Cours MP2I

Alexandre

Table des matières

1 Notes

Nullstellensatz : (démo ?)

— Idéaux
— Algébriquement clos
— Bézout ?

Topologie de Zariski : ? ? ? ?

— Lemme de Zorn (AC)

Dimension : ?
Projectif/Affine : ?

2 Notions d'ensemble

2.1 Relations d'ordre

Remarque 1

Dans un ordre total, les notions d'élément maximal et de plus grand élément sont confondues (de même pour l'élément minimal et le plus petit élément)

TODO : définition élément maximal et pge

2.2 ZFC

Définition 2 (chaîne)

Une chaîne d'un ensemble partiellement ordonée est une partie sur laquelle l'ordre est total.

Définition 3 (ensemble inductif)

Soit $(E, \leqslant)$ un ensemble ordonné. On dit que E est un ensemble inductif si toute partie totalement ordonné (càd toute chaine) admet un majorant dans E.

On remarque alors que tout ensemble ordonné fini est inductif. Cependant ce n'est pas le cas d'ensemble comme $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$, on a bien $\mathbb{N} \subseteq \mathbb{Z}$ mais $\mathbb{N}$ n'admet aucun majorant dans $\mathbb{Z}$.

Théorème 4 (lemme de Zorn)

Tout ensemble non vide et inductif admet au moins un élément maximal.

Définition 5 (bon ordre)

Un ensemble E est bien ordonnée si toute partie non vide de E admet un plus petit élément. Toute relation d'ordre vérifiant cette propriété sur E est un bon ordre.

On remarque aussi qu'un bon ordre est forcément total. Si on regarde une paire $\{a,b\}$ de E, on peut toujours comparer a et b car il y a un plus petit élément.

Théorème 6 (théorème de Zermelo)

Tout ensemble E non vide, peut être bien ordonné.

Théorème 7 (axiome du choix)

Pour tout ensemble non vide E, il existe au moins une application f de $\mathcal{P}(E)$ dans E telle que $\forall A \subseteq E$, avec $A \neq \varnothing$, on ait $f(A) \in A$.

Donc f est une "fonction de choix" qui permet de choisir un élément dans une partie de E non vide.

Proposition 8

Le lemme de Zorn, le théorème de Zermelo et l'axiome du choix sont équivalent.

Démonstration. Zermelo $\Longrightarrow$ Choix

Soit E un ensemble non vide qu'on munit d'un bon ordre grâce au théorème de Zermelo. Soit A une partie non vide de E, alors elle admet un plus petit élément a. On pose $f(A) = a$ tel qu'on a définit $f: \begin{array}{ccc} \mathcal{P}(E)\backslash\{\varnothing\} & \longrightarrow & E \\ A & \longmapsto & a \end{array}$.

On peut ensuite définir $f(\varnothing)$ de manière quelconque pour avoir une fonction de choix f sur E. Par exemple on prends $f(\varnothing) = f(E)$.

□

Si on veut maintenant justifier Zorn $\Longrightarrow$ Zermelo, on doit d'abord considérer les parties de E que l'on peut munir d'un bon ordre, et montrer que leur ensemble est inductif.

Proposition 9
Soit un ensemble non vide E, on considère $\mathcal{M}$ l'ensemble des couples (A,O_A) où A est une partie non vide de E et O_A un bon ordre sur A.

Remarque 10
On a clairement $\mathcal{M} \neq \varnothing$ car si on prends une partie A de cardinal fini n, alors il existe une bijection $\varphi : \begin{array}{ccc} [1;n] & \longrightarrow & A \\ n & \longmapsto & a_n \end{array}$ (avec $a_1, \ldots, a_n$ éléments distincts de A).
On peut ordonner A par O_A défini par $a_i O_A a_j \iff i < j$: c'est un bon ordre car l'élément le plus petit d'une partie A est associé à l'entier le plus petit.

<TODO : remplacer les []>

Proposition 11
On peut munir l'ensemble $\mathcal{M}$ de la relation d'ordre suivante :

$$(A, O_A) \preccurlyeq (B, O_B) \Leftrightarrow \begin{cases} A \subseteq B \\ O_A \text{ est la restriction de } O_B \text{ à } A^2 \\ A \text{ est partie héréditaire de } B \end{cases}$$

Démonstration. Exercice (cf Bernard Gaustiaux) □

<segment initial = partie héréditaire ?>

Proposition 12
L'ensemble $\mathcal{M}$, non vide, ainsi ordonné, est inductif.

