Algèbre commutative et géométrie algébrique

Christophe Mourougane

Master de Mathématiques

Table des matières

Chapitre 1

Propriétés des anneaux

Conventions

Tous les anneaux considérés sont commutatifs, et soit réduits à $\{0\}$, soit munis d'un élément neutre pour la multiplication. Les morphismes d'anneaux respectent les éléments neutres.

1. Propriétés de base

On résume les caractéristiques usuelles des anneaux et leurs relations.

1.1. Définition. On cherche à décomposer chaque élément d'un anneau en briques élémentaires.

DÉFINITION 1. *Deux éléments a et b d'un anneau sont dits* associés *si a divise b et b divise a. Un élément a d'un anneau A est dit*

a) inversible *s'il existe un élément b de A tel que $ab = 1_A$.*
b) diviseur de zéro *s'il est non nul et s'il est annulé par multiplication par un élément non nul de A.*
c) irréductible *s'il est non nul, non inversible et non produit de deux éléments non inversibles.*
d) premier *s'il est non inversible et si pour tout $(b, c) \in A^2$, $(a \mid bc \implies a \mid b \text{ ou } a \mid c)$*

PROPOSITION 2. *Soit A un anneau intègre.*

— *Deux éléments a et b de A sont associés s'il existe un inversible u de A tel que $a = ub$ i.e. $(a) = (b)$.*
— *Un élément a est irréductible si et seulement s'il est non nul, non inversible et pour tout $(b, c) \in A^2$, $(a = bc \implies a \mid b \text{ ou } a \mid c)$ i. e. ses seuls diviseurs sont inversibles ou associés à a.*
— *Un élément a est irréductible si et seulement s'il est non nul et non inversible et l'idéal (a) est maximal parmi les idéaux principaux.*
— *Un élément premier non nul est irréductible.*
— *Si $a = bc$ avec c non inversible alors $(a) \subsetneq (b)$.*

Ces définitions de briques élémentaires ont des contreparties en termes (de grande taille) d'idéaux.

DÉFINITION 3. *Un idéal $\mathcal{I}$ d'un anneau A est dit*

— propre *s'il est strictement contenu dans A.*
— premier *s'il est propre et si pour tout $(b, c) \in A^2$,*
$(bc \in \mathcal{I} \implies b \in \mathcal{I} \text{ ou } c \in \mathcal{I})$
— maximal *s'il est propre et si tout idéal $\mathcal{J}$ de A vérifie*
$(\mathcal{I} \subset \mathcal{J} \subset A \implies \mathcal{J} = \mathcal{I} \text{ ou } \mathcal{J} = A)$.

Les propriétés précédentes se caractérisent par la

PROPOSITION 4. *Soit a un élément d'un anneau A et $\mathcal{I}$ un idéal.*

— a *est inversible* $\iff (a) = A$.
— a *est premier* $\iff (a)$ *est premier.*
— $\mathcal{I}$ *est premier* $\iff A/\mathcal{I}$ *est intègre.*
— $\mathcal{I}$ *est maximal* $\iff A/\mathcal{I}$ *est un corps.*
— $\mathcal{I}$ *maximal* $\implies \mathcal{I}$ *premier.*

DÉFINITION 5. *Un ensemble* $(E, \leqslant)$ *muni d'une relation d'ordre est dit* inductif *si toute partie totalement ordonnée* F *de* E *admet un majorant dans* E *(i.e. il existe* $x \in E$ *supérieur à tous les éléments de* F*).*

LEMME 6 (Lemme de Zorn). *Tout ensemble non vide ordonné inductif admet un élément maximal.*

Puisqu'une réunion croissante d'idéaux propres est un idéal propre, l'ensemble des idéaux propres d'un anneau est ordonné inductif. Par le lemme de Zorn, on a donc

PROPOSITION 7. *Soit* A *un anneau.*
a) Tout idéal propre de A *est inclus dans un idéal maximal de* A*.*
b) Un élément de A *est inversible si et seulement s'il n'est dans aucun idéal maximal de* A*.*

1.2. Existence des décompositions d'éléments en produits d'irréductibles. On peut renforcer le lemme de Zorn par la

DÉFINITION 8. *Un anneau* A *est dit* noethérien *s'il satisfait l'une des trois propriétés équivalentes suivantes :*
a) chacun de ses idéaux $\mathcal{I}$ *est engendré par un nombre fini d'éléments de* $\mathcal{I}$ *i.e. est de type fini.*
b) toute suite croissante d'idéaux est stationnaire.
c) toute partie non vide de l'ensemble de ses idéaux possède un élément maximal.

Les anneaux principaux, les quotients d'anneaux noethériens sont noethériens. Par le théorème de Hilbert, si A est noethérien $A[X]$ l'est aussi ainsi donc que toute A-algèbre de type fini (voir proposition 27).

DÉFINITION 9. *Un anneau* A *est dit* atomique *s'il est intègre et si tout élément de* A *non nul et non inversible s'écrit comme produit d'un nombre fini d'irréductibles.*

En utilisant le dernier item de la proposition 2, on obtient la

PROPOSITION 10. *Les anneaux noethériens intègres sont atomiques.*

1.3. Unicité des décompositions. La recherche des diviseurs communs à deux éléments conduit aux

DÉFINITION 11. *Soit* A *un anneau. Deux éléments* a *et* b *de* A *sont dits*
— premiers entre eux *si tous leurs diviseurs communs sont inversibles*
i.e. si le seul idéal principal qui contient $(a) + (b)$ *est* A*.*
— étrangers *si* $(a) + (b) = A$*.*

DÉFINITION 12. *(Voir [B]) On dit qu'un anneau* A *intègre vérifie*
— le lemme d'Euclide *si ses éléments irréductibles sont premiers*
i.e. pour tout $(a, b, c) \in A^3$*, si* a *est irréductible et* $a \nmid b$ *alors* $(a \mid bc \implies a \mid c)$*.*
— le lemme de Gauss *si*
pour tout $(a, b, c) \in A^3$*, si* a *et* b *sont premiers entre eux alors* $(a \mid bc \implies a \mid c)$*.*
— le théorème de Bezout *si ses éléments premiers entre eux sont étrangers.*

PROPOSITION 13. *On a les implications :*

Le théorème de Bezout $\Longrightarrow$ *Le lemme de Gauss* $\Longrightarrow$ *Le lemme d'Euclide.*

DÉFINITION 14. *Un anneau A est dit*

- factoriel *s'il est intègre et si tout élément de A non nul et non inversible s'écrit comme produit d'irréductibles, de façon unique à l'ordre et à association près.*
- principal *s'il est intègre et si chacun de ses idéaux est principal. (Il suffit en fait de tester ses idéaux premiers. voir [M] page 38)*
- Euclidien *s'il est intègre et s'il existe une fonction $\nu : A - \{0\} \to \mathbb{N}$ telle que pour tout couple $(a, d) \in A \times (A - \{0\})$ il existe un couple $(q, r) \in A^2$ tel que $a = qd + r$ et $r = 0$ ou $\nu(r) < \nu(d)$.*

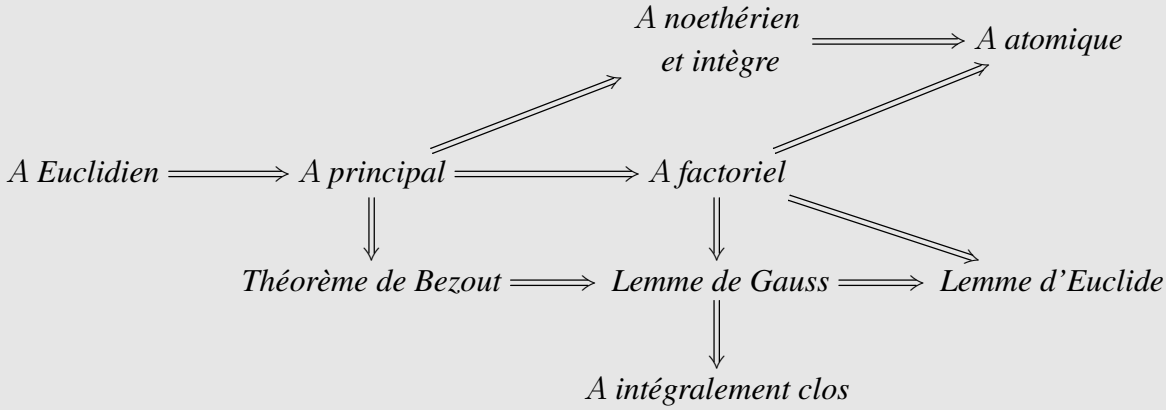
Les anneaux Euclidiens sont principaux, par une démonstration proche de celle pour $\mathbb{Z}$.

PROPOSITION 15.

a) Dans un anneau factoriel, les éléments irréductibles sont exactement les éléments premiers non nuls.
b) Dans un anneau principal, les idéaux maximaux sont exactement les idéaux engendrés par un élément irréductible.

DÉFINITION 16. *Un anneau A est dit* intégralement clos *s'il est intègre et si tout élément de son corps de fractions, entier sur A, est en fait dans A.*

THÉORÈME 17. *(Propriétés des anneaux) On a les implications suivantes*



Plus précisément,

PROPOSITION 18.

- *Un anneau atomique est factoriel si et seulement si il vérifie le lemme d'Euclide.*
- *Un anneau atomique est principal si et seulement si il vérifie le théorème de Bezout.*

Pour le premier item, on constate que le lemme d'Euclide assure l'unicité des décompositions en produit d'irréductibles. Pour le second item, un anneau atomique qui vérifie le théorème de Bezout est factoriel. L'existence du pgcd et le théorème de Bezout permettent de montrer d'abord que tout idéal de type fini est principal (On dit que A est un anneau de Bezout). On montre ensuite que dans un anneau factoriel toute suite croissante d'idéaux PRINCIPAUX est stationnaire. (Voir [B])

1.4. Autour de la notion de $pgcd$.

DÉFINITION 19. *Un $pgcd$ de deux éléments a et b d'un anneau A est un élément maximal (pour la relation de divisibilité) de l'ensemble des diviseurs communs de a et de b.*

Il résulte de la définition que deux $pgcd$ d'un même couple sont associés.

PROPOSITION 20.
— *Dans un anneau factoriel, tout couple d'éléments admet un $pgcd$ construit à l'aide des valuations associées à chaque classe d'irréductibles modulo association.*
— *Dans un anneau principal, tout couple d'éléments (a, b) admet un $pgcd$ choisi comme générateur de l'idéal $(a) + (b)$.*

1.5. Autour de la notion de dimension de Krull.

DÉFINITION 21.
— *Un anneau est dit* de dimension 0 *si ses idéaux premiers sont maximaux.*
— *Un anneau est dit* Artinien *s'il est noethérien est de dimension 0.*
— *Un anneau est dit* de dimension inférieure à 1 *si ses idéaux premiers non nuls sont maximaux.*
— *Un anneau est dit* de Dedekind *s'il est intègre, intégralement clos et de dimension inférieure à 1.*

THÉORÈME 22. *(Anneaux principaux)*
— *Les anneaux principaux sont de Dedekind.*
— *Un anneau atomique est principal si et seulement si il est de dimension inférieure à 1.*

Pour montrer qu'un anneau atomique de dimension inférieure à 1 est principal, on montre en prenant un irréductible dans la décomposition d'un élément non nul et non inversible que les idéaux maximaux d'un anneau factoriel sont principaux. On considère ensuite grâce au lemme de Zorn un élément maximal de l'ensemble supposé non vide des idéaux non principaux et on montre qu'il est strictement inclus dans un idéal maximal, principal, et en travaillant dans le corps des fractions qu'il est principal. (voir [M] page 37)

1.6. Exemples d'anneaux. L'intégrité ne se conserve pas par passage au quotient.

La noethérianité se conserve par passage au quotient, par localisation et par passage de l'anneau A à l'anneau de polynômes $A[X_1, \cdots, X_n]$ en un nombre fini de variables.

Les exemples classiques d'anneaux euclidiens incluent l'anneau des entiers relatifs $\mathbb{Z}$; l'anneau des entiers de Gauss $\mathbb{Z}[i]$ et les anneaux de polynômes $k[X]$ en une variable à coefficients dans un corps k.

La factorialité se conserve par localisation et par passage à l'anneau $A[X_1, \cdots, X_n]$ en un nombre fini de variables et même à l'anneau $A[X_i]_{i\in\mathbb{N}}$. L'exemple $\mathbb{C}[X, Y, Z]/(X^2 - YZ)$ montre que la factorialité ne se conserve pas par quotient (l'élément $[X]$ est irréductible, mais pas premier car il divise $[Y][Z]$ sans diviser $[Y]$ ou $[Z]$). Un analogue arithmétique : l'application norme $z = a + bi\sqrt{5} \mapsto z\overline{z} = a^2 + 5b^2$ multiplicative sur l'anneau intègre $\mathbb{Z}[i\sqrt{5}] = \frac{\mathbb{Z}[X]}{(X^2+5)}$ permet de montrer que ses inversibles sont 1 et -1 et que 2 est irréductible. L'égalité $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \times 3$ montre alors que l'élément irréductible 2 n'est pas premier. L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est donc pas factoriel. Mais, comme c'est l'anneau des entiers de $\mathbb{Q}(i\sqrt{5})$ il est intégralement clos.

L'anneau $\mathbb{Z}[X]$ est factoriel, non principal car il ne vérifie pas le théorème de Bezout : ses éléments premiers entre eux 2 et X ne sont pas étrangers. Il est par contre intègre et noethérien.

L'anneau $k[X,Y]$ est factoriel, n'est pas de dimension inférieure à 1 car l'idéal premier (X) n'est pas maximal. Par conséquent, $k[X,Y]$ n'est pas principal (noter que l'idéal (X,Y) n'est pas principal).

Un corps est de dimension 0. Un anneau principal qui n'est pas un corps est de dimension 1. L'anneau non intègre $k[x]/(x^k)$ est de dimension 0 car son seul idéal premier est $(x)/(x^k)$. L'anneau $\mathbb{Z}[\sqrt{5}]$ n'est pas intégralement clos, car le nombre d'or $\frac{1+\sqrt{5}}{2}$ est solution de l'équation $X^2 - X - 1$. Il est par contre intègre et noethérien. L'anneau $k[X,Y]/(X^2 - Y^3)$ est intègre, noethérien, mais non intégralement clos (voir en exercice).

Dans l'anneau $\mathbb{Z}/6\mathbb{Z}$ noethérien non intègre, 2 est non nul et non inversible. Il est non irréductible car $2 = 2 \times (-2)$. Comme ses seuls diviseurs sont les inversibles et 2 et -2 non irréductibles, 2 n'admet pas d'écriture en produits d'irréductibles.

2. Algèbre de polynômes

On rappelle que si A est un anneau, une A-algèbre (associative commutative, unitaire) $(B,+,\cdot,\times)$ est la donnée d'un anneau (commutatif, unitaire) $(B,+,\times)$ muni d'un morphisme d'anneaux $\varphi : A \to B$. La loi définie alors pour $a \in A$ et $x \in B$ par $a \cdot x = \varphi(a) \times x$ fait de $(B,+,\cdot)$ un A-module. De façon équivalente, la donnée d'un anneau (commutatif, unitaire) $(B,+,\times)$ muni d'une structure de A-module $\cdot$ telle que pour tout $a,b \in A$ et $x,y \in B$,

$$(a \cdot x) \times (b \cdot y) = (ab) \cdot (x \times y)$$

est une structure d'algèbre sur B par le morphisme d'anneau $A \to B, a \mapsto a \cdot 1_B$.

Un morphisme d'A-algèbres entre les algèbres B et B' est un morphisme d'anneaux $m : B \to B'$ qui est en plus A-linéaire pour les structures de A-modules.

Définition 23. *Soit $(A,+,\times)$ un anneau (commutatif unitaire). L'algèbre $\iota : A \to A[X_1,\cdots,X_n]$ des polynômes en n indéterminées à coefficients dans A est caractérisée (à isomorphisme près) par la propriété universelle : Pour toute A-algèbre $\varphi : A \to B$ et tout n-uplet $(b_1,\cdots,b_n)$ d'éléments de B, il existe un unique morphisme d'A-algèbres $\Phi : A[X_1,\cdots,X_n] \to B$ tel que pour tout $i = 1,\cdots,n$, $\Phi(X_i) = b_i$.*

Les constructions des algèbres de polynômes, et en particulier de bases canoniques montrent les inclusions naturelles, pour tout $1 \leqslant i_1 < i_2 < \cdots, < i_r \leqslant n$, $1 \leqslant j_{r+1} < j_{r+2} < j_n \leqslant n$, avec $\{i_1, i_2, \cdots i_r, j_{r+1}, \cdots, j_n\} = \{1,2,\cdots,n\}$

$$A[X_{i_1}, X_{i_2}, \cdots, X_{i_r}] \subset A[X_1,\cdots,X_n]$$

et les isomorphismes

$$A[X_{i_1}, X_{i_2}, \cdots, X_{i_r}][X_{j_{r+1}}, \cdots, X_{j_n}] \equiv A[X_1,\cdots,X_n].$$

On synthétise les propriétés des algèbres de polynômes dans

Proposition 24. *Soit A un anneau intègre. Soit n un entier naturel non nul. On note ici $\underline{X} := (X_1,\cdots,X_n)$. Soit $P,Q \in A[X_1,\cdots,X_n]$. Alors*

a) $A[X_1,\cdots,X_n]$ *est intègre.*
b) $\deg_{X_i} P = 0 \iff P \in A[X_1,\cdots,X_{i-1},X_{i+1}\cdots,X_n]$.
c) $\deg_{\underline{X}} P = 0 \iff P \in \iota(A)$
d) $\deg_{X_i}(PQ) = \deg_{X_i} P + \deg_{X_i} Q$.
e) $\deg_{\underline{X}}(PQ) = \deg_{\underline{X}} P + \deg_{\underline{X}} Q$.
f) Les inversibles de l'anneau $A[X_1,\cdots,X_n]$ sont les polynômes constants inversibles : $A[X_1,\cdots,X_n]^\times = \iota(A^\times)$.

(L'application ι est en général omise dans les notations.)

THÉORÈME 25. *(Division euclidienne) Soit A un anneau intègre et P, D deux polynômes de $A[X]$. On suppose que le coefficient dominant de D est inversible dans A. Alors, il existe un unique couple $(Q, R) \in A[X]^2$ tel que*

- $P = QD + R$
- $\deg_X(R) < \deg_X(D)$.

Noter que même si A est principal, $A[X]$ n'est en général pas principal, comme le montre l'idéal $(2, X)$ de $\mathbb{Z}[X]$. L'anneau $A[X]$ n'est donc pas euclidien en général.

DÉFINITION 26. *Soit B une A-algèbre et S une partie de B. On dit que S engendre B si la plus petite A-sous-algèbre de B qui contient S est B. On dit qu'une A-algèbre est de type fini, si elle admet une partie génératrice finie.*

PROPOSITION 27. *Une A-algèbre est de type fini si et seulement si elle peut être décrite comme quotient d'une A-algèbre de polynômes.*

3. Calculs sur les idéaux

DÉFINITION 28. *Soit A un anneau, I et J deux idéaux de A et X une partie de A. On définit alors*

- *la somme $I + J$ comme l'ensemble des sommes d'un élément de I et d'un élément de J.*
- *l'intersection $I \cap J$ comme l'ensemble des éléments de A qui sont dans I et dans J.*
- *le produit IJ comme l'ensemble des sommes finies de produits d'un élément de I par un élément de J.*
- *le quotient $(I : X)$ l'ensemble des éléments a de A pour lesquels pour tout élément x de X le produit xa est dans I.*

Ce sont des idéaux de A.

