Résumé 16 : Structures algébriques

I La structure de groupe

§ 1. ***Lois de composition interne.–*** Définition d'une loi, de la commutativité, de l'associativité, de l'élément neutre, du symétrique.

Définition I.1

Un groupe est un ensemble G muni d'un loi de composition interne $*$ vérifiant les propriétés suivantes :

(i) La loi $*$ est associative.

(ii) Elle est munie d'un élément neutre e.

(iii) Tout élément de G admet un symétrique.

Si la loi est commutative, le groupe est dit abélien ou commutatif.

Si $x \in G$, pour tout $n \in \mathbb{N}$, on note $x^0 = e$, $x^n = \underbrace{x * x * \cdots * x}_{n \text{ fois}}$, et $x^{-n} = (x^n)^{-1}$, si bien que pour tous $a, b \in \mathbb{Z}, x^a x^b = x^{a+b}$.

Attention : ceci est la notation multiplicative, i.e que c'est celle pour la loi $\times$ et la loi $\circ$. Pour la loi $+$, les itérés de x se notent plutôt $\{nx, n \in \mathbb{Z}\}$.

Exemples :

- Pour la loi $+$: tous les espaces vectoriels que nous avons vus jusqu'à présent sont des groupes multiplicatifs. Par exemple, $\mathbb{C}, \mathscr{M}_{n,p}(\mathbb{K}), E$, où E est un espace vectoriel , $\mathscr{F}(X, E)$, où X est un ensemble.
- Pour la loi $\times$: $\mathbb{C}^*, Gl_n(\mathbb{K})$.
- Pour la loi $\circ$: pour tout ensemble X, on définit

$$S_X = \{f : X \to X \text{ bijectives }\}.$$

S_X est appelé **groupe de permutations de** X.
En particulier S_n l'ensemble des permutations de $[\![1, n]\!]$.. Profitons-en pour un bref rappel sur S_n, notamment les transpositions, les $p-$cycles, la notation en deux lignes. Décomposition d'un permutation comme produit de cycles à supports disjoints, unicité de cette décomposition et commutativité (les étudiants doivent savoir décomposer une permutation, dixit le programme).

Définition I.2 (*Groupe-Produit*)

Etant donnés deux groupes $(G_1, *)$ et $(G_2, \sharp)$, on définit une loi T sur $G_1 \times G_2$ par

$$(x_1, x_2)T(y_1, y_2) = (x_1 * y_1, x_2 \sharp y_2).$$

Muni de cette loi, $G_1 \times G_2$ est un groupe. Le symétrique de (x_1, x_2) est (x_1^{-1}, x_2^{-1}). Par récurrence, on définit une structure de groupe sur un produit fini de groupes.

Venons-en à la notion de sous-groupe :

Définition I.3 (*sous-groupe*)

Une partie H d'un groupe $(G, *)$ est un sous-groupe de G lorsqu'elle vérifie les propriétés suivantes :

(i) H n'est pas vide.

(ii) H est stable par $*$.

(iii) Muni de $*$, H est un groupe.

Puisque la loi sur H hérite de certaines propriétés de la loi sur G, il est plus aisé de prouver la structure de sous-groupe que celle de groupe :

Proposition I.4

Soit $(G, *)$ un groupe et $H \subset G$. H est un sous-groupe de G si et seulement si

(i) $e \in H$.

(ii) Pour tout $x, y \in G, x * y^{-1} \in H$.

Exemples :

1. Dans $(\mathbb{C}, +)$, il y a $\mathbb{R}, \mathbb{R}[i], \mathbb{Q}, \mathbb{Z}, \ldots$
2. Dans $(\mathbb{C}^*, \times)$, il y a $\mathbb{R}^*, \mathbb{R}_+^*, \mathbb{Q}^*, S^1, U_n, \ldots$.
3. Dans $\big(GL_n(\mathbb{K}), \times\big)$, il y a $Sl_n, \mathscr{O}_n, T_n \cap Gl_n, \ldots$
4. Pour la loi de composition, il y a le sous-groupe alterné, l'ensemble des permutations qui fixent un point,...

