

M51 - Groupes, anneaux & corps

page
modèle?
cf

(a) Ensembles, équivalences, cardinal, dénombrabilité

1. Ensembles (N_p)

$$\Delta \text{ diff } \emptyset \leftrightarrow \{\emptyset\}.$$

2. Cardinal, dénombrabilité

2.1. Cardinal

(b) 2 ens E & F st équipotents s'il y a bijet de l'1 vers l'autre. Si eq^+ : ils ont même cardinal.

(c) un ens non vide E est fini si $\exists m \in \mathbb{N}^*$ tq E soit équivalent à l'ens $\{1, 2, \dots, m\}$.
on dit Card E = m.

D.4.0 | Déf des entiers

On pose $0 = \text{card}(\emptyset)$

$$1 = \text{card}\{\emptyset\}$$

$$2 = \text{card}\{0, 1\}$$

:

$$\dots m+1 = \text{card}\{0, 1, \dots, m\}$$

$1 \neq 0$ sinon $\text{card}\{\emptyset\} = \text{card} \emptyset$

i.e. $\{\emptyset\}$ & \emptyset st équipotents

i.e. \exists une biject $\{\emptyset\} \rightarrow \emptyset$

cela est contradictoire.

non-vide

Il n'y a pas biject \leftrightarrow ens \emptyset & ens $\{1\}$.

\rightarrow On montre généralement que $m+1 \notin \{0, 1, \dots, m\}$.

[R9] On montre aussi (PR) que si $\text{card}(E) = m$ & $F \subset E$ alors $\text{card}(F) \in \{0, 1, \dots, m\}$.
Dès lors, si $\text{card } F = m \Rightarrow \text{card } E = F$.

[P] $\mathbb{N} = \{ \text{les cardinaux obtenus par ce procédé} \}$

(P) Soit E un ens. Ainsi:

(i) \exists inject $\mathbb{N} \xrightarrow{i} E$

(ii) E équivalent à une partie de E distincte de E

(iii) $\forall n \in \mathbb{N}, \text{card}(E) \neq n$

On dira que l'ensemble est infini.

distincte (\subset) stricte, propre.

@ \mathbb{N} est infini : $\begin{cases} \mathbb{N} \rightarrow \mathbb{N}^* \\ n \mapsto n+1 \end{cases}$ est une biject.

\mathbb{N} & \mathbb{N}^* sont équipotents.

⑤ E est dit fini s'il n'est pas infini.

Preuve de (i) \Leftrightarrow (ii) \Leftrightarrow (iii)

(i) \Rightarrow (ii) On suppose i. On a

$$E = i(N) \cup (E \setminus i(N))$$

car a
n'est
pas
sujet à f .

Considérons l'application :

$$\begin{aligned} f: E &\longrightarrow E \\ x &\longmapsto \begin{cases} \text{si } x \notin i(N), & f(x)=x \\ \text{si } x \in i(N), & \end{cases} \end{aligned}$$

$\rightarrow \exists ! n \in \mathbb{N}$ tq $x = i(n)$, on pose alors
 $f(x) = i(n+1)$.

g à l'injection de i .

• f est injective. Soit $x, y \in E$ tq
 $f(x) = f(y)$.

Il est impossible que $x \in i(\mathbb{N})$ ($\Rightarrow f(x) \in i(\mathbb{N})$)
et dc $f(x) \neq f(y)$.
 $\Rightarrow f(y) = y \notin i(\mathbb{N})$

• $y \in i(\mathbb{N})$ (idem)
et $x \notin i(\mathbb{N})$

Reste 2 cas :

$$f(y) = y$$

cas 1 : $x, y \notin i(\mathbb{N})$ alors $f(x) = x$ & dc $x = y$.

cas 2 : $x, y \in i(\mathbb{N})$

$$x = i(n) \quad f(n) = i(n+1)$$

$$y = i(m) \quad f(m) = i(m+1)$$

$$f(n) = f(m) \Rightarrow n+1 = m+1 \Rightarrow n = m \Rightarrow i(n) = i(m)$$

ie $x = y$.

⑥ Ccl f est une bijection entre E & $f(E)$
ie E équipotent à $f(E)$ qui est une partie
(distincte) propre de E . ($i(0) \notin f(E)$)

(ii) \Rightarrow (iii), mq mon (iii) \Rightarrow mon (ii)

(y réfléchir en utilisant RQ précédte & Fersens.)

$$\begin{aligned} E &\longrightarrow P(E) \\ x &\longmapsto \{x\} \end{aligned}$$

Th.2 Cantor

(iii) \Rightarrow (i) On construit une applicat c'st:

- card $E \neq 0$ ie $E \neq \emptyset$.

On choisit $e_0 \in E$ & on pose $i(0) = e_0$.

card(E) $\neq 1$ dc $E \neq \{e_0\}$. On choisit $e_1 \in E$ tq $e_1 \neq e_0$.

On pose $i(1) = e_1$.

- card(E) $\neq 2$ dc $E \neq \{e_0, e_1\}$...

... & ainsi de suite

soit E un ens (nv) & $P(E)$ l'ens de ses parties. \nexists pas de surject de E sur $P(E)$.

?? $P(E) \rightarrowtail E$ à cause Th. Cantor.

g^o Mg \nexists injec de $P(E)$ dans E .

Voir DM Th. Cantor

Th. Cantor-Bernstein.

soit E, F 2 ens, on appelle inject $f: E \rightarrow F$ & appli inject $g: F \rightarrow E$. Alors les ens E, F st en bijec, ils ont de m cardinal.

Th. L'ens $P(E)$ des parties d'un ens E est en bijec w l'ens $\{0,1\}^E$ des appli de E ds $\{0,1\}$.
ens de ttes appli possible de E ds $\{0,1\}$.

$P(E)$ équivalent à $\{0,1\}^E$.

③ DM

at ons: les élts st applicabls.

2.2. Dénombrabilité

⑤ Un ens infini E est dit dénombrable s'il est en biject^o de l'ens \mathbb{N} , ie équivalent à \mathbb{N} .

• équivalent à $\mathbb{N} \Leftrightarrow$ ^{cot} ens et infini.

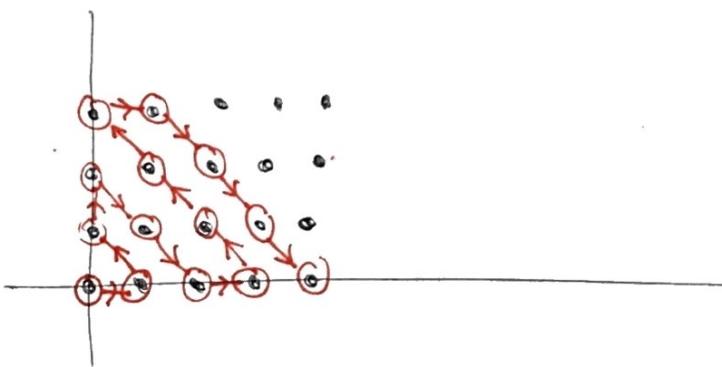
$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\text{bij}} & E \\ 1 & \mapsto & 1^{\circ} \text{ él} \\ 2 & \mapsto & 2^{\circ} \text{ él} \\ \vdots & & \end{array}$$

• ens dénombrable

$$\mathbb{N} \rightarrow 2\mathbb{N}$$

$$x \mapsto 2^n$$

$$\mathbb{N} \times \mathbb{N}$$



• P2 Tout ss-ens infini d'un ens dénombrable est dénombrable.

DM soit F un ens. dénombrable & $E \subset F$ un ens infini.

• Il existe une biject^o $f : F \rightarrow \mathbb{N}$.
(hypothèse que F est dénombrable par déf^o).

• E infini. D'après une Prop-précédente,
 \exists une inject^o $\mathbb{N} \rightarrow E$

• $\Rightarrow f|_E : E \rightarrow \mathbb{N}$
est injective

al d'après le Thm Cantor-Bernstein,
 E & \mathbb{N} st équivalents, ie dénombrables.

④ fixe
① ↗ 3 - ② ↘ 1.

C1

§2 Cardinal dénombrabilité

2.2 Dénombrabilité

(P2) ✓ Tous ensembles ∞ d'un ensemble fin. est fin.

(P3) Soit E un ensemble ∞ , on appelle q' \exists surjectif $f: \mathbb{N} \rightarrow E$ alors E fin.

NB: E infini $\Rightarrow E$ contient un ensemble fin. (dén)

(si E est infini, \exists une injectif $\mathbb{N} \rightarrow E$
Donc E contient $i(\mathbb{N})$ qui est équivalent à \mathbb{N} .)

Démonstration Prop 3: (vp)

Prop 4 Soit E, F 2 ensembles finis

\Rightarrow produit cartésien $E \times F$ est ensemble fin.

Démonstration (vp): "il suffit de montrer $\mathbb{N} \times \mathbb{N}$ est fin."
Cas général:

Soit E, F finis, soit $f: \mathbb{N} \rightarrow E$ & $g: \mathbb{N} \rightarrow F$.
& bijectifs.

Considérons l'application

$$F: \mathbb{N} \times \mathbb{N} \rightarrow E \times F$$

$$(m, n) \mapsto (f(m), g(n))$$

Montrons F est bijective

$$\begin{aligned} \text{Montrons } F \text{ injective: } & \forall (n, m), (n', m') \in (\mathbb{N} \times \mathbb{N})^2 \\ F(n, m) = F(n', m') & \Leftrightarrow (f(n), g(m)) = (f(n'), g(m')) \\ \Leftrightarrow \begin{cases} f(n) = f(n') \\ g(m) = g(m') \end{cases} & \Leftrightarrow \begin{cases} n = n' \\ m = m' \end{cases} \quad \begin{array}{l} \text{(injectivité)} \\ \text{de } f, g \end{array} \\ \Leftrightarrow (n, m) = (n', m') & \end{aligned}$$

Montrons F surjective: Soit $(x, y) \in E \times F$, f surjective
de $\exists n \in \mathbb{N}, x = f(n)$.

g surjective de $\exists m \in \mathbb{N}, y = g(m)$.

On a alors $(n, m) = F(x, y)$.

Cela F est bijective cad

$\mathbb{N}^V \times \mathbb{N}^V$ équivalent à $E \times F$

$\mathbb{N}^V \times \mathbb{N}^V$ équivalent à \mathbb{N}^V (1° cas)

D'où \mathbb{N}^V équivalent à $E \times F$.

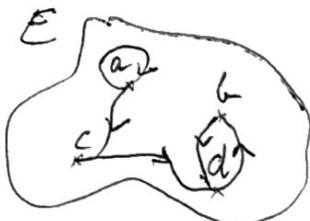
④ P5 Tte réunion de \mathbb{N} d'ens \mathbb{N} est \mathbb{N} .

DM (vp)

⑤ P6 L'ens R n'est pas \mathbb{N}
DM (vp)

§ 3. Relat's d'équivalence

3.1. Définitions



R correspond au ss-ens,
 $\{(a,a), (a,c), (c,d), (d,b), (b,d)\}$
 $C \subseteq E \times E$

⑥ Une relat' binaire R , defin si ens E est
 ss-ens $R \subseteq E \times E$, pr $(a,b) \in R$.
 On note $a R b$.

(D)
NST

⑦ E, R

$x \in E$

classe d'équivalence.

$$\bar{x} \stackrel{\text{def}}{=} \{y \in E \mid x R y\}$$

[$\bar{x} \subseteq E$ ou $\bar{x} \in \mathcal{P}(E)$]

$$E/R \stackrel{\text{def}}{=} \{\bar{x} \mid x \in E\} \subset \mathcal{P}(E)$$

(D)

NB Pr $x, y \in E$, on a :
 $(\bar{x} = \bar{y} \Leftrightarrow x R y)$

(\Rightarrow) On R y $x R x$, dc $x \in \bar{x}$
 de $x \in \bar{y}$, dc $x R y$.

(\Leftarrow) app s $x R y$

(C) Soit $z \in \bar{x}$, i.e. $z R x$ comme $x R y$
 on a aussi $z R y$ (par transitivity)
 i.e. $z \in \bar{y}$. D'où $\bar{x} \subseteq \bar{y}$.

(D) Iciem.

Congruence modulo 7 :

pr $x, y \in \mathbb{Z}$, $x \equiv y \pmod{7}$

si $x-y$ divisible par 7

ssi ils ont m̄m reste per div eucl. par 7.

$$\mathbb{Z}/_7 = \mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$$

ainsi $\bar{3} = \{7k+3 \mid k \in \mathbb{Z}\}$

(34) soit E un ens, $(A_i)_{i \in I}$ une famille de n -ens \textcircled{m} de E , on dit la famille $(A_i)_{i \in I}$ forme une partie de l'ens E si:

- $A_i \cap A_j = \emptyset \quad \forall (i,j) \in I^2 \text{ tq } i \neq j$
- $\bigcup_{i \in I} A_i = E$.

(P7) soit E ens \textcircled{m} , R \Rightarrow def sur E .
Les classes d'équivalence forment une partie de E , tte partie de E pt s'obtient de manière unique \textcircled{C} rel^o à R .

$\textcircled{C} \bar{x} \& \bar{y}$

$\exists \bar{z} \in \bar{x}, \bar{y} \in \bar{y}$

$\exists z \in \bar{x} \Rightarrow z R x$

$\exists y \in \bar{y} \Rightarrow z R y$

$\Rightarrow x R y \Rightarrow \bar{x} = \bar{y}$.

2 classes d'éq: soit E EXACTES
soit DISJOINTES.

DM (vp, ad)

3.2. Compatibilité

(D10) E, F ; $f: E \rightarrow F$. E munie \textcircled{R} .

L'appli f est compatible $\textcircled{z} R z'$

$\forall (x,y) \in E^2, x R y \Rightarrow f(x) = f(y)$.

$\textcircled{z} f$ est compatible $\textcircled{z} R$, on dit qu'elle passe au quotient, ie f propt.

(P8) $E, F, f: E \rightarrow F$, suppose f compatible $\textcircled{z} R$ def sur E .

$\exists!$ appli \bar{f} def sur E/R

tq $\forall x \in E: f(x) = \bar{f}(\bar{x})$.