REMARQUE 29. Soit A un anneau et I, J deux idéaux de A. Alors $IJ \subset I \cap J$. Si de plus I et J sont étrangers (i.e. $I + J = A$) alors $I \cap J = (I \cap J)(I + J) \subset IJ$ et donc $I \cap J = IJ$.

Si f est un quotient, on a aussi

PROPOSITION 30. *Soit A un anneau, I un idéal de A et $p : A \to A/I$ le quotient par I. Alors l'application*

$$\begin{array}{rccc} \rho : & \{\text{idéaux de } A/I\} & \to & \{\text{idéaux de } A \text{ contenant } I\} \\ & J & \mapsto & p^{-1}(J) \end{array}$$

est bijective de réciproque

$$\begin{array}{rccc} \pi : & \{\text{idéaux de } A \text{ contenant } I\} & \to & \{\text{idéaux de } A/I\} \\ & K & \mapsto & p(K) \end{array}$$

croissante pour l'inclusion, conserve les idéaux premiers et maximaux.

La conservation de la primalité repose sur l'isomorphisme, pour un idéal K de A contenant I,

$$\frac{A/I}{K/I} \equiv \frac{A}{K}.$$

De façon générale,

DÉFINITION 31. *Soit $f : A \to B$ un morphisme d'anneaux.*

- *L'image réciproque $f^{-1}J$ d'un idéal J de B est un idéal de A (appelé contraction de J par f) :*
$$J^c := f^{-1}(J).$$
- *L'extension d'un idéal I de A par f est l'idéal de B engendré par $f(I)$:*
$$I^e := f(I)B.$$

LEMME 32. *Soit $f : A \to B$ un morphisme d'anneaux. Soit I un idéal de A et J un idéal de B.*

- *$I^{ec} \supset I$ et $J^{ce} \subset J$.*
- *$I^{ece} = I^e$ et $J^{cec} = J^c$.*
- *l'ensemble des idéaux de la forme I^e pour I idéal de A est en bijection avec l'ensemble des idéaux de la forme J^c pour J idéal de B.*
- *Si P est un idéal premier de B, alors P^c est un idéal premier de A.*

La dernière propriété provient de l'injection de $A/f^{-1}(P)$ dans l'anneau intègre B/P.

EXEMPLE 33. Pour l'inclusion $\iota : \mathbb{Z} \to \mathbb{Z}[i]$, l'extension d'un idéal premier n'est en général pas premier (dans l'anneau euclidien $\mathbb{Z}[i]$). Le théorème des deux carrés donne en effet les décompositions d'idéaux

$$(2)^e = ((1+i))^2 \text{ et } (5)^e = (2+i)(2-i) \text{ et } (7)^e \text{est premier}$$

DÉFINITION 34. *Le* spectre *d'un anneau A est l'ensemble noté $\mathrm{Spec}(A)$ de ses idéaux premiers. Si $f : A \to B$ est un morphisme d'anneaux, le lemme précédent donne une application $f^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A), P \mapsto f^{-1}(P) = P^c$.*

4. Anneaux locaux

Rappelons que, puisque tout idéal propre d'un anneau est inclus dans un idéal maximal, un élément a d'un anneau A est inversible si et seulement si il n'est dans aucun idéal maximal :

$$A - A^\times = \bigcup_{M \text{ idéal maximal de } A} M.$$

PROPOSITION 35. *Soit A un anneau. Les deux propriétés suivantes sont équivalentes*

a) le complémentaire dans A du groupe $A^\times$ des inversibles de A est un idéal propre de A.
b) A possède un unique idéal maximal M.

On dit alors que (A, M) est un anneau local *et que le corps $\kappa_A := A/M$ est son corps résiduel.*

DÉMONSTRATION. Tout idéal propre de A est inclus dans $I := A - A^\times$. Si I est un idéal, alors il est l'unique idéal maximal. Réciproquement, si A possède un unique idéal maximal M, les éléments de $A - M$ ne sont dans aucun idéal maximal et sont donc inversibles. On en déduit que A est réunion disjointe de $A^\times$ et de l'idéal M. □

DÉFINITION 36. *Un morphisme d'anneaux $f : (A, M_A) \to (B, M_B)$ entre deux anneaux locaux est dit* local *si $f(M_A) \subset M_B$ (ou de façon équivalente si $f^{-1}(M_B) = M_A$). Le morphisme f induit alors un morphisme de corps $\overline{f} : \kappa_A \to \kappa_B$ entre les corps résiduels.*

EXEMPLE 37. Si k est un corps et d un entier naturel non nul, $A = k[X]/(X^d)$ est un anneau local d'idéal maximal $M_A = ([X])$ engendré par la classe $[X]$ et de corps résiduel $\kappa_A = k$. Plus généralement, si I est un idéal de $k[X_1, \cdots, X_n]$ de radical $(X_1 - a_1, \cdots, X_n - a_n)$, alors $k[X_1, \cdots, X_n]/I$ est un anneau local d'idéal maximal $([X_1 - a_1], \cdots, [X_n - a_n])$.

5. Localisation

5.1. Localisation d'anneaux.

DÉFINITION 38. *a) Une partie S d'un anneau est dite* multiplicative *si 1 appartient à S et si S est stable par multiplication.*

b) Soit A un anneau et S une partie multiplicative de A. On appelle localisé de A par rapport à S *l'anneau $S^{-1}A := A \times S/\equiv$ quotient par la relation d'équivalence*

$$(a,s) \equiv (a',s') \iff \exists r \in S / r(s'a - sa') = 0$$

muni des opérations bien définies

$$[(a,s)] + [(a',s')] = [(s'a + sa', ss')] \text{ et } [(a,s)][(a',s')] = [(aa', ss')].$$

et du morphisme d'anneaux

$$\begin{array}{rccc} \varphi : & A & \to & S^{-1}A \\ & a & \mapsto & [(a,1)] \end{array}$$

c) La classe d'équivalence $[(a,s)]$ de (a,s) sera notée a/s. En particulier, $a/s = \varphi(a)\varphi(s)^{-1}$.

LEMME 39. *Soit A un anneau et S une partie multiplicative de A. Soit $\varphi : A \to S^{-1}A$ le localisé de A par rapport à S. Alors*

a) les images par φ des éléments de S sont inversibles dans $S^{-1}A$.

b) le noyau de φ est l'ensemble des a de A annulés par multiplication un élément de S, soit $\bigcup_{s\in S}((0) : s)$.

c) l'application φ est injective si et seulement si S ne contient ni 0 ni aucun diviseur de zéro (en particulier si 0 n'est pas dans S et A est intègre).

d) le morphisme d'anneaux $\varphi : A \to S^{-1}A$ vérifie la propriété universelle : tout morphisme d'anneaux $m : A \to B$ dont l'image de S est composée d'éléments inversibles dans B se factorise de façon unique par

$$\begin{array}{ccc} A & \xrightarrow{m} & B \\ {\scriptstyle\varphi}\downarrow & \nearrow_{\overline{m}} & \\ S^{-1}A & & \end{array}$$

e) Le morphisme $\varphi : A \to S^{-1}A$ est caractérisé (à isomorphisme près) comme le seul vérifiant la propriété universelle précédente.

5.2. Localisation de modules et d'idéaux.

DÉFINITION 40. *Soit A un anneau et S une partie multiplicative de A. Soit M un A-module. On appelle* localisé de M par rapport à S *le $S^{-1}A$-module $S^{-1}M := M \times S/\equiv$ quotient par la relation d'équivalence*

$$(m,s) \equiv (m',s') \iff \exists r \in S / r(s'm - sm') = 0$$

muni des opérations bien définies

$$(m,s) + (m',s') = (s'm + sm', ss') \text{ et } (a,s)\cdot(m,s') = (am, ss')$$

et du morphisme de A-module $\varphi_M : M \to S^{-1}M, m \mapsto (m,1)$ (où $S^{-1}M$ est vu comme A-module via la localisation $A \to S^{-1}A$).

LEMME 41. *(Voir [Pes96]) Soit A un anneau et S une partie multiplicative de A. Soit M un A-module.*

a) Le $S^{-1}A$-module $S^{-1}M$ vérifie la propriété universelle suivante : pour tout $S^{-1}A$-module N et tout morphisme de A-modules $f : M \to N$ (où N est vu comme A-module via la localisation $A \to S^{-1}A$), il existe un unique morphisme de $S^{-1}A$-modules $\overline{f} : S^{-1}M \to N$ tel que le diagramme suivant commute

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\varphi}\downarrow & \nearrow_{\overline{f}} & \\ S^{-1}M & & \end{array}$$

b) (En particulier) Soit N un A-module et $f : M \to N$ un morphisme de A-modules. Alors, il existe un unique morphisme de $S^{-1}A$-module $S^{-1}f : S^{-1}M \to S^{-1}N$ tel que le diagramme suivant commute

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\varphi_M}\downarrow & & \downarrow{\scriptstyle\varphi_N} \\ S^{-1}M & \xrightarrow[S^{-1}f]{} & S^{-1}N \end{array}$$

c) Avec les notations précédentes, si f est injective $S^{-1}f$ l'est aussi et les $S^{-1}A$-modules $S^{-1}N/S^{-1}M$ et $S^{-1}(N/M)$sont isomorphes via $S^{-1}p$.

$$\begin{array}{ccccc} M & \xrightarrow{f} & N & \xrightarrow{p} & N/M \\ {\scriptstyle\varphi_M}\downarrow & & \downarrow{\scriptstyle\varphi_N} & & \downarrow{\scriptstyle\varphi_{N/M}} \\ S^{-1}M & \xrightarrow[S^{-1}f]{} & S^{-1}N & \xrightarrow[S^{-1}p]{} & S^{-1}(N/M) \end{array}$$

LEMME 42. *Soit A un anneau et S une partie multiplicative de A. Soit $\varphi : A \to S^{-1}A$ le morphisme de localisation. Soit I un idéal de A. Alors le $S^{-1}A$-module $S^{-1}I$ est un idéal isomorphe à l'idéal de $S^{-1}A$ engendré par $\varphi(I)$: $S^{-1}I = I^e$*

DÉMONSTRATION. Par le lemme précédent, $S^{-1}I$ est un sous-$S^{-1}A$-module, donc un idéal, de l'anneau $S^{-1}A$, engendré par $\varphi(I)$. □

PROPOSITION 43. *Soit A un anneau et S une partie multiplicative de A et $\varphi : A \to S^{-1}A$ la localisation de A par rapport à S. Alors*

a) Tous les idéaux de $S^{-1}A$ sont de la forme $S^{-1}I = I^e = \{i/s, i \in I, s \in S\}$ pour un idéal I de A.
b) Si I est un idéal de A, $I^e = S^{-1}A$ si et seulement si I rencontre S.
c) l'application $\alpha : P \mapsto P^e$ est une bijection croissante entre les idéaux premiers de A disjoints de S et les idéaux premiers de $S^{-1}A$. Sa bijection réciproque est $\beta : \mathcal{P} \mapsto \mathcal{P}^c$.

DÉMONSTRATION. a) Soit J un idéal de $S^{-1}A$. Notons $I := J^c$ l'idéal image réciproque. Par définition $I^e = J^{ce}$ est contenu dans J. Soit $a/s \in J$. Puisque $\varphi(a) = a/1 = s/1 \cdot a/s$ est dans J, a est dans $\varphi^{-1}J = J^c = I$ et $a/s = \varphi(a)\varphi(s)^{-1}$ est donc dans $\varphi(I)S^{-1}A = I^e$. Donc $J = I^e$. Reste à noter que $\{i/s, i \in I, s \in S\}$ est un idéal de $S^{-1}A$ (en particulier stable pas somme), qui contient $\varphi(I)$ et qui est contenu dans tout idéal contenant I.

b) Si I rencontre S, I^e est un idéal de $S^{-1}A$ qui contient un élément inversible : c'est donc $S^{-1}A$. Si I ne rencontre pas S, comme il n'existe pas de triplets $(s, r, i) \in S^2 \times I$ tel que $1/1 = i/s$ i.e $r(i - s) = 0$, $1_{S^{-1}A}$ n'est pas dans I^e.

c) Soit $\mathcal{P}$ un idéal premier de $S^{-1}A$. On a montré en a) que $\mathcal{P} = (\mathcal{P}^c)^e$ avec $\mathcal{P}^c = \varphi^{-1}\mathcal{P}$ premier disjoint de S. L'application $\alpha \circ \beta$ est donc l'identité.

Soit P un idéal premier de A disjoint de S. L'idéal P^e est strict. Soit p/s et p'/s' deux éléments de P^e tels que $p/s \times p'/s' = 0/1$. Il existe donc $\sigma \in S$ tels $\sigma pp' = 0$ dans A. Mais, comme P est premier et $\sigma \in S$ n'est pas dans P, p ou p' est dans P et donc p/s ou p'/s' est dans P^e, qui est donc premier.

Soit P un idéal premier de A disjoint de S. Alors $\beta\alpha(P) = P^{ec}$ contient P. Soit $a \in P^{ec}$. Il existe $p \in P$ et $(r, s) \in S^2$ tels que $r(sa - p) = 0$. Comme rs n'est pas dans P premier, on en déduit que a est dans P. Par conséquent, $\beta\alpha(P) = P$. □

EXEMPLE 44. a) Si A est un anneau intègre, $S := A - \{0\}$ est une partie multiplicative et $A \to S^{-1}A$ est alors le plongement de A dans son corps de fractions $\mathrm{Frac}(A)$. Tous les idéaux non réduits à $\{0\}$ rencontrent S : l'application α envoie $\{0\}$ sur $\{0\}$.

b) Si A est un anneau et P un idéal premier, $A - P$ est une partie multiplicative et on notera $(A - P)^{-1}A$ simplement par A_P. Dans ce cas, L'application α réalise une bijection entre les idéaux de A inclus dans P et les idéaux de A_P (voir proposition 43) et A_P est un anneau local, avec $P^e = \varphi(P)A_P$ comme seul idéal maximal.

c) Si A est un anneau et f un élément de A, l'ensemble S des puissances de f est une partie multiplicative de A et $S^{-1}A$ est alors simplement noté par $A_{(f)}$.

6. Décomposition des idéaux en produit d'idéaux primaires

6.1. Radical.

DÉFINITION 45.

- *Le* radical $\sqrt{I}$ *d'un idéal I est l'idéal*

$$\sqrt{I} := \{a \in A / \exists n \in \mathbb{N}, a^n \in I\}.$$

- *Un anneau est dit* réduit *si son seul élément nilpotent est nul.*
- *Un idéal I d'un anneau A est dit* radiciel *s'il est égal à son radical $\sqrt{I}$ (i.e. si A/I est réduit).*
- *Le* nilradical *d'un anneau A est le radical de l'idéal nul, c'est à dire l'idéal des éléments nilpotents de A.*

PROPOSITION 46. *a) Le nilradical d'un anneau non nul A est l'intersection de tous les idéaux premiers de A.*

b) Le radical d'un idéal I propre est l'intersection de tous les idéaux premiers de A qui contiennent I :

$$\sqrt{I} = \bigcap_{\substack{P \in \mathrm{Spec}(A) \\ P \supset I}} P$$

DÉMONSTRATION. a) Par définition de la primalité, un élément nilpotent de A est dans tous les idéaux premiers de A. Soit donc a un élément non nilpotent. L'ensemble des idéaux de A qui ne contiennent aucune puissance de a est non vide (il contient (0)) et inductif. Par le lemme de Zorn, il admet donc un élément maximal disons $\mathcal{P}$. Reste donc à montrer que $\mathcal{P}$ qui ne contient pas a est premier. Soit $x, y \in A$ tels que $x \notin \mathcal{P}$ et $y \notin \mathcal{P}$. Par maximalité de $\mathcal{P}$, les idéaux $(x, \mathcal{P})$ et $(y, \mathcal{P})$ strictement plus grands que $\mathcal{P}$ contiennent une puissance de a : il existe donc $p, q \in \mathcal{P}$, $n, m \in \mathbb{N}$ tels que $a^n = p + \alpha x$, $a^m = q + \beta y$. La puissance a^{n+m} somme d'éléments de $\mathcal{P}$ et de $\alpha\beta xy$ n'est pas dans $\mathcal{P}$: par conséquent, xy n'est pas dans $\mathcal{P}$.

b) Il suffit d'appliquer le a) dans l'anneau non nul A/I. □

6.2. Idéaux irréductibles, primaires. Dans l'anneau $A = \mathbb{Z}[\sqrt{-5}]$, l'élément 6 admet deux décompositions $6 = 2 \times 3$ et $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ qui ne se déduisent pas l'une de l'autre par multiplication par des inversibles. Mais, en étudiant $A/2A$ on obtient que le seul idéal de A contenant 2 est $(2, 1+\sqrt{-5})$ et par la suite

$$(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$

est l'unique décomposition de l'idéal (6) en produit d'idéaux premiers.

DÉFINITION 47. *a) Un idéal propre I d'un anneau est dit* irréductible *si toutes écritures $I = I_1 \cap I_2$ impliquent $I = I_1$ ou $I = I_2$.*

b) Un idéal propre I d'un anneau A est dit primaire *si pour tout couple $(a, b) \in A$, l'appartenance $ab \in I$ implique $a \in I$ ou $b \in \sqrt{I}$.*

LEMME 48. *Soit A un anneau et I un idéal de A.*

a) I est irréductible $\iff$ (0) est irréductible dans A/I.

b) I est primaire $\iff$ les diviseurs de zéro dans A/I sont nilpotents.

c) Si I est primaire, alors $\sqrt{I}$ est le plus petit idéal premier contenant I.

EXEMPLE 49. a) Si p est un nombre premier et n un entier naturel non nul, l'idéal $p^n\mathbb{Z}$ de $\mathbb{Z}$ est irréductible et primaire de radical $p\mathbb{Z}$.

b) Dans l'anneau noethérien $k[x, y]$, l'idéal $I = (x, y^2)$ est primaire mais n'est pas puissance d'un idéal premier :

$$\sqrt{I} = (x, y), \sqrt{I}^2 \subsetneq I \subsetneq \sqrt{I}.$$

c) Dans l'anneau $A = k[x, y, z]/(xy - z^2)$, l'idéal $\mathcal{P} = (\overline{x}, \overline{z})$ est premier car $A/\mathcal{P} = k[y]$ est intègre. Par contre, $\mathcal{P}^2$ n'est pas primaire. En effet, $\overline{xy} = \overline{z}^2 \in \mathcal{P}^2$, mais $\overline{x} \notin \mathcal{P}^2$ et $\overline{y} \notin r(\mathcal{P}^2) = \mathcal{P}$.

PROPOSITION 50. *Soit A un anneau et I un idéal de A. Si le radical $\sqrt{I}$ de I est maximal dans A, alors I est primaire.*

DÉMONSTRATION. Soit $ab \in I$. Si $b \notin \sqrt{I}$ maximal alors $(b, \sqrt{I}) = A$ et il existe donc $f \in A$ et $j \in \sqrt{I}$ tels que $1 = fb + j$. Donc, en élevant à une puissance N telle que $j^N \in I$, on obtient g dans A tel que $1 = gb + j^N$, puis $a = abg + aj^N$ est dans I. □

6.3. Existence de décomposition primaire.

PROPOSITION 51. *a) Tout idéal premier est irréductible.*

b) Dans un anneau noethérien, tout idéal irréductible est primaire.

