Résumé de TIPE: le Nullstellensatz de Hilbert

Alexandre

Table des matières

1 Anneaux et idéaux

1.1 Définitions

On parle d'algèbre commutative, c'est à dire que les anneaux qu'on concidère sont commutatif pour la multiplication. On parelrai alors d'idéaux bilatères.

Définition 1 (idéal d'un anneau)
Soit A un anneau. Un sous-ensemble $I \subseteq A$ est un idéal de A si :

(a) $(I, +)$ est un sous groupe de $(A, +)$
(b) $\forall a \in A, \forall b \in I, ab = ba \in I$

Proposition 2
L'idéal engendré par une partie S de A correspond à l'intersection de tous les idéaux de A contenant S.

Si I et J sont des idéaux, l'ensemble $\{i + j \mid i \in I, j \in J\}$ est un idéal, noté $I + J$. De même pour $IJ = \{ij \mid i \in I, j \in J\}$. De même pour l'intersection $I \cap J$

1.2 Anneau quotient

Définition 3 (anneau quotient)
Soit I un idéal bilatère d'un anneau A. La relation d'équivalence $\mathcal{R}$ définie par :

$$\forall x, y \in A,\ x\mathcal{R}y \Longleftrightarrow x - y \in I$$

est compatible avec la structure d'anneau de A et l'ensemble quotient $A/\mathcal{R}$ aussi noté A/I est muni d'une structure d'anneau.

Exemple 4
— $A/A = \{0\}$ car il n'y a qu'une seule unique classe d'équivalence
— $A/\{0\} = A$ car chaque classe d'équivalence ne possède qu'un seul élément de A

Proposition 5 (lien idéaux et morphisme d'anneaux)
Une partie I d'un anneau A est un idéal si et seulement si I est le noyau d'un morphisme d'anneaux.

Démonstration. Si I est un idéal de A, on conscidère le morphisme $\varphi : \begin{array}{ccc} A & \longrightarrow & A/I \\ a & \longmapsto & a + I \end{array}$.
Le noyau de φ est égal à I car si $x \in \ker(\varphi)$ alors $\varphi(x) = 0 = x + I$, donc $x \in I$. L'implication réciproque est claire. $\square$

Théorème 6 (bijection idéaux d'un anneau quotient)
Il existe un bijection entre les idéaux de A/I et les idéaux de A contenant I.
Si on note p la surjection canonique de A dans A/I, alors l'application $J \longmapsto p^{-1}(J)$ est cette bijection (où J est un idéal de A/I).

1.2.1 Théoreme d'isomorphisme

Théorème 7 (théoreme d'isomorphisme)

Soient A et B deux anneaux et $f : \quad A \longrightarrow \quad B$ un morphisme d'anneau. On pose $I = \ker f$.
Soit J un idéal de A contenu dans I et $\pi : \quad A \longrightarrow \quad A/J$ la projection canonique.
Alors on a :

(a) il existe une unique morphisme $\overline{f} : \quad A/J \longrightarrow \quad B$ tel que $f = \overline{f} \circ \pi$ (on dit que f se factorise par A/J)

(b) $\overline{f}$ est injectif si et seulement si $J = I$

(c) $\overline{f}$ est surjectif si et seulement f l'est aussi

En particulier on a $\operatorname{Im} f \simeq A/\ker f$.

https ://www.bibmath.net/ressources/justeunexo.php ?id=1368
<idéaux d'un anneau qotient>
<image d'un idéal est un idéal par un morphisme ?>
<noyeau morphisme idéal ?>

1.3 Propriétés

1.3.1 Idéaux premiers et maximaux

Définition 8 (idéal premier)

Soit A un anneau, I un idéal de A, I est premier si et seulement si l'anneau A/I est intègre. Cela revient au même d'imposer :

— $A \neq I$

— $\forall a, b \in A, ab \in I \Longrightarrow a \in I$ ou $b \in I$

Définition 9 (idéal maximal)

Un idéal I de A est dit maximal si $I \neq A$ et si pour tout idéal J de A tel que $I \subseteq J$ et $J \neq A$, on a $J = I$. (I est l'élément maximal pour l'inclusion)

Lemme 10

Soit A un anneau, A est un corps si et seulement si on a :

(1) $A \neq \{0\}$

(2) les seuls idéaux de A sont $\{0\}$ et A

Démonstration. Si on a (1) et (2), on prends $a \in A$ non nul de sorte que l'idéal (a) soit non nul. On a donc $(a) = A$. Donc $1 \in (a)$. Donc il existe $x \in A$ tel que $ax = 1$. Donc a inversible. Donc A corps.
Reciproquement, si A est un corps et I un idéal non nul. Alors on a $a^{-1}a = 1 \in I$. Donc $I = A$ (car I possède l'unité de A). $\square$

Proposition 11
Soit I un idéal de A. On a donc :

$$I \text{ maximal} \iff A/I \text{ est un corps} \implies A/I \text{ intègre} \iff I \text{ premier}$$

Démonstration. TODO □

1.3.2 Théorème des restes chinois

Proposition 12 (produit cartésien d'idéaux)
Les idéaux de $A \times B$ sont de la forme $I \times J$ où I et J sont des idéaux de A et B respectivement.

Proposition 13 (idéaux premiers entre eux)
Soient I et J des idéaux de A. Ces idéaux sont premiers entre eux si $I + J = A$.

1.3.3 Théorème de Krull

Théorème 14 (Krull)
Soit I un idéal de A, $I \neq A$, il existe un idéal maximal de A contenant I.

