Notes de Cours : Géométrie Algébrique Computationnelle

Chenyang Zhao

18 janvier 2025

Ces notes d'étude sont basées sur les notes de cours de l'Inria, disponibles ici : CAGNotes-Nov21.pdf.

Elles sont également rédigées dans le cadre d'une pratique du français académique en mathématiques. Pour assurer un usage correct et idiomatique de la langue, l'assistance de ChatGPT a été utilisée pour la rédaction en français.

Table des matières

1 Idéaux et Variétés

1.1 Introduction aux Anneaux et Modules

1.1.1 Définitions de base

Définition 1.1. Un **anneau** est une structure algébrique $(R, +, \cdot)$ composée d'un ensemble R, avec deux opérations : l'addition $(+)$ et la multiplication $(\cdot)$. Ces opérations satisfont les propriétés suivantes :
- $(R, +)$ est un groupe abélien.
- La multiplication est associative : $(ab)c = a(bc)$ pour tous $a, b, c \in R$.
- La multiplication est distributive par rapport à l'addition : $a(b+c) = ab+ac$ pour tous $a, b, c \in R$.

Remarque 1.1. Tous les anneaux que nous considérons ici sont **commutatifs avec unité**, c'est-à-dire qu'ils vérifient $ab = ba$ pour tous $a, b \in R$ et qu'il existe un élément $1 \in R$ tel que $1 \cdot a = a$ pour tout $a \in R$.

1.1.2 Modules

Définition 1.2. Un **R-module** M (où R est un anneau) est une généralisation d'un espace vectoriel. Il s'agit d'un ensemble M avec une opération d'addition et une action scalaire (multiplication par les éléments de R), satisfaisant les axiomes suivants :
- $(M, +)$ est un groupe abélien.
- Pour tous $r_1, r_2 \in R$ et $m_1, m_2 \in M$, nous avons :
  - $r_1(m_1 + m_2) = r_1m_1 + r_1m_2$,
  - $(r_1 + r_2)m_1 = r_1m_1 + r_2m_1$,
  - $(r_1r_2)m_1 = r_1(r_2m_1)$,
  - $1 \cdot m = m$, où 1 est l'unité de R.

Remarque 1.2. Un R-module peut être vu comme une généralisation d'un espace vectoriel, mais où les scalaires proviennent d'un anneau plutôt que d'un corps.

1.1.3 Idéaux et Exemples

Définition 1.3. Un **idéal** $I \subseteq R$ est un sous-ensemble tel que :
- I est un sous-groupe additif de $(R, +)$,
- Pour tout $a \in R$ et $x \in I$, le produit $ax \in I$.

Exemples :
1. Dans l'anneau $R = \mathbb{Z}$, les idéaux sont les sous-ensembles de la forme $(n) = n\mathbb{Z}$, où $n \in \mathbb{Z}$.
2. Dans $R[x]$, l'idéal (x^2) est l'ensemble des polynômes multiples de x^2.

1.1.4 Modules Finitement Engendrés

Définition 1.4. Un module M est **finitement engendré** s'il existe un ensemble fini $\{m_1, \ldots, m_n\} \subset M$ tel que tout élément $m \in M$ peut s'écrire comme une combinaison linéaire :

$$m = r_1m_1 + \cdots + r_nm_n, \quad \text{où } r_i \in R.$$

Remarque 1.3. Tout idéal d'un anneau commutatif peut être vu comme un module finiment engendré. Par exemple, l'idéal (x^2, y^2) dans $k[x, y]$ est engendré par x^2 et y^2.

1.2 Idéaux et Variétés

Définition 1.5 (Variété affine)**.** Une **variété affine** est le lieu des zéros d'un ensemble de polynômes dans un espace affine. Plus précisément, pour un idéal $I \subset k[x_1, \ldots, x_n]$, la variété affine associée est définie comme :

$$V(I) = \{a = (a_1, \ldots, a_n) \in \mathbb{A}_k^n \mid f(a) = 0 \text{ pour tout } f \in I\}.$$

Remarque 1.4. La variété $V(I)$ ne dépend que de l'idéal I, pas de ses générateurs spécifiques. Géométriquement, $V(I)$ est le lieu où tous les polynômes de I s'annulent.

