Structures Algebriques

David Wiedemann

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.

1.0.1 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]

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*
> $$r < q$$

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

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

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

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* $s = q - 1$

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

1.1 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.

Preuve

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 :

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) $A, B \subseteq C$

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

Lecture 2: Applications entre ensembles

Tue 22 Sep

2 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 $\phi : A \to B$

1. *injective :*
$$\phi(a) = \phi(b) \iff a = b$$
2. *surjective*
$$\forall b \in B \exists a : \phi(a) = b$$
3. *bijective* $\iff$ *injective et bijective*
L'inverse
$$\phi^{-1} : B \to A \iff \phi(a) \qquad = b$$
4. *Image*
$$\phi(A) = \{\phi(a) | a \in A\} \subseteq B$$
5. $\phi : A \to B, \xi : B \to C$, *alors*
$$(\xi \circ \phi)(a) = \xi(\phi(a))$$
L'ordre est etrange.

Proposition 4 (Surjectivite de la composition)
(i) ξ *surjectif*
(ii) ϕ *pas necessairement* $\iff$ *il existe un contre exemple.*

Preuve
(i) $\forall c \in C : \exists a : \xi(\phi(a)) = c$
Donc $\exists b := \phi(a) \Rightarrow \xi(b) = c$
(ii) □

2.1 Relations d'equivalence

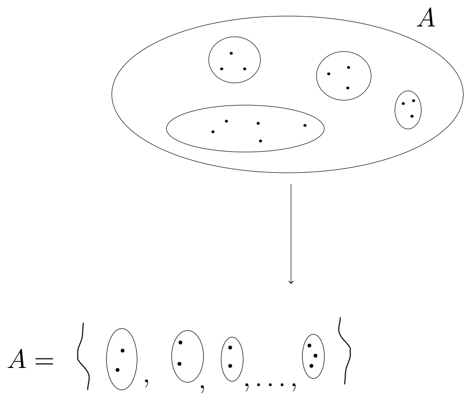

FIGURE 1 – schema relation d equivalence

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 (Exemple de transitivite)
$A = \mathbb{Z}$, alors :

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

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

2. $(a, b) \in R \Rightarrow (b, a) \in R$

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

   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 (Cas de relation d'equivalence)
$m = 3$ et R la relation d'equivalence precedente.

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

Alors :

$$\begin{aligned} R \supseteq & (0.3) \\ & (1, 4) \\ & (1, 7) \\ & (11, 8) \end{aligned}$$

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

$$\begin{aligned} R_1 = \{\dots, -5, -2, 1, 4, 7, \dots\} = 1 + 3\mathbb{Z} \\ R_0 = 3\mathbb{Z} \\ R_2 = \{\dots, -4, -1, 2, 5, \dots\} \\ A/R = \{3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2\} \end{aligned}$$

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 $|R| = \kappa$

Exemple

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

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

$$\phi : \begin{array}{l} 0 \leq x \mapsto 2x \\ 0 > x \mapsto -2x - 1 \end{array}$$

Devoir : montrer que ϕ est une bijection.

Theorème 8 (Cantor-Schroeder-Bernstein)

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

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

Lemme 9

Si il existe

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

Ou g et f sont des injections.

Alors il existe une bijection $A \mapsto B$

Preuve

$$Y_A := A \setminus X = g(Y)$$
$$X_B = f(X)$$
$$Y = B \setminus f(x)$$

Union disjointe $B = Y \perp X_B$ □

Preuve

$f : A \hookrightarrow B$ et $g : B \hookrightarrow A$.

Il faut : X tq :

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

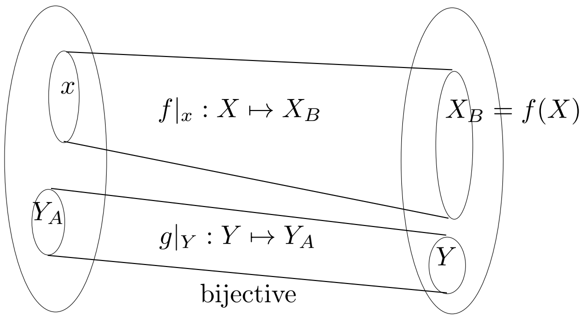

FIGURE 2 – preuve fonction bizarre

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

$$\begin{aligned}
&\Rightarrow B \setminus f(x) \supseteq B \setminus f(Z) \\
&\Rightarrow g(B \setminus f(x)) \supseteq g(B \setminus f(Z)) \\
&\Rightarrow A \setminus g(B \setminus f(x)) \supseteq g(B \setminus f(Z)) \\
&\Rightarrow A \setminus g(B \setminus f(Z)) \subseteq A \setminus g(B \setminus f(x)) \\
&\Rightarrow H(X) \subseteq H(Z)
\end{aligned}$$ □

