Chapitre 16
Compléments d'algèbre et d'arithmétique

1. Groupes : compléments

1.1. Sous-groupe engendré par une partie A

a) Définition

Définition 5 : sous-groupe engendré

Soit $(G,*)$ un groupe et A une partie de G.

On appelle sous-groupe engendré par A le plus petit (au sens de l'inclusion) sous-groupe de G contenant A. On le note souvent $Gr(A)$.

- On peut montrer que $Gr(A)$. existe bien : c'est tout simplement l'intersection de tous les sous-groupes de G contenant A (exercice).
- Remarque : la définition est similaire pour $Vect(A)$, sous-espace vectoriel d'un espace vectoriel E.

Propriété : Si H est un sous-groupe de G tel que $H \supset A$, alors $H \supset Gr(A)$.

- Démonstration **1**.

b) Exemples :

- Dans un groupe $(G,*)$ de neutre e : $Gr(\varnothing) = \{e\}$, $Gr(G) = G$
- Dans un groupe $(G,.)$ le sous-groupe engengré par a est le sous-groupe des puissances de a : $\boxed{Gr(a) = \{a^k \ ; k \in \mathbb{Z}\}}$ **2**.
  - Attention : en notation additive – i.e. dans un groupe $G,+$ -, $\boxed{Gr(a) = \{ka \ ; k \in \mathbb{Z}\}}$
  - Dans $(\mathbb{Z},+)$: $\boxed{Gr(n) = \{kn \ ; k \in \mathbb{Z}\} = n\mathbb{Z}}$
  - Dans $(\mathbb{R},+)$: $\boxed{Gr(\alpha) = \{k\alpha \ ; k \in \mathbb{Z}\} = \alpha\mathbb{Z}}$
- Dans $(\mathbb{R},+)$: ▪ $Gr(1) = \mathbb{Z}$
  ▪ $Gr(1,\sqrt{2}) = \{a + b\sqrt{2} \ ; \quad a,b \ \in \mathbb{Z}^2\} = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ (ex .)
- Dans $(\mathbb{C},+)$: $\boxed{Gr(1,i) = \{a + bi \ ; \quad a,b \ \in \mathbb{Z}^2\} = \mathbb{Z} + i\mathbb{Z}}$ est appelé le groupe des **entiers de Gauss**.
- $\mathfrak{S}_n$ est « engendré par les transpositions, ce qui signifie qu'en notant $\mathcal{T}$ l'ensemble des transpositions de $\mathfrak{S}, n$¨, alors $Gr(\mathcal{T}) = \mathfrak{S}_n$.

1.2. Le groupe $\mathbb{Z}/n\mathbb{Z}$

a) Rappel : relation d'équivalence, classes d'équivalence

- Relation d'équivalence : réflexive $\forall x \in E,\ x\mathcal{R}x$

  symétrique $\forall (x,y) \in E^2,\ [x\mathcal{R}y] \Rightarrow [y\mathcal{R}x]$

  transitive $\forall (x,y,z] \in E^3,\ [x\mathcal{R}y \text{ et } y\mathcal{R}z] \Rightarrow\ [x\mathcal{R}z]$
- Classe d'équivalence de x : $Cl(a) = \{x \in E \,/\, x\mathcal{R}a\}$
- Exemple : la relation de congruence modulo n ($n \in \mathbb{N}^*$)

  $[a \equiv b[n]] \Leftrightarrow [\exists k \in \mathbb{Z} \,/\, a = b + kn]$
  - La classe d'un élément a modulo n sera notée $\bar{a}$ ou $\bar{a}^{[n]}$ en cas d'ambiguïté
  - $\forall a \in \mathbb{Z},\ \exists r \in [\![\, 0, n-1 \,]\!] \,/\ \ a \equiv r\ [n]$ **3**.
  - Exemple dans $\mathbb{Z}/3\mathbb{Z}$: $\overline{2017} = \bar{1}$, $\overline{1998} = \bar{0}$

b) Structure de groupe

Définition 1 : **l'ensemble $\mathbb{Z}/n\mathbb{Z}$ et l'addition dans cet ensemble**