Définition 1.6 (Idéal d'un ensemble)**.** Pour un sous-ensemble $S \subseteq \mathbb{A}_k^n$, l'**idéal de** S est défini comme :

$$I(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ pour tout } a \in S\}.$$

Théorème 1.1 (Correspondance entre algèbre et géométrie)**.** Pour un idéal $I \subseteq k[x_1, \ldots, x_n]$, on a toujours :

$$I \subseteq I(V(I)).$$

Cependant, $I(V(I))$ peut être plus grand que I si I n'est pas un idéal radical. En particulier :

$$\sqrt{I} = I(V(I)),$$

où $\sqrt{I}$ est l'idéal radical associé à I.

Exemple 1.1 (Idéal radical et non radical)**.** Soit $I = (x^2)$ dans $k[x]$. Alors :

$$V(I) = \{(0)\}, \quad I(V(I)) = (x).$$

On remarque que :

$$I \subsetneq I(V(I)),$$

car $x^2 \in I$ mais $x \notin I$. Cependant, $\sqrt{I} = (x)$, qui est radical.

Définition 1.7 (Variété irréductible)**.** Une variété V est dite **irréductible** si elle ne peut pas être exprimée comme l'union de deux sous-variétés propres :

$$V \neq V_1 \cup V_2 \quad \text{où } V_1, V_2 \subsetneq V.$$

Théorème 1.2 (Irréductibilité et idéaux premiers)**.** Une variété affine $V(I)$ est irréductible si et seulement si l'idéal I est **premier**.

Remarque 1.5. L'irréductibilité géométrique d'une variété (elle ne peut pas être décomposée en deux sous-variétés propres) correspond à la propriété algébrique d'un idéal premier.

Exemple 1.2 (Décomposition en variétés irréductibles)**.** Soit $I = (xy)$ dans $k[x, y]$. Alors :

$$V(I) = V(x) \cup V(y),$$

où $V(x) = \{(x, y) \mid x = 0\}$ et $V(y) = \{(x, y) \mid y = 0\}$. Ici, $V(x)$ et $V(y)$ sont irréductibles, mais I n'est pas premier car $xy \in I$ alors que $x, y \notin I$.

Théorème 1.3 (Opérations sur les idéaux)**.** Pour deux idéaux $I, J \subseteq k[x_1, \ldots, x_n]$, les relations suivantes relient les opérations algébriques aux opérations géométriques :

$$V(I + J) = V(I) \cap V(J),$$
$$V(I \cap J) = V(I) \cup V(J).$$

Exemple 1.3 (Intersection et union)**.** Soit $I = (x)$ et $J = (y)$ dans $k[x, y]$. Alors :

$$V(I) = \{(x, y) \mid x = 0\}, \quad V(J) = \{(x, y) \mid y = 0\}.$$

L'intersection $V(I + J) = V(x, y)$ est le point $(0, 0)$, et la réunion $V(I \cap J) = V(xy)$ est l'union des axes $x = 0$ et $y = 0$.

1.3 Théorème de la Base de Hilbert

Théorème 1.4 (Théorème de la Base de Hilbert)**.** Si un anneau R est noethérien, alors l'anneau des polynômes $R[x]$ est également noethérien.

Définition 1.8 (Anneau noethérien)**.** Un anneau R est dit **noethérien** si toute chaîne croissante d'idéaux dans R se stabilise, c'est-à-dire :

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \implies \exists n \text{ tel que } I_n = I_{n+1} = \ldots$$

De manière équivalente, tout idéal dans R est **finitement engendré**.

Idée de la démonstration du Théorème de la Base de Hilbert. L'idée principale est la suivante :

1. Soit $I \subseteq R[x]$ un idéal. On veut montrer que I est engendré par un nombre fini de polynômes.
2. On considère les degrés des polynômes dans I. Pour chaque degré d, on peut associer les coefficients des termes de degré d à un idéal dans R.
3. Étant donné que R est noethérien, ces idéaux dans R sont finiment engendrés.
4. En combinant ces résultats, on montre qu'il existe un ensemble fini de polynômes dans I qui engendre l'ensemble entier de I.