DÉMONSTRATION. a) Soit I un idéal premier et $I = I_1 \cap I_2$ une décomposition de I. On a $I \subset I_1$. Supposons que $I_1 \neq I$ et considérons $a \in I_1, a \notin I$. On a $I \subset I_2$. Soit $b \in I_2$. Alors $ab \in I_1 \cap I_2 = I$ et $a \notin I$ et I premier impliquent $b \in I$, soit donc $I_2 \subset I$ et par suite $I_2 = I$. L'idéal I est donc irréductible.

b) Soit A un anneau noethérien et I un idéal irréductible de A. On travaille dans A/I. On a donc (0) irréductible. Montrons que les diviseurs de zéro sont nilpotents. Soit a un diviseur de zéro. Soit $b \neq 0$ tel que $ab = 0$. La suite

$$((0) : a) \subset ((0) : a^2) \subset \cdots ((0) : a^n) \subset \cdots$$

est une suite croissante d'idéaux. Comme A est noethérien, il existe $n \in \mathbb{N}$ tel que $((0) : a^n) = ((0) : a^{n+1})$. Montrons que $(0) = (a^n) \cap (b)$. Soit $x \in (a^n) \cap (b)$. On peut écrire $x = a^n c = bd$ avec $c, d \in A$. Alors $a^{n+1}c = abd = 0$. Donc $a^n c = x = 0$. Puisque (0) est irréductible, on déduit de l'égalité $(0) = (a^n) \cap (b)$ et de $b \neq 0$ que $a^n = 0$. Donc a est nilpotent. □

THÉORÈME 52. *(Décompositions primaires) Dans un anneau noethérien,*

a) tout idéal propre est intersection finie d'idéaux primaires.

b) tout idéal propre radiciel est intersection finie d'idéaux premiers.

DÉMONSTRATION. Soir A un anneau noethérien.

a) Par noethérianité, s'il était non-vide, l'ensemble

$$\{I, \text{ idéaux de } A, \text{ non intersection finie d'idéaux primaires}\}$$

admettrait un élément maximal disons $\mathcal{I}$. Par le théorème précédent, $\mathcal{I}$ ne serait pas irréductible : il existerait donc une écriture de $\mathcal{I}$ avec $\mathcal{I} = I_1 \cap I_2$ et $I_1 \neq \mathcal{I}$, $I_2 \neq \mathcal{I}$. Par maximalité de $\mathcal{I}$, comme I_1 et I_2 contiennent strictement $\mathcal{I}$, ils s'écriraient chacun comme intersection finie d'idéaux primaires. Mais $\mathcal{I}$ s'écrirait alors comme intersection finie d'idéaux primaires, ce qui contredirait sa définition. En conclusion, tout idéal de A est intersection finie d'idéaux primaires.

b) Comme le radical d'une intersection d'idéaux est l'intersection des radicaux, et que le radical d'un idéal primaire est premier (voir lemme 54), toute écriture de I radiciel comme intersection finie d'idéau primaires donne après passage aux radicaux une écriture de $I = \sqrt{I}$ comme intersection finie d'idéaux premiers. □

EXEMPLE 53. Dans $A = k[x, y]$, $(x^2, xy) = (x) \cap (x, y)^2$. L'idéal (x) est premier (donc primaire). L'idéal $(x, y)^2$ est puissance d'un idéal maximal, donc primaire.

6.4. Attributs communs à toutes les décompositions minimales.

LEMME 54. *Dans un anneau noethérien,*

a) si I est un idéal, il existe une puissance $\sqrt{I}^N$ du radical de I telle que

$$\sqrt{I}^N \subset I \subset \sqrt{I}.$$

b) le radical d'un idéal primaire est premier.

c) l'intersection de deux idéaux primaires de même radical est primaire de même radical.

DÉMONSTRATION. a) Si $(f_1, \cdots, f_r)$ engendre $\sqrt{I}$ et m_i est tel que $f_i^{m_i}$ appartient à I, alors par la formule du binôme, $N := \sum m_i$ convient.

b) Soit I un idéal primaire et $fg \in \sqrt{I}$. Par le point précédent, il existe N tel que $(fg)^N = f^N g^N$ soit dans I primaire. Alors, soit $f^N \in I$, soit $g^N \in \sqrt{I}$: ainsi, soit $f \in \sqrt{I}$, soit $g \in \sqrt{I}$.

c) Soit I et J deux idéaux de A, P-primaires. Alors $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = P$. Soit $fg \in I \cap J$ tel que $f \notin I \cap J$, par exemple $f \notin I$. Alors, puisque I est P-primaire g est dans $\sqrt{I} = P = \sqrt{I \cap J}$. Donc $I \cap J$ est P-primaire.

□

COROLLAIRE 55. *Dans un anneau noethérien, tout idéal propre I est intersection finie d'idéaux primaires Q_i de radicaux P_i deux à deux différents. On peut aussi imposer que pour tout i_0, $I \neq \bigcap_{i \neq i_0} Q_i$. Une telle décomposition est dite minimale.*

THÉORÈME 56. *(Unicité des radicaux dans les décompositions minimales) Soit A un anneau noethérien et I un idéal de A. Soit $I = \bigcap_{i=1}^{N} Q_i$ une décomposition primaire minimale de I. Alors les radicaux $\sqrt{Q_i}$ sont exactement les quotients $(I : x)$ de I par un élément de A qui sont premiers.*

DÉMONSTRATION. Si $x \in A$ est tel que $(I : x)$ est premier donc irréductible, alors, comme $(I : x) = \bigcap(Q_i : x)$, $(I : x)$ est l'un $(Q_k : x)$ des $(Q_i : x)$. Par conséquent, $(I : x) \supset Q_k$, et $(I : x) \supset \sqrt{Q_k} = P_k$. De plus, comme $(I : x) = (Q_k : x)$ est propre, $x \notin Q_k$. Soit $y \in (I : x) = (Q_k : x)$. Alors $yx \in Q_k$, $x \notin Q_k$ et Q_k primaire impliquent que y est dans $\sqrt{Q_k} = P_k$. Donc, $(I : x) = P_k$.

Réciproquement, soit $P_1 = \sqrt{Q_1}$. Comme la décomposition est minimale, $Q_1 \not\supset \bigcap_{i>1} Q_i$, il existe $y \in \bigcap_{i>1} Q_i$ et $y \notin Q_1$. On a $yQ_1 \subset I$ et en particulier par noethérianité, pour N assez grand $yP_1^N \subset I$. On choisit le plus petit tel n et $x \in yP_1^{n-1}$ et $x \notin I$. Notons que comme $y \in \bigcap_{i>1} Q_i$, $x \notin Q_1$. Alors, $xP_1 \subset I$ donc $P_1 \subset (I : x)$. Soit $z \in (I : x)$. Alors $xz \in I$, $xz \in Q_1$. Comme Q_1 est primaire et $x \notin Q_1$, $z \in P_1$. Donc $P_1 = (I : x)$. □

DÉFINITION 57. *Soit A un anneau noethérien et I un idéal de A.*

- *les* premiers associés à I *sont ceux qui apparaissent dans une/toutes les décompositions primaires minimales de I.*
- *on dit qu'un idéal premier P est* un idéal premier minimal de I *si P contient I mais ne contient strictement aucun idéal premier contenant I.*

LEMME 58. *Soit A un anneau noethérien et I un idéal de A. Alors les idéaux premiers minimaux de I sont tous associés à I.*

DÉMONSTRATION. Soit P un idéal premier minimal de I et $I = \bigcap Q_i$ une décomposition primaire minimale de I. L'idéal P premier contient $I = \bigcap_{i=1}^{N} Q_i$: il contient donc l'un des Q_i et même l'un des $\sqrt{Q_i} = P_i$: par minimalité, il est l'un des P_i. □

THÉORÈME 59. *(Composantes P-primaires, pour P minimal) Soit $I = \bigcap_{i=1}^{N} Q_i$ une décomposition primaire minimale de I, $P_1 = \sqrt{Q_1}$ un premier minimal de I. Alors $Q_1 = \bigcup_{s \in A - P_1} (I : s)$. La composante P_1-primaire de I ne dépend donc pas de la décomposition primaire minimale choisie.*

DÉMONSTRATION. Soit $s \in A - P_1$ et $a \in (I : s)$. Alors $as \in I$, $as \in Q_1$ primaire, $s \notin P_1 = \sqrt{Q_1}$ et donc $a \in Q_1$. Donc, $\bigcup_{s \in A - P_1} (I : s) \subset Q_1$.

Le premier P_1 ne contient aucun autre P_i par minimalité. A fortiori, P_1 ne contient aucun Q_i, $(2 \leqslant i \leqslant N)$ et donc pas non plus $\bigcap_{i=2}^{N} Q_i$ par irréductibilité de P_1. Soit $s \in \bigcap_{i=2}^{N} Q_i$ et $s \notin P_1$. Alors $Q_1 \subset (I : s)$. □

Exercices

Tous les anneaux considérés seront commutatifs et unitaires.

R-algèbres et polynômes.

EXERCICE 1. (*Polynômes*)

a) Donner l'exemple d'un anneau R et de deux polynômes P et Q de $R[X]$ tels que $\deg(PQ) < \deg P + \deg Q$.
b) Donner l'exemple d'un corps K et d'un polynôme $P \in K[X]$ non nul et tel que pour tout $r \in K$, $P(r) = 0$.
c) Soit K un corps et $f \in K[X, Y]$. On suppose qu'il existe deux parties infinies S_1 et S_2 de K telles que f s'annule pour tous les (x, y) de $S_1 \times S_2$. Montrer que f est nul.

Idéaux premiers, idéal maximaux.

EXERCICE 2. (*Élements et idéaux particuliers*)

a) Rappeler les définitions dans un anneau intègre d'irréductibilité d'un élément, d'association de deux éléments, de primalité et de maximalité d'un idéal.
b) Soit A un anneau intègre et p un élément non nul tel que (p) est premier. Montrer que p est irréductible.
c) Soit A un anneau intègre et p un élément irréductible. Montrer que (p) est maximal parmi les idéaux principaux.

EXERCICE 3. (*Opérations sur les idéaux*)

Soit R un anneau principal. Soit $I = aR$ et $J = bR$ deux idéaux de l'anneau R (avec a, b deux éléments de R. Expliciter un générateur de $I + J$, IJ, $I \cap J$, et $(I : J)$.

EXERCICE 4. (*Images réciproques d'idéaux*)

a) L'image d'un idéal par un morphisme d'anneau est-elle un idéal ? et si le morphisme est surjectif ?
b) Montrer que l'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier.
c) L'image réciproque d'un idéal maximal par un morphisme d'anneaux est-elle un idéal maximal ?

EXERCICE 5. (*Idéaux maximaux*)

a) Décrire les idéaux maximaux de $\mathbb{Z}$, de $k[X]$ (k est un corps) et d'un anneau principal A.
b) Montrer que les idéaux de la forme (p, f) où p est un nombre premier et f un polynôme unitaire irréductible modulo p sont maximaux dans $\mathbb{Z}[X]$.
c) Soit k un corps et $(a_1, a_2, \cdots, a_n) \in k^n$. Montrer à l'aide de l'application d'évaluation en $(a_1, a_2, \cdots, a_n)$ que l'idéal $(X_1 - a_1, X_2 - a_2, \cdots, X_n - a_n)$ de $k[X_1, X_2, \cdots, X_n]$ est maximal.

EXERCICE 6. (*Idéaux primaires*)

Soit k un corps.

a) L'idéal $I = (x^2, y^2)$ de $k[x, y]$ est-il premier ?
b) Montrer que si le radical $r(J)$ d'un idéal J est maximal dans un anneau A, alors J est primaire. *On pourra prendre a et b dans A tels que $ab \in J$ et $b \notin r(J)$.*
c) Calculer le radical de $I = (x^2, y^2)$ et montrer que I est un idéal primaire de $k[x, y]$.

Anneaux principaux, factoriels.

EXERCICE 7. (*Irréductibles dans un anneau factoriel*)

Soit A un anneau factoriel. Montrer qu'un élément p de A est irréductible si et seulement si l'idéal (p) est premier non nul.

EXERCICE 8. (*Exemple d'anneaux*)

Soit K un corps. On rappelle que si A est un anneau commutatif noethérien, alors $A[X]$ est aussi noethérien (Théorème de la base de Hilbert).

a) Soit I un idéal de $K[X,Y]$. Montrer que l'anneau $K[X,Y]/I$ est noethérien.
b) L'anneau $K[X,Y]/(XY)$ est-il factoriel ?
c) L'anneau $K[X,Y]/(Y^3 - X^2)$ est-il factoriel ? *On pourra montrer que* $[Y]$ *est irréductible et non premier.*
d) L'anneau $K[X,Y]/(Y - X^2)$ est-il factoriel ? *On pourra considérer le morphisme d'algèbres* $K[X,Y] \to K[T], X \mapsto T, Y \mapsto T^2$.
e) L'anneau $K[X,Y]/(XY - 1)$ est-il factoriel ?

EXERCICE 9. (*Condition de régularité*)

Soit P et Q deux polynômes de l'anneau factoriel $\mathbb{C}[X,Y]$ sans facteurs communs.

a) Montrer qu'il existe un polynôme non nul D de $\mathbb{C}[X]$ et des polynômes U, V de $\mathbb{C}[X,Y]$ tels que $D = UP + VQ$. *On pourra travailler dans l'anneau* $\mathbb{C}(X)[Y]$.
b) En déduire que l'ensemble $V(P,Q) := \{(x,y) \in \mathbb{C}^2, P(x,y) = Q(x,y) = 0\}$ est un ensemble fini.

EXERCICE 10. (*Caractérisation des anneaux principaux*)

a) Montrer qu'un anneau principal est noethérien.
b) Montrer qu'un anneau noethérien vérifie l'existence de la décomposition en produit d'irréductibles. *On pourra raisonner par l'absurde et considérer l'ensemble des idéaux* (x) *engendrés par les éléments qui n'admettent pas d'écriture en produits d'irréductibles.*
c) Soit A un anneau intègre avec l'existence de la décomposition en produit d'irréductibles. Supposons de plus que pour tout élément irréductible p, l'idéal (p) est premier. Montrer qu'il y a alors unicité dans la décomposition en produit d'irréductibles à association et ordre près. *On pourra raisonner par récurrence sur la longueur des décompositions et considérer un anneau quotient.*
d) Montrer qu'un anneau principal est factoriel et que tout idéal premier non nul et strict y est maximal.

EXERCICE 11. (*Caractérisation des anneaux principaux*)

On admet qu'un anneau intègre dont tous les idéaux premiers sont principaux est principal. Montrer qu'un anneau factoriel, dont chaque idéal premier non nul est maximal, est un anneau principal. *On pourra prendre un idéal premier* I*, un élément non nul* x *de* I *et montrer l'existence d'un facteur irréductible* p *de* x *qui engendre* I.

Anneaux intégralement clos.

EXERCICE 12. (*Anneaux intégralement clos*)

Soit A un sous-anneau d'un anneau B. On dit qu'un élément b de B est *entier* sur A s'il est solution d'une équation polynômiale unitaire à coefficients dans A. On dit qu'un anneau intègre A est *intégralement clos* si tout élément x de son corps des fractions K entier sur A est en fait dans A.

a) Montrer que tout élément non nul du corps des fractions d'un anneau factoriel A s'écrit comme quotient x/y d'éléments de A sans facteurs communs. Montrer que cette écriture est unique à association près.
b) Montrer qu'un anneau factoriel est intégralement clos.
c) Construire un morphisme d'algèbre injectif de $A := \mathbb{C}[X,Y]/(Y^3 - X^2)$ dans $\mathbb{C}[T]$. En déduire que le corps des fractions de A est isomorphe à $\mathbb{C}(T)$. En utilisant l'image de T dans le corps des fractions de A, montrer que A n'est pas intégralement clos.

Localisation.

EXERCICE 13. (*Partie multiplicative et localisation*)

On rappelle qu'une partie d'un anneau est dite *multiplicative*, si elle contient 1 et si elle est stable par multiplication.

a) Montrer que l'image et l'image réciproque d'une partie multiplicative par un morphisme d'anneaux est une partie multiplicative.
b) Montrer que si I est un idéal de l'anneau A, $1 + I$ est une partie multiplicative de A.
c) À quelle condition sur A le sous-ensemble des éléments non-nuls est-il une partie multiplicative ? Quelle est alors la localisation d'un tel anneau par rapport à la partie multiplicative des éléments non nuls ?
d) Montrer que le localisé $S^{-1}A$ de l'anneau A par rapport à la partie multiplicative S est $\{[(0_A, 1_A)]\}$ si et seulement si 0_A appartient à S.
e) Montrer que les éléments de $S^{-1}A$ s'écrivent sous la forme $\frac{a}{s} := \varphi(a)\varphi(s)^{-1}$ avec $(a,s) \in A \times S$ et l'application $\varphi : A \to S^{-1}A$, $a \mapsto [(a,1)]$.
f) Montrer que si A est intègre et S une partie multiplicative de A qui ne contient pas 0, alors $S^{-1}A$ s'injecte dans le corps des fractions de A et l'application $\varphi : A \to S^{-1}A$, $a \mapsto [(a,1)]$ de A dans le localisé $S^{-1}A$ est injective.
g) Montrer que les idéaux premiers de $S^{-1}A$ sont exactement les $S^{-1}P$, pour P idéal premier de A ne rencontrant pas S.

EXERCICE 14. (*Anneaux locaux*)

a) On rappelle que si A est un anneau et I un idéal propre, puisque l'ensemble des idéaux propres de A contenant I est inductif (i.e. toute famille totalement ordonnée admet un élément maximal), il existe par le lemme de Zorn un idéal maximal contenant I. Montrer qu'un élément de A est inversible si et seulement si il n'appartient à aucun idéal maximal.
b) Montrer que A admet un unique idéal maximal si et seulement si $A - A^\times$ est un idéal de A. (On dit alors que A est *local*. L'unique idéal maximal est alors $M = A - A^\times$.)
c) Pour quels entiers naturels n, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il local ?

EXERCICE 15. (*Localisation par rapport à un idéal premier*)

Soit A un anneau intègre.

a) Montrer que si P est un idéal premier de l'anneau A, alors $S := A - P$ est une partie multiplicative de A.
b) Montrer que les éléments de S sont inversibles dans le localisé $S^{-1}A$ et que l'image de P dans le localisé $S^{-1}A$ engendre l'unique idéal maximal M.
c) Montrer le corps résiduel $S^{-1}A/M$ est le corps des fractions de A/P.
d) Soit $u : A \to B$ un morphisme d'anneaux et Q un idéal premier de B. Montrer que $P = u^{-1}(Q)$ est un idéal premier de A et que u se prolonge de manière unique en un morphisme d'anneaux locaux $u_P : A_P \to B_Q$.

EXERCICE 16. (*Localisation par rapport à une famille de puissances*)

a) Montrer que si s est un élément non nilpotent d'un anneau A, alors l'ensemble S des puissances de s est une partie multiplicative de A qui ne contient pas 0. On notera $A_s := S^{-1}A$. Montrer alors que le morphisme de A-algèbres $A[X] \to A_s$, $P \mapsto P(1/s)$ induit un isomorphisme de $A[X]/(sX-1)$ sur A_s.
b) Décrire la localisation $\mathbb{Z}_{10}$ de $\mathbb{Z}$ par rapport à la partie multiplicative des puissances de 10 ?
c) Avec les notations de la première question, l'anneau localisé A_s est-il local ?