(vp)

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \downarrow & & \\ E/R_0 & \xrightarrow{\bar{f}} & \end{array}$$

$\bar{f}?$ tq $\bar{f}(\bar{x}) = f(x) \quad \forall x \in E$

L'unicité démontre de $\bar{f}(\bar{x}) = f(x)$ qui détermine \bar{f} .

~~E~~ on pose $\bar{f}(\bar{x}) = f(x) \quad \forall x \in E$.

si $\bar{x} = \bar{y} = c$, $f(c) = \underline{f(x)}$ ou $f(y)$?
ils sont égaux.

$$\begin{array}{ccc} & x \mapsto f(x) & \\ x & \downarrow & \\ & E \xrightarrow{f} F & \\ \downarrow p & \swarrow \bar{f} & \\ p(x) = \bar{x} & E/R_0 & \bar{x} \end{array}$$

$\bar{f}(\bar{x}) = f(x)$

On a

$$\boxed{\bar{f} \circ P = f}$$

(9)

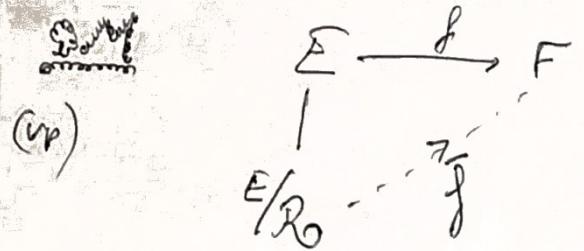
@ $f: \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto \sin(x)$

$x R y$ si $x-y = 2\pi k$ et $k \in \mathbb{Z}$.
 f est compatible avec R .

D'après la prop 8, $\exists \bar{f}: \mathbb{R}/R \rightarrow \mathbb{R}$ qui fait commuter le diagramme.

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ \downarrow p & & \nearrow \bar{f} \\ \mathbb{R}/R & & \end{array}$$

\mathbb{R}/R se note $\mathbb{R}/2\pi\mathbb{Z}$.

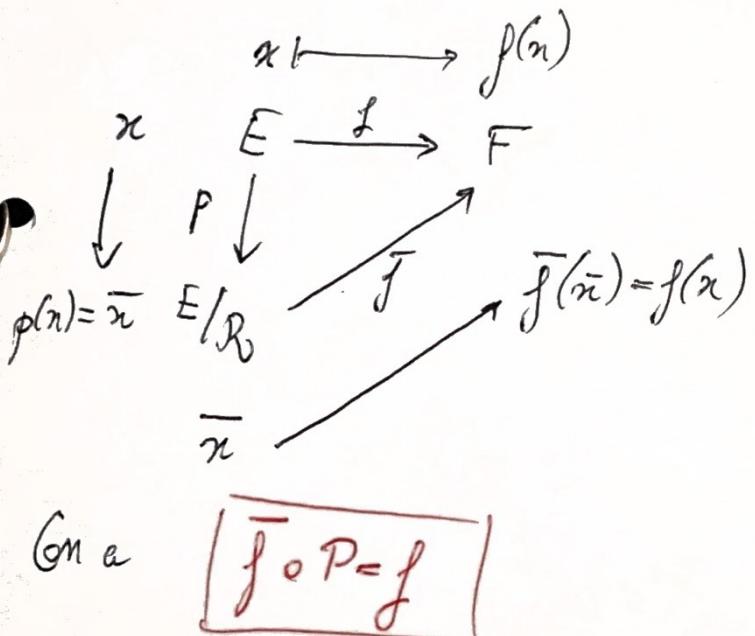


\bar{f} ? tq $\bar{f}(\bar{x}) = f(x) \quad \forall x \in E$

L'unicité démontre de $\bar{f}(\bar{x}) = f(x)$ qui détermine \bar{f} .

~~D~~ on pose $\bar{f}(\bar{x}) = f(x) \quad \forall x \in E$.

si $\bar{x} = \bar{y} = c$, $f(c) = \underline{f(x)}$ ou $\underline{f(y)}$?
ils sont égaux.



@ $f: \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto \sin(x)$

$x R y$ si $x-y = 2\pi k$ tq $k \in \mathbb{Z}$.

f est compatible avec R .

D'après la prop 8, $\exists \bar{f}: \mathbb{R}/R_0 \rightarrow \mathbb{R}$ qui fait commuter le diagramme.

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ p \downarrow & & \nearrow \bar{f} \\ \mathbb{R}/R_0 & & \end{array}$$

\mathbb{R}/R_0 se note $\mathbb{R}/2\pi\mathbb{Z}$.

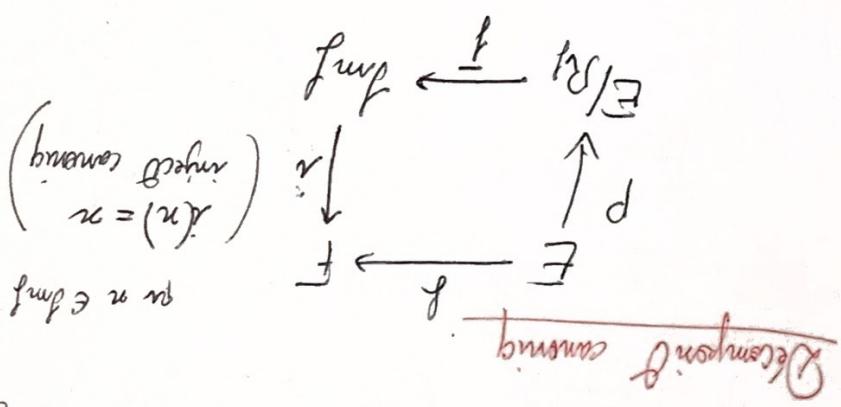
P3.10 E, F en, $f: E \rightarrow F$ appli, pr $x, y \in E$,
 $x R_0 y \Leftrightarrow f(x) = f(y)$. On sait que f passe au quotient.
 $\exists \bar{f}: E/R_0 \rightarrow F$ tq $\bar{f} \circ p = f$

La restriction $\bar{f}: E/R_0 \rightarrow \text{Im } f$
est une bijection.

(5)

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ p \downarrow & & \nearrow \bar{f} \\ E/R_0 & & \end{array}$$

(4)



b

$$\begin{aligned}
 & h = \underline{x} \Rightarrow h \in E/F \Rightarrow h \in E \quad (\underline{x})f = (x) \\
 \Leftrightarrow & (\underline{x})f = (\underline{x})f \quad \text{by } f \circ g = h \\
 & (\underline{x})f = h \quad h \in E/F \Rightarrow h \in E \\
 & (\underline{x})f = (x)f \quad h \in E \Rightarrow h \in f(E) \quad \text{by } f^{-1}(h) = x
 \end{aligned}$$

C2) Groupes

d.2. Sous-groupes

un groupe \rightarrow moy et groupe
en tenant tous que
contient tout groupe.

Def)

Opérat (fam de compo' interne)

- Def) Sous-groupe
pre H d'G est sg si
 - o H stable par opérat de G : $\forall (a, b) \in H^2, ab \in H$
 - o $\exists i \in H$
 - o $\forall a \in H, a^{-1} \in H$ ainsi (H, \cdot) est G.

Un groupe (G, \cdot)

Env's

Def) G, $H \subset G, H \neq \emptyset \Rightarrow H sg de G M
 $\forall a \in H, \forall b \in H, ab^{-1} \in H$.$

Def) M, I en nv, $(H_i)_{i \in I}$ fam sg de G
 $\Rightarrow \bigcap_{i \in I} H_i$ est sg de G .

Def) $\forall i \in I$, él't neutre e_G , $e_G \in H_i \Rightarrow e_G \in \bigcap_{i \in I} H_i$
 \therefore él't de $\bigcap_{i \in I} H_i \Rightarrow e \in H_i$ et sg de G : on a $ab^{-1} \in H_i \forall i \in I$

Def)

Commutativ'. abélien

Ex: $(\mathbb{Z}, +)$, $a = \frac{m}{n} \in \mathbb{Q}$ et $b = \frac{p}{q} \in \mathbb{Q}$ $a + b = \frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq} \in \mathbb{Q}$
ordre \Rightarrow ordinal groupe $(\mathbb{N}, +)$ pas groupe

D15) $G \circlearrowleft$, S sous-groupe de G ,

$\text{def}^{\text{de } G}$
engendré par les éléments de S .
 $\langle S \rangle = \text{intervor de tous les éléments de } G$ qui contiennent S .

1. $\langle S \rangle$ est (sg) de G . (P12) qui contient S

2. si H est (sg) de G qui contient S alors
 $\langle S \rangle \subset H$.

(H fait partie des (sg) en définissant $\langle S \rangle$).

1. et 2. $\Leftrightarrow \langle S \rangle$ est le + petit (sg) de G qui contient S .

De plus, pour $S = \{a\}$, si $a \in G$, on a:

$$\rightarrow \langle S \rangle = \{a^k, k \in \mathbb{Z}\}$$

$$\text{DM} \quad \langle S \rangle = \{a^n, n \in \mathbb{Z}\}$$

(C) On a $a \in \langle S \rangle$, comme

$\langle S \rangle$ est un (g) , on a $a^n \in \langle S \rangle \quad \forall n \in \mathbb{Z}$

(C) $\{a^n, n \in \mathbb{Z}\}$ est (sg) de G . (on le vérifie)

$$\rightarrow a^n (a^{n-m})^{-1} = a^{n-m} \quad \checkmark \quad \text{qui s'annule}$$

qui contient $S = \{a\}$.

Par d., $\langle S \rangle \subset \{a^n, n \in \mathbb{Z}\}$.

Complément Plus généralement

$\langle S \rangle = \{ \text{produits finis d'éléts de } S \text{ & de leurs inverses} \}$

D16) On appelle ordre d'un élét a d'un groupe G , le + petit entier $n \geq 1$ tel que $a^n = e$ où e : élét neutre. Sinon a est dit d'ordre infini.

NB: pr $a \in G$, a d'ordre n

$$\begin{aligned} &\Leftrightarrow a^n = e \text{ et } a^k \neq e \quad \forall 0 < k < n. \quad \text{①} \\ &\Leftrightarrow a^n = e \text{ et } a^k \neq e \quad \forall \text{diviseur } k \text{ de } n \quad \text{②} \\ &\quad \text{et } 0 < k < n. \quad ! \end{aligned}$$

DM

① \Rightarrow ② clair
② \Rightarrow ① appr (2). (2)

appr $\exists k, 0 < k < n$ et $a^k = e$. (2)

On peut appr de + que k est le + petit entier qui vérifie (2).

La division euclidienne de n par k s'écrira
 $n = kg + r, \quad 0 \leq r < k$.

$$\begin{array}{c} \text{ordre } k. \\ \begin{array}{c} 4, 3 \\ = 12 \\ 12 \in \mathbb{Z} \end{array} \end{array} \quad \left| \begin{array}{l} \text{@ groupe symétrig} \\ \text{permutat \in Z} \\ \text{ordre } 2. \end{array} \right.$$

Mais $a^n = (a^k)^q$. a^r donne $a = a^r$.

$$\textcircled{a} \quad \left\{ \begin{array}{l} \mathbb{R}_+^* \longrightarrow \mathbb{R} \\ x \longmapsto \ln(x) \end{array} \right.$$

morphisme entre (\mathbb{R}_+^*, \times) et $(\mathbb{R}, +)$.

$$\ln(xy) = \ln(x) + \ln(y).$$

Par chain de k, on a nécessairement $x = 0$
ie k divise n, ce qui contredit (e).

Donc (1) est vrai.

$$\boxed{\text{F}\ddot{\text{o}}\text{r}\text{m}\text{u}\text{l}\text{a}}$$

NB L'ordre n de a est aussi le cardinal du groupe $\langle a \rangle$.

ie

$$\text{ordre de } a = |\langle a \rangle|$$



$$= \text{Card}(\langle a \rangle).$$

△ ordre élé = ordre \textcircled{g} engendré.

1.3. Morphismes

intro

D17 Soit (G, \circ) , (G', \star) \textcircled{g} .

Une appli $\varphi: G \rightarrow G'$ est un morphisme de groupes si

$$\forall (a, b) \in G^2, \varphi(a \circ b) = \varphi(a) \star \varphi(b)$$

ordre élé
ordre gpe engendré

Un morphisme bijectif est appelé isomorphisme.

P14 (G, \circ) , (G', \star) \textcircled{g} ; $\varphi: G \rightarrow G'$ MDG

$$\circ \varphi(e) = e'$$

$$\circ \varphi(a^{-1}) = (\varphi(a))^{-1} \quad \forall a \in G.$$

DM (vp) $\varphi(e) = \varphi(e \circ e) = \varphi(e) \star \varphi(e)$ d'où $\varphi(e) = e'$
 $a \in G, \varphi(a a^{-1}) = \varphi(a) \varphi(a^{-1}) \Rightarrow \varphi(a) \star \varphi(a^{-1}) = e' \text{ ie } \varphi(a^{-1}) = ((\varphi(a))^{-1})^{-1}$

P15 $\text{MDG} \circ \text{MDG} = \text{MDG}$

$$\begin{aligned} a, b \in G \Rightarrow \varphi \circ \varphi(a \circ b) &= \varphi(\varphi(a) \star \varphi(b)) \\ &= (\varphi \circ \varphi(a)) \star (\varphi \circ \varphi(b)) \end{aligned}$$

si φ isdg \Rightarrow MDG bijectif $\Rightarrow \varphi^{-1}: G' \rightarrow G$ \exists .
 Vraies si mdg; $a', b' \in G'$:

$$\begin{aligned} \text{DM (vp). } \varphi(\varphi^{-1}(a' \star b')) &= \varphi \circ \varphi^{-1}(a' \star b') = a' \star b' \\ &\& \varphi(\varphi^{-1}(a') \star \varphi^{-1}(b')) = \varphi \circ \varphi^{-1}(a') \star \varphi \circ \varphi^{-1}(b') = a' \star b' \\ \Rightarrow \varphi(\varphi^{-1}(a) \star \varphi^{-1}(b)) &= \varphi(\varphi^{-1}(a' \star b')) \text{ or } \varphi \text{ est bijectif} \end{aligned}$$

$$\text{dc } \varphi^{-1}(a' \star b') = \varphi^{-1}(a') \star \varphi^{-1}(b')$$

13

② si G est ⑨ & $a \in G$ alors l'application

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \langle a \rangle \\ n & \longmapsto & a^n \end{array}$$

est un morphisme surjectif entre $(\mathbb{Z}, +)$ et $(\langle a \rangle, \star)$.