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

Lecture 3: mardi

Tue 29 Sep

Preuve

C'est suffisant de montrer que

$$H(W) = W$$

On montre la double inclusion $\subset$:
$W \subseteq \bigcap_{x \subseteq A, H(X) \subseteq X} X$, *alors*

$$\begin{aligned}
H(W) &\subseteq \bigcap_{x \subseteq A, H(X) \subseteq X} H(X) \\
&\subseteq \bigcap_{x \subseteq A, H(X) \subseteq X} X = W
\end{aligned}$$

$\supseteq$:
$H(W)$ *est un* X *comme dans la definition de* W.

$$\Rightarrow W \subseteq H(W)$$ □

Question :
$|\mathbb{R}| = \omega_1$?
Hypothese du continu
On peut montrer qu'on ne peut pas demontrer ca.

3 Theorie des nombres

3.1 Algorithme d'Euclide

Definition 7
$a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0,$ alors

$$\underbrace{(a,b)}_{\text{plus grand commun diviseur}} = \left\{c \in \mathbb{Z}^{>0} | \ c|a, c|b\right\}$$

Cette valeur existe car il y a une borne superieure donnee par $|b|$.

Lemme 10
$a_1, b \in \mathbb{Z}, a \neq 0, r \in \mathbb{Z}$

$$(a,b) = (a, b + ra)$$

Preuve
Si qqchose divise a et b, il divse aussi a. Il divise aussi b + a

$$(b + ra) - ra = b$$

Detail dans les notes moodle □

Definition 8 (Algorithme d'Euclide)
$a, b \in \mathbb{Z}^0$, soit

$$a_1 := \max\{a, b\}$$
$$a_2 := \min\{a, b\}\ i := 2$$

Pas recursif :
Si $qi|q_{i-1} \rightarrow$ on arrete et on pose $t := i$.
Sinon $q_{i-1} = s_i q_i + q_{i+1}$

$$q_i \not| q_{i-1} \Rightarrow q_{i+1 \neq 0}$$
$$\textit{et } q_{i+1} < q_i$$

$$q_1 > q_2 > q_3 > \ldots q_t > 0, \ \textit{avec } q_i \ \textit{entier}$$

Lemme 11
$\exists m, n \in \mathbb{Z}$ tel que
$$am + bn = q_t$$

Preuve
On demontre que q_i
$$m_i q_i + n_i q_{i+1} = q_t$$
On utilise l'induction descendante sur i. $\exists m_i, n_i \in \mathbb{Z}$
$i = t - 1$
$$1q_t + 0q_{t-1} = q_t$$
Pas d'induction

$$q_i = s_o q_{i+1} + q_{i+2}$$
Par hypothese d'induction
$$\underbrace{m_{i+1}q_{i+1} + n_{i+1}q_{i+2}}_{=m_{i+1}q_{i+1}+n_{i+1}(q_i - s_{i+1}q_{i+1})} = q_t$$
$$= \underbrace{n_{i+1}}_{m_i} q_i + \underbrace{(m_{i+1} - n_{i+1}s_{i+1})}_{n_i} q_{i+1}$$

□

Lemme 12
$q_t | q_i$ pour chaque i.

Preuve
On demontre de la meme facon que le lemme d'avant avec induction descendante. □

On peut combiner les deux lemmes : donc
$$(a, b) | q_t$$
$$q_t | (a, b)$$
Donc l'algorithme d'Euclide donne le pgcd.