□

Exemple 1.4 (Exemple d'application)**.** Considérons $R = k[x_1, \ldots, x_n]$, l'anneau des polynômes en n variables à coefficients dans un corps k. Par le Théorème de la Base de Hilbert, cet anneau est noethérien, ce qui signifie que :

— Tout idéal dans R est engendré par un nombre fini de polynômes.

— Cela rend les calculs algébriques, comme les bases de Gröbner ou les éliminations, algorithmiquement faisables.

Remarque 1.6. Le Théorème de la Base de Hilbert a des implications profondes en géométrie algébrique :

— Il garantit que chaque variété affine peut être définie par un nombre fini d'équations polynomiales.

— Cela constitue la base pour travailler avec des algorithmes effectifs en géométrie algébrique computationnelle.

Définition 1.9 (Anneau des polynômes noethérien)**.** En appliquant le Théorème de la Base de Hilbert de manière itérative, on montre que :

$$R[x_1, \ldots, x_n] \text{ est noethérien si } R \text{ est noethérien.}$$

Ainsi, les anneaux des polynômes sur un corps (ou sur un anneau noethérien) sont toujours noethériens.

1.4 Décomposition Primaire

Définition 1.10 (Idéal primaire)**.** Un idéal $I \subseteq R$ est dit **primaire** si :

$$fg \in I \implies f \in I \text{ ou } g^m \in I \text{ pour un certain } m \in \mathbb{N}.$$

Remarque 1.7. Un idéal primaire est une généralisation d'un idéal premier. Si I est premier, alors la condition $fg \in I \implies f \in I$ ou $g \in I$ est stricte (sans puissance g^m).

Théorème 1.5 (Décomposition Primaire)**.** Dans un anneau noethérien R, tout idéal I peut être écrit comme une **intersection finie d'idéaux primaires** :

$$I = q_1 \cap q_2 \cap \cdots \cap q_s,$$

où chaque q_i est primaire.

Définition 1.11 (Radical d'un idéal)**.** Le **radical** d'un idéal I, noté $\sqrt{I}$, est défini par :

$$\sqrt{I} = \{f \in R \mid f^m \in I \text{ pour un certain } m \in \mathbb{N}\}.$$

Un idéal I est dit **radical** si $I = \sqrt{I}$.

Remarque 1.8. Pour chaque idéal primaire q_i, son radical $\sqrt{q_i}$ est un idéal **premier**. En termes géométriques, cela correspond à dire que les idéaux primaires q_i définissent des sous-variétés qui sont irréductibles.

Exemple 1.5 (Décomposition Primaire)**.** Soit $I = (x^2, xy) \subset k[x, y]$. On peut écrire I comme une intersection :

$$I = (x) \cap (x^2, y).$$

Ici :

— $q_1 = (x)$ est un idéal premier (et donc primaire) ;
— $q_2 = (x^2, y)$ est primaire, avec $\sqrt{q_2} = (x)$.

Théorème 1.6 (Décomposition Primaire Minimale)**.** Une **décomposition primaire minimale** de I est une décomposition où :
— Les radicaux $\sqrt{q_1}, \sqrt{q_2}, \ldots, \sqrt{q_s}$ sont distincts ;
— Aucune composante q_i n'est superflue (on ne peut pas supprimer q_i sans modifier I).

Définition 1.12 (Idéaux associés)**.** Les **idéaux associés** de I sont les radicaux des idéaux primaires dans une décomposition primaire minimale de I. Les idéaux associés se divisent en deux types :
— Les **idéaux premiers minimaux**, qui sont inclus dans I ;
— Les **idéaux premiers imbriqués** (embedded primes), qui ne sont pas minimaux mais apparaissent dans la décomposition.

Exemple 1.6 (Décomposition Primaire et Idéaux Associés)**.** Soit $I = (x^2, xy, y^2) \subset k[x, y]$. On a :

$$I = (x, y) \cap (x^2, y).$$

Ici :
— (x, y) est un idéal premier minimal ;
— (x^2, y) est un idéal primaire, avec un idéal associé (x), qui est imbriqué.

Remarque 1.9. La décomposition primaire est importante en géométrie algébrique car elle permet de décomposer une variété en ses composantes irréductibles :

$$V(I) = V(q_1) \cup V(q_2) \cup \cdots \cup V(q_s),$$

où $V(q_i)$ sont les sous-variétés irréductibles définies par les idéaux q_i.

