(1) ~ 45 min
~ 10 min

Exposé : théorie des modèles.

Idée : ne pas étudier des ensembles seul et mettre des f.t et des relations dessus

NB : Il y aura des abus de notation partout.

Plan

I] Formaliser les notions de structure, formules, théorie, et définir les modèles.

→ quels résultats grâce à l'étude des structures ?

II] Construction intéressante : les ultraproduits

III] Théorie des corps finis et modèles infinis de la th des corps finis

---

I] **Def** : Langage. C'est la donnée de :

1) Ensemble infini dénombrable de variable $\{v_i\}_{i \in \mathbb{N}}$
2) Symboles logiques $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, \forall, \exists$
3) Ensembles $(\mathcal{F}_n)_{n \geq 0}$, où si $f \in \mathcal{F}_n$ on dit que f est un symbole de fonction n-aire
4) Ensembles $(\mathcal{R}_n)_{n \geq 0}$, où si $R \in \mathcal{R}_n$, on dit que R est un symbole de relation n-aire.

$T \in \mathcal{R}_0$ (symbole → toujours vrai) ; les $\in \mathcal{F}_0$ = cstes.

Ex de langage : • Ensemble ordonnés $\mathcal{L}_{ord} = \{=, \leq\}$

• Langage des anneaux $\mathcal{L}_{an} = \{=, +, -, \cdot, 0, 1\}$

• Un mot est une suite de symbole du langage : $\vee \vee \vee$; $\vee \wedge x \neg$
↳ mot un peu pourri.

• On va se fixer des règles de syntaxe pour formes des mots plus intéressants ; qu'on va construire par induction.

- <u>Termes</u>. $\mathcal{T}_0(L) = \{$ variables et constantes $\}$

$$\left[\begin{array}{l} \mathcal{T}_k(L) = \mathcal{T}_{k-1}(L) \cup \left\{ \underbrace{f(t_1, \dots, t_n)}_{\substack{\text{qu'on écrit plutôt} \\ f\, t_1 \dots t_n}} \; ; \text{ où } f \in \mathcal{F}_n \text{ et } t_i \in \mathcal{T}_{k-1}(L) \right\} \\ \mathcal{T}(L) = \bigcup_{k \geq 0} \mathcal{T}_k(L) \end{array}\right.$$

Exemple avec $L = \{=, +, -, \cdot, 0, 1\}$

$0, 1, x$ ← variable sont des termes.

$((1+1)+) - +1)$ est un terme.

$(x^2 + x) + 1$ ——————— etc

Lorsque des variables apparaissent ds un terme t, on note $t = t(v_{i_1}, \dots, v_{i_n})$.

- <u>Formules</u> : Si $R \in \mathcal{R}_n$ et $t_1, \dots, t_n$ sont des termes

alors $R(t_1, \dots, t_n)$ est une <u>formule atomique</u>

Si φ et ψ sont des formules, $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \Rightarrow \psi$ et $\varphi \Leftrightarrow \psi$ sont des formules.

Si, de plus, x est une variable alors $\forall x\, \varphi$ ou $\exists x\, \varphi$ sont des formules

<u>Exemples</u> . $\mathcal{L}_{ord} = \{=, >\}$

$x > y$ est une formule atomique.

$\exists x \; x > y$ est une formule, tout comme $\exists z \; x > y$.

- $\mathcal{L}_a = \{=, +, -, \cdot, 0, 1\}$
  - $x^2 + x + 1 = 0$ formule atomique
  - $\forall x \; x^2 + x + 1 = 0$ formule
  - $\forall x \; x^2 + x + 1 = 0 \Rightarrow \exists y \; y^2 + 1 = 0$.

Exposé : théorie des modèles.

I] Variables libre, variables liées.

• Lorsque des variables apparaissent dans une formule, elles peuvent être précédée (ou non) d'un quanteur.

Pour le dire rapidement, si dans une formule toutes les occurrence d'une variable sont précédées d'un quanteur, la variable est dite <u>liée</u> sinon elle est libre.

<u>Ex</u> : $\mathcal{L}_n = \{=, +, -, \cdot, 0, 1\}$

$x^2+1=0$; x est libre.

$\exists x \; x^2+1=0$: x est liée.

$(\exists x \; x^2+1=0) \vee (x=0)$: x est libre

on aurait pu écrire $(\exists x \; x^2+1=0) \vee (y=0)$

c'est différent si le parenthésage avait été $\exists x \; (x^2+1=0 \vee x=0)$

<u>Enoncé</u> : Des formules où toutes les variables sont liée sont appelées des énoncés.

