Révisions 4.5 : Arithmétique

I — Le B.A.BA

1) Définitions théorèmes :

Liste non exhaustive des éléments du cours à maîtriser :

— Théorème de division euclidienne dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$.
— Définition d'un entier premier. Définition d'un polynôme irréductible dans $\mathbb{K}[X]$.
— Théorème fondamental de l'arithmétique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$.
— Définition d'un PGCD et d'un PPCM en utilisant les idéaux.
— Construction de $\mathbb{Z}/n\mathbb{Z}$: compatibilité de la somme et du produit de classes d'équivalence (**Exo 66**) .
— Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$. Division euclidienne, PGCD, PPCM.
— Relation de Bézout. Théorème de Gauss.
— Polynômes irréductibles de $\mathbb{R}[X]$ puis de $\mathbb{C}[X]$.
— Théorème fondamental de l'analyse de d'Alembert et Gauss.
— L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier (**Exo 66**).
— Idéaux de $(\mathbb{Z}, +\times)$ et de $\mathbb{K}[X], +, \times)$.
— Générateurs de $\mathbb{Z}/n\mathbb{Z}$. Indicatrice d'Euler.
— Théorème des restes chinois. Version groupe et version anneau. L'indicatrice d'Euler est "multiplicative".
— Formule d'Euler. Petit théorème de Fermat (**Exo 86**).
— Formule de Taylor exacte pour les polynômes.
— Racines de polynômes. Caractérisation de l'ordre de multiplicité d'une racine de P.
— Théorème fondamental de l'algèbre (de d'Alembert - Gauss).

II — Méthodes :

- Pour déterminer un PGCD, on peut
  — faire une décomposition en facteurs premiers (ou irréductibles)
  Dans $\mathbb{Z}$ ou $\mathbb{K}[X]$, en écrivant $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ avec les mêmes irréductibles p_i, on obtient :

$$\text{le PGCD } a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \dots p_k^{\min(\alpha_k,\beta_k)} \text{ et le PPCM } a \vee b = p_1^{\max(\alpha_1,\beta_1)} \dots p_k^{\max(\alpha_k,\beta_k)}.$$

  — ou bien appliquer l'algorithme d'Euclide
- Pour résoudre une équation Diophantienne du type $ax + by = c$ dans $\mathbb{Z}^2$, on commence par vérifier la condition nécessaire et suffisante $a \wedge b$ divise c, puis on divise l'équation par $a \wedge b$. On se ramène donc à une équation du type $a'x + b'y = c'$ avec $a' \wedge b' = 1$. On calcule alors u, v tels que $au + bv = 1$ et on pose $x_0 = cu$ et $y_0 = cv$. Alors (x_0, y_0) est une solution particulière. Alors on retranche $ax_0 + b_y 0 = c$ à $ax + by = c$ et on résout $a(x - x_0) = -b(y - y_0)$. Comme a et b sont premiers entre eux, par théorème de Gauss, $a|(y - y_0)$ et $b|(x - x_0)$.
  Penser à faire une réciproque.
- Pour trouver le reste de la division euclidienne de A par B , on peut évaluer l'équation $A = BQ + R$ en les racines de B. Si B admet une racine multiple, on peut dériver l'équation $A = BQ + R$ et l'évaluer en les racines multiples de B.
- Pour décomposer P en facteurs irréductibles dans $\mathbb{R}[X]$, on commence par décomposer P en facteurs irréductibles dans $\mathbb{C}[X]$, puis on apparie les facteurs où les racines complexes sont conjuguées : $(X - \alpha)(X - \overline{\alpha}) = X^2 - 2Re(\alpha) + |\alpha|^2$.

III — Interrogations de cours quotidiennes (lunid-mardi-mercredi) :

Série 1

1. Rappeler la définition d'un PGCD et d'un PPCM en terme d'idéaux.
2. Appliquer l'algorithme d'Euclide pour les polynômes $X^4 - 3X^3 + X2 + 4$ et $X^3 - 3X^2 + 3X - 2$.
3. Citer le théorème de Bézout et le théorème de Gauss.
4. Définir un entier premier. Définir un polynôme irréductible dans $\mathbb{K}[X]$.
5. Citer le théorème fondamental de l'arithmétique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$.
6. Citer la formule d'Euler et le petit théorème de Fermat.

Série 2

1. Rappeler la formule de Taylor exacte pour les polynômes.
2. Rappeler la définition et la caractérisation de l'ordre de multiplicité d'une racine d'un polynôme P.
3. Si $P = \lambda \prod_{k=1}^{n}(X - r_k) = \sum_{k=1}^{n} a_k X^k$. Exprimer les coefficients a_n, a_{n-1} et a_0 en fonction des racines λ et les r_k.
4. Citer le théorème de division euclidienne dans $\mathbb{K}[X]$. Définir le PGCD unitaire et le PPCM unitaire en terme d'idéaux.
5. Citer le théorème de d'Alembert - Gauss.
6. Donner la formule du i-ième polynôme de Lagrange tel que $L_i(a_j) = \delta_i^j$.