- On définit $\mathbb{Z}/n\mathbb{Z}$ comme l'ensemble des classes d'équivalence de la relation de congruence modulo n dans $\mathbb{Z}$ (où $n \in \mathbb{N}^*$) .
- Ainsi $\boxed{\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}}$
- On définit sur $\mathbb{Z}/n\mathbb{Z}$ une addition notée $+$ par :

$$\forall (\bar{x}, \bar{y}) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^2,\ \bar{x} + \bar{y} = \overline{x+y}$$

- Justification : $+$ est bien définie. **4**. **CCP oral...**

Théorème 1 : $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

- Démonstration **5**.

- Exemple : table de groupe de $\mathbb{Z}/6\mathbb{Z}$ et détermination des éléments générateurs **6**.

c) Eléments générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$

Définition : un élément a d'un groupe G est dit **générateur** si $Gr(a) = G$

- Exemple : dans $\mathbb{Z}/12\mathbb{Z}$, détermination de $Gr(\bar{7})$ **7**.

Théorème 2 : **éléments générateurs de $\mathbb{Z}/n\mathbb{Z}$**

Soit $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$.

$[\overline{m}$ est générateur de $\mathbb{Z}/n\mathbb{Z}] \Leftrightarrow [m \wedge n = 1]$

- Démonstration **8**.

1.3. Ordre d'un élément dans un groupe

a) Etude de $Gr(a)$ **9** ↙.

b) Théorème fondamental et définition

Théorème : Pour tout élément a d'un groupe $(G,.)$:

- ou bien $Gr(a)$ est infini :
  - $Gr(a) = \{..., a^{-2}, a^{-1}, e, a, a^2, ...\}$ est alors isomorphe à $(\mathbb{Z}, +)$
  - on dit que a est d'ordre infini
  - $\forall k \in \mathbb{Z} \ : [a^k = e] \Leftrightarrow [k = 0]$
- ou bien $Gr(a)$ est fini, de cardinal n :
  - $Gr(a) = \{e, a, a^2, ..., a^{n-1}\}$ est alors isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$
  - on dit que a est d'ordre n
  - $\forall k \in \mathbb{Z} \ : [a^k = e] \Leftrightarrow [k \in n\mathbb{Z}]$

Ainsi, l'**ordre** d'un élément dans un groupe fini est :

- le plus petit entier naturel n tel que $a^n = e$
- le cardinal de $Gr(a)$

c) Théorème de Lagrange

Théorème : Soit H sous-groupe d'un groupe fini G : $\text{card}(H) \mid \text{card}(G)$

Corollaire :
l'ordre d'un élément dans un groupe fini divise le cardinal de ce groupe.

- Démonstration dans le cas d'un groupe commutatif **10**.
- Exercice : ordre de $\overline{26}$ dans $\mathbb{Z}/58\mathbb{Z}$? **11**.

1.4. Groupe monogène, groupe cyclique

a) Définition

Un groupe G est dit **monogène** s'il est engendré par un seul élément a.
Il est dit **cyclique** si de plus il est de cardinal fini.

- Exemples : $\mathbb{Z}/n\mathbb{Z} = Gr(\bar{1})$ est cyclique de cardinal n, $\mathbb{Z} = Gr(1)$ est monogène.

b) Isomorphismes fondamentaux

- La relecture du théorème 2.4.2 s'écrit :

Théorème : Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.
Tout groupe cyclique est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

- Conséquence : les éléments générateurs d'un groupe cyclique $Gr(a)$ de cardinal n sont les éléments a^k pour lesquels $k \wedge n = 1$.

c) Exemples :

- Groupe U_n des racines n-ièmes de l'unité **12**.
- En géométrie : groupe de frises ; groupe engendré par une rotation **13**.

