Principales structures : groupe, anneau, corps, algèbre.

I) Lois de composition :

Déf : Soit E un ensemble. Une loi de composition interne sur E est une application de $E \times E$ dans E .

Déf : Soit K et E deux ensembles. Une loi de composition externe sur E (définie à partir de K) est une application de $K \times E$ dans E .

Exples :

- Dans $\mathbf{Z}$, + et . définissent des lois de composition internes .
- Soit X un ensemble non vide, soit E l'ensemble des applications de X dans X .

Soit o la composition des applications. o est une loi de composition interne sur E

$E \times E \to E$, $(f,g) \mapsto f \circ g$.

Sur E , on peut définir une loi de composition externe :

$\mathbf{N}^* \times E \to E$, $(n,f) \mapsto f \circ f \circ \dots \circ f$ (n fois)

II) <u>Lois de composition interne :</u>

<u>Notations :</u> + : notation additive .
. , * ,$\times$: notations multiplicatives .

E muni d'une loi de composition interne . (A gauche , loi additive, à droite, loi multiplicative)

Déf : La loi est dite <u>commutative</u> si pour tous x,y de E :

$x + y = y + x$; $x . y = y . x$

Déf : La loi est dite <u>associative</u> si pour tous x,y de E :

$x + (y + z) = (x + y) + z$; $x . (y . z) = (x . y) . z$

Déf : La loi admet <u>un élément neutre</u> :

$\exists\, 0_E \in E , \forall x \in E , x + 0_E = 0_E + x = x$; $\exists\, 1_E \in E, \forall x \in E , x . 1_E = 1_E . x = x$

En particulier :

$0_E + 0_E = 0_E$; $1_E . 1_E = 1_E$

Théorème : Si la loi admet un élément neutre, ce dernier est unique .

Exples :

- Dans $\mathbf{Z}$, 0 est élément neutre pour la loi + , 1 est élément neutre pour la loi $\times$
- Dans E , ensemble des applications de X sur X (X non-vide), Id_X est élément neutre pour la loi o .

Déf : On suppose que E admet un élément neutre. On dit que x de E admet <u>un opposé</u> s'il existe y de E tel que : $x + y = y + x = 0_E$.

On dit que x de E admet <u>un inverse</u> s'il existe y de E tel que $x . y = y . x = 1_E$.

Théorème : (en notation $\times$)
Si la loi est associative , admet un élément neutre et si x est inversible, alors son inverse est unique.

Notations : En loi $\times$, l'inverse de x se note x^{-1} .
En loi + , l'opposé de x se note $-x$.

Théorème : (en notation multiplicative)
On suppose que la loi admet un élément neutre et que x de E est inversible .
$\forall$ y,z $\in$ E :

(i) $(x . y = x . z) \Leftrightarrow (y = z)$

(ii) $(y . x = z . x) \Leftrightarrow (y = z)$

<u>III) Groupes :</u>

1) <u>Généralités :</u>

Déf : Soit G ensemble muni d'une loi de composition interne notée + . On dit que (G,+) est <u>un groupe</u> si :

- \+ est associative
- \+ admet un élément neutre
- tout élément admet un opposé

On définit de même un groupe en notation multiplicative . (on change opposé en inverse)

Si de plus la loi est commutative, on dit que le groupe est <u>abélien</u> .

Remarque : Si (G,+) est un groupe, alors $G \neq \emptyset$ car G admet au moins l'élément neutre .

Propriétés élémentaires :

(notation +) $\forall$ a, b, c $\in$ (G , +)

(i) $(a + b = a + c)$ ssi $(b = c)$

(ii) $(a = b + c)$ ssi $(a - c = b)$

(notation .) $\forall$ a, b, c $\in$ (G , .)

(i) (ab = ac) ssi (b = c)
(ii) (ba = ca) ssi (b = c)
(iii) (a = bc) ssi (ac^{-1} = b)
(iv) (a = bc) ssi ($b^{-1}a$ = c)

Exples :

($\mathbf{Z}$, +) , ($\mathbf{R}^*$, $\times$) sont des groupes abéliens.

Soit X un ensemble non-vide. Soit E l'ensemble des bijections de X dans X, alors (E, o) est un groupe .

2) Les notations x^n et n.x ($n \in \mathbf{Z}$, $x \in G$) :

Déf : On considère G , groupe multiplicatif

$$n \in \mathbf{Z},\ x \in G : \quad x^n = \begin{cases} x\times x\times..\times x\ (n\ fois, si\ n\geq 1) \\ x^{-1}\times x^{-1}\times..\times x^{-1}(|n|\ fois\ si\ n\leq -1) \\ 1_G\ (si\ n=0) \end{cases}$$

Remarques :

- x^{-1} (pour n = -1) est encore l'inverse de x .
- $x^0 = 1_G = 1_G{}^n$ ($\forall n \in \mathbf{Z}$)

Prop :

(i) $x^1 = x$ ($\forall x \in G$)

(ii) $(x^n)^m = x^{nm}$ $(\forall\, x \in G)(\forall\, m,n \in \mathbf{Z})$

(iii) $x^{m+n} = x^n \,.\, x^m$ $(\forall\, x \in G)(\forall\, m,n \in \mathbf{Z})$

Conséquence du (ii) : $(x^{-1})^n = x^{-n} = (x^n)^{-1}$ $(\forall\, n \in \mathbf{Z})$

Prop : $(\forall\, x, y \in G)$, $xy = yx \Rightarrow (xy)^n = x^n \,.\, y^n$ $(\forall\, n \in \mathbf{Z})$

Déf : On considère G , groupe additif.

$$n \in \mathbf{Z},\ x \in G :\ n\,.\,x = \begin{cases} x+x+\ldots+x\ (n \text{ fois}, si\ n \geq 1) \\ -x-x.-x\ldots-x\ (|n| \text{ fois}, si\ n \leq -1) \\ 0_G\ si\ n=0 \end{cases}$$

Remarques : $(-1)x = -x$

$0 \,.\, x = 0_G = n \times 0_G$ $(\forall\, n \in \mathbf{Z})$ (ATTENTION : $0 \in \mathbf{Z}$, alors que $0_G \in G$)

Prop :

(i) $1 \,.\, x = x$ $(\forall\, x \in G)$ (ici $1 \in \mathbf{Z}$)

(ii) $m(nx) = (mn)x$ $(\forall\, x \in G, \forall\, m,n \in \mathbf{Z})$

(iii) $(m + n)x = mx + nx$ $(\forall\, x \in G, \forall\, m,n \in \mathbf{Z})$

(iv) $m(x + y) = mx + my$ $(\forall\, x, y \in G, \forall\, n \in \mathbf{Z})$

Remarque : Les propriétés (i), (ii) , (iii) et (iv) nous disent que G est un **Z** – module .

Si x_1 , x_2 , … , $x_n \in$ G , x est combinaison linéaire des $(x_i)_{1\leq i\leq n}$ à coefficients entiers ssi :

$$\exists\ (\lambda_i)_{1\leq i\leq n} \in \mathbf{Z}\ ,\ x = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n$$

3) Les sous-groupes :

On considère G groupe multiplicatif .

Déf : H ,sous-ensemble de G ,est un sous-groupe si :

- $H \neq \varnothing$
- $(\forall\ x,y \in H)$, $xy \in H$
- (H, .) est un groupe

Prop : (H : sous-groupe de G)

(i) $1_G \in H$ et $1_G = 1_H$

(ii) $(\forall\ x \in H)$, $x^{-1} \in H$ (c'est aussi son inverse dans le groupe H)

(iii) $(\forall\ x \in H)$ $(\forall\ n \in \mathbf{Z})$, $x^n \in H$.

Prop : (G : groupe multiplicatif, H un sous-ensemble de G)

Les propriétés suivantes sont équivalentes :

(i) H est un sous-groupe de G

(ii) - $H \neq \varnothing$

- $(\forall\, x,y \in H)$, $xy \in H$
- $(\forall\, x \in H)$, $x^{-1} \in H$

(iii) - $H \neq \varnothing$
- $(\forall\, x,y \in H)$, $xy^{-1} \in H$

Déf : (on considère G groupe additif)
Soit H sous-ensemble de G. H <u>sous-groupe</u> si :

- $H \neq \varnothing$
- $(\forall\, x,y \in H)$, $x + y \in H$
- $(H , +)$ groupe

Prop : (H sous-groupe de G)
G abélien $\Rightarrow$ H abélien

Prop : (H sous-groupe de G) (G groupe additif)

(i) $0_G \in H$ et $0_G = 0_H$.
(ii) $(\forall\, x \in H)$, $-x \in H$ (c'est aussi son opposé dans le groupe H)
(iii) $(\forall\, x \in H)\ (\forall\, n \in \mathbf{Z})$ $nx \in H$
(iv) Si $x_1 , x_2 , \ldots , x_n \in H$, alors toute combinaison linéaire $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n$ $(\lambda_j \in \mathbf{Z})$ est dans H.