3.2 Theoreme fondamental de l'arithmetique

Definition 9 (Entier)
Soit $p \geq 2$ un entier

1. *p irreductible si pour chaque $a|p \Rightarrow a = 1$ ou $a = p$, $a \in \mathbb{N}$*
2. *p premier : $\forall a, b \in \mathbb{Z}^{>0}$*
$$p | a.b \Rightarrow p | a \text{ ou } p | b$$

Lemme 13
$q, a, b \in \mathbb{Z}^{>0}$

$$q|a.b \ et \ (q,a) = 1$$
$$\Rightarrow q|b$$

Preuve
$(q, a) = 1$

$$1 = mq + na \ ,avec \ m, n \in \mathbb{Z}$$
$$b = mqb + nab$$
$$\Rightarrow q|b$$

□

Proposition 14
Soit $p \geq 2$ *entier*
p *irreductible* $\iff$ p *premier*

Preuve
$\Leftarrow$
On veut montrer que $a.b = p, \Rightarrow a = 1$ *ou* $b = 1$ *On sait que* p *premier*

$$p|a.b \Rightarrow p|a \ ou \ p|b$$

$$\underbrace{\Rightarrow}_{a,b \geq p} p|a \ ou \ p|b$$

$\Rightarrow$ *:*
p *irreductible*

$$p|ab$$

Deux possibilites :

1. $p|a$ *on a fini*
2. $p \not| a \Rightarrow (p, a) \neq p$
   p *irreductible (* $(p, a)|p$*), donc*

   $$(p, a) = 1$$

   Donc $\Rightarrow p|b$

□

Theorème 15
$n \in \mathbb{Z}^{>0}$,

$$n = \prod_{i=1}^{r} p_i, \ avec \ p \ premiers$$

et c'est unique modulo l'ordre des premiers

Preuve
Existence
Induction sur n
$n = 2$ *premier donc verifie.*
Pas d'induction : 2 possibilites :

- n *premier* $\Rightarrow p_1 = n, r = 1$
- n *n'est pas premier* $\Rightarrow$ *pas irreductible*
  $\Rightarrow a.b = n$
  tel que $a, b < n$
  $\Rightarrow a = \prod p_i$ *et* $b = \prod p_i$, *donne la decomposition pour* n.

Unicite

$$n = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j, \text{ avec } r \leq s$$

- $s = 1 \Rightarrow r = 1$ *verifie*
- $s > 1$, *alors*

$$q_1 | \prod_{i=1}^{r} p_i$$

  $\Rightarrow q_1$ *premier*

$$\Rightarrow \forall l : q_1 | p_l$$

  donc

$$\frac{n}{q_1} = \prod_{i=1, i \neq l}^{r} p_i = \prod_{j=2}^{s} a_j$$

□

Lecture 4: mardi moitie

Tue 06 Oct

4 Théorie des Groupes

4.1 Groupe symmétrique de n

Le groupe $Bij(X)$ pour $X = \{1, \ldots, n\} \to S_n$

$$\sigma \in S_n \to \begin{pmatrix} 1 & 2 & \ldots n & \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

La multiplication (loi de composition) est simplement la composition des applications, attention le groupe n'est pas abélien.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Dans l'autre sens :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Les autres exemples seront contruit par une relation d'équivalence, on note

$$G/R$$

Question :
Quand est-ce que G/R est-il un groupe ?
Construction :

$$[g] = R_g = \{h \in G | (g, l) \in R\}$$

la classe de G.
Multiplication sur $\frac{G}{R}$
Soit $x, y \in G/R$, alors

$$x = [g], y \in [f]$$

On définit

$$x \cdot y := [g \cdot f]$$

Problème on peut choisir différents représentatifs.
Donc Pour que la définition sooit sensée, iil faut que

$$[g \cdot f] = [g' \cdot f'] (\forall (g, g') \in R (f, f') \in R)$$

Pour l'inverse

$$\begin{aligned} x &\in G/R \\ x &= [g] \\ x^{-1} &= [g^{-1}] \end{aligned}$$

Elément neutre de G/R :
$[e] \in G/R$

Proposition 16
La définition précédente nous donne une structure de groupe sur G/R.

Les opérations sont bien définies.

$$(g, g') \in R (h, h') \in R \Rightarrow (g.h, g'.h') \in R$$

$$(g, g') \in R \Rightarrow (g^{-1}, (g')^{-1}) \in R$$

Preuve
Il faut vérifier les 3 conditions de groupe.