2. L'anneau $\mathbb{Z}/n\mathbb{Z}$

2.1. Rappels sur les congruences

Propriétés : **propriétés des congruences**

1. Soient $n \in \mathbb{N}^*$, $k \in \mathbb{N}$ et $(a,b,c,d) \in \mathbb{Z}^4$ tel que $a \equiv b\ [n]$ et $c \equiv d\ [n]$.
   Alors : $a+c \equiv b+d\ [n]$, $ac \equiv bd\ [n]$ et $a^k \equiv b^k\ [n]$
2. Soient $n \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$ tels que $m \wedge n = 1$.
   Soit $(a,b) \in \mathbb{Z}^2$ tel que $a \equiv b\ [n]$ et $a \equiv b\ [m]$.
   Alors : $a \equiv b\ [mn]$

- On dit que la congruence est compatible avec les lois $+$ et $\times$.
- Exemple : 6006 est-il divisible par 66 ? **14**.

2.2. Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

Définition : **multiplication dans $\mathbb{Z}/n\mathbb{Z}$**

On définit sur $\mathbb{Z}/n\mathbb{Z}$ une multiplication notée $\times$ par :

$$\forall (\overline{x},\overline{y}) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^2,\ \overline{x} \times \overline{y} = \overline{x \times y}$$

- Justification : $\times$ est bien définie. **15**.

Théorème : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

- Démonstration **16**.

- Exemple : calculs dans $\mathbb{Z}/12\mathbb{Z}$, éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ **17**.

2.3. Eléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$

a) Le théorème fondamental

Théorème : **éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$**

Soit $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Alors

$[\overline{m}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}] \Leftrightarrow [m \wedge n = 1]$

- Démonstration **18**.

- Il est remarquable que ce sont exactement les éléments générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Rechercher à ce sujet l'argument essentiel de ce fait.
- Exemple : éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ **19**.

b) Cas où $p \in \mathbb{P}$

Théorème : Soit $p \in \mathbb{N}^*$ avec $p \geqslant 2$. Alors :

$[\mathbb{Z}/p\mathbb{Z}$ est un corps$] \Leftrightarrow [p \in \mathbb{P}]$

- Démonstration **20**.

- Exemple : résolution de $x^2 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$, dans $\mathbb{Z}/12\mathbb{Z}$.

2.4. Théorème chinois

- Rappelons que $\overline{a}^{[n]}$ désigne la classe de a modulo n.

Théorème chinois : Isomorphisme entre $\mathbb{Z}/(mn)\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Soient m et n deux entiers naturels tels que $m \wedge n = 1$.

L'application $\Phi : \mathbb{Z}/(mn)\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ définie par $\Phi(\overline{a}^{[mn]}) = (\overline{a}^{[m]}, \overline{a}^{[n]})$ est un isomorphisme d'anneaux.

Corollaire : Soient m et n deux entiers naturels tels que $m \wedge n = 1$.

Le système d'équations $\begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases}$ $(x \in \mathbb{Z})$ admet une unique solution $x_0 \in [\![0 ; mn - 1]\!]$ et pour ensemble solution $\{x \in \mathbb{Z} / \ x \equiv x_0 \ [mn]\}$

- Démonstrations **21**.
- Conséquence : pour résoudre un tel système,
  - On cherche une solution particulière x_0 (il y en a une $< mn$!)
  - On a alors $\boxed{\begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases} \Leftrightarrow x \equiv x_0 \ [mn]}$
- Exemple : Mars et Jupiter… conjonction de planètes

  Recherche de l'année de naissance de Jésus-Christ.