(Voir ② 9.1-3)

9.8 soit

$$\ker \varphi = \{x \in G, \varphi(x) = e'\}$$

$$\text{Im } \varphi = \{\varphi(x), x \in G\}$$

P(6) ⑨), MDG φ .

$\Rightarrow \ker \varphi$ ⑨ de G & $\text{Im } \varphi$ ⑨ G' .

DM (up)

\rightarrow le noyau n'est pas nul (car $\varphi(e) = e' \notin \ker \varphi$ il contient e).
 x, y élts $\ker \varphi \Rightarrow \varphi(xy^{-1}) = \varphi(x) \star \varphi(y^{-1}) = \varphi(x) \star (\varphi(y))^{-1}$
 ainsi $xy^{-1} \in \ker \varphi$ dc $\ker \varphi$ ⑨ de G .

$\rightarrow \exists \hat{x} \varphi(x) = e'$, $e' \in \text{Im } \varphi$ dc $\text{Im } \varphi$ n'est pas nul.

x, y élts $\text{Im } \varphi \Rightarrow \exists x, y$ dans G tq $x = \varphi(x)$, $y = \varphi(y)$

$\Rightarrow x \star y^{-1} = \varphi(x) \star (\varphi(y))^{-1} = \varphi(x) \star \varphi(y^{-1}) = \varphi(xy^{-1}) = e'$

ainsi $x \star y^{-1} = \varphi(xy^{-1}) \in \text{Im } \varphi$

$\Rightarrow \text{Im } \varphi$ ⑨ de G .

PT

$\rightarrow M_\varphi$ ① si $\ker \varphi = \{e\}$

$\rightarrow M_\varphi$ ② si $\text{Im } \varphi = G'$

DM (up) $Mdg \varphi$ ③ si $\text{Im } \varphi = G'$ (Voirie & Vassere).

• $\varphi(e) = e'$. Supposons ①, soit $a \in \ker \varphi \Rightarrow \varphi(a) = e' = \varphi(e)$
 dc $a = e$ & ④ $\ker \varphi = \{e\}$

• Supposons $\ker \varphi = \{e\}$, a, b élts G tq $\varphi(a) = \varphi(b) \Rightarrow$

$$\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a) \star (\varphi(b))^{-1} = e'$$

$$\Leftrightarrow \varphi(a) \star (\varphi(b^{-1})) = e'$$

$$\Leftrightarrow \varphi(ab^{-1}) = e'$$

$$\Leftrightarrow ab^{-1} = e$$

$$\Leftrightarrow a = b . \quad \text{dc (nyc) } \underline{\text{MDG}} \varphi.$$

14

P18 $\text{Aut}(G)$

\uparrow
isom de l.m

aut ∇ $HdG \circ HdG = HdG$ & $(isHdG)^{-1} = isHdG$
Dm (up) et $bij^{\theta} \circ bij^{\phi} = bij^{\phi}$. $\varphi, \psi \in \text{Aut}(G)$
 $\Rightarrow \varphi \circ \psi^{-1} \in \text{Aut}(G)$.

ari elt m.t $id_G: G \rightarrow G$ tq $id(g) = g, \forall g \in G$
 est elt de $\text{Aut}(G)$.

P19 automorphisme intérieur

$G \oplus, g \in G$, l'appl $\psi_g: G \rightarrow G$
 est un automorphisme de G $x \mapsto g x g^{-1}$
 appelé automorphisme intérieur.

Dm $g \in G$; • check ψ_g Mdg,
 $x, y \in G: \psi_g(xy) = g x y g^{-1} = (g x g^{-1})(g y g^{-1}) = \psi_g(x) \cdot \psi_g(y)$

• check ψ_g

2. Groupe quotient & groupe produit

2.1. Classes d'équivalence Relais de congruences

$\frac{a}{3} \equiv \frac{b}{3+12\mathbb{Z}} [\text{mod } 12] \rightarrow (\mathbb{Z}, +) \times \text{sg} 12 \mathbb{Z}$

D19 relais congra à D & G.

Situation générale

sont $G \oplus, H \oplus G$, pr $x, y \in G$;
 $x \equiv y \pmod{H}$ si $x^{-1}y \in H$ ($\begin{pmatrix} x \\ y \end{pmatrix} \in H$)

si $x^{-1}y = h$ dp $h \in H$

si $y = xh$ q $h \in H$

si $y \in xH$

Notat

$xH = \{xh \mid h \in H\}$.

D'où $\overline{x}^2 = xH$.

(dm $\overline{x}^d = Hx = \{hx \mid h \in H\}$).

Q5, Ch 3 p 2, 3

(P21) $G \otimes H \otimes G$

Tte classe à drt mod H est en bijct $\Leftrightarrow H$.
(négation)

$$\cancel{xH} \rightarrow H \xrightarrow{b} xH \\ h \mapsto xh$$

(P22) Ens quotients $(G/H)_g$ & $(G/H)_d$ et en bijct.

$$(G/H)_g = \{xH \mid x \in G\}$$

$$\begin{array}{l} \text{DM} \\ (G/H)_g \rightarrow (G/H)_d \\ xH \mapsto Hx^{-1} \end{array} \quad \left| \begin{array}{l} \text{bien def?} \\ \text{inj?} \\ \text{suj?} \end{array} \right.$$

$$(P4) \text{ si } xH = yH \Leftrightarrow Hx^{-1} = Hy^{-1}$$

\Rightarrow bien def - appli compatible

\Leftarrow appl inject

$$\begin{array}{c} \text{sujet} \\ yH \Leftrightarrow H^{-1}x^{-1} = H^{-1}y^{-1} \quad \overbrace{H=H^{-1}} \\ \end{array}$$

$$(P5) |(G/H)_g| = |(G/H)_d| = [G:H]$$

\uparrow
l'indice de H dans G.

nbr de classes ↗

2.2. TH de Lagrange

(T4) $|H|$ divise $|G|$.

(Cor 1) (Lagrange)

soit $G \otimes$ fini & $H \otimes$.

$$\text{alors } [G:H] \cdot |H| = |G|$$

ep $|H|$ divise $|G|$.

Prouve

G est la réunion disjointe des classes à gauche de G modulo H .

Il y a $[G:H]$ classes.

Chaque classe a $|H|$ élts. (P21)

$$\text{D'où } |G| = [G:H] \cdot |H|$$

(Cor 2) $G \otimes$ fini, $x \in G$: $|x|$ divise $|G|$.

(car $|x|$ est $|<x>| \leftarrow \otimes$ de G).

(Cor 3) $G \otimes$ fini, notons $n = |G|$, e_G élmt neutre de G

$$\forall x \in G, x^n = e$$

(16)

additif @ $\mathbb{Z}/6\mathbb{Z}$

$m^{\frac{1}{2}}$ pte qd est élevé à la puissance 6;

$$x^m = mx = 6x = \bar{0}$$

$\forall n \in \mathbb{Z}/6\mathbb{Z}$,

@ multiplicatif

groupe symétrique

S_4 .

$$|S_4| = 4! = 24$$

La réciprocité
du (1) de
Lagrange
est

F

A

S

E

$$\text{Ta H} \circ (123)H = \{(123), (123)(12), (12)(123)\}$$

Cet ens a au moins 3 élts. (13) (23)

Le qd est trop. Or tous les classes (à gauche) ont $2 = |H|$ élts.

• A_4 (sg) alterné de card $\frac{4!}{2} = 12$.

⚠ A_4 n'a pas de (sg) d'ordre 6.

⚠ les diviseurs du card du groupe sont les seuls possibles ! Mais ils ne le sont pas forcément tous.

2.3. Sous-groupes distingués

But: Mettre $\pm 5^{\text{e}}$ d' G et $(G/H)_g$ (ou $(G/H)_d$).

⚠ On n'a pas en général.

$$xH \cdot yH \in (G/H)_g$$

@ $G = \mathfrak{S}_3$, $H = \langle (1,2) \rangle = \{\text{Id}, (1,2)\}$

Notation: $A, B \subset G$,

$$A \cdot B = \{ab \mid a \in A, b \in B\}$$

si $A = \{x\}$, on note $\{x\}B = xB$.

NB: $An = B \iff A = B_n^{-1}$

(P22) Un (sg) H d'un (g) G est dit distingué ou normal dans G , noté $H \triangleleft G$ si

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H.$$

(P23) $G \oplus H$ (sg), A.S.E:

(i) le (sg) H est distingué de G

$$(ii) \forall g \in G, ghg^{-1} \subset H$$

$$(iii) \forall g \in G, ghg^{-1} = H$$

$$(iv) \forall g \in G, gH \subset Hg$$

$$(v) \forall g \in G, gH = Hg$$

(P)

les classes à gauche & les classes à droite coïncident.

Preuve Prop. 23

$$(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (v) \Rightarrow (vi)$$

D22

not. $\frac{g \in G}{[gHg^{-1} \subset H]}$

$$\begin{array}{l} g \in G \\ gHg^{-1} \subset H \\ g^{-1}Hg \subset H \\ H \subset gHg^{-1} \end{array}$$

$$\begin{array}{l} g \in G, \\ gHg^{-1} \subset H \\ gHg^{-1} = H \end{array}$$

Prop 25

$G \oplus$, tt $\oplus H$ d'indice 2 dans G et distingué

$$[G:H] = 2 \Rightarrow H \triangleleft G.$$

$$\begin{array}{c} G \\ | \\ H \\ | \\ aH = Ha \\ | \\ a \notin H \end{array}$$

Prop 26

8g Int(G)

Exemples de situations où G & H sont distingués

@1 Gabélien: tt $\oplus H$ est distingué.

@2 Prop 24. (noyau de morphisme).

$$\varphi: G \rightarrow G'$$

ker φ est distingué de G .

on note $K = \text{ker } \varphi$ & e'_G .

$x \in G, k \in K$, check $xkx^{-1} \in K$:

$$\begin{aligned} \varphi(xkx^{-1}) &= \varphi(x)\varphi(k)\varphi(x^{-1}) \\ &= \varphi(x)e'(\varphi(x))^{-1} \\ &= \varphi(x)(\varphi(x))^{-1} \\ &= e' \end{aligned}$$

et par preuve $xkx^{-1} \in K$ dc $xKx^{-1} = K$.

i.e. K distingué de G .

et G est distingué car le \oplus est l'noyau d'un morphisme).

D23

Le centre d'un $\oplus G$ est l'ens des élts de G qui commutent avec toutes les autres, noté $Z(G)$

$$Z(G) =$$

D24

2.4. Groupe Quotient

(P₂) soit $G \textcircled{g}$ & $H \textcircled{x}$ distingué.

$$\text{On a } (G/H)_g = (G/H)_d$$

On note $\frac{G}{H}$ cet ensemble.

La loi définie sur $\frac{G}{H}$ par :

$x, c, c' \in \frac{G}{H}$, alors

$$c.c' = \{c.c' \mid c \in c, c' \in c'\}$$

donne à $\frac{G}{H}$ une structure de groupe.

Premre

soit $c, c' \in \frac{G}{H}$, on peut les écrire

$$\begin{cases} c = xH \\ c' = x'H \end{cases}$$

$\forall x \in G, n' \in H$.

$$\text{On a : } c.c' = xH \cdot x'H = \overset{Hx' = x'H}{= xHx'H} \in \frac{G}{H}$$

$$= xH$$

$(HH = H)$ car (a) si $h \in H$ alors $h = h \cdot 1_G \in H \cdot H$
 (b) si $hh' \in H$ alors $hh' \in H$

Donc la loi est interne.

Associative

$$\text{soit } c = xH, c' = x'H, c'' = x''H$$

trois classes
 $(x, x', x'' \in G)$

$$(c.c').c'' = (xx')H \cdot x''H \xrightarrow{\text{associativité de la loi}} = (xx').x''H = x(x'.x'')H$$

$$= xH \cdot (x'.x'')H = xH(x'.H \cdot x''H)$$

$$= c(c'c'')$$

• Elément neutre : $H = 1_G H$

$$(xH \cdot 1_G H = x \cdot 1_G H = xH)$$

• Symétrique : de xH : $(xH)^{-1} = x^{-1}H$.

Prop et (suite & fin)

\Rightarrow la morpho canoniq

est un [MDG]

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \frac{G}{H} \\ x & \mapsto & s(x) = xH \end{array}$$

Contente : $G \textcircled{g}$, $H \triangleleft G$, $\frac{G}{H}$ gype quotient.

$$s: G \longrightarrow \frac{G}{H}$$

$$g \mapsto s(g) = gH$$

$$s(gg') = s(g) \cdot s(g')$$

produit de 2 classes = produit 2 représentantes classes.