— *(associativité)*

$$x \cdot (y \cdot z) = [g] \cdot [f \cdot h] = [g \cdot f] \cdot [h] = (x \cdot y) \cdot z$$

Les deux autres propriétés sont laissées en exercice. □

Exemple ($G = \mathbb{Z}, +$)
Soit

$$R = \{(x, y) \in \mathbb{Z} | m | x - y\}$$

$$G/R = \{m \cdot \mathbb{Z}, m\mathbb{Z} + 1, \ldots, m\mathbb{Z} + (m - 1)\}$$

Les éléments sont de G/R sont des éléments et des groupes.
Il faut vérifier que $+$ et $-$ sont bien définis par rapport à R et ainsi on obtien le groupe

$$(\mathbb{Z}/m\mathbb{Z}, +)$$

Lecture 5: mardi

Tue 13 Oct

4.2 Construction de Groupes avec des quotients

Exemple

$$G = (\mathbb{Z}, +)$$

On dénote

$$G/_R = \{R_x | x \in G\} = \{[x] | x \in G\}$$

Dans ce cas

$$\mathbb{Z}/_{m\mathbb{Z}} = \{m\mathbb{Z}, m\mathbb{Z} + 1, \ldots, m\mathbb{Z} + m - 1\}$$

4.2.1 Recette générale

Construction de la structure de groupes sur $G/_R$
— Représentant

$$x \in G/_R$$

g est un représentant de x si $x = [g]$.
— $[g] \cdot [f] = [g \cdot f]$
— $[g]^{-1} = [g^{-1}]$

— $e_{G/R} = [e]$
Il faut que ce soit bien défini, donc si

$$(g, g') \in R, (f, f') \in R$$

Alors

$$(g.f, g'.f') \in R$$

De même, si $(g, g') \in R$

$$\Rightarrow (g^{-1}, g'^{-1}) \in R$$

Exemple
$(\mathbb{Z}/m\mathbb{Z}, +)$
Il faut vérifier la condition la condition.

— $(g, g') \in R, (f, f') \in R \implies (g.f, g'.f') \in R$, *alors*

$$m|g - g' \text{ et } m|f - f' \text{ et } m|g + f - (g' + f')$$

— $(g, g') \in R$, *alors* $(g^{-1}, g'^{-1}) \in R$, *en effet*

$$m|g - g' \text{ et } m| - g - -g'$$

Donc on a vérifié que c'est un groupe.

Exemple
$\mathbb{Z}/m\mathbb{Z}^{\times}$
pas stable avec la multiplication.

Par contre $(\mathbb{Z}/m\mathbb{Z}, \bullet)$ monoide avec $[1]$ l'élément neutre. Mais $[0]^{-1}$ n'existe pas
Donc il faut jeter les classes qui n'ont pas d'inverses,i.e. tous les éléments sauf $[p]$, p premiers.
Donc

$$\left\{[g] \in \mathbb{Z}/m\mathbb{Z} | (g, m) = 1\right\} = (\mathbb{Z}/m\mathbb{Z})^{\times} \subseteq \mathbb{Z}/m\mathbb{Z}$$

Pour le moment, il s'agit que d' un sous-ensemble
On veut voir que la structure de monoide induit une structure de groupe sur $\mathbb{Z}/m\mathbb{Z}$.
$[g], [f] \in (\mathbb{Z}/m\mathbb{Z})^{\times} \Rightarrow [g.f] \in (\mathbb{Z}/m\mathbb{Z})^{\times}$
Autrement dit $(g, m) = 1(f, m) = 1 \Rightarrow (g.f, m) = 1$
Clairement, $\{1\} \in (\mathbb{Z}/m\mathbb{Z})^{\times}$
De plus, soit $[g] \in (\mathbb{Z}/m\mathbb{Z})^{\times}$, on veut montrer que

$$\Rightarrow [g^{-1}] \in (\mathbb{Z}/m\mathbb{Z})^{\times}$$

autrement dit,

$$(g, m) = 1 \implies \exists f \in \mathbb{Z}, \exists x \in \mathbb{Z} \text{ tel que } g.f = 1 + mx$$

Ce qui est immédiat, par Bézout.
Donc $(\mathbb{Z}/m\mathbb{Z})^{\times}$ est un groupe !