Série 3

1. Soient $a_0, \dots a_n$ scalaires 2 à 2 distincts. Soit (L_i) les polynômes de Lagrange associés. Donner la formule de l'unique polynôme $P \in \mathbb{K}_n[X]$ tel que $\forall i \in [0, n], P(a_i) = b_i$.
2. Quel est le reste de la division euclidienne de $A = (X + 1)^n X^n 1$ par $B = X^2 3X + 2$
3. Rappeler la formule du déterminant de Vandermonde (on écrira la matrice correspondante)
4. Quel sont les polynômes caractéristique et minimal de $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$
5. Citer le théorème des restes chinois et donner un exemple d'application.

Interrogations de cours quotidiennes (lundi - mardi - mercredi) CORRIGÉS :

Série 1

1. Rappeler la définition d'un PGCD et d'un PPCM en terme d'idéaux.
   (1) : *$d = a \wedge b$ est l'un des générateurs de l'idéal $(a) + (b) = \{ua + vb,\ u, v \in A\}$.*
   (2) : *$m = a \vee b$ est l'un des générateurs de l'idéal $(a) \cap (b) = \{$multiples communs à a et $b\}$.*
   (3) : *d et m sont uniques à association près ; on les rend uniques dans $\mathbb{Z}$ en imposant $d, m \in \mathbb{N}$. On les rend uniques dans $\mathbb{K}[X]$ en imposant qu'ils soient nuls ou unitaires.*
2. Appliquer l'algorithme d'Euclide pour les polynômes $X^4 - 3X^3 + X2 + 4$ et $X^3 - 3X^2 + 3X - 2$.

$$\begin{aligned} X^4 - 3X^3 + X^2 + 4 &= (X^3 - 3X^2 + 3X - 2)X + (-2X^2 + 2X + 4) \\ X^3 - 3X^2 + 3X - 2 &= (-2X^2 + 2X + 4)\left(\frac{-X}{2} + 1\right) + 3X - 6 \\ (-2X^2 + 2X + 4) &= (3X - 6) \times \left(\frac{-2X}{3} - \frac{2}{3}\right). \end{aligned}$$

   Un pgcd est donc $3X - 6$ (ou $X - 2$).
3. Citer le théorème de Bézout et le théorème de Gauss.
   *a et b sont premiers entre eux $\iff (a \wedge b) = (1) \iff \exists\, (u, v) \in A^2$ tel que $ua + vb = 1$ (*Bézout*).*
   *Si $(a \wedge b) = (1)$ et $a \mid bc$ alors $a \mid c$ (*Gauss*).*
4. Définir un entier premier. Définir un polynôme irréductible dans $\mathbb{K}[X]$.
   p est un entier premier ssi $p \notin \{-1, 1\}$ et les seuls diviseurs positifs de p sont 1 et p.
   Autrement dit, si d divise p, alors $d = \pm 1$ ou bien $d = \pm p$.
   P est un polynôme irréductible ssi P n'est pas constant et les seuls diviseurs positifs de P sont les polynômes constants non nuls et les polynômes associés à P, c'est à dire de la forme λP pour $\lambda \in \mathbb{K}^*$.
   Autrement dit, si D divise P, alors $D = \lambda$ ou bien $D = \lambda P$ pour $\lambda \in \mathbb{K}^*$.
5. Citer le théorème fondamental de l'arithmétique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$.
   Si $n \geqslant 2$ est un entier, il existe une unique famille finie $\{p_i\}_{i\in[1,k]}$ d'entiers premiers et $(r_i)_{i\in[1,k]}$ d'entiers strictement positifs tels que $n = \prod p_i^{r_i}$.
   Autrement dit, tout entier supérieur ou égal à 2 admet une unique décomposition en produit de facteurs premiers.
   Pour les polynômes :
   Si $deg(P) \geqslant 1$ est un polynôme non constant, il existe un scalaire $\lambda \in \mathbb{K}^*$, une unique famille finie $\{P_i\}_{i\in[1,k]}$ de polynômes irréductibles unitaires et $(r_i)_{i\in[1,k]}$ d'entiers strictement positifs tels que $P = \lambda \prod P_i^{r_i}$.
   Autrement dit, tout polynôme non constant admet une unique décomposition en produit de polynômes irréductibles.
   Plus généralement, si A est un anneau principal et $a \in A \setminus \{0\}$. Alors il existe $u \in A^*$, $n \in \mathbb{N}$ et $b_1, \ldots, b_n$ premiers tels que $a = ub_1 \ldots b_n$.
   Une telle décomposition est unique à ordre et association près.
6. Citer la formule d'Euler et le petit théorème de Fermat.
   (4) : *Pour $x \in \mathbb{Z}$ et $x \wedge n = 1$, on a $x^{\varphi(n)} \equiv 1\ [n]$ (*Euler*).*
   (5) : *Pour $x \in \mathbb{Z}$ et n premier, on a $x^n \equiv x \bmod n$ (*Fermat*).*