1) Les (i) de M0G et fuis ds (ii) \Leftrightarrow , (la réciproque est)
mais

$$\begin{aligned} \text{NB } \ker s &= \{g \in G \mid gH = H\} \\ &= \{g \in G \mid \varphi(g) = 1_{G/H}\} \end{aligned}$$

Preuve: La relation $\equiv_g [\text{mod } H]$

est compatible avec φ :

pour $x, y \in G$, si $x \equiv_g y \pmod{H}$,

ie $x^{-1}y \in H$, alors $x^{-1}y \in \ker(\varphi)$

& de $\varphi(x^{-1}y) = 1_G$,

$$\varphi(x)^{-1} \varphi(y) = 1_G,$$

$$\varphi(y) = \varphi(x).$$

2.5. TH d'isomorphismes

(a) (1° TH d'isomorphisme)

$$\varphi: G \rightarrow G' \quad \boxed{\text{M0G}}$$

$H \triangleleft G$ tq $H \subset \ker \varphi$ alors

$$\exists! \boxed{\text{M0G}} \quad \bar{\varphi}: G/H \rightarrow G' \text{ tq } \bar{\varphi} = \varphi \circ s.$$

$$\text{D}, \quad \text{Im } \bar{\varphi} = \text{Im } \varphi$$

$$\ker \bar{\varphi} = \ker \varphi / H \quad (\text{car } H \subset \ker \varphi)$$

φ pour $H = \ker(\varphi)$.

$$\bar{\varphi} \mid \text{Im } \varphi: G/\ker \varphi \rightarrow \text{Im } \varphi \quad \text{est un isomorphisme.}$$

$$(G/\ker \varphi \simeq \text{Im } \varphi).$$

On sait alors que φ "passe au quotient" G/H :

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ s \downarrow & \nearrow \exists! \bar{\varphi} \text{ tq } \bar{\varphi} \circ s = \varphi & \\ G/H & & \end{array}$$

• $\text{Im } \bar{\varphi} = \text{Im } \varphi$ résulte de $\bar{\varphi} \circ s = \varphi$

• soit $\bar{x} = xH = s(x) \in G/H$ tq $\bar{\varphi}(\bar{x}) = 1_{G'}$

$$\text{Alors } \bar{\varphi}(s(x)) = 1_{G'}$$

$$\varphi(x) = 1_{G'}$$

$$x \in \ker(\varphi)$$

On obtient que $\bar{x} \in \frac{\ker \varphi}{H} = \{\bar{x}, x \in \ker \varphi\}$

si non
 $s(\ker \varphi)$

$$\text{NB } G/G = \{g\}, G/\{1_G\} = G$$

$\ker \varphi_H = \{1_H\}$ par hypothèse d'où $\ker \overline{\varphi}_H = \{h\}$
de $\overline{\varphi}$ est injective. $\ker \overline{\varphi}$

- Le reste est un gp facile

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow s & & \uparrow \varphi_{\text{func}} \\ G/H & \xrightarrow{\text{defn } \varphi} & \text{dom } \varphi \end{array}$$

(Th) 5 (2° Th isomorphisme)

$G \circledcirc, H, K \trianglelefteq G, K \trianglelefteq G$

alors l'ens $HK = \{hka, h \in H, k \in K\}$

est \circledcirc de G & on a

$$HK/K \simeq H/H \cap K \quad (\text{as})$$

$\nexists K \trianglelefteq HK, H \cap K \trianglelefteq H$.

$$G/\ker \varphi \simeq \text{Im } \varphi.$$

Preuve :

• $HK \subset G, HK \neq \emptyset$.

Stabilité de l'ens. HK :

soit $h_1 k_1, h_2 k_2 \in HK$ ($h_1, h_2 \in H, k_1, k_2 \in K$).

$$\begin{aligned} \text{On a : } (h_1 k_1) \cdot (h_2 k_2)^{-1} &= h_1 k_1 k_2^{-1} h_2^{-1} \\ &= \underbrace{h_1 h_2^{-1}}_{\in H} \underbrace{h_2 k_2 k_1^{-1} h_1^{-1}}_{\in K} \underbrace{h_1^{-1} h_2^{-1}}_{\in K} \in HK. \end{aligned}$$

• $K \trianglelefteq HK$ car $\begin{cases} K \trianglelefteq G \\ G \supset HK \end{cases}$

$H \cap K \trianglelefteq H$ ($h \in H \cap K, g \in H$)

$g \cdot h \cdot g^{-1} \in H$ (car $h, g \in H$)

$g \cdot h \cdot g^{-1} \in K$ (car $K \trianglelefteq G$) d'où $g \cdot h \cdot g^{-1} \in H \cap K$.

Preuve de $HK/K \simeq H/H \cap K$.

Considérons les morphismes $i: \begin{cases} H \rightarrow HK \\ h \mapsto h \end{cases}$

$p: \begin{cases} HK \rightarrow HK/K \\ h \mapsto h/H \end{cases}$ ($p = s|_{HK}$).

et le morphisme $\varphi = p \circ i: H \rightarrow HK/K$

o Ψ est surjective : H est de HK/K
s'écrit $hkK \neq h'K$ (ou $hK = K$)

$$\text{D'où } hkK = h'K = p \circ i(h)$$

• $\ker(\Psi)$?

$$\begin{aligned} \text{soit } h \in H, h \in \ker \Psi &\Leftrightarrow \Psi(h) = 1_{HK/K} \\ &\Leftrightarrow hK = K \\ &\Leftrightarrow h \in K. \end{aligned}$$

Par conséquent

$$\ker \Psi = H \cap K.$$

Q'apres 1^e Th d'isom. :

$$H/(H \cap K) \simeq HK/K.$$

Preuve à commenté \square

faire hypo.

Th 6 3^e Th d'isomorphisme

$$G/H \simeq (G/K)/(H/K)$$

$$\text{considérez } G/K \rightarrow G/H \text{ de } \ker \Psi = H/K$$

$$G/\ker \Psi \simeq G/H$$

Th 7 (Th de correspondance)

$G \otimes K$, $K \triangleleft G$; on note $p: G \rightarrow G/K$ la
application canonique

Les applications $\{H \otimes G / H \triangleleft K\} \xrightarrow{\pi} \{H \otimes G\} \text{ de } G/K$

$$H \longmapsto H/K = p(H)$$

et $\{H \otimes G\} \xrightarrow{p} \{H \otimes G / H \triangleleft K\}$

$$H \longmapsto p^{-1}(H)$$

1^e (bien défini : $H/K = \{hk \mid h \in H\} = p(H)$)

2^e (bien défini : $p^{-1}(H) \otimes G$
 $p^{-1}(H) \supset p^{-1}(1_{G/K}) = \ker p = K$)

st réciproques l'une de l'autre.

Et elles st bijectives.

(e2)

Beweis: Il s'agit de vérifier

$$\rho \circ \pi = \text{Id}, \quad \pi \circ \rho = \text{Id}$$



ici $\rho(\rho^{-1}(\mathcal{H})) = \mathcal{H}$ (car ρ surjective).

Voir ② B.

2.6. Groupe produit

$$H \times K = \{(h, k) \mid h \in H, k \in K\}$$

$$(h, k)(h', k') = (hh', kk')$$

H, K 2 ⑨

Propriété: Soit $h, k \in G$ alors

G isom au $H \times K$ si

$$H \triangleleft G, K \triangleleft G, H \cap K = \{e_G\}, G = HK.$$

Démonstration:

$$(\Leftrightarrow) \quad H \triangleleft G, K \triangleleft G, H \cap K = \{e_G\} \quad \& \quad G = HK.$$

soit $h \in H, k \in K$:

$$hkh^{-1}k^{-1} = (\underbrace{hkh^{-1}}_{\in H})k^{-1} - h(\underbrace{k^{-1}k}_{\in H}) \in H \cap K = \{e_G\}$$

d'où $hk = kh$.

soit $\phi: H \times K \rightarrow HK = G$

$$(h, k) \mapsto hk$$

Vérifions que c'est un isomorphisme

soit $(h, k), (h', k')$ 2 élts de $H \times K$, on a:

$$\phi((h, k)(h', k')) = \phi((hh', kk')) = hh'kk' = hkh'k = \phi(h, k)\phi(h', k')$$

il s'agit de bien d'un morphisme, il est surjectif par hypo: $G = HK$

Considérons son ⑩:

$$\ker \phi = \{(h, k) \in H \times K, hk = e_G\} = \{(h, k) \in H \times K, h = k^{-1}\}$$

à $H \cap K = \{e_G\}$ d'où $h = k = e_G$ de MDG injectif.

Donc ϕ est bien un isomorphisme.

Réciproque ⑪

3. Groupes Cycliques

3.1 Définitions

(D25) Groupe monogène

ordre (groupe) = ordre (elt)

(R9) Soit $G = \langle a \rangle$, un grp cycliq engendré par a & n l'ordre de G . (\bar{a} est aussi l'ordre de a).

2^e application :

$\begin{cases} \mathbb{Z} \rightarrow \langle a \rangle \\ n \mapsto a^n \end{cases}$ est un morphisme
($a^{m+n} = a^m \cdot a^n$)

& de (n) $\{h \in \mathbb{Z}, a^h = 1\} = \mathbb{Z}/n\mathbb{Z}$

Donc $\mathbb{Z}/n\mathbb{Z} \simeq \langle a \rangle = G$

• n est l'ordre de a si $a^n = 1$ & $\forall h \in \mathbb{Z}$, $a^h = 1 \Leftrightarrow n \mid h$. (24)

- 1. ° Def An autre \bar{k} d'ordre
 - ° ordre $\langle a \rangle$ + $\exists k \in \mathbb{N}$ t.q. $n > 0$, $a^k = 1$
 - ° ordre $\langle a \rangle$
 - ° entier $m \neq 0$ tel que $a^m = 1$ & $a^{\frac{m}{k}} \neq 1$ pour tout diviseur de n
 - ° 1^e vain.

Prop 36 $\forall \bar{k} \in \mathbb{Z}/n\mathbb{Z}$,
 $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z} \Leftrightarrow k$ est premier à n .

Beweis :

\Rightarrow On appelle $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$, et $\bar{l} \in \langle \bar{k} \rangle$
 i.e. $\exists u \in \mathbb{Z} \mid \bar{l} = u\bar{k} = \bar{uk}$
 $\exists u \in \mathbb{Z}, \exists v \in \mathbb{Z} \quad l = uk + vn$
 et $k \& n$ p.c. (Bézout)

\Leftarrow Supposons $k \& n$ p.c. i.e. $\exists u, v \in \mathbb{Z}, uk + vn = 1$ (25)
 Mq $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$,

(C) trivial.

(D) soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ ($a \in \mathbb{Z}$)
 on a $a = uka + vna$

d'où $\bar{a} = \bar{u}\bar{k}\bar{a} + \bar{v}\bar{n}\bar{a} \in \langle \bar{k} \rangle$.

($k \& n$ est premier alors nous avons : $n - 1$ et premier à n)

33 Ppt's

Prop 37

Tout \textcircled{G} cycliq d'ordre n est isomorphe au groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

$$|\textcircled{G}| = n \simeq \mathbb{Z}/n\mathbb{Z}.$$

(v)
Rém $\phi: \mathbb{Z}/n\mathbb{Z} \rightarrow G$ où $G = \langle x \rangle$

$$\bar{k} \mapsto x^k$$

isomorphisme
bien def
morphisme
surjective?
injective?

* De plus $f^{-1}(H) = k\mathbb{Z} \supset f^{-1}(e_G) = \ker(f) = n\mathbb{Z}$
 $kx = 0 \Leftrightarrow \text{ord}(x) | k \quad \text{De } k\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}_n$.

Prop 38

soit p un nbr premier & G un \textcircled{G} ordre p
alors G est \textcircled{G} cycliq.

P) $|G| = p \Rightarrow G \text{ } \textcircled{G}$

Prop 39 soit $G = \langle x \rangle$ \textcircled{G} d'ordre n alors

1) si H est \textcircled{G} de G , H est cyclique & on note $k > 0$,
le + petit entier tq $kx \in H$, alors H est engendré par kx & $|H| = n/k$.

2) si d est un diviseur de $n \Rightarrow G$ possède unig \textcircled{G}
d'ordre d q est engendré par $\frac{n}{d}x$.

Preuve

NB: L'applicat $f: \mathbb{Z} \rightarrow G$
 $\ell \mapsto \ell x$ est MDG surjectif
(car $G = \langle x \rangle$).

soit H un \textcircled{G} de G ,

$f^{-1}(H)$ est \textcircled{G} de \mathbb{Z} , de la forme $f^{-1}(H) = k\mathbb{Z}$
pr un $k \in \mathbb{N}$. $\textcircled{\times}$

(NB: kx est le + petit entier tq $kx \in H$)

On ad $H = f(f^{-1}(H))$ car f surjectif
 $= f(k\mathbb{Z}) = \{k\ell x, \ell \in \mathbb{Z}\}$
 $\overset{f(k\ell)}{\sim}$

d'où $H = \langle kx \rangle \subset G$.

sp H est monog.

Prop est de \textcircled{G} groupe, son ordre est divisible par 7 & 1

2 Ch. sur les groupes

De plus, kx est d'ordre $\frac{m}{k}$:

$$\frac{m}{k} \cdot kx = mx = 0$$

$$kx \neq 0$$

$$2kx \neq 0$$

$$\left(\frac{m}{k}-1\right)kx \neq 0$$

alors $H = \langle kx \rangle$ est d'ordre $\frac{m}{k}$.

H cyclique.

(On a démontré a).

(2) soit $d \in \mathbb{Z}$ tq $m=kd$ et $k \in \mathbb{Z}$

Δ : $\langle kx \rangle$ \oplus de G d'ordre $\frac{m}{k}=d$
(d'après l'analyse de (1))

3^e: si $H \oplus G$, $|G|=d$, d'après (1),
necess^{RT} $H = \langle kx \rangle$ et $k = \frac{m}{d}$

x d'ordre 6: En d'ordre 3?