Puisque toute intersection de sous-groupes de G est un sous-groupe de G, on peut définir le **Sous-groupe engendré par une partie**A **de** G ainsi : L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G, appelé sous-groupe engendré par A, et noté $< A >$.

Exemples :

(i) $< \{x\} >$, que l'on note plutôt $< x >$, est égal à $\{x^n, n \in \mathbb{Z}\}$.

(ii) S_n est engendré par l'ensemble des permutations, mais aussi par l'ensemble des cycles.

Proposition I.5

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

§ 2. ***Morphismes de groupes.–*** : Définition, image et noyau, isomorphisme, réciproque d'isomorphisme.

Exemples :

> $\exp, \det, z \mapsto z^n, z \mapsto |z|, \sigma \mapsto \varepsilon(\sigma)$. Je vous laisse retrouver les lois et les groupes.

Proposition I.6

- *L'image directe par un morphisme d'un groupe est un groupe.*
- *$f^{-1}(H')$ est un sous-groupe de G. Par exemple, le noyau.*
- *f est injective si et seulement si $\ker f = \{e\}$.*

Définition I.7 (*Groupes monogènes et cycliques*)

Un groupe G est dit monogène s'il est engendré par un de ses éléments, i.e s'il existe $x \in G$ tel que $G =< x >$.
S'il est monogène et de cardinal fini, il est dit cyclique.

Par exemple, $(\mathbb{Z}, +)$ est monogène et pour tout $n \in \mathbb{N}^*, (\mathbb{U}_n, \times)$ est cyclique.

Théorème I.8 (*Classification des groupes monogènes*)

(i) Si $(G, *)$ est monogène de cardinal infini, il est isomorphe à $(\mathbb{Z}, +)$.

(ii) Si $(G, *)$ est monogène de cardinal $n \in \mathbb{N}^*$, il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

(iii) Les groupes monogènes sont abéliens.

§ 3. ***Ordre d'un élément d'un groupe.–*** Définition par le noyau du morphisme de groupes $n \in (\mathbb{Z}, +) \longmapsto x^n \in (G, *)$.

Proposition I.9

Si x est d'ordre fini $d \in \mathbb{N}^*$, alors

(i) l'ordre de x est le cardinal du sous-groupe engendré par x.

(ii) pour tout $n \in \mathbb{Z}$, nous avons $x^n = e \iff d|n$.

Théorème I.10

Si G est de cardinal fini $n \in \mathbb{N}^*$, alors tout élément de G est d'ordre d fini et d divise n. Autrement dit,

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

II Structure d'anneaux

- Un ensemble $\mathscr{A}$ est un anneau s'il est muni de deux lois <u>internes</u> $+$ et $\times$ telles que
  - $(\mathscr{A}, +)$ est un groupe commutatif, dont le neutre est noté $0_{\mathscr{A}}$.
  - $\times$ est une loi associative, admettant un élément neutre $1_{\mathscr{A}}$.
  - $\times$ est distributive par rapport à $+$.

  Si la loi $\times$ est de plus commutative, devinez comment on désigne l'anneau !

  Exemples :

  > Munis des lois $+$ et $\times$ usuelles, les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathscr{M}_n(\mathbb{K}), \mathscr{F}(X, \mathbb{R}), \mathbb{Z}/n\mathbb{Z}$, pour tout entier non nul n et pour tout ensemble X.

  L'anneau commutatif $\mathscr{A}$ est dit $\boxed{\text{intègre}}$ lorsque

  $$\text{pour tous } a, b \in \mathscr{A}, \qquad \text{si } ab = 0, \text{ alors } a = 0 \text{ ou } b = 0.$$

  Par exemple, $\mathbb{K}[X]$ est intègre, mais $\mathscr{M}_n(\mathbb{R})$ ne l'est pas.
  Un élément $a \in \mathscr{A}$ est dit $\boxed{\text{nilpotent}}$ lorsqu'une de ses puissances est nulle.
  Une application $f : \mathscr{A} \longrightarrow \mathscr{A}'$ entre deux anneaux est un $\boxed{\text{morphisme d'anneaux}}$ lorsque pour tous $a, b \in \mathscr{A}$, $\begin{cases} f(a+b) = f(a) + f(b), \\ f(a \times b) = f(a) \times f(b) \\ f(1) = 1 \end{cases}$.