Prop : (G groupe additif, H sous-ensemble de G)
Les propriétés suivantes sont équivalentes :

(i) H est un sous-groupe de G

(ii) - $H \neq \emptyset$

- $(\forall\, x,y \in H)$, $x + y \in H$
- $(\forall\, x \in H)$, $- x \in H$

(iii) - $H \neq \emptyset$

- $(\forall\, x,y \in H)$, $x - y \in H$

<u>Sous-groupes triviaux :</u> Soit G groupe . H = G est un sous-groupe .
Si G multiplicatif : $H = \{ 1_G \}$ est un sous-groupe de G
Si G additif : $H = \{ 0_G \}$ est un sous-groupe de G

Convention : H sous-groupe <u>propre</u> de G si $H \neq G$.

Prop : Soit G groupe et H un sous-groupe .

(i) Tout sous-groupe de H est un sous-groupe de G

(ii) Sous-groupes de H = les sous-groupes de G contenus dans H .

Exple :
$n \geq 1$, $U_n = \{ z \in \mathbf{C} \setminus \{0\} , z^n = 1 \}$ est un sous-groupe de $(\mathbf{C} \setminus \{0\} , \times)$

Déf : Soient G_1 , G_2 , … , G_n n groupes multiplicatifs.

On pose $G = G_1 \times G_2 \times \ldots \times G_n = \{ x = (x_1, x_2, \ldots, x_n) \ / \ x_j \in G_j \}$. G est appelé <u>produit direct</u> des groupes $G_1, \ldots, G_n$.

Prop :

(i) $(G\ , .\ )$ est un groupe

(ii) $1_G = (\ 1_{G1}, 1_{G2}, \ldots, 1_{Gn}\ )$

(iii) $x = (x_1\ , \ldots\ , x_n) \in G \Rightarrow x^{-1} = (x_1^{-1}, \ldots\ , x_n^{-1})$

(iv) $x = (x_1\ , \ldots\ , x_n) \in G$ et $m \in \mathbf{Z} \Rightarrow x^m = (x_1^m\ , \ldots\ , x_n^m)$

(v) Si les G_i sont tous abéliens, alors G est abélien .

Remarque : On peut ,bien sûr, traduire la définition et la proposition précédente avec G_i groupes additifs .

<u>4)Homomorphisme de groupes :</u>

Déf : Soient $(G\ , *)$, $(G'\ , \times)$ deux groupes , $f : G \rightarrow G'$, une application.
On dit que f est <u>un homomorphisme de groupes</u> (pour les lois * et $\times$) si :

$$(\forall\ (x,y) \in G^2)\ ,\ f(x * y) = f(x) \times f(y)$$

Soient $(G\ , \times)$ et $(G'\ , \times)$ deux groupes multiplicatifs. $f : G \rightarrow G'$. f est un homomorphisme de groupes si :

$(\forall (x,y) \in G^2)$, $f(xy) = f(x)f(y)$

Prop : $f : G \to G'$, homomorphisme de groupes multiplicatifs .
Alors :

(i) $f(1_G) = 1_{G'}$
(ii) $(\forall x \in G)$, $f(x^{-1}) = (f(x))^{-1}$.
(iii) $(\forall x \in G)(\forall n \in \mathbf{Z})$, $f(x^n) = (f(x))^n$.

Déf : $(G , +)$, $(G' , +)$: groupes additifs. $f : G \to G'$.
f est <u>un homomorphisme</u> si :

$(\forall x,y \in G)$, $f(x + y) = f(x) + f(y)$

Prop : $f : G \to G'$, homomorphisme de groupes additifs.
Alors :

(i) $f(0_G) = 0_{G'}$
(ii) $(\forall x \in G)$ $f(-x) = -f(x)$
(iii) $(\forall x \in G)(\forall n \in \mathbf{Z})$, $f(nx) = nf(x)$
(iv) $(\forall x_1 , \dots , x_s \in G)(\forall n_1, \dots, n_s \in \mathbf{Z})$,
$f(n_1x_1 + \dots + n_sx_s) = n_1f(x_1) + \dots + n_sf(x_s)$

<u>5) Action des homomorphismes sur les sous-groupes :</u>

Déf : f : G → G' , homomorphisme de groupes.

Noyau de f = Ker f = { $f^{-1}(\{0_{G'}\})$ } (en notation additive)

= { $f^{-1}(\{1_{G'}\})$ } (en notation multiplicative)

Donc Ker f = { $x \in G$ / $f(x) = 0_{G'}$ } (notation additive)

et Ker f = { $x \in G$ / $f(x) = 1_{G'}$ } (notation multiplicative)

Prop :

(i) L'image par f de tout sous-groupe H de G est un sous-groupe H' = f(H) de G' .
(ii) Im f = f(G) est un sous-groupe de G'
(iii) Quel que soit H' sous-groupe de G' , f^{-1}(H') est un sous-groupe de G.
(iv) Ker f est un sous-groupe de G .

Prop : Soit f : G → G' , homomorphisme de groupes.

- f injectif ⇔ Ker f = $\{0_G\}$
- f surjectif ⇔ Im f = G'

Déf : Soit f : G → G' , homomorphisme de groupes.

- Si G' = G , f est un endomorphisme .

- Si f est bijectif (=injectif+surjectif) , f est un <u>isomorphisme</u> .
- Si f est un isomorphisme et que G’ = G , alors f est un <u>automorphisme</u> .

Si il existe un isomorphisme entre G et G’ , on dit que G et G’ sont <u>isomorphes</u> . Et on note : $G \approx G'$

Prop : Soit $f : G \to G'$, un homomorphisme de groupes surjectifs.
Alors, G abélien $\Rightarrow$ G’ abélien .

Corollaire : Si $G \approx G'$, alors si l’un est abélien, l’autre l’est aussi.

Prop : Soient G et G’, deux ensembles munis chacun d’une loi de composition interne.
Soit $f : G \to G'$, un homomorphisme surjectif.

Alors, si G est un groupe, G’ l’est aussi.

<u>6) Quotient d’un groupe abélien par un sous-groupe :</u>

G groupe (pas forcément abélien) , H sous-groupe.
Relation binaire $\mathfrak{R}$ sur G : Soient $x,y \in G$.

$$x \,\mathfrak{R}\, y \Leftrightarrow xy^{-1} \in G$$

(en notation additive : $x \,\mathfrak{R}\, y \Leftrightarrow x - y \in H$)

Lemme 1 : $\Re$ est une relation d'équivalence.

Convention : Si $x \in G$, $\overline{x}$ = classe de x modulo H .

$G / \Re$ se note G / H : <u>ensemble quotient du groupe G par le sous-groupe H</u>.

Prop :

(i) $G / H = \{ \alpha = \overline{x} \; / \; x \in G \}$

(ii) $(\forall x,y \in G)$, $\overline{x} = \overline{y} \Leftrightarrow xy^{-1} \in H$ ($\Leftrightarrow x - y \in H$, en notation additive)

(iii) $(\forall x \in G)$, $\overline{x} = \overline{1} \Leftrightarrow x \in H$ ($\overline{x} = \overline{0} \Leftrightarrow x \in H$, en notation additive)

$\alpha , \beta \in G / H : \alpha = \overline{x}$, $\beta = \overline{y}$ ($x,y \in G$)

On pose : $\gamma = \overline{xy}$ (en notation additive : $\gamma = \overline{x+y}$)

Lemme 2 : Si G est abélien, γ ne dépend pas du choix de x et y .

γ dépend uniquement de α et de β . D'où une loi de composition interne sur G / H : $\gamma = \alpha\beta$ (en notation multiplicative) et $\gamma = \alpha + \beta$ (en notation additive)

Prop :

- Si G est abélien multiplicatif, alors l'ensemble G / H est muni d'une multiplication qui vérifie $\overline{xy} = \overline{x}\,\overline{y}$ ($\forall$ x,y $\in$ G)
- Si G est abélien additif , alors l'ensemble G / H est muni d'une addition qui vérifie $\overline{x+y} = \overline{x} + \overline{y}$ ($\forall$ x,y $\in$ G)

Prop : (G abélien multiplicatif)

- (G / H , $\times$) est un groupe abélien
- $1_{G/H} = \overline{1_G}$
- $\alpha = \overline{x}$, (x $\in$ G) $\Rightarrow \alpha^{-1} = \overline{x^{-1}}$
- $\alpha = \overline{x}$, (x $\in$ G) , n $\in$ **Z** $\Rightarrow \alpha^n = \overline{x^n}$

Rappel : x $\in$ H $\Leftrightarrow \overline{x} = \overline{1} = 1_{G/H}$.

Prop : (G groupe abélien additif)

- (G / H , +) est un groupe abélien
- $0_{G/H} = \overline{0_G}$
- - ($\overline{x}$) = $\overline{-x}$ ($\forall$ x $\in$ G)
- x $\in$ G, n $\in$ **Z** , n($\overline{x}$) = $\overline{nx}$ ($\forall$ x $\in$ G)

Rappel : x $\in$ H $\Leftrightarrow \overline{x} = \overline{0} = 0_{G/H}$.

