainsi infini.

Un autre argument consiste à supposer que $K = \{\alpha_1, \ldots, \alpha_n\}$ est fini et dès lors le polynôme $1 + (X - \alpha_1) \cdots (X - \alpha_n)$ ne possède aucune racine dans K. □

Lemme 5.4. *Soit K un corps algébriquement clos et soit $f \in K[X, Y]$; alors f n'admet pas de racine dans K^2 si et seulement si $f \in K^\times$.*

Preuve. Si f est non constante, il peut être supposé sans perte de généralité que $\deg_X f \geq 1$; notons-le n. Alors $f(X, Y) = f_n(Y)X^n + \cdots + f_0$ où les $f_i \in K[Y]$ et avec $f_n(Y)$ non nul. Comme le nombre de racines dans K de f_n est borné par son degré, il y en un nombre fini et comme K est infini (puisqu'il est algébriquement clos), il existe un $y \in K$ en lequel f_n ne s'annule pas. Ainsi $f(X, y)$ est un polynôme de $K[X]$ de degré $n \geq 1$; il possède donc une racine, à nouveau puisque K est algébriquement clos. □

Exemple 5.5. Le polynôme $X^2 + Y^2 + 1$ admet des racines dans $\mathbf{C}^2$ mais pas dans $\mathbf{R}^2$.

Remarque 5.6. Ce résultat se généralise par induction à un nombre fini d'indéterminées (dans l'anneau $K[X_1, \ldots, X_n]$), toujours sous l'hypothèse que K est algébriquement clos.

Stabilité 5.7. Un sous-anneau d'un corps n'est pas forcément un corps : si A est un anneau intègre alors $A[X]$ est un sous-anneau de son corps des fractions $\operatorname{Frac} A[X] = A(X)$, le premier n'est pas un corps, alors que le deuxième oui. Le quotient d'un corps par un idéal premier (donc par l'idéal nul) est isomorphe au corps et est donc un corps.

Résumé 5.8. Le tableau suivant résume les différentes analyses de stabilité des précédentes notions :

A anneau commutatif	Intègre	Intégralement clos	Factoriel	Principal	Corps
B sous-anneau de A	oui	non	non	non	non
$\mathfrak{p} \in \operatorname{Spec}(A)$; $A/\mathfrak{p}$	oui	non	non	oui	oui

6 Les idéaux premiers

L'ensemble des idéaux premiers d'un anneau commutatif possède quantité de propriétés remarquables sur lesquelles est fondée la géométrie algébrique moderne (théorie des schémas d'A. Grothendieck). Pour la fin de ce document, fixons A un anneau commutatif.

Rappel 6.1. Un idéal $\mathfrak{p}$ de A est *premier* si $\mathfrak{p} \neq A$ et si pour tous a, $b \in A$, quand $ab \in \mathfrak{p}$ alors $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Autrement dit, si $A/\mathfrak{p}$ est intègre.

Exemple 6.2. Soit K un corps. Ci-après est listé l'ensemble des idéaux premiers de divers anneaux :

— $\operatorname{Spec} \mathbf{Z} = \{(0)\} \cup \{p\mathbf{Z} \mid p \in \mathbf{Z} \text{ premier}\}$ (justifiant la terminologie de premier).

— $\operatorname{Spec} K = \{(0)\}$.

— $\operatorname{Spec} K[X] = \big\{(f) \bigm| f = 0 \text{ ou est irréductible dans } K[X]\big\}$.

— $\operatorname{Spec} K[X,Y] = \big\{(f) \bigm| f = 0 \text{ ou est irréductible dans } K[X,Y]\big\} \cup \operatorname{Spm} K[X,Y]$.

Remarque 6.3 (Origine de la terminologie)**.** Soit E un K-espace vectoriel de dimension n et soit $\ell\colon E \to E$ un endomorphisme. L'évaluation en ℓ :

$$\mathrm{ev}_\ell\colon \left\{ \begin{array}{rcl} K[X] & \longrightarrow & \mathrm{End}_K(E) \\ f & \longmapsto & f(\ell) \end{array} \right.$$

est un morphisme de K-algèbres, de noyau $\operatorname{Ker}(\mathrm{ev}_\ell) = (M_\ell)$ où M_ℓ est le polynôme minimal de ℓ. Alors $K[X]/(M_\ell) \simeq K[\ell]$. Si K est algébriquement clos alors $M_\ell(X) = \prod_{i=1}^r (X - \lambda_i)^{s_i}$ aves les λ_i deux-à-deux distincts et donc $K[\ell] \simeq \prod_{i=1}^r K[X]/(X-\lambda_i)^{s_i}$ par le théorème des restes chinois. Ainsi