Un ensemble d'énoncés s'appelle une théorie.

<u>Ex</u> : théorie des groupes (dans le langage des groupes)

$\mathcal{L}_g = \{=, \cdot, e\}$

- $\forall x \; \forall y \; \forall z \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\forall x \quad (x \cdot e = e \cdot x = x)$
- $\forall x \; \exists y \quad (x \cdot y = y \cdot x = e)$

. On a défini un langage et des formules, mais on a rien pour les interpréter.

<u>Structures</u> : On fixe un langage $\mathcal{L}$.

Une structure $\mathcal{M}$ est la donnée de :

1) Un ensemble sous-jacent M.
2) Pour tout $f \in \mathcal{F}_n$; une fonction $f^{\mathcal{M}} : M^n \to M$
3) Pour toute $R \in \mathcal{R}_n$; un sous-ensemble $R^{\mathcal{M}} \subset M^n$.

<u>Ex</u> : $(\mathbb{Z}, =, +, -, \cdot, 0, 1)$ est une structure

$=$: diagonale de $\mathbb{Z}^2$

$+, -, \cdot$: loi de composition usuelles.

$0, 1$: cste.

→ Interprétation des formules dans la structure.

. Pour un terme $t(\bar{v})$; où $\bar{a} \in M^n$.

$t(\bar{a})$ c'est le terme où on a remplacé les apparitions de $\bar{v}$ par $\bar{a}$.

Ex : $x^2+1 := t(x)$ ⇝ donne ⇝ avec $a = 3$ ⇝ 3^2+1 dans $\mathbb{Z}$.

S : $\varphi(\bar{x}) = R(t_1(\bar{x}), \dots, t_n(\bar{x}))$ une formule atomique.

$\mathcal{M} \models \varphi(\bar{a})$ <u>ssi</u> $(t_1(\bar{a}), \dots, t_n(\bar{a})) \in R^{\mathcal{M}}$

(ex : $\mathbb{Z} \models a^2 - 1 = 0$ ssi $(a^2-1, 0) \in \mathrm{diag}(\mathbb{Z}^2)$)
$(a \in \mathbb{Z})$.

S : $\varphi = \psi \alpha \psi'$ où $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$

$\mathcal{M} \models \varphi(\bar{a}) \Leftrightarrow \mathcal{M} \models \psi(\bar{a})$ α $\mathcal{M} \models \psi'(\bar{a})$.

$\mathcal{M} \models \neg\varphi(\bar{a}) \Leftrightarrow \mathcal{M} \not\models \varphi(\bar{a})$.

idem pour $\mathcal{M} \models \forall v\, \varphi$ et $\mathcal{M} \models \exists v\, \varphi$

On dira que la formule φ est vérifiée dans $\mathcal{M}$.

Exposé : théorie des modèles

Modèle : Soit L un langage et T une théorie, on dit qu'une structure $\mathcal{M}$ est un modèle, si tout énoncé de T est satisfait dans $\mathcal{M}$. $(\forall \varphi \in T ; \mathcal{M} \models \varphi)$

II] Ultraproduits

Filtres : Soit E un ensemble ; un filtre $\mathcal{F}$ sur E est un ensemble de parties de E tq.

(F1) Si $X \subset Y \subset E$ et $X \in \mathcal{F}$ alors $Y \in \mathcal{F}$

(F2) Si $X, Y \in \mathcal{F}$ alors $X \cap Y \in \mathcal{F}$

(F3) $\emptyset \notin \mathcal{F}$

Exemples de filtres sur E (non vide).

- $\mathcal{F} = \{E\}$ est un filtre.
- $\mathcal{F}_{x_0} = \{ X \subset E ; x_0 \in X \}$ filtre principal
- $\{ X \subset E ; \complement_E X \text{ est fini} \}$ est dit le filtre de Fréchet.

→ on peut comparer les filtre par la relation d'inclusion.

Un ultrafiltre est un elt maximal sur l'ensemble des filtres (existe par le lemme de Zorn).

* Prop Un ultrafiltre est un filtre qui vérifie de plus

(F4) $\forall X \subset E, \ X \in \mathcal{F} \Leftrightarrow (E \setminus X) \notin \mathcal{F}$

* **Prop** : Un ultrafiltre est soit principal, soit contient le filtre de Fréchet.

<u>Ultraproduit</u> : On se fixe un langage L. Soit $(\mathcal{M}_i)_{i\in I}$ une famille de L-structures, où I est un ensemble non vide.

On va construire une structure à partir des $\mathcal{M}_i$.