EXERCICE 17. (*Hérédité par localisation]*)

a) Montrer que le localisé $S^{-1}A$ d'un anneau principal A par rapport à une partie multiplicative S reste principal.
b) En déduire que $\mathbb{C}[X,Y]/(XY-1)$ est principal.
c) Montrer que le localisé $S^{-1}A$ d'un anneau factoriel par rapport à une partie multiplicative S reste factoriel. On montrera que les éléments premiers de $S^{-1}A$ sont les éléments premiers p de A tels que $(p) \cap S = \varnothing$.

EXERCICE 18. (*Localisation explicite*)

Soit n et s deux entiers naturels non nuls. On note S la partie multiplicative des puissances de la classe $[s]_n$ dans $\mathbb{Z}/n\mathbb{Z}$. Déterminer le morphisme de localisation $\varphi : \mathbb{Z}/n\mathbb{Z} \to S^{-1}(\mathbb{Z}/n\mathbb{Z})$ dans les trois situations suivantes :

a) n et s sont premiers entre eux.
b) tous les diviseurs premiers de n divisent s.
c) n et s sont deux entiers naturels non nuls quelconques. On écrit $n = ab$ où les nombres premiers qui apparaissent dans les décompositions de n et de s sont exactement ceux qui apparaissent dans celle de a avec la même multiplicité que dans celle de n.

Radicaux.

EXERCICE 19. (*Radicaux*)

Soit A un anneau et I un idéal de A.

a) Rappeler la définition du radical $\sqrt{I}$ de I.
b) Montrer que le radical $\sqrt{I}$ d'un idéal I de A est un idéal de A contenant I.
c) Donner l'exemple d'un anneau A et d'un idéal I tel que $\sqrt{I} \neq I$.
d) Montrer que si A est noethérien alors une puissance du radical de I est incluse dans I.

EXERCICE 20. (*radical*)

Soit A un anneau (commutatif, unitaire).

a) Soit $a \in A$ hors de $\sqrt{(0)}$. Montrer en utilisant le lemme de Zorn qu'il existe un idéal premier qui ne contient pas la partie multiplicative S des puissances de a.
b) Montrer que $\sqrt{(0)}$ est l'intersection de tous les idéaux premiers de A : on l'appelle le nilradical de A.

Chapitre 2

Résultants, bases de Gröbner

Dans tout ce chapitre, on fixe un corps k et un entier naturel non nul n. On travaille dans l'algèbre $k[x_1, \cdots, x_n]$.

1. Bases de Gröbner

1.1. Définitions. Il est facile de déterminer si un polynôme P de $k[x, y, z]$ est dans l'idéal engendré par les monômes $x^2y^3z^4, xy^2z^5, yz^{10}$ par exemple : il faut et il suffit que chaque monôme de P soit divisible par l'un de ces trois monômes.

Plus généralement,

LEMME 60. *Soit $\mathcal{I}$ un sous-ensemble de $\mathbb{N}^n$. Alors tout monôme de tout polynôme de l'idéal monomial de $k[x_1, \cdots, x_n]$ engendré par les monômes $x^I, I \in \mathcal{I}$ est divisible par l'un des x^I.*

DÉMONSTRATION. Il suffit de développer les sommes $\sum_{J\in\mathcal{J}} A_J(x_1, \cdots, x_n)x^J$, pour $\mathcal{J}$ sous-ensemble fini de $\mathcal{I}$, qui est la forme générale d'un élément de l'idéal engendré par les x^I. □

DÉFINITION 61. *Un ordre monomial $>$ sur $k[x_1, \cdots, x_n]$ est une relation d'ordre total sur les monômes respectée par la multiplication i.e. pour tout monôme ,*

- $\forall m, m',\ (m \neq 1) \implies mm' > m'$
- $\forall m_1, m_2,\ (m_1 > m_2) \implies (mm_1 > mm_2)$

Ayant fixé un ordre monomial $>$, le plus grand terme monomial d'un polynôme P sera appelé terme dominant et noté $\mathrm{LT}_>(P)$ ou simplement $\mathrm{LT}(P)$.

EXEMPLE 62.
- L'ordre lexicographique $x^\alpha >_{\text{lex}} x^\beta$ si la première composante non nulle de $\alpha - \beta$ est positive. $(x_1x_3 >_{\text{lex}} x_2^4)$
- L'ordre gradué lexicographique $x^\alpha >_{\text{glex}} x^\beta$ si $\deg x^\alpha > \deg x^\beta$ ou si $\deg x^\alpha = \deg x^\beta$ et si la première composante non nulle de $\alpha - \beta$ est positive. $(x_1x_3 >_{\text{glex}} x_2^2)$
- l'ordre gradué inverse lexicographique $x^\alpha >_{\text{grelex}} x^\beta$ si $\deg x^\alpha > \deg x^\beta$ ou si $\deg x^\alpha = \deg x^\beta$ et si la dernière composante non nulle de $\alpha - \beta$ est négative $(x_2^2 >_{\text{grelex}} x_1x_3)$.

PROPOSITION 63. *Soit $P \in k[x_1, \cdots, x_n]$.*

- *si $\mathrm{LT}_{lex}(P) \in k[x_i, \cdots, x_n]$, alors $P \in k[x_i, \cdots, x_n]$.*
- *si P est homogène et $\mathrm{LT}_{grelex}(P) \in (x_i, \cdots, x_n)$ alors $P \in (x_i, \cdots, x_n)$.*

LEMME 64. *(Lemme de Dickson) Tout idéal monomial de $k[x_1, \cdots, x_n]$ est engendré par un nombre fini d'éléments.*

DÉMONSTRATION. Ce lemme résulte du caractère noethérien de $k[x_1, \cdots, x_n]$, mais on en donne une démonstration élémentaire.

Si $n = 1$, considérons un idéal I monomial de $k[x]$. Par division euclidienne, si x^α est un monôme de I de degré minimal, tout x^β de I est multiple de x^α.

Si le résultat est vrai pour $k[x_1, \cdots, x_n]$, soit $J \subset k[x_1, \cdots, x_n, y]$ un idéal monomial engendré par $x^\alpha y^k$ pour (α, k) parcourant un sous-ensemble Ω de $\mathbb{N}^{n+1}$. Considérons les

idéaux monomiaux $J_k :=< x^\alpha \in k[x_1, \cdots, x_n] / x^\alpha y^k \in J >$. La suite J_m est croissante. Sa réunion est par hypothèse de récurrence engendrée par un nombre fini d'éléments. La suite est donc stationnaire, disons de limite J_N. L'idéal J est ainsi engendré par une famille finie de générateurs de $J_0, J_1 y, \cdots J_N y^N$ puisque tout monôme $x^\alpha y^k$ de J aura une écriture à l'aide de ces générateurs. □

LEMME 65. *Tout ordre monomial est un bon ordre (i.e. toute partie non vide admet un plus petit élément.)*

DÉMONSTRATION. Soit $>_m$ un ordre monomial sur $k[x_1, \cdots, x_n]$. Soit S un ensemble non vide de monômes de $k[x_1, \cdots, x_n]$. L'ordre partiel usuel sur les monômes $x^\alpha \geqslant_u x^\beta \iff \forall i,\ \alpha_i \geqslant \beta_i$ vérifie alors

$$x^\alpha \geqslant_u x^\beta \implies x^\alpha \geqslant_m x^\beta.$$

En particulier, les éléments minimaux de l'ensemble S pour l'ordre monomial, sont aussi minimaux pour l'ordre usuel. Or le lemme de Dickson permet d'affirmer, en considérant l'idéal engendré par S, que S n'a qu'un nombre fini non nul d'éléments minimaux pour l'ordre usuel. On peut donc en conclure que S admet un plus petit élément pour l'ordre monomial total : on dit que cet ordre est alors un bon ordre. □

1.2. Algorithme de division. Soit $>$ un ordre monomial sur $k[x_1, \cdots, x_n]$. Soit $f_1, \cdots f_r \in k[x_1, \cdots, x_n]$. On étudie l'appartenance d'un polynôme $g \in k[x_1, \cdots, x_n]$ à l'idéal $I := (f_1, \cdots, f_r)$. On initialise avec $g_1 := g$ et $k = 1$.

- On pose $h := g_k$ et $k := k + 1$.
- Si aucun $\mathrm{LT}(f_i)$ ne divise $\mathrm{LT}(h)$, l'algorithme s'arrête sans conclure.
- Sinon, si $\mathrm{LT}(f_j)$ divise $\mathrm{LT}(h)$, on pose $g_k := h - \frac{\mathrm{LT}(h)}{\mathrm{LT}(f_j)} f_j$. L'appartenance de h à I est équivalente à celle de g_k à I mais $\mathrm{LT}(g_k) < \mathrm{LT}(h)$.
- si $g_k = 0$, alors l'algorithme s'arrête en concluant que g, somme de polynômes de la forme $\frac{\mathrm{LT}(h)}{\mathrm{LT}(f_i)} f_i$ est dans I, avec de plus $\mathrm{LT}(\frac{\mathrm{LT}(h)}{\mathrm{LT}(f_i)} f_i) \leqslant \mathrm{LT}(g)$.
- sinon, on reprend la procédure.

Noter que même si g est dans I, l'algorithme peut s'arrêter sans conclure.

DÉFINITION 66. *Soit $>$ un ordre monomial sur $k[x_1, \cdots, x_n]$ et I un idéal de $k[x_1, \cdots, x_n]$. Une base de Gröbner de I est une famille $\{f_1, \cdots, f_r\}$ de polynôme de I telle que l'idéal $< \mathrm{LT}(f_i) >$ engendré par les termes dominants des f_i soit l'idéal $\mathrm{LT}(I)$ engendré par tous les termes dominants des éléments de I.*

PROPOSITION 67. *Soit $>$ un ordre monomial sur $k[x_1, \cdots, x_n]$ et I un idéal de $k[x_1, \cdots, x_n]$. Si $\{f_1, \cdots, f_r\}$ est base de Gröbner de I, alors pour tout $g \in k[x_1, \cdots, x_n]$, l'algorithme de division se termine en un nombre fini d'étape*

- *soit par $g_N = 0$ et donc une écriture de $g = \sum h_i f_i$ avec $\mathrm{LM}(h_i f_i) \leqslant \mathrm{LM}(g)$.*
- *soit par $\mathrm{LT}(g_N)$ n'est divisible par aucun $\mathrm{LT}(f_i)$ et donc par le lemme 60 $\mathrm{LT}(g_N)$ n'appartient pas à l'idéal $< \mathrm{LT}(f_i) >= \mathrm{LT}(I)$. Par conséquent, g_N et donc g ne sont pas dans I, puisque $g = \sum h_i f_i + g_N$.*

1.3. Forme normale.

PROPOSITION 68. *Soit $>$ un ordre monomial sur $k[x_1, \cdots, x_n]$ et I un idéal de $k[x_1, \cdots, x_n]$. Alors tout polynôme g de $k[x_1, \cdots, x_n]$ a un unique reste modulo I de la forme*

$$g \equiv \sum_{x^\alpha \notin \mathrm{LT}(I)} c_\alpha x^\alpha \pmod{I}$$

REMARQUE 69. Noter que si $\{f_1, \cdots, f_r\}$ est une base de Gröbner de I, la condition $x^\alpha \notin \mathrm{LT}(I)$ de non appartenance à l'idéal monomial $\mathrm{LT}(T) =< \mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_r) >$ se vérifie en montrant que x^α n'est multiple d'aucun $\mathrm{LT}(f_i)$. On peut alors simplement calculer la dimension de $k[x_1, \cdots, x_n]/I$ en dénombrant les points de $\mathbb{N}^n$ hors des secteurs de sommets $\mathrm{LT}(f_i)$.

DÉMONSTRATION. Unicité : si $g \equiv \sum_{x^\alpha \notin \mathrm{LT}(I)} c_\alpha x^\alpha \pmod I \equiv \sum_{x^\alpha \notin \mathrm{LT}(I)} c'_\alpha x^\alpha \pmod I$, alors $\sum_{x^\alpha \notin \mathrm{LT}(I)} (c_\alpha - c'_\alpha) x^\alpha$ est dans I. Mais aucun monôme x^α de cette somme n'est dans $\mathrm{LT}(I)$. Par conséquent, tous les $(c_\alpha - c'_\alpha)$ sont nuls et le reste est unique.

Existence : supposons que l'un des polynômes de $k[x_1, \cdots, x_n]$ n'ait pas de forme normale. Considérons l'ensemble non vide des termes dominants de tels polynômes. Choisissons un élément g sans forme normale avec un terme dominant minimal, puisque l'ordre monomial est un bon ordre.

Si $\mathrm{LT}(g) \in \mathrm{LT}(I)$, il existe $f \in I$ tel que $\mathrm{LT}(f) = \mathrm{LT}(g)$. Comme $\mathrm{LT}(g - f) < \mathrm{LT}(g)$, $g - f$ a une forme normale, mais ceci est contradictoire car $g - f \equiv g \pmod I$.

Si $\mathrm{LT}(g) \notin \mathrm{LT}(I)$, comme $\mathrm{LT}(g - \mathrm{LT}(g)) < \mathrm{LT}(g)$, $g - \mathrm{LT}(g)$ admet une forme normale $g - \mathrm{LT}(g) \equiv \sum_{x^\alpha \notin \mathrm{LT}(I)} c_\alpha x^\alpha \pmod I$. Mais alors $g = \sum_{x^\alpha \notin \mathrm{LT}(I)} c_\alpha x^\alpha + \mathrm{LT}(g)$ est une forme normale pour g. Contradiction. □

1.4. Existence de bases de Gröbner.

THÉORÈME 70. *(Existence) Tout idéal de $k[x_1, \cdots, x_n]$ admet une base de Gröbner finie.*

DÉMONSTRATION. Soit I un idéal de $k[x_1, \cdots, x_n]$ et $\mathrm{LT}(I)$ l'idéal monomial engendré par tous les termes dominants des éléments de I. Par le lemme de Dickson, $\mathrm{LT}(I)$ est engendré par un nombre fini d'éléments de $LT(I)$, disons $x^{\alpha_i}, i = 1 \cdots N$. Or il existe une écriture $x^{\alpha_i} = \sum_{j=1}^{n_i} \mathrm{LT}(f_{i,j}) P_{i,j}$ avec $f_{i,j} \in I$ et $P_{i,j} \in k[x_1, \cdots, x_n]$. On obtient

$$\mathrm{LT}(I) \supset < \mathrm{LT}(f_{i,j}) > \supset < x^{\alpha_i}, i = 1 \cdots, N >= \mathrm{LT}(I).$$

La famille $\{f_{i,j}, i = 1 \cdots N, j = 1 \cdots n_i\}$ est donc une base de Gröbner de I. □

1.5. Critère de Buchberger. On cherche un critère pour assurer qu'une famille génératrice d'un idéal en est une base de Gröbner.

DÉFINITION 71. *Soit $>$ un ordre monomial sur $k[x_1, \cdots, x_n]$ et f, g deux polynômes non nuls de $k[x_1, \cdots, x_n]$. On note*

- $\mathrm{ppcm}(\mathrm{LM}(f), \mathrm{LM}(g)) := x_1^{\max(\alpha_1, \beta_1)} \cdots x_n^{\max(\alpha_n, \beta_n)}$ *si* $\mathrm{LM}(f) = x^\alpha$ *et* $\mathrm{LM}(g) = x^\beta$.
- $S(f, g) := \frac{\mathrm{ppcm}(\mathrm{LT}(f), \mathrm{LT}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{ppcm}(\mathrm{LT}(f), \mathrm{LT}(g))}{\mathrm{LT}(g)} g$. *On note que $S(f, g)$ est dans l'idéal engendré par f et g, et que* $\mathrm{LM}(S(f, g)) < \mathrm{ppcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.

LEMME 72. *([CLO15] lemma 5, page 85) Soit $f = \sum_{i=1}^N p_i$ telle que tous les monômes dominants $\mathrm{LM}(p_i)$ sont égaux à x^δ mais $\mathrm{LM}(f) < x^\delta$. Alors f s'écrit comme combinaison linéaire de $S(p_i, p_j)$ avec $\mathrm{LM}(S(p_i, p_j)) < x^\delta$.*

DÉMONSTRATION. On écrit $\mathrm{LT}(p_i) = c_i \mathrm{LM}(p_i) = c_i x^\delta$. Par hypothèse, $\sum_{i=1}^N c_i = 0$ et $S(f_i, f_j) = \frac{f_i}{c_i} - \frac{f_j}{c_j}$ a un terme dominant strictement inférieur à x^δ. On trouve

$$\sum_{i=1}^{N-1} c_i S(p_i, p_N) = \sum_{i=1}^{N-1} p_i - (\sum_{i=1}^{N-1} c_i / c_N) f_N = f \quad \square$$

THÉORÈME 73. *(Critère de Buchberger) Soit $>$ un ordre monomial sur $k[x_1, \cdots, x_n]$, $F = \{f_1, \cdots f_N\}$ une famille finie d'éléments de $k[x_1, \cdots, x_n]$ et $I :=< F >$. Alors, F est une base de Gröbner de I si et seulement si l'algorithme de division par les f_i appliqué à chaque S-polynôme $S(f_i, f_j)$ se termine par 0.*

DÉMONSTRATION. (inspirée de [Has07]) Si F est une base de Gröbner, puisque chaque $S(f_i, f_j)$ est dans I, l'algorithme de division se termine par 0.

Réciproquement, on suppose donc que tout $S(f_i, f_j)$ s'écrit $S(f_i, f_j) = \sum a_{ijk} f_k$ avec $\mathrm{LT}(a_k f_k) \leqslant \mathrm{LT}(S(f_i, f_j))$. Si F n'est pas une base de Gröbner, il existe un élément $h = \sum_{i=1}^{N} h_i f_i$ de I dont $\mathrm{LT}(h)$ n'est pas dans $< \mathrm{LT}(f_i) >$. On peut supposer que h soit choisi tel que

- $\max(\mathrm{LT}(h_i f_i)) := x^\delta$ soit minimal
- et $m = \mathrm{card}\{i/\, \mathrm{LT}(h_i f_i) = x^\delta\}$ soit minimal.