$$\operatorname{Spec}(K[\ell]) \simeq \operatorname{Spec}\left(\textstyle\prod_{i=1}^r K[X]/(X-\lambda_i)^{s_i}\right) \simeq \{X - \lambda_i \bmod (M_\ell) \mid 1 \leq i \leq r\} \simeq \operatorname{Spec}(\ell)$$

dans la catégorie des ensembles – afin d'obtenir le dernier isomorphisme.

Lemme 6.4. *Soient $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ des idéaux de A et soit $\mathfrak{p} \in \operatorname{Spec} A$; si leur produit $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ est contenu dans $\mathfrak{p}$ alors $\mathfrak{p}$ contient l'un des $\mathfrak{a}_i$.*

Preuve. Par induction sur n : si $n = 2$ supposons que ni $\mathfrak{a}_1 \subseteq \mathfrak{p}$, ni $\mathfrak{a}_2 \subseteq \mathfrak{p}$. Il est alors possible de trouver un $a \in \mathfrak{a}_1 - \mathfrak{p}$ et un $b \in \mathfrak{a}_2 - \mathfrak{p}$; alors $ab \in \mathfrak{a}_1\mathfrak{a}_2$ et comme $\mathfrak{p}$ est premier, $ab \notin \mathfrak{p}$. Ainsi $\mathfrak{a}_1\mathfrak{a}_2 \not\subseteq \mathfrak{p}$. Le résultat général s'obtient en remarquant que $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_1(\mathfrak{a}_2 \cdots \mathfrak{a}_n)$. □

Exemple 6.5. Ceci généralise la notion de nombre premier p dans $\mathbf{Z}$: si p divise $a_1 \cdots a_n$ alors il existe un i pour lequel p divise a_i :

— $a_1\mathbf{Z} \cdots a_n\mathbf{Z} = (a_1 \cdots a_n)\mathbf{Z} \subseteq p\mathbf{Z}$ si et seulement si p divise $a_1 \cdots a_n$, et

— $a_i\mathbf{Z} \subseteq p\mathbf{Z}$ si et seulement si p divise a_i.

Lemme 6.6. *Soit $\mathfrak{a}$ un idéal non premier et distinct de A ; alors il existe deux idéaux $\mathfrak{b}_1$, $\mathfrak{b}_2$ de A tels que $\mathfrak{a} \subset \mathfrak{b}_1$, $\mathfrak{a} \subset \mathfrak{b}_2$ et $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$.*

Preuve. Comme $\mathfrak{a}$ est non premier, il est possible de trouver deux éléments b_1, $b_2 \in A - \mathfrak{a}$ dont seul le produit b_1b_2 est dans $\mathfrak{a}$. Les idéaux $\mathfrak{b}_1 = \mathfrak{a} + (b_1)$ et $\mathfrak{b}_2 = \mathfrak{a} + (b_2)$ contiennent strictement $\mathfrak{a}$ et leur produit $\mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{a} + (b_1b_2)$ est contenu dans $\mathfrak{a}$ puisque $b_1b_2 \in \mathfrak{a}$. □

Lemme 6.7 (Évitemment des idéaux premiers)**.** *Soit $\mathfrak{a}$ un idéal de A et soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec} A$; si $\mathfrak{a}$ n'est contenu dans aucun des $\mathfrak{p}_i$ alors il n'est pas non plus contenu dans l'union $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$.*

Preuve. Par induction sur n. Si $n = 1$, le résultat est trivial. Supposons que $n \geq 2$ et considérons en chaque i un $x_i \in \mathfrak{a} - \bigcup_{j \neq i} \mathfrak{p}_j$ (non vide par hypothèse d'induction). Si l'un des $x_i \notin \mathfrak{p}_i$ alors le résultat est vérifié. Sinon chaque $x_i \in \mathfrak{p}_i$ et donc l'élément $x = x_1 \cdots x_{n-1} + x_n \in \mathfrak{a} - \bigcup_i \mathfrak{p}_i$: en effet, si $x \in \mathfrak{p}_i$ pour $i < n$ alors $x_n \in \mathfrak{p}_i$ et cela est absurde ; sinon $x \in \mathfrak{p}_n$ et l'un des x_i où $i < n$ aussi, ce qui est à nouveau absurde. □

