MP 20-21

MEMO ALGEBRE GENERALE

I. STRUCTURES ALGEBRIQUES USUELLES

I.1 Lois de composition interne

Définition 1 Soit E un ensemble non vide.
On appelle loi de composition interne sur E toute application de $E \times E$ dans E.
Pour $(x, y) \in E^2$, au lieu de $f(x, y)$, on note $x * y$, $x + y$ ou $x\,y$ l'image du couple (x, y) par une loi de composition interne.
Quasiment par convention, une loi de composition interne notée $+$, est commutative (et appelée addition).

Dans ce §, E est un ensemble non vide muni d'une loi de composition interne $*$.

Définition 2 On dit que la loi $*$ est associative si elle vérifie

$$\forall (a, b, c) \in E^3,\ a * (b * c) = (a * b) * c$$

On dit que la loi $*$ est commutative si elle vérifie

$$\forall (a, b) \in E^2,\ a * b = b * a$$

On dit que l'élément e de E est neutre pour la loi $*$ si

$$\forall a \in E,\ a * e = e * a = a$$

Il y a unicité de l'élément neutre.
Si la loi $*$ a un élément neutre e, on dit que l'élément a de E est symétrisable, ou inversible, s'il existe un élément a' de E tel que

$$a * a' = a' * a = e$$

Lorsque la loi $*$ est associative le symétrique, ou l'inverse, de tout élément de E est unique.
Une partie A de E est dite stable par la loi $*$ si elle vérifie $A * A \subset A$, c'est-à-dire

$$\forall (a, b) \in A^2,\ a * b \in A$$

Propriété I.1 Si la loi $*$ est associative et a un élément neutre e, et si a et b sont deux éléments symétrisables de E, alors $a * b$ est symétrisable et $(a * b)' = b' * a'$.

Remarque I.1 *Si a est un élément symétrisable, ou inversible, on note souvent a^{-1} son symétrique. Les lois usuelles, telles que $+, \times, \Delta$, ont généralement leurs propres notations et terminologies.*

I.2 Structure de groupe

Définition 3 On appelle groupe la donnée d'un couple $(G, \cdot)$ où G est un ensemble non vide et $\cdot$ une loi de composition interne sur G vérifiant :
- $\cdot$ est associative
- la loi de composition interne $\cdot$ admet un élément neutre dans G
- tout élément de G est symétrisable dans G

Par abus de langage, on dit aussi que G est un groupe.

Le groupe G est dit commutatif (ou abélien) lorsque $\cdot$ est commutative.

Définition 4 Soit $(G, \cdot)$ un groupe.
On appelle sous-groupe de G toute partie non vide H de G stable par la loi $\cdot$ et telle que la loi induite sur H par $\cdot$ munisse H d'une structure de groupe.

Par exemple, G et $\{e\}$ sont des sous-groupes de G (resp. le plus grand et le plus petit pour l'inclusion).

Propriété I.2 Soit $(G,\cdot)$ un groupe et H un sous-groupe de G.
Les deux groupes $(G,\cdot)$ et $(H,\cdot)$ ont le même élément neutre et tout élément de H a le même symétrique dans G et dans H.

Théorème 1 *Caractérisation d'un sous-groupe*
Soit $(G,\cdot)$ un groupe d'élément neutre e (pour tout élément x de G, on note x^{-1} le symétrique de x dans G) et H une partie de G.
Les assertions suivantes sont équivalentes :
- *H est un sous-groupe de G*
- *H est stable par la loi $\cdot$, $e \in H$ et $\forall x \in H,\ x^{-1} \in H$*
- *H est stable par la loi $\cdot$, $H \neq \emptyset$ et $\forall x \in H,\ x^{-1} \in H$*
- *$H \neq \emptyset$ et $\forall x, y \in H,\ x \cdot y^{-1} \in H$*

Remarque I.2 *Pour prouver que $(G,\cdot)$ est un groupe, on peut penser à prouver qu'il s'agit d'un sous-groupe d'un groupe connu.*

I.3 Structures d'anneau et de corps

Définition 5 On appelle anneau la donnée d'un triplet $(\mathbb{A},+,\times)$ où $\mathbb{A}$ est un ensemble non vide et $+$ et $\times$ deux lois de composition interne sur $\mathbb{A}$ vérifiant :
- $(\mathbb{A},+)$ est un groupe commutatif
- $(\mathbb{A},\times)$ est un monoïde dont l'élément neutre, noté 1, est appelé l'élément unité de l'anneau
- la multiplication $\times$ est distributive par rapport à l'addition $+$

Lorsque de plus la multiplication est commutative, l'anneau est dit commutatif.

Dans ce §, $(\mathbb{A},+,\times)$ est un anneau.

