ARB. Christophe Mourougane

Chapitre I : Les anneaux $\mathbb{Z}/n\mathbb{Z}$.

I) Notions de groupes et d'anneaux.

1) Définitions

* Soit E un ensemble.
Une loi de composition interne ou une opération sur E est une application
$$f : E \times E \longrightarrow E$$
$$a, b \longrightarrow f(a, b)$$
* On note souvent $f(a, b)$ par $a * b$, $a \Delta b$ ou $a + b$
* Une opération $*$ sur un ensemble E est dite :
- associative si $\forall (a, b, c) \in E^3$
$$(a * b) * c = a * (b * c)$$
- commutative si $\forall (a, b) \in E^2$ $a * b = b * a$
- admet un élément neutre s'il existe $e \in E$ tq $\forall a \in E$, $a * e = e * a = a$.
- si $*$ admet un élément neutre e, on dit qu'un élément $x \in E$ admet y pour symétrique si $x * y = y * x = e$.

Prop : 1) Si $(E, *)$ admet un élément neutre, celui-ci est unique.
2) Si $(E, *)$ admet un élément neutre et si x admet un symétrique alors le symétrique de x est unique.

dem: 1) Soit e et e', 2 éléments neutres.

$\Rightarrow \begin{cases} e * e' = e & \text{car } e' \text{ neutre} \\ e * e' = e' & \text{car } e \text{ neutre} \end{cases}$

$\Rightarrow e = e'$

2) Soit y et y', 2 symétriques de $x \in E$.

$y = e * y = (y' * x) * y = y' * (x * y)$

$= y' * e = y'$.

Déf: Un groupe $(G, *)$ est un ensemble G muni d'une opération $*$ qui est: associative, qui admet un élément neutre et tq tt élément est un symétrique.

ex: $(\mathbb{Z}, +)$ est un groupe, d'élément neutre 0.
Le symétrique de $n \in \mathbb{Z}$ est $-n$.
$(\mathbb{Z}, \times)$ n'est pas un groupe. Par exc, 2 n'a pas de symétrique.

2) Sous groupes

Déf: Un sous groupe de G est une partie H de G stable par $*$ ($\forall (a,b) \in H$, $a * b \in H$ (dans G)) et si le symétrique de tt élément de H calculé dans G appartient à H et $e_G \in H$

Si H est un ss groupe de G, $(H, *)$ est un groupe.

ex: $\mathbb{N} \subset \mathbb{Z}$. $\mathbb{N}$ stable par + mais $2 \in \mathbb{N}$ et $-2 \notin \mathbb{N}$
$\Rightarrow \mathbb{N}$ n'est pas un ss groupe.
$2\mathbb{Z}$, l'ensemble des nb pairs est

un ss groupe de $\mathbb{Z}$. Si $n \in \mathbb{N}$, l'ensemble des multiples de n, noté $n\mathbb{Z}$ est un ss groupe de $(\mathbb{Z}, +)$.

3) Morphismes de groupes

Déf: Un morphisme de groupe $F : (G, *) \to (L, \Delta)$ entre 2 groupes est une application tq :
$\forall (g, h) \in G, \quad F(g * h) = F(g) \Delta F(h)$

Prop: Si $F(G, *) \longrightarrow (L, \Delta)$ est un morphisme de groupes :
i) $F(e_G) = e_L$
ii) $\forall g \in G \quad F(g^{-1}) = (F(g))'$
où g^{-1} désigne le symétrique de g dans G et $(F(g))'$ de $F(g)$ dans L

dem: i) $F(e_G * e_G) = F(e_G)$
$= F(e_G) \Delta F(e_G)$
car F morphisme.
$\Rightarrow [F(e_G)]' \Delta F(e_G) = e_L$
(On multiplie par le symétrique $[F(e_G)]'$ de $F(e_G)$)
$[F(e_G)]' \Delta (F(e_G) \Delta F(e_G)) = F(e_G)$
(par associativité).
ii) $F(g * g^{-1}) = F(e_G) = e_L$
$= F(g) \Delta F(g^{-1})$
$\Rightarrow F(g^{-1})$ est le symétrique de $F(g)$ dans L.

4) Sous groupe engendré par un élément.

Prop: Soit G un groupe et $(H_i)_{i \in I}$ des ss-

groupe de G. Alors l'intersection $\bigcap_{i\in I} H_i$ de tous les ss groupes H_i est encore un ss groupe de G.

dem: Soient $a, b \in \bigcap_{i\in I} H_i$.
$\forall i \in I$, $a, b \in H_i$
Comme H_i est un ss groupe, il est stable par $*$: $\forall i \in I$, $a*b \in H_i$
$a*b \in \bigcap_{i\in I} H_i$
$\Rightarrow \bigcap_{i\in I}$ est stable par $*$.
$\bigcap_{i\in I} H_i$ est stable par symétrique.
Comme e_G appartient à chaque H_i,
$\Rightarrow e_G \in \bigcap_{i\in I} H_i$

Def: Soit $(G, *)$ un groupe. Soit P une partie de G. L'intersection de tous les ss groupe de G contenant P est un sous groupe de G appelé ss groupe engendré par P.

Puissance d'un élément :
Soit $(G, *)$ un groupe et $x \in G$.
Soit $k \in \mathbb{Z}$.
↳ Si $k = 0$ On pose $x^0 = e_G$.
↳ Si $k \in \mathbb{N}^*$, on pose $x^k = \underbrace{x * \dots * x}_{k \text{ fois}}$
↳ Si $k \in -\mathbb{N}^*$, on pose :
$$x^k = \underbrace{x^{-1} * \dots * x^{-1}}_{-k \text{ fois}}.$$

Prop: Soit $(G, *)$ un groupe et $x \in G$.
Alors le ss groupe engendré par x est l'ensemble $\langle x \rangle$ des puissances de x.

$\langle x \rangle$ = le ss groupe engendré par x.

dem: Soit H un ss groupe de G contenant x.

My $H \supset \langle x \rangle$.

- $k = 0$ $\quad e_G \in H$.
- $k \in \mathbb{N}^*$ $\quad x^k = x^{k-1} * \dots * x \in H$ car stable par $*$.
- $k \in -\mathbb{N}^*$ $\quad x^k = x^{-1} * \dots * x^{-1} \in H$ car $x^{-1} \in H$.

Réciproquement My $H \subset \langle x \rangle$

- $\langle x \rangle \supset e_G$
- Si $(k, l) \in \mathbb{Z}^2$, $x^k * x^l = x^{k+l} \in \langle x \rangle$
- Si $x^k \in \langle x \rangle$, son symétrique est $x^{-k} \in \langle x \rangle$.

$\Rightarrow \langle x \rangle$ contient le ss groupe engendré par $\{x\}$.

Déf: Un groupe $(G, *)$ est dit: monogène
si $\exists x \in G$ tq $G = \langle x \rangle$.

- cyclique s'il est monogène et fini

5) Ecriture additive et multiplicative.

	$(G, *)$	élément neutre: e_G	symétrique: y'	puissances y^k
notation multiplicative	$(G, \times)$	1	inverse: y^{-1}	y^k
notation additive	$(G, +)$	0	opposé: $-y$	ky

NB: La notation additive est utilisé sur des groupes commutatifs (ou abélien).

ex: $(\mathbb{Z}, +)$ est monogène engendré par 1 (ou -1)

6) Anneaux

Def : Un anneau $(A, +, \cdot)$ est un ensemble A muni de 2 opérations $+$ et $\cdot$ tq :

(i) $(A, +)$ est un groupe abélien.

(ii) $\cdot$ est associative et admet un élément neutre.

iii) $\cdot$ est distributive par rapport à $+$.

ex : $(\mathbb{Z}, +, \times)$ est un anneau.

exercice : Vq la formule du binome est vraie dans tout anneau où $\cdot$ est commutative.

Def : Un anneau est dit commutatif si $\cdot$ est commutative.

7) Sous anneau.

Def Soit $(A, +, \cdot)$ un anneau. Une partie B de A est dite sous anneau de A si :

i) $0_A, 1_A \in B$.

ii) $(B, +)$ est un ss groupe de $(A, +)$ stable par $+$ et par passage à l'opposé.

iii) B est stable par $\cdot$.
($\forall b, c \in B \quad b \cdot c \in B$ calculé dans A).

II) L'anneau $(\mathbb{Z}, +, \times)$

Rq: Dans $(\mathbb{Z}, +, \times)$, si $n \in \mathbb{N}$, $a \in \mathbb{Z}$

$$na = \underbrace{a + a + \dots + a}_{n \text{ fois}} = n \times a.$$

Le ss groupe de $(\mathbb{Z}, +)$ engendré par $\{a\}$ est $\langle a \rangle$, l'ensemble des multiples de a.

Il est noté $\langle a \rangle = a\mathbb{Z} = \{n \in \mathbb{Z} \mid \exists k \in \mathbb{Z},\ n = \dots\}$

Th 1: Tout ss groupe de $(\mathbb{Z}, +)$ est monogène (c-à-d est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{Z}$).

Th 2: Soit $(a, b) \in \mathbb{Z}^2$ $(a, b) \neq (0, 0)$

(i) $a\mathbb{Z} \subset b\mathbb{Z} \iff a$ multiple de b

(ii) $a\mathbb{Z} + b\mathbb{Z}$ est un ss groupe.

$a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$

(iii) $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a, b)\mathbb{Z}$.

dem: (i) - $a\mathbb{Z} \subset b\mathbb{Z} \Rightarrow a = a \times 1 \in b\mathbb{Z}$

$\Rightarrow a$ multiple de b

- a multiple de $b \Rightarrow a \in b\mathbb{Z}$

Or $b\mathbb{Z}$ est un ss groupe de $(\mathbb{Z}, +)$

Donc le plus petit ss groupe contenant a noté $\langle a \rangle$ est inclus dans $b\mathbb{Z}$.

$\Leftrightarrow a\mathbb{Z} \subset b\mathbb{Z}$.

ii) $a\mathbb{Z} + b\mathbb{Z} = \{n \in \mathbb{Z} \mid \exists (u, v) \in \mathbb{Z}^2,\ n = \dots\}$

Il contient 0, est stable par $+$ et par passage à l'opposé. C'est donc un ss groupe de $(\mathbb{Z}, +)$.

a est multiple de $\text{pgcd}(a, b)$

$\Rightarrow a\mathbb{Z} \subset \text{pgcd}(a, b)\mathbb{Z}$.

De ii) $b\mathbb{Z} \subset \text{pgcd}(a,b)\mathbb{Z}$.

Comme $\text{pgcd}(a,b)\mathbb{Z}$ est stable par $+$:

$$a\mathbb{Z} + b\mathbb{Z} \subset \text{pgcd}(a,b)\mathbb{Z}.$$

Réciproquement, par Bézout : $\exists (u,v) \in \mathbb{Z}^2$

tq $\text{pgcd}(a,b) = au + bv$

$\Rightarrow \text{pgcd}(a,b) \in a\mathbb{Z} + b\mathbb{Z}$.

$\Rightarrow \text{pgcd}(a,b)\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$.

$\Rightarrow \text{pgcd}(a,b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

iii) $\text{ppcm}(a,b)$ est un multiple de a et de b $\Rightarrow \text{ppcm}(a,b)\mathbb{Z} \subset a\mathbb{Z}, b\mathbb{Z}$

$\Rightarrow \text{ppcm}(a,b)\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

Réciproquement : Soit $n \in a\mathbb{Z} \cap b\mathbb{Z}$.

n est multiple de a et de b.

$\Rightarrow n$ est multiple du $\text{ppcm}(a,b)$.

$\Rightarrow n \in \text{ppcm}(a,b)\mathbb{Z}$.

$$a\mathbb{Z} \cap b\mathbb{Z} \subset \text{ppcm}(a,b)\mathbb{Z}.$$

ex : $6\mathbb{Z} \subset 2\mathbb{Z}$ car 6 est multiple de 2.

dem : Th 1 : Soit H un sous groupe de $\mathbb{Z}$.

- Si $H = \{0\}$ alors $H = 0\mathbb{Z}$
- Sinon, il y a un élément non nul dans H : disons n.

n ou $-n$ est un élément strictement positif dans H (stable par symétrique)

Donc $H_n \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$.