Conjecture de Jordan

3.4 Sg & produits

Prop 40 Les \oplus de $\mathbb{Z}/m\mathbb{Z}$ et les groupes

$k\mathbb{Z}/m\mathbb{Z}$ et $k\mathbb{Z}/m$. On a:

$$k\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/(n/k)\mathbb{Z}$$

$$k\mathbb{Z}/m\mathbb{Z} = \{\overline{kl}, l \in \mathbb{Z}\}$$

$$3\mathbb{Z}/6\mathbb{Z} = \{\overline{3}, \overline{0}\}$$

$$7\mathbb{Z}/6\mathbb{Z} = \{\overline{5}, \overline{2}, \overline{4}\} \cong \mathbb{Z}/3\mathbb{Z}$$

On a $2\mathbb{Z}/6\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z}$ Δ

Déf à l'inst. (1)

Prouve $\frac{k\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{n/k\mathbb{Z}}$
pour $k|n$

$$f: \mathbb{Z} \longrightarrow \frac{k\mathbb{Z}}{n\mathbb{Z}}$$

est un MG surjectif de moyen $\frac{n}{k}\mathbb{Z}$

(*) cl. $\frac{\mathbb{Z}}{\frac{n}{k}\mathbb{Z}} \cong \frac{k\mathbb{Z}}{n\mathbb{Z}}$ (d'après $G/\ker f \cong \text{Im } f$)

$$\overline{k(n+n')} = \overline{kn} + \overline{k'n}$$

Pk de moyen $\frac{n}{k}\mathbb{Z}$:

$$x \in \mathbb{Z}, n \in \text{ker } f, m \overline{kn} = \overline{0}$$

$$\text{ssi } n \mid kn$$

$$\text{ssi } \frac{n}{k} \mid n$$

$$\text{ssi } n \in \frac{n}{k}\mathbb{Z}.$$

$$\Delta \frac{\mathbb{Z}}{n\mathbb{Z}} \not\cong \left(\frac{\mathbb{Z}}{k\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{l\mathbb{Z}}\right)$$

$$\exists_{Bij(X)} \pi(1_G) = \pi(gg^{-1}) = \pi(g) \circ \pi(g^{-1}) \rightarrow \pi(g^{-1}) = \pi(g)^{-1} \quad (*)$$

Prop 41, $m & n$ p.e alors

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

(*) Δ

4. Action de groupe

4.1 Définition

D26 soit X ens, G . Une action (ou opérat.) de G sur X est un homomorphisme de G ds le groupe $Bij(X)$ des bijets de X ds lui-même:

$$\pi: G \longrightarrow Bij(X)$$

$$g \longmapsto \pi(g): X \longrightarrow X \text{ bijective}$$

$\pi(g)$ agit sur x : il faut $\pi(gg') = \pi(g) \circ \pi(g')$.

g. x (résultat de l'act de g sur x)

n dans X

② $X : \mathbb{R} \odot$, $G = GL(X)$
 $= \{ \text{appl. liné. biject. } X \xrightarrow{g} X \}$

action de $GL(X)$ sur X .

soit $g \in GL(X)$, $x \in X$

$$\pi(g)(x) = g(x)$$

L'action est formellement définie par

$$\begin{aligned} \pi : GL(X) &\longrightarrow \text{Bij}(X) \\ g &\longmapsto \pi(g) : X \longrightarrow X \\ &\quad x \mapsto \pi(g)(x) \\ &\quad \text{def} \\ &\quad g(x) \end{aligned}$$

③ soit G un Ⓛ opérant sur l'ens X , soit $x \in X$:

• l'ens $\text{Stab}_G(x) = \{g \in G, g \cdot x = x\}$, noté aussi G_x , est un Ⓛ de G appelé stabilisateur de l'élémt x .

• si A est une pte de X , on déf. le stabilisateur de A dans G & le fixateur de A ds G par:
 $\text{Stab}_G(A) = \{g \in G, g \cdot A = A\}$, $\text{Fix}_G(A) = \{g \in G, \forall a \in A, g \cdot a = a\}$

28

$$\text{Stab}_G(A) = \{g \in G \mid \pi(g)(A) = A\}.$$

Déf 28 • Un élmt n de X est un point fixe

$$\text{si } \forall g \in G, g \cdot n = n$$

• L'ens $\mathcal{O}_n = \{\pi(g)(n), g \in G\} = \{g \cdot n, g \in G\}$ est appelé l'orbite de n ss l'act de G .

④ AL à \mathcal{O}_n réduit au \mathcal{O}_n .

Prop 43 soit G un Ⓛ opérant sur l'ens X alors les orbites de X forment une partie de X de l'act

Preuve car les orbites st les classes d'équivalence de la relati d'équivalence suivante:

pr $x, y \in X$; on pose $x R y \iff \exists g \in G, g \cdot x = y$.

R équivalence
 (Ref.)
 (sym.)
 (trans.)

$$cl(n) = \{y \in X \mid n R y\}$$

$$= \{y \in X \mid \exists g \in G \text{ tq } y = g \cdot n\}$$

= orbite \mathcal{O}_n

Notation: $\{ \text{Stab}_G(x) = \{g \in G, g \cdot x = x\} \}$ (stabilité) ou G_x de G

(Orbita) $\{ \underset{\text{ou}}{x} = \{g \cdot x, g \in G\} \subset X \}$ O_x

$$\text{ssi } |G/\text{Stab}_G(x)| = 1.$$

• x fixe si $\text{Stab}_G(x) = G$ ssi $O_x = \{x\}$

① Les orbites qd x varie de X forment une partie de X . (Prop 43)

② $G/\text{Stab}_G(x)$ en bijeo $\rightarrow O_x$ (Prop 44) ||

⚠ pas un \mathbb{Q} quotient, en g^{-1} , $\text{Stab}_G(x)$ n'est pas distingué.
ens quotient pr la relation de congruence à gauche
modulo $\text{Stab}_G(x)$

$$\begin{array}{ccc} G/\text{Stab}_G(x) & \longrightarrow & O_x \\ g \text{Stab}_G(x) & \longmapsto & g \cdot x \end{array}$$

man (π): $\sigma(i) \in \text{Stab}(x)$

Vérifier que c'est une bijeo

• Application bien définie?

$$g \text{Stab}_G(x) = g' \text{Stab}_G(x) \Leftrightarrow g^{-1}g' \in \text{Stab}_G(x)$$

$$\Leftrightarrow (g^{-1}g') \cdot x = x$$

$$\Leftrightarrow g' \cdot x = g \cdot x$$

• Surjective? par déf de O_x .

• Injective voir preuve de bien définie

$$g \cdot x = g' \cdot x \Leftrightarrow (g^{-1}g') \cdot x = x \Leftrightarrow g^{-1}g' \in \text{Stab}_G(x) \Leftrightarrow g \text{Stab}_G(x) = g' \text{Stab}_G(x)$$

Prop 45: Formule des Classes

si X est fini & O_{x_1}, \dots, O_{x_n} : la liste finie des orbites de l'action, alors :

$$\boxed{\text{card}(X) = \sum_{i=1}^n \frac{|G|}{|\text{Stab}_G(x_i)|}}$$

= nbr pts fixes + nomme de diviseurs de $|G|$ distincts de 1.

Preuve: Combina les points ① ② + Prop 44.

1) nbr élts de $X = \sum$ nbr élts des orbites

2) chacune des orbites, son nbr d'eltl vaut $\frac{|G|}{|\text{Stab}_G(x)|} \hookrightarrow O_{x_i}$

4.3. Action par conjugaison

$G \otimes G$, $X = G$, action par conjugaison de $G \otimes G$:

$$c: G \longrightarrow \text{Bij}(G)$$

$$\begin{cases} g \mapsto c_g: & G \longrightarrow G \\ x \mapsto g x g^{-1} & \end{cases}$$

$\Rightarrow C_n$ est la classe de conjugaison

$$C_x = \{g x g^{-1} \mid g \in G\}$$

Pour l'act par conjugaison :

$$(*) |G| = |\mathcal{Z}(G)| + \begin{matrix} \text{Somme de diviseurs} \\ \text{de } |G| \text{ distincts de 1.} \end{matrix}$$

Prop 4.7: si G est un p -gpe (ie un \otimes est l'ordre est une puissance d'un nbr premier p) alors $\mathcal{Z}(G) \neq \{1\}$.

(ie $\exists g \in G, g \neq 1 \text{ et } g \in \mathcal{Z}(G)$)

$$3^1, 3^2, 3^3, 3^4.$$

Preuve: (*) modulo p donne

$$0 = |\mathcal{Z}(G)| + O \pmod{p}$$

$$\text{d'où } |\mathcal{Z}(G)| = O \pmod{p} \text{ et } |\mathcal{Z}(G)| \neq 1.$$

On peut dire $|\mathcal{Z}(G)| \geq p$.

5. Groupes symétriques

5.1. Définitions

$$\mathcal{S}_n = \text{Bij}(\{1, \dots, n\}) \quad \text{pour } n \geq 1.$$

gpe qui comporte \circ

NB: \mathcal{S}_n agit sur $X = \{1, \dots, n\}$ via le morphisme

$$\mathcal{S}_n \xrightarrow{\text{Id}} \text{Bij}(X) = \mathcal{S}_n$$

(cad: si $\sigma \in \mathcal{S}_n$ & $i \in \{1, \dots, n\}$; $\sigma \cdot i = \sigma(i)$)

D33 • Une permutad $\sigma \in \mathcal{S}_n$ se note $(\begin{smallmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{smallmatrix})$ où $\sigma(k) = i_k \in \mathcal{S}_n$

• On a cycle ou permutad circulaire de longueur k une permutad σ notée $(\begin{smallmatrix} i_1 & i_2 & \dots & i_k \\ \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_k) \end{smallmatrix})$ où $1 \leq k \leq n-1$

• L'ens $\{i_1, \dots, i_k\}$ est le souspot du cycle.

30

- Le support d'une permutation $\sigma \in S_n$ est l'ensemble $\{i \in E_n \mid \sigma(i) \neq i\}$.

- Un cycle de longueur k est **transposé**.

$\gamma_{i,j} = (i \ j)$ vérifie $\gamma_{i,j}(i) = j$, $\gamma_{i,j}(j) = i$ & pour $k \notin \{i, j\}$, $\gamma_{i,j}(k) = k$

$$\textcircled{P18} \quad |\mathfrak{S}_n| = n! \quad (\text{preuve } \textcircled{P8}).$$

5.2. Décomposition en cycles.

Théorème Toute permutation se décompose de manière unique (à l'ordre près) en produit de cycles à supports disjoints.

L1 Le support d'une permutation $\sigma \in S_n$ est stable sous l'acte du \mathfrak{S}_n engendré par σ .

$$\sigma \in S_n, \quad \sigma(\text{supp}(\sigma)) \subset \text{supp}(\sigma)$$

$$\text{où } \text{supp}(\sigma) = \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}$$

Preuve : soit $i \in \text{supp}(\sigma)$; $\sigma(i) \in \text{supp}(\sigma)$ car $\sigma(\sigma(i)) \neq \sigma(i)$ (puisque $\sigma(i) \neq i$ & σ injective)

$$\sigma(\sigma(\text{supp}(\sigma))) \subset \sigma(\text{supp}(\sigma)) \subset \text{supp}(\sigma)$$

L2 soit $\gamma \in S_m$ est un k -cycle, alors son support S contient exactement k élts & l'orbite de γ est de S de γ sous l'acte du groupe $\langle \gamma \rangle$ est le support S tout entier. $\langle \gamma \rangle \cong \mathbb{Z}/k\mathbb{Z}$. (groupe d'indice k et $\cong \mathbb{Z}/k\mathbb{Z}$
cycle est monoïd régulier)

$$@ \gamma \in \mathfrak{S}_5, \text{supp}(\gamma) = \{1, 2, 3, 4\} \neq \{1, 2, 3, 4, 5\}$$

$$\begin{aligned} \text{P} \text{ l'acte de } \langle \gamma \rangle \text{ sur } \{1, 2, \dots, 5\}, \quad & \gamma \in \Omega_1 \text{ car } ? \cdot 1 = 2 \\ & 5 \notin \Omega_1 \quad \left| \begin{array}{l} \gamma \cdot 1 = 2 \\ 3 \in \Omega_1 \text{ car } \gamma^2 \cdot 1 = 3 \\ 4 \in \Omega_1 \text{ car } \gamma^3 \cdot 1 = 4. \end{array} \right. \\ \text{de } \Omega_1 = \{1, 2, 3, 4\}. \quad & \end{aligned}$$

Enfin $\langle \gamma \rangle$ monoïd & $|\langle \gamma \rangle| = 4$

$$\text{car } \langle \gamma \rangle = \{\text{Id}, \gamma, \gamma^2, \gamma^3\}$$

$$(\gamma^4 = \text{Id} \\ \gamma^k \neq \text{Id}, 0 \leq k \leq 3)$$

$$\text{en général : } \gamma = (i_1 \ i_2 \ \dots \ i_k)$$

(P9) Deux cycles à supports disjoints commutent.

$$\tau = c_1 \circ \dots \circ c_m.$$

DS à savoir sauf

Chap "ens" | o TH 1
o Prop 6

chap "(9)" | o Prop 33 o TH 8
o Prop 34 o Prop 52

Ré $\mathfrak{S}_n = \text{Bij}(\{1, 2, \dots, n\})$

\mathfrak{S}_n agit sur $\{1, 2, \dots, n\}$ par le morphisme :

$$\mathfrak{S}_n \xrightarrow{\text{Id}} \text{Bij}(\{1, 2, \dots, n\}) = \mathfrak{S}_n$$

ie $\sigma \in \mathfrak{S}_n$ pr $i \in \{1, \dots, n\}$; $\sigma \circ i = \sigma(i)$.

Seulement pr $\sigma \in \mathfrak{S}_n$, on a une act du (9) $\langle \sigma \rangle$ sur $\{1, \dots, n\}$, donnée par le morphisme :

Prop 49, 50, Th 8 

 $\langle \sigma \rangle \xrightarrow{\text{Id}} \text{Bij}(\{1, \dots, n\})$.

(NB) $\langle \sigma \rangle \subset \mathfrak{S}_n$

① Le support d'une permutat $\sigma \in \mathfrak{S}_n$ est stable ss l'act du (9) de \mathfrak{S}_n engendré par σ .

Les orbites de σ st les orbites de l'act précédent

Voir DM. prop. 49

$\delta_1 = (i_1 \dots i_k)$, $\delta_2 = (j_1 \dots j_l)$ deux cycles de \mathfrak{S}_n dt supports $I = \{i_1, \dots, i_k\}$, $J = \{j_1, \dots, j_l\}$. & $I \cap J = \emptyset$.

Vérifier $\delta_1 \circ \delta_2 = \delta_2 \circ \delta_1$

1) cas $i \in I$: $\delta_1 \circ \delta_2(i) = \delta_1(i) = \delta_2 \circ \delta_1(i)$
car $\delta_2(i) = i$ & $\delta_1(i) \in I$ dc $\delta_2 \circ \delta_1(i) = \delta_1(i)$
car $i \in I$ et $I \not\subset J$

2) $i \in J$: $\delta_1 \circ \delta_2(i) = \delta_2 \circ \delta_1(i) = \delta_2(i)$
car $\delta_2(i) \in \delta_2(\text{supp}(\delta_2)) \subset \text{supp}(\delta_2)$

3) $i \notin I \& i \notin J$: $i \notin I \cup J$
 $\delta_1 \circ \delta_2(i) = i = \delta_2 \circ \delta_1(i) = i$

Des 2 cycles commutent

②

Q50 Le conjugué d'un k -cycle est un k -cycle & 2 cycles de m̄ longueur st conjugués.