Démonstration. Se montre à l'aide du théorème de Zorn, à voir. □

1.4 Types d'anneaux

1.4.1 Anneaux noethériens

On rappelle qu'on idéal I d'un anneau A est dit de type fini s'il est engendré par un nombre fini d'éléments.

Définition 15 (anneau noethérien)
Un anneau noethérien est un anneau qui vérifie l'une des trois propriété équivalentes suivantes :

(1) tout idéal de A est de type fini
(2) toute suite croissante $(I_n)_n$ d'idéaux de A est stationnaire
(3) tout ensemble non vide d'idéaux de A a un élément maximal pour l'inclusion

Démonstration.
(1) $\Rightarrow$ (2) : On défini une suite $(I_n)_n$ croissante et on pose $I = \prod_{n\in\mathbb{N}} I_n$. Alors il existe $N \in \mathbb{N}$ tel que $I \subseteq I_N$. On a par définition de I : $I_N \subseteq I$. Donc $I = I_n$
(2) $\Rightarrow$ (3) : Soit E un ensemble non vide d'idéaux. On suppose par l'absurde que E n'admet pas d'élément maximal. On peut alors construire par récurrence une suite $(I_n)_n$ qui contredit (2). D'ou le resultat.
(3) $\Rightarrow$ (1) : Pas compris

□

Théorème 16 (Hilbert)
Si A est noethérien, $A[X]$ est noethérien.

Corollaire 17
Si A est noethérien, $A[X_1, \ldots, X_n]$ est noethérien.

1.4.2 Anneaux factoriels

La notion d'anneau factoriel généralsie la propriété de décomposition unique en facteurs premiers dans $\mathbb{Z}$. Il faut noter que toutes les propriétés de $\mathbb{Z}$ ne s'y applique pas forcément.

Définition 18
Soit A un anneau. L'anneau A est factoriel s'il vérifie ces trois propriétés :

(1) A est intégre (il n'a pas de diviseur de zéro)

(2) tout élément a non nul de A s'écrit $a = up_1 \ldots p_r$ avec $u \in A^\times$ et $p_1, \ldots, p_r$ irréductible dans A

(3) cette décomposition est unique, à permutation près et à des inversibles près : si $a = up_1 \ldots p_r = vq_1 \ldots q_s$, alors $r = s$ et il existe $\sigma \in \mathscr{S}_r$ tel que p_i et $q_{\sigma(i)}$ soient associé

1.4.3 Anneaux intégralement clos

Définition 19 (élément entier)
Soit B un anneau et A un sous-anneau de B. On dit que $b \in B$ est entier sur A s'il est racine d'un polynôme unitaire à cofficients dans A. C'est à dire :

$$b \text{ entier} \Longleftrightarrow \exists P \in A[X] \text{ unitaire}, \ P(b) = 0$$

Proposition 20 (anneau intégralement clos)
Soit A un anneau intègre. Il est dit intégralement clos si les seuls éléments entier sur A de son corps des fractions $Fr(A)$ sont les éléments de A.

Proposition 21
Tout anneau factoriel est intégralement clos.

Démonstration. Soit A un anneau factoriel, donc A intègre.
Soit $x \in Fr(A)$ entier sur A. Alors il existe $a_0, \ldots, a_{n-1} \in A$ tel que :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

On suppose par l'absurde que $x \notin A$.
On pose donc $x = \frac{y}{z}$ avec $y \in A$, $z \in A \backslash \{0,1\}$ et $y \wedge z = 1$. Donc :

$$z^n P(\frac{y}{z}) = z^n \frac{y^n}{z^n} + a_{n-1} z^n \frac{y^{n-1}}{z^{n-1}} + \cdots + a_0 z^n = 0$$

$$z^n P(\frac{y}{z}) = y^n + a_{n-1}zy^{n-1} + \cdots + a_0 z^n = 0$$
$$y^n = z(-a_{n-1}y^{n-1} - \cdots - a_0 z^n)$$

Or $z \nmid y^n$ car ils sont premier entre eux. Contradiction. Donc $x \in A$. □

EXEMPLE 22
Soit $d \in \mathbb{Z}*$ un entier sans facteur carré et différent de 1. On a alors :

$$d \equiv 1[4] \Longrightarrow \mathbb{Z}[\sqrt{d}] \text{ non intégralement clos}$$

On pensera à la contraposée comme exemple d'anneau intégralement clos.

Définition 23 (éléments associés)
Soit A un anneau intègre. Deux éléments a et b de A sont dits associés si a divise b et si b divise a.

Par exemple, si on se place dans $\mathbb{K}[X]$, deux polynomes associés sont égaux s'ils sont unitaire.

<anneaux principaux>

2 Ensembles algébriques affines

On fixe un corps $\mathbf{k}$ et un entier n. On note A l'anneau $\mathbf{k}[X_1, \ldots, X_n]$ des polynômes à n indéterminées à coefficients dans $\mathbf{k}$.

Si P est un élément de A, on dit qu'un point $x = (x_1, \ldots, x_n)$ appartenant à $\mathbf{k}^n$ est un *zéro* de P si $P(x_1, \ldots, x_n) = 0$

Définition 24 (ensemble algébrique affine)
Soit S une partie de A. On pose :

$$V(S) = \{x \in \mathbf{k}^n \mid \forall P \in S,\ P(x) = 0\}$$

et alors les $x \in V(S)$ sont les zéros communs à tout les polynômes de S. On dit que $V(S)$ est l'ensemble algébrique affine défini par S.

Références

[1] Daniel Perrin, *Cours d'algèbre*

[2] M.F. Atiyah, I.G. MacDonald *Introduction to Commutative Algebra*

[3] J.S. Milne, *Algebraic Geometry*

[4] Daniel Perrin, *Géométrie algébrique. Une introduction*