Comme toute partie non vide de $\mathbb{N}$ admet un plus petit élément, appelons

$a = \min H \cap \mathbb{N}^*$.

Mq $H = a\mathbb{Z}$.

$a \in H$, H ss groupe de $\mathbb{Z}$ $\Rightarrow \langle a \rangle = a\mathbb{Z} \subset H$

Soit $h \in H$. On effectue la division euclidienne de h par a.

$\exists (q,r) \in \mathbb{Z}^2$ tq $h = aq + r$ $0 \leq r < a$.

$r = \underset{\in H}{h} - \underset{\in H}{aq} \in H$.

Donc r est un élément positif (strictement) de H plus petit que a.

Ceci contredit a minimal $\Rightarrow r = 0$.

$\Rightarrow h = aq \in a\mathbb{Z}$. ☒

III) Groupes et anneaux quotients

1) Classes modulo un sous groupe

Soit G un groupe et H un sous-groupe de G. La relation binaire sur G :

$x \mathcal{R}_H y \iff x^{-1}y \in H$.

est une relation réflexive, symétrique, transitive : c'est une <u>relation d'équivalence</u>, appelée relation à gauche modulo H.

L'ensemble $[x] = \{y \in G \mid x \mathcal{R}_H y\}$

$= \{y \in G \mid x^{-1}y \in H\} = \{y \in G, \exists h \in H / y = xh\}$

$= xH$

est appelé classe d'équivalence de x modulo H.

Puisque $\mathcal{R}_H$ est une relation d'équivalence, 2 classes d'équivalences sont soit égales soit disjointes. Les classes d'équivalence recouvrent G. Les classes d'équivalences forment une partition de G. On notera G/H l'ensemble des classes

d'équivalence pour cette relation.

Th. Lagrange

Si G est un groupe fini et H un sous groupe de G, alors :

$$\text{card } G = \text{card } H \times \text{card } G/H.$$

dem : card G/H = nb de classe d'équivalence

Mq que chaque classe d'équivalence a exactement card H éléments.

Soit $x \in G$.

L'application $\varphi : H \longrightarrow xH$
$h \longmapsto xh$

est une bijection.

↳ injective car si $\varphi(h) = \varphi(h')$
$\Rightarrow xh = xh' \quad h = h'$

↳ surjective, $xH = \{y \in G \mid \exists h \in H, y = xh\}$
$\forall y \in xH, \exists h \in H \mid y = xh = \varphi(h)$
donc φ surjective

$\Rightarrow$ Donc toute classe d'équivalence a card H éléments. □

N.B. Si G est un groupe fini, on appelle ordre de G son cardinal

Corollaire : Si G est un groupe fini et H un sous groupe de G alors l'ordre de H divise l'ordre de G.

Déf: Soit G un groupe et $g \in G$.
Si $\exists k \in \mathbb{N}^*$ tq $g^k = e_G$, on appelle ordre(g) le plus petit entier ℓ tq $g^\ell = e_G$

Prop: Soit G un groupe et g un élément d'ordre fini. Alors ordre(g) = ordre($\langle g \rangle$)
l'ordre de g est égal à l'ordre du sous groupe engendré par g.
En particulier, si G est fini, l'ordre de g divise l'ordre de G.

dem: Soit $g \in G$. Notons ℓ son ordre.
* Mq $e_G, g, g^2, \dots, g^{\ell-1}$: ℓ éléments distincts.
Si $g^a = g^b$ $0 \leq a < b \leq \ell - 1$
$(g^{-1})^a g^a = (g^{-1})^a g^b$
$\Rightarrow e_G = g^{b-a}$ $b-a < \ell = \text{ordre}(g)$.
$\Rightarrow b - a = 0 \Rightarrow a = b$.
* Mq $\langle g \rangle = \{e_G, g, g^2, \dots, g^{\ell-1}\}$
- $\langle g \rangle$ est l'ensemble des puissances de g.
$\Rightarrow \langle g \rangle \supset \{e_G, g, g^2, \dots, g^{\ell-1}\}$
- $\{e_G, g, \dots, g^{\ell-1}\}$ est un ss groupe de G contenant g, car $g^\ell = e_G$
Donc $\langle g \rangle \subset \{e_G, g, \dots, g^{\ell-1}\}$ □.

2) Opération sur l'ensemble quotient

Déf: Soit G un groupe et H un ss groupe de G.
H est dit distingué ou normal si
$\forall g \in G$, $\forall h \in H$ $\quad g h g^{-1} \in H$

Rq: Si G est commutatif, tous sous groupe est distingué.

Prop: Soit G un groupe et H un ss groupe distingué de G.

Si $x_1 \mathcal{R}_H x_2$ alors $x_1 y_1 \mathcal{R}_H x_2 y_2$

$y_1 \mathcal{R}_H y_2$.

La relation à gauche modulo H est compatible avec la multiplication.

dem: $x_1 \mathcal{R}_H x_2 \Rightarrow x_1^{-1} x_2 \in H \Rightarrow \exists k \in H \mid x_1^{-1} x_2 = k$

$y_1 \mathcal{R}_H y_2 \Rightarrow y_1^{-1} y_2 \in H. \Rightarrow \exists k \in H \mid y_1^{-1} y_2 = k$

$\Rightarrow x_2 = x_1 k$ et $y_2 = y_1 k$.

$\Rightarrow x_2 y_2 = x_1 k y_1 k$

$= x_1 y_1 \underbrace{y_1^{-1} k y_1}_{\in H} \underbrace{k}_{\in H}$. □

Construction de l'opération $\overline{*}$ sur G/H

Pour multiplier 2 éléments xH et yH de G/H on choisit $x_1 \in xH$ et $y_1 \in yH$ (des représentants de xH et yH) et on pose

$$xH \overline{*} yH = x_1 y_1 H$$

la proposition précédente montre que la classe $x_1 y_1 H$ ne dépend pas du choix de représentants.

Th.: 1) $(G/H, \overline{*})$ est un groupe (quand H est un ss groupe distingué de G.

2) L'application $(G, *) \longrightarrow (G/H, \overline{*})$

$x \longrightarrow [x] = xH$

est un morphisme de groupe.

3) Anneaux quotients

Déf : Soit $(A, +, \times)$ un anneau commutatif. Soit I une partie de A. I est appelé <u>idéal de</u> A si :
- $\hookrightarrow (I, +)$ est un sous-groupe de $(A, +)$
- $\hookrightarrow \forall a \in A, \forall i \in I, \quad a i \in I$.

Comme $(A,+)$ est un groupe commutatif, $(I, +)$ est un sous-groupe distingué de $(A, +)$. Donc $(A/I, \bar{+})$ est un groupe commutatif et l'application $\pi : (A,+) \to (A/I, \bar{+})$ est un morphisme de groupe.

Prop : Si I est un idéal de $(A, +, \times)$
Si $x_1 \mathcal{R}_I x_2$ alors $x_1 y_1 \mathcal{R}_I x_2 y_2$ et $y_1 \mathcal{R}_I y_2$
la multiplication est compatible avec la relation d'équivalence

Dém : Comme $x_1 \mathcal{R}_I x_2 \Rightarrow x_1 + x_2 \in I$.
$\Rightarrow \exists i \in I \;/\; x_2 = x_1 + i$
$y_1 \mathcal{R}_I y_2 \Rightarrow -y_1 + y_2 \in I$
$\Rightarrow \exists j \in I \;/\; y_2 = y_1 + j$
$x_2 \times y_2 = (x_1 + i)(y_1 + j)$
$= x_1 y_1 + i y_1 + x_1 j + ij$
$\in I \quad \in I \quad \in I$
$\Rightarrow x_1 \mathcal{R}_I x_1 y_1 \in I$. ∎

Thm : Si $(A, +, \times)$ est un anneau commutatif et I un idéal. On peut construire de façon naturelle une addition et une multiplication

sur l'ensemble quotient A/I (qui ne dépendent pas des représentants).
L'ensemble $(A, \bar{+}, \bar{\times})$ devient un anneau et l'application $(A, +, \times) \longrightarrow (A/I, \bar{+}, \bar{\times})$
$$a \longrightarrow a + I$$
devient un morphisme d'anneau.

IV) L'anneau $(\mathbb{Z}/a\mathbb{Z}, +, \times)$

Lemme: Les sous-groupes $a\mathbb{Z}$ de $(\mathbb{Z}, +)$ sont des idéaux de $(\mathbb{Z}, +, \times)$.

dem: Soit $a \in \mathbb{Z}$, $a\mathbb{Z}$ le sous-groupe des multiples de a. Soit $\hat{a} \in \mathbb{Z}$ et $i \in a\mathbb{Z}$
p.r.: $\exists k \in \mathbb{Z}$ tq $i = ka$.
$$\hat{a}i = \hat{a}(ka) = (\hat{a}k)a \in a\mathbb{Z}.$$
On peut donc construire les anneaux $(\mathbb{Z}/a\mathbb{Z}, +, \times)$.

Rq: Soient $n, n' \in \mathbb{Z}$.
$$n \mathcal{R}_{a\mathbb{Z}} n' \iff -n + n' \in a\mathbb{Z}.$$
$$\iff \exists k \in \mathbb{Z} \text{ tq } n' = n + ak$$
$$\iff n' \equiv n \,[a].$$

L'application $(\mathbb{Z}, +, \times) \longrightarrow (\mathbb{Z}/a\mathbb{Z}, +, \times)$
$$n \longrightarrow [n]_a = n + a\mathbb{Z}$$
est un morphisme d'anneau qui formalise l'application de reste modulo a.

Tables d'opération

$\star$ $(\mathbb{Z}/3\mathbb{Z}, +, \times)$

$+$	$[0]_3$	$[1]_3$	$[-1]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[-1]_3$
$[1]_3$	$[1]_3$	$[-1]_3$	$[0]_3$
$[2]_3 = [-1]_3$	$[-1]_3$	$[0]_3$	$[1]_3$

N.B : symétrie $\Leftrightarrow$ groupe commutatif.
carré latin $\Leftrightarrow$ Sur chaque colonne et sur chaque ligne on a tous les éléments une et une seule fois
$\Leftrightarrow$ on a un groupe et tous les éléments sont simplifiables.

$\times$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

carré latin

$\star$ $(\mathbb{Z}/4\mathbb{Z}, \times)$

n'est pas un carré latin.

$\times$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$			
$[2]_4$			$[0]_4$
$[3]_4$			

Déf : Soit $(A, +, \times)$ un anneau commutatif et $x \in A$.
- L'élément x est dit simplifiable (pour $\times$) si $\forall (y, z) \in A^2$ $x \times y = x \times z \Rightarrow y = z$.
- L'élément x est dit inversible (pour $\times$) si $\exists\, x' \in A$ tq $x x' = x' x = 1_A$.

Lemme : Si x est inversible alors il est simplifiable.

Prop: Soit $(A, +, \times)$ un anneau commutatif. Alors l'ensemble $(A^*, \times)$ des éléments inversibles de A muni de la multiplication est un groupe.

Ex: Soit $a \in \mathbb{Z}$

$[n]_a$ est inversible dans $\mathbb{Z}/a\mathbb{Z}$

$\Leftrightarrow \exists n' \in \mathbb{Z}$ tq $[n]_a [n']_a = [1]_a$

$\Leftrightarrow \exists n' \in \mathbb{Z}$ tq $nn' \equiv 1 [a]$

$\Leftrightarrow n$ est inversible modulo a.

$\Leftrightarrow n$ et a sont premier entre eux.

⇕

Csq: Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, les éléments inversibles sont les classes des éléments $m \in \mathbb{Z}$ premier avec n.

c-à-d: $[m] \in \mathbb{Z}/n\mathbb{Z}$ inversible

$\Leftrightarrow pgcd(m, n) = 1$

* Si $[a][b] = 0$ et $[a]$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors $[b] = 0$
* Si $ab \equiv 0 [n]$ et $a \wedge n = 1$
  $\Rightarrow b \equiv 0 [n]$.
* Si $n | ab$ et $n \wedge a = 1 \Rightarrow n | b$
  (lemme de Gauss).

Prop: Si $(A, +, \times)$ est un anneau commutatif l'ensemble A^* des éléments <u>inversibles</u> de A muni de la loi $\times$ est un <u>groupe</u>.