On considère $N = \prod_{i\in I} M_i$; si $f \in \mathcal{F}_m$ on définit

$$f^{\mathcal{N}} : N^m \longrightarrow N$$
$$(a_1, \dots, a_m) \longmapsto (f^{\mathcal{M}_i}(a_1(i), \dots, a_m(i)))_{i\in I}$$
où $a_j = (a_j(i))_{i\in I}$

Si $R \in \mathcal{R}_m$, $N \models R(a_1, \dots, a_m) \iff \forall i\ M_i \models R(a_1(i), \dots, a_m(i))$

→ On va quotienter N par un ultrafiltre $\mathcal{F}$ sur I.

$a, b \in N$ $\quad a \underset{\mathcal{F}}{\equiv} b \iff \{i \in I \mid a(i) = b(i)\} \in \mathcal{F}$

C'est une relation d'équivalence sur N, compatible avec les fonctions et les relations.

i.e. si $a_j \underset{\mathcal{F}}{\equiv} b_j$ $\forall j$ alors $f^{\mathcal{N}}(a_1, \dots, a_m) \underset{\mathcal{F}}{\equiv} f^{\mathcal{N}}(b_1, \dots, b_m)$.
pour les fct.

Cela se vérifie bien à l'aide des axiomes (F_1) et (F_2) des filtres.

Ainsi $\prod_{i\in I} M_i/\mathcal{F}$ est une L-structure.

Si $\mathcal{F} = \mathcal{F}_{i_0}$ est un filtre principal $\prod M_i/\mathcal{F}_{i_0} \cong M_{i_0}$ (comme struct)

Exposé : théorie des modèles

- Les ultraproduits ont des propriétés intéressantes lorsque $\mathcal{F}$ est un ultrafiltre.

Théorème de Łos (mathématicien polonais).

Si $\mathcal{F}$ est un ultrafiltre ; en notant $M = \prod_{i \in I} M_i / \mathcal{F}$
si φ est une formule

$$M \models \varphi(\bar{a}) \iff \{ i \in I \mid M_i \models \varphi(\bar{a}(i)) \} \in \mathcal{F}$$

En particulier si tous les M_i sont des modèles d'une théorie T, alors M est aussi un modèle de T.

III) Corps pseudo-fini

- Grâce aux ultraproduits on va construire un modèle <u>infini</u> de la théorie des corps finis.
- La théorie des corps fini est l'ensemble des énoncés (i.e formule où toutes les variables sont liées) vrais dans <u>tous</u> les corps finis.

Il se trouve que la propriété "d'être fini" ne s'exprime pas dans le langage des anneaux. Naïvement on aurait envie d'écrire

$$\exists n \quad \forall x_1 \, \forall x_2 \ldots \forall x_{n+1} \quad (x_1 = x_2 \vee x_1 = x_3 \vee \ldots \vee x_n = x_{n+1})$$

qui dit qu'il existe un entier n tq si on prend $n+1$ éléments on pourra toujours en trouver 2 égaux.

Mais $\exists n \ldots$ ne fait pas parti du langage des anneaux.

Existence de corps pseudo-finis

Soit $\mathcal{F}$ un ultrafiltre non principal sur $\mathbb{N}$. Soit p

$M = \prod_{n \geq 1} \mathbb{F}_{p^n} / \mathcal{F}$ est un modèle de la théorie des corps fini par le thm de Łos.

On va montrer qu'il est infini.

Pour k fixé à l'avance, la prop "il existe plus que k éléments distincts" est vérifiée dans tous les $\mathbb{F}_{p^n}$ sauf un nb fini

or comme $\mathcal{F}$ est un ultrafiltre non principal, il contient le filtre de Frechet en conséquence

$$\{n \in \mathbb{N} \mid \mathbb{F}_{p^n} \models \text{il existe plus de } k \text{ elt distincts}\} \in \mathcal{F}.$$

donc par le thm de Łos cette prop est vérifiée dans $\prod_{n \geq 1} \mathbb{F}_{q^n} / \mathcal{F}$ qui est donc infini.

De plus M est de caractéristique p. Avec $Q = \{p^m \mid p \in \mathcal{P}, m \geq 1\}$ et $\mathcal{U}$ un ultrafiltre sur Q, on aurait pu considérer

$M' = \prod_{q \in Q} F_q / \mathcal{U}$ un corps pseudo fini de caractéristique 0.

- - - - -

Bonus : les corps pseudo fini vérifient les 3 prop suivantes

(P_1) Le corps F est parfait

(P_2) $\forall n \geq 1$; F a exactement une extension algébrique de degré n.

(P_3) Toute variété V définie sur F a un point F-rationnel.