(FF) pr $\sigma \in S_m$ & $(i_1 \dots i_k)$ un k -cycle de S_m :
 τ conjugué d'un k -cycle

$$\boxed{\begin{aligned} \tau \cdot (i_1 i_2 \dots i_k) \tau^{-1} = \\ = (\tau(i_1) \tau(i_2) \dots \tau(i_k)) \end{aligned}}$$

@ $(123)(1034)(132) = (234)$

@ $(32)(123)(3e) = (132)$

(FF) $\tau(i_1) \rightarrow \tau(i_2)$

$$\tau(i_1) \rightarrow \tau^{-1}(\tau(i_1)) = i_1 \rightarrow i_2 \rightarrow \tau(i_2)$$

Deux cycles de m̄ longueur st conjugués

$$\gamma_1 \in (4532) \in S_5$$

$$\gamma_2 \in (1352) \in S_5.$$

On a $\gamma_2 = \sigma \gamma_1 \sigma^{-1}$

$$\text{pour } \sigma = \begin{pmatrix} 4 & 5 & 8 & 3 & 1 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}$$

(Th) Tte permutations $\tau \in S_m$ s'écrit de façon uniq (à l'ordre près) comme produit

$\tau = c_1 \circ c_2 \circ \dots \circ c_m$ de cycles à supports disjoints.

$$c \circ \tau = \begin{pmatrix} 1 & 8 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 4 & 6 & 1 & 8 & 2 \end{pmatrix} \in S_8$$

$$\tau = (1348256) \quad 7\text{-cycle}$$

$$\circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 5 & 8 & 4 & 3 & 6 & 7 \end{pmatrix} = (12)(354876)$$

(L) Pr $\tau \in S_m$, \mathcal{O} une orbite de τ (ie \mathcal{O} est de la forme, pr i donné de $\{1, \dots, m\}$)

$$\mathcal{O} = \{\tau^t(i), t \in \mathbb{Z}\}$$

on a $\tau|\mathcal{O}$ est un cycle de longueur $\text{card}(\mathcal{O})$.

Chaque cycle ci pr Th^{es} correspond à un @ $\text{Prod}(23)_{\text{irr}} = (123) = (12)(23)$
restrict de τ à chaque de ses orbites.

Preuve ①: soit k le + petit entier > 0
tq $\tau^{(k)}(i) = i$. (voir @).

$$\text{alors } \mathcal{O} = \{i, \tau(i), \dots, \tau^{(k-1)}(i)\}$$

$$\text{NB: } \tau^k(i) = i$$

• les élts $i, \tau(i), \dots, \tau^{(k-1)}(i)$ st
distincts car si $\tau^{(l)}(i) = \tau^{(l')}(i)$
alors $\tau^{(l'-l)}(i) = i$.

pour $l, l' \in \{0, \dots, k-1\}; l < l'$

avec $0 < l'-l < k$.

Cor 6 Le G_9 symétriq \mathfrak{S}_n est engendré
par les transpos.

(ne st pas disjoints)

$$(i_1 i_2 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k)$$

Cor 7 Deux permutations τ & τ' de \mathfrak{S}_n
st conjugués si t q $t \in \mathfrak{S}_n$,
apparait m nbr k -cycles de leur
décomposition canoniq en produit de cycles
à supports disjoints.

$$@ \quad \bar{\tau} = (9352)(14)(67) \in \mathfrak{S}_9$$

$$\tau \in \mathfrak{S}_9$$

$$\{\text{conjugués de } \bar{\tau}\} = \{\tau \bar{\tau} \tau^{-1}, \tau \in \mathfrak{S}_9\}.$$

$$\text{Pr } \tau \in \mathfrak{S}_9,$$

$$\begin{aligned} \tau \bar{\tau} \tau^{-1} &= [\tau(9352) \tau^{-1}] [\tau(14) \tau^{-1}] [\tau(67) \tau^{-1}] \\ &= (\tau(9) \tau(3) \tau(5) \tau(2)) (\tau(1) \tau(4)) (\tau(6) \tau(7)) \end{aligned}$$

à la "forme" que $\bar{\tau}$
4-cycle • 2 cycle • 2 cycle.

Réciprocité - - - ordre (2) = ppcm(2,4) = 2

$$\alpha = (1234)(56)(78) \quad | \quad \epsilon(\alpha) = -1$$

Existe-t-il $\sigma \in S_9$ tel que $\alpha = \sigma^{-1} \circ \sigma$?

On prend $\sigma = \begin{pmatrix} 3 & 5 & 2 & 1 & 4 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} \in S_9$

$$\sigma = (153246789)$$

Prop 51 L'ordre d'une permutation $\tau \in S_m$ est égal au ppcm des longueurs des cycles à supports disjoints entrant dans la décomposition de τ .

5.3. Signature

D34 Soit $\sigma \in S_m$, signature de σ : $\epsilon(\sigma)$:

$$\frac{\prod_{1 \leq i < j \leq m} (\sigma(j) - \sigma(i))}{m!}$$

$$\frac{\prod_{1 \leq i < j \leq m} (j-i)}{m!}$$

P52 L'application $\epsilon: S_m \rightarrow \{-1, 1\}$ est MDG. ($\epsilon(\sigma \circ \tau) = \epsilon(\sigma) \circ \epsilon(\tau)$).

L'ensemble $\{-1, 1\}$ est un groupe multiplicatif isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Uniq morphisme résultant $\epsilon(\tau) = (-1)^k$ où k cycle de longueur τ .

Si transposés: signature toujours -1.

\circ $\sigma = (1234) \in S_4$.

$$\epsilon(\sigma) = \frac{(3-2)(4-2)(1-2)(4-3)(1-3)(1-4)}{(2-1)(3-1)(4-1)(3-2)(4-2)(4-3)}$$

D $\ker \epsilon = \{ \tau \in S_m, \epsilon(\tau) = 1 \}$

est DG distinguée de S_m d'indice 2 de S_m , qu'on appelle le G alterné.

\circ les 3-cycles (voir P54 G alterné engendré par les 3-cycles).

$$\textcircled{55} \quad (\dots) = (\dots)(\dots)(\dots) = (-1)^3 = -1$$

$$(\dots)_k = \begin{cases} 1 & \text{si } k \text{ impair} \\ -1 & \text{si } k \text{ pair} \end{cases}$$

signature

Ch2 : Anneau

D33 Un anneau $(A, +, \cdot)$ und inv munis d'opérations:

1. $(A, +)$ \circledcirc abélien
2. La mult est associative
3. — distributive

D40 A est un anneau si il possède un élément neutre. (\mathbb{Z}_A)

D41 Anneau commutatif \Leftrightarrow mult commutative.

\circledcirc $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{K}, +, \cdot)$ HS pas $(\mathbb{R}, +, \cdot)$
obtenu de (\mathbb{R})

L5 élément neutre de l'addition est absorbant par mult plaus.

P58 FFN si a et b sont éléments commutatifs d'un anneau A

$$(a+b)^m = \sum_{k=0}^m \binom{m}{k} a^k b^{m-k}$$

$\frac{m!}{k!(m-k)!}$

D42 Anneau intègre

si } commutatif

$$\forall (a, b) \in A^2, ab = 0 \Leftrightarrow a = 0 \text{ ou } b = 0$$

Si \mathbb{A} n'est pas intègre, $a, b \neq 0$ vérifient $ab = 0$ et divisibles de zéro.

\circledcirc $\mathbb{Z}/6\mathbb{Z}$ anneau non-intègre

car $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$ et $\bar{2}\bar{3} = \bar{0}$. $\bar{2}, \bar{3}$ et appellés diviseurs de zéro.

D43 Un élément de A est dit inv si $\exists b \in A$ tq $ab = 1$ & $ba = 1$, b : inverse de a , $b = a^{-1}$.

Notez $A^\times = U(A)$: ensemble des inv : dits unités de A .

(A^\times, \cdot) : \circledcirc abélien

Un anneau dont l'élément neutre et inv est corps

\circledcirc $(\mathbb{Q}, +, \cdot)$ anneau tq tt élémt $\frac{p}{q} \in \mathbb{Q} \setminus \{0\}$ est inv (et l'inverse $\frac{p}{q}$)

$\rightarrow (\mathbb{Q}, +, \cdot)$ est un corps.

$A^\times = \{a \in A, \exists b \in A, ab = 1\}$ et $A^\times = A \setminus \{0\}$!

P59 Tous corps commutatifs sont \circledcirc intègres.

D44 $B \subset A$ est s-à de A si \circledcirc unitaire

1. $(B, +)$ est \circledcirc $(A, +)$.
2. ens B stable par mult plaus
3. $1_A \in B$

$\Rightarrow (B, +, \cdot)$ est anneau.

$\mathbb{Z}/6\mathbb{Z}$ n'est pas un corps, $\frac{2 \times \frac{1}{2}}{2} = 1$. bcp d'inv!... $\mathbb{Z}/6\mathbb{Z} = \{-1, 1\}$

ce qui entraîne $\bar{3} \cdot \bar{2} \cdot \bar{2} = \bar{3} \cdot \bar{1}$

soit $\bar{0} = \bar{3}$ absurde.

$\mathbb{Z}/6\mathbb{Z}$ n'est pas un corps.

$\bar{2}$ n'a pas d'inverse:
sinon $\exists x \in \mathbb{Z}/6\mathbb{Z}$ tq $\bar{2} \cdot \bar{x} = \bar{1}$.

36

$$@ \mathbb{Z} \times \mathbb{Z} = \{(m, n) \mid m \in \mathbb{Z}, n \in \mathbb{Z}\}$$

$$+ : (m, n) + (m', n') = (m+m', n+n')$$

$$\times : (m, n) \times (m', n') = (mm', nn').$$

©23 $\forall n \in \mathbb{Z}$, $n\mathbb{Z}$ est un idéal de \mathbb{Z} .

Réqnt, tt idéal I de \mathbb{Z} est de la forme $n\mathbb{Z}$
tp $n \in \mathbb{Z}$.

95 $A @, B @ \Rightarrow A \times B @$ produit.

en \mathbb{Z} ~~est-a~~ de \mathbb{Q} .

Mais $2\mathbb{Z}$ pas ~~ss à~~ de \mathbb{Z} car $(1 \notin 2\mathbb{Z})$

mais $2\mathbb{Z}$ ~~ss à~~ de \mathbb{Z} car $+ \in 2\mathbb{Z}$ stable par \times .
et satisfait m : $\forall n \in \mathbb{Z}, \forall a \in 2\mathbb{Z}, an \in 2\mathbb{Z}$: $2\mathbb{Z}$ est idéal.

K9 • Tous les anneaux que nous étudierons sont supposés unitaires.

• On appelle aussi $0_A \neq 1_A$.

$$\text{sp } |A| \geq 2.$$

II / Idéaux

96 pie I d'un ~~com~~ A est un idéal

de A si 1) $(I, +) \rightarrow g (A, +)$

$$2) \forall a \in A, \forall x \in I, ax \in I.$$

Rq: idéaux à droite & à gauche
ds g rps idéaux st commut)

On sait déjà que ~~ss~~ de $(\mathbb{Z}, +)$ st les $n\mathbb{Z}$ de $n \in \mathbb{Z}$

~~TM1~~ Anneau quotient d'un ~~com~~ (\mathbb{A} , commut) A
par un idéal I :

$$(A/I, +, \times)$$

(+) celle du quotient A/I où A est vu à ~~ab~~
& I \supseteq ~~ss~~. (distingué)

$$A/I = \{a + I, a \in A\}$$

$$\times: (a+I), (b+I) \stackrel{\text{def}}{=} ab + I$$

$$\text{bien défini car } a+I = a'+I \\ b+I = b'+I$$

$$\text{alors } ab+I = a'b'+I$$

$$\begin{aligned} (\text{en effet } a'b' - ab) &= a'(b' - b) + a'b - ab \\ &= a' \underbrace{(b - b)}_{\in I} + b \underbrace{(a' - a)}_{\in I} \\ &\quad \underbrace{\in I}_{\in I} \end{aligned}$$

Reste à vérifier que les conditions de (P39) sont satisfaites.

D98 si $S \subseteq A$, l'idéal engendré par S est $\{ \sum_{\text{finie}} a_k s_k, a_k \in A, s_k \in S \}$

P60 si $A @$, $I @$ de A :

$$I = A \Leftrightarrow \exists u \in A^*, u \in I \Leftrightarrow 1_A \in I.$$

D47: si $I, J @$ de A :

$$I+J = \{x+y, x \in I, y \in J\}$$

$$IJ = \left\{ \sum_{\text{finie}} x_k y_k, x_k \in I, y_k \in J \right\}.$$

$$= \left\{ \text{somme finie de termes } xy \text{ où } x \in I \text{ et } y \in J \right\}$$

P61 si $I, J @$ de $A \Rightarrow I+J \& IJ$ @ de A .

Vérfions @ que

$\forall a \in A, \forall x \in IJ, ax \in IJ$:

$$\rightarrow \text{si } a \in A, x = \sum_{k=1}^n i_k j_k \text{ où } i_k \in I, j_k \in J, \rightarrow ax \in IJ$$

$$\rightarrow ax = \sum_{k=1}^n (a i_k) j_k \in IJ \quad \begin{array}{l} \text{car } j_k \in J, \\ a i_k \in I \end{array}$$

• Idéal engendré par $x \in A$:

$$(x) = \{ ax \mid a \in A \} \text{ noté } Ax.$$

Ce type d'idéal s'appelle un idéal principal.

Un @ des tgl de \mathbb{Z} est principal et @ ppl.

@ Un idéal de \mathbb{Z} est de la forme $n\mathbb{Z}$ où $n \in \mathbb{Z}$.
 \mathbb{Z} est un @ ppl d'@ id@ st pp@.