Lemme 6.8. *Dans un anneau noethérien, tout idéal contient un produit d'idéaux premiers non nuls.*

Preuve. Supposons que le lemme soit faux pour un anneau A et considérons un contre-exemple maximal $\mathfrak{a}$. Comme $\mathfrak{a}$ n'est en particulier pas premier, il existe $x, y \in A$ dont seul le produit appartient à $\mathfrak{a}$. Les idéaux $\mathfrak{a} + (x)$ et $\mathfrak{a} + (y)$ contiennent strictement $\mathfrak{a}$; par maximalité de $\mathfrak{a}$ parmi les contre-exemples, ils contiennent tout deux un produit d'idéaux premiers. Alors $(\mathfrak{a} + (x))(\mathfrak{a} + (y))$ est contenu dans $\mathfrak{a}$ et contient un produit d'idéaux premiers, amenant une contradiction. □

Remarque 6.9. Nous posons $\operatorname{Spec}(A)_{\min} := \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \text{ est minimal pour l'inclusion}\}$; alors A est intègre si et seulement si $\operatorname{Spec}(A)_{\min} = \{(0)\}$. En effet, A est intègre si et seulement si (0) est premier ; or (0) est contenu dans tout idéal premier.

Proposition 6.10. *Dans un anneau noethérien A, $\operatorname{Spec}(A)_{min}$ est fini.*

Preuve. En appliquant le lemme 6.8 à l'idéal (0), nous obtenons un nombre fini d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ de A tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq (0)$. Nous affirmons que $\operatorname{Spec}(A)_{\min} \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ et est donc fini. En effet, soit $\mathfrak{p}$ un idéal premier de A, alors $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq (0) \subseteq \mathfrak{p}$ et par le lemme 6.4, l'un des $\mathfrak{p}_i$ est contenu dans $\mathfrak{p}$. □

7 Les idéaux maximaux

Rappel 7.1. Un idéal $\mathfrak{m}$ de A est *maximal* si $\mathfrak{m} \neq A$ et si pour tout idéal $\mathfrak{a}$ de A, quand $\mathfrak{m} \subset \mathfrak{a}$ alors $\mathfrak{a} = A$. Autrement dit, si $A/\mathfrak{m}$ est un corps.

Remarque 7.2. Tout anneau commutatif non nul possède un idéal maximal : ceci découle du théorème de Krull (tout idéal distinct de l'anneau est contenu dans un idéal maximal). Ainsi $\operatorname{Spm} A \neq \varnothing$ dès que A est non nul. Puisque $\operatorname{Spec} A \supseteq \operatorname{Spm} A$, il est également non vide lorsque A est non nul.

Exemple 7.3. Soit K un corps. Ci-après est listé l'ensemble des idéaux maximaux de divers anneaux :

— $\operatorname{Spm} \mathbf{Z} = \operatorname{Spec} \mathbf{Z} - \{(0)\}$.

— $\operatorname{Spm} K = \operatorname{Spec} K$.

— $\operatorname{Spm} K[X] = \operatorname{Spec} K[X]$.

— $\operatorname{Spm} K[X,Y] = \{(X-\alpha, Y-\beta) \mid \alpha, \beta \in K\}$ (cf. Chapitre I).

Remarque 7.4. Noter que $\operatorname{Spm} K[X,Y] \subset \operatorname{Spec} K[X,Y]$ car ce dernier comprend tous les idéaux engendré par un irréductible : $(X-\alpha)$ et $(Y-\beta)$ ne sont pas maximaux (mais sont engendrés par des irréductibles).

Références

[Per95] Daniel Perrin. *Géométrie algébrique. Une introduction.* InterÉditions-CNRS, 1995, p. 301. isbn : 2-271-05271-8.

[Vol07] Maja Volkov. « Géométrie algébrique : compléments d'algèbre commutative ». US-M1-SCMATH-003-M, Projet en géométrie algébrique. 2007.

[Mil17] James S. Milne. *Algebraic Geometry (v6.02).* 2017. url : `https://www.jmilne.org/math/CourseNotes/AG.pdf`.

[Woo20] Russ Woodroofe. *Polynomial rings and unique factorization domains.* 2020. url : `https://osebje.famnit.upr.si/~russ.woodroofe/wustl-notes/ufds.pdf`.