- On note $\mathscr{A}^*$ l'ensemble des inversibles de $\mathscr{A}$. On démontre que c'est un groupe pour la loi $\times$.

  Exemples :

  > 1. $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. De même, pour tout corps, comme $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{Z}/p\mathbb{Z}$ quand p est un nombre premier, l'ensemble des inversible est constitué de tous les éléments non nuls.
  > 2. $(\mathbb{R}[X])^*$ est l'ensemble des polynômes de degré nul.
  > 3. $(\mathbb{Z}/4Z)^* = \left\{\bar{1}, \bar{3}\right\}$ et $(\mathbb{Z}/6Z)^* = \left\{\bar{1}, \bar{5}\right\}$.
  > 4. $z \mapsto \bar{z}$ est un isomorphisme d'anneaux de $\mathbb{C}$, et $a + ib \in \mathbb{R} + i\mathbb{R} \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ est un morphisme d'anneaux entre $\mathbb{C}$ et $\mathscr{M}_2(\mathbb{R})$.

- On appelle $\boxed{\text{corps}}$ tout anneau commutatif dont tout élément non nul est inversible. On le note génériquement $\mathbb{K}$. Les exemples notoires sont $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ lorsque p est premier.

- **Sous-ensembles remarquables :** Soit $\mathscr{B}$ une partie d'un anneau $\mathscr{A}$. On dit

que $\mathscr{B}$ est un $\boxed{\text{sous-anneau}}$ de $\mathscr{A}$ lorsque B contient 1, et que pour tous $a, b \in B, a - b$ et $a \times b$ appartiennent aussi à $\mathscr{B}$.
Par exemple, si $f : \mathscr{A}_1 \to \mathscr{A}_2$ est un morphisme d'anneaux, l'image $f(\mathscr{A}_1)$ est un sous-anneau de $\mathscr{A}_2$. En revanche, ce n'est pas le cas du noyau de f puisque $f(1) = 1 \neq 0$. On a alors une autre structure qui apparait :
une partie $\mathscr{I}$ d'un anneau $\mathscr{A}$ est un $\boxed{\text{idéal}}$ si $(\mathscr{I}, +)$ est un sous-groupe de $\mathscr{A}$ et si pour tous $(a, b) \in \mathscr{A} \times \mathscr{I}$, l'élément $a \times b$ appartient à $\mathscr{I}$.

Exemples :

1. Soit $\mathscr{A}$ un anneau commutatif. Pour tout $a \in \mathscr{A}$, l'ensemble $a\mathscr{A} = \{ab \text{ où } b \in \mathscr{A}\}$ est un idéal de $\mathscr{A}$. On dit que cet idéal est $\boxed{\text{principal}}$. C'est le cas de $\mathbb{Z}$ et de $\mathbb{K}[X]$, lorsque $\mathbb{K}$ est un corps. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$, et ceux de $\mathbb{K}[X]$ sont les $P(X)\mathbb{K}[X]$, où P est un polynôme unitaire.
2. Si 1 appartient à l'idéal $\mathscr{I}$, alors $\mathscr{I} = \mathscr{A}$. Ainsi, les seuls idéaux d'un corps $\mathbb{K}$ sont 0 et $\mathbb{K}$.
3. Comme bien souvent pour les structures algébriques, une intersection d'idéaux de $\mathscr{A}$ est un idéal de $\mathscr{A}$. Ce qui permet de parler d'idéal engendré par une partie de $\mathscr{A}$. Une somme d'idéaux de $\mathscr{A}$ est aussi un idéal de $\mathscr{A}$.