D49 un @ est dit premier si

$\forall a, b \in A, (ab \in I \Rightarrow a \in I \text{ ou } b \in I)$

• si A est intègre alors

$I = \{0_A\}$ est un idéal premier.

$$\Leftrightarrow (\forall \bar{a}, \bar{b} \in A/I) \quad \bar{ab} = \bar{0} \Rightarrow \bar{a} = \bar{0} \text{ ou } \bar{b} = \bar{0}$$

de A/I

P62 I est premier si A/I est un intégrle

P67 1) $\text{ker } \phi = \{x \in A, \phi(x) = 0_B\}$

2) $\text{Im } \phi = \phi(A)$, d'un MDA ϕ est \oplus de B

3) $\phi^{-1}(J) = \{x \in A, \phi(x) \in J\}$ est \ominus de A .

D50 Un idéal M d'un \oplus A est dit maximal si $M \neq A$ & si pour $\ominus I$ de A ,

$$M \subset I \quad \& \quad I \neq A \Rightarrow I = M.$$

$$\text{d'où } M \subset I \quad \& \quad M \neq I \Rightarrow I = A.$$

P64 Un idéal M est maximal si

l'anneau-quotient A/M est un corps

$$\begin{array}{c} \oplus: \mathbb{Z} \rightarrow \mathbb{Q} \\ x \mapsto x \end{array}$$

$2\mathbb{Z}$ idéal de \mathbb{Z} , $\mathbb{Q}/(2\mathbb{Z}) \cong \mathbb{Z}_2$ pas un idéal de \mathbb{Q} .

$2\mathbb{Z} \ni 2, 2$ inv de \mathbb{Q} .

RG: on a dc maximal \Rightarrow premier \Rightarrow P65.
(car corps \Rightarrow \oplus intégre).

Donc DM devrait $\neq 0$: M_0 devrait et inv.

P66 T est \oplus d'un \oplus A et contenu de \ominus man.

III / Morphismes d'Anns & TU posse à quelli

S51 $\oplus: A \rightarrow B$ est MDA si

$$\begin{array}{l} 1) \forall (n, y) \in A^2, \quad \oplus(n+y) = \oplus(n) + \oplus(y) \\ 2) \quad \quad \quad \oplus(n \cdot y) = \oplus(n) \cdot \oplus(y) \\ 3) \quad \quad \quad \oplus(1_A) = 1_B. \end{array}$$

(S9)

de [I est premier si A/I est un intégré]

P62

D50 Un idéal M d'un \mathbb{O} A est dit maximal si $M \neq A$ & si pour \mathbb{O} I de A,

$$M \subset I \text{ et } I \neq A \Rightarrow I = M.$$

$$\text{d'où } M \subset I \wedge I \neq A \Rightarrow I = A.$$

P64 Un idéal M est maximal si

l'anneau-quotient A/M est un corps

RG On a dc maximal \Rightarrow premié \Rightarrow P65.
(car corps \Rightarrow \mathbb{O} intégre).

Voir DM classe $\neq 0$: M_0 clste est inv.

P66 Tl \mathbb{O} d'un \mathbb{O} A est contenu dans \mathbb{O} max.

III / Morphismes d'Anneaux & TU posé à quitté

D51 $\phi: A \rightarrow B$ est MDA si

- 1) $(n+y)^c A^2$, $\phi(n+y) = \phi(n) + \phi(y)$
- 2) $\phi(n \cdot y) = \phi(n) \cdot \phi(y)$
- 3) $\phi(1_A) = 1_B$.

P67 1) $\ker \phi = \{x \in A, \phi(x) = 0_B\}$

2) $\text{Im } \phi = \phi(A)$, d'un MDA ϕ est \mathbb{O} de B

3) $\phi^{-1}(J) = \{n \in A, \phi(n) \in J\}$ est \mathbb{O} de A.

4).

$$\begin{array}{c} \phi: \mathbb{Z} \rightarrow \mathbb{Q} \\ x \mapsto x \end{array}$$

$2\mathbb{Z}$ idéal de \mathbb{Z} , $\mathbb{Q}/(2\mathbb{Z}) \cong \mathbb{Z}$ pas un idéal de \mathbb{Q} .

$2\mathbb{Z} \ni 2, 2$ inv de \mathbb{Q} .

§ 3. Morphismes d'anneaux

Δ D.51, P67. $\rightarrow \ker \phi, \text{Im } \phi, \phi^{-1}(J), \text{singularité}$

TU 12: (Th d'isomorphisme)

soit $\phi: A \rightarrow B$ un morphisme d'anneaux

soit I un idéal de A tq $I \subset \ker \phi$

alors $\phi: " passe au quotient modulo I "$, c'est à-dire:

$\exists!$ un morphisme d'anneau $\overline{\phi}: A/I \rightarrow B$

tq $\overline{\phi} \circ \sigma = \phi$, ie le diag ci-dessous commut.

(39)

$\left\{ \begin{array}{l} \text{voir ps.} \\ \text{voir ps.} \end{array} \right.$

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow s & \nearrow \overline{\phi} & \\ A/I & & \end{array}$$

où $s: A \rightarrow A/I$
est la
surjectivité canonique.

soit $s(a), s(b) \in A/I$

$$\begin{aligned} \overline{\phi}(s(a)s(b)) &= \overline{\phi}(s(ab)) = \phi(ab) = \phi(a)\phi(b) \\ &= \overline{\phi}(s(a))\overline{\phi}(s(b)). \end{aligned}$$

De plus $\text{Im } \overline{\phi} = \text{Im } \phi$

$$\ker \overline{\phi} = s(\ker \phi) = \ker \phi / I$$

¶ pour $I = \ker \phi$, on obtient

$$A/\ker \phi \cong \text{Im } \phi.$$

Preuve: $\phi: A \rightarrow B$ est MDG (abéliens)

On sait (par le 1^{er} TH d'isomorphisme pr les groupes) qu'il $\exists!$ morphisme de \mathcal{G}

$$\overline{\phi}: A/I \rightarrow B \text{ tq } \overline{\phi} \circ s = \phi$$

& que $\text{Im } \overline{\phi} = \text{Im } \phi$

$$\ker \overline{\phi} = s(\ker \phi).$$

On vérifie ensuite que $\overline{\phi}$ est un MDA:

$$\overline{\phi}(s(1_A)) = \phi(1_A) = 1_B$$

¶ $\ker \overline{\phi} = \ker \phi$,

$$\text{Im } \overline{\phi} = \text{Im } \phi$$

$$\ker \overline{\phi} = s(\ker \phi) = \{0\}$$

$$\text{dc } \overline{\phi}: A/\ker \phi \longrightarrow B$$

injectif & dc un isom. entre $A/\ker \phi \& \text{Im } \phi$

Correspondance entre idéaux d'un anneau
et d'un quotient de cet anneau

A anneau, K idéal de A. A/K anneau quotient.

Notat°: $\text{Id}(A/K) = \{ \text{idéaux de } A/K \}$

$\text{Id}_K(A) = \{ \text{idéaux de } A \text{ contenant } K \}$

$$s: A \longrightarrow A/K$$

surject°.

Considérons les applications :

$$f: \begin{array}{c} \mathbb{J}_{d_K}(A) \\ j \end{array} \longrightarrow \begin{array}{c} \mathbb{J}_d(A/K) \\ s(j) \end{array}$$

bien défini
p67
l'idéal est un sous-
ensemble de l'ensemble des idéaux de A/K

$$g: \begin{array}{c} \mathbb{J}_d(A/K) \\ J \end{array} \longrightarrow \begin{array}{c} \mathbb{J}_{d_K}(A) \\ s^{-1}(J) \end{array}$$

image unique.

J bien défini : $s^{-1}(J)$ idéal de A (p67)

$$\bullet s^{-1}(J) = s^{-1}(0_{A/K}) = \ker(s) = K$$

(Th) f & g st 2 bijections n'ayant pas l'une de l'autre. De plus, pour $j \in \mathbb{J}_{d_K}(A)$; on a :

$$A/J \cong \frac{A}{K} \xrightarrow{s(j)} A/J \cong \frac{A}{K}/J_K$$

(Rq) \circledast signifie que l'idéal J de A/K s'écrit de façon unique $J = s(j) = j/K$ le j idéal de A contenant K .

$(j \text{ idéal } \mathbb{Z}/12\mathbb{Z} \Rightarrow j = m\mathbb{Z}/12\mathbb{Z} \text{ et } m \in \mathbb{Z} \cap 12\mathbb{Z})$
cad $m|12$.

Premre $\Rightarrow f \circ g$? \circledast

$$\begin{aligned} \text{soit } J &\in \mathbb{J}_d(A/K), \quad f \circ g(J) = f(s^{-1}(J)) \\ &= s(s^{-1}(J)) = J \quad (\text{en utilisant "s surjectif"}) \end{aligned}$$

$\Rightarrow g \circ f$?

$$\text{soit } j \in \mathbb{J}_{d_K}(A),$$

$$g \circ f(j) = g(s(j)) = s^{-1}(s(j))$$

On a bien : $j \subset s^{-1}(s(j))$ tjs

soit $x \in s^{-1}(s(j))$, i.e. $s(x) \in s(j)$ i.e.
 $s(x) = s(j) \Leftrightarrow x \in j$

On a : $s(n-h) = 0_{A/K}$ i.e. $n-h \in K \subset j$

D'où $x = (n-h) + h \in j$

D'où $s^{-1}(s(h)) \subset j$.

idéal,

$$(\mathbb{Z}/12\mathbb{Z})$$

$\mathbb{Z}/12\mathbb{Z}$

$\in 3\mathbb{Z}/12\mathbb{Z}$ est \circledast de $\mathbb{Z}/12\mathbb{Z}$

41

⑥ Soit $j \in \text{Id}_K(A)$; comme $K \subset j = \ker(s_j)$,
la surjecto canoniq s_j
passe au quotient mod K :
 $A \xrightarrow{s_j} A/j$
 $\downarrow s$ $\downarrow \bar{s_j}$
 $A/K \xrightarrow{\bar{s_j}}$

$$\exists \bar{s_j} : A/K \rightarrow A/j$$

morphisme
tq $\bar{s_j} \circ s = s_j$

$$\text{De plus, } \text{Im } \bar{s_j} = \text{Im } s_j = A/j$$

$$\ker \bar{s_j} = s(\ker s_j) = s(j)$$

$$\frac{a}{s} \underset{\ker \bar{s_j}}{\cancel{\in A/K}} \simeq \text{Im } \bar{s_j}$$

$$\text{donne } A/K \underset{s(j)}{\cancel{/}} \simeq A/j$$

$$\frac{a}{s} : \text{classe d'équivalence du couple } (a, s) \left(\frac{1}{2}, \frac{2}{9}, \frac{3}{6} \right)$$

$$\left[\begin{array}{l} \\ \frac{a}{s} + \frac{a'}{s'} \end{array} \right]$$

P68
ans $((A \times \mathbb{R}) / R, +, \cdot)$ est corps dgf & $F_n(A)$.
 $\psi : A \rightarrow F_n(A)$ est MDA injectif.
 $a \mapsto \frac{a}{1}$
Le corps $F_n(A)$ est le + petit corps contenant A .

Rq $\frac{a}{s} \neq 0 \Leftrightarrow a \neq 0$ alors
on peut considérer $\frac{1}{a} \times \frac{a}{s} = 1$

Rq $\mathbb{Z} \rightarrow \mathbb{Q}$ MDA
 $m \mapsto \frac{m}{1}$ injectif
on identifie m & $\frac{m}{1}$.

Rq 0.49 Hypo en+ $I \neq A$!

Rq $R(x) = \left\{ \frac{P}{Q}, P \in R[x], Q \in (R[x])^*$

$A @ O$: nomb \mathbb{Z} , construct corps des fractions.

$$S = A^* = A \setminus \{0\}$$

$$(a, s) R(a, s') \Leftrightarrow (s'a - sa') = 0 \Leftrightarrow \frac{a}{s} = \frac{a'}{s'} \Leftrightarrow s'a = sa'$$

(48)

\mathbb{Z} n'est pas un corps car 2 n'a pas d'inverse.

§5. Anneaux principaux

(D52) Un \textcircled{a} de \mathbb{Z} est dt principal s'il est intègre & si tt idéal de \mathbb{Z} est principal, ie si I idéal de \mathbb{Z} ,
 $\exists n \in \mathbb{Z}, I = (n)$

\textcircled{a} des entiers

(D53) soit A \textcircled{a} un élé de A
 divise un élé b de A ,
 on note a/b si :

$$\left\{ \begin{array}{l} a/b \text{ si } \exists c, b=ac \\ \text{ou } bA \subset aA \end{array} \right.$$

\parallel

irréductible,

(D53) Un élé x d'un \textcircled{A} est dit irréductible,
 s'il n'est pas inv & si
 $\forall a, b \in A: (x=a \cdot b \Rightarrow a \text{ ou } b \text{ est inv})$

ie l'élé x ne pt pas s'écrire comme produit de 2 élés
 a & b de A sans que l'un des deux soit
 inversible.

$$n=1 \cdot n = n \cdot 1$$

$$3 = 1 \cdot 3 = 3 \cdot 1 = (-1)(-3) = (-3)(-1)$$

$$\textcircled{a} A = \mathbb{R}[x]$$

$$x^2 + 1 \text{ irréductible car } x^2 + 1 = A(x)B(x)$$

$$\Rightarrow \boxed{\deg A = 0 \text{ car } \deg B = 0}$$

$\Leftrightarrow A$ ou B est ds \mathbb{R}

$\Leftrightarrow A$ ou B est inversible ds $\mathbb{R}[x]$

(D54) soit A \textcircled{a} principal & $x \neq 0$ de A : ADÉ
 (i) élé x est irréductible.
 (ii) idéal (x) est premier.
 (iii) idéal (x) est maximal.

(D54) (iii) \Rightarrow (ii).

(ii) maximal $\Leftrightarrow A/(x)$ est un corps

$\Leftrightarrow A/(x)$ est intègre (quadratique)
 (c'est à dire premier)

$\Leftrightarrow (x)$ premier.

(i) \Rightarrow (ii)

supposons idéal engendré par x est premier. Mq q'il est
 irréductible

supposons $a, b \in A$, tq $x = ab$.