Definition 10 (Homomorphismes de groupes)
Soient G, H deux groupes.
Une application

$$\phi : G \to H$$

est un homomorphisme si

$$\forall g, f \in G : \phi(g.f) = \phi(g).\phi(f)$$

ϕ est un endomorphisme si ϕ est un homomorphisme

$$\phi : G \to G$$

ϕ est un isomorphisme si

$$\phi : G \to H$$

est un homomorphisme bijectif.
G et H sont isomorphes si il existe

$$\phi : G \to H$$

un isomorphisme. On note

$$G \simeq H$$

Lemme 21

$$\phi : G \to H$$

un homomorphisme, alors

$$\phi(g^n) = \phi(g)^n$$

Preuve
pour n=0 :

$$\text{à montrer : } \phi(e_G) = e_H$$

$$e_H \cdot \phi(g) = \phi(g) = \phi(e_G.g) = \phi(e_G)\phi(g)$$

Donc $e_H = \phi(e_G)$.
Pour $n > 0$:

$$\phi(g^n) = \phi(g. \dots .g) = \phi(g). \dots .\phi(g) = \phi(g)^n$$

Pour $n < 0$:
On a démontré la semaine passée

$$\phi(g)^n \cdot \phi(g)^{-n} = phi(g)^0 = e_H$$

$$\textit{Il suffit de montrer que}$$
$$\phi(g^{n)} \textit{ est aussi un inverse de } \phi(g)^{-n}$$
$$\phi(g^n)\phi(g^{-n}) = \phi(g^n g^{-n}) = \phi(e_G) = e_H$$
□

Exemple

— $(G,+)$ *abélien,* $n \in \mathbb{N}$

$$G \ni x \mapsto n.x$$

C'est un homomorphisme car

$$n(x+y) = nx + ny$$

—

$$\phi : \mathbb{Z} \mapsto G$$

quelconque, alors

$$\phi(n \cdot 1) = \phi(1)^n \forall n \in \mathbb{Z}$$

Autre direction :
Est-ce qu'il existe

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

tel que

$$\phi(1) = g$$

Il y a une seule possibilité que ce soit le cas, quand

$$\phi(n) = g^n$$

C'est un homomorphisme :

$$g^n g^m = g^{n+m}$$

Cet homomorphisme existe donc, et il est uniquemenent determinem on l'appelle

$$dexp_g$$

pour "exponentielle discrete"

Lecture 6: Th. des Groupes

Tue 20 Oct

4.3 Produits de Groupes

4.4 Produits de Groupes

Definition 11

Soit G, H *deux groupes*

$$G \times H = \{(g,h) | g \in G, h \in H\}$$

si $|G|, |H| < \infty$*, alors* $|G \times H| = |G| \cdot |H|$*, on munit* $G \times H$ *d'une structure de groupe avec la loi*

$$(g,h) \cdot (g',h') = (g',h')$$

Lemme 23
C'est un groupe avec

- $e_{G\times H} = (e_G, e_H)$
- $(g,h)^{-1} = (g^{-1}, h^{-1})$

Preuve
En exo □

4.5 Propriété universelle des Produits

Si on a $G \times H$, on a deux projections (homomorphismes) naturels

$$F \times H \underbrace{\rightarrow}_{pr_H} H$$
$$pr_F((f,h)) = f$$
$$pr_H((f,h)) = h$$

Ce sont trivialement des homomorphismes.

Proposition 24
Soit G, F, H des groupes

$$F \times H \underbrace{\rightarrow}_{pr_H} H$$
$$et$$
$$F \times H \underbrace{\rightarrow}_{pr_F} F$$
$$de\ plus\ soit\ \beta : G \rightarrow H$$
$$\alpha : G \rightarrow F$$

Il existe un homomorphisme unique

$$\gamma : G \rightarrow F \times H$$

tel que les compositions ci-dessus commutent.

$$
\begin{tikzcd}
 & H \\
G \arrow[ur, "\alpha"] \arrow[r, "\gamma"] \arrow[dr, "\beta"'] & F \times H \arrow[u] \arrow[d] \\
 & F
\end{tikzcd}
$$

FIGURE 3 – diagrammes produits

Donc que

$$\alpha = pr_F \circ \gamma \text{ et } \beta = pr_H \circ \gamma$$

Donc

$$\alpha(g) = pr_F(\gamma(g)) = pr_F(f, h) = f$$

De plus

$$\beta(g) = pr_H(\gamma(g)) = pr_H(f, h) = h$$

Donc

$$\gamma(g) = (\alpha(g), \beta(g))$$

Preuve

Il faut montrer que γ est un homomorphisme.