1.5 Le Nullstellensatz et la Topologie de Zariski

1.5.1 Topologie de Zariski

Définition 1.13 (Topologie de Zariski)**.** La **topologie de Zariski** sur l'espace affine $\mathbb{A}_k^n$ est définie en prenant comme ensembles fermés les variétés affines, c'est-à-dire les ensembles de la forme :

$$V(I) = \{a \in \mathbb{A}_k^n \mid f(a) = 0 \text{ pour tout } f \in I\},$$

où $I \subseteq k[x_1, \ldots, x_n]$ est un idéal.

Remarque 1.10. Dans la topologie de Zariski :
— L'ensemble vide $\emptyset$ et l'espace entier $\mathbb{A}_k^n$ sont fermés.
— Les intersections finies de fermés sont fermées.
— Les unions arbitraires de fermés sont fermées.
Cela en fait une **topologie**.

Définition 1.14 (Fermés distingués)**.** Pour un polynôme $f \in k[x_1, \ldots, x_n]$, l'ensemble **ouvert distingué** associé est défini comme :

$$D(f) = \mathbb{A}_k^n \setminus V(f),$$

c'est-à-dire l'ensemble des points où f ne s'annule pas.

Exemple 1.7 (Exemple simple)**.** Soit $f = x^2 - 1$ dans $k[x]$. Alors :

$$V(f) = \{-1, 1\}, \quad D(f) = \mathbb{A}_k^1 \setminus \{-1, 1\}.$$

1.5.2 Le Nullstellensatz de Hilbert

Théorème 1.7 (Nullstellensatz Faible)**.** Si k est un corps algébriquement clos et si $I \subseteq k[x_1, \ldots, x_n]$ est un idéal tel que $V(I) = \emptyset$, alors $I = (1)$, c'est-à-dire que l'idéal contient 1 et est égal à tout l'anneau.

Remarque 1.11. Cela signifie que si un système de polynômes n'a pas de solutions dans $\mathbb{A}_k^n$, alors ces polynômes engendrent l'idéal trivial (1).

Théorème 1.8 (Nullstellensatz Fort)**.** Si k est un corps algébriquement clos, alors pour tout idéal $I \subseteq k[x_1, \ldots, x_n]$, on a :

$$\sqrt{I} = I(V(I)).$$

En d'autres termes, un polynôme $f \in k[x_1, \ldots, x_n]$ s'annule sur toutes les solutions de $V(I)$ si et seulement si une certaine puissance de f appartient à I.

Exemple 1.8 (Application du Nullstellensatz)**.** Soit $I = (x^2)$ dans $\mathbb{C}[x]$. On a $V(I) = \{0\}$, et $I(V(I)) = (x)$. Ici :

$$\sqrt{I} = I(V(I)) = (x).$$

Cela montre que le radical d'un idéal correspond exactement aux polynômes qui s'annulent sur sa variété.

1.5.3 Fermeture de Zariski

Définition 1.15 (Fermeture de Zariski)**.** Pour un sous-ensemble $S \subseteq \mathbb{A}_k^n$, la **fermeture de Zariski** de S, notée $\overline{S}$, est la plus petite variété affine contenant S. Formellement :

$$\overline{S} = V(I(S)),$$

où $I(S)$ est l'idéal de S.

Exemple 1.9 (Fermeture de Zariski)**.** Soit $S = \{(0,0), (1,1)\} \subset \mathbb{A}_k^2$. Alors :

$$I(S) = (x(x-1), y(y-1)),$$

et la fermeture de S est $\overline{S} = V(I(S))$.

1.5.4 Propriétés de la Topologie de Zariski

Théorème 1.9. Pour deux idéaux $I, J \subseteq k[x_1, \ldots, x_n]$, les relations suivantes s'appliquent :

$$V(I \cap J) = V(I) \cup V(J),$$
$$V(I + J) = V(I) \cap V(J).$$

Remarque 1.12. Ces propriétés montrent que les opérations sur les idéaux (intersection et somme) se traduisent par des opérations géométriques (réunion et intersection).