2.5. Fonction indicatrice d'Euler

Définition : **Fonction indicatrice d'Euler**

On appelle fonction indicatrice d'Euler la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ définie par

$$\varphi(n) = card(\{k \in [\![0, n-1]\!] / \ k \wedge n = 1\})$$

- Ainsi $\varphi(1) = 1$ et si $n \geqslant 2$, $\varphi(n)$ est donc
  - le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
  - mais aussi le nombre d'éléments générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
- Exemples : $\varphi(2) = 1$, $\varphi(7) = 6$, $\varphi(12) = 4$

Propriétés : 1. $\forall (m,n) \in \mathbb{N}^{*2} : [m \wedge n = 1] \Rightarrow [\varphi(m \times n) = \varphi(m) \times \varphi(n)]$

2. $\forall p \in \mathbb{P}, \ \forall \alpha \in \mathbb{N}^* : \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Théorème : expression de $\varphi(n)$

Si $n \geqslant 2$ admet pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$,

alors $\varphi(n) = \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$ soit $\boxed{\varphi(n) = n \times \prod_{i=1}^{r} (1 - \frac{1}{p_i})}$

- Démonstrations **22**.
- Exemples : $\varphi(12) = 4$, $\varphi(666) = 216$.

2.6. Théorème d'Euler et petit théorème de Fermat

Théorème d'Euler

Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z} / a \wedge n = 1$. Alors $\boxed{a^{\varphi(n)} \equiv 1\,[n]}$

- Conséquence 1 :

Petit théorème de Fermat

Soient $p \in \mathbb{P}$ et a un entier non multiple de p : $\boxed{a^{p-1} \equiv 1\,[p]}$

- Conséquence 2 : codage R.S.A.
- Démonstrations **23**.

Remarque : nombres de Carmichaël (ex. $561 = 3 \times 11 \times 17$)

$$\exists n \in \mathbb{N} / \ \forall n \in \mathbb{Z} / a \wedge n = 1 : a^{n-1} \equiv 1\,[n]$$

3. Anneaux et idéaux

3.1. Relation de divisibilité dans un anneau A

Définition 3 : **diviseur**

Soient a et b deux éléments d'un anneau commutatif $(A,+,\times)$.

On dit que a divise b ou que b est un multiple de a et on écrit $\boxed{a \mid b}$ si

$$\boxed{\exists k \in A / b = k \times a}$$

3.2. Rappels

Définition 3 : **idéal d'un anneau commutatif**

On dit que $\mathcal{I}$ est un idéal de l'anneau commutatif $(A,+,\times)$ si

- $(\mathcal{I},+)$ est un sous-groupe du groupe $(A,+)$
- $\forall a \in A,\ \forall x \in \mathcal{I}$: $a \times x \in \mathcal{I}$ (surstabilité)

3.3. Exemples :

- Exemple 1 : l'idéal bA des multiples d'un élément b de A, noté (b)
- Exemple 2 (rappel) le noyau d'un morphisme d'anneaux est un idéal

3.4. Divisibilité et idéaux

Propriété : Soient a et b deux éléments d'un anneau commutatif $(A,+,\times)$.

Alors $\boxed{[a \mid b] \Leftrightarrow [(b) \subset (a)]}$

- Démonstrations **24**.

3.5. Intersection et somme d'idéaux

Propriété : Si $\mathcal{I}$ et $\mathcal{J}$ sont des idéaux d'un anneau commutatif $(A,+,\times)$, alors $\mathcal{I} \cap \mathcal{J}$ et $\mathcal{I} + \mathcal{J} = \{a+b\,;(a,b) \in \mathcal{I} \times \mathcal{J}\}$ sont des idéaux de A.

- Démonstrations **25**.

3.6. Conséquence 1 : arithmétique dans $\mathbb{Z}$

a) Idéaux de $\mathbb{Z}$ (rappel) : les seuls idéaux de $\mathbb{Z}$ sont du type $n\mathbb{Z}$

b) Si $m = a \vee b$, alors $\boxed{a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}}$, si $d = a \wedge b$, alors $\boxed{a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}}$

c) Conséquence : théorème de Bezout, théorème de Gauss (réviser)

d) Savoir faire : algorithme de recherche des coefficients de Bezout **26**.

3.7. Conséquence 2 : arithmétique dans $\mathbb{K}[X]$

a) Idéaux de $\mathbb{K}[X]$ (rappel) :

Les idéaux de $\mathbb{K}[X]$ sont tous du type $(P) = \{P \times Q\,,\, Q \in \mathbb{K}[X]\}$.