$$
\begin{aligned}
\gamma(g)\gamma(g') &= (\alpha(g), \beta(g)) \cdot (\alpha(g'), \beta(g')) \\
&= (\alpha(g)\alpha(g'), \beta(g)\beta(g')) \\
&= (\alpha(gg'), \beta(gg')) = \gamma(gg')
\end{aligned}
$$

On a utilisé que la composition d'homomorphismes est un homomorphisme. □

Utilisation

Regardons les homomorphismes de

$$\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

est la meme chose que considérer les morphismes de

$$\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

et

$$\mathbb{Z} \to {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}}$$

On peut par exemple prendre l'exponentielle discrete de $\mathbb{Z} \to {}^{\mathbb{Z}}\!/\!_{2\mathbb{Z}}$ et $\mathbb{Z} \to {}^{\mathbb{Z}}\!/\!_{2\mathbb{Z}}$ et les combiner.
On ne doit pas vérifier que la "composition" est un morphisme car on l'a montré dans la propriété universelle.

4.6 Sous-groupes

Definition 12 (Sous-Groupe)
Soit $(G, \cdot)$ un groupe et $H \subseteq G$ un sous-ensemble.
H est un sous-groupe si

1. $\{h \cdot h' | h, h' \in H\} = H \cdot H \subseteq H$
2. $\cdot|_H : H \times H \to H$ *nous donne un groupe sur* H.

Proposition 25
Soit $H \subseteq (G, \cdot)$ un sous-ensemble.
C'est un sous-groupe si et seulement si

1. $H \neq \emptyset$
2. $h, g \in H \implies h.g \in H$
3. $h \in H \implies h^{-1} \in H$

De plus, les éléments neutres de G et de H sont les mêmes, inverses aussi

Preuve
$\Rightarrow$

1. $e_H \in H \Rightarrow H \neq \emptyset$
2. *Vrai*
3. *Il faut démontrer que*
$$e_H = e_G$$
En effet
$$e_H \cdot e_H = e_H = e_G \cdot e_H$$
Or on peut simplifier, donc
$$e_H = e_G$$

$\Leftarrow$
Il faut démontrer que $e_G \in H$. En effet
$$H \neq \emptyset \Rightarrow \exists g \in H \Rightarrow g^{-1}g = e_G \in H$$ □

Exemple

1. *Sous-groupes triviaux*

$$\{e\} \subseteq G$$
$$G \subseteq G$$

2. $\{1, -1\} \subseteq (\mathbb{Q} \setminus \{0\}, \cdot)$
3. $m\mathbb{Z} = \{mx | x \in \mathbb{Z}\} \subseteq (\mathbb{Z}, +)$
4. $\mathbb{Z}/_{n\mathbb{Z}}, m|n$ *être divisible par* m *est bien définit sur les classes d'équivalences, autrement dit*

$$x, y \in \mathbb{Z}, n|x - y \text{ alors } m|x \iff m|y$$

Donc

$$\left\{[x] \in \mathbb{Z}/_{n\mathbb{Z}} | m|[x]\right\} \subseteq \mathbb{Z}/_{n\mathbb{Z}}$$

est un sous-groupe.

Definition 13

Soit

$$\phi : G \to H$$

un morphisme.

1. *noyau :*

$$\ker \phi = \{g \in G | \phi g = e_H\} \subset G$$

2. *image :*

$$Im\phi = \{\phi(g) | g \in G\} \subset H$$

Proposition 27

L'image et le noyau sonnt des sous-groupes.

Preuve

La preuve pour l'image est dans le cours.

$$\ker \phi \neq \emptyset, \text{ car } \phi(e_G) = e_H$$

On démontre que c'est stable par composition

$$g, f \in \ker \phi$$

, alors

$$\phi(g.f) = \phi(g).\phi(f) = e_H \cdot e_H e_H$$

On vérifie que c'est stable par inversion.

$$g \in \ker \phi$$
$$\phi(g)^{-1} = \phi(g^{-1})$$

donc c'est fini. □

Lecture 7: theorie des groupes

Tue 27 Oct

Supposons $o(g) \neq \infty$, alors on note

$$|\langle g \rangle| = 0(g)$$

On remarque que

$$g^n = (g^{0(g)})^r \cdot g^s$$

Proposition 28
$\phi : G \to H$ avec

$$\ker \phi = \{e\}$$

Alors ϕ injectif.