Démonstration. TODO □

<Pertinence de l'axiome du choix dans le cas d'un ensemble fini ?>
<TODO probleme 2 alain troesh>

2.3 Ensemble quotient

Définition 13 (classe d'équivalence)
Soit R une relation d'équivalence sur un ensemble E. Soit $x \in E$, on considère la partie $\tilde{x}$ de E définie par :

$$y \in \tilde{x} \Leftrightarrow xRy$$

C'est la classe d'équivalence de x

C'est l'ensemble des y équivalent à x. Cette partie est non vide car $x \in \tilde{x}$.

Définition 14 (partition)
Une partition d'un ensemble E est définie par :

(a) l'union des classes d'équivalences donne $\biguplus_{x \in E} \tilde{x} = E$

(b) $\forall x \in E, \tilde{x} \neq \emptyset$

(c) $\forall x, y \in E, x \neq y \Rightarrow \tilde{x} \cap \tilde{y} \neq \emptyset$

Lemme 15
Soient $x, y \in E$. On a :

$$x \sim y \iff \tilde{x} = \tilde{y}$$

On déduit que deux classes distinctes sont disjointes.

Théorème 16 (parition formée par les classes d'équivalence)
L'ensemble des classes d'équivalences sous $\sim$ forme une parition de E.

Les différentes classes d'équivalence des éléments de E sont des parties E, non vides, disjointes, dont la réunion donne E (d'après la définition d'une partition).

Définition 17 (ensemble quotient)
L'ensemble des parties de E dont les éléments sont des classes d'équivalence s'appelle l'ensemble quotient de E par R, noté E/R

Proposition 18 (application canonique)
Si R est une relation d'équivalence, l'application $\pi : \; E \longrightarrow \; E/R$ associe un élément x de E à sa classe d'équivalence.
Elle est surjective car chaque classe d'équivalence F est non vide, tout élément de F est envoyé par π sur F (donc on a : $\forall x \in F, \pi(x) = F$)

3 Anneaux et idéaux

3.1 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 19 (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 20
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 $I \cap J$

3.2 Anneau quotient

Définition 21 (anneau quotient)
Soit I un idéal bilatère d'un anneau A. La relation d'équivalence $\mathcal{R}$ définie par :

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

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 22

— $A/A = \{0\}$ 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 23 (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. □

Théorème 24 (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).

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 ?>

3.3 Propriétés

3.3.1 Idéaux premiers et maximaux

Définition 25 (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 :

— $A \neq I$

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

Définition 26 (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 27

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). □

Proposition 28

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 □

3.3.2 Théorème des restes chinois

Proposition 29 (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 30 (idéaux premiers entre eux)

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

3.3.3 Théorème de Krull

Théorème 31 (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. □

4 Propriétés des anneaux

4.1 Définitions

Définition 32 (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>

4.1.1 Propositions

4.2 Propriétés remaquables

4.2.1 Théoreme d'isomorphisme

Théorème 33 (théoreme d'isomorphisme)
Soient A et B deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneau. On pose $I = \ker f$. Soit J un idéal de A contenu dans I et $\pi : A \longrightarrow A/J$ la projection canonique. Alors on a :

(a) il existe une unique morphisme $\overline{f} : A/J \longrightarrow B$ 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 $\operatorname{Im} f \simeq A/\ker f$.

4.2.2 Opérations sur les idéaux

4.2.3 Algèbres

4.3 Types d'anneaux

4.3.1 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 34 (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 35 (Hilbert)
Si A est noethérien, $A[X]$ est noethérien.

Corollaire 36
Si A est noethérien, $A[X_1, \ldots, X_n]$ est noethérien.

4.3.2 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 37
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

4.3.3 Anneaux intégralement clos

Définition 38 (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 :

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

Proposition 39 (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 40
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 :

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

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

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

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

Exemple 41
Soit $d \in \mathbb{Z}*$ un entier sans facteur carré et différent de 1. On a alors :

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

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

5 Corps

5.1