Série 2

1. Rappeler la formule de Taylor exacte pour les polynômes.
   Pour $P \in \mathbb{K}[X]$ et $z \in \mathbb{K}$, $P(X) = \sum_{n\geqslant 0} \frac{P^{(n)}(z)}{n!}(X - z)^n$.
2. Rappeler la définition et la caractérisation de l'ordre de multiplicité d'une racine d'un polynôme P.
   Soit P polynôme et $z \in \mathbb{K}$. On dit que z est racine de P d'ordre égal à k ssi $(X - z), \ldots, (X - z)^k$ divisent P et $(X - z)^{k+1}$ ne divise pas P.
   Alors z est racine de P d'ordre égal à k ssi $P(z) = P'(z) = \cdots = P^{(k-1)}(z) = 0$ et $P^{(k)}(z) \neq 0$.
3. Si $P = \lambda \prod_{k=1}^{n}(X - r_k) = \sum_{k=1}^{n} a_k X^k$. Exprimer les coefficients a_n, a_{n-1} et a_0 en fonction des racines λ et les r_k.
   $a_n = \lambda$, puis $a_{n-1} = -\lambda \cdot \sum r_k$ et enfin $a_0 = (-1)^n \lambda \cdot \prod r_k$.
4. Citer le théorème de division euclidienne dans $\mathbb{K}[X]$. Définir le PGCD unitaire et le PPCM unitaire en terme d'idéaux.
   (6) : *Pour $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$, B non nul, il existe un unique couple (Q, R) tel que $A = BQ + R$ et $deg(R) < deg(B)$.*
   (7) : *Le PGCD unitaire $D = A \wedge B$ est l'unique générateur unitaire de l'idéal $(A) + (B) = \{UA + VB,\ U, V \in \mathbb{K}[X]\}$.*
   (8) : *LePPCM unitaire $M = A \vee B$ est l'unique générateur unitaire de l'idéal $(A) \cap (B) = \{$multiples communs à A et $B\}$.*

5. Citer le théorème de d'Alembert - Gauss.
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine complexe.
Corollaires importants :
— *tout polynôme non constant de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}$.*
— *les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.*

6. Donner la formule du i-ième polynôme de Lagrange tel que $L_i(a_j) = \delta_i^j$.
$L_i(x) = \prod_{j \neq i} \frac{X - a_j}{a_i - a_j}$.

Série 3

1. Soient $a_0, \dots a_n$ scalaires 2 à 2 distincts. Soit (L_i) les polynômes de Lagrange associés. Donner la formule de l'unique polynôme $P \in \mathbb{K}_n[X]$ tel que $\forall i \in [0, n], P(a_i) = b_i$.
$P = \sum_{i=1}^{n} P(a_i) L_i$.

2. Quel est le reste de la division euclidienne de $A = (X+1)^n X^n 1$ par $B = X^2 3X + 2$
$(X^2 3X + 2) = (X-2)(X-1)$. *On écrit $A = BQ + R$ avec $R = aX + b$. Alors en évaluant en 1 : $2^n - 2 = a + b$ et en évaluant en 2 : $3^n - 2^n - 1 = 2a + b$, donc $a = 3^n - 2^{n+1} + 1$ et $b = -3^n + 2^{n+1} + 2^n - 3$.*

3. Décomposer $(X^2 X + 1)^2 + 1$ dans $\mathbb{R}[X]$.
On factorise dans $\mathbb{C}[X]$: $(X^2 X + 1)^2 + 1 = (X^2 X + 1)^2 i^2 = (X^2 X + 1i)(X^2 X + 1 + i)$.
Alors $(X^2 X + 1)^2 + 1 = (X + i)(X 1i)(X i)(X 1 + i) = (X^2 + 1)(X^2 2X + 2)$.

4. Rappeler la formule du déterminant de Vandermonde (on écrira la matrice correspondante)

$$\begin{vmatrix} 1 & a_1 & a_1^2 \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots \dots & \vdots \\ 1 & a_n & a_n^2 \dots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (a_j - a_i).$$

5. Quel sont les polynômes caractéristique et minimal de $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$

Si $M = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, $\chi_M = X^2 - X + 1 = (X - e^{i\pi/3})(X - e^{-i\pi/3})$. Comme $\mu_M | \chi_M$ et $\mu_M \in \mathbb{R}[X]$, on en déduit que $\mu_M = \chi_M$.

6. Citer le théorème des restes chinois et donner un exemple d'application.
Si n et p sont premiers entre eux, l'application $\phi : \mathbb{Z}/np\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times Z/p\mathbb{Z}$ définie par $\phi(x \bmod np) = (x \bmod n, x \bmod p)$ est un isomorphisme d'anneaux.
Si $nu + pv = 1$, les solutions du système $\begin{cases} x \equiv a[n] \\ x \equiv b[p] \end{cases}$ sont les $x \equiv x_0[np]$ où $x_0 = nub + pva$.
On peut aussi en déduire que si n et p sont premiers entre eux, $\varphi(np) = \varphi(n)\varphi(p)$.

IV — Exercices d'arithmétique et sur les polynômes :

`http://www.bibmath.net/ressources/justeunefeuille.php?id=13441`