Preuve
Soient $g, h \in G$.
Supposons $\phi(g) = \phi(h)$. On a

$$\phi(g^{-1}h) = \phi(g^{-1})\phi(h) = \phi(g)^{-1}\phi(h) = e$$

Donc $g^{-1}h \in \ker \phi$ Donc

$$\begin{aligned} g^{-1}h &= e \\ g &= h \end{aligned}$$

□

4.7 L'homomorphisme sgn

Rappelons que un cycle $\sigma \in S_n$ tel que $\exists a_1, \ldots, a_r$ éléments différents de

$$\{1, \ldots, n\}$$

$$\begin{aligned} \sigma(a_1) &= a_2 \\ &\vdots \\ \sigma(a_{r-1}) &= a_r \\ \sigma(a_r) &= a_1 \\ \sigma(i) &= i \text{ sinon} \end{aligned}$$

Proposition 29
Soit $\sigma \in S_n$, avec σ un produit de cycles disjoints de taille ≥ 2.
Cette décomposition est unique modulo l'ordre des cycles

Proposition 30
$\sigma \in S_n$, alors on peut ecrire σ comme un produit de transpositions.

Preuve
Il suffit de poser

$$\sigma = (a_1 \dots a_r)$$

On peut écrire σ comme produit de transpositions.
Induction sur r

— $r = 2$

On peut simplement envoyer chaque élément sur son prochain. □

Definition 14 (sgn)

$$\operatorname{sgn} : S_n \to \{-1, 1\}$$

On dénote

$$\operatorname{sgn} \sigma = (-1)^{\left|\left\{(i,j)\in\mathbb{N}^2 | 1\leq j<i\leq n, \sigma(j)<\sigma(i)\right\}\right|}$$

Lemme 31
$\sigma \in S_n$ et

$$1 \leq r < s \leq n$$

On définit

$$\tau = \sigma(rs)$$

Alors

$$\operatorname{sgn}(\tau) = -\operatorname{sgn}(\sigma)$$

Preuve
Si on applique (rs) les autres éléments restent les mêmes.
On a donc que

$$\tau(r) = \sigma(s) \text{ et } \tau(s) = \sigma(r)$$

— *$i \neq j \notin \{r, s\}$ implique*

$$\sigma(i) = \tau(i)$$
$$\sigma(j) = \tau(j)$$

Pas de changement.

— *Soit $j < r$ ou $j > s$, alors Donc j et r sont en inversion pour σ si et seulement si j et s sont en inversions pour τ Donc il n'y a pas de contribution au nombre de paires d'inversions.*

— *Si $r < j < s$, alors r et j pour τ est le même que s et j pour σ. (car $\tau(r) = \sigma(s)$ et $\tau(j) = \sigma(j)$)*

et s et j sont en inversion pour τ si et seulement si r et j ne sont pas en inversion pour τ

Si r et s sont en inversion pour τ si et seulement si r et s ne sont pas en inverson pour σ □

Corollaire 32

sgn *est un homomorphisme*

Preuve

$\sigma, \tau \in S_n$, alors

$$\operatorname{sgn}(\sigma\tau) = (-1)^{r+s} = \operatorname{sgn}\sigma \operatorname{sgn}\tau$$ □

Lecture 8: 3 Novembre

Tue 03 Nov

4.8 Theoreme de Lagrange

Definition 15

Soit $H \leq G$, une classe à gauche (resp. à droite) est un sous-ensemble

$$g.H = \{g.h | h \in H\}$$

Ce n'est pas forcément un sous-groupe.

Exemple

Soit $G = S_3$,

$$H = \{\langle(12)\rangle\} = \{id, (12)\}$$

Regardons les classe à gauche

1. $g = Id$

$$Id.H = \{Id, (12)\} = (12).H$$

2. $g = (13)$

$$(13).H = \{(13), (123)\}$$

3.

$$(23).H = \{(23), (132)\}$$

Lemme 34

$$|gH| = |H| \forall g \in G$$

Preuve

$$\beta : x \mapsto g^{-1}x$$

et

$$gy \leftarrow y : \alpha$$

Ces deux applications sont inverses $\Rightarrow$ ils sont en bijection. $\square$

> **Proposition 35**
> *Soit $H \leq G$.*
> *On définit*
> $$R = \{(g,f) \in G \times G | g^{-1}f \in H\} \subseteq G \times G$$
> *Alors*
> 1. *R est une relation d'équivalence*
> 2. *les classes d'équivalence de R sont les classes à gauche*