Proposition I.1 *Identités remarquables.*
Soient n un entier naturel et a,b,c,d des éléments de $\mathbb{A}$ qui commutent deux à deux.
On a la formule dite du binôme : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k}$. *Notamment, on obtient* $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.
On a aussi $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$ *et ainsi* $a^{2n+1} + b^{2n+1} = (a+b)\sum_{k=0}^{2n} (-1)^k\, a^k b^{2n-k}$.
Notamment, si 1 désigne l'élément unité de $\mathbb{A}$, pour tout élément x de $\mathbb{A}$, on a

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \qquad 1 - x^n = (1-x)\sum_{k=0}^{n-1} x^k$$

Sans oublier l'identité de Lagrange : $(a\,c+b\,d)^2 + (a\,d-b\,c)^2 = \left(a^2+b^2\right)\left(c^2+d^2\right)$ *qui a une interprétation géométrique.*
At last but not least : $a^3+b^3+c^3-3\,a\,b\,c = (a+b+c)\left(a^2+b^2+c^2-a\,b-b\,c-c\,a\right)$.

Définition 6 L'élément a de $\mathbb{A}$ est dit inversible lorsqu'il existe un élément a' de $\mathbb{A}$ vérifiant $a\,a' = a'\,a = 1$.
On note généralement $a' = a^{-1}$.

Proposition I.2 *L'ensemble des éléments inversibles de l'anneau* $(\mathbb{A}, +, \times)$, *noté* $\mathbb{A}^*$ *ou* $U(\mathbb{A})$, *est un groupe multiplicatif d'élément neutre* 1.

Définition 7 On appelle corps la donnée d'un triplet $(\mathbb{K}, +, \times)$ où $\mathbb{K}$ est un ensemble non vide et $+$ et $\times$ deux lois de composition interne sur $\mathbb{K}$ vérifiant :
- $(\mathbb{K}, +, \times)$ est un anneau vérifiant $1 \neq 0$
- $(\mathbb{K} \setminus \{0\}, \times)$ est un groupe commutatif.

On précise parfois que le corps est commutatif. Dans le cadre du programme, un corps est toujours commutatif.

II. GROUPE SYMETRIQUE

Dans ce §, sauf cas particulier, n désigne un entier naturel supérieur ou égal à 2 et $\mathbb{N}_n = [\![1, n]\!]$. L'ensemble des permutations de l'ensemble $\mathbb{N}_n$, noté $\mathcal{S}_n$, est un groupe pour la loi de composition des applications, généralement notée multiplicativement, appelée groupe symétrique d'ordre n : il s'agit d'un groupe d'ordre $n!$.

II.1 Transpositions

Définition 8 Soient $i, j \in [\![1, n]\!], i \neq j$. La permutation τ de $\mathbb{N}_n$ définie par

$$\tau(i) = j, \tau(j) = i \text{ et } \forall k \in E,\ k \neq i,\ k \neq j,\ \tau(k) = k$$

est appelée transposition de support $\{i, j\}$, notée $(i\ j)$.

Remarque II.1 *Les transpositions de $\mathbb{N}_n$ sont des éléments d'ordre 2 de $\mathcal{S}_n$.*

Proposition II.1 *Les transpositions engendrent $\mathcal{S}_n$.*

II.2 Décomposition d'une permutation en produit de cycles à supports disjoints

Définition 9 Soient p appartenant à $[\![2, n]\!]$, $a_1, a_2, \ldots, a_p$ des éléments distincts de $\mathbb{N}_n$. La permutation γ de $\mathbb{N}_n$ définie par

$$\begin{array}{rcl} \gamma(a_1) & = & a_2 \quad \gamma(a_2) = a_3 \quad \ldots \quad \gamma(a_{p-1}) = a_p \quad \gamma(a_p) = a_1 \\ \forall x & \in & E,\ x \notin \{a_1, a_2, \ldots, a_p\} \Longrightarrow \gamma(x) = x \end{array}$$

est appelée un cycle de longueur p ou un p-cycle, et est noté $(a_1\, a_2\, \ldots\, a_p)$.
L'ensemble $\{a_1, a_2, \ldots, a_p\}$ est appelé le support du p-cycle γ.

Propriété II.1 Les p-cycles de $\mathbb{N}_n$ sont des éléments d'ordre p de $\mathcal{S}_n$.

Définition 10 Un cycle γ de longueur n est aussi appelé une permutation circulaire de $\mathbb{N}_n$. Dans ce cas, il existe a appartenant à $\mathbb{N}_n$ tel que l'on ait $\gamma = \left(a\ \gamma(a)\ \cdots\ \gamma^{n-1}(a)\right)$ et $\mathbb{N}_n = \left\{a, \gamma(a), \ldots, \gamma^{n-1}(a)\right\}$.