Déf : Le groupe (abélien) G / H ainsi défini s'appelle le <u>groupe quotient de G par H</u>.

L'application $\varphi : G \to G / H$, $x \mapsto \bar{x}$ s'appelle <u>l'homomorphisme canonique</u> de G dans G / H .

Prop : L'homomorphisme canonique φ est un homomorphisme surjectif, de noyau Ker φ = H

Remarque : Si G non-abélien, le lemme 2 est encore vrai, à condition de faire une hypothèse « spéciale » sur H (H doit être sous-groupe distingué).

<u>7) Indice d'un sous-groupe, théorème de Lagrange :</u>

Rappel : Soit $f : E \to F$, application surjective.
E fini $\Rightarrow$ F fini et Card F $\leq$ Card E

Notation : Card E = | E |

G groupe , pas forcément abélien, fini.
Convention : | G | = ordre de G $\in \mathbf{N} \cup \{+\infty\}$ (Cas général)

H sous-groupe de G. H est d'ordre fini avec | H | $\leq$ | G |

G / H (ensemble quotient) est un ensemble fini
(car $\varphi : G \to G / H$, $x \mapsto \bar{x}$ est une application surjective).

Déf : $| G / H |$ s'appelle <u>l'indice de H dans G</u> .

Notons $| G / H | = [G : H]$

Lemme 1 : $x \in G$, $\bar{x} = \{ y = hx / h \in H \}$

Lemme 2 : $(\forall x \in G)$, $| \bar{x} | = | H |$

Théorème : Soit G groupe fini, H sous-groupe de G .
Alors , $| G | = [G : H] | H |$

Remarque : $| G | , | H | , | G / H | \in \mathbf{N}^*$

Corollaire (Théorème de Lagrange) :
Si G groupe fini (pas forcément abélien), et si H est un sous-groupe de G alors : $| H |$ divise $| G |$ (dans $\mathbf{N}^*$)

<u>8) Propriété universelle et théorème d'isomorphisme :</u>

G groupe abélien, H sous-groupe de G .
φ l'homomorphisme canonique associé.

Théorème : (propriété universelle de G / H)

Soit $f : G \to G'$, un homomorphisme de groupe abélien.
$N = \mathrm{Ker}\, f$.
Supposons $H \subset N$.

Alors :

- Il existe une unique application $\overline{f}$: G / H $\to$ G'
telle que : ($\forall$ x $\in$ G) , $\overline{f}(\overline{x})$ = f(x)
- $\overline{f}$ est un homomorphisme de groupes
- Im ($\overline{f}$) = Im (f)
- Ker ($\overline{f}$) = φ (N) = { $\overline{x}$ / x $\in$ N } $\subset$ G / H

Théorème d'isomorphisme :
Soit f : G $\to$ G' , un homomorphisme surjectif de groupes abéliens. Soit H = Ker f
Alors G / H $\approx$ G' par l'isomorphisme
$\overline{f}$: G / H $\to$ G', $\overline{x} \mapsto$ f(x) .

9) Groupes monogènes, groupes cycliques :

Soit G groupe multiplicatif , a $\in$ G.

Prop : < a > = { a^n / n $\in$ $\mathbf{Z}$ } est un sous-groupe de G . Il contient a, et c'est le plus petit sous-groupe de G qui contient a .

Remarque : Dans le cas additif , < a > = { na / n $\in$ $\mathbf{Z}$ }

Déf : Le groupe G est monogène s'il existe a de G tel que G = < a >
(En notation multiplicative , G ne contient que des puissances de a et en notation additive, G ne contient que des multiples de a).

On dit que G est engendré par a ou que a est un générateur de G .

Déf : Si G est fini, on remplace monogène par cyclique.

Exples :

1. $\mathbf{Z} = \{ n \times 1 \ / \ n \in \mathbf{Z} \}$ est monogène , non-cyclique, engendré par 1 .

1 et –1 sont les seuls générateurs de $\mathbf{Z}$ (comme groupe monogène).

2. ($n \in \mathbf{N}^*$) $U_n = \{ z \ / \ z^n = 1 \}$ = sous-groupe multiplicatif de $\mathbf{C}^*$.

   $a = e^{\frac{2ip}{n}}$, $U_n = \{ a^k \ / \ k \in \mathbf{Z} \}$ est monogène, engendré par a .
   Il est cyclique ,car $|U_n| = n$

Prop : Si G est cyclique ,alors G est abélien .

Prop : Soit $f : G \to G'$, homomorphisme surjectif de groupes . G monogène (ou cyclique) engendré par a , alors G’ est monogène (ou cyclique) engendré par f(a) = a’ (image par f de a).

Sous-groupes de $\mathbf{Z}$:

Théorème : Tout sous-groupe de $\mathbf{Z}$ est de la forme n$\mathbf{Z}$, n $\in$ $\mathbf{N}$).

10) Les groupes quotients $\mathbf{Z}$ / n$\mathbf{Z}$:

Soit n $\in$ $\mathbf{N}^*$, H = n $\mathbf{Z}$ sous-groupe de $\mathbf{Z}$
On considère le groupe quotient $\mathbf{Z}$ / n$\mathbf{Z}$ = $\{\bar{x}$ / x $\in$ $\mathbf{Z}\}$

Prop : $\mathbf{Z}$ / n$\mathbf{Z}$ est un groupe fini d'ordre | $\mathbf{Z}$ / n$\mathbf{Z}$ | = n

En fait , $\mathbf{Z}$ / n$\mathbf{Z}$ **=** $\{ \bar{0},\bar{1},\ldots,\overline{n-1} \}$

Prop : ($\mathbf{Z}$ / n$\mathbf{Z}$, +) est un groupe cyclique (d'ordre n) ayant pour générateur $\bar{1}$.

11) Ordre d'un élément :

G : groupe multiplicatif (pas forcément abélien) a $\in$ G

Déf : a est d'ordre fini s'il existe n de $\mathbf{N}^*$ tel que $a^n = 1$. Le plus petit entier n de $\mathbf{N}^*$ tel que $a^n = 1$ s'appelle l'ordre de a .

Notation : ordre de a = o(a)

Déf : a est <u>d'ordre infini</u> si ($\forall$ n $\in$ $\mathbf{N}^*$) , $a^n \neq 1$.
o(a) = ∞ .

Supposons maintenant G additif :

Déf : a est <u>d'ordre fini</u> ou <u>de torsion</u> s'il existe un entier n de $\mathbf{N}^*$ tel que : na = 0_G .
Le plus petit entier n de $\mathbf{N}^*$ tel que na = 0_G s'appelle alors <u>l'ordre</u> de a .

Notation : o(a)

Déf : a est <u>d'ordre infini</u> ou est <u>sans torsion</u> , si ($\forall$ n $\in$ $\mathbf{N}^*$) , na $\neq 0_G$.
o(a) = ∞ .

Soit f : $\mathbf{Z} \to$ G , n $\mapsto$ f(n) = a^n (en notation multiplicative) et f(n) = na (en notation additive)

f est un homomorphisme de groupes et Im f = < a >

Remarque d'ordre général : Soit f : E $\to$ E' application . F = Im f = { f(x) / x $\in$ E } $\subset$ E' .
On peut considérer f : E $\to$ F , alors f devient surjective .

Considérons , dans notre cas, f : $\mathbf{Z} \to$ < a > = H (sous-groupe de G engendré par a)

D'après la remarque précédente, f est un homomorphisme surjectif .

Lemme :

- Si $o(a) = \infty$, alors Ker f = { 0 }
- Si $o(a) = d < +\infty$, ($d \geq 1$) , alors Ker f = $d\mathbf{Z}$

Prop : (en notation multiplicative)
Supposons $o(a) = \infty$.

- $H = < a >$ est isomorphe à $\mathbf{Z}$ par l'isomorphisme
  $\mathbf{Z} \to H = < a >$, $n \mapsto f(n) = a^n$.
- $< a >$ est un groupe monogène infini.
- Les a^n ($n \in \mathbf{Z}$) sont 2 à 2 distincts .

Remarque : On obtient la même proposition en notation additive, en remplaçant a^n par na .

Prop : (en notation multiplicative)
Supposons a d'ordre fini et posons $o(a) = d \geq 1$.

- $H = < a > \approx \mathbf{Z} / d\mathbf{Z}$ par l'isomorphisme :

  $\mathbf{Z} / d\mathbf{Z} \to H = < a >, \bar{n} \mapsto a^n \quad (\forall\, n \in \mathbf{Z})$
- $| < a > | = d$ (donc $< a >$ est cyclique d'ordre d)
- $(\forall\, k \in \mathbf{Z})$, $< a > = \{ a^k , a^{k+1} , \ldots , a^{k+d-1} \}$ (les éléments sont deux à deux distincts)

Remarque : Il est aisé d'écrire la même proposition en notation additive.

Corollaire : $(\forall a \in G)$ (G pas forcément abélien)

$o(a) = | < a > | \in \mathbf{N}^* \cup \{ \infty \}$

Corollaire : Soit G groupe fini , pas forcément abélien. $| G | = N$ ($N \geq 1$). Soit $a \in G$:

- a est toujours d'ordre fini
- $d = o(a)$ divise N

Corollaire : Soit G groupe fini , $N = | G | \geq 1$
$(\forall a \in G)$, $a^N = 1$ ($Na = 0$, en notation additive)

Prop : Soit $a \in G$, G : groupe multiplicatif. Soit $n \in \mathbf{Z}$.

- Si $o(a) = \infty$, $a^n = 1$ ssi $n = 0$.
- Si $o(a) = d \in \mathbf{N}^*$, $a^n = 1$ ssi $d | n$.

12) Classification des groupes cycliques :

Soit $d \in \mathbf{N}^*$

Prop : Tout groupe isomorphe à $\mathbf{Z} / d\mathbf{Z}$ est un groupe cyclique d'ordre d .

Prop : Les groupes cycliques d'ordre d sont les groupes isomorphes à $\mathbf{Z} / d\mathbf{Z}$ et aucun autre .

IV) Généralités sur les anneaux :

1) Anneaux :

Déf : Soit A un ensemble non-vide. On munit A de deux lois de composition internes + et $\times$.
On dit que (A , + , $\times$) est un anneau si :

- (A,+) est un groupe abélien
- $\times$ est associative
- $\times$ est distributive , à droite et à gauche sur + (c'est-à-dire : ($\forall$ a,b,c $\in$ A) , a(b + c) = ab + ac et (b + c)a = ba + ca).
- Il existe un élément neutre , noté 1_A , pour $\times$

Déf : On dit que A est commutatif si $\times$ est commutatif .

Prop : 1_A est unique .

Prop : 0_A est absorbant.
(c'est-à-dire : ($\forall$ x $\in$ A) , $x \,.\, 0_A = 0_A \,.\, x = 0_A$.)

Prop : (règle des signes)
($\forall$ a,b $\in$ A)

- a(-b) = (-a)b = -(ab)
- (-a)(-b) = ab

Remarque : Toutes les règles du calcul algébrique connues dans **Z** sont valables dans A sous reserve que xy peut être différent de yx .

Prop : Si A n'est pas réduit à un seul élément, alors $1_A \neq 0_A$.

Déf : (caractéristique de A)
1er cas : $o(1_A) = \infty$ (dans (A,+)) . Alors A a pour caractéristique 0 . (caractéristique nulle)

2ième cas : $o(1_A) = d \in \mathbf{N}^*$. Alors, A est de caractéristique d .(caractéristique positive)

Prop : Si A est de caractéristique positive d ($d \in \mathbf{N}^*$), alors ($\forall a \in A$) , $da = 0_A$.

2)Sous-anneaux :

A anneau , pas forcément commutatif.

Déf : Soit B sous-ensemble de A . On dit que B est un sous-anneau si :

- $1_A \in B$
- B stable par + et $\times$
- (B, + , $\times$) est un anneau

Remarque 1 : (B, +) est sous-groupe de (A, +)
Remarque 2 : $1_B = 1_A$

Prop : Soit B sous-ensemble de A. C'est un sous-anneau de A si :

- $1_A \in B$
- $(B , +)$ sous-groupe de $(A , +)$
- B stable par $\times$

Prop : Soit B sous-ensemble de A . C'est un sous-anneau de A si :

- $1_A \in B$
- $(\forall x,y \in B) , x - y \in B$
- $(\forall x,y \in B) , xy \in B$

Prop : Soit B sous-anneau de A.

(i) A commutatif $\Rightarrow$ B commutatif

(ii) Caractéristique de B = caractéristique de A

(iii) C = sous-ensemble de A.

C sous-anneau de B $\Leftrightarrow C \subset B$ et C sous-anneau de A .

Exples :

$(\mathbf{Z} , + , \times)$, $(\mathbf{Q} , + , \times)$, $(\mathbf{R} , + , \times)$, $(\mathbf{C} , + , \times)$ sont des anneaux commutatifs .

$(\mathbf{Z} , + , \times)$ sous-anneau de $(\mathbf{Q} , + , \times)$,de $(\mathbf{R} , + , \times)$,de $(\mathbf{C} , + , \times)$.

Si on considère l'anneau des matrices carrées à coefficients complexes , il est <u>non-commutatif</u>.

<u>Anneau des entiers de Gauss</u>

$\mathbf{Z}[i] = \{ z = x + iy \,/\, x \in \mathbf{Z}, y \in \mathbf{Z} \} \subset \mathbf{C}$.

$(\mathbf{Z}[i] ,+ , \times)$ est un sous-anneau commutatif de $(\mathbf{C} ,+ , \times)$

<u>3)Eléments inversibles :</u>

A est un anneau, A non-réduit à $\{0\}$.

Déf : $x \in A$, x est <u>inversible</u> s'il existe y de A tel que $xy = yx = 1_A$.
y = inverse de x . $y = x^{-1}$.

Remarque : y est unique .
Exples :

- 1_A est inversible, d'inverse $1_A^{-1} = 1_A$.
- 0_A n'est pas inversible (sinon : $\exists\, y \in A, 0_A . y = 1_A$ Impossible car $0_A \neq 1_A$)

Prop : Soient x,y deux éléments inversibles de A .
Alors :

(i) xy est inversible , $(xy)^{-1} = y^{-1}x^{-1}$.
(ii) x^{-1} est inversible , $(x^{-1})^{-1} = x$

Déf : Les éléments inversibles de A sont appelés les unités de A .

U(A) = ensemble de toutes les unités de A .

U(A) est stable par la multiplication de A .

Prop : (U(A) , $\times$) est un groupe (multiplicatif)

Remarque : A anneau commutatif $\Rightarrow$ U(A) groupe abélien.

Déf : U(A) : groupe des unités (ou groupe des éléments inversibles) dans A .

Remarques : $1_{U(A)} = 1_A$.
$\forall$ x $\in$ U(A) , l'inverse de x dans U(A) = l'inverse de x dans A .

Prop : Soit B sous-anneau de A.

- Soit x de B :

(x est inversible dans B) $\Leftrightarrow$ (x est inversible dans A et , de plus son inverse y dans A appartient à B)

- U(B) est un sous-groupe de U(A)

Remarque : U(A) $\subset$ A \ { 0 } (toujours vrai)

Déf : (Corps)
A est <u>un corps</u> ssi U(A) = A \ {0}, c'est-à-dire, si tous les éléments non-nuls de A sont inversibles .

Si,de plus, A est commutatif, on dit que c'est un <u>corps commutatif</u> .

Convention : Si A est un corps commutatif, si a,b $\in$ A, et si b $\neq$ 0 , alors : $ab^{-1} = \frac{a}{b}$. (Règles habituelles du calcul sur les fractions s'appliquent) .

Remarque : Dans le cas non-commutatif, ceci ne marche pas, car en général $ab^{-1} \neq b^{-1}a$

Exples :

- ($\mathbf{Z}$, + , $\times$) n'est pas un corps

car U($\mathbf{Z}$) = { -1 ,+1 } $\neq$ $\mathbf{Z}$ \ {0}

- A = **Q** , **R** , **C** sont des corps commutatifs .

- **Z**[i] n'est pas un corps
  car U(**Z**[i]) = { -1 ;1 ;i ;-i } $\neq$ **Z**[i] \ {0}

<u>4) Anneau intègre ,corps des fractions :</u>

Déf : Un anneau A est <u>intègre</u> si A est non-réduit à {0} et si :
($\forall$ x,y $\in$ A) , xy = 0 $\Rightarrow$ x = 0 ou y = 0

(Ce qui équivaut à : $x \neq 0$ et $y \neq 0 \Rightarrow xy \neq 0$)

Exples :

Z , **Q** , **R** et **C** sont des anneaux intègres .

Remarque : Tout corps est un anneau intègre .

Prop : Si A est intègre, B sous-anneau de A ,alors B sous-anneau intègre .

Conséquence : **Z**[i] est un anneau intègre (car sous-anneau de **C**).

Prop : Soit A un anneau intègre.

- Tout élément a de A , $a \neq 0_A$, est simplifiable à gauche et à droite

$$(\forall (b,c) \in A^2) \quad \begin{array}{l} ab = ac \Rightarrow b = c \\ ba = ca \Rightarrow b = c \end{array}$$

- Si A a une caractéristique $p > 0$, alors p est un nombre premier .

Déf : (corps des fractions)
Soit A un anneau commutatif. On appelle <u>corps des fractions de A</u> , un corps commutatif K tel que :

- A est un sous-anneau de K
- Tout élément x de K peut s'écrire : x = $\frac{a}{b}$ avec a,b dans A , b $\neq$ 0 .

Exple : **Q** est corps des fractions de **Z** .

Remarque : Si A (anneau commutatif) admet un corps des fractions K, alors A est intègre .

Théorème : Tout anneau A commutatif et intègre possède un corps des fractions .

Prop : (cas particulier du théorème)
Soit A un anneau commutatif, A contenu dans un corps commutatif L (c'est-à-dire A=sous-anneau de L)
(Donc A est intègre)
Posons K = { x = $\frac{a}{b}$ / a,b $\in$ A , b $\neq$ 0 } (c'est un sous-ensemble de L)

- K est un sous-corps de L
- K corps des fractions de A .

Exple :
Q[i] = { z = x + iy / x , y $\in$ **Q** } est corps des fractions de **Z**[i]

5) Idéaux d'un anneau commutatif :

Soit A un anneau commutatif.

Déf : Soit I sous-ensemble de A. On dit que I est un idéal de A si :

- (I,+) sous-groupe de (A,+)
- I est absorbant , c'est-à-dire : $(\forall\ x \in I)(\forall\ a \in A)$, $xa \in I$.

Remarque : I sous-groupe de (A,+) ,alors $0_A \in I$

Prop : Soit I sous-ensemble de A. I est un idéal de A si il vérifie :

(i) $I \neq \emptyset$

(ii) I est stable par +

(c'est-à-dire : $x,y \in I \Rightarrow x + y \in I$)

(iii) I est absorbant.

Exples :

{0} est un idéal de A.

I = A est un idéal de A . On l'appelle l'idéal impropre .

Déf : Tout idéal I tel que $I \neq A$, est appelé idéal propre .

Prop : Soit I idéal de A .

$I = A \Leftrightarrow 1 \in I$

Prop : Soit I idéal de A, A $\neq \{0\}$

I = A $\Leftrightarrow$ I contient un élément inversible de A (au moins)

<u>Opérations sur les idéaux :</u>

Prop : Soit $(I_u)_{u \in U}$, une famille d'idéaux. ($U \neq \varnothing$)
Alors :

$$\bigcap_{u \in U} I_u \quad \text{est un idéal de A.}$$

Prop : Soient I_1 , I_2 , … , I_n n idéaux de A ($n \geq 1$).
Posons $I = \{ x = x_1 + x_2 + \ldots + x_n \,/\, x_1 \in I_1 , x_2 \in I_2 , \ldots, x_n \in I_n \}$
(Par convention , on note $I = I_1 + I_2 + \ldots + I_n$)
Alors :

- I est un idéal de A (appelé <u>somme des idéaux I_1 ,…, I_n</u>)
- $I_1 , I_2 , \ldots , I_n \subset I$
- I est le plus petit idéal de A qui contient I_1 , … ,I_n

Remarque : La somme $I = I_1 + I_2 + \ldots + I_n$ est inchangée quand on modifie l'ordre des idéaux I_1 , I_2 , … , I_n .

6) Idéaux particuliers :

Soit A anneau commutatif. Soit a de A :

Notation : $Aa := \{ xa \,/\, x \in A \} \subset A$

Prop : I = Aa est un idéal de A. I contient a. C'est le plus petit idéal de A qui contient a .

Déf : I = Aa s'appelle l'idéal principal de A engendré par a .

Si J est un idéal , J est principal s'il existe b de A tel que J = Ab . b est un générateur de J .

Déf : Soit I idéal de A.
I est premier si :

(i) I est propre (c'est-à-dire $I \neq A$)
(ii) $(\forall a,b \in A)\ \ ab \in I \Rightarrow a \in I$ ou $b \in I$

Remarque : Si A est intègre , $I = \{0\}$ est un idéal premier.

Déf : Soit I idéal de A .
I est un idéal maximal si :

(i) I est propre
(ii) $(\forall J$ idéal de A) , $I \subset J$ et $I \neq J \Rightarrow J = A$.

Remarque : Si A est un corps , alors I = {0} est maximal .

7) Homomorphismes d'anneaux :

Soient A et B deux anneaux (pas forcément commutatifs). $f : A \to B$ application .

Déf : f est un homomorphisme d'anneaux si :

(i) $f(1_A) = 1_B$

(ii) $f(x + y) = f(x) + f(y)$ $(\forall\ x,y \in A)$(f additif)

(iii) $f(xy) = f(x)f(y)$ $(\forall\ x,y \in A)$(f multiplicatif)

$\mathrm{Ker}\, f = \{ x \in A \,/\, f(x) = 0_B \} = f^{-1}(\{0_B\})$

$\mathrm{Im}\, f = \{ f(x) \,/\, x \in A \} \subset B$

Remarque : En particulier , (avec le (ii))
$f : (A,+) \to (B,+)$ est un homomorphisme de groupes additifs .

Prop : $f : A \to B$, homomorphisme d'anneaux .

(i) $f(0_A) = 0_B$

(ii) $(\forall\ x \in A)$, $f(-x) = -f(x)$

(iii) $(\forall\, x \in A)(\forall\, n \in \mathbf{Z})$, $f(nx) = nf(x)$
(iv) $f(x - y) = f(x) - f(y)$ $(\forall\, x,y \in A)$
(v) f injectif $\Leftrightarrow$ Ker f = $\{0_A\}$

Prop :

- $(\forall\, x_1 , x_2 , \ldots , x_n \in A)$, $f(x_1x_2 \ldots x_n) = f(x_1)f(x_2)\ldots f(x_n)$
- $(\forall\, x \in A)(\forall\, n \in \mathbf{N})$, $f(x^n) = (f(x))^n$.

Prop : Soit $f : A \rightarrow B$, homomorphisme d'anneaux

- Im f est un sous-anneau de B
- Si A est commutatif, alors Ker f est un idéal de A.

Prop : Soit A, B et C trois anneaux , f et g deux homomorphismes d'anneaux tels que :
$f : A \rightarrow B$, $g : B \rightarrow C$.
Alors : $h = gof : A \rightarrow C$ est un homomorphisme d'anneaux .

Déf : Soient A et B deux anneaux. $f : A \rightarrow B$ une application.
f est un <u>isomorphisme d'anneaux</u> si :
(i) f est un homomorphisme d'anneaux
(ii) f est bijectif

Notation : S'il existe un isomorphisme d'anneaux
$f : A \rightarrow B$. On dit que l'anneau A est <u>isomorphe</u> à l'anneau B et on écrit : $A \approx B$

Prop : Soit f : A $\to$ B , un isomorphisme d'anneaux. Alors, la bijection réciproque f^{-1} : B $\to$ A est aussi un isomorphisme d'anneaux .

Prop : Si f : A $\to$ B est un isomorphisme d'anneaux et g : B $\to$ C également, alors h = gof : A $\to$ C est aussi un isomorphisme d'anneaux .

Prop : Soient A et B deux ensembles munis (pour chacun) d'une loi de composition interne + et d'une loi $\times$.
Soit f : A $\to$ B une application additive et multiplicative. Supposons que (A , + , $\times$) soit un anneau et que f : A $\to$ B soit surjective .
Alors :

(i) (B , + , $\times$) est un anneau
(ii) f : A $\to$ B est un homomorphisme d'anneaux (surjectif)
(iii) A anneau commutatif $\Rightarrow$ B anneau commutatif .

Prop : f : A $\to$ B homomorphisme d'anneaux surjectif.
Alors :
A commutatif $\Rightarrow$ B commutatif

Prop : Soient A et B deux anneaux tels que : A $\approx$ B .

- Si l'un des deux est commutatif , l'autre l'est aussi .
- Si l'un des deux est intègre, l'autre l'est aussi.
- Si l'un des deux est un corps, l'autre l'est aussi.

8) Anneaux quotients :

A anneau commutatif. I idéal de A.
Rappel : I sous-groupe de (A,+) = groupe abélien.
On sait alors définir <u>le groupe quotient</u> A / I .
(cf. les groupes quotients : III)6))

On munit A / I d'une seconde loi de composition interne $\times$ telle que :
$(\forall\, x,y \in A) : \bar{x} \times \bar{y} = \overline{x \times y}$

Prop :

- (A / I , + , $\times$) est un anneau commutatif
- $1_{A/I} = \overline{1_A}$
- $(x \in A,\ n \in \mathbf{N})$, $(\bar{x})^n = \overline{x^n}$

Prop : $\varphi : A \to A / I$, $x \mapsto \bar{x}$ est un homomorphisme d'anneaux surjectif de noyau I .

Déf :
A / I <u>l'anneau quotient de l'anneau commutatif par son idéal I</u> .
φ <u>l'homomorphisme canonique</u> de A dans A / I .

Exple :

A = $\mathbf{Z}$, d $\in \mathbf{Z}$, d > 0, d $\mathbf{Z}$ = { nd / n $\in \mathbf{Z}$ } = idéal de $\mathbf{Z}$ (= idéal principal engendré par d)

Donc $(\mathbf{Z} / d\,\mathbf{Z}, +, \times)$ est un anneau commutatif .

$\mathbf{Z} / d\,\mathbf{Z} = \langle \bar{1} \rangle \Rightarrow o(\bar{1}) = |\ \langle \bar{1} \rangle\ | = d$

Conséquence :

$\mathbf{Z} / d\,\mathbf{Z}$ est un anneau de caractéristique d ($d > 0$) .

9) Quotients par des idéaux particuliers :

Soit A anneau commutatif , I idéal de A .

Prop : A / I non-réduit à $\{\bar{0}\}$ $\Leftrightarrow$ I idéal propre.

Prop : A / I est intègre $\Leftrightarrow$ I idéal premier de A .

Prop : A / I est un corps (commutatif) $\Leftrightarrow$ I est maximal

Corollaire : Soit I idéal de A.

I maximal $\Rightarrow$ I premier .

10) Propriété universelle , théorème d'isomorphisme :

A anneau commutatif, I idéal de A .

$\varphi : A \to A / I$ homomorphisme canonique .

Théorème : (Propriété universelle de A / I)
Soit f : A $\rightarrow$ B un homomorphisme d'anneaux (B pas forcément commutatif)
N = Ker f (N : idéal de A) . Supposons $I \subset N$.

(i) Il existe une unique application :
$\overline{f}$: A / I $\rightarrow$ B , telle que $\overline{f}(\overline{x}) = f(x)$ ($\forall$ x $\in$ A)
(ii) $\overline{f}$ est un homomorphisme d'anneaux .
(iii) Im $\overline{f}$ = Im f
(iv) Ker $\overline{f} = \varphi(N) = \{ \overline{x} \ / \ x \in N \}$.

Remarques :

- f surjective $\Rightarrow$ $\overline{f}$ surjective
- Si N = I , alors $\overline{f}$ injective

Théorème : (Théorème d'isomorphisme)
Soit f : A $\rightarrow$ B homomorphisme d'anneaux surjectif, l'anneau A étant commutatif (de sorte que B est aussi commutatif)
Soit I = Ker f
Alors : B $\approx$ A / I par l'isomorphisme : A / I $\rightarrow$ B ,
$\overline{x} \mapsto f(x)$ ($\forall$ x $\in$ A)

<u>11) Produits directs d'anneaux :</u>

Soient A_1 , A_2 , … , A_n n anneaux .($n \geq 2$)

On pose $A = A_1 \times A_2 \times \ldots \times A_n$. On munit A de deux lois :
Si on pose $a = (a_1 , \ldots , a_n)$, $b = (b_1 , \ldots , b_n)$, $a,b \in A$ et $a_i \in A_i$, $b_i \in B_i$.

$a + b = (a_1 + b_1 , \ldots , a_n + b_n) \in A$
$a \times b = (a_1 \times b_1 , \ldots , a_n \times b_n) \in A$

Prop :

(i) $(A , + , \times)$ est un anneau
(ii) $0_A = (0_{A1}, \ldots , 0_{An})$ et $1_A = (1_{A1}, \ldots , 1_{An})$
(iii) $A_1 , \ldots , A_n$ tous commutatifs $\Rightarrow$ A commutatif .

Déf : A est appelé produit direct des anneaux $A_1 , \ldots , A_n$.

Prop : Soit $i \in [| 1 ; n |]$.
On pose $\Pi_i : A \to A_i$, $a = (a_1 , \ldots ,a_n) \mapsto \Pi_i (a) = a_i$.
Π_j est un homomorphisme d'anneaux surjectif.

Par suite, si A est commutatif, A_i est aussi commutatif ($\forall i \in [| 1 ; n |]$) .

Remarque : Soit $a = (a_1 , \ldots , a_n) \in A$.
$a \in \operatorname{Ker} \Pi_i \Leftrightarrow a_i = 0_{Ai}$

Prop :
Ker $\Pi_i = A_1 \times \ldots \times A_{i-1} \times \{0_{A_i}\} \times A_{i+1} \times \ldots \times A_n$.
Prop : Supposons $A_1, \ldots, A_n$ commutatifs (de sorte que A est commutatif)
Soit $i \in [| 1 ; n |]$:

$I_i = A_1 \times \ldots \times A_{i-1} \times \{0_{A_i}\} \times A_{i+1} \times \ldots \times A_n \subset A$
Alors :
I_i est un idéal de A et $A_i \approx A / I_i$ par l'isomorphisme :
$A / I_i \rightarrow A_i$, $\bar{a} = \overline{(a_1, a_2, \ldots, a_n)} \mapsto a_i = (\Pi_i (a))$.

12) Quelques anneaux particuliers :

Soit A anneau . On note $A^* = A \setminus \{0\}$.

Déf : A est un anneau <u>euclidien</u> si :
- A est commutatif et intègre
- Il existe une application $g : A^* \rightarrow \mathbf{N}$, appelée <u>stathme euclidien</u> sur A , telle que :

$(\forall (a,b) \in A \times A^*) (\exists (q , r) \in A \times A)$ vérifiant :

- $a = bq + r$
- $r = 0$ ou $g(r) < g(b)$ (lorsque $r \neq 0$)

Exples :

(i) $\mathbf{Z}$ est euclidien par le stathme $g : \mathbf{Z}^* \rightarrow \mathbf{N}$, $x \mapsto g(x) = | x |$

(ii) $\mathbf{Z}[i]$ est euclidien par le stathme
$g : \mathbf{Z}[i]^* \to \mathbf{N}$, $z \mapsto g(z) = N(z) = | z |^2$.

Prop : (k = corps commutatif , X = indéterminée)
Il existe un unique anneau commutatif A tel que :

- k = sous-corps de l'anneau A (de sorte que : $0_A = 0_k$, $1_A = 1_k$)
- $X \in A$ et tout élément P de A peut s'écrire :

$P = a_0 + a_1X + \ldots + a_nX^n$ ($a_i \in k$)

- Si $a_0 + a_1X + \ldots + a_nX^n = 0$ ($a_i \in k$) , alors : $a_0 = a_1 = \ldots = a_n = 0$

Déf : A s'appelle <u>l'anneau des polynômes en l'indéterminée X à coefficients dans k</u> .

On le note A = k[X] . Ses éléments s'appellent <u>polynômes</u>.

Les éléments de k s'appellent <u>les polynômes constants</u> .

n = degré de P =deg(P) . $\deg(P) \in \mathbf{N}$
(n'a de sens que si $P \neq 0$)

Remarque : $\deg(P) = 0 \Leftrightarrow P \in k^*$.

Prop : $P , Q \in k[X] \setminus \{0\}$
(i) $PQ \neq 0$ et $\deg(PQ) = \deg(P) + \deg(Q)$
(ii) Si $P + Q \neq 0$, alors $\deg(P + Q) \leq \sup(\deg P, \deg Q)$
(iii) Si $\deg(P) \neq \deg(Q)$,alors $P + Q \neq 0$ et $\deg(P + Q) = \sup(\deg P , \deg Q)$

Conséquence : $A = k[X]$ est un anneau commutatif et intègre et $U(A) = k \setminus \{0\}$

Prop : $A , B \in k[X] , B \neq 0$.
Il existe un unique couple $(Q,R) \in A \times A$ tel que : $A = BQ + R$ et $R = 0$ ou $\deg R < \deg B$.
(division euclidienne dans $k[X]$) .

Prop : $d : k[X] \setminus \{0\} \rightarrow \mathbf{N}$, $P \mapsto d(P) = \deg(P)$ est un stathme euclidien pour $k[X]$.

Prop : (k corps commutatif)
$k[X]$ est un anneau euclidien .

Déf : (Anneau principal)
A anneau est dit <u>principal</u> si :
(i) A est commutatif et intègre
(ii) Tous les idéaux de A sont principaux .

Prop : A euclidien $\Rightarrow$ A principal .

Conséquence : **Z** , **Z**[i] et k[X] (avec k corps commutatif) sont des exemples d'anneaux principaux .

12) Divisibilité dans un anneau commutatif intègre :

On considère A un anneau commutatif intègre .
$A^* = A \setminus \{0\}$. U(A) =groupe des unités de A.

Déf : Soient a,b de A^* .
a divise b (a diviseur de b, b multiple de a) si b =aq (q $\in$ A) .

Remarque : Nécessairement, $q \in A^*$.
On note a | b .

Remarque : $a \mid b \Leftrightarrow b \in Aa \Leftrightarrow Ab \subset Aa$. (car Ab est le plus petit idéal qui contient b)

Prop : Dans A^* , la relation binaire « a | b » est réflexive et transitive .

Déf : Soient $a,b \in A^*$. On dit que a et b sont associés ssi a | b et b | a .

Prop : Soient $a,b \in A^*$. Les propriétés suivantes sont équivalentes :

(i) a et b associés
(ii) $Aa = Ab$
(iii) $a = \varepsilon b$ avec $\varepsilon \in U(A)$.

Notation : a et b associés : $a \equiv b$.

Prop : Dans A^* , la relation binaire « $a \equiv b$ » est une relation d'équivalence .

Prop : Si $a \equiv b$, alors a et b ont les mêmes diviseurs et les mêmes multiples .

Soient A anneau commutatif intègre .
$a_1 , \dots , a_n \in A^*$ $(n \geq 1)$, $d \in A^*$.

Déf :
d est un <u>PGCD</u> de $a_1 , \dots , a_n$ si :
(i) d est un diviseur commun à $a_1 , \dots , a_n$.
(ii) $(\forall\, \delta \in A^*)$ δ diviseur commun à $a_1 , \dots , a_n$ $\Rightarrow$ $\delta \mid d$.

Notation : $d = \mathrm{PGCD}(a_1 , \dots , a_n)$

Exple :
Supposons que $a_1 \mid a_2 , \dots , a_n \Rightarrow a_1 = \mathrm{PGCD}(a_1 , \dots , a_n)$.

Remarques :

- Il n'existe pas toujours de PGCD
- On n'a pas unicité du PGCD .

Prop : Soit $d = PGCD(a_1 , \dots , a_n)$.
Soit $d' \in A^*$, $d' = PGCD(a_1 , \dots , a_n) \Leftrightarrow d' \equiv d$.

Prop : Soit $\delta \in A^*$:
$\delta \mid a_1 , \dots , a_n \Leftrightarrow A\delta \supset Aa_1 + \dots + Aa_n$.

Prop : Supposons A principal. Soient $a_1 , \dots , a_n \in A^*$ et $d \in A^*$, $d = PGCD(a_1 , \dots , a_n) \Leftrightarrow Ad = Aa_1 + \dots + Aa_n$

Remarque : $\Leftarrow$ est toujours vrai .

Prop : Tout anneau principal est un anneau avec PGCD.

Déf :
Soit A anneau commutatif intègre . $a_1 , \dots , a_n \in A^*(n \geq 2)$. $m \in A^*$.
m = <u>PPCM</u>$(a_1 , \dots , a_n)$ si :

(i) m = multiple commun de $a_1 , \dots , a_n$.

(ii) $(\forall \mu \in A^*)$, μ = multiple commun de $a_1 , \dots , a_n$, alors μ = multiple de m .

Exple :
Si a_1 est un multiple de $a_2 , \dots , a_n$, alors $a_1 = PPCM(a_1 , \dots , a_n)$.

Remarque : Il n'y a pas toujours de PPCM .

Prop : $m = \mathrm{PPCM}(a_1 , \dots , a_n)$. Soit $m' \in A^*$ tel que $m' = \mathrm{PPCM}(a_1 , \dots , a_n) \Leftrightarrow m' \equiv m$.

Remarque : b multiple de a $\Leftrightarrow Ab \subset Aa$.

Prop : Soit $\mu \in A^*$, μ : multiple commun de $a_1 , \dots , a_n$ $\Leftrightarrow A\mu \subset Aa_1 \cap \dots \cap Aa_n$.

Prop : Supposons A principal . Soit $m \in A^*$.
$m = \mathrm{PPCM}(a_1 , \dots , a_n) \Leftrightarrow Am = Aa_1 \cap \dots \cap Aa_n$.

Remarque : ($\Leftarrow$) est vraie si A n'est pas principal .

Prop : Si A est un anneau principal, alors A est un anneau avec PPCM .

Déf : Soient $a_1 , \dots , a_n \in A^*$. $a_1 , \dots , a_n$ sont <u>premiers entre eux</u> si :
$(\forall \delta \in A^*)\ \ \delta \mid a_1 , \dots , a_n \Rightarrow \delta \in U(A)$

Prop : $a_1 , \dots , a_n$ sont premiers entre eux
$\Leftrightarrow 1 = \mathrm{PGCD}(a_1 , \dots , a_n)$.

Prop : (Propriétés de Bezout)
Supposons l'anneau A principal et soient $a_1 , \ldots , a_n \in A^*$.
$a_1 , \ldots , a_n$ premiers entre eux $\Leftrightarrow$ ($\exists\, u_1 , \ldots , u_n \in A$) tels que : $u_1a_1 + \ldots + u_na_n = 1$.

Déf :
a est <u>irréductible</u> si :
(i) $a \neq 0$ et $a \notin U(A)$
(ii) $(\forall\, \delta \in A^*)$, $\delta \mid a \Rightarrow (\delta \in U(A)$ ou $\delta \equiv a)$

Exples :
1) Supposons A corps commutatif : il n'existe aucun élément irréductible.

2) Considérons $A = \mathbf{Z}$.
Rappel : $U(A) = \{ -1 ; 1 \}$

Soit $a \in \mathbf{Z}$, a est irréductible ssi :
(i) $a \neq 0 , 1 , -1$
(ii) $(\forall\, \delta \in \mathbf{Z}^*)$, $\delta \mid a \Rightarrow \delta = \pm 1$ ou $\delta = \pm a$

Rappel : Un <u>nombre premier</u> est un entier p tel que :
(i) $p \geq 2$
(ii) $(\forall\, d \in \mathbf{N}^*)$, $d \mid p$ (dans $\mathbf{N}$) $\Rightarrow d = 1$ ou $d = p$.

Prop : Soit $a \in \mathbf{Z}$. Les propriétés suivantes sont équivalentes :

(i) a est irréductible dans $\mathbf{Z}$
(ii) $p = | a |$ est un nombre premier .
(iii) $a = \pm p$ avec p : nombre premier .

Cas particulier : Soit $a \in \mathbf{N}$
a est irréductible dans $\mathbf{Z} \Leftrightarrow$ a est un nombre premier (car $| a | = a$)

Exple :
$A = k[X]$ avec k : corps commutatif
Rappel : A est commutatif intègre ; mieux : A est principal.

- $U(A) = k^* = k \setminus \{0\}$
- $P , P' \in A^*$, $P \equiv P' \Leftrightarrow P' = \lambda P$ avec $\lambda \in k^*$. (deg (P) = deg(P')) .
- Soit $P \in A$. Il est irréductible (dans $A = k[X]$) ssi :
  1) P non-constant (c'est-à-dire : $P \notin k$)
  2) $(\forall D \in A^*)$, $D | P \Rightarrow D \in k^*$ ou $D = \lambda P$ ($\lambda \in k^*$)

- Si deg(P) = 1 (c'est-à-dire : $P = aX + b$, $a,b \in k$, $a \neq 0$) , alors P est irréductible .

  - Cas où $k = \mathbf{C}$, { polynômes irréductibles } = { polynômes de degré 1 } (car $\mathbf{C}$ est algébriquement clos)
  - Cas où $k = \mathbf{R}$, { polynômes irréductibles } = { polynômes de degré 1} $\cup$ { polynômes de la forme $aX^2 + bX + c$ tels que $b^2 - 4ac < 0$ }

- Cas où $k = \mathbf{Q}$: Il existe des polynômes irréductibles de degré arbitrairement grand . Exple : $X^n - 2$ est irréductible dans $A = \mathbf{Q}[X]$.($\forall n \in \mathbf{N}^*$)

Prop : Soient a,b de A^* tels que a et b sont irréductibles.

$a \mid b \Leftrightarrow a \equiv b$.

Prop : Soient a,b de A^* , a irréductible.
a ne divise pas b $\Leftrightarrow$ a,b premiers entre eux .

Prop : Supposons $a \equiv b$. Si l'un des deux est irréductible, alors l'autre l'est aussi .

Prop : Supposons A principal et soit a de A^* .
Les propriétés suivantes sont équivalentes :

(i) a est irréductible
(ii) Aa est un idéal premier
(iii) Aa est un idéal maximal .

Conséquence : (Propriété de Gauss)
Supposons A principal . Soit a de A^* , a irréductible :

$(\forall b,c \in A^*)$, $a \mid bc \Rightarrow a \mid b$ ou $a \mid c$.

Prop : Soit p de $\mathbf{N}^*$. Les propriétés suivantes sont équivalentes :

(i) p est nombre premier

(ii) $\mathbf{Z} / p\,\mathbf{Z}$ est intègre

(iii) $\mathbf{Z} / p\,\mathbf{Z}$ est un corps

13) Décompositions en produits de facteurs irréductibles :

Lemme 1 : (A commutatif intègre)
Soit $a \in A^* \setminus U(A)$:
Supposons a non-irréductible. Alors :

1) $a = bc$ avec $b,c \in A^* \setminus U(A)$
2) $Ab \supset Aa$ avec $Ab \neq Aa$ et $Ac \supset Aa$ avec $Ac \neq Aa$.

Lemme 2 : Supposons l'anneau A principal .
Soit $I_1 , I_2 , \dots , I_n , \dots$ une suite d'idéaux de A (n de $\mathbf{N}^*$)
tels que $I_1 \subset I_2 \dots \subset I_n \subset \dots$
Alors il existe $N \in \mathbf{N}^*$ tel que $I_n = I_N$ ($\forall\ n \geq \mathbf{N}$)

Théorème : Soit A un anneau principal .
Soit a de $A^* \setminus U(A)$. Alors, a se décompose en produit de facteurs irréductibles c'est-à-dire :

$\exists\, a_1 , \dots , a_s \in A^*$, les a_i irréductibles tels que :
$a = a_1 \times \dots \times a_s$ ($s \geq 1$)

Corollaire : Si A est un anneau principal , et si A n'est pas un corps , alors A contient des éléments irréductibles .

Soit A anneau commutatif intègre .

