Résumé de cours :
Semaine 25, du 31 mars au 4 avril.

Les polynômes (suite et fin)

1 Arithmétique sur un anneau principal (fin)

1.1 Les théorèmes de l'arithmétique

Théorème de *Bézout*. Soit $(a, b) \in A^2$.
a et b sont premiers entre eux si et seulement si : $\exists (u, v) \in A^2 \ \ ua + vb = 1$.

Propriété. Soit $(a, b) \in A^2$. Notons d un PGCD de a et b. Alors
il existe $(a', b') \in A^2$, avec a' et b' premiers entre eux, tel que $a = a'd$ et $b = b'd$.

Théorème de *Gauss*. Soit $(a, b, c) \in A^3$. Si $a|bc$ avec a et b premiers entre eux, alors $a|c$.

Corollaire. Soit $p, a, b \in A$. Si $p \mid ab$ avec p irréductible, alors $p \mid a$ ou $p \mid b$.

Propriété. Soit $(a, b, c) \in A^3$, $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in A$.
On désigne par $a \wedge b$ un PGCD de a et b et par $a \vee b$ un PPCM de a et b.
⋄ Si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.
⋄ Si $a \wedge b = 1$, $\forall (k, l) \in (\mathbb{N}^*)^2 \ \ a^k \wedge b^l = 1$.
⋄ Si $a|b$, $c|b$ et $a \wedge c = 1$ alors $ac|b$.
Si pour tout $i \in \{1, \ldots, n\}$, $a_i|b$ et si $i \neq j \Longrightarrow a_i \wedge a_j = 1$, alors $a_1 \times \cdots \times a_n \mid b$.
⋄ $ab \sim (a \wedge b)(a \vee b)$. En particulier, $a \wedge b = 1 \Longrightarrow a \vee b \sim ab$.
Il faut savoir le démontrer.

1.2 $\mathbb{K}[X]$ est un anneau factoriel

Notation. On suppose ici que $A \in \{\mathbb{Z}, \mathbb{K}[X]\}$ ($\mathbb{K}$ étant un corps quelconque).
Si $A = \mathbb{Z}$, on pose $\mathcal{P} = \mathbb{P}$, et si $A = \mathbb{K}[X]$, $\mathcal{P}$ est l'ensemble des polynômes irréductibles et unitaires.

Théorème. Soit $a \in A$ avec $a \neq 0$. Il existe un unique couple $(u, (\nu_p)_{p \in \mathcal{P}})$, où $u \in U(A)$ et où $(\nu_p)_{p \in \mathcal{P}}$ est une famille presque nulle d'entiers, tel que $a = u \prod_{p \in \mathcal{P}} p^{\nu_p}$: c'est la ***décomposition de** a **en facteurs irréductibles***. ν_p s'appelle la valuation p-adique de a.
Il faut savoir le démontrer.

Propriété. Soit $(a, b) \in (A \setminus \{0\})^2$, dont les décompositions en facteurs irréductibles sont
$a = u \prod_{p \in \mathcal{P}} p^{\nu_p}$ et $b = v \prod_{p \in \mathcal{P}} p^{\mu_p}$. Alors $a \mid b \Longleftrightarrow [\forall p \in \mathcal{P}, \ \ \nu_p \leq \mu_p]$.
De plus, $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)}$ et $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\nu_p, \mu_p)}$. En particulier, a et b sont premiers entre eux si et seulement si aucun élément de $\mathcal{P}$ n'intervient à la fois dans la décomposition en facteurs irréductibles de a et dans celle de b.

Lemme d'Euclide. Soient $(a,b) \in A^2$ avec $b \neq 0$, et q,r tels que $a = bq + r$. Alors $a \wedge b = b \wedge r$.

Algorithme d'Euclide. Soit $(a_0, a_1) \in A^2$.
• Pour $i \geq 1$, tant que $a_i \neq 0$, on note a_{i+1} le reste de la division euclidienne de a_{i-1} par a_i. On définit ainsi une suite finie $(a_i)_{0 \leq i \leq N}$ d'éléments de A telle que $a_N = 0$ et, pour tout $i \in \{0, \ldots, N-1\}$, $a_0 \wedge a_1 = a_i \wedge a_{i+1}$. En particulier, pour $i = N-1$, on obtient $a_0 \wedge a_1 = a_{N-1}$.
• Supposons maintenant que $a_0 \wedge a_1 = a_{N-1} = 1$. D'après le théorème de Bézout, il existe $(s,t) \in A^2$ tel que $sa_0 + ta_1 = 1$. La suite de l'algorithme d'Euclide permet le calcul d'un tel couