SYSTEMES ALGEBRIQUES

Table des matières

1	Preuves 4	
	1.1 Proprietes de preuves formelles	4
	1.2 Ensembles 6	
2	Applications entre ensembles	8
	2.1 Relations d'equivalence 9	
	2.2 Cardinal d'un ensemble 11	

∠ List of Theorems

1	■ Definition (division d'entiers)	5
1	♦ Proposition (Division avec reste)	5
		5
2	♦ Proposition (Paradoxe de Russel)	6
	▶ Proof	6
2	■ Definition (Formalisation des applications)	8
4	♦ Proposition (Surjectivite de la composition)	9
		9
3	■ Definition (Relations d'equivalence)	9
4	■ Definition (Classes d'equivalence)	10
5	■ Definition (L'ensemble quotient)	10
6	E Definition (Cardinal d'un ensemble)	11

2		
.7		

8	■ Theorem (Cantor-Bernhard-quelquechose)	12
9	♣ Lemme	12
		12
	ℰ Proof	12

Parties

- preuves et ensembles
- Theorie des nombres
- Theorie des groupes



Une grande partie du bachelor est de faire des preuves, il est donc important de comprendre quand une preuve est correcte.

Il y a deux types de preuves :

- Preuves formelles
 Tres precise, mais difficile a lire.
- Preuves d'habitude
 Approximation des preuves formelles, en remplacant ques parties par du texte "humain". Il faut s'assurer qu'on peut traduire cette preuve en preuve formelle.

1.1 Proprietes de preuves formelles

 Elles utilisent seulement des signes/symboles mathematiques.
— ∃ (existe)
$ \forall$ (pour tout)
— ∃! (existe unique)
— ∧ (et)

- ∨ (ou)
- ¬ (non)
- \rightarrow (implique)
- etc
- Elle consiste de lignes, et il y a des regles strictes que ces lignes doivent suivre.
- Regles

- Axiomes
- Propositions qu'on a deja montrees.
- Tautologies

Exemples

$$\neg (A \lor B) \iff ((\neg A) \lor (\neg B))$$

- Modus Ponens : Si on a que

$$\begin{cases} A \Rightarrow B \\ A \end{cases}$$

Alors B est vrai¹

Dans ce cours 0 n'est ni positif, ni negatif.

1. Pour lire plus, regarder "Calcul des predicats" sur wikipedia

■ Definition 1 (division d'entiers)

q divise a (q|a) si il existe un entier r tel que $a = q \cdot r$.

♦ Proposition 1 (Division avec reste)

 $a, q \neq 0$ entiers non-negatifs,

 $\Rightarrow \exists$ entiers non-negatifs

b et r t.q.

$$a = b \cdot q + r$$

et

Proof

Unicite Supposons que $\exists b, r, b', r'$ entiers non-negatifs et r < q et r' < q.

$$a = bq + r$$
$$a = b'q + r'$$

Alors

$$\underbrace{(b-b')}_{-q,0,q}q = \underbrace{r'-r}_{-q< r'-r< q}$$

$$\Rightarrow r' - r = 0$$

$$(b-b')q=0 \Rightarrow b=b'$$

Existence

Par induction sur *a*.

•
$$a = 0 \Rightarrow b = 0$$
 et $r = 0$

0 supposons que on connaît l'existence pour a remplace par a-1. Alors, $\exists c, s$ tq

$$a - 1 = cq + s$$
$$s < q$$

Alors, soit s < q - 1

$$a = (a-1) + 1$$
$$= cq + s + 1$$

Alors on peut dire que s + 1 = r. Sinon s = q - 1

$$a = (a-1) + 1$$

$$= cq + \underbrace{s+1}_{=q}$$

$$= (c+1) \cdot q + 0$$

1.2 Ensembles

Premiere approche:

ensemble = { collection de choses }

Exemple:

$$\underbrace{\{\{\{\emptyset\},\emptyset\}\emptyset\}}_A$$

$\Rightarrow A \in A$

♦ Proposition 2 (Paradoxe de Russel)

$$B = \{Aest \ un \ ensemble | A \in A\}$$

peut pas etre un ensemble.

Supposons que B est un ensemble et $B \subset B \iff B \not\subset B \iff \Box$

Question:

Alors, qui sont les ensembles? Reponse :

Axiome de Zermelo-Fraenkel

Quelques exemples de Zermelo-Fraenkel

- 1) et 2) impliquent que \emptyset est un ensemble.
- 2)A ensemble, E(x) expression $\rightarrow \{a \in A | E(a) \text{vrai}\}$ 3) A_i ensembles ($i \in I$)

$$\rightarrow \bigcup_{i \in I} A_i$$

est un ens. 4)...

5) axiome de l'ensemble puissance

A ensemble

$$\rightarrow 2^A = \{B \subseteq A | B$$
sous-ens. $deA\}$

Exemple : $\{0,1\} = A$

$$2^A = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$$

6) A_i ensembles ($i \in I$) \rightarrow on peut choisir $a_i \in A_i$ a la meme fois 7) etc...

Consequences 1) Les ensembles finis existent.

- (i) Ø
- (ii) $\{\emptyset\}$

...

2)
$$\mathbb{N} = \{0, 1, 2, ...\}$$
 est un ensemble 3) $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$

4)
$$2 \cdot \mathbb{N} = \{x \in \mathbb{N} | 2|x\}$$
 5) $A \subseteq B$

Alors on peut definir la difference

$$B \setminus A = \{x \in B | x \notin A\}$$

6)
$$A, B \subseteq C$$

$$A \cap B = \{x \in C | x \in A, x \in B\}$$

Applications entre ensembles

Plus complet dans les notes de cours.

■ Definition 2 (Formalisation des applications)

Soit A, B deux ensembles, alors

$$\phi:A\to B$$

On la definit comme un sous-ensemble du produit cartesien :

$$\Gamma_{\phi} \subseteq A \times B$$

$$\forall a \exists ! b : (a, b) \in \Gamma_{\phi}$$

Une maniere de penser d'une application est comme une machine qui prend a et qui sort b, la machine aura un fonctionnement deterministe.

♣ Propriete 3 (Propriete des applications)

Soit ϕ : $A \rightarrow B$

1. injective:

$$\phi(a) = \phi(b) \iff a = b$$

2. surjective

$$\forall b \in B \exists a : \phi(a) = b$$

3. bijective ←⇒ injective et bijective L'inverse

$$\phi^{-1}: B \to A \iff \phi(a) = b$$

4. Image

$$\phi(A) = {\phi(a)|a \in A} \subseteq B$$

5. $\phi: A \rightarrow B, \xi: B \rightarrow C$, alors

$$(\xi \circ \phi)(a) = \xi(\phi(a))$$

1. L'ordre est etrange.

♦ Proposition 4 (Surjectivite de la composition)

- (i) ξ surjectif
 - (ii) ϕ pas necessairement \iff il existe un contre exemple.

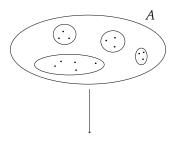
Proof

(i)
$$\forall c \in C : \exists a : \xi(\phi(a)) = c$$

Donc $\exists b := \phi(a) \Rightarrow \xi(b) = c$

Figure 2.1: contre-exemple injectivite

2.1 Relations d'equivalence



 $A = \left\langle \begin{array}{c} \bigcirc, \bigcirc, \bigcirc, \bigcirc, \\ \end{array} \right\rangle$

Figure 2.2: schema relation d equiva-

■ Definition 3 (Relations d'equivalence)

Une relation d'equivalence de A est un sous ensemble du produit $R\subseteq A\times A$ tq.

- 1. (identite) $\forall a \in A : (a, a) \in R$
- 2. (reflexivite): $(a,b) \in R \iff (b,a) \in R$
- 3. (transitivite): $(a,b) \in R$, $(b,c) \in R \Rightarrow (a,c) \in R$.

● Exemple 5 (Exemple de transitivite)

 $A = \mathbb{Z}$, alors:

$$R \subseteq \mathbb{Z} \times \mathbb{Z} : (a,b) \in R \iff m|a-b|$$

- 1. $(a,a) \in R : m|a-a$.
- $(a,b) \in R \Rightarrow (b,a) \in R$

$$\Rightarrow m|a-b \ m|b-a=-(a-b)$$

Ce qui est equivalent.

3.
$$(a,b) \in R, (b,c) \in R \Rightarrow (a,c) \in R$$

$$m|a-b, m|b-c \Rightarrow m|(a-b)+(b-c)=a-c$$

■ Definition 4 (Classes d'equivalence)

Soir $R \subseteq A \times A$ rel. d'equivalence. et $a \in A$.