$ab \in$ idéal engendré par x car $x = ab$.

Mais x est premier; de sorte que a ou b est élé de (x) .

Supposons $a = bc$:
 $x = cnb = nbc \Leftrightarrow x(1_A - bc) = 0_A$ et $1_A - bc \neq 0_A$
 $\Rightarrow 1_A - bc = 0_A$
donc $bc = 1_A$ & b est inv.

§ 5.2 Décomposition en produit d'elts inéductibles

[Tout élmt d': il s'écrit à l'prod de 2 elts inéductibles]

Q55

(i) \Rightarrow (ii) M_q est corps.

Soit $\bar{y} \in A/(n) \neq 0$, dc $y \notin (n)$,

considérons $(x, y) = \{ax + by, (a, b) \in A^2\}$.

l'idéal engendré par un seul élmt.

Or $(x, y) = z \cdot$ dc $\exists 2$ els n', y de A

Thm 14

tq $x = zn'$ & $y = zg$.

soit z est inv
comme x est inéductible $\Rightarrow z$ est inv.

\rightarrow si x inv $\Rightarrow x = zn' \Rightarrow (x) = (z) \subset q$

est impossible, car $y \in (z) = (x, y)$ mais $y \notin (n)$.

\rightarrow dc y est inv & do q as $(z) = A$.

On a donc obtenu $\{ax + by, (a, b) \in A^2\} = A$, d'où l'A

de 2 els a & b tq $1_A = ax + by$ aussi

$\exists \bar{z} \in A/(n)$ tq $\bar{b} \cdot \bar{z} = \bar{1}_A$ - Tt est non nul dc

$A/(n)$ est de inv, $A/(n)$ est un corps, Q56 de l'idéal (n) est maximal. □

Prepared § 5.3, 5.6, 5.8 pour les 2 prochaines années.

$A @$ intègre, $a, b \in A$,

$a|b$ si $\exists c \in A$, $b = ac$

si $(a) \supset (b)$

si $b \in (a)$.

$a|b$ et $b|a \Leftrightarrow (a) = (b)$

$\Leftrightarrow b = ac$ & c inversible de A .

a & b sont dits associés.

5.3. Euclide, Gauss, Bézout.

556 $\text{pgcd}(a, b) = d \in A \rightarrow$ vérifie $\begin{cases} d|a \text{ et } d|b \\ \forall c \in A, c|a \text{ et } c|b \Rightarrow c|d \end{cases}$

$\text{ppcm}(a, b) = m \in A \rightarrow$ vérifie $\begin{cases} a|m \text{ et } b|m \\ \forall c \in A \text{ et } a|ac \text{ et } b|bc \Rightarrow m|c \end{cases}$

Rq $a, b \in A$ \downarrow idéal engendré par m .

$m = \text{ppcm}(a, b) \Leftrightarrow (m) = (a) \cap (b)$

$d = \text{pgcd}(a, b) \Leftrightarrow (d) = (a) + (b)$
= idéal engendré par a & b

En conséquence, si A est un pl alors $\text{pgcd}(a, b)$ & $(\text{ppcm})(a, b) \exists$ tjs.

En effet, $(a) + (b)$ est un idéal principal de la forme (d) & $d \in A$.

D'après ce q précéde, $d = \text{pgcd}(a, b)$ ($\text{cusp } m = \text{ppcm}(a, b)$)

Rq: pgcd défini au signe près.

$$\text{Rq} \quad a = u \prod_{i \in I} \alpha_i^{\alpha_i} \quad b = v \prod_{i \in I} \alpha_i^{\beta_i}$$

→ on affecte + petit exposant q apparaît de b

$$\text{si } a|b \Leftrightarrow \forall i \in I, \alpha_i \leq \beta_i$$

570 $A @$ pl, $\{\alpha_i, i \in I\}$ SDR $\in IA$

$a, b \in A$; u, v éts inv α_i, β_i min

$$a = u \prod_{i \in I} \alpha_i^{\alpha_i}, \quad b = v \prod_{i \in I} \alpha_i^{\beta_i} \quad \text{min max}$$

$$\Rightarrow \text{ppcm}(a, b) = \prod_{i \in I} \alpha_i^{\max(\alpha_i, \beta_i)}$$

$$\text{pgcd}(a, b) = \prod_{i \in I} \alpha_i^{\min(\alpha_i, \beta_i)}$$

575 $m + p$ tlt commun multiple = intérco idéal engendré par a & b

⑤ $a, b \in A$, $\exists p \in A$ st $p \text{ est pgcd}(a, b) = 1_A$
 Les nuls divs communs de $a \wedge b = 1_A$.
 $a \wedge b$ st les inv.

⑥ (Euclide)

• Soit $x \in \text{ap}^{\text{induct}} A$,

$$x \mid ab \Rightarrow x \mid a \text{ ou } x \mid b$$

⑦ DM

$$x \mid ab \Rightarrow x \mid a \text{ ou } x \mid b$$

$$\Leftrightarrow ab \in (x) \Rightarrow a \in (x) \text{ ou } b \in (x)$$

pple' Ideal premier

(do $A \oplus$, est ind engendre un ① premier). Psg

x est induct, d'après Psg, ① engendré par x est premier.

Rq: $a, b \in A$,

$$\text{pgcd}(ca, cb) = c \cdot \text{pgcd}(a, b)$$

Preuve: on fait que: $\min(\gamma + \alpha_i, \gamma + \beta_i) = \gamma + \min(\alpha_i, \beta_i)$

⑦ (Appl) $A \oplus, x \in A$,

$$n \mid ab \wedge \cancel{n \mid x} \Rightarrow n \mid b$$

$$a \wedge b = 1_A$$

$$\begin{array}{l} \text{DM: } \\ \left. \begin{array}{l} x \mid ab \\ n \mid ab \end{array} \right\} \Rightarrow x \mid \text{pgcd}(ab, ab) = b, \text{pgcd}(x, a) = b \end{array}$$

$$x \wedge a = 1_A$$

⑧ (Bézout) $A \oplus$ (on TD: bien le j'explique)

$$a, b \in A \Rightarrow (a) + (b) = a \wedge b = (d)$$

$$\rightarrow \text{si } a, b \text{ pcc}, (a) + (b) = A$$

$$\text{i.e. } \exists u, v \in A \text{ tq } \boxed{ua + vb = 1}.$$

(Preuve \leftrightarrow réécriture de la defis)

g pote' A soit \oplus .

⑨ faire \prod d'el R premia

$$c = \prod_{i \in I} x_i^{\alpha_i}$$

$$G \quad b = \prod_{i \in I} x_i^{\beta_i}$$

$$a = \prod_{i \in I} x_i^{\alpha_i}$$

§6. Anneaux euclidiens $\mathbb{Z}[x]$ (^{anneau des entiers de Gauss}) de posséder un plus petit él. k .
 @ d'anneaux ppk : \mathbb{Z} , $k[x]$ & k corps
contre-@ : $\mathbb{Z}[x]$, $\mathbb{Z}[\sqrt{5}]$

(les anneaux euclidiens st tjs ppk).

Euclidien \Rightarrow Principal.

⑥ A est euclidien s'il est intègre & muni DE. i.e $\exists \nu: A \setminus \{0\} \rightarrow \mathbb{N}$

(stathme euclidien) tq $\forall (a, b), b \neq 0, \in A \exists$

$\exists q, r \in A$, $a = bq + r$ & $(\nu(r) < \nu(b)$ ou $r=0$)

soit $a \in I \setminus \{0\}$ tq $\nu(a) = k$.
 soit $x \in I \setminus \{0\}$, $\exists q \& r$ ds A tq
 $x = aq + r$, $(\nu(r) < \nu(a) = k$ ou $r=0$)

mais $r = x - aq \in I$ aim p minimalité de k , on a $r=0$ d'où $r = aq \in (a)$, dc $I = (a)$

$I \subset (a)$
 $(a) \subset I$ puisq $a \in I$.

F7. ⑦ entiers de Gauss (voir TD)

⑧ Tt @ euclidien est pl.

or soit A @ euc, p def $\exists \nu: A \setminus \{0\} \rightarrow \mathbb{N}$.

But: Mq tt idéal est pl, soit I idéal de A.

(si idéal nul: bien pl car engendr p 0).

ppm $I \neq 0$, l'ens rpls nulos p $\nu(I) \setminus \{0\}$

$\nu(I \setminus \{0\}) = \{ \nu(x), x \in I, x \neq 0 \} \subset \mathbb{N}$

T Apl est !! ④

S8. (A) $\mathbb{Z}/m\mathbb{Z}$ (B) premiers et des indép. de \mathbb{Z}

(P76) L'^o \mathbb{Z} est euclidien de (p)

DIM

(Con) Les idéaux de \mathbb{Z} sont $m\mathbb{Z} = \{nh, h \in \mathbb{Z}\}$ pour $m \in \mathbb{N}$.

8.2. Congruences

(D) Soit $m \in \mathbb{N}^*$ entiers x & y de \mathbb{Z} st congrus modulo m , si m divise $x-y$
 $x \equiv y \pmod m \Leftrightarrow m | x-y \Leftrightarrow \exists k \in \mathbb{Z}, x = y + km$

(P77)

(P78)

(18)

(P79)

8.3. Elts inversibles

sont $n \in \mathbb{N}^*$, tels $\mathbb{Z}/n\mathbb{Z}$ @ q' n'est pas intègre en général.

$(\mathbb{Z}/n\mathbb{Z})^\times$?

$$\rightarrow \overline{5}, \overline{4}, \overline{3}, \overline{2}, \overline{1} \left(\begin{array}{l} \text{t' engendre} \\ (\mathbb{Z}/m\mathbb{Z}, +) \end{array} \right)$$

$$@ (\mathbb{Z}/6\mathbb{Z})^\times = \left\{ \overline{1}, \overline{5} \right\}$$

Un él't de 0 n'est jamais inversible.

Q+g) Les él't $(\mathbb{Z}/n\mathbb{Z})^\times = \{ \overline{k}, k \wedge n = 1 \}$

{ générat'n du g) $(\mathbb{Z}/n\mathbb{Z}, +)$. }

$$(i) k \wedge n = 1$$

$$(ii) (\mathbb{Z}/n\mathbb{Z})^\times = \{ \overline{k}, k \wedge n = 1 \}$$

(iii) t' engendre $\oplus (\mathbb{Z}/n\mathbb{Z}, +)$.

D.M. $n \wedge k = 1 \Rightarrow$ M.B. \exists entiers u, v tq

u $\overline{k} + v \overline{n} = 1$ soit $\overline{u} \cdot \overline{k} = \overline{1}$.

et q' pour ce \overline{k} est inversible.

(ii) \Rightarrow (iii)

Supposons \overline{k} inv de $\mathbb{Z}/n\mathbb{Z}$, $\exists \overline{u} \in \mathbb{Z}/n\mathbb{Z}$ tq $\overline{u} \cdot \overline{k} = \overline{1}$, d'où $\overline{1} \vee \in \mathbb{Z}$, $u \overline{k} + v \overline{n} = 1$. Dc $\forall a \in \mathbb{Z}$, on peut écrire $a = u \overline{k} + v \overline{n}$, d'où $\overline{a} = u \overline{k}$, et q' mq \overline{k} engendre $\oplus (\mathbb{Z}/n\mathbb{Z}, +)$.

(iii) \Rightarrow (i)

Supposons \overline{k} est générateur \oplus \Rightarrow q, $\exists u \in \mathbb{Z}$, $\overline{1} = \overline{u} \overline{k}$ par conséquent, \exists entier $v \in \mathbb{Z}$ tq $u \overline{k} + v \overline{n} = 1$, ainsi d'après Q+g) B'd'rest, d & n st pcc.

NB $u \overline{k} = \underbrace{\overline{k} + \overline{k} + \dots + \overline{k}}_{u \text{ fois}}$ $\overline{u} \overline{k}$

Corola $m \in \mathbb{N}^*$, $\mathbb{Z}/m\mathbb{Z}$ est corps si m=p premier

Rq. m premier si $m \wedge k = 1$ $\forall k=1, 2, \dots, p-1$

$$\text{si } (\mathbb{Z}/n\mathbb{Z})^\times = \{ \overline{1}, \overline{2}, \dots, \overline{p-1} \}$$

$$= (\mathbb{Z}/n\mathbb{Z}) \setminus \{ \overline{0} \}$$

⑥ ① $\phi(n) = \text{card}((\mathbb{Z}/_n\mathbb{Z})^*)$

= nbr de $k \in \{1, \dots, n\}$ tel que $k \perp n = 1$

② $\phi(6) = 2$
 $\phi(p) = p-1$

↑ indication d'Euler

③ soit $n \in \mathbb{N}^*$ alors $n = \sum_{d|n} \phi(d)$.

④ $6 = \phi(1) + \phi(2) + \phi(3) + \phi(6)$
 $6 = 1 + (2-1) + (3-1) + 2$

⑤ soit $n \in \mathbb{N}^*$, on sait \forall diviseur d de n ($d > 0$), $\exists !$ \mathcal{G}_d de $\mathbb{Z}/_n\mathbb{Z}$ d'ordre d .

soit $\mathcal{G}_d = \{\text{els d'ordre } d \text{ de } G\}$

On a $\mathcal{G}_d \subset \mathcal{C}_d$ (puisque un elt d'ordre d engendre un \mathcal{G}_d de $\mathbb{Z}/_n\mathbb{Z}$ d'ordre d , dc \mathcal{G}_d).

On a de $\mathcal{G}_d = \{\text{elts d'ordre } d \text{ de } \mathcal{C}_d\}$
 $= \{\text{elts d'ordre } d \text{ de } \mathbb{Z}/_d\mathbb{Z}\}$

car $\mathcal{C}_d \cong \mathbb{Z}/_d\mathbb{Z}$

alors $\mathcal{G}_d = \{\text{générateur de } \mathbb{Z}/_d\mathbb{Z}\}$

$\hookrightarrow \mathbb{Z}/_n\mathbb{Z} = \bigsqcup_{d|n} \mathcal{G}_d$

les cardinaux donnent

$n = \sum_{d|n} \phi(d)$