Comme $\mathrm{LT}(h) \notin < \mathrm{LT}(f_i) >, x^\delta = \mathrm{LT}(h_i)\,\mathrm{LT}(f_i) > \mathrm{LT}(h)$. On peut supposer que $\{i/\, \mathrm{LT}(h_i f_i) = x^\delta\} = \{1, 2, \cdots m\}$ avec $m \geqslant 2$ pour assurer des simplifications et donc $\mathrm{LT}(h) < x^\delta$. On écrit

$$h = h_1 f_1 + h_2 f_2 + \sum_{i=3}^{m} h_i f_i + \sum_{i=m+1}^{N} h_i f_i.$$

Par ailleurs, $\mathrm{ppcm}(\mathrm{LT}(f_1), \mathrm{LT}(f_2)) | x^\delta = \mathrm{LT}(h_1 f_1) = \mathrm{LT}(h_2 f_2)$ et il existe donc μ tel que $x^\mu \,\mathrm{ppcm}(\mathrm{LT}(f_1), \mathrm{LT}(f_2)) = x^\delta$. Ainsi,

$$\frac{x^\delta}{\mathrm{LT}(f_1)} f_1 - \frac{x^\delta}{\mathrm{LT}(f_2)} f_2 - \sum_k x^\mu a_{12k} f_k = 0.$$

Comme $\mathrm{LT}(x^\mu a_{12k} f_k) \leqslant x^\mu\, \mathrm{LT}(S(f_1, f_2)) < x^\delta$ et $\mathrm{LT}(h_1 f_1) = x^\delta = \mathrm{LT}(\frac{x^\delta}{\mathrm{LT}(f_1)} f_1)$, l'écriture

$$h = (h_1 - \frac{x^\delta}{\mathrm{LT}(f_1)}) f_1 + (h_2 + \frac{x^\delta}{\mathrm{LT}(f_2)}) f_2 + \sum_{i=3}^{m} (h_i + x^\mu a_{12i}) f_i + \sum_{i=m+1}^{N} (h_i + x^\mu a_{12i}) f_i$$

contredit la minimalité de m. □

COROLLAIRE 74. *(Algorithme de Buchberger) Soit $>$ un ordre monomial sur $k[x_1, \cdots, x_n]$, $F = \{f_1, \cdots f_N\}$ une famille finie d'éléments de $k[x_1, \cdots, x_n]$ et $I :=< F >$. Alors, on obtient une base de Gröbner de I par application de l'algorithme suivant*

- *On initialise par $\ell := 1$, $F_\ell := F$*
- *Par l'algorithme de division, on écrit chaque S-polynôme $S(f_i, f_j)$ des éléments de F_ℓ comme*
$$S(f_i, f_j) = (\sum h_{ijk} f_k) + r_{ij}$$
avec un reste r_{ij} dont le terme dominant $\mathrm{LT}(r_{ij})$ n'est divisible par aucun $\mathrm{LT}(f_k)$.
- *Si tous les r_{ij} sont nuls, F est une base de Gröbner de I par le critère de Buchberger. On arrête l'algorithme.*
- *Sinon, on pose $F_{\ell+1} := F_\ell \cup \{r_{ij}\}$ et $\ell := \ell + 1$ et on reprend à la deuxième étape.*

DÉMONSTRATION. Notons que tous les F_ℓ engendrent I, car les r_{ij} sont dans I. Si pour un ℓ, F_ℓ n'est pas une base de Gröbner, par le critère de Buchberger, l'inclusion $< \mathrm{LT}(F_\ell) > \subset < \mathrm{LT}(F_{\ell+1}) >$ est stricte. Mais la suite $< \mathrm{LT}(F_\ell) >$ est une suite croissante d'idéaux monomiaux de $k[x_1, \cdots, x_n]$. Par le lemme de Dickson, cette suite est stationnaire, et l'algorithme aboutit donc à une base de Gröbner de I. □

2. Résultants

2.1. Définitions. Le but de ce paragraphe est de déterminer une condition sur les coefficients (a_i) et (b_j) des polynômes $A(X) = \sum_{i=0}^{m} a_i X^i$ et $B(X) = \sum_{j=0}^{n} b_j X^j$ de $k[X]$ qui assure qu'ils aient une racine commune dans une extension finie de k, autrement dit qu'ils aient un facteur irréductible commun non constant dans $k[X]$.

Soit R un anneau. On notera $R[X]_d$ l'espace vectoriel des polynômes de $R[X]$ de degré inférieur à d. On considère $A(X) \in R[X]_m$ de degré m et $B(X) \in R[X]_n$ de degré n, $d := m + n - 1$ et

$$\begin{array}{rccc} \mu_{A,B} : & R[X]_{n-1} \times R[X]_{m-1} & \to & R[X]_d \\ & (S,T) & \mapsto & AS + BT \end{array} .$$

LEMME 75. *Si R est un anneau factoriel, l'application $\mu_{A,B}$ est bijective si et seulement si A et B n'ont pas de facteur irréductible commun non constant dans $R[X]$.*

DÉMONSTRATION. Si A et B ont un facteur irréductible commun non constant F dans $R[X]$, alors il existe $A' \in R[X]_{m-1}$ et $B' \in R[X]_{n-1}$ tels que $A = FA'$ et $B = FB'$. Alors, $F\mu(B', -A') = F(AB' - BA') = 0$. Par intégrité de $R[X]$, on en déduit que $(B', -A')$ est dans le noyau de μ, et donc que μ n'est pas injective.

Si A et B n'ont pas de facteur irréductible commun non constant dans $R[X]$ et si (S,T) est dans le noyau de μ, alors $AS = -BT$. Comme A et B sont premiers entre eux, le lemme de Gauss dans $R[X]$ factoriel, implique que A divise T, avec $\deg A = m > m - 1 \geqslant \deg T$. Par intégrité de R, on en déduit que $T = 0$, puis $S = 0$. Donc, μ est injective. □

On considère $A(X) = \sum_{i=0}^{m} a_i X^i \in R[X]_m$ et $B(X) = \sum_{j=0}^{n} b_j X^j \in R[X]_n$. La matrice de μ dans les bases canoniques $\{(1,0),(X,0),\cdots(X^{n-1},0),(0,1),(0,X),\cdots,(0,X^{m-1})\}$ de $R[X]_{n-1} \times R[X]_{m-1}$ et $\{1, X, \cdots X^d\}$ de $R[X]_d$ est la matrice carrée de taille $d = m + n - 1$, dont les $n = \deg B$ premières colonnes contiennent les coefficients de A, et les $m = \deg A$ dernières les coefficients de B.

$$M(\mu_{A,B}) = \begin{pmatrix} a_0 & 0 & \cdots & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & & \vdots & b_1 & b_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 0 \\ a_{m-1} & \ddots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & b_0 \\ a_m & a_{m-1} & \ddots & \ddots & a_0 & b_{n-1} & \ddots & \ddots & b_1 \\ 0 & a_m & \ddots & \ddots & a_1 & b_n & b_{n-1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & 0 & b_n & \ddots & \vdots \\ \vdots & & \ddots & \ddots & a_{m-1} & \vdots & \ddots & \ddots & b_{n-1} \\ 0 & \cdots & \cdots & 0 & a_m & 0 & \cdots & 0 & b_n \end{pmatrix}$$

DÉFINITION 76. *Soit R un anneau. Le résultant $\mathrm{Res}(A,B)$ des polynômes $A(X) = \sum_{i=0}^{m} a_i X^i \in R[X]_m$ et $B(X) = \sum_{j=0}^{n} b_j X^j \in R[X]_n$ est le déterminant de la matrice $M(\mu)$ précédente. Par le lemme, si R est un anneau factoriel, le résultant $\mathrm{Res}(A,B)$ est nul si et seulement A et B ont un facteur irréductible non constant dans $R[X]$.*

2.2. Propriétés des résultants. La forme de la matrice $M(\mu)$ permet de calculer

- $\mathrm{Res}(B,A)(X) = (-1)^{\deg A \deg B} \mathrm{Res}(A,B)$
- $\mathrm{Res}(A,XB) = a_0 \mathrm{Res}(A,B) = A(0)\mathrm{Res}(A,B)$.
- par changement de base $\mathrm{Res}(A(X-\beta), B(X-\beta)) = \mathrm{Res}(A,B)$.

- $\mathrm{Res}(A,(X-\beta)B) = \mathrm{Res}(A(X+\beta), XB(X+\beta)) = A(\beta)\,\mathrm{Res}(A,B)$.
- et par itérations, si $A(X) = a_m \prod(X-\alpha_i)$ et $B(X) = b_n \prod(X-\beta_j)$, alors
$$\mathrm{Res}(A,B) = b_m^{\deg A} \prod A(\beta_j) = a_m^{\deg B} b_m^{\deg A} \prod_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} (\beta_j - \alpha_i)$$
- et par division euclidienne, si $A = QB + R$,
$$\begin{aligned}\mathrm{Res}(A,B) &= b_m^{\deg A} \prod A(\beta_j) = b_m^{\deg A - \deg R} b_m^{\deg R} \prod R(\beta_j)\\ &= b_m^{\deg A - \deg R}\,\mathrm{Res}(R,B)\end{aligned}$$
Même si cette formule a été obtenue dans un sur-anneau de R où B est scindé, elle est vraie dans R.

PROPOSITION 77. *Soit R un anneau. Le résultant $\mathrm{Res}(A,B)$ des polynômes $A(X) \in R[X]_m$ et $B(X) \in R[X]_n$ est dans l'image de $\mu_{A,B}$ i.e. il existe $(S,T) \in R[X]_{n-1} \times R[X]_{m-1}$ tel que $\mathrm{Res}(A,B) = AS + BT$.*

DÉMONSTRATION. On note $M^\star$ la transposée de la comatrice de $M = M(\mu_{A,B})$. Par les formules de développement de déterminant, on trouve $MM^\star = \mathrm{Res}(A,B)Id_{R[X]_d}$. Reste à appliquer cette formule sur le vecteur 1 de $R[X]_d$. On retrouve en particulier, que si A et B on une racine commune dans un sur-corps de R, alors $\mathrm{Res}(A,B)$ s'annule. □

Exercices

Plusieurs exercices de cette feuille sont inspirés du livre de Daniel Perrin (Cours d'Algèbre), du livre de Brendan Hassett (Algebraic Geometry) et du poly de Bernard Le Stum et du texte de Michel Coste "Elimination, résultant. Discriminant".

Résultants.

EXERCICE 21. (*Propriétés de base*)

Soit K un corps. Rappeler la démonstration de l'égalité $\mathrm{Res}(F,G) = a_f^{g-h}\,\mathrm{Res}(F,H)$ si F, G sont deux polynômes de $K[X]$ de degré f et g et H dans $K[X]$ vérifie $G = QF + H$ et $\deg H = h \leqslant g$. Ici a_f est le coefficient dominant de F.

EXERCICE 22. (*Sur les facteurs communs*)

Soit F et G deux polynômes de $R[X]$ tels que la matrice qui définit leur résultant soit de rang $\deg F + \deg G - 1$. Montrer que F et G ont un facteur de degré 1 commun, mais pas de facteur de degré 2.

EXERCICE 23. (*Résolution de systèmes*)

Résoudre dans $\mathbb{C}$, dans $\mathbb{F}_5$ puis dans $\mathbb{F}_3$ le système

$$\begin{cases} x^3 + 3x + 1 &= 0 \\ x^2 - 4x + 1 &= 0. \end{cases}$$

EXERCICE 24. (*Résolution de systèmes*)

a) Montrer le résultant en X de $P(X,Y) = X^2 + Y^2 + X^3 + Y^3$ et $Q(X,Y) = X^3 + Y^3 - 2XY$ vaut $\mathrm{Res}_X(P,Q) = \mathrm{Res}_X(P, -(X+Y)^2) = P(-Y,Y)^2 = 4Y^4$.

b) En déduire les solutions du système

$$\begin{cases} X^2 + Y^2 + X^3 + Y^3 &= 0 \\ X^3 + Y^3 - 2XY &= 0 \end{cases}$$

EXERCICE 25. (*Résolution de systèmes*)

a) Calculer le résultant en Y de $P(X,Y) = X^2 - XY + Y^2 - 1$ et $Q(X,Y) = 2X^2 + Y^2 - Y - 2$.

b) En déduire les solutions du système

$$\begin{cases} X^2 - XY + Y^2 &= 1 \\ 2X^2 + Y^2 - Y &= 2 \end{cases}$$

EXERCICE 26. (*Paramétrage et équation*)

Soit K un corps et $x, y \in K$. Montrer à l'aide d'un résultant que

$$(\exists t \in \overline{K} / x = t^2, y = t^5) \iff y^2 = x^5$$

EXERCICE 27. (*Folium de Descartes*)

Déterminer une équation cartésienne de l'image de la courbe paramétrée par

$$\begin{cases} x(t) &= \frac{3t}{1+t^3} \\ y(t) &= \frac{3t^2}{1+t^3} \end{cases}$$

EXERCICE 28. (*Nombres algébriques*)

Soit R un anneau intègre, $\alpha, \beta \in R$ et $F, G \in R[X]$ tels que $F(\alpha) = G(\beta) = 0$.

a) Montrer que $R(X) := \mathrm{Res}_Y(F(Y), G(X-Y))$ est un polynôme annulateur de $\alpha + \beta$.

b) En déduire un polynôme annulateur de $\sqrt{2} + \sqrt[3]{7}$.
c) Construire un polynôme annulateur du produit $\alpha\beta$.

EXERCICE 29. (*Discriminants*)

Soit K un corps. On rappelle que le discriminant d'un polynôme $P \in K[X]$ de degré d premier à la caractéristique de K et de coefficient dominant a_d est défini par l'égalité $\mathrm{Res}(P, P') = (-1)^{d(d-1)/2} a_d \,\mathrm{disc}(P)$.

a) Démontrer qu'un polynôme P a une racine multiple dans la clôture algébrique $\overline{K}$ de K (i.e. se factorise dans $\overline{K}[X]$ par $(X-\alpha)^2$ pour un $\alpha \in \overline{K}$) si et seulement si $\mathrm{disc}(P) = 0$.
b) Calculer le discriminant de $aX^2 + bX + c$.
c) Calculer le discriminant de $X^3 + pX + q$.

EXERCICE 30. (*Discriminant*)

Soit

$$P(X, Y) = Y - X(X-1)(X+1).$$

a) Calculer le discriminant $d(Y)$ de P considéré dans $\mathbb{C}(Y)[X]$.
b) Interpréter ses racines en termes géométriques pour la courbe affine d'équation $P(X, Y) = 0$.

Pour aller plus loin.

EXERCICE 31. (*Irréductibilité de l'hypersurface universelle*)

Soit k un corps. Le but de l'exercice est de montrer que l'équation de l'hypersurface universelle

$$H(X, a_0, \cdots, a_d) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0 \in k[X, a_0, \cdots, a_d]$$

est irréductible. On considère le morphisme d'algèbres

$$\begin{array}{rccc} \varphi : & k[X, a_0, \cdots, a_d] & \to & k[X, \alpha_1, \cdots, \alpha_d, a_d] \\ & X & \mapsto & X \\ & a_{d-k} & \mapsto & (-1)^k a_d \sum_{i_1 < \cdots < i_k} \alpha_{i_1} \cdots \alpha_{i_k}. \end{array}$$

qui correspond aux relations coefficients-racines, c'est à dire $\varphi(\sum_{i=1}^d a_i X^i) = a_d \prod_{i=1}^d (X - \alpha_i)$.

a) Montrer que φ conserve le degré en X.
b) Supposons que H s'écrive $H = P_1 P_2$ avec $P_i \in k[X, a_0, \cdots, a_d]$ et que $(X - \alpha_1)$ divise $\varphi(P_1)$. Montrer que $\prod_{i=1}^d (X - \alpha_i)$ divise $\varphi(P_1)$. En déduire que $\varphi(P_2)$ est constant.
c) Conclure.

Bases de Gröbner.

EXERCICE 32. (*Sur le cours*)

a) Soit K un corps. Soit $I =< x^{I(1)}, \cdots, x^{I(r)} >$ un idéal monomial de $K[x_1, \cdots, x_n]$. Soit $P = \sum c_I x^I$ un polynôme de I. Montrer que chaque x^I tel que $c_I \neq 0$ est divisible par l'un des $x^{I(j)}$.
b) Lister dans l'ordre pour les ordres lex, grlex et grinvlex les monômes en trois variables X, Y et Z (avec $X > Y > Z$) jusqu'au degré total 3 inclus.
c) La base $(x_1 - x_2^{37}, x_1 - x_2^{38})$ de l'idéal $< x_1 - x_2^{37}, x_1 - x_2^{38} >$ est-elle une base de Gröbner pour l'ordre lexicographique ?

EXERCICE 33. (*Restriction d'idéaux*)

Soit k un corps. On note $k[y,z]$ la sous algèbre de $k[x,y,z]$ engendrée par y et z.
Soit I l'idéal de $k[x,y,z]$ engendré par (x^2y, xz^2, y^2z, yz^2). Déterminer un système de générateurs de $I \cap k[y,z]$, vu comme idéal de $k[y,z]$.

EXERCICE 34. (*Base de Gröbner et appartenance*)

a) En utilisant le critère des S-polynômes, dire si la famille $(X+Z, Y-Z)$ est une base de Gröbner pour l'ordre lexicographique de l'idéal I de $K[X,Y,Z]$ qu'elle engendre.
b) Déterminer si le polynôme $X^2+Y^2+Z^2$ appartient à I.
c) Même question avec le polynôme $X^2+2XY-Y^2+2YZ$.

EXERCICE 35. (*Appartenance*)

Le polynôme $f = 2X^2Y^2 - X^2 + Y^2$ est-il dans l'idéal engendré par $f_1 = X^2Y + Y$ et $f_2 = Y^2 - 1$?

EXERCICE 36. (*Calcul de dimension*)

Soit $f = x^4 + x^2y^2 + y^3 - x^3 \in \mathbb{C}[x,y]$ et $I =< f, \partial f/\partial x, \partial f/\partial y >$. On admet que $\{x^2, y^2\}$ est une base de Gröbner réduite de I est pour l'ordre lexicographique avec $x < y$,

a) Calculer la dimension de $\mathbb{C}[x,y]/I$.
b) A-t-on $x^5 = y^5 \mod I$?

EXERCICE 37. (*Forme normale*)

a) Déterminer une base de Gröbner pour l'idéal $< x_3 - x_1^5, x_2 - x_1^3 >$ pour l'ordre lexicographique, puis pour l'ordre lexicographique gradué inverse.
b) Déterminer la forme normale de $x_1x_2x_3$ pour chacune de ces bases.

EXERCICE 38. (*Base de Gröbner et équations*)

On rappelle que si S est une base de Gröbner de $I \subset k[X_1, ..., X_n]$ pour l'ordre invlex et $m \leqslant n$, alors $S' := S \cap k[X_1, ..., X_m]$ est une base de Gröbner de $I' := I \cap k[X_1, ..., X_m]$. Le but de l'exercice est d'obtenir des équations de l'image de l'application $f : \mathbb{C} \to \mathbb{C}^3, t \mapsto (t^3, t^4, t^5)$. On admet qu'une base de Gröbner de $< x - t^3, y - t^4, z - t^5 >$ pour l'ordre lexicographique $x < y < z < t$ est $(t^3 - x, zt - x^2, yt - z, xt - y, z^2 - x^2y, yz - x^3, x * z - y^2, y^3 - x^4)$.

a) Déterminer une base de Gröbner pour l'idéal $< x - t^3, y - t^4, z - t^5 > \cap k[x,y,z]$ pour l'ordre lexicographique $x < y < z$.
b) Vérifier que I est l'idéal du graphe de f dans $\mathbb{C} \times \mathbb{C}^3$ et que $I' := I \cap \mathbb{C}[x,y,z]$ est l'idéal de l'image de f.
c) Conclure.

Chapitre 3

Les grands théorèmes

1. Extension d'anneaux

On s'inspire dans ce paragraphe du livre [Pes96].