Prop : Il existe un ensemble $\wp$ formé d'éléments irréductibles de A tel que :

- (p1) ($\forall$ a élément irréductible de A)($\exists\, p \in \wp$) , $a \equiv p$
- (p2) ($\forall\, p,q \in \wp$) $p \equiv q \Rightarrow p = q$

Remarques :

- $\wp$ non-unique en général .
- Si on note E = { éléments irréductibles de A } , $\wp$ est un sous-ensemble de E obtenu en prélevant, dans chaque classe d'équivalence (rappel : « $\equiv$ » est une relation d'équivalence), un unique élément . $\wp \subset E$, par construction .

Exples :

1) Si A = **Z** ; $\wp$ = { nombres premiers }

Rappel : $a,b \in \mathbf{Z}^*$, $a \equiv b \Leftrightarrow a = \pm b$

$\wp$ est constitué d'éléments irréductibles :

(p1) $a \in \mathbf{Z}$, a irréductible $(\exists\, p \in \wp)$ $a = \pm p$
(p2) p,q de $\wp$, $p = \pm q$.

Exple :

A = k[X] , k corps commutatif .

Rappel : P, Q de $k[X]^*$, $P \equiv Q \Leftrightarrow P = \lambda Q$ ($\lambda \in k^*$)
(deg (P) = deg(Q))

Déf :
1) $P \in k[X]^*$. $P = a_0 + a_1X + \ldots + a_nX^n$
$a_n \neq 0$, $a_i \in k$, $n \geq 0$, n = deg P .
a_n : <u>le coefficient dominant de P</u> .

2) P est <u>unitaire</u> si coefficient dominant est égal à 1 .

$\wp$ = { polynômes irréductibles et unitaires } $\subset$ { polynômes irréductibles }

(p1) Soit S polynôme irréductible . $S \neq 0$, d = deg(S)
$S = s_0 + s_1X + \ldots + s_dX^d$. ($s_i \in k$, $s_d \neq 0$)
$P = s_d^{-1} S$ = polynôme de degré d . ($s_d^{-1} \in k^*$) . Il est unitaire et $S \equiv P$.

P est irréductible car $P \equiv S$ et S irréductible .
$P \in \wp$ et $P \equiv S$.

(p2) $P,Q \in \wp$, $P \equiv Q \Rightarrow P = \lambda Q$ avec $\lambda \in k^*$. (P , Q unitaires)
$d = \deg(P) = \deg(Q)$. Coefficient de X^d : $1 = \lambda\times1$
$\Rightarrow \lambda = 1$.
$\Rightarrow P = Q$.
Cas particuliers :
- $k = \mathbf{C}$, $\wp = \{ X + b \,/\, b \in \mathbf{C} \}$
- $k = \mathbf{R}$, $\wp = \{ X + b \,/\, b \in \mathbf{R} \} \cup \{ X^2 + bX + c \,/\, b^2 - 4ac < 0 , b,c \in \mathbf{R} \}$

Prop : (A principal , $a \in A^* \setminus U(A)$)
a s'écrit sous la forme :

$$a = \varepsilon\, p_1^{\alpha1} p_2^{\alpha2} \ldots p_s^{\alpha s} \quad (*) \text{ , avec } \varepsilon \in U(A)$$

$p_1 , \ldots , p_s \in \wp$, 2 à 2 distincts . $\alpha_1 , \ldots , \alpha_s \in \mathbf{N}^*$.

Lemme : (Propriété de Gauss généralisée)
Soit A anneau principal . $a \in A$, a irréductible .

$a \mid b_1 b_2 \ldots b_n$, ($b_i \in A^*$) ($n \geq 1$)

Alors :

a divise l'un des b_i ($1 \leq i \leq n$) .

Prop : La décomposition de a (*) est unique, c'est-à-dire :
Si $a = \varepsilon' q_1^{\beta 1} \ldots q_t^{\beta t}$ ($\varepsilon' \in U(A)$, $q_1, \ldots, q_t \in \wp$, q_i deux à deux distincts , $\beta_i \in \mathbf{N}^*$, $t \geq 1$) .

Alors :

- $\varepsilon' = \varepsilon$
- $t = s$
- Quitte à changer l'ordre des q_i , on a $q_1 = p_1$ et $\alpha_1 = \beta_1$, … , $q_s = p_s$ et $\alpha_s = \beta_s$.

Théorème : Soit A anneau principal , $\wp$ = ensemble d'éléments irréductibles de A vérifiant (p1) et (p2) .
Alors, tout a de A^* s'écrit d'une manière unique(**) :

$$a = \varepsilon\, p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_s^{\alpha s} \text{ , avec } \varepsilon \in U(A)$$

$$p_1 , \ldots , p_s \in \wp \text{ , 2 à 2 distincts . } \alpha_1 , \ldots , \alpha_s \in \mathbf{N}^*$$

((**) à l'ordre près des $p_i^{\alpha i}$)

Corollaire :
Tout élément a de $\mathbf{Z} \setminus \{0,1,-1\}$ s'écrit d'une manière unique :

$$a = \pm\, p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_s^{\alpha s} \text{ ,}$$

$p_1 , \ldots , p_s$ nombres premiers , 2 à 2 distincts . $\alpha_1 , \ldots , \alpha_s \in \mathbf{N}^*$.

Corollaire : Soit k corps commutatif . Tout polynôme P de k[X] \ k s'écrit d'une manière unique :

$$P = \varepsilon\, p_1^{\alpha 1} p_2^{\alpha 2} \dots p_s^{\alpha s} \quad , \text{avec } \varepsilon \in k^*$$

p_1 , … , p_s polynômes irréductibles , unitaires , 2 à 2 distincts . α_1 , … , $\alpha_s \in \mathbf{N}^*$.

Corollaire : ($\forall$ P $\in$ **C**[X] \ **C**), P s'écrit d'une manière unique sous la forme :

$P = \varepsilon(X - \lambda_1)^{\alpha 1} \dots (X - \lambda_s)^{\alpha s}$ ($\varepsilon \in \mathbf{C}^*$, λ_1 , … , $\lambda_s \in \mathbf{C}$, les λ_i 2 à 2 distincts , $\alpha_i \in \mathbf{N}^*$.

Déf :
λ_1 , … , λ_s : <u>racines</u> de P .
α_1 , … , α_s : <u>ordres de multiplicité</u> de ces racines .

Soit A anneau commutatif intègre . $\wp$ = ensemble d'éléments irréductibles de A vérifiant (p1) et (p2) .

Déf : (Anneau factoriel)
A est <u>un anneau factoriel</u> si tout a de A^* \ U(A) s'écrit de manière unique (**) :

$$a = \varepsilon\, p_1^{\alpha 1} p_2^{\alpha 2} \dots p_s^{\alpha s} \quad , \text{avec } \varepsilon \in U(A) \text{ , s de } \mathbf{N}^*$$

$p_1 , \dots , p_s \in \wp$, 2 à 2 distincts . $\alpha_1 , \dots , \alpha_s \in \mathbf{N}^*$

((**) à l'ordre près des $p_i^{\alpha i}$)

Remarque : Cette définition ne dépend pas du choix de $\wp$.

Théorème : Soit A un anneau :

A principal $\Rightarrow$ A factoriel

14) Anneaux noetheriens :

Soit E un ensemble partiellement ordonné .

Déf :

- On dit que E vérifie la « condition maximale » (C.M.) , si tout sous-ensemble non-vide de E admet au moins un élément maximal.
- On dit que E vérifie la « condition de chaîne ascendante »(C.C.A.), si toute suite strictement croissante d'éléments de E

$x_1 < x_2 < \dots < x_k < x_{k+1} < \dots$

est finie .

Cette condition s'exprime aussi sous la forme :

Toute suite croissante d'éléments de E

$x_1 \leq x_2 \leq \dots \leq x_k \leq x_{k+1} \leq \dots$

est stationnaire .

Prop : Dans un ensemble partiellement ordonné , la condition maximale est équivalente à la condition de chaîne ascendante .

Déf : On dit qu'un anneau unitaire et commutatif est <u>noetherien</u> si l'ensemble de ses idéaux, partiellement ordonné par l'inclusion vérifie la C.C.A.($\Leftrightarrow$ C.M.)

Déf : Dans un anneau A , on dit qu'un idéal est de <u>type fini</u>, s'il est engendré par un nombre fini d'éléments .

Théorème : Un anneau A unitaire , commutatif est noetherien , si et seulement si tout idéal de A est de type fini .

Corollaire : Tout anneau principal est noetherien .

Exples :

- Tout corps commutatif est noetherien
- $\mathbf{Z}$ est principal donc noetherien
- Si k est un corps, l'anneau k[X] des polynômes à une indéterminée est principal, donc k[X] est noetherien.

Prop : A étant un anneau unitaire et commutatif , on a :
A noetherien $\Leftrightarrow$ A / I noetherien, quel que soit I idéal propre de A .

15) Algèbres :

Pour définir une algèbre, il faut connaître la définition d'espace vectoriel : ce qui fait l'objet du résumé de cours suivant .