Remarque II.2 *Si γ est une permutation circulaire de $\mathbb{N}_n$, alors pour tout élément x de $\mathbb{N}_n$, on a $\gamma = \left(x\ \gamma(x)\ \cdots\ \gamma^{n-1}(x)\right)$ ainsi que $\mathbb{N}_n = \left\{x, \gamma(x), \ldots, \gamma^{n-1}(x)\right\}$.*

Propriété II.2 Deux cycles de $\mathbb{N}_n$, de supports disjoints, commutent.

Théorème 2 *Soit $\sigma \in \mathcal{S}_n \setminus \{\mathrm{id}_{\mathbb{N}_n}\}$. Il existe une famille de cycles $(\gamma_1, \ldots, \gamma_r)$, et une seule (à l'ordre près), dont les supports sont deux à deux disjoints, telle que $\sigma = \gamma_1\, \gamma_2\, \ldots\, \gamma_r$.*

Remarque II.3 *Si γ est le p-cycle $(a_1\, a_2\, \ldots\, a_p)$, on peut écrire $\gamma = (a_1\, a_2)\,(a_2\, a_3)\, \ldots\, (a_{p-1}\, a_p)$: le théorème de décomposition en produit de "cycles disjoints" fournit une démonstration de la proposition II.1..*

II.3 Signature d'une permutation

Définition 11 Soit $\sigma \in \mathcal{S}_n$. On appelle inversion de σ tout couple (i,j) d'éléments de $[\![1,n]\!]$ vérifiant $i < j$ et $\sigma(i) > \sigma(j)$: on dit aussi que le couple (i,j) présente une inversion pour la permutation σ.
En notant $I(\sigma)$ le nombre d'inversions de σ, on appelle signature de σ l'élément de $\{-1,+1\}$, noté $\varepsilon(\sigma)$ défini par $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.
Une permutation de signature égale à $+1$ (resp. -1) est dite paire (resp. impaire).

Remarque II.4 $\varepsilon\left(\mathrm{id}_{\mathbb{N}_n}\right) = 1$. *Pour toute transposition* τ *de* $\mathbb{N}_n$, $\varepsilon(\tau) = -1$.

Théorème 3 *L'application* $\begin{array}{ccc} \varepsilon : \mathcal{S}_n & \longrightarrow & \{-1,+1\} \\ \sigma & \longrightarrow & \varepsilon(\sigma) \end{array}$ *est un morphisme de groupes, c'est-à-dire*

$$\boxed{\forall \sigma, \rho \in \mathcal{S}_n,\ \varepsilon(\sigma\,\rho) = \varepsilon(\sigma)\,\varepsilon(\rho)}$$

Définition 12 L'ensemble des permutations paires de $\mathbb{N}_n$ est le noyau de ε. C'est un sous-groupe de $\mathcal{S}_n$ appelé le groupe alterné d'ordre n, noté $\mathcal{A}_n$.
Dans le cas $n \geqslant 2$, l'ordre de $\mathcal{A}_n$ est $\dfrac{n!}{2}$.

III. DENOMBREMENT

Etant donné un entier naturel n, la factorielle de n (ou " n factorielle"), est l'entier naturel, noté $n!$, défini par $0! = 1$ et si n est non nul $n! = n \times (n-1)!$.
Si n est non nul, on a ainsi $n! = 1 \times 2 \times \cdots \times n = \prod_{k=1}^{n} k$.

Proposition III.1 *Soient $(p, n) \in \mathbb{N}^2$ et F, E deux ensembles finis de cardinaux respectifs p et n. Alors E^F est fini et*

$$\operatorname{card}\left(E^F\right) = n^p$$

Il s'agit aussi du nombre de $p-$listes d'éléments de E.

Proposition III.2 *Soient $(p, n) \in \mathbb{N}^2$ et F, E deux ensembles finis de cardinaux respectifs p et n. L'ensemble des injections de F dans E est fini. On note $\mathcal{A}_n^p$ son cardinal et on a*

$$\mathcal{A}_n^p = n\,(n-1)\cdots(n-p+1)$$

$\mathcal{A}_n^p$ est aussi le nombre de $p-$listes d'éléments deux à deux distincts de E.
En particulier pour $p > n$, on a $\mathcal{A}_n^p = 0$.
Lorsque l'on a $p \leqslant n$, ceci s'écrit : $\mathcal{A}_n^p = \dfrac{n!}{(n-p)!}$. □

Définition 13 Avec ces notations, $\mathcal{A}_n^p$ est aussi appelé le nombre d'arrangements (sans répétition) de p éléments parmi n.

Corollaire III.1 *Soient F, E deux ensembles finis de même cardinal n.*
L'ensemble des bijections de F sur E est fini de cardinal égal à $n!$.
Notamment le nombre de permutations de E est égal à $n!$.

Définition 14 Soit n un entier naturel, E un ensemble fini de cardinal n et $p \in \mathbb{N}$. On appelle combinaison sans répétition de p éléments de E toute partie de E de cardinal p.
Avec ces notations, l'ensemble $\mathcal{P}_p(E)$ des combinaisons sans répétition de p éléments de E est fini de cardinal noté C_n^p ou $\left(\begin{array}{c} n \\ p \end{array}\right)$.
L'entier $\left(\begin{array}{c} n \\ p \end{array}\right)$ est appelé coefficient binomial d'indices n et p. Pour $p > n$, on a $\left(\begin{array}{c} n \\ p \end{array}\right) = 0$.
Par convention, lorsque $p < 0$, on pose $\left(\begin{array}{c} n \\ p \end{array}\right) = 0$.

Propriété III.1 *Formule de Pascal.*
On a

$$\forall\,(n,p) \in \mathbb{N}^2,\ \left(\begin{array}{c} n \\ p \end{array}\right) = \left(\begin{array}{c} n-1 \\ p-1 \end{array}\right) + \left(\begin{array}{c} n-1 \\ p \end{array}\right)$$

Proposition III.3 *On a*

$$\forall\,(n,\,p) \in \mathbb{N}^2,\ p \leqslant n \Longrightarrow \left(\begin{array}{c} n \\ p \end{array}\right) = \frac{n!}{p!\,(n-p)!}$$

IV. NOMBRES COMPLEXES

Pour tout réel θ, on pose $e^{i\theta} = \cos\theta + i\sin\theta$. On obtient ainsi les formules d'Euler

$$\forall\theta \in \mathbb{R},\ \cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2\,i}$$

L'utilisation de la formule d'Euler fournit un procédé de linéarisation (ce n'est pas toujours le meilleur). Par exemple : $\forall n \in \mathbb{N},\ \forall\theta \in \mathbb{R}$,

$$\cos^n\theta = \frac{1}{2^n}\left(e^{i\theta} + e^{-i\theta}\right)^n = \frac{1}{2^n}\sum_{k=0}^{n}\left(\begin{array}{c} n \\ k \end{array}\right)\exp\left(i\left(2\,k - n\right)\theta\right) = \frac{1}{2^n}\sum_{k=0}^{n}\left(\begin{array}{c} n \\ k \end{array}\right)\cos\left(\left(2\,k - n\right)\theta\right).$$

On a la formule de Moivre : $\forall n \in \mathbb{N},\ \forall\theta \in \mathbb{R},\ \cos\left(n\,\theta\right) + i\sin\left(n\,\theta\right) = \left(\cos\theta + i\sin\theta\right)^n$, ce qui permet d'exprimer $\cos\left(n\,\theta\right)$ en fonction de $\cos\theta$ (polynômes de Tchebychev de première espèce) et $\sin\left(n\,\theta\right)$ comme le produit de $\sin\theta$ et d'un polynôme de $\cos\theta$ (polynômes de Tchebychev de seconde espèce).

Soit $n \in \mathbb{N}^*$. Les racines n^{mes} de l'unité dans $\mathbb{C}$ sont les nombres $\exp\left(i\,\dfrac{k\,2\,\pi}{n}\right)$, $k \in [\![0, n-1]\!]$.

Ainsi pour tout $(\rho,\theta) \in \mathbb{R}_+^* \times \mathbb{R}$, les solutions dans $\mathbb{C}$ de l'équation $z^n = \rho\,e^{i\theta}$ sont les nombres $\sqrt[n]{\rho}\exp\left(i\left(\theta + \dfrac{k\,2\,\pi}{n}\right)\right)$, $k \in [\![0, n-1]\!]$.

Etant donné z, $z = x + i\,y$, $x, y \in \mathbb{R}$, on pose $\exp\left(z\right) = \exp\left(x + i\,y\right) = e^x\,e^{i\,y}$, que l'on note aussi e^z. On a alors : $\forall z, z' \in \mathbb{C},\ \exp\left(z + z'\right) = \exp\left(z\right)\exp\left(z'\right)$. L'exponentielle ne s'annule pas sur $\mathbb{C}$.

Etant donné $(\rho,\theta) \in \mathbb{R}_+^* \times \mathbb{R}$, l'équation $e^z = a$ admet une infinité de solutions (notées $x + i\,y$, $x, y \in \mathbb{R}$) dans $\mathbb{C}$ données par : $x = \ln\rho \quad y \equiv \theta\,[2\,\pi]$.

Soient $a, b, c \in \mathbb{C}$, $a \neq 0$ et $z_1, z_2 \in \mathbb{C}$. Une condition nécessaire et suffisante pour que z_1 et z_2 soient les racines de l'équation $a\,z^2 + b\,z + c = 0$ est que l'on ait : $z_1 + z_2 = -\dfrac{b}{a} \qquad z_1\,z_2 = \dfrac{c}{a}$.

V. TRIGONOMETRIE

Les fonctions sinus et cosinus, notées respectivement sin et cos, sont définies sur $\mathbb{R}$ à valeurs dans $[-1,+1]$ dérivables, périodiques de période 2π.
Par exemple la relation $e^{i\,x}\ e^{-i\,x}=1$ fournit l'identité remarquable $\cos^2(x)+\sin^2(x)=1$.
La fonction tangente, notée tan, définie sur $\mathbb{R}$ privé des points de la forme $\dfrac{\pi}{2}+k\,\pi,\ k\in\mathbb{Z}$, par $\tan(x)=\dfrac{\sin(x)}{\cos(x)}$, est périodique de période π.
La fonction cotangente, notée cotan, définie sur $\mathbb{R}$ privé des points de la forme $k\,\pi,\ k\in\mathbb{Z}$, par $\operatorname{cotan}(x)=\dfrac{\cos(x)}{\sin(x)}=\dfrac{1}{\tan(x)}$, est périodique de période π.
A partir de la dérivée de la fonction tangente et de cette définition, on obtient la dérivée de la cotangente sur son ensemble de définition, à savoir : $\operatorname{cotan}'(x)=-\dfrac{1}{\sin^2(x)}=-1-\operatorname{cotan}^2(x)$.

V.1 Périodicité et symétrie

Sous réserve d'existence des quantités apparaissant ci-dessous, on a les relations suivantes :

$$\begin{array}{rcl@{\qquad}l@{\qquad}l}
\cos(-x) & = & \cos(x) & \sin(-x)=-\sin(x) & \tan(-x)=-\tan(x)\\
\cos(\pi+x) & = & -\cos(x) & \sin(\pi+x)=-\sin(x) & \tan(\pi+x)=\tan(x)\\
\cos(\pi-x) & = & -\cos(x) & \sin(\pi-x)=\sin(x) & \tan(\pi-x)=-\tan(x)\\
\cos\left(\dfrac{\pi}{2}+x\right) & = & -\sin(x) & \sin\left(\dfrac{\pi}{2}+x\right)=\cos(x) & \tan\left(\dfrac{\pi}{2}+x\right)=-\operatorname{cotan}(x)\\
\cos\left(\dfrac{\pi}{2}-x\right) & = & \sin(x) & \sin\left(\dfrac{\pi}{2}-x\right)=\cos(x) & \tan\left(\dfrac{\pi}{2}-x\right)=\operatorname{cotan}(x)
\end{array}$$

V.2 Formules d'addition

On a les relations suivantes :

$$\begin{array}{rcl@{\qquad}l}
\cos(a+b) & = & \cos(a)\cos(b)-\sin(a)\sin(b) & \cos(a-b)=\cos(a)\cos(b)+\sin(a)\sin(b)\\
\sin(a+b) & = & \sin(a)\cos(b)+\cos(a)\sin(b) & \sin(a-b)=\sin(a)\cos(b)-\cos(a)\sin(b)
\end{array}$$

ainsi que $\tan(a+b)=\dfrac{\tan(a)+\tan(b)}{1-\tan(a)\ \tan(b)}$ (sous réserve d'existence de ces quantités).

V.3 Transformation d'un produit en somme

On a les relations suivantes :

$$\begin{array}{rcl}
\cos(a)\cos(b) & = & \dfrac{1}{2}\left(\cos(a+b)+\cos(a-b)\right)\\
\sin(a)\sin(b) & = & \dfrac{1}{2}\left(\cos(a-b)-\cos(a+b)\right)\\
\sin(a)\cos(b) & = & \dfrac{1}{2}\left(\sin(a+b)+\sin(a-b)\right)
\end{array}$$

V.4 Transformation d'une somme en produit

On a les relations suivantes :

$$\cos(p)+\cos(q) \ = \ 2\cos\left(\frac{p+q}{2}\right)\cos\left(\frac{p-q}{2}\right)$$

$$\begin{aligned}
\cos(p)-\cos(q) &= -2\sin\left(\frac{p+q}{2}\right)\sin\left(\frac{p-q}{2}\right)\\
\sin(p)+\sin(q) &= 2\sin\left(\frac{p+q}{2}\right)\cos\left(\frac{p-q}{2}\right)\\
\sin(p)-\sin(q) &= 2\sin\left(\frac{p-q}{2}\right)\cos\left(\frac{p+q}{2}\right)
\end{aligned}$$

V.5 Lignes trigonométriques de l'angle double

Pour tout réel x, on a les relations suivantes :
$\cos(2x)=\cos^2(x)-\sin^2(x)=2\cos^2(x)-1=1-2\sin^2(x)$
$\sin(2x)=2\sin(x)\cos(x)$
et sous réserve d'existence de ces quantités :

$$\cos(2\,x)=\frac{1-\tan^2(x)}{1+\tan^2(x)} \qquad \sin(2\,x)=\frac{2\,\tan(x)}{1+\tan^2(x)} \qquad \tan(2\,x)=\frac{2\,\tan(x)}{1-\tan^2(x)}$$

V.6 Linéarisation de polynômes trigonométriques

Les relations rappelées précédemment permettent de linéariser des polynômes trigonométriques, c'est-à-dire des expressions de la forme $\cos^m(x)\,\sin^n(x)$, où m et n sont des entiers naturels, afin par exemple d'en obtenir des primitives ou la dérivée.

V.7 Autre transformation

Si a, b et θ sont trois réels, vérifiant $a^2+b^2\neq 0$, on transforme la quantité $a\cos(\theta)+b\sin(\theta)$ en introduisant le réel c défini par $c=\sqrt{a^2+b^2}$. On peut alors définir un réel φ vérifiant $\cos(\varphi)=\dfrac{a}{c}\quad \sin(\varphi)=\dfrac{b}{c}$.
Ainsi on obtient $\quad a\cos(\theta)+b\sin(\theta)=c\,\cos(\theta-\varphi)$.

VI. ARITHMETIQUE DANS $\mathbb{Z}$

C'est le théorème de division euclidienne qui permet de faire de l'arithmétique dans $\mathbb{Z}$.
Théorème : *Division euclidienne dans* $\mathbb{Z}$.
Soit $(a, b) \in \mathbb{Z}\times\mathbb{N}^*$. Il existe un et un seul couple d'entiers relatifs (q, r) vérifiant : $a = b\,q+r,\ 0 \leqslant r < b$.
q (resp. r) est appelé le quotient (resp. le reste) de la division euclidienne de a par b.

Etant donnés $a, b,\ a, b \in \mathbb{Z}$, l'algorithme d'Euclide fournit une démonstration et un procédé constructif du PGCD de a et b, noté $a \wedge b$, ainsi que d'un couple d'entiers relatifs (u, v) tels que $a\,u + b\,v = a \wedge b$.
Le théorème de Bézout permet de caractériser les couples d'entiers premiers entre eux et le théorème de Gauss en est une conséquence.
On définit ensuite le PPCM de a et b, noté $a \vee b$, qui vérifie $(a \wedge b)\,(a \vee b) = |a\,b|$.
De plus tout entier naturel supérieur ou égal à 2 admet une "unique" décomposition en produit de facteurs premiers : on peut l'utiliser pour obtenir une expression du PGCD et du PPCM de deux entiers relatifs.

VII.POLYNOMES

$(\mathbb{K}[X],+,\cdot,\times)$ est une algèbre sur $\mathbb{K}$ de dimension infinie dénombrable dont la suite $(X^n)_{n\in\mathbb{N}}$ est une base appelée la base canonique de $\mathbb{K}[X]$. Tout polynôme P de $\mathbb{K}[X]$ s'écrit de manière unique $P=\sum_{n=0}^{+\infty} a_n X^n$ (les coefficients sont presque tous nuls).

VII.1 Propriétés arithmétiques de $\mathbb{K}[X]$

L'existence d'une division euclidienne dans $\mathbb{K}[X]$ permet ici aussi de faire de l'arithmétique.
Théorème : *Division euclidienne dans* $\mathbb{K}[X]$.
Soient $A,B\in\mathbb{K}[X], B\neq 0$.
Il existe un et un seul couple (Q,R) d'éléments de $\mathbb{K}[X]$ tels que : $A=BQ+R$, $\deg(R)<\deg(B)$.
Cette opération est appelée division euclidienne (ou suivant les puissances décroissantes) de A par B. Q et R s'appellent respectivement le quotient et le reste de la division euclidienne de A par B.

Etant donnés A,B, $A,B\in\mathbb{K}[X]$, l'algorithme d'Euclide fournit une démonstration et un procédé constructif d'un PGCD D de A et B, ainsi que d'un couple de polynômes (U,V) tels que $AU+BV=D$.
Le théorème de Bézout permet de caractériser les couples de polynômes premiers entre eux et le théorème de Gauss en est une conséquence.
On définit ensuite un PPCM M de A et B qui vérifie $MD=AB$.
De plus tout polynôme de $\mathbb{K}[X]$ non constant admet une "unique" décomposition en produit de facteurs irréductibles : on peut l'utiliser pour obtenir une expression d'un PGCD et d'un PPCM de deux polynômes.
Le corps $(\mathbb{C},+,\times)$ étant algèbriquement clos, les polynômes irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1. Les polynômes unitaires irréductibles de $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de la forme X^2+aX+b, avec $a^2-4b<0$. On ne sait pas expliciter tous les polynômes irréductibles de $\mathbb{Q}[X]$.

VII.2 Dérivation et racines

On définit la dérivation (formelle, il s'agit d'algèbre !) des polynômes. On définit de même les dérivations successives et on obtient la formule de Taylor.
Théorème : *Formule de Taylor*
Soient $\mathbb{K}$ un sous-corps de $\mathbb{C}$, $P\in\mathbb{K}[X]$ et $\alpha\in\mathbb{K}$.
On a $P(X)=\sum_{k=0}^{+\infty}\frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$ ou encore $P(X+\alpha)=\sum_{k=0}^{+\infty}\frac{P^{(k)}(\alpha)}{k!}X^k$ (les deux sommes sont finies).

Avec les notations précédentes, la formule de Taylor fournit un procédé de calcul des coordonnées du polynôme $P(X+\alpha)$ dans la base canonique de $\mathbb{K}[X]$.
Par ailleurs, elle fournit la caractérisation de la multiplicité d'une racine d'un polynôme. Ainsi, étant donnés α, $\alpha\in\mathbb{K}$, m, $m\in\mathbb{N}^*$, les assertions suivantes sont équivalentes :
- α est racine de P de multiplicité m
- $P(\alpha)=P'(\alpha)=\cdots=P^{(m-1)}(\alpha)=0 \quad P^{(m)}(\alpha)\neq 0$
- $P(\alpha)=0$ et α est racine de P' de multiplicité $m-1$

Formule de Taylor

Soient $n \in \mathbb{N}$, $\mathbb{K}$ un sous-corps de $\mathbb{C}$, $P \in \mathbb{K}_n[X]$ et $h \in \mathbb{K}$. Alors

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(h)}{k!} (X-h)^k = P(h) + \frac{P'(h)}{1!}(X-h) + \cdots + \frac{P^{(n)}(h)}{n!}(X-h)^n$$

On a de même

$$P(X+h) = \sum_{k=0}^{n} \frac{P^{(k)}(h)}{k!} X^k = P(h) + \frac{P'(h)}{1!} X + \cdots + \frac{P^{(n)}(h)}{n!} X^n$$

On écrit ce qui précède sous la forme

$$\forall P \in \mathbb{K}[X],\ P(X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(h)}{k!}(X-h)^k \qquad P(X+h) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(h)}{k!} X^k$$

Algorithme de Hörner :

Etant donné $(\alpha, P) \in \mathbb{K} \times \mathbb{K}[X]$, l'algorithme de Hörner a pour objet le calcul de $P(\alpha)$. Si on a $P = \sum_{k=0}^{n} a_k X^k$, il s'écrit :

$B := 0;$
$for\ k\ from\ n\ to\ 0\ by\ -1\ do\ B := A[k] + B * alpha : od :$
$B\ ;$

Relations coefficients-racines :

Soit P, $P \in \mathbb{K}[X]$, un polynôme scindé sur $\mathbb{K}$ non constant, de racines $\alpha_1, \alpha_2, \ldots, \alpha_n$ (non nécessairement distinctes).
Ainsi $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = a_n (X-\alpha_1)\ldots(X-\alpha_n)$ avec $a_n \neq 0$.
En développant, on obtient $P = a_n \left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \cdots + (-1)^n \sigma_n\right)$ où l'on pose

$$\forall k \in [\![1,n]\!],\ \sigma_k = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} \alpha_{i_1}\, \alpha_{i_2}\, \ldots\, \alpha_{i_k}$$

et alors $\forall k \in [\![1,n]\!]$, $\boxed{\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}}$.

Les quantités $\sigma_k, 1 \leqslant k \leqslant n$, sont appelées fonctions (polynômes) symétriques élémentaires des racines de P.
Leur importance est due au fait que toute fonction polynôme symétrique des racines du polynôme scindé non constant P est fonction polynôme de $\sigma_1, \sigma_2, \ldots, \sigma_n$ et donc rationnelle des coefficients de P.

Formule d'interpolation de Lagrange

Soient $n \in \mathbb{N}^*$ et $a_1, a_2, \ldots, a_n$ des éléments deux à deux distincts de $\mathbb{K}$.

Les éléments de $\mathbb{K}[X]$ admettant $a_1, a_2, \ldots, a_n$ pour racines sont les multiples dans $\mathbb{K}[X]$ de $\prod_{k=1}^{n}(X-a_k)$.

Soient $b_1, b_2, \ldots, b_n \in \mathbb{K}$. Il existe un et un seul élément L de $\mathbb{K}_{n-1}[X]$ tel que

$$\forall k \in [\![1,n]\!],\ L(a_k) = b_k$$

Ce polynôme L est appelé polynôme d'interpolation de Lagrange.
Les éléments P de $\mathbb{K}[X]$ vérifiant $\forall k \in [\![1,n]\!]$, $P(a_k) = b_k$ sont les polynômes de la forme

$$L + Q \prod_{k=1}^{n}(X-a_k),\ Q \in \mathbb{K}[X]$$

On définit les polynômes d'interpolation de Lagrange "élémentaires" associés à $(a_1, a_2, \ldots, a_n)$ par

$$\forall i \in [\![1, n]\!],\ L_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{X - a_j}{a_i - a_j}$$

caractérisés par les propriétés suivantes

$$\forall (i, j) \in [\![1, n]\!]^2,\ L_i \in \mathbb{K}_{n-1}[X] \text{ et } L_i(a_j) = \delta_{i,j}$$

et alors

$$L = \sum_{i=1}^{n} b_i L_i$$

VIIIFRACTIONS RATIONNELLES

Le principal résultat pratique à connaître sur les fractions rationnelles est le théorème de la décomposition en éléments simples dans $\mathbb{C}(X)$ et dans $\mathbb{R}(X)$.

Théorème : *Décomposition d'une fraction rationnelle en éléments simples dans* $\mathbb{C}(X)$.

Toute fraction rationnelle à coefficients dans $\mathbb{C}$ est égale à la somme de sa partie entière et de ses parties polaires.

Plus précisément, soit $F = \dfrac{P}{Q}$ une fraction rationnelle irréductible à coefficients dans $\mathbb{C}$, avec $\deg(Q) \geqslant 1$. Si la décomposition de Q en produit de facteurs irréductibles unitaires s'écrit $Q = \lambda \prod_{i=1}^{N} (X-a_i)^{m_i}$ avec $\lambda \in \mathbb{C}^*$, $a_1, a_2, \ldots, a_N$ sont des nombres complexes deux à deux distincts et $m_1, m_2, \ldots, m_N$ des entiers naturels non nuls, alors il existe un et un seul polynôme E à coefficients dans $\mathbb{C}$, une et une seule famille $(c_{ij})_{\substack{1\leqslant i\leqslant N \\ 1\leqslant j\leqslant m_i}}$ de nombres complexes tels que $\boxed{F = E + \sum_{i=1}^{N} \left(\sum_{j=1}^{m_i} \frac{c_{ij}}{(X-a_i)^j} \right)}$.

Théorème : *Décomposition d'une fraction rationnelle en éléments simples dans* $\mathbb{R}(X)$.

Soit $F = \dfrac{P}{Q}$ une fraction rationnelle irréductible à coefficients dans $\mathbb{R}$ avec $\deg(Q) \geqslant 1$. La décomposition de Q en produit de facteurs irréductibles (unique à l'ordre près des facteurs) est de la forme

$$Q = \lambda \prod_{i=1}^{p} (X-\alpha_i)^{\mu_i} \prod_{j=1}^{q} (X^2 + 2\,a_j\,X + b_j)^{m_j}$$

où $\alpha_1, \alpha_2, \ldots, \alpha_p$ sont les racines réelles deux à deux distinctes de Q, les trinômes deux à deux distincts $X^2 + 2\,a_j\,X + b_j$, $1 \leqslant j \leqslant q$, sont irréductibles dans $\mathbb{R}[X]$ et $\mu_1, \mu_2, \ldots, \mu_p, m_1, m_2, \ldots, m_q$ sont des entiers naturels non nuls.

Alors il existe $E \in \mathbb{R}[X]$ et des familles de réels $(\lambda_{i\,r})_{\substack{1\leqslant i\leqslant p \\ 1\leqslant r\leqslant \mu_i}}$ $(c_{j\,s}, d_{j\,s})_{\substack{1\leqslant j\leqslant q \\ 1\leqslant s\leqslant m_j}}$ tels que

$$F = E + \sum_{i=1}^{p} \left(\sum_{r=1}^{\mu_i} \frac{\lambda_{i\,r}}{(X-\alpha_i)^r} \right) + \sum_{j=1}^{q} \left(\sum_{s=1}^{m_j} \frac{c_{j\,s}\,X + d_{j\,s}}{(X^2 + 2\,a_j\,X + b_j)^s} \right)$$

et cette décomposition est unique.

La décomposition en éléments simples d'une fraction rationnelle permet de calculer les primitives ou les dérivées successives de la fonction rationnelle associée.

Il ne faut pas hésiter à revoir le cours de première année pour se remettre en mémoire les techniques de calcul de la décomposition en éléments simples. Rappelons notamment :

- E est le quotient de la division euclidienne de P par Q
- valeur du résidu pour un pole simple $c_{i\,1} = \dfrac{P(a_i)}{Q'(a_i)} = \dfrac{P(a_i)}{Q_1(a_i)}$ avec $Q = (X-a_i)\,Q_1$
- penser à un calcul de développement limité pour les parties polaires relatives aux pôles réels au moins doubles
- minimiser les calculs en tenant compte de la (im)parité de F, ou si elle est à coefficients réels
- si $\deg F < -1$ la somme des résidus est nulle
- utiliser des valeurs particulières ou le comportement de la fonction associée au voisinage de $\pm\infty$