DÉFINITION 78. *Soit $A \subset B$ une extension d'anneaux.*

- *L'extension $A \subset B$ est dite* finie *si B est un A-module de type fini.*
- *L'extension $A \subset B$ est dite* entière *si tout élément x de B est racine d'une équation polynômiale unitaire à coefficients dans A.*

PROPOSITION 79.
- *Toute extension finie $A \subset B$ d'anneaux est entière.*
- *Si $A \subset B$ est une extension entière d'anneaux intègres, alors A est un corps si et seulement si B aussi.*

DÉMONSTRATION.
- Soit $A \subset B$ une extension finie et soit donc $(b_1, \cdots, b_N)$ un système de générateurs de B comme A-module. Soit $x \in B$. Soit $M_x = (a_{ij}) \in M_N(A)$ tels que l'endomorphisme m_x de multiplication par x dans le système (b_i) s'écrive

$$m_x(b_i) = x \cdot b_i = \sum a_{ij} b_j$$

  Considérons le polynôme unitaire $\chi(X) := \det(X\,\mathrm{Id} - M_x) \in A[X]$. Par le théorème de Cayley-Hamilton, $\chi(m_x) = \chi(x)\cdot$ est l'endomorphisme nul. En particulier, $\chi(x) \cdot 1_B = \chi(x) = 0$. Donc, x est entier sur A.
- Supposons que A est un corps. Soit $b \in B$ entier sur A par hypothèse. Il existe donc une relation de la forme

$$b^n + a_{n-1}b^{n-1} + \cdots a_1 b + a_0 = 0 = b(b^{n-1} + \cdots a_1) + a_0$$

  avec $n \geqslant 1$, les $a_i \in A$ et $a_n \neq 0$, quitte à simplifier par une puissance de b dans l'anneau intègre B. On en déduit que b admet $-a_0^{-1}(b^{n-1} + \cdots a_1)$ comme inverse dans B.

  Réciproquement, si B est un corps et a un élément de A, l'inverse a' de a dans B vérifie une équation de la forme

$$(a')^n + a_{n-1}(a')^{n-1} + \cdots + a_1 a' + a_0 = 0$$

  est donc, en multipliant par a^{n-1} on obtient que a' est un inverse de a dans A. □

EXEMPLE 80. Si R est un anneau intègre et $P \in R[X]$ de coefficient dominant inversible dans R, alors par division euclidienne, on obtient que le R-module $R[X]/(P)$ est engendré par la famille finie $(X^i)_{0 \leqslant i < \deg P}$. Par conséquent, $R \subset R[X]/(P)$ est une extension d'anneaux finie donc entière.

2. Théorème de normalisation de Noether

THÉORÈME 81. *(normalisation de Noether) Soit k un corps infini. Soit A une k-algèbre de type fini engendrée par des éléments $(x_i)_{1\leqslant i\leqslant N}$. Alors, il existe $M \leqslant N$ et des éléments $(y_j)_{1\leqslant j\leqslant M}$ de A tels que*

a) y_j est une combinaison linéaire des x_i.
b) les éléments y_j sont algébriquement indépendants (i.e. l'application $k[Y_1, \cdots, Y_M] \to k[y_1, \cdots y_M] =: B$ d'évaluation en $(y_1, \cdots, y_M)$ des polynômes est un isomorphisme d'algèbres)
c) l'extension $B \subset A$ est une extension finie d'anneaux.

DÉMONSTRATION. On montrera seulement le cas particulier où l'algèbre A est de la forme $A = k[X_1, \cdots, X_n]/(f)$ pour $f \in k[X_1, \cdots, X_n]$ et $x_i = cl(X_i)$. Soit $f = F_d + \cdots F_1 + F_0$ la décomposition de f en somme de polynômes homogènes avec $F_d \neq 0$. Comme le corps k est infini, en raisonnant par récurrence sur le nombre de variables, on montre l'existence d'un n-uplet de k^n tels que $F_d(a_1, \cdots, a_n) \neq 0$. Puisque F_d est homogène, on peut même supposer $a_n = 1$. On pose $Y_i := X_i - a_i X_n$ et $Y_n := X_n$ de sorte que $X_i = Y_i + a_i Y_n$ et $X_n = Y_n$

$$F_i(X_1, \cdots, X_n) = Y_n^i F_i(a_1, \cdots, a_{n-1}, 1) + R_i(Y)$$

$$f(X_1, \cdots, X_n) = Y_n^d F_d(a_1, \cdots, a_{n-1}, 1) + R(Y) =: g(Y_1, \cdots, Y_n)$$

où $\deg_{Y_n} R_i$ et $\deg_{Y_n} R$ sont strictement plus petits que d. On en déduit, en notant $y_i := cl(Y_i) \in A$ que l'algèbre $A = k[Y_1, \cdots, Y_n]/(g)$ est finie sur $k[y_1, \cdots, y_{n-1}]$. Reste à montrer que les y_i sont algébriquement indépendants. Si pour $P \in k[Y_1, \cdots, Y_{n-1}]$, $P(y_1, \cdots, y_{n-1}) = 0$, alors $P(Y_1, \cdots Y_{n-1}) \in (g)$ ce qui compte tenu de la dépendance de g en Y_n implique $P = 0$. □

3. Théorème des zéros de Hilbert

THÉORÈME 82. *(Théorème des zéros de Hilbert) Soit $k \subset L$ une extension de corps. Si $k \subset L$ est une extension de type fini comme k-algèbre, alors $k \subset L$ est une extension finie (comme k-espace vectoriel).*

DÉMONSTRATION. Par le théorème 81, on écrit $k \subset k[a_1, \cdots, a_m] \subset L$ où $a_1, \cdots, a_m$ sont algébriquement indépendants sur k et $k[a_1, \cdots, a_m] \subset L$ est une extension finie. Puisque $k[a_1, \cdots, a_m] \subset L$ est une extension entière d'anneaux intègres et L est un corps, la proposition 79 affirme que l'algèbre $k[a_1, \cdots, a_m]$ est un corps, donc égale à k. □

COROLLAIRE 83. *Si k est un corps algébriquement clos et I un idéal de $k[X_1, \cdots X_n]$, alors*

- *les idéaux maximaux de $k[X_1, \cdots X_n]$ sont les idéaux de la forme*

$$(X_1, -a_1, \cdots X_n - a_n) = \ker ev_a : k[X_1, \cdots, X_n] \to k$$

  avec $(a_1, \cdots, a_n) \in k^n$.
- *les idéaux maximaux de $k[X_1, \cdots X_n]$ contenant I sont les idéaux de la forme $(X_1, -a_1, \cdots X_n - a_n)$ avec $(a_1, \cdots, a_n) \in k^n$ tel que pour tout $f \in I$, $f(a_1, \cdots, a_n) = 0$.*

DÉMONSTRATION. Soit M un idéal maximal de $k[X_1, \cdots X_n]$. Alors, l'extension $k \subset k[X_1, \cdots, x_n]/M$ de type fini comme k-algèbre est par le théorème 82 une extension finie de k. Puisque k est supposé algébriquement clos, c'est même un isomorphisme. Soit doit $a_i \in k$ antécédent de $[X_i] \in k[X_1, \cdots, x_n]/M$. Alors, $X_i - a_i$ est dans M et donc l'idéal maximal $(X_1 - a_1, \cdots, X_n - a_n)$ est inclus dans M, donc égal à M. □

COROLLAIRE 84. *Soit k un corps et A et B deux k-algèbres de type fini. Soit $f : A \to B$ un morphisme d'algèbres. Alors, l'image réciproque de tout idéal maximal de B est un idéal maximal de A.*

DÉMONSTRATION. Soit M un idéal maximal de B. Le morphisme $A/f^{-1}(M) \to B/M$ est une injection de l'anneau $A/f^{-1}(M)$ dans le corps B/M. Mais $k \subset B/M$ est une extension de corps avec B/M algèbre de type fini : par le théorème des zéros de Hilbert, $k \subset B/M$ et a fortiori $k \subset A/f^{-1}(M)$ sont des extensions finies d'anneaux intègres (ici même des k-espaces vectoriels de dimension finie). Par la proposition 79, $A/f^{-1}(M)$ est donc un corps, et $f^{-1}(M)$ un idéal maximal. □

4. Propriété de Jacobson

On utilise ici la présentation de [Mil]

DÉFINITION 85. *Le radical de Jacobson d'un anneau A est l'intersection de tous les idéaux maximaux de A. Le radical de Jacobson $\mathrm{Jac}(I)$ d'un idéal I d'un anneau A est l'intersection de tous les idéaux maximaux de A qui contiennent I.*

$$\mathrm{Jac}(I) := \bigcap_{\substack{M \text{ idéal maximal de } A \\ \text{contenant } I}} M.$$

LEMME 86. *Un élément a d'un anneau A est dans $\mathrm{Jac}(A)$ si et seulement si pour tout x de A, $1 - ax$ est inversible.*

DÉMONSTRATION. Si a n'est pas dans l'idéal maximal M alors $(M, a) = A$ et il existe donc $m \in M$ et $x \in A$ tels que $1 = m + ax$. Alors, $1 - ax$ qui est dans l'idéal propre M n'est pas inversible. Réciproquement, si $1 - ax$ n'est pas inversible, il est dans un idéal maximal M, et puisque 1 n'est pas dans M, a non plus. □

LEMME 87. *(Lemme de Nakayama) Soit A un anneau et $I \subset \mathrm{Jac}(A)$ un idéal de A. Soit V un A-module de type fini tel que $V = IV$. Alors $V = \{0\}$.*

DÉMONSTRATION. Si V n'est pas nul, on choisit un système de générateurs $(v_1, \cdots v_N)$ de V avec un nombre minimal d'éléments. On écrit v_1 comme $i_1 v_1 + \cdots + i_N v_N$. L'élément $(1 - i_1)v_1$, et, puisque $1 - v_1$ est inversible, l'élément v_1 sont dans le module engendré par $v_2, \cdots, v_N$. Ceci contredit la minimalité. □

COROLLAIRE 88. *Soit A un anneau local de corps résiduel $\kappa = A/M$. Soit V un A-module de type fini. Alors V/MV est naturellement un κ-espace vectoriel et $(v_1, \cdots, v_N) \in V^N$ engendre V si et seulement si $(v_1 + M, \cdots, v_N + M)$ engendre V/MV.*

DÉMONSTRATION. Si $(v_1 + M, \cdots, v_N + M)$ engendre V/MV, en notant V' le sous-module de V engendré par $(v_1, \cdots, v_N)$, comme $V' \to V \to V/MV$ est surjective, $V = V' + MV$. Par le lemme de Nakayama, $V/V' = \{0\}$ et $V = V'$. □

COROLLAIRE 89. *Soit A un anneau local noethérien de corps résiduel $\kappa = A/M$. Alors le nombre minimal de générateurs de M est au moins égal à la dimension du κ-espace vectoriel M/M^2.*

Pour les algèbres de type fini sur un corps quelconque, on peut affiner la description 46 du radical d'un idéal en termes d'idéaux premiers

PROPOSITION 90. *Soit k un corps et J un idéal propre de $k[X_1, \cdots, X_n]$. Alors, pour tout idéal propre I de $A := k[X_1, \cdots, X_n]/J$*

$$\sqrt{I} = \mathrm{Jac}(I)$$

DÉMONSTRATION. Si M est un idéal maximal de A, donc premier contenant I, alors il contient aussi $\sqrt{I}$. Réciproquement, soit $g \in A$ qui n'est pas dans le radical $\sqrt{I}$. On note S la partie multiplicative $\{g^k, k \in \mathbb{N}\}$. Comme I ne rencontre pas S, par localisation $\varphi : A \to S^{-1}A$, l'idéal $I^e = (\varphi(I))$ est un idéal propre de $S^{-1}A$. Soit donc N un idéal maximal qui le contient.

$$k \subset A/N^c \subset^{\varphi} S^{-1}A/N.$$

Si G est un antécédent de g dans $k[X_1, \cdots, X_n]$, le localisé

$$k[X_1, \cdots, X_n]_G = k[X_1, \cdots, X_n, Z]/(ZG - 1)$$

est une algèbre de type fini. De même, le localisé $S^{-1}A = k[X_1, \cdots, X_n, Z]_G/J_G$ est une algèbre de type fini. Par le corollaire 84, $N^c = \varphi^{-1}(N)$ est un idéal maximal de A contenant I mais pas g. □

Exercices

Quelques propriétés des anneaux.

EXERCICE 39. (*Idéaux particuliers*)

Soit k un corps. Justifier toutes vos réponses.

a) Donner l'exemple d'un idéal maximal de $k[X, Y]$.
b) Donner l'exemple d'un idéal premier non maximal de $k[X, Y]$.
c) Donner l'exemple d'un idéal primaire non premier de $k[X, Y]$.
d) Donner l'exemple d'un idéal radiciel non primaire de $k[X, Y]$.

EXERCICE 40. (*extensions entières d'anneaux*)

On dit qu'une extension d'anneau B d'un anneau A est une extension entière si tout élément de B est entier sur A. On dit qu'une extension d'anneau B d'un anneau A est une extension finie si B est un A module de type fini.

a) Montrer qu'une extension finie B d'un anneau A est entière. *Indication :* Pour un élément x de b, on pourra considérer le A-endomorphisme X de B de multiplication par x.
b) Montrer que si $A \subset B$ est une extension entière d'anneaux intègres, A est un corps si et seulement si B est un corps.
c) Le résultat reste-il vrai sans l'hypothèse d'intégrité ?

EXERCICE 41. (*Hypersurfaces de k^2*)

Soit k un corps. Montrer qu'aucun idéal principal de $k[X, Y]$ n'est maximal.

Indication : Si $I = (P)$ avec $\deg_Y P \geqslant 1$, $P(X, Y) = P_d(X)Y^d + \cdots P_0(X)$, on pourra commencer par le cas où $P_d(x) = 1$ puis considérer une extension finie de k où P_d admet une valeur non nulle.

Sur la normalisation.

EXERCICE 42. (*Normalisation explicite*)

Soit A l'anneau $A = \mathbb{C}[x_1, x_2, x_3, x_4, x_5]/(x_1^2 + x_2^2 + x_3^2 - 1)$. Donner une base $z_1, \cdots, z_d$ de transcendance de A sur $\mathbb{C}$ et expliciter l'extension algébrique $\mathbb{C}[z_1, \cdots z_d] \subset A$.

EXERCICE 43. (*Annulations communes*)

Soit $F \in \mathbb{C}[X, Y]$ irréductible. Montrer que si $G \in \mathbb{C}[X, Y]$ s'annule en tous les points où F s'annule alors F divise G. Ce résultat reste-t-il vrai dans $\mathbb{R}[X, Y]$?

Chapitre 4

Ensembles algébriques affines

1. Ensembles algébriques affines

1.1. Définitions.

DÉFINITION 91. *Si S est une partie de $k[X_1, \cdots, X_n]$, et E un sous-ensemble de k^n*

- *L'espace affine $\mathbb{A}^n(k)$ est l'ensemble k^n muni de l'espace des fonctions polynômiales.*
- *l'ensemble algébrique affine défini par S est le sous-ensemble*

$$V_m(S) := \{(x_1, \cdots, x_n) \in \mathbb{A}^n(k) / \forall f \in S, f(x_1, \cdots, x_n) = 0\}$$

  de l'espace affine $\mathbb{A}^n(k)$.
- *l'idéal de E est*

$$I(E) := \{f \in S, \forall p \in E, f(p) = 0\}.$$

LEMME 92. *Avec les notations précédentes*

- *Pour toute partie S de $k[X_1, \cdots, X_n]$, $V_m(S) = V_m((S))$ où (S) est l'idéal engendré par S.*
- *Pour tout idéal I de $k[X_1, \cdots, X_n]$, $V_m(I) = V_m(\sqrt{I})$.*
- *Pour toute partie E de $\mathbb{A}^n(k)$, $I(E)$ est un idéal radiciel.*
- *Pour toute partie E de $\mathbb{A}^n(k)$, $V_m(I(E)) \supset E$ avec égalité si et seulement si E est un ensemble algébrique affine.*
- *Pour tout idéal I de $k[X_1, \cdots, X_n]$, $I(V_m(I)) \supset \sqrt{I}$.*

DÉMONSTRATION. Toutes les propriétés découlent des définitions. □

1.2. Topologie de Zariski.

LEMME 93. *Soit k un corps. Alors, l'ensemble $\{V_m(I), I$ idéal de $k[X_1, \cdots, X_n]\}$ forme l'ensemble des fermés d'une topologie, qu'on appellera topologie de Zariski.*

DÉMONSTRATION. On note que $V_m(k[X_1, \cdots, X_n]) = \varnothing$, $V_m((0)) = \mathbb{A}^n(k)$. Par définition, si f et g sont deux polynômes de $k[X_1, \cdots, X_n]$, $V_m((f)) \bigcup V_m((g)) = V_m((fg))$ et $V_m((f)) \bigcap V_m((g)) = V_m((f, g))$.

Plus généralement, $\bigcup_{1 \leqslant i \leqslant N} V_m(I_i) \subset V_m(\bigcap I_i) \subset V_m(\prod I_i)$. Soit $x \in V_m(\prod I_i)$, $x \notin V_m(I_i)$ pour $2 \leqslant i \leqslant N$. Il existe donc $f_i \in I_i$ tel que $f_i(x) \neq 0$. Soit $f \in I_1$. Alors $f \prod_{i=2}^N f_i$ qui est dans $\prod I_i$ s'annule en x. Par conséquent, $f(x) = 0$ et x est dans $V_m(I_1)$. En conclusion, $\bigcup_{1 \leqslant i \leqslant N} V_m(I_i) = V_m(\bigcap I_i) = V_m(\prod I_i)$.

Enfin, une intersection quelconque $\bigcap V_m(I_i)$ se réécrit $V_m(\bigcup I_i) = V_m(\sum I_i)$. □

LEMME 94. *L'adhérence de Zariski d'une partie E de $\mathbb{A}^n(k)$ (i.e. le plus petit fermé de Zariski qui contient E) est $V_m(I(E))$.*

1.3. Ensembles algébriques irréductibles. Un espace topologique est dit irréductible s'il n'est pas réunion de deux fermés stricts.

LEMME 95. *Soit k un corps.*

- *Soit F un sous-ensemble algébrique de $\mathbb{A}^n(k)$. Alors F est irréductible si et seulement si $I(F)$ est premier.*
- *Soit I un idéal radiciel de $k[X_1, \cdots X_n]$. Si $V_m(I)$ est un espace topologique irréductible alors I est premier.*

DÉMONSTRATION. On suppose que $I = I(F)$ n'est pas premier. Soit $f, g \in k[X_1, \cdots X_n]$ hors de I mais tel que fg soit dans I. D'abord $(V_m(I) \bigcap V_m(f)) \bigcup (V_m(I) \bigcap V_m(g)) = V_m(I) \bigcap V_m(fg) = V_m(I)$. Par la propriété de Jacobson (proposition 90), comme $\sqrt{I} \neq \sqrt{(I, f)}$, l'inclusion $(V_m(I) \bigcap V_m(f)) = V_m((I, f)) \subset V_m(I)$ est stricte et de même $(V_m(I) \bigcap V_m(g)) \subsetneq V_m(I)$. Donc, $V_m(I)$ est réductible.

On suppose que F est réductible et s'écrit $F = F' \bigcup F''$ avec $F' \subsetneq F$ et $F'' \subsetneq F$. En particulier $V(I(F')) = F' \neq V(I(F))$. Il existe donc $g', g'' \in k[X_1, \cdots, X_n]$ avec $g' \in I(F')$, $g \notin I(F)$ et $g' \in I(V_m(J))$, $g' \notin I$. Mais $gg' \in I(F' \bigcup F'') = I(F)$: donc $I(F)$ n'est pas premier. □

1.4. Applications régulières entre ensemble algébriques affines.

DÉFINITION 96.