Ex: $(\mathbb{Z}/3\mathbb{Z})^* = \{[1], [2]\}$

$(\mathbb{Z}/4\mathbb{Z})^* = \{[1], [3]\}$

×	1	3
1	1	3
3	3	1

carré latin.

dem: ✓ la multiplication est bien définie
Si a et b sont inversibles, $a, b \in A^*$
$\exists a' \in A$ tq $aa' = 1$ et $\exists b' \in A$ tq $bb' = 1$.
$(ab)(b'a') = a(bb')a' = aa' = 1$.
Donc ab est inversible $ab \in A^*$
* la multiplication est associative sur A^* car elle l'est sur A.
* 1_A est neutre pour $(A^*, \times)$
* Si $a \in A^*$, a admet un inverse pour $\times$.
$\Rightarrow (A^*, \times)$ est un groupe □

Déf: $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe d'ordre (de cardinal) $\varphi(n)$ où φ est l'indicatrice d'Euler.
$\varphi(n)$ est le nbre d'entiers compris entre 1 et $n-1$, premiers avec n.

Pour ce groupe, le th de Lagrange donne :
L'ordre d'un élément de $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ divise l'ordre du groupe $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ c-à-d $\varphi(n)$: $\forall [m] \in A^*$, $[m]^{\varphi(n)} = [1]$

En termes de congruences :
Soit m premier avec n, alors $m^{\varphi(n)} \equiv 1 [n]$.
(Théorème d'Euler)
En particulier, si n est premier, $\varphi(n) = n-1$ on retrouve le petit théorème de Fermat.

Déf: Un anneau $(A, +, \times)$ est dit intègre si :
$\forall (a,b) \in A^2 \quad ab = 0 \Rightarrow a = 0$ ou $b = 0$.

ex: $\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$

Soit $[a], [b] \in \mathbb{Z}/3\mathbb{Z}$ tq $[a][b] = [ab] = [0]$

Supposons $[a] \neq [0]$. $a \neq 0 \ [3]$, $3 \nmid a$

Comme 3 est premier, 3 est premier avec a

$[a]$ est inversible donc simplifiable dans $\mathbb{Z}/3\mathbb{Z}$.

$[a][b] = [a][0]$, $[b] = [0]$.

$\Rightarrow \mathbb{Z}/3\mathbb{Z}$ est intègre.

$\mathbb{Z}/4\mathbb{Z}$ $[2] \neq [0]$ $[2][2] = [0]$

Donc $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre

Lemme : Si $n > 1$ est un entier, non premier alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Déf : Un anneau commutatif $(A, +, \times)$ est appelé corps si tout élément non nul de A est inversible ; autrement dit si $A^* = A \setminus \{0\}$.

Prop : Tout corps est intègre (démo en exo)

Th : Soit $n \geq 1$. L'anneau $\mathbb{Z}/n\mathbb{Z}, +, \times$ est un corps ssi n est premier

Dem : * Si n n'est pas premier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps car $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

* Si n est premier, soit $[a] \neq [0]$

donc $\mathbb{Z}/n\mathbb{Z}$.

$[a] \neq [0] \Rightarrow n \nmid a$ $\left.\begin{array}{l} \\ n \text{ premier} \end{array}\right\} \Rightarrow n \wedge a = 1$

$x \in \mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Factorisation des morphismes

Déf: Soit E un ensemble, $\mathcal{R}$ une relation d'équivalence sur E. f application de E vers un ensemble F.
L'application f est dite compatible avec la relation $\mathcal{R}$ si $\forall (x,y) \in E$ si $x \mathcal{R} y \Rightarrow f(x) = f(y)$
(f prend le même valeur sur tous les éléments d'une même classe d'équivalence)

ex: La relation de congruence modulo 2 sur $\mathbb{Z}$.

$f : \mathbb{Z} \to \mathbb{Z}$

$x \mapsto x$

0 ↦ 0
1 ↦ 1
2 ↦ 2
...

OK 2 mais $f(0) \neq f(2)$
Donc f n'est pas compatible.

Rappel: Si $\mathcal{R}$ est relation d'équivalence sur E, on a une application naturelle

$\pi : E \to E/\mathcal{R}$ ($E/\mathcal{R}$ l'ensemble des classes d'équivalence)

$x \mapsto \overline{x}$ (cette classe d'équivalence)
$= \{y \in E \mid y \mathcal{R} x\}$ de ...

Th: Factorisation des applications
Soit E un ensemble avec une relation d'équivalence $\mathcal{R}$. Soit f de E dans un ensemble F compatible avec $\mathcal{R}$.

Alors il existe une unique application

$\bar{f} : E/R \to F$ tq $f = \bar{f} \circ \pi$

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle \pi}\downarrow & \nearrow_{\bar{f}} & \\ E/R & & \end{array}$$

Rem : Soit $c \in E/R$ une classe d'équivalence
$\exists$ un représentant $x \in E$ tq $c = [x]$

$$\begin{array}{ccc} x & & E \to F \\ \downarrow & & \pi\downarrow \\ [x] = c \in E/R & & \end{array}$$

Nécessairement $f(c) = f(x)$.
Mais c admet d'autres représentants :
$\exists x' \in E \ / \ [x'] = c$.
Nécessairement $f(c) = f(x')$
Puisque f est compatible on a
$[x] = [x'] \iff x R x'$
et donc $f(x) = f(x')$
La définition de $\bar{f}$ ne dépend donc pas du représentant.
Avec ce choix :
$\bar{f} \circ \pi(x) = \bar{f}([x]) = f(x)$
car x est un représentant de $[x]$.
$\bar{f} \circ \pi = f$.

Lemme : Si $(G, \times)$ est un groupe et Γ un sous-groupe de G. On considère la relation à gauche modulo Γ.

$(x R_H y \Leftrightarrow x^{-1} y \in H)$.

Un morphisme de groupes $f : G \to G'$ est compatible avec cette relation si le noyau $N(f) = \{g \in G \mid f(g) = e_{G'}\}$ contient H.

dem : ⇒ Si $H \subset N(f)$,

Soit $x, y \in G$ tq $x R_H y$. $\Rightarrow x^{-1} y \in H$.

$\Rightarrow x^{-1} y \in N(f)$

$\Rightarrow f(x^{-1} y) = e_{G'}$ Comme f est morphisme de groupe

$\Leftrightarrow (f(x))^{-1} f(y) = e_{G'}$

$\Leftrightarrow f(y) = f(x)$.

⇐ Réciproquement, si f est compatible,

soit $h \in H$, $e_G^{-1} h \in H$

$e_G R_H h$, $f(e_G) = f(h) = e_{G'}$

car f est morphisme de groupes.

$\Rightarrow H \subset N(f)$

Th : Factorisation des morphismes de groupes

Soit G un groupe, H un sous groupe distingué de G. Soit $f : G \to G'$ un morphisme de groupes tq $N(f) \supset H$.

Alors il existe un morphisme de groupes $\tilde{f} : G/H \to G'$ tq $f = \tilde{f} \circ \pi$.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & \nearrow \tilde{f} & \\ G/H & & \end{array}$$

dem : Il suffit de vérifier que l'application $\tilde{f}$ construite précédemment est un morphisme de groupes.

Soit $x, y \in G/H$, $\tilde{f}(xy) = f(\dots)$ où $\dots$

Si $c, c' \in G/H \Rightarrow \exists x, y \in G$ tq $[x] = c$ et $[y] = c'$

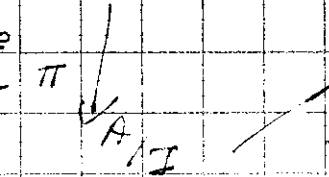
$\Rightarrow cc' = [x][y] = [xy]$.

$\phi(cc') = f(xy) = f(x) f(y) = \phi(c)\phi(c')$

Th: Factorisation des morphismes d'anneaux.

Soit $(A, +, \times)$ un anneau commutatif, I un idéal. Soit $f : A \to A'$ un morphisme d'anneaux tq $N(f) = \{a \in A \mid f(a) = 0_{A'}\} \supset I$.

Alors, il existe un morphisme d'anneaux $\tilde{f} : A/I \to A'$ tq $f = \tilde{f} \circ \pi$ où π est le morphisme d'anneaux $A \to A/I$.



Cas pour les anneaux $\mathbb{Z}/n\mathbb{Z}$

Pour la relation sur $\mathbb{Z}$ de congruence modulo n (c-à-d la relation à gauche modulo l'idéal $n\mathbb{Z}$)

l'application $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

a pour noyau $n \mapsto \overline{n}$

l'idéal $n\mathbb{Z}$ (l'ensemble des multiples de n).

Si $a \mathcal{R} b$ alors $a\mathbb{Z} = b\mathbb{Z}$

$b\mathbb{Z}$ est donc le noyau de $\pi_a : \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}$

π_a est donc compatible avec la relation modulo $b\mathbb{Z}$: $\mathbb{Z} \xrightarrow{\pi_a} \mathbb{Z}/a\mathbb{Z}$

$\pi_b \downarrow \quad \nearrow \pi$

$\mathbb{Z}/b\mathbb{Z}$

Il existe donc un morphisme d'anneaux π tq $\pi_a = \pi \circ \pi_b$

ex : 3 | 15 .

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

$\downarrow$ ↗

$\mathbb{Z}/15\mathbb{Z}$

Si $N = ab$ où $a, b \in \mathbb{Z}$, on a : $a \mid N$ et $b \mid N$

On peut donc construire $\mathbb{Z}/N\mathbb{Z} \xrightarrow{\varphi_a} \mathbb{Z}/a\mathbb{Z}$

$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\varphi_b} \mathbb{Z}/b\mathbb{Z}$

L'application $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

$c \mapsto (\varphi_a(c), \varphi_b(c))$

est un morphisme d'anneaux.

Th : Si a et b sont 2 entiers premiers entre eux (relatifs)

alors l'application précédente

$\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

est un isomorphisme d'anneaux

(une bijection dont la bijection réciproque est un morphisme d'anneaux).

(C'est le th chinois) $\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

$[c]_{ab} \mapsto ([c]_a, [c]_b)$

dem : $\operatorname{card}(\mathbb{Z}/ab\mathbb{Z}) = ab = \operatorname{card}(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})$.

Il suffit de MQ φ est injective.

Soit $c \in \mathbb{Z}/ab\mathbb{Z}$ tq $\varphi(c) = ([0]_a, [0]_b)$

$\exists x \in \mathbb{Z}$ tq $c = x.ab$

Alors $\varphi(c) = ([x]_a, [x.b])$

$\Rightarrow [x]_a = [0]_a$ et $[x.b] = [0]_b$

$\Rightarrow x \equiv 0 [a]$ et $x \equiv 0 [b]$

$\Rightarrow x$ est multiple de a et de b

$\Rightarrow x$ est un multiple de ppcm$(a,b) = ab$ car $a \wedge b = 1$

$\Rightarrow [x] = 0$

Donc φ est injective.

ex: $\mathbb{Z}/72\mathbb{Z} \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$.

Corollaire: Si m et n sont premier entre eux
$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est surjective.

c-à-d: $\forall (c,d) \in \mathbb{Z}^2$
$\exists x \in \mathbb{Z}$ tq $x \equiv c\,[m]$ et $x \equiv d\,[m]$

ex: $\begin{cases} x \equiv 1\,[12] \\ x \equiv 4\,[8] \end{cases}$ n'a pas de solution.

car $x \equiv 1\,[12] \Rightarrow x$ impair
et $x \equiv 4\,[8] \Rightarrow x$ pair.

Corollaire: Si $m \wedge n = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$
où φ est la fonction d'Euler.
c-à-d $\varphi(n) = \operatorname{card}\{k \in \mathbb{N}$ tq $k \leq n$ et $\operatorname{pgcd}(k,n) = 1\}$.

Rappel: $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ est inversible ssi $\operatorname{pgcd}(a,m) = 1$.
$\Rightarrow$ le nombre d'éléments inversibles dans $\mathbb{Z}/m\mathbb{Z}$ est donc $\varphi(m)$.

Par le TCR chinois, on a un isomorphisme d'anneau : $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Les groupes d'éléments inversibles sont donc aussi isomorphes.

$$\left((\mathbb{Z}/mn\mathbb{Z})^*, \times\right) \xrightarrow{\sim} \left((\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*, \times\right)$$

de cardinal $\varphi(mn)$ — de cardinal $\varphi(m)\varphi(n)$ $\left((\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*, \times\right)$.

ex : $(\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$

$(\mathbb{Z}/6\mathbb{Z})^* = \{[1]_6, [5]_6\}$

$(\mathbb{Z}/30\mathbb{Z})^* = \{[1]_{30}, [7]_{30}, [11]_{30}, [13]_{30}, [17]_{30}, [19]_{30}, [23]_{30}, [29]_{30}\}$

$\varphi(30) = 8$.

IV) Anneaux de polynômes en une variable sur un corps.

Soit $\mathbb{K}$ un corps commutatif ($\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ par ex). On note $(\mathbb{K}[X], +, \times)$ l'anneau des polynômes en une variable à coefficients dans $\mathbb{K}$.

Par exemple $[1]_7 X^3 + [-1]_7 X^2 + [3]_7 X + [4]_7 \in \mathbb{Z}/7\mathbb{Z}[X]$.

Mais dans $\mathbb{Z}/6\mathbb{Z}[X]$:

$X^3 + 4X^2 + X + 2$ | $2X^2 + 1$
$2^{-1} X$

La division euclidienne est impossible (2 n'a pas d'inverse)

D'où la nécessité d'avoir un corps

Rq : Si A est un anneau commutatif, $(A[X], +, \times)$ est aussi un anneau commutatif.

Th. : Soit $\mathbb{K}$ un corps commutatif,
Soient $D, A \in \mathbb{K}[X]$, $D \neq 0$.
Alors il existe un unique couple
$(Q, R) \in \mathbb{K}[X]^2$ tq :
$A = DQ + R$ avec $\deg R < \deg D$

Corollaire : Tous les idéaux de l'anneau $\mathbb{K}[X]$ sont principaux, c-à-d de la forme $F\,\mathbb{K}[X]$, l'ensemble des multiples d'un polynôme F.

Rq : Les idéaux de $\mathbb{Z}$ sont les ensembles de la forme $n\mathbb{Z}$.

Dem : *Les ensemble de la forme $F\,\mathbb{K}[X]$ sont des idéaux :
$\forall f \in F\,\mathbb{K}[X]$, $\forall g \in \mathbb{K}[X]$,
$fg \in F\,\mathbb{K}[X]$.
* Soit $I \neq \{0\}$ un idéal de $\mathbb{K}[X]$.
$\{d \in \mathbb{N} \text{ tq } \exists f \in I \quad \deg f = d\}$
est un ensemble non vide de $\mathbb{N}$
$\Rightarrow$ il a un plus petit élément.
Notons le d_0.
$\Rightarrow \exists f_0 \in I$ tq $\deg f_0 = d_0$.
Soit $f \in I$. Mq f est multiple de f_0.
J'effectue la division euclidienne de f par f_0 : $\exists (q, r) \in \mathbb{K}[X]^2$
tq $f = qf_0 + r$ et $\deg r < \deg f_0$.
$\Rightarrow r = \underbrace{f}_{\in I} - q\underbrace{f_0}_{\in I} \in I$.
Donc $r = 0$ $\Rightarrow f$ est multiple de f_0

- Si $I = \{0\} = (0)$ $K[X]$ trivial ■

Def: Soient A et B, 2 polynômes de $K[X]$.
On note $(A)+(B)$ l'idéal engendré par A et B c-à-d $AK[X]+BK[X]$, l'ensemble des multiples de A.

1) $(A)+(B)$ est un idéal.
Il existe un polynôme unitaire noté $pgcd(A,B)$ tq $(A)+(B) = (pgcd(A,B))$

2) $(A)\cap(B)$ est un idéal.
Il existe donc un polynôme unitaire noté $ppcm(A,B)$ tq $(A)\cap(B) = (ppcm(A,B))$

Dem: 1) Soit $P \in (A)+(B)$ et $P \in K[X]$.
$\Rightarrow$ Il existe $U, V \in K[X]$ tq
$P = UA + VB$.
Or $P = AP + BP \in (A)+(B)$ ■
$\exists$ donc $P_0 \in K[X]$ tq $(P_0) = (A)+(B)$
$P_0 = a_d X^d + \dots + a_0$
$= a_d (X^d + a_d^{-1} a_{d-1} X^{d-1} + \dots + a_d^{-1} a_0)$.
$a_d^{-1} P_0 \in I$ $\deg(a_d^{-1} P_0) = \deg(P_0)$
$a_d^{-1} P_0$ est unitaire et
$(a_d^{-1} P_0) = (A)+(B)$.

IV Corps de fractions.

L'anneau $(\mathbb{Z}, +, \times)$ a le défaut suivant:
L'équation $x = 3$ a une solution mais pas $5x = 3$. (car 5 n'a pas d'inverse dans $\mathbb{Z}$).

Soit $(A, +, \times)$ un anneau commutatif. On définit une relation binaire $\mathcal{R}$ sur $A \times (A - \{0\})$

$(a,d) \mathcal{R} (a',d') \iff ad' = a'd$

↳ réflexivité : $(a,d) \mathcal{R} (a,d)$

↳ symétrie : Soit $(a,d) \mathcal{R} (a',d')$

$\Rightarrow ad' = a'd \Rightarrow a'd = ad'$

$\Rightarrow (a',d') \mathcal{R} (a,d)$

↳ transitivité : Soit $(a,d) \mathcal{R} (a',d')$ et $(a',d') \mathcal{R} (a'',d'')$; $ad' = a'd$ et $a'd'' = a''d$

On a : $d'(ad'' + a''d) = ad'd'' + a''d'd = 0$.

Si A est intègre, comme $d' \neq 0$

on en déduit que $ad'' = a''d$ ☒.

tk : Soit $(A, +, \times)$ un anneau commutatif et intègre. Alors la relation binaire sur $A \times (A - \{0\})$ précédente est une relation d'équivalence.

* L'ensemble quotient $\frac{A \times (A - \{0\})}{\mathcal{R}}$ (l'ensemble des classes d'équivalences) peut être muni de 2 opérations $\oplus$ et $\otimes$ telles que $\left(\frac{A \times (A - \{0\})}{\mathcal{R}}, \oplus, \otimes\right)$ soit un corps qui contient A comme sous anneau.

dem : * Construction de l'addition $\oplus$ sur $A \times (A - \{0\})/\mathcal{R}$.

Soient $q, q' \in A \times (A - \{0\})/\mathcal{R}$.

Il existe $(a,d) \in A \times (A - \{0\})$ tq q soit la classe de (a,d).

Il existe aussi $(a',d') \in A \times (A - \{0\})$ tq q' soit la classe de (a',d')

On choisit pour $q \oplus q'$ la classe de $(ad' + a'd, dd')$. Comme A est intègre, $dd' \neq 0$.
On vérifie que cette construction ne dépend pas des choix des représentants (a,d) de q, (a',d') de q'.
Si q est la classe de (A,D) et q' la classe de (A',D')
Donc $(A,D) \mathcal{R} (a,d)$ et $(A',D') \mathcal{R} (a',d')$
et $Ad = aD$, $A'd' = a'D'$
Vérifions que $(ad' + a'd, dd') \mathcal{R} (AD' + A'D, DD')$
(en exo).

* Mq tout élément non nul de $(A \times (A \setminus \{0\}))/\mathcal{R}$ admet un inverse.
L'élément neutre de l'addition $\oplus$ sur K est la classe de $(0, 1_A)$.
Soit q non nul dans K. q est la classe d'un élément de la forme (a,d) avec $d \neq 0$ et $a \neq 0$. Un inverse de q est alors la classe de (d,a).
$[(d,a)] * [(a,d)] = [(da, da)] = [(1,1)]$
élément neutre de $\otimes$

* Mq K contient A un sous corps.
$(A, +, \times) \to (K, \oplus, \otimes)$
$a \mapsto [(a, 1_A)]$ est un morphisme d'anneaux qui est injectif.
(car $[(a, 1_A)] = [(b, 1_A)] \Rightarrow a 1_A = b 1_A \Rightarrow a = b$)

Conc : $(K, +, \times)$ est commutatif intègre. Le corps des fractions associé à $(A \setminus \{0\})/\mathcal{R}$ est noté $\mathbb{Q}$, le corps

des rationnels.

$\mathbb{Z} \hookrightarrow \mathbb{Q}$

$n \mapsto \frac{n}{1} = [(n, 1)]$

L'équation $3x = 5$ admet $[(5, 3)] = \frac{5}{3}$ comme solution.

* Si A est un anneau intègre commutatif (par ex un corps commutatif), $(A[X], +, \times)$ est un anneau intègre commutatif.

Le corps des fractions associé $A[X] \times (A[X] \setminus \{0\})$ / $\mathcal{R}$ est noté $A(X)$, l'ensemble des fractions rationnelles en une variable à coeff dans A (représentées par le quotient de 2 polynômes de $A[X]$, le second étant non nul).

Chapitre 2 :
Exemples de groupes et d'anneaux

I) Les groupes cycliques

Déf : * Un groupe $(G, *)$ est dit monogène s'il existe un élément $a \in G$ tq le sous groupe $\langle a \rangle$ engendré par a est le groupe G tout entier.
(On dit alors que a est un générateur de G)
* Un groupe $(G, *)$ est dit cyclique s'il est monogène et fini.

Rq : Si G est monogène engendré par a,
$\forall g \in G$, $\exists m \in \mathbb{Z}$ tq $g = a^m$
$g = a^m = \underbrace{a * \cdots * a}_{m \text{ fois}} = a^{-1} * \cdots * a^{-1}$
$= m$ fois si $m \in \mathbb{N}$.
En particulier, G est donc commutatif.
$\forall g \in G$, $g' \in G$,
$\exists m, m' \in \mathbb{Z}$ tq $g = a^m$ et $g' = a^{m'}$.
$g * g' = a^m * a^{m'} = a^{m+m'} = a^{m'} * a^m = g' * g$

exo : Trouver un groupe cyclique d'ordre 4.
non cyclique d'ordre 4.

$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +) = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\}$
$\langle (\bar{0},\bar{0}) \rangle = \{ m(\bar{0},\bar{0}),\ m \in \mathbb{Z} \} = \{(\bar{0},\bar{0})\}$
$\langle (\bar{1},\bar{0}) \rangle = \{ m(\bar{1},\bar{0}),\ m \in \mathbb{Z} \}$
$= \{(\bar{0},\bar{0}), (\bar{1},\bar{0})\}$
$\langle (\bar{0},\bar{1}) \rangle = \{(\bar{0},\bar{0}), (\bar{0},\bar{1})\}$

$\langle (1,1) \rangle = \{(0,0), (1,1)\}$

$\Rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas monogène

donc non cyclique

$\mathbb{Z}/4\mathbb{Z}$ est monogène engendré par $\bar{1}$ ou $\bar{3}$

c.c. $(\mathbb{Z}, +)$ est monogène engendré par 1

$(\mathbb{Q}, +)$ n'est pas monogène.

En effet, soit $a \in \mathbb{Q}$. a s'écrit

$a = \frac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{Z}^*$, $p \wedge q = 1$

$\langle a \rangle = \{ r \in \mathbb{Q}, \exists m \in \mathbb{Z}^*, r = \frac{mp}{q} \}$

Donc $\forall r \in \langle a \rangle$, $qr \in \mathbb{Z}$.

Mais si $q \neq 1, -1$, $q \frac{1}{q^2} \notin \mathbb{Z}$

$\frac{1}{q^2} \in \mathbb{Q}$, $\frac{1}{q^2} \notin \langle a \rangle$.

Donc a n'est pas un générateur de $\mathbb{Q}$

$((\mathbb{Z}/7\mathbb{Z})^*, \times) = \{1, 2, 3, 4, 5, 6\}$.

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{1, 2, 4\}$

$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\}$

C'est un groupe cyclique engendré par 3. (Rq : 5 est aussi générateur).

exo : $(\mathbb{Z}/9\mathbb{Z})^*$ est-il cyclique ?

Rappel : Un élément a d'un groupe G est d'ordre fini s'il existe un entier $k \in \mathbb{N} - \{0\}$ tq $a^k = e_G$.

* L'ordre d'un élément a d'ordre fini dans un groupe G est $\min \{k \in \mathbb{N} - \{0\} / a^k = e_G\}$

* Si a est un élément d'ordre fini ν alors $\langle a \rangle = \{e_G, a, a^2, \dots, a^{\nu-1}\}$

En particulier $\text{ord}(a) = \text{ord}\langle a \rangle$.

Prop: Tous les groupes cycliques d'ordre n sont isomorphes à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Ex: $((\mathbb{Z}/7\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/6\mathbb{Z}, +)$.

Dém: Soit G un groupe cyclique d'ordre n, engendré par un élément $a \in G$

$$\begin{aligned} f : (\mathbb{Z}, +) &\to (G, *) \\ m &\mapsto a^m \end{aligned}$$

↳ f est un morphisme de groupe :

soit $m, m' \in \mathbb{Z}$:

$$f(m+m') = a^{m+m'} = \underbrace{a * a * \cdots * a}_{m+m' \text{ fois}}$$

$$f(m) * f(m') = a^m * a^{m'} = \underbrace{a * \cdots * a}_{m \text{ fois}} * \underbrace{a * \cdots * a}_{m' \text{ fois}}$$

↳ L'image de f est $\{a^m, m \in \mathbb{Z}\} = G$

$\Rightarrow f$ est surjective.

↳ Le noyau f est $\{m \in \mathbb{Z} \mid f(m) = a^m = e_G\}$

Lemme : Soit $a \in G$, un élément d'ordre λ.

Soit $m \in \mathbb{Z}$ alors $a^m = e_G$

$\Leftrightarrow m$ est multiple de λ.

Ici le noyau de f est l'ensemble des multiples de $\text{ord}(a) = n$.

Par factorisation de f, on obtient :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & G \\ \downarrow & \nearrow \bar{f} \text{ isomorphisme car :} & \begin{cases} \text{Im } f = G \\ \ker f = n\mathbb{Z}. \end{cases} \\ \mathbb{Z}/n\mathbb{Z} & & \end{array}$$

Lem : (du lemme).

• Si $m = k\lambda$, $k \in \mathbb{Z}$ alors $a^m = a^{k\lambda} = (a^\lambda)^k = e_G^k = e_G$

* Réciproquement si $a^m = e_G$

On effectue la division euclidienne de m par ν :

$\exists q \in \mathbb{Z}$, $\exists r \in \mathbb{Z}$ $\quad m = q\nu + r \quad 0 \leq r < \nu$

$\Rightarrow a^r = a^{m-q\nu} = a^m (a^\nu)^{(-q)} = e_G$

$\Rightarrow r = 0$.

$\Rightarrow m$ est multiple de ν $\quad \square$.

Lemme: Soit $(G, \star)$ un groupe et a un élément d'ordre ν. Soit $k \in \mathbb{Z}$.

Alors, l'ordre de a^k est $\dfrac{\nu}{\operatorname{pgcd}(\nu, k)}$.

En particulier $\operatorname{ord}(a^k) = \operatorname{ord}(a)$

$\Leftrightarrow k \wedge \operatorname{ord}(a) = 1$.

Dem: Soit $d = \operatorname{pgcd}(\nu, k) \Rightarrow \nu = d\nu'$ et $k = dk'$

et on a $\operatorname{pgcd}(\nu', k') = 1$.

$$\frac{\nu}{\operatorname{pgcd}(\nu, k)} = \nu'.$$

et $(a^k)^{\nu'} = a^{dk'\nu'} = (a^\nu)^{k'} = e_G^{k'} = e_G$

$\Rightarrow \nu'$ est un multiple de l'ordre de a^k

Et $(a^k)^{\operatorname{ord}(a^k)} = e_G = a^{k \operatorname{ord}(a^k)}$

$\Rightarrow k \operatorname{ord}(a^k)$ est un multiple de $\operatorname{ord}(a) = \nu$.

et $d k' \operatorname{ord}(a^k)$ — — — de $d\nu'$

et $k' \operatorname{ord}(a^k)$ — — — de ν'

$\Rightarrow \nu' \mid k' \operatorname{ord}(a^k)$

or $\nu' \wedge k' = 1$, par le lemme de Gauss

$\nu' \mid \operatorname{ord}(a^k)$

$\Rightarrow \nu' = \operatorname{ord}(a^k)$.

Th: Tout groupe cyclique d'ordre n admet exactement $\varphi(n)$ générateurs où φ est la fonction Phi d'Euler.

Ex: $(\mathbb{Z}/7\mathbb{Z})^*$ est cyclique d'ordre 6
$\varphi(6) = \varphi(2\times 3) = \varphi(2)\cdot\varphi(3) = 1\times 2 = 2$.
Les générateurs sont 3 et 5.

dem: Si a un générateur de G. G est un élément d'ordre n. Les générateurs de G sont exactement les éléments d'ordre n. $G = \langle a \rangle = \{e_G, a, a^2, \dots, a^{n-1}\}$
$\mathrm{ord}(a^k) = \mathrm{ord}(a) = n$ ssi $k \wedge n = 1$.
Or $\varphi(n) = \mathrm{card}\{k \in \{1, \dots, n-1\} \mid \gcd(k,n) = 1\}$

Prop: Soit G un groupe cyclique d'ordre n soit d un diviseur de n.
Soit $U_d = \{g \in G \mid g^d = e_G\}$
Alors U_d est un sous groupe de G, d'ordre d, cyclique. C'est le seul sous groupe de G d'ordre d.
En particulier, tous les sous groupes des groupe cycliques sont cycliques.
G admet exactement $\varphi(d)$ éléments d'ordre d.

dem: $\star$ $e_G^d = e_G$ donc $e_G \in U_d$
$\star$ Soit $g \in U_d$ $(g^{-1})^d = (g^d)^{-1} = e_G^{-1} = e_G$
$\star$ Soit $g \in U_d$, $g' \in U_d$
$(g \star g')^d = \underbrace{(g \star g') \star (g \star g') \star \cdots \star (g \star g')}_{d \text{ fois}}$
G commutatif
$= g^d \star (g')^d = e_G \star e_G = e_G$
Donc U_d est un sous groupe. cf (*)

Soit a un générateur de G et d un diviseur de n. $\exists\, n' \in \mathbb{N}$ tq $n = d n'$

$$\mathrm{ord}(a^{n'}) = \frac{\mathrm{ord}(a)}{\gcd(\mathrm{ord}(a), n')} = \frac{n}{\gcd(n, n')} = \frac{n}{n'} = d.$$

$a^{n'} \in U_d$, $\langle a^{n'} \rangle \subset U_d$

Soit $g \in U_d$. $\exists\, m \in \mathbb{Z}$ tq $g = a^m$ (car g est cyclique) $g^d = e$, $c = a^{mnd}$

Donc mnd est un multiple de $n = \mathrm{ord}(a) = dn'$

$\Leftrightarrow$ m est un multiple de n'

Donc $U_d \subset \langle a^{n'} \rangle$.

Corollaire: Dans un groupe cyclique d'ordre n, pour tout diviseur d de n il y a $\varphi(d)$ éléments d'ordre d.

$$n = \sum_{d \text{ diviseur de } n} \varphi(d)$$

Rem: • Soit g un élément d'ordre d cyclique. $g \in U_d$ est générateur du groupe U_d.

• Réciproquement, tout générateur de U_d est d'ordre d.

• Il y a donc, dans G, autant d'éléments d'ordre d que de générateur U_d, c-à-d $\varphi(d)$.

• G = $\{$ éléments d'ordre $1\} \cup \{$ éléments d'ordre $d_1\} \cup \dots \cup \{$ éléments d'ordre $d_k\}$ est une partition de G.

$$\mathrm{card}\, G = n = \sum_{d \text{ diviseur } n} \varphi(d).$$

(*) Tous les sous-groupes d'un groupe cyclique sont cycliques. Soit $H \subset G$ un sous-groupe

Par le th de Lagrange, $\mathrm{ord}(H)$ est un diviseur de $\mathrm{ord}(G) = n$. On note d.

$\forall g \in H$, $g^d = e_G$, donc $H \subset V_d$

Comme $\mathrm{card}\, H = \mathrm{card}\, V_d \Rightarrow H = V_d$ □

Th: Soit G un groupe fini d'ordre n.

On note pour tout diviseur d de n

$V_d = \{ g \in G \ / \ g^d = e_G \}$

et $\alpha_G(d)$ le nombre d'éléments d'ordre d dans G. Il y a équivalence entre :

i) $\forall d$ diviseur de n $\quad \mathrm{card}\, V_d \leq d$

ii) $\forall d$ diviseur de n $\quad \alpha_G(d) \leq \varphi(d)$

iii) $\forall d$ diviseur de n $\quad \alpha_G(d) = \varphi(d)$

iv) G est cyclique

v) $\forall d$ diviseur de n $\quad \mathrm{card}\, V_d = d$

Dem: i) $\Rightarrow$ ii) Soit d un diviseur de n.

Supposons $\# V_d \leq d$.

* Si $\alpha_G(d) \geq 1$, il y a un élément x d'ordre d. Par le th. de Lagrange, $\langle x \rangle \subset V_d$. Comme $\# \langle x \rangle = d$ et $\# V_d \leq d$ on a : $\langle x \rangle = V_d$

Les éléments de G sont dans V_d, et sont donc générateur du groupe cyclique $\langle x \rangle$.

On a $\alpha_G(d) \leq \varphi(d)$ = nombre de générateur de $\langle x \rangle$.

* Si $\alpha_G(d) = 0$: $\alpha_G(d) \leq \varphi(d)$.

ii) $\Rightarrow$ iii) On suppose que tout diviseur d de n, on a $\alpha_G(d) \leq \varphi(d)$ (*) pour

On sait que $n = \sum_{d \text{ diviseur de } n} \varphi(d)$ (**)

Dans le groupe G, tout élément à un ordre diviseur de n.

$\sum_{d \text{ diviseur } n} \alpha_G(d) = \#G = n$ (cf ex)

$\alpha(1) + \alpha(2) + \alpha(3) + \alpha(6) =$

$\forall d$ diviseur de n, $\alpha_G(d) = \psi(d)$

iii) $\Rightarrow$ iv) $\alpha_G(n) = \psi(n) \geq 1$

Il y a donc un élément d'ordre n, donc un générateur de G. G est cyclique.

iv) $\Rightarrow$ v) C'est le th précédent sur les groupes cycliques.

v) $\Rightarrow$ i) évident.

ex: $(\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, +)$

$V_2 = \{y \in \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z},\ 2y = 0\}$

$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} = \{(0,0); (0,1); (1,0); (1,1)\}$

$\Rightarrow V_2 = \{(0,0); (0,1); (1,0); (1,1)\}$

$\Rightarrow \operatorname{card} V_2 = 4$

$\Rightarrow$ Le groupe n'est pas cyclique.

II) Groupes de petits ordres

On cherche à déterminer à isomorphisme près, tous les groupes d'ordre 1, 2, 3, 4, 5, 6, 7.

ordre 1

$\times$	e
e	e

$\simeq$

$+$	0
0	0

lemme: Tout groupe fini d'ordre premier est cyclique

dem: Soit G un groupe d'ordre premier $p \geq 2$

Soit $g \in G$, $g \neq e_G$

$\langle g \rangle \Rightarrow \{e_G, g, \dots\}$ ordre $\langle g \rangle \geq 2$.

Par le th de Lagrange : ordre $\langle g \rangle$ / ord $(G) = p$

$\Rightarrow$ donc ord $\langle g \rangle = p = \text{ord } G$

$\Rightarrow \langle g \rangle = G$ qui est cyclique

(en particulier commutatif).

• groupe d'ordre 4.

On connaît : $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/4\mathbb{Z}, +)$

non cyclique n'a pas d'élément d'ordre 4.

cyclique a un élément d'ordre 4.

$\Rightarrow$ Ils ne sont pas isomorphes.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

carré latin

Lemme :

Tout groupe d'ordre pair admet un élément d'ordre 2.

dem : $G = \{g \in G \mid g = g^{-1}\} \cup \{g \in G \mid g \neq g^{-1}\}$

partition de G

contient l'élément neutre

un nombre pair d'éléments on peut regrouper par couple g et g^{-1}.

Donc $\{g \in G \mid g = g^{-1}\}$ a un nombre pair d'éléments. Donc :

$\exists\, x \in G - \{e_G\}$ tq $x = x^{-1}$

$x^2 = e_G$, $x \neq e_G \Rightarrow \text{ord } x = 2$

On notera a, un élément d'ordre 2

et $G = \{e, a, b, c\}$.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

$a * b$ est ni a, ni b. (carré latin) $\Rightarrow a * b = c$.

Quel est l'inverse de b ?

b^{-1} est ni e, ni a (car $e^{-1} = e$ et $a^{-1} = a$)

donc est soit b, soit c.

↳ si $b^{-1} = b \Rightarrow b * b = e$.

On retrouve la table de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

↳ si $b^{-1} = c \Rightarrow b * c = e_G$

et

$*$	b	c
b	c	a
c	a	e

$*$	b	c
b	a	e
c	e	a

En changeant l'ordre des colonnes (e, b, a, c) on retrouve la table de $\mathbb{Z}/4\mathbb{Z}$.

$G \longrightarrow \mathbb{Z}/4\mathbb{Z}$

$e \longrightarrow \bar{0}$

$b \longrightarrow \bar{1}$

$a \longrightarrow \bar{2}$

$c \longrightarrow \bar{3}$

est un isomorphisme de groupe.

* groupe d'ordre 6

Par le lemme précédent, il y a un élément a d'ordre 2.

- Supposons que tous les éléments soit d'ordre 1 ou 2. Soit $b \neq a$ et $b \neq e$.

$\{e, a, b, c\}$ est un sous ensemble de G de cardinal 4. Car si :

si $ab = e$, $cab = ac \Rightarrow b = a$ a'

si $ab = a$, $b = e$

si $ab = b$, $a = e$.

- Comme tous les éléments sont d'ordre 1 ou 2, $\{e, a, b, ab\}$ est stable par inverse.

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

et G est commutatif.

$\{e, a, b, ab\}$ serait donc un sous groupe de G.

impossible de par le th de Lagrange

$\Rightarrow$ Il y a au moins un élément dans G d'ordre 3 ou 6.

↳ Si G a un élément d'ordre 6, il est cyclique, donc isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$

↳ Si G a un élément d'ordre 3.

Notons le b.

$G = \{e, a, b, ab, b^2, ab^2\}$

($b^2 \neq a$ car a est d'ordre 2 et b d'ordre 3)

×	e	a	b	ab	b^2	ab^2
e	e	a	b	ab	b^2	ab^2
a	a	e	ab	b	ab^2	b^2
b	b	ab^2	b^2	a	e	ab
ab	ab	b^2	ab^2	e	a	b
b^2	b^2	ab	e	ab^2	b	a
ab^2	ab^2	b	a	b^2	ab	e

Quelles sont les valeurs possibles de ba ? (le groupe n'est pas commutatif).

$ba = ab$ ou ab^2

- Si $ba = ab$, ab est d'ordre 6.

$ba \neq e_G$. $(ba)^2 = baba = baab = ba^2b$

$= b^2 \neq e_G$

$(ba)^3 = b^2ba = a \neq e_G$.

$\Rightarrow ba$ est d'ordre 6

$\Rightarrow$ le groupe est cyclique.

(c'est l'ancien cas).

- Si $ba = ab^2$

$ab\,ab = a(ab^2)b = a^2b^3 = e$

$ab.ab^2 = eb = b$.

$b^2a = b.ba = bab^2 = ab^2b^2 = ab$

$\Rightarrow$ carré latin.

Réciproquement: soit un ensemble $\{e, a, b, ab, b^2, ab^2\}$ avec la table précédente.

Il faudrait montrer que c'est un groupe et en particulier, il faudrait vérifier l'associativité.

On écrit la table de $\mathfrak{S}_3$, le groupe de permutation $\{1, 2, 3\}$

$\mathfrak{S}_3 = \{Id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

$(1,2).(1,2,3) = (2,3)$

	Id	(1,2)	(1,2,3)	(2,3)	(1,3,2)	(1,3)
Id	Id	(1,2)	(1,2,3)	(2,3)	(1,3,2)	(1,3)
(1,2)	(1,2)	Id	(3,2)	(1,2,3)	(3,1)	(1,3,2)
(1,2,3)	(1,2,3)	(1,3)	(1,3,2)	(1,2)	Id	(2,3)
(2,3)	(2,3)	(1,3,2)	(1,3)	Id	(1,2)	(1,2,3)
(1,3,2)	(1,3,2)	(2,3)	Id	(1,3)	(1,2,3)	(1,2)
(1,3)	(1,3)	(1,2,3)	(1,2)	(1,3,2)	(2,3)	Id

carré latin.

Concl: Les groupes d'ordre 6 sont isomorphes soit à $(\mathbb{Z}/6\mathbb{Z}, +)$ (commutatif) soit à $(S_3, \circ)$ (non commutatif).

III) Groupes symétriques

1) Définitions

Pour $n \in \mathbb{N}^*$, on notera $\mathbb{N}_n = \{1, 2, 3, \dots, n\}$ l'ensemble des n premiers entiers non nul.

le groupe symétrique $(\mathcal{S}_n, \circ)$ est le groupe des bijections de $\mathbb{N}_n$ dans lui-même (aussi appelé permutations) muni de la loi de composition.

ex: * $n = 1$: $\mathbb{N}_1 = \{1\}$, $\mathcal{S}_1 = \{Id\}$

* $n = 2$: $\mathbb{N}_2 = \{1, 2\}$, $\mathcal{S}_2 = \{Id, \tau_{12}$ (transposition$\}$

* $n = 3$: $\mathbb{N}_3 = \{1, 2, 3\}$

$\mathcal{S}_3 = \{Id, \tau_{12}, \tau_{23}, \tau_{13}, \underbrace{\in \{1\to2, 2\to3, 3\to1\}}, \in \{1\to3, 2\to1, 3\to2\}\}$

a 6 éléments

3-cycle = cycle de longueur 3.

* $n = 4$

$\mathcal{S}_4 = \{Id, \binom{4}{2} = 6$ transpositions, 3-cycles, 4-cycles, doubles transpositions$\}$.

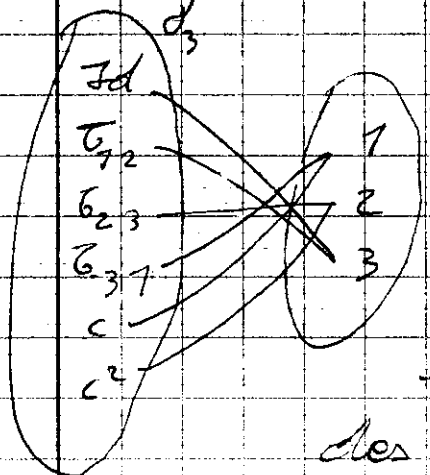
2) Calcul du cardinal

Prop: $\forall n \in \mathbb{N}^*$, $\underline{\text{card } \mathcal{S}_n = n!}$

dem: Le nombre d'injection d'un ensemble

à p éléments dans un ensemble à n éléments est le nombre d'arrangement ($p \leq n$) A_n^p qui vaut $\frac{n!}{(n-p)!}$.
Toute injection de $\mathbb{N}_n$ dans lui-même est une bijection, donc $\text{card } \sigma_n = A_n^n = n!$ □

Autre dem: $\sigma_n \longrightarrow \mathbb{N}_n$
$\sigma \longrightarrow \sigma(n)$



Les antécédents de $i \in \mathbb{N}_n$ sont les permutations σ de $\mathbb{N}_n$ telles que $\sigma(n) = i$.
Cet ensemble est en bijection avec l'ensemble des bijections $\{1, 2, \dots, n-1\}$ dans $\{1, 2, \dots, i-1, i+1, i+2, \dots, n\}$.
Il est donc de même cardinal que σ_{n-1}.
On trouve que $\text{card } \sigma_n = n \text{ card } \sigma_{n-1}$.
Par réc., $\forall n \in \mathbb{N}^*$ $\text{card } \sigma_n = n!$

3) Décomposition

Th: Toute permutation de σ_n s'écrit comme composée d'au plus $n-1$ transpositions.

Dem: Par rec sur n.
$n = 1$, OK.
$n = 2$, $\sigma_2 = \{Id, \tau\}$
Soit $n \in \mathbb{N}^*$ tq toute permutations d'un ensemble à n éléments s'écrive comme composé d'au plus $n-1$ transpositions. Soit $\sigma \in \sigma_{n+1}$

* Si σ admet un point fixe i, σ s'identifie à une permutation de $\{1, 2, \dots, i-1, i+1, \dots, n+1\}$ (n éléments)
Donc σ s'écrit comme produit d'au plus $n-1$ transposition

* Si σ n'admet pas de point fixe.
$\tau_{1,\sigma(1)} \circ \sigma$ admet 1 comme point fixe
=> il s'écrit comme un produit d'au plus $n-1$ transpositions. Donc
$\sigma = \tau_{1,\sigma(1)} \circ (\tau_{1,\sigma(1)} \circ \sigma)$ est produit d'au plus n transpositions.
=> Hérédité ☐ $\tau_{1,\sigma(1)} \circ \tau_{1,\sigma(1)} = Id$

ex: $c = (1,2,3) = \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix}$

$$\tau_{12} \circ c = \begin{matrix} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{matrix} = \tau_{23}$$

$$\Rightarrow c = \tau_{12} \circ \tau_{23}$$

Th: Toute permutation de $\mathfrak{S}_n$ s'écrit comme composé de cycles à support disjoints (Cette écriture est unique à l'ordre près)

ex:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 2 & 4 & 6 & 1 \end{pmatrix}$$
$$= (1\ 3\ 7)(2\ 5\ 4)$$
$$= (1\ 3\ 7)(2\ 5\ 4)(6)$$

dem:
n est fixé. Par récurrence forte sur le nombre de points fixes de σ.
* Si σ admet n points fixes, $\sigma = Id$

$\sigma = (1)(2)\cdots(n) = Id$

• Soit $p \leq n$, un entier tq toute permutation avec au moins p points fixes s'écrit comme composé de cycles à supports disjoints et disjoints de l'ensemble des points fixes.
Soit σ une permutation de $\mathfrak{S}_n$ qui admet $(n-1)$ points fixes. Soit $a \in \mathbb{N}_n$ un point non fixé par σ.
q est le premier itéré de σ qui envoie a sur a. Soit $\sigma' = (\sigma^{q-1}(a), \sigma^{q-2}(a), \ldots, \sigma(a), a) \circ \sigma$.
↳ Aucun des éléments de $a, \sigma(a), \ldots, \sigma^{q-1}(a)$ n'est fixé par σ'
↳ tous les points fixes de σ sont points fixes de σ'
↳ a est un "nouveau" point fixe de σ' ainsi que $\sigma(a), \sigma^2(a), \ldots, \sigma^{q-1}(a)$
Donc σ' s'écrit comme composé de cycles à supports disjoints et disjoints des points fixes de σ'
$\sigma' = c_r \circ c_{r-1} \circ \cdots \circ c_2 \circ c_1$
où les c_i sont les cycles à supports disjoints et disjoints de $\{a, \sigma(a), \ldots, \sigma^{q-1}(a)\}$
$c = (a, \sigma(a), \ldots, \sigma^{q-1}(a)) \circ c_r \circ \cdots \circ c_1$.

Lemme : Soit $\sigma \in \mathfrak{S}_n$, 2 permutations de $\mathfrak{S}_n$ à supports disjoints
Alors : ✱ $\sigma \circ \delta = \delta \circ \sigma$
✱ Si $\sigma^k = \delta^k$ alors $\sigma^k = \delta^k = Id$
✱ ordre $(\sigma \circ \delta) = pgcm(ord(\sigma), ord(\delta))$

ord σ = nb de compositions tq $\sigma^{\cdots} \circ \sigma = Id$
= longueur du cycle

dem: Le support est le complémentaire de = points fixes. C'est l'ensemble des points modifiés par σ.

* Aucun élément n'est changé par σ et par δ :
  ⇒ $\sigma \circ \delta$ vaut σ sur le support σ
  δ sur le support δ
  Id ailleurs
  Donc $\sigma \circ \delta = \delta \circ \sigma$
* Soit $(\ell, k) \in \mathbb{N}^{*2}$
  ↳ $\sigma^k = \delta^\ell$.
  En dehors du support de σ (c-à-d sur Fix σ) $\sigma^k = Id$
  En dehors du support δ, $\delta^\ell = Id$
  (support σ) $\cap$ (support δ) $= \emptyset$
  ⇒ (support σ)$^c \cup$ (support δ)$^c = \mathbb{N}_n$
  Donc $\sigma^k = \delta^\ell = Id$.
* a = ordre (σ), b = ordre(δ), d = ordre$(\sigma \circ \delta)$
  $m = ppcm(a, b)$
  $(\sigma \circ \delta)^m = (\sigma \circ \delta) \circ \cdots \circ (\sigma \circ \delta)$
  $= \sigma^m \circ \delta^m$ (σ et δ commutent)
  $= Id \circ Id$ car m est multiple de a et de b.
  ⇒ $d \mid m$.
  ⇒ $(\sigma \circ \delta)^d = Id = \sigma^d \circ \delta^d$
  $(\sigma^{-1})^d = \delta^d$
  support(σ^{-1}) = support(σ) est disjoint des support de δ
  $(\sigma^{-1})^d = Id$ et $\delta^d = Id$.
  d est multiple de a et multiple de b
  ⇒ d est multiple de m ⇒ $d = m$.

signature (σ) = { 1 si σ est produit de nombre pair de transpositions
                { -1 si σ est produit de nombre impair de transpositions

Ex: Calcul de l'ordre de :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix}$$

$$= (1\,3\,5) \circ (2\,7) \circ (4\,6)$$

ordre 3 ordre 2 ordre 2

à pour ordre ppcm(2, 2, 3) = 6.

4) Formules de conjugaison

Lemme : Soit σ une permutation de $\mathfrak{S}_n$

* $\sigma \circ (i_1, i_2, \dots, i_\ell) \circ \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \dots, \sigma(i_\ell))$

* $\sigma \circ (c_r \circ \dots \circ c_1) \circ \sigma^{-1} = (\sigma c_r \sigma^{-1})(\sigma c_{r-1} \sigma^{-1}) \dots (\sigma c_1 \sigma^{-1})$

dém : $\sigma(i_k) \xrightarrow{\sigma^{-1}} i_k \xrightarrow{c=(i_1 \dots i_\ell)} i_{k+1} \xrightarrow{\sigma} \sigma(i_{k+1})$

Si $i \notin \{\sigma(i_1), \dots, \sigma(i_\ell)\}$

$\sigma^{-1}(i) \notin \{i_1, \dots, i_\ell\}$ = support c

$c \circ \sigma^{-1}(i) = \sigma^{-1}(i)$

$\sigma \circ c \circ \sigma^{-1}(i) = \sigma \circ \sigma^{-1}(i) = i$

* résulte de l'associativité.

Th : Toute permutation de $\mathfrak{S}_n$ s'écrit comme :
- composé de transpositions de la forme $(1, i)$
- composé de $(i, i+1)$
- composé de $(1, 2)$ et des puissances du cycle $(1, 2, \dots, n) = c$.

dém : • On a vu que toute permutation s'écrit comme composée de transposition

$i \neq j$: $(1,j)(1,i)(1,j) = c_{1,j}(1,i)\tau_{1,j}^{-1}$

$i \neq 1$: $= (\tau_{1,j}(1), \tau_{1,j}(i)) = (j, i) = (i, j)$

• $((1,2)(2,3)\dots(i-2,i-1))(i-1,i)$

σ

$((1,2)(2,3)\dots(i-2,i-1))^{-1} = (\sigma(i-1), \sigma(i)) = (1,i)$

• $c^{i-1}(1,2)(c^{i-1})^{-1} = (c^{i-1}(1), c^{i-1}(2))$

$= (i, i+1)$

IV) Groupes de matrices.

1) Groupes linéaires

Groupes additifs: Soit $M_n(K)$ l'ensemble des matrices $n \times n$ à coeff. dans un corps K. Muni de l'addition, $M_n(K)$ est un groupe commutatif (car K l'est).

On ne considère désormais que la multiplication des matrices.

Déf: Le groupe général linéaire $GL_n(K)$ est l'ensemble des matrices $n \times n$ à coeff. dans K (un corps commutatif), inversible. muni de la multiplication.

Déf: Une matrice $A \in M_n(K)$ est dite inversible s'il existe une matrice $B \in M_n(K)$ tq $AB = BA = Id$.

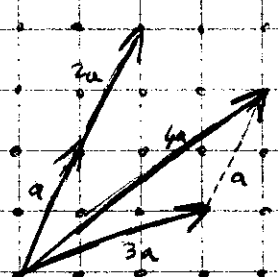
En d'autres termes $(GL_n(K), \cdot)$ est le groupe des inversibles de l'anneau non commutatif $(M_n(K), +, \cdot)$.

Cas où K est le corps fini à p éléments, p premier

Prop. Le groupe $(GL_2(\mathbb{Z}/p\mathbb{Z}), \cdot)$ est un groupe fini d'ordre $(p^2-1)(p^2-p)$.

dem: On dénombre les matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ inversibles avec $(a,b,c,d) \in (\mathbb{Z}/p\mathbb{Z})^4$.
On choisit $\begin{pmatrix} a \\ b \end{pmatrix}$ parmi les vecteurs non nuls de $(\mathbb{Z}/p\mathbb{Z})^2$. Il y a p^2-1 possibilités.
On choisit $\begin{pmatrix} c \\ d \end{pmatrix}$ parmi les vecteurs de $(\mathbb{Z}/p\mathbb{Z})^2$ non colinéaire avec $\begin{pmatrix} a \\ b \end{pmatrix}$. Il y a p^2-p possibilités.

ex: $a\begin{pmatrix}1\\2\end{pmatrix}$ $2a\begin{pmatrix}2\\4\end{pmatrix}$ $3a\begin{pmatrix}3\\1\end{pmatrix}$ $4a\begin{pmatrix}4\\3\end{pmatrix}$ $5a\begin{pmatrix}0\\0\end{pmatrix}$



$(\mathbb{Z}/5\mathbb{Z})^2$

ex: $p=2$. $GL_2(\mathbb{Z}/2\mathbb{Z})$ est un groupe à $(2^2-1)(2^2-2)=6$ éléments.

$$GL_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ e=\begin{pmatrix}1&0\\0&1\end{pmatrix}, a=\begin{pmatrix}0&1\\1&0\end{pmatrix}, c=\begin{pmatrix}1&1\\1&0\end{pmatrix}, b=\begin{pmatrix}1&1\\0&1\end{pmatrix}, c^2=\begin{pmatrix}0&1\\1&1\end{pmatrix}, d=\begin{pmatrix}1&0\\1&1\end{pmatrix} \right\}$$

L'ordre de a est 2 car $a^2 = e$
L'ordre de b est 2 car $b^2 = e$
c est d'ordre 3 car $c^3 = e$ et $c^2 \neq e$.

$c^2 = \begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}$

$\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}$

$c\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}$

$\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&1\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}$

c^2 est d'ordre $\frac{\text{ord } r}{\text{pgcd}(\text{ord } r, 2)} = \frac{3}{1} = 3$.

d est d'ordre 2 $\quad \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

On peut MQ $GL_2(\mathbb{Z}/2\mathbb{Z})$ est isomorphe au groupe $\mathfrak{S}_3$.

2) Sous groupes du groupe $GL_n(K)$

* L'ensemble des matrices diagonales inversibles de $GL_n(K)$ est un sous groupe commutatif de $GL_n(K)$.

Dans $GL_2(\mathbb{R})$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}$$

$\in GL_2(\mathbb{R})$ diagonale

$$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & c \\ c & b \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & -a \\ 0 & -b \end{pmatrix} = \begin{pmatrix} a & -a+b \\ 0 & b \end{pmatrix}$$

Cq : Le sous groupe de $GL_n(K)$ des matrices diagonales n'est pas distingué dans $GL_n(K)$

Si un endomorphisme u de $\mathbb{R}^2$ a une matrice diagonale D dans une base $\mathcal{B}$ alors sa matrice dans une base $\mathcal{B}'$ est donnée par :

$$\text{Mat}(u, \mathcal{B}') = P_{\mathcal{B} \to \mathcal{B}'} \, \text{Mat}(u, \mathcal{B}) \, P^{-1}_{\mathcal{B} \to \mathcal{B}'}$$

$\text{Mat}(u, \mathcal{B}')$ n'est pas toujours diagonale

* On considère l'application déterminant :

$$(GL_n(\mathbb{R}), \circ) \to (\mathbb{R}^*, \times)$$
$$A \mapsto \det A$$

Comme $\forall (A,B) \in GL_n(\mathbb{R})$,
$\det(AB) = \det(A)\det(B)$
$\Rightarrow$ <u>$\det$ est un morphisme de groupes.</u>

Lemme : Soit $f : (G, *) \to (H, \cdot)$ un morphisme de groupe. Alors le noyau de f, noté $N(f) = \{g \in G, f(g) = e_H\}$ est un sous-groupe distingué de G.

Dem : * $e_G \in N(f)$ car $f(e_G) = e_H$
* stabilité par produit :
Soient $a, b \in N(f)$
$f(a * b) = f(a) \cdot f(b) = e_H \cdot e_H = e_H$
* stabilité par inversion : Soit $a \in N(f)$
$f(a^{-1}) = (f(a))^{-1} = e_H^{-1} = e_H$
$\Rightarrow a^{-1} \in N(f)$
$\Rightarrow N(f)$ est un sous-groupe de G.
* Soit $g \in G$ et $a \in N(f)$
Mq $g * a * g^{-1} \in N(f)$
$f(g * a * g^{-1}) = f(g) \cdot f(a) \cdot (f(g))^{-1}$
$= f(g) \cdot e_H \cdot (f(g))^{-1}$
$= e_H$
$\Rightarrow N(f)$ est distingué. □

Déf : <u>Le noyau du morphisme de groupe $(GL_n(\mathbb{R}), \circ) \xrightarrow{\det} (\mathbb{R}^*, \times)$ est appelé groupe spécial linéaire :</u>
c'est un sous-groupe distingué de

$SL_n(\mathbb{R})$:

$\underline{SL_n(\mathbb{K})} = \{ A \in GL_n(\mathbb{K}) \,,\ \det A = 1 \in (\mathbb{K}^*, \times) \}$

* L'ensemble U des matrices de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ avec $a \in \mathbb{K}$ est un sous groupe de $GL_n(\mathbb{K})$ isomorphe à $(\mathbb{K}, +)$.

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$$

$$(\mathbb{K}, +) \longrightarrow U$$
$$a \longmapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$ est un

un isomorphisme (morphisme bijectif).

* Sous-groupe des matrices de permutation.

L'ensemble S des matrices de $GL_3(\mathbb{K})$ dont tous les termes sont nuls sauf un sur chaque ligne et chaque colonne qui vaut 1 est un sous groupe.

$$S = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}$$

S est isomorphe à

$\mathfrak{S}_3 = \{ Id, (1,2), (2,3), (1,3), (1,2,3), (1,3,2) \}$

* Rappel : Trace de A : $\mathrm{Tr}(A) = \sum a_{ii}$ (A est carrée)

* L'ensemble R des matrices de la forme $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ est un sous groupe commutatif de $GL_2(\mathbb{R})$.

$$\begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix} \cdot \begin{pmatrix} \cos b & -\sin b \\ \sin b & \cos b \end{pmatrix}$$

$$= \begin{pmatrix} \cos a \cos b + \sin a \sin b & -\cos a \sin b - \cos b \sin a \\ \sin a \cos b + \cos a \sin b & -\sin a \sin b + \cos a \cos b \end{pmatrix}$$

$$= \begin{pmatrix} \cos(a+b) & -\sin(a+b) \\ \sin(a+b) & \cos(a+b) \end{pmatrix}$$

* Matrices de quaternions : dans $GL_2(\mathbb{C})$

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$j = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad k = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

$1 \cdot 1 = 1$; $1 \cdot i = i$; $1 \cdot j = j$; $1 \cdot k = k$

$i \cdot 1 = i$; $i \cdot i = -1$; $i \cdot j = k$; $i \cdot k = -j$

$j \cdot 1 = j$; $j \cdot i = -k$;

$Q = \{1, i, j, k, -1, -i, -j, -k\}$ est un sous groupe non commutatif de $GL_2(\mathbb{C})$ à 8 éléments.

IV) Corps finis

1) Etude des algèbres $(\mathbb{K}[X]/(P), +, \times, \cdot)$

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ l'anneau quotient de l'anneau $(\mathbb{Z}, +, \times)$ par la relation de congruence modulo n.

$a \equiv y\ [n] \iff x - y \in (n)$ l'idéal engendré par n, l'ensemble des multiples de n.
Dans chaque classe d'équivalence c de $\mathbb{Z}/n\mathbb{Z}$, il y a un unique représentant $r \in \mathbb{Z}$ tq $0 \leq r \leq n-1$, $r \in c$.

ex : $c = [78]_7$ contient l'élément $r = 4$.

* $(\mathbb{K}[X], +, \times)$, l'anneau des polynômes à une indéterminée à coeff. dans un corps $\mathbb{K}$. $\forall P \in \mathbb{K}[X]$, (P) l'idéal engendré par P est l'ensemble des multiples de (P).

$(P) = \{ \exists Q \in \mathbb{K}[X] \mid \exists R \in \mathbb{K}[X] \mid Q = RP \}$

ex : $X^3 + X \in (X^2+1)$

La relation binaire sur $\mathbb{K}[X]$ définie par $R = S\ [P] \iff R - S \in (P)$ est une relation d'équivalence. ($\deg P \geq 1$)

Comme (P) est un idéal, l'ensemble quotient (des classe d'équivalence est muni d'une structure naturelle d'anneau. On le note $\left(\mathbb{K}[X]_{/(P)}, +, \times \right)$

Car la division euclidienne dans $\mathbb{K}[X]$, on montre que dans chaque classe $c \in \mathbb{K}[X]_{/(P)}$ il y a un unique représentant $R \in \mathbb{K}[X]$ tq $R \in c$, $0 \leq \deg R < \deg P - 1$

ex : dans $\mathbb{R}[X]_{/(X^2+1)}$, $c = [X^3 + 2X]$.

$X^3 + 2X \mid X^2 + 1$

$X^3 + X \quad \mid X$

$X^2 + 2X$

$\boxed{X}$

$\Rightarrow (X^2 + 2X) = X [X^2 + 1]$

L'application naturelle $\pi : K[X] \to K[X]_{/(P)}$, $Q \mapsto [Q]_P$ est un morphisme d'anneaux.

Si $Q = \sum_{i=0}^{d} a_i X^i$, $a_i \in K$.

$$\pi(Q) = \pi\left(\sum_{i=0}^{d} a_i X^i\right) = \sum_{i=0}^{d} a_i (\pi(X))^i$$

$$= \sum_{i=0}^{d} a_i \alpha^i = Q(\alpha) \qquad \alpha = [X]_P = \pi(X)$$

↑ notation

Toute classe c s'écrit de façon unique comme $c = R(\alpha)$ où $R \in K[X]$ de degré $\leq \deg P - 1$.

En fait, $(K[X], +, \times, \cdot)$ et $(K[X]_{/(P)}, +, \times, \cdot)$ sont des algèbres.

$\cdot$: multiplication par un scalaire.

↳ $(K[X], +, \times)$ est un anneau commutatif.

↳ $(K[X], +, \cdot)$ est une espace vectoriel

↳ $\forall (Q, S) \in K[X]^2$, $\forall (a, b) \in K^2$

$(a \cdot Q) \times (b \cdot S) = (ab) \cdot (Q \times S)$

Th : Soit $P \in K_{\geq 1}[X]$. Alors $(K[X]_{/(P)}, +, \cdot)$ est un espace vectoriel de dimension $\deg P$, de base $1, \alpha, \alpha^2, \dots, \alpha^{\deg P - 1}$.

Ex : $K = \mathbb{Z}/2\mathbb{Z}$, $P = X^2 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$

$K[X]_{/(P)}$ est un espace vectoriel de dimension 2 sur $\mathbb{Z}/2\mathbb{Z}$ de base $1, \alpha$.

$$K[X]_{/(P)} = \{c_1 \cdot 1 + c_2 \alpha,\ c_1, c_2 = 0 \text{ ou } 1\}$$

$$= \{0, 1, \alpha, 1 + \alpha\}$$

a \ b	0	1	α	1+α
0	0	0	0	0
1	0	1	α	1+α
α	0	α	1+α	1
1+α	0	1+α	1	α

$\pi(P) = P(\alpha) = 0$

$= \alpha^2 + \alpha + 1$

$\Rightarrow \alpha + \alpha = \alpha^2 = 1 + \alpha$

$(1+\alpha)^2 = 1 + 2\alpha + \alpha^2$

$= 1 + 0 + 1 + \alpha = \alpha$

Si $\mathbb{K}$ est un corps fini et si $P \in \mathbb{K}[X]_{\neq 1}$ alors $\mathbb{K}[X]/(P)$ est un espace vectoriel sur $\mathbb{K}$ de dimension $\deg P$, de cardinal $(\mathrm{card}\,\mathbb{K})^{\deg P}$.

Th : * Dans l'anneau $(\mathbb{K}[X]/(P), +, \times)$, les éléments inversibles sont les classes des polynômes premiers avec P.
* L'anneau $(\mathbb{K}[X]/(P), +, \times)$ est un corps si P est irréductible dans $\mathbb{K}[X]$.

dem : * Soit $Q \in \mathbb{K}[X]$ tq $P \wedge Q = 1$
$\Rightarrow$ Bezout : $\exists (U, V) \in \mathbb{K}[X]^2$ tq $1 = UP + VQ$
$\overline{1}^{P} = \overline{0} + \overline{V}\,\overline{Q}$
$\Rightarrow Q$ est inversible dans $\mathbb{K}[X]/(P)$
- Réciproquement : si c est inversible dans $\mathbb{K}[X]/(P)$. Soit $Q \in c$, $c = \overline{Q}^{P}$.
$\exists c'$ tq $cc' = 1$. Soit $Q' \in c'$, $c' = \overline{Q'}^{P}$
$cc' = 1$ dans $\mathbb{K}[X]/(P) \Rightarrow \overline{Q}^{P}\overline{Q'}^{P} = 1$
$\Rightarrow \exists R \in \mathbb{K}[X]$ tq $QQ' = 1 + RP$
$1 = Q'Q + (-R)P \in \mathbb{K}[X]$

Donc c est la classe d'un polynôme Q premier avec P.
* Si P est irréductible, tout polynôme non multiple de P est premier avec P.
Donc, toute classe non nulle de $\mathbb{K}[X]/(P)$

est inversible. Donc $K[X]/(P)$ est un corps.

- si P est réductible, $P = P_1 P_2$

$\deg P_1 < \deg P$, $\deg P_2 < \deg P$.

$[P_1]_P \neq 0$, $[P_2]_P \neq 0$.

mais $[P_1]_P [P_2]_P = 0$.

$\Rightarrow K[X]$ n'est pas intègre.

Ce n'est $/(P)$ donc pas un corps.

2) Corps finis

Soit K un corps. En particulier $(K, +)$ est un groupe fini. On note K l'ordre de 1 dans $(K, +)$

$1 + \dots + 1 = 0$ (K fois). $K \cdot 1$ est le plus petit multiple de 1 qui est nul.

K s'appelle la <u>caractéristique</u> de K.

C.ex : - caractéristique $\mathbb{Z}/p\mathbb{Z}$ où p est premier est p. $[1]_p + \dots + [1]_p = [0]_p$

- La caractéristique de $\left(\frac{\mathbb{Z}/2\mathbb{Z}[X]}{(X^2+X+1)}\right)$ est 2.

$[1]_p + [1]_p = [0]_p$

Th. Soit $K = \mathbb{Z}/p\mathbb{Z}$ (p premier). Soit $P \in K[X]$ un polynôme irréductible de degré ≥ 1. Alors : $(K[X]/(P), +, \times)$ est un corps de cardinal $p^{\deg P}$ et de caractéristique p.

3) Groupe des inversibles d'un corps fini

Th: Soit K un corps fini. Alors le groupe $(K^*, \times)$ des inversibles de $(K, +)$ est un groupe cyclique.

Dem: Soit $q = \text{card } K$, $q-1 = \text{card } K^*$

Soit d un diviseur de $q-1$.

$U_d = \{ y \in K^* / y^d = 1 \}$

U_d est inclus dans l'ensemble des solutions dans K de l'équation $x^d - 1 = 0$.

Donc $\text{card } U_d \leq d$

Par théorème, U_d est cyclique

(En particulier, $(K^*, \times)$ a $f(q-1)$ générateurs).

Cor: Tous les éléments de K^* ont deux écritures

- naturelle : $K = \mathbb{F}_p[x]/(P)$
- $c = R(\alpha) = \sum_{i=0}^{\deg P - 1} c_i x^i$ c adapté pour l'addition
- $c = g^k$ où g est un générateur adapté pour la multiplication de K^*

Ex: $K = \mathbb{Z}/3\mathbb{Z}$, $P = x^2 + 1$ irréductible sur $\mathbb{Z}/3\mathbb{Z}[x]$.

$\mathbb{K}[x]/(P) = \mathbb{Z}/3\mathbb{Z}[x]/(x^2+1)$ est un corps de caractéristique 3, un $\mathbb{Z}/3\mathbb{Z}$-ev de dimension 2 de cardinal $3^2 = 9$

$(K^*, \times)$ est un groupe cyclique d'ordre 8.

(?)

$\alpha = [x]_\rho$, $[\rho]_\rho = 0$ donc $\alpha^2 + 1 = 0$

$K = \{0, \alpha, 2\alpha, 1, 1+\alpha, 1+2\alpha, 2, 2+\alpha, 2+2\alpha\}$

$\times$	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
1	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	2	1	2α	α	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$
α	α	2α	2	1	$2+\alpha$	$1+\alpha$	$2+2\alpha$	$1+2\alpha$
2α	2α	α	1	2	$1+2\alpha$	$2+2\alpha$	$\alpha+1$	$\alpha+2$
$1+\alpha$	$1+\alpha$	$2+\alpha$	$2+2\alpha$	$1+2\alpha$	2α	2	1	α
$1+2\alpha$	$1+2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	2	α	2α	1
$2+\alpha$	$2+\alpha$	$2+2\alpha$	$2+\alpha$	$\alpha+1$	1	2α	α	2
$2+2\alpha$	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	$\alpha+2$	α	1	2	2α

$(1+\alpha)^2 = 1 + 2\alpha + \alpha^2 = 1 + 2\alpha + 2 = 2\alpha$

$(1+\alpha)^3 = 2\alpha(1+\alpha) = 1 + 2\alpha$

$(1+\alpha)^4 = (2\alpha)^2 = 2$.

Il y a $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$ générateurs.

$(1+\alpha)^5 = 2 + 2\alpha$

$(1+\alpha)^6 = (2\alpha).2 = \alpha$

$(1+\alpha)^7 = 2(1+2\alpha) = 2+\alpha$.

$g = 1+\alpha$ est un générateur

$1 = g^0$

$\alpha = g^6$

$2\alpha = g^2$

$1+\alpha = g$

$1+2\alpha = g^3$

$2+\alpha = g^7$

$2+2\alpha = g^5$

$1 + \alpha^2 = 0 \Rightarrow \alpha^2 = -1 = 1$

$2\alpha.2\alpha = 4\alpha^2 = 4.2 = 1$

$2.(1+\alpha) = 2 + 2\alpha = 2\alpha + 1$

$2\alpha.(1+2\alpha) = 2\alpha + 4\alpha^2 = 2\alpha + 2$

$2\alpha(1+\alpha) = 2\alpha + 2\alpha^2$

$= 2\alpha + 2.2$

$= 2\alpha + 1$