III L'anneau $\mathbb{Z}$

- Pour tous $a, b \in \mathbb{Z}$, on a équivalence entre $a|b$ et $b\mathbb{Z} \subset a\mathbb{Z}$.
- Le fait que tout idéal de $\mathbb{Z}$ soit principal permet de définir le pgcd $a \wedge b$ et le ppcm $a \vee b$ de deux entiers relatifs ainsi :

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z} \text{ et } a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}.$$

Ainsi, $m \in \mathbb{Z}$ est un multiple commun de a et de $b \iff a \vee b$ divise m, et $d \in \mathbb{Z}$ est un diviseur commun à a et $b \iff d$ divise $a \wedge b$.
Avec cette définition, le théorème de Bezout est une paraphrase :

$$\forall a, b \in \mathbb{Z}^*, \qquad a \wedge b = 1 \iff \exists n, m \in \mathbb{Z} \text{ tels que } an + bm = 1.$$

Notons le lien avec la décomposition en produit de nombres premiers :
Si $a = \prod_{k=1}^{m} p_k^{a_k}$ et $b = \prod_{k=1}^{m} p_k^{b_k}$, où $p_1 < p_2 < \cdots < p_m$ sont des nombres premiers et où les a_k et les b_k sont des entiers naturels (dont certains peuvent être nuls), alors

$$\boxed{a \wedge b = \prod_{k=1}^{m} p_k^{\min(a_k, b_k)} \text{ et } a \vee b = \prod_{k=1}^{m} p_k^{\max(a_k, b_k)}}.$$

IV L'anneau $\mathbb{Z}/n\mathbb{Z}$

- On note pour tout $k \in \mathbb{Z}$, $\bar{k}$ l'ensemble des entiers relatifs congrus à k modulo n, i.e $\bar{k} = k + n\mathbb{Z}$. Ainsi, $\bar{k} = \bar{\ell} \iff n$ divise $k - \ell$. On note

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{k} \text{ où } k \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \ldots \overline{n-1}\}.$$

Le fait que la congruence soit compatible avec les lois $+$ et $\times$ permet de définir deux lois internes $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ de la manière la plus naturelle qui soit, à savoir

$$\text{pour tous } a, b \in \mathbb{Z}, k \in \mathbb{N}, \boxed{\bar{a} + \bar{b} = \overline{a + b}} \text{ et } \boxed{\bar{a} \times \bar{b} = \overline{a \times b}}.$$

On montre alors que $\mathbb{Z}/nZ$ est un anneau commutatif muni de ces deux lois.

- Les **inversibles** de $\mathbb{Z}/n\mathbb{Z}$ sont alors les éléments $\bar{k}$ où $k \in \mathbb{Z}$ et $k \wedge n = 1$.
On note $\varphi(n)$ le cardinal du groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$:

$$\varphi(n) = \text{ Card } \{k \in [\![1, n-1]\!] \text{ tels que } k \wedge n = 1\}.$$

φ s'appelle l'indicatrice d'Euler.

- **Théorème IV.1 (*chinois*)**

Si m et n sont premiers entre eux, alors

$$\Psi : \bar{x} \in \mathbb{Z}/nm\mathbb{Z} \longmapsto (\bar{x}, \bar{x}) \in \mathbb{Z}/nZ \times \mathbb{Z}/m\mathbb{Z}$$

est bien définie et est un isomorphisme d'anneaux.

Proposition IV.2

(i) *Si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*
(ii) *Si p est premier, $\varphi(p) = p - 1$.*
(iii) *Si p est premier et si $\alpha \in \mathbb{N}^*$, alors $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*
(iv) *Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ est la décomposition en produit de nombres premiers de n, alors*

$$\varphi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Théorème IV.3 (*$\mathbb{Z}/pZ$ est un corps*)

Soit $n \geqslant 2$. Alors on a l'équivalence entre

$$\mathbb{Z}/n\mathbb{Z} \text{ est intègre} \iff \mathbb{Z}/n\mathbb{Z} \text{ est un corps} \iff n \text{ est un nombre premier.}$$

Finissons par deux illustres théorèmes qui facilitent les calculs de ceratines congruences. notons que le premier est une conséquence du deuxième.

Théorème IV.4

- **de Fermat (le petit) :** *Pour tous $x \in \mathbb{Z}, p \geqslant 2$,*

$$\text{Si } \begin{cases} p \text{ est un nombre premier, et} \\ x \wedge p = 1 \end{cases} \quad \text{alors } \bar{x}^{p-1} = \bar{1} \text{ dans } \mathbb{Z}/p\mathbb{Z}.$$

- **d'Euler :** *Soit n un entier $\geqslant 2$ et a un entier premier avec n. Alors,*

$$\bar{a}^{\varphi(n)} = \bar{1} \qquad \text{dans } \mathbb{Z}/n\mathbb{Z},.$$

V L'anneau $\mathbb{K}[X]$

§ 1. ***PGCD et PPCM.***— $\mathbb{K}$ est un sous-corps de $\mathbb{C}$. $\mathbb{K}[X]$ est un anneau commutatif intégre, on peut donc y faire de l'arithmétique. Les inversibles sont les polynômes constants non nuls. Ces polynômes divisent tous les autres polynômes et ce sont les seuls à avoir cette propriété.