Preuve

1. *reflexivite $g^{-1}g = e \in H$ donc $(g,g) \in R$*
2. *Symétrie $(g,f) \in R$ donc $g^{-1}f \in H$*
$$f^{-1}g = f^{-1}(g^{-1})^{-1} = (g^{-1}f)^{-1} \in H$$
3. *Transitivité $(g,f) \in R$, $(f,h) \in R$, alors $g^{-1}f, f^{-1}h \in H$,*
$$g^{-1}h = g^{-1}ff^{-1}h \in H$$
Donc $(g,h) \in R$

On veut $R_g = gH$

$$R_g = \{f \in G | (g,f) \in R\} = \{f \in G | g^{-1}f \in H\} = \{f \in G | \exists x \in H : f = gx\} = gH$$

$\square$

En somme :
$H \leq G$
Les classes à gauche

- Ont les même tailles
- $H_1, \ldots, H_r$ sont les classes à gauche
$$G = \amalg_i H_i$$
La notation $\amalg_i$ signifie que l intersection deux-à-duex est vide.
Donc, si G est fini
$$|G| = \sum |H_i| = r|H|$$

Theorème 36 (Lagrange)
G est fini et $H \leq G$, alors
$$|H|\big||G|$$
De plus $\frac{|G|}{|H|} =$ *nombre de classes à gauche* $= [G : H]$

Corollaire 37
$g \in G$, alors
$$\Rightarrow o(g)\big||G|$$

Preuve
$H = \langle g \rangle$ et ensuite on utilise Lagrange. □

Definition 16
G groupe est cyclique si il existe $g \in G$ tel que
$$\langle g \rangle = G$$

Corollaire 38
$|G| = p > 0$ avec p premier, alors G cyclique

Preuve
$g \in G \setminus \{e\}$, donc
$$1 < o(g)|p$$
par Lagrange.
Donc $o(g) = p$ et donc $\langle g \rangle = G$. □

Theorème 39 (Petit theoreme de Fermat)
Soit $m > 0$ et a entier, avec
$$(a, m) = 1$$
Alors
$$a^{\phi(m)} \equiv 1(m)$$

Preuve
On sait que
$$[a] \in \left(\mathbb{Z}/m\mathbb{Z}\right)^{\times}$$
Donc par lagrange
$$o([a])|\phi(m)$$
et donc
$$[a]^{\phi(m)} = [1] = [a^{\phi(m)}]$$ □

Prenons un groupe G

et une relation d'équivalence R sur G.

On a vu que

$$G/_{R}$$

est un groupe si la multiplication et l'inverse sont bien définis.

Dans ce cas

$$[g] \cdot [h] = [gh]$$

Il est équivalent de demander que

$$\begin{aligned} \xi : G &\to G/R \\ g &\to Rg \end{aligned}$$

est un homomorphisme de groupe et donc

$$R_g \cdot R_h = R_{gh}$$

On applique çà aux classes à gauche

$$R = \left\{ (g, f) | g^{-1} f \in H \right\}$$

On essaie de tourner

$$G/R = \{ \text{ classes à gauche } \}$$

C'est nécessaire que

$$\begin{aligned} \xi_h : G &\to G/H \\ g &\to gH \end{aligned}$$

est un homomorphisme.

$$\ker \xi_h = H$$

Quelles conditions est-ce que ca pose ?

Definition 17

$H \leq G$ est <u>normal</u> si $\forall g \in G$

$$\forall h \in H$$

on a

$$g^{-1} h g \in H$$

On appelle ceci le conjugué de h par g.

Definition 18 (Groupe simple)

Si $H \leq G$ normal $\Rightarrow$ H trivial.

Proposition 40
Soit $\phi : G \to H$ *un homomorphisme, alors le noyau de cet homomorphisme est normal* $\ker \phi$ *est normal.*

Preuve
Soit $g \in G,\ h \in \ker \phi$

$$\phi(g^{-1}hg) = \phi(g^{-1})\phi(h)\phi(g) = \phi(g^{-1})e\phi(g) = e$$

□

Theorème 41
$H \trianglelefteq G$ *et* R *relation d'équivalence des classes à gauche de* H

G/R *un groupe et*

$$\begin{aligned} \xi_H : G &\to G/R \\ g &\mapsto gH \end{aligned}$$

un homomorphisme.