- *L'algèbre des fonctions régulières sur un sous-ensemble algébrique F de $\mathbb{A}^n(k)$ est*

$$k[X_1, \cdots, X_n] \xrightarrow{\pi_F} k[F] := \frac{k[X_1, \cdots, X_n]}{I(F)}.$$

- *L'application d'évaluation en un point $x = (x_1, \cdots, x_n$ de $F \subset \mathbb{A}^n(k)$ est*

$$\begin{array}{rccc} ev_v : & k[F] & \to & k \\ & [P] & \mapsto & P(x_1, \cdots, x_n) \end{array}$$

- *Une application régulière $\varphi : F \to G$ entre deux sous-ensembles algébriques $F \subset \mathbb{A}^n(k)$ et $G \subset \mathbb{A}^m(k)$ est la restriction à F d'une application polynômiale*

$$\begin{array}{rccc} \Phi : & \mathbb{A}^n(k) & \to & \mathbb{A}^m(k) \\ & (X_1, \cdots X_n) & \mapsto & (\Phi_1(X_1, \cdots, X_n), \cdots, \Phi_m(X_1, \cdots, X_n)) \end{array}$$

  telle que $\Phi(F) \subset G$. Elle est continue pour la topologie de Zariski.
- *L'application duale d'une application régulière $\varphi : F \to G$ est le morphisme de k-algèbres*

$$\begin{array}{rccc} \varphi^\star : & k[G] & \to & k[F] \\ & [Q] & \mapsto & [Q \circ \Phi] \end{array}$$

  Elle est bien définie et ne dépend pas du choix du relèvement Φ.

THÉORÈME 97. *(Application régulière et morphisme de k-algèbre) Soit $F \subset \mathbb{A}^n(k)$ et $G \subset \mathbb{A}^m(k)$ deux sous-ensembles algébriques. Alors, l'application*

$$\begin{array}{rccc} D : & \left\{ \begin{array}{c} \text{applications régulières} \\ \text{de } F \text{ vers } G \end{array} \right\} & \to & \left\{ \begin{array}{c} \text{morphismes de } k \text{ algèbres} \\ k[G] \to k[F] \end{array} \right\} \\ & \varphi & \mapsto & \varphi^\star \end{array}$$

est une correspondance bijective.

DÉMONSTRATION. On va définir un inverse ρ à $\varphi \mapsto \varphi^\star$. Soit $\mu : k[G] \to k[F]$ un morphisme de k-algèbres. Soit $\mu \circ \pi_G : k[Y_1, \cdots, Y_m] \xrightarrow{\pi_G} k[G] \xrightarrow{\mu} k[F]$. Notons $P_j \in k[X_1, \cdots, X_n]$ un polynôme tel que $\mu \circ \pi_G(Y_j) = \pi_F(P_j)$. Soit

$$\begin{array}{ccc} Y_j \in k[Y_1, \cdots, Y_m] & \xrightarrow{M} & k[X_1, \cdots, X_n] \ni P_j \\ {\scriptstyle \pi_G}\downarrow & & \downarrow{\scriptstyle \pi_F} \\ k[G] & \xrightarrow{\quad\mu\quad} & k[F] \end{array}$$

$$\begin{array}{rccc} \Phi : & \mathbb{A}^n(k) & \to & \mathbb{A}^m(k) \\ & (X_1, \cdots, X_n) & \mapsto & (P_1, \cdots, P_m) \end{array}$$

On vérifie alors que $\Phi^\star = M$ (i.e. $\Phi^\star(Y_j) = Y_j \circ \Phi = P_j = M(Y_j)$), que l'application polynômiale Φ envoie F dans G (i.e. $M(I(G)) \subset I(F)$) et définit donc une application régulière $\rho_\mu : F \to G$ telle que $(\rho_\mu)^\star = \mu$.

Reste à vérifier que si $\varphi : F \to G$ est une application régulière, alors $\rho_{\varphi^\star} = \varphi$. □

1.5. Pour les corps algébriquement clos.

COROLLAIRE 98. *Si k est un corps algébriquement clos et I un idéal de $k[X_1, \cdots X_n]$, alors $I(V_m(I)) = \sqrt{I}$.*

DÉMONSTRATION. L'inclusion $\sqrt{I} \subset I(V_m(I))$ résulte des définitions. Réciproquement, soit $g \in I(V_m(I))$. Puisque S est noethérien, il existe $(f_1, \cdots, f_r) \in I$ tel que $I = (f_1, \cdots, f_r)$. Alors, comme aucun élément de k^{n+1} n'annule simultanément les f_i et $Zg - 1$, et comme k est algébriquement clos, l'idéal $(f_1, \cdots, f_r, Zg - 1)$ de $k[X_1, \cdots, X_n, Z]$ n'est dans aucun idéal maximal et contient donc le polynôme 1 : il existe de polynômes $P_i, P \in k[X_1, \cdots, X_n, Z]$ tels que

$$\sum P_i(X, Z) f_i(X) + P(X, Z)(g(X)Z - 1) = 1.$$

En substituant Z par $1/g$ (i.e. par l'application $k[X_1, \cdots, X_n, Z] \to k(X_1, \cdots X_n), Z \mapsto 1/g$), on obtient une égalité dans le corps des fractions $k(X_1, \cdots X_n)$ qui multipliée par une puissance de g donne $\sum R_i(X) f_i(X) = g^N \in I$: g est donc dans le radical de I. □

LEMME 99. *Soit k un corps algébriquement clos. Soit I un idéal premier de $k[X_1, \cdots X_n]$. Alors $V_m(I)$ est irréductible.*

DÉMONSTRATION. Si k est algébriquement clos, et si $V_m(I)$ est réductible, le lemme 95 et le corollaire 98 montrent que $I(V_m(I)) = \sqrt{I} = I$ est premier. □

EXEMPLE 100. Le polynôme irréductible $x^2(x-1)^2 + y^2 + z^2$ de $\mathbb{R}[x, y, z]$ définit la variété réductible $\{(0, 0, 0), (1, 0, 0)\}$.

THÉORÈME 101. *(Ensembles algébriques et idéaux radiciels) Soit k un corps algébriquement clos. Alors, l'application V_m est une bijection décroissante, de réciproque I, entre les idéaux radiciels de $k[X_1, \cdots X_n]$ et les sous-ensembles algébriques affines de $\mathbb{A}^n(k)$. Par cette bijection, les idéaux premiers correspondent aux ensembles algébriques irréductibles et les idéaux maximaux aux points.*

2. Spectre

2.1. Définitions.

DÉFINITION 102. *Soit A un anneau et I un idéal de A.*

- *L'ensemble des idéaux premiers de l'anneau A sera noté* $\mathrm{Spec}(A)$ *et l'ensemble des idéaux maximaux de A sera noté* $\mathrm{Spec_m}(A) \subset \mathrm{Spec}(A)$.
- *Le sous-ensemble de* $\mathrm{Spec}(A)$ *des idéaux premiers de A contenant I est appelé variété de I et noté* $\mathcal{V}(I) \subset \mathrm{Spec}(A)$.
- *Le sous-ensemble de* $\mathrm{Spec}_m(A)$ *des idéaux maximaux de A contenant I est appelé variété maximale de I et noté* $\mathcal{V}_{\mathrm{m}}(I) \subset \mathrm{Spec}(A)$.

REMARQUE 103. Comme pour l'espace affine $\mathbb{A}^n(k)$, on enrichira la structure de $\mathrm{Spec}(A)$ avec une topologie et un anneau de fonctions.

LEMME 104. *Soit A un anneau. Alors $\{\mathcal{V}(I), I$ idéal de $A\}$ forme l'ensemble des fermés d'une topologie sur* $\mathrm{Spec}(A)$*, qu'on appellera* topologie de Zariski.

DÉMONSTRATION. D'abord $\mathcal{V}(A) = \varnothing$ et $\mathcal{V}((0)) = \mathrm{Spec}(A)$.

Si $(I_i)_{1\leqslant i\leqslant N}$ est une famille finie d'idéaux de A, alors la réunion des $\mathcal{V}(I_i)$ est l'ensemble des idéaux premiers de A qui contiennent l'un des I_i. En particulier $\bigcup_{1\leqslant i\leqslant N} \mathcal{V}(I_i) \subset V(\bigcap_{1\leqslant i\leqslant N} I_i)$. D'autre part, si P est un idéal premier de A qui ne contient aucun des I_i, pour tout i, il existe $a_i \in I_i$ et $a_i \notin P$. Comme P est premier, $\prod_{1\leqslant i\leqslant N} a_i$ n'est pas dans P, et $\bigcap_{1\leqslant i\leqslant N} I_i$ n'est donc pas contenu dans P. En conclusion, $\bigcup_{1\leqslant i\leqslant N} \mathcal{V}(I_i) = V(\bigcap_{1\leqslant i\leqslant N} I_i)$.

L'intersection d'une famille $\mathcal{V}(I_i)$ quelconque est l'ensemble des idéaux premiers de A qui contiennent tous les I_i : c'est donc $\mathcal{V}(\sum I_i)$. □

LEMME 105. *Si $f : A \to B$ est un morphisme d'anneaux, l'application $f^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A), P \mapsto f^{-1}(P) = P^c$ est continue pour les topologies de Zariski.*

2.2. Caractérisation des fermés à l'aide du spectre maximal.

PROPOSITION 106. *Soit A un anneau et $F = \mathcal{V}(I)$ un fermé de* $\mathrm{Spec}(A)$*. Alors*

$$F = \mathcal{V}\Big(\bigcap_{M\in\mathcal{V}_{\mathrm{m}}(I)} M\Big)$$

DÉMONSTRATION. Il s'agit simplement d'une reformulation de la propriété de Jacobson (proposition 90) de I. □

2.3. Ensemble algébrique et spectre maximal.

PROPOSITION 107. *Si k est un corps algébriquement clos et I un idéal de $k[X_1, \cdots X_n]$, alors la variété maximale $\mathcal{V}_{\mathrm{m}}(I)$ et l'ensemble algébrique affine $V_m(I)$ de I munis de leur topologie de Zariski sont homéomorphes.*

DÉMONSTRATION. Considérons l'application

$$\begin{array}{rccc} \iota : & V_m(I) & \to & \mathcal{V}_{\mathrm{m}}(I) \\ & (x_1, \cdots, x_n) & \mapsto & (X_1 - x_1, \cdots, X_n - x_n) \end{array}$$

Par le corollaire 83 du théorème des zéros de Hilbert, ι est une bijection, car si $x \in V_m(I)$ et $P \in I$ alors $P \in \ker(ev_x : k[X_1, \cdots, X_n] \to k) = (X_1 - x_1, \cdots, X_n - x_n)$. Un fermé de $\mathcal{V}_{\mathrm{m}}(I)$ est un $\mathcal{V}_{\mathrm{m}}(J) \cap \mathcal{V}_{\mathrm{m}}(I) = \mathcal{V}_{\mathrm{m}}(I + J)$. Son image réciproque par ι est alors le fermé $V_m(I + J)$ des points qui annulent les élements de I et de J. L'application ι est donc continue. De même, l'image par ι du fermé $V_m(J) \cap V_m(I)$ est $\mathcal{V}_{\mathrm{m}}(J) \cap \mathcal{V}_{\mathrm{m}}(I)$: l'application ι est donc ouverte. □

REMARQUE 108. C'est cet homéomorphisme qui explique la similitude entre les énoncé et démonstration du corollaire 90 et du corollaire 98 pour un corps algébriquement clos.

3. Anneaux de fonctions régulières

Soit A un anneau intègre noethérien. Les ouverts de $\mathrm{Spec}(A)$ sont les complémentaires des $\mathcal{V}(I) = \mathcal{V}((f_1, \cdots, f_N)) = \bigcap_{i=1}^N \mathcal{V}(f_i)$ par noethérianité de A. Ils sont donc de la forme $\bigcup_{i=1}^N D(f_i)$ où pour $f \in A - \{0\}$,

$$D(f) := \mathrm{Spec}(A) - V(f) = \{P \text{ idéal premier de } A \text{ ne contenant pas } f\}$$

On définit l'anneau des fonctions $\mathcal{O}(D(f)) := A_f \subset \mathrm{Frac}(A)$ le localisé de A le long de la partie multiplicative des multiples de f de sorte que $P \mapsto P^c$ réalise un homéomorphisme de

$$\mathrm{Spec}(A_f) \to D(f).$$

Proposition 109. *Soit A un anneau intègre. Alors,*

$$A = \bigcap_{M \in \mathrm{Spec_m}(A)} A_M \subset \mathrm{Frac}(A).$$

Démonstration. Par la propriété universelle, l'injection $A \to \mathrm{Frac}(A)$ se factorise par toutes les localisations suivant les idéaux maximaux $A \subset A_M \subset \mathrm{Frac}(A_M) = \mathrm{Frac}(A)$. Soit $x/y \in \cup A_M$. Considérons l'idéal quotient $I = ((y) : x) = \{z \in A / zx \in (y)\}$. Soit $M \in \mathrm{Spec_m}(A)$. Il existe $(a, z) \in A \times (A - M)$ tel que $zx = ay$. Donc, I n'est pas inclus dans M. Comme I n'est inclus dans aucun idéal maximal de A, $I = A$ et $x \in (y)$, soit $x/y \in A$. □

4. Composantes irréductibles

Exercices

Premières propriétés des spectres.

EXERCICE 44. (*À l'aide des idéaux maximaux*)

a) Soit A un anneau intègre. Montrer que dans $Frac(A)$, le corps des fractions de A, l'anneau A est l'intersection des localisés suivant les complémentaires des idéaux maximaux
$$A = \bigcap_{M \in \mathrm{Spec}_m(A)} A_M.$$
Indication : Pour $x \in \bigcap_{M \in \mathrm{Spec}_m(A)} A_M$, on pourra considérer le conducteur de x dans A défini par $(A : x) := \{a \in A, ax \in A\}$.

b) Soit $f \in \mathbb{C}[X_1, \cdots, X_n]$. On rappelle que $D(f) := \{M \in \mathrm{Spec}_m\, \mathbb{C}[X_1, \cdots, X_n]/f \notin M\}$ s'identifie à l'ouvert de $\mathbb{C}^n$ défini par $\{x \in \mathbb{C}^n, f(x) \neq 0\}$ et que l'anneau des fonctions régulières sur $D(f)$ est $\Gamma(D(f), \mathcal{O}_{\mathbb{A}^n}) := \bigcap_{x \in D(f)} \mathbb{C}[X_1, \cdots, X_n]_{\mathcal{M}_x}$. Montrer que
$$\Gamma(D(f), \mathcal{O}_{\mathbb{A}^n}) = \mathbb{C}[X_1, \cdots, X_n]_f.$$

c) Soit $f, g \in \mathbb{C}[X_1, \cdots, X_n]$ sans facteurs irréductibles communs. Montrer que
$$\Gamma(D(f) \cup D(g), \mathcal{O}_{\mathbb{A}^n}) = \mathbb{C}[X_1, \cdots, X_n].$$

EXERCICE 45. (*Spectre de $A \times B$*)

Le but de l'exercice est de montrer l'isomorphisme
$$\mathrm{Spec}(A \times B) = \mathrm{Spec}(A) \cup \mathrm{Spec}(A).$$

a) Soit $P \in \mathrm{Spec}(A \times B)$. Montrer que si $(0_A, 1_B) \notin P$ alors $P = \pi_2^{-1}\pi_2(P)$ où $\pi_2 : A \times B \to B$ est la projection naturelle. *Remarque : π_2 est la localisation de $A \times B$ par rapport à $\{(1,1),(0,1)\}$.*

b) En déduire que les idéaux premiers de $A \times B$ sont de la forme $P \times B$ ou $A \times Q$ où P est un idéal premier de A et Q un idéal premier de B.

c) Conclure.

Idéaux et variétés.

EXERCICE 46. (*Ensembles algébriques*)

Soit k un corps.

a) Soit E un sous-ensemble de $\mathbb{A}^n(k)$ et x un point de $\mathbb{A}^n(k) - E$. Existe-t-il un polynôme F de $k[X_1, \cdots, X_n]$ tel que $F_{|E} = 0$ et $F(x) = 1$?

b) Soit V un sous-ensemble algébrique de $\mathbb{A}^n(k)$ et x un point de $\mathbb{A}^n(k) - V$. Existe-t-il un polynôme F de $k[X_1, \cdots, X_n]$ tel que $F_{|V} = 0$ et $F(x) = 1$?

c) Soit V un sous-ensemble algébrique de $\mathbb{A}^n(k)$. L'ensemble V est-il une intersection finie (éventuellement vide) d'hypersurfaces de $\mathbb{A}^n(k)$? *Une hypersurface de $\mathbb{A}^n(k)$ est le lieu des zéros d'un polynôme non constant de $k[X_1, \cdots, X_n]$.*

EXERCICE 47. (*Idéaux annulateurs*)

a) À l'aide de division euclidienne, déterminer des générateurs l'idéal $I(S)$ de $\mathbb{C}[X, Y]$ des polynômes nuls sur $S = \{(1, 2)\} \subset \mathbb{C}^2$.

b) Déterminer des générateurs l'idéal $I(T)$ de $\mathbb{C}[X, Y]$ des polynômes nuls sur $T = \{(0, 0), (0, 1)\} \subset \mathbb{C}^2$.

EXERCICE 48. (*Variétés maximales*)

Soit I_1 et I_2 deux idéaux de $\mathbb{C}[x_1, \cdots, x_n]$. Vérifier que

$$V_m(I_1) \cup V_m(I_2) = V_m(I_1 \cap I_2) = V_m(I_1 I_2).$$

EXERCICE 49. (*Variété et idéaux*)

Soit k un corps, S un sous-ensemble de $k[X_1, \cdots, X_n]$ et E un sous-ensemble de $\mathbb{A}^n(k)$. Montrer que

a) $V_m(I(E)) \supset E$.
b) $V_m(I(V_m(S))) = V_m(S)$.
c) $I(V_m(S)) \supset S$.
d) $I(V_m(I(E))) = I(E)$.

EXERCICE 50. (*Image d'une application*)

Soit k un corps

a) Montrer que l'image de l'application

$$\begin{cases} \varphi : \mathbb{A}^1(k) & \to & \mathbb{A}^3(k) \\ t & \mapsto & (t, t^2, t^3) \end{cases}$$

est incluse dans l'ensemble $D := \{(x_1, x_2, x_3) \in k^3, x_1^2 = x_2 \text{ et } x_1 x_2 = x_3\}$.
b) Montrer que l'image de l'application φ est un sous-ensemble algébrique de $\mathbb{A}^3(k)$.

EXERCICE 51. (*Réunion de droites*)

Déterminer un système de générateurs pour l'idéal de la réunion $\ell_1 \cup \ell_2 \cup \ell_3$ des axes de coordonnées canoniques dans $\mathbb{A}^3(\mathbb{R})$. i.e. $\ell_1 := \{(x_1, x_2, x_3) \in \mathbb{R}^3, x_2 = x_3 = 0\}$.

Topologie de Zariski.

EXERCICE 52. (*Propriétés de base*)

a) Soit k un corps infini. La topologie de Zariski sur $\mathbb{A}^n(k)$ est-elle séparée ?
b) Tout ouvert de Zariski est-il une réunion finie de complémentaires d'hypersurfaces ?

EXERCICE 53. (*Comparaison avec la topologie métrique*)

a) Toute fonction continue pour la topologie métrique sur $\mathbb{C}^n$, nulle sur un sous-ensemble E de $\mathbb{C}^n$ est-elle nulle sur l'adhérence de Zariski de E ?
b) Toute fonction polynômiale sur $\mathbb{C}^n$, nulle sur un sous-ensemble E de $\mathbb{C}^n$ est-elle nulle sur l'adhérence de E pour la topologie métrique ?
c) Soit E un sous-ensemble de $\mathbb{C}^n$. Comparer pour l'inclusion E, l'adhérence $\overline{E}^{met}$ de E pour la topologie métrique et l'adhérence $\overline{E}^{Zar}$ de E pour la topologie de Zariski.