- Si $P \neq 0$, P peut être choisi unitaire.

b) P.G.C.D. de deux polynômes

Définition : Soient A et B deux polynômes dont l'un au moins n'est pas nul.
Le P.G.C.D. de A et B, noté $A \wedge B$, est l'unique polynôme D unitaire tel que $(A) + (B) = (D)$.

- Justification **27**.
- Conséquences : **28**.
  - Si $A \wedge B = D$, il existe $(U,V) \in \mathbb{K}[X]^2$ tel que $AU + BV = D$
  - Les diviseurs communs de A et B sont les diviseurs de D .
  - D est un diviseur commun de A et B de degré maximal.

c) **Théorème de Bezout :** Soient A et B deux polynômes,

$\boxed{[A \wedge B = 1] \Leftrightarrow [\exists (U,V) \in \mathbb{K}[X]^2 \,/\, AU + BV = 1]}$ Démo. **29**.

- Savoir faire : algorithme d'Euclide (calcul de $A \wedge B$ et de U et V).

d) **Théorème de Gauss :** Soient A et B deux polynômes

$\boxed{\text{Si } A \,|\, (BC) \text{ et si } A \wedge B = 1 \text{ alors } A \,|\, C}$ Démo. **30**.

e) Polynômes irréductibles de $\mathbb{K}[X]$

Définition : **polynôme irréductible** de $\mathbb{K}[X]$
Un polynôme P est dit irréductible s'il n'est pas constant et s'il n'admet pas de diviseurs autres que k et kP $(k \in \mathbb{K}^*)$.

- Ainsi :

$\boxed{P \text{ irréductible } \Leftrightarrow \text{ les seuls polynômes unitaires qui divisent } P \text{ sont } 1 \text{ et } P}$

- Exemple : tout polynôme de degré 1 est irréductible
- Conséquence : pour un polynôme P non constant :

$$\boxed{[P \text{ non irréductible}] \Leftrightarrow \exists (A,B) \in K[X]^2 \,/\, \begin{cases} P = A \times B \\ 0 < d^\circ(A) \leqslant d^\circ(B) < d^\circ(P) \end{cases}}$$

- Remarque : propriété similaire à : pour un entier naturel $n \geqslant 2$

$$\boxed{[n \text{ non premier}] \Leftrightarrow [\exists (a,b) \in \mathbb{Z}^2 \,/\, n = a \times b \text{ et } 1 < a \leqslant b < n]}$$

f) **Théorème de décomposition en polynômes irréductibles**

Tout polynôme $P \in K[X]$ non constant s'écrit de manière unique, à l'ordre près

$$\boxed{P = \lambda . \prod_{i=1}^{r} P_i^{\alpha_i}} \qquad \text{où}$$

- $\lambda \in K^*$, $r \in \mathbb{N}^*$, $(\alpha_1, \alpha_2, ... \alpha_r) \in (\mathbb{N}^*)^r$
- $(P_1, P_2, ... P_r)$ est un r-uplet de polynômes irréductibles tous distincts.

- Démonstration vue en M.P.S.I. (récurrence forte)
- Définition : P est dit **scindé** si tous les polynômes P_i sont de degré 1

g) Polynômes irréductibles de $\mathbb{C}[X]$ (rappel M.P.S.I.)

Théorème de D'Alembert (trois versions équivalentes)

- Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$
- Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1
- Tout polynôme de $\mathbb{C}[X]$ est scindé.

h) Polynômes irréductibles de $\mathbb{R}[X]$ (rappel M.P.S.I.)

Les seuls polynômes irréductibles de $\mathbb{R}[X]$ sont :

- les polynômes de degré 1
- les polynômes de degré 2 à discriminant strictement négatif

- Exemple : décomposition de $X^n - 1$ dans $\mathbb{C}[X]$ (resp. $\mathbb{R}[X]$)