DAVID WIEDEMANN

SYSTEMES ALGEBRIQUES

Table des matières

List of Theorems

Lecture 1: Introduction

Tue 15 Sep

Parties

— preuves et ensembles

— Theorie des nombres

— Theorie des groupes

1 Preuves

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 qqes 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.

  — $\exists$ (existe)

  — $\forall$ (pour tout)

  — $\exists!$ (existe unique)

  — $\wedge$ (et)

  — $\vee$ (ou)

  — $\neg$ (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

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

— Modus Ponens : Si on a que

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

Alors B est vrai [1]

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

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

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,

$$\Rightarrow \exists \text{ entiers non-negatifs}$$

b et r t.q.

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

et

$$r < q$$

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 connait l'existence pour a remplace par $a - 1$. Alors, $\exists c, s$ tq

$$\begin{aligned} a - 1 &= cq + s \\ s &< q \end{aligned}$$

Alors, soit $s < q - 1$

$$\begin{aligned} a &= (a-1) + 1 \\ &= cq + s + 1 \end{aligned}$$

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

$$\begin{aligned} a &= (a-1) + 1 \\ &= cq + \underbrace{s+1}_{=q} \\ &= (c+1) \cdot q + 0 \end{aligned}$$

□

1.2 Ensembles

Premiere approche :

ensemble = { collection de choses }

Exemple :

$$\underbrace{\{\{\{\emptyset\},\emptyset\}\emptyset\}}_{A}$$

$\Rightarrow A \in A$

Proposition 2 (Paradoxe de Russel)

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

peut pas etre un ensemble.

Proof

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

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 $\to \{a \in A | E(a)\text{vrai}\}$ 3) A_i ensembles ($i \in I$)

$$\to \mathbb{U}_{i \in I} A_i$$

est un ens. 4)...

5) axiome de l'ensemble puissance

A ensemble

$$\to 2^A = \{B \subseteq A | B\text{sous-ens.}de A\}$$

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

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

6) A_i ensembles ($i \in I$) $\to$ on peut choisir $a_i \in A_i$ a la meme fois

7) etc...

Consequences 1) Les ensembles finis existent.

(i) $\emptyset$

(ii) $\{\emptyset\}$

...

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

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) $A, B \subseteq C$

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