La classe d'equivalence de a est

$$R_a = \{b \in A | (a, b) \in R\}$$

■ Definition 5 (L'ensemble quotient)

L'ensemble quotient de R :

$$A/R = \{R_a | a \in A\} \subseteq 2^A$$

© Exemple 6 (Cas de relation d'equivalence)

m = 3 et R la relation d'equivalence precedente.

$$A = \mathbb{Z} = \{-2, -1, 0, 1, 2\}$$

Alors:

$$R \supseteq (0.3)$$
 $(1,4)$
 $(1,7)$
 $(11,8)$

$$R_a = \{b \in A | (a, b) \in R\} = \{b \in \mathbb{Z} | 3|a - b\} \text{ Pour le cas } a = 1, \text{ on } a:$$

$$R_1 = \{\dots, -5, -2, 1, 4, 7, \dots\} = 1 + 3\mathbb{Z}$$

$$R_0 = 3\mathbb{Z}$$

$$R_2 = \{\dots, -4, -1, 2, 5, \dots\}$$

$$A/R = \{3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2\}$$

En general, pour m arbitraire

$$A/R = \{m\mathbb{Z}, m\mathbb{Z} + 1, \dots, m\mathbb{Z} + (m-1)\}\$$

2.2 Cardinal d'un ensemble

La question generale est : comment mesure-t'on la taille d'un ensemble (meme pour des ensembles infinis)?

■ Definition 6 (Cardinal d'un ensemble)

- 1. A et B ont le meme cardinal si il existe $\phi: A \to B$ bijection, on note |A| = |B|
- 2. A a un cardinal plus petit que B si \exists une injection

$$\psi:A\hookrightarrow B$$

On note $|A| \leq |B|$.

Par exemple, il n'existe pas de bijection de \mathbb{Z} a \mathbb{R} , par contre il existe une injection $\mathbb{Z} \hookrightarrow \mathbb{R}$ donc $|\mathbb{Z}| < |\mathbb{R}|$. On dit quue $|\mathbb{Z}| = \omega_0 = \aleph_0$ et on note $|R| = \kappa$

D Exemple 7

On veut montrer que $|\mathbb{N}| = |\mathbb{Z}|$ et

$$\phi: \mathbb{Z} \to \mathbb{N}$$

$$\phi: 0 \le x \mapsto 2x \\ 0 > x \mapsto -2x - 1$$

Devoir : montrer que ϕ est une bijection.

■Theorem 8 (Cantor-Bernhard-quelquechose)

 $|A| \le |B|$, $|B| \le |A|$ alors |A| = |B|. Autrement dit:

$$f: A \hookrightarrow B, B \hookrightarrow A \Rightarrow \exists bijA \mapsto B$$

♣ Lemme 9

Si il existe

$$X \subseteq A$$

$$X = A \setminus g(B \setminus f(X))$$

Alors il existe une bijectin $A \mapsto B$

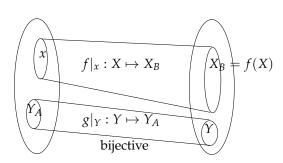
Proof

$$Y_A := X \setminus A = g(Y)$$

$$X_B = f(X)$$

$$Y = B \setminus f(x)$$

Figure 2.3: preuve fonction bizarre



Union disjointe $B = Y \perp X_B$

$$f: A \hookrightarrow B \text{ et } g: B \hookrightarrow A.$$

Il faut : X tq :

$$X = A \setminus g(B \setminus f(x)) = H(X)$$

$$X \subseteq Z \Rightarrow f(X) \subseteq f(Z)$$

$$\Rightarrow B \setminus f(x) \supseteq B \setminus f(Z)$$

$$\Rightarrow g(B \setminus f(x)) \supseteq g(B \setminus f(Z))$$

$$\Rightarrow A \setminus g(B \setminus f(x)) \supseteq g(B \setminus f(Z))$$

$$\Rightarrow A \setminus g(B \setminus f(Z)) \subseteq A \setminus g(B \setminus f(x))$$

$$\Rightarrow H(X) \subseteq H(Z)$$

Soit $W = \bigcap_{X \subseteq A, \ H(X) \subseteq X} X$ Lire les notes pour voir que W =H(W)