EXERCICE 54. (*Adhérence de Zariski*)

a) Déterminer à l'aide de générateurs l'idéal $I(E)$ des polynômes de $\mathbb{C}[X, Y]$ nuls sur $E = \{(x, y) \in \mathbb{C}^2, \exists n \in \mathbb{N}, (x, y) = (n^2, n^3)\}$. *Si $P(X, Y)$ est dans $I(E)$, on pourra effectuer une division euclidienne de P par le polynôme unitaire $Y^2 - X^3$ dans $k[X][Y]$.*
b) Déterminer l'adhérence de Zariski $\overline{X}$ de X.

EXERCICE 55. (*Adhérence de Zariski*)

a) Soit k un corps algébriquement clos. On a défini l'adhérence de Zariski d'un sous-ensemble E de l'espace affine $\mathbb{A}^n(k)$ comme $\overline{E}^{\text{zar}} := V_m(I(E))$, la variété maximale de l'idéal des polynômes de $k[X_1, \cdots, X_n]$ nuls sur E.

Montrer que $\overline{E}^{\text{zar}}$ est l'intersection de tous les fermés de Zariski de l'espace affine $\mathbb{A}^n(k)$ contenant E.

b) Soit A un anneau. Rappeler la définition de l'ensemble $\mathrm{Spec}(A)$ et de sa topologie de Zariski.

c) Soit A un anneau. On munit $\mathrm{Spec}(A)$ de la topologie de Zariski. Soit $\mathcal{E}$ un sous-ensemble de $\mathrm{Spec}\, A$. Montrer que l'adhérence de $\mathcal{E}$ (i.e. l'intersection de tous les fermés contenant $\mathcal{E}$) est $V(I(\mathcal{E}))$ où $I(\mathcal{E})$ est l'idéal de A donné par $I(\mathcal{E}) := \bigcap_{P\in\mathcal{E}} P$ et $V(I(\mathcal{E}))$ la variété de l'idéal $I(\mathcal{E})$.

EXERCICE 56. (*Ensembles de matrices*)

Soit n un entier supérieur à 3.

a) Le sous ensemble de $M_n(\mathbb{R})$ des matrices orthogonales est-il un fermé de Zariski de $M_n(\mathbb{R})$?

b) Le sous-ensemble de $M_n(\mathbb{C})$ des matrices inversibles est-il un ouvert de Zariski de l'espace affine $M_n(\mathbb{C})$.

c) Soit $r \leqslant R$ deux entiers naturels. Montrer que toute matrice de rang r est dans l'adhérence de Zariski du sous-ensemble de $M_n(\mathbb{C})$ des matrices de rang R.

d) Le sous-ensemble de $M_n(\mathbb{C})$ des matrices de rang $n-2$ est-il un fermé de Zariski de l'espace affine $M_n(\mathbb{C})$.

e) Si non, déterminer son adhérence de Zariski.

Retour sur le théorème de normalisation de Noether.

EXERCICE 57. (*Lemme de Nakayama*)

Soit $A \subset B$ deux anneaux. On suppose que B est une algèbre finie sur A (i.e. B est une A-algèbre de type finie). Soit I un idéal propre de A. Montrer que l'idéal IB de B engendré par I est propre dans B. *On pourra raisonner par l'absurde et écrire dans IB une famille génératrice de B sur A.*

EXERCICE 58. (*Interprétation géométrique du théorème de normalisation de Noether*)

Soit k un corps algébriquement clos. Soit $I = I \subset k[x_1, \cdots, x_n]$ un idéal premier. Soit $X = V_m(I) \subset \mathbb{A}^n(k)$. Soit $A = k[x_1, \cdots, x_n]/I = k[a_1, \cdots, a_n]$ l'anneau des fonctions de X. Ici, $a_i = [x_i]_A$ est la classe de x_i dans le quotient $A = k[x_1, \cdots, x_n]/I$. Soit $b_1, \cdots, b_m$ dans A fournis par le théorème de Noether, linéaires en les a_i, algébriquement indépendants et tels que A soit finie sur $B := k[b_1, \cdots, b_m]$.

Soit $y_1, \cdots, y_m$ linéaires dans $k[x_1, \cdots, x_n]$ des relevés de $b_1, \cdots, b_m$ et $\pi : \mathbb{A}^n \to \mathbb{A}^m$, $(x_1, \cdots, x_n) \mapsto (y_1(x), \cdots, y_m(x))$ la projection linéaire associée. Soit p sa restriction à X. Le but est de montrer que les fibres de p sont finies et non vides.

a) Montrer que p ne dépend pas du choix des relèvements y_i.

b) En considérant a_i, montrer qu'il existe N et $f_{ij} \in k[y_1, \cdots y_m]$ et $g_i \in I$ tels que

$$x_i^N + \sum_{j=0}^{N-1} f_{ij}(y) x_i^j = g_i(x).$$

c) Pour tout $y \in \mathbb{A}^m(k)$ fixé, en déduire que l'ensemble des $x \in X$ tels que $p(x) = y$ est fini.

d) Soit $y^0 \in \mathbb{A}^m(k)$ fixé. Montrer que

$$I + (y_1 - y_1^0, \cdots, y_m - y_m^0) = k[x_1, \cdots, x_n] \iff (b_1 - b_1^0, \cdots, b_m - b_m^0) = A.$$

En déduire par le Nullstellensatz et le lemme de Nakayama que la fibre $p^{-1}(y^0)$ n'est pas vide.

Étude des schémas affines.

EXERCICE 59. (*Topologie de Zariski*)

Soit A un anneau intègre. On admettra que la longueur maximale d'une suite strictement croissante d'idéaux premiers de $\mathbb{C}[X, Y]$ est 3 (à comparer avec le fait que tout idéal premier non nul de $\mathbb{C}[X]$ est maximal

a) Montrer que si M est un idéal maximal de A alors $\{M\}$ est un sous-ensemble fermé de $\mathrm{Spec}(A)$.
b) Montrer que si A est un anneau intègre le singleton $\xi := \{(0)\}$ de $\mathrm{Spec}(A)$ est dense dans $\mathrm{Spec}(A)$.
c) Soit f un polynôme irréductible de $\mathbb{C}[X, Y]$. Déterminer les singletons de $\mathrm{Spec}\,\mathbb{C}[X, Y]$ inclus dans $V((f))$ et leur adhérence.

EXERCICE 60. (*Lemme du cours*)

a) Montrer que le radical d'un idéal primaire dans un anneau est premier.
b) Montrer que si deux idéaux primaires d'un anneau ont même radical, leur intersection est primaire avec même radical

Applications polynômiales, applications rationnelles.

EXERCICE 61. (*Groupe linéaire*)

Soit k un corps.

a) L'application de multiplication $\left\{ \begin{array}{ccc} M_n(k) \times M_n(k) & \to & M_n(k) \\ (A, B) & \mapsto & AB \end{array} \right.$ est-elle une application polynômiale ?
b) Soit $\mathcal{A} := k[X_{ij}, 1 \leqslant i, j \leqslant n]$ une algèbre de polynôme en n^2 indéterminées à coefficients dans un corps k. Soit $\det := \sum_{\sigma \in \sigma_n} \epsilon(\sigma) \prod_i X_{i\sigma(i)} \in \mathcal{A}$. Soit $\mathcal{A}_{\det}$ la localisation de $\mathcal{A}$ par rapport à la partie multiplicative des puissances de $\det \in \mathcal{A}$. Montrer que $\mathcal{A}_{\det}$ est isomorphe à $\mathcal{A}[t]/(t \det -1)$.
c) L'ensemble $\{(M, t) \in M_n(k) \times k / t \det M = 1\}$ est-il un sous-ensemble algébrique de $M_n(k) \times k$. On le notera

$$GL_n(k) := \{(M, t) \in M_n(k) \times k / t \det M = 1\}.$$

d) La multiplication dans $GL_n(k)$ est-elle polynômiale ?
e) L'application $\left\{ \begin{array}{ccc} GL_n(k) & \to & GL_n(k) \\ (A, t) & \mapsto & (A^{-1}, t^{-1}) \end{array} \right.$ est-elle une application polynômiale ?

EXERCICE 62. (*Applications polynômiales*)

Soit k un corps.

a) Soit $P \in k[X]$. La projection

$$\left\{ \begin{array}{ccc} V(Y - P(X)) & \to & \mathbb{A}^1(k) \\ (x, y) & \mapsto & x \end{array} \right.$$

est-elle une application polynômiale ? Déterminer son image. Est-elle un isomorphisme ?

b) L'application

$$\begin{cases} \mathbb{A}^1(k) & \to & \mathbb{A}^2(k) \\ t & \mapsto & (t^2-1, t(t^2-1)) \end{cases}$$

est-elle polynômiale ? Déterminer son image. Est-elle un isomorphisme sur son image ?

EXERCICE 63. (*Ensembles algébriques*)

Soit $n \geqslant 2$ un entier naturel. Soit k un corps algébriquement clos et $\mathbb{A}^n(k)$ l'espace affine algébrique de dimension n sur k. Dans les deux dernières questions, on identifiera l'ensemble $M_n(k)$ des matrices carrées de taille n à coefficients dans k à l'espace affine algébrique $A^{n^2}(k)$ en associant à une matrice A le n^2-uplet (a_{ij}) de ses coefficients.

a) Rappeler sans démonstration les deux applications réciproques entre l'ensemble des fermés de Zariski de $\mathbb{A}^n(k)$ et l'ensemble des idéaux radiciels de $k[X_1, \cdots, X_n]$. Quels idéaux donnent par cette correspondance les fermés irréductibles ?
b) Le sous-ensemble D^n de $A^{n^2}(k)$ des matrices diagonales est-il un fermé de Zariski de $A^{n^2}(k)$. Est-il irréductible ?
c) Le sous-ensemble S^n de $A^{n^2}(k)$ des matrices diagonales non inversibles est-il un fermé de Zariski de $A^{n^2}(k)$. Est-il irréductible ?

EXERCICE 64. (*Applications entre schémas*)

Soit k un corps algébriquement clos, $A := k[X_1, X_2, \cdots, X_n]$ l'algèbre des polynômes en n indéterminées à coefficients dans k et I un idéal de A.

a) Rappeler la construction de l'application $F : \mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ associée à la projection d'anneaux $f : A \to A/I$.
b) Montrer que F est continue.
c) Montrer que pour tout idéal π de A, $f^{-1}(f(\pi)) = \pi + I$.
d) Montrer que l'image de F est un fermé de $\mathrm{Spec}(A)$.
e) Montrer que F est un homéomorphisme sur son image.

Chapitre 5

Courbes affines planes

1. Multiplicité d'intersection

DÉFINITION 110. *Soit k un corps. Soit p un point de $\mathbb{A}^n(k)$.*

- *Soit $Q \subset k[X_1, \cdots, X_n]$ un idéal primaire de radical maximal $M_p = \ker ev_p$. La multiplicité de la variété $\mathcal{V}(Q)$ en p est*

$$\mathrm{Mult}_p(Q) := \dim_k \frac{k[X_1, \cdots, X_n]}{Q}$$

- *Soit $I \subset k[X_1, \cdots, X_n]$ un idéal. La multiplicité de la variété $\mathcal{V}(I)$ en p est*

$$\mathrm{Mult}_p(I) := \dim_k \frac{k[X_1, \cdots, X_n]_{M_p}}{I}$$

REMARQUE 111.

- Si $Q \subset k[X_1, \cdots, X_n]$ est un idéal primaire de radical maximal M_p, par noethérianité de $k[X_1, \cdots, X_n]$, il existe N tel que $M_p^N \subset Q \subset M_p$: l'application de projection

$$\frac{k[X_1, \cdots, X_n]}{M_p^N} \to \frac{k[X_1, \cdots, X_n]}{Q}$$

  est donc surjective : on en déduit que $\mathrm{Mult}_p(Q)$ est finie (inférieure à $\dim_k \frac{k[X_1, \cdots, X_n]}{M_p^N} = \binom{n+N-1}{N-1}$).
- Soit $I = \bigcap_{i=1}^r Q_i$ une décomposition primaire minimale et $\varphi : k[X_1, \cdots, X_n] \to k[X_1, \cdots, X_n]_{M_p}$ la localisation suivant la partie multiplicative $S := k[X_1, \cdots, X_n] - M_p$. Alors $Q_i \bigcap S = \varnothing \iff Q_i \subset M_p$. Donc,

$$\frac{k[X_1, \cdots, X_n]_{M_p}}{I} = \frac{k[X_1, \cdots, X_n]_{M_p}}{\bigcap_{\sqrt{Q_i} \subset M_p} Q_i}$$

  En particulier, si M_p est un premier minimal de I, sa composante M_p primaire Q_p ne dépend par de la décomposition minimale de I (Théorème 59) et

$$\mathrm{Mult}_p(I) := \dim_k \frac{k[X_1, \cdots, X_n]}{Q_p}$$

THÉORÈME 112. *(Somme de multiplicité) Soit $I \subset k[X_1, \cdots, X_n]$ un idéal dont tous les premiers associés sont de la forme M_p.*

$$\sum_{p \in \mathcal{V}_{\mathrm{m}}(I)} \mathrm{Mult}_p(I) = \dim_k \frac{k[X_1, \cdots, X_n]}{I}.$$

DÉMONSTRATION. Noter que sous l'hypothèse, tous les premiers associés à I sont minimaux, car $M_p \subset M_{p'} \iff p = p'$. Soit $I = Q_1 \bigcap \cdots \bigcap Q_r$ une décomposition primaire minimale. Soit

$$\pi : k[X_1, \cdots, X_n] \to \oplus_{i=1}^{s} \frac{k[X_1, \cdots, X_n]}{Q_i}$$

Par construction, $\ker \pi = I$. Reste à montrer que π est surjective. Mais, comme il existe une puissance N telle que pour tout i $M_{p_i}^N = \sqrt{Q_i}^N \subset Q_i$, il suffit de le vérifier dans le cas $Q_i = M_{p_i}^N$. Mais, ayant fixé des jets d'ordre N en les points p_i, il existe un polynôme qui les réalise. □

2. Théorème de Bézout

EXEMPLE 113.

- Si $(x_i)_{1 \leqslant i \leqslant c}$ et $(y_j)_{1 \leqslant j \leqslant d}$ sont des uplets de points de $\mathbb{A}^2(k)$ deux à deux distincts et si $C = V_m(\prod_{i=1}^{c}(X - x_i))$ et $C = V_m(\prod_{j=1}^{d}(Y - y_j))$ sont deux courbes de $\mathbb{A}^2(k)$, alors $C \bigcap D$ consiste en $cd = \deg C \deg D$ points distincts de multiplicité $\dim_k \frac{k[X,Y]}{(X-x_i, Y-y_j)} = 1$.
- Si $C = V_m(F(X, Y))$ est une courbe donnée par une équation F et $D = V_m(G(X, Y))$ où $G(X, Y) = Y - g(X))$ est une courbe donnée par un paramétrage, alors les abscisses des points d'intersection sont les racines (x_i) de $F(X, g(X))$ et les points d'intersection sont donc les $(x_i, g(x_i))$: il y en a au plus $\deg F \deg G$.

THÉORÈME 114. *(Théorème de Bezout) Si C et D sont deux courbes planes sans composantes communes alors*

$$\sum \mathrm{Mult}_p(C, D) \leqslant \deg C \deg D.$$

DÉMONSTRATION. Notons $C = V_m(F)$ et $D = V_m(G)$. Alors $\sum \mathrm{Mult}_p(C, D) = \dim_k \frac{k[X,Y]}{(F,G)}$. Alors, le complexe

$$0 \xrightarrow{f_1} k[X, Y] \xrightarrow{f_2} k[X, Y] \oplus k[X, Y] \xrightarrow{f_3} k[X, Y] \xrightarrow{f_4} k[X, Y]/(F, G) \xrightarrow{f_5} 0$$

$$P \longmapsto (PG, -PF)$$

$$(P, Q) \longmapsto PF + QG$$

$$P \longmapsto P \pmod{F, G}$$

est exact $i.e.$ $\ker f_i = \mathrm{Im}\, f_{i-1}$. La suite

$0 \to k[X, Y]_{<N-f-g} \to k[X, Y]_{<N-f} \oplus k[X, Y]_{<N-g} \to k[X, Y]_{<N} \to k[X, Y]/(F, G) \to 0$

reste exacte pour N grand. Comme $\dim_k k[X, Y]_{<N} = \binom{N+1}{2}$ On obtient donc

$$\dim_k \frac{k[X, Y]}{(F, G)} = \dim_k k[X, Y]_{<N-f-g} - (\dim_k k[X, Y]_{<N-f} + \dim_k k[X, Y]_{<N-g}) + \dim_k k[X, Y]_{<N-f-g} = gf$$

□

Exercices

EXERCICE 65. (*Composantes*)

a) Soit k un corps. Soit I un idéal de $k[X,Y]$. Rappeler la définition d'un idéal premier minimal de I.

b) Dans $\mathbb{C}[X,Y]$ montrer que $I =< X^2, XY >$ admet pour décompositions primaires minimales

$$I =< X > \cap < Y, X^2 >=< X > \cap < X^2, XY, Y^2 > .$$

c) En déduire les composantes irréductibles et les composantes plongées de $\mathrm{Spec}(\mathbb{C}[X,Y]/I)$.

EXERCICE 66. (*Multiplicités d'intersection*)

Soit k un corps. Soit $F = Y$ et $G = Y^4 - X^4 - X^5$ deux polynômes de $k[X,Y]$. Calculer la multiplicité d'intersection des courbes d'équation $F = 0$ et $G = 0$ en l'origine O.

EXERCICE 67. (*Intersection de courbes algébriques*)

a) Soit $(x,y) \in \mathbb{C}^2$. Montrer que $x^3 - y^2 = 0$ si et seulement s'il existe $t \in \mathbb{C}$ tel que $x = t^2$ et $y = t^3$.

b) En déduire les points d'intersection des courbes algébriques C_1 d'équation $X^3 - Y^2 = 0$ et C_2 d'équation $2X^2 + XY^2 + 1 = 0$.

c) Déterminer les points d'intersection des courbes algébriques C_1 d'équation $X^3 - Y^2 = 0$ et C_3 d'équation $X^5 + Y^5 = 0$.

d) Existe-il un couple $(U,V) \in \mathbb{C}[X,Y]$ tel que

$$U(X,Y)(X^3 - Y^2) + V(X,Y)(2X^2 + XY^2 + 1) = 1$$

e) Existe-il un triplet $(U,V,W) \in \mathbb{C}[X,Y]$ tel que

$$U(X,Y)(X^3 - Y^2) + V(X,Y)(X^5 + Y^5) + W(X,Y)(2X^2 + XY^2 + 1) = 1$$

Bibliographie

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts Math. Cham : Springer, 4th revised ed. edition, 2015.

[Has07] Brendan Hassett. *Introduction to algebraic geometry*. Cambridge University Press, Cambridge, 2007.

[Mil] Milne. *A primer on commutative algebra*. ., .

[Pes96] Christian Peskine. *An algebraic introduction to complex projective geometry. 1*, volume 47 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. Commutative algebra.

[B] Texte de David Bourqui

[C] Texte de Gaëtan Chennevier

[LP] Texte de Joseph Le Potier

[LS] Texte de Bernard Le Stum

[M] Marie-Paule Malliavin (*Algèbre commutative*)

[P] Daniel Perrin (*Cours d'algèbre*)

Version du 17 janvier 2025