Proposition V.1

Tous les idéaux de $\mathbb{K}[X]$ sont principaux.

Définition V.2

Soient $A, B \in \mathbb{K}[X]$ non nuls. Le PGCD de A et B est l'unique polynôme unitaire P de $\mathbb{K}[X]$ tel que $(A) + (B) = (P)$.
Le PPCM est l'unique polynôme unitaire P de $\mathbb{K}[X]$ tel que $(A) \cap (B) = (P)$
Extension au cas d'une famille finie.

Remarques :

- **Caractérisation du PGCD** : un polynome D est le PGCD de A et $B \iff$
  (i) D est unitaire.
  (ii) $D|A$ et $D|B$.
  (iii) Pour tout polynome R, si $R|A$ et $R|B$ alors $R|D$.
- **Caractérisation du PPPCM** : un polynome M est le PPCM de A et $B \iff$
  (i) M est unitaire.
  (ii) $A|M$ et $B|M$.
  (iii) Pour tout polynome R, si $A|R$ et $B|R$ alors $M|R$.

Proposition V.3 (*Relation de Bézout*)

Si $A_1, \ldots A_n \in \mathbb{K}[X]$ sont premiers dans leur ensemble, i.e s'ils n'admettent aucun diviseur commun de degré $\geqslant 1$, alors il existe des polynômes $P_1, \ldots P_n \in \mathbb{K}[X]$ tels que $\sum_{i=1}^{n} P_i A_i = 1$.

Proposition V.4 (*lemme de Gauss*)

Si D divise AB et si $D \wedge A = 1$, alors D divise B.

Penser à ces deux théorèmes lorsque vous vous retrouvez face à des polynômes premiers entre eux.

L'algorithme d'Euclide étendu est également au programme.

§ 2. ***Polynômes irréductibles de*** $\mathbb{K}[X]$.— Un polynôme est dit irréductible dans $\mathbb{K}[X]$ lorsque $\deg P \geqslant 1$ et que ses seuls diviseurs sont les polynomes de degré 0 et les λP, où $\lambda_i n \mathbb{K}^*$.

Théorème V.5

Soit $P \in \mathbb{K}[X]$ de degré $\geqslant 1$. Il existe $\lambda \in \mathbb{K}^*$ et un $k$uplet $(P_1, \ldots, P_k)$ de polynômes irréductibles deux à deux distincts, ainsi que $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ tels que $P = \lambda P_1^{n_1} \ldots P_k^{n_k}$.
λ est le coefficient dominant de P et il y a unicité, à l'ordre près des facteurs, d'une telle décomposition.

Il faut connaitre la description des irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$.

VI $\mathbb{K}-$Algèbres

Dans cette section, $\mathbb{K}$ désigne un corps commutatif.

Définition VI.1

On appelle $\mathbb{K}-$algèbre tout quadruplet $(A, +, \times, .)$ tel que :

(i) $(A, +, .)$ *est un* $\mathbb{K}-$ *espace vectoriel .*

(ii) $(A, +, \times)$ *est un anneau.*

(iii) $\forall \lambda \in \mathbb{K}, \forall (a, b) \in A^2, (\lambda.a) \times b = a \times (\lambda.b) = \lambda.(a \times b)$.

Une $\mathbb{K}$algèbre est dite de dimension finie lorsque le $\mathbb{K}-$ espace vectoriel sous-jacent l'est. Elle est dite commutative, ou intègre, lorsque l'anneau sous-jacent l'est.

Exemples :

$\mathbb{K}[X], \mathscr{L}(E), \mathscr{F}(X, \mathbb{K}), \mathscr{M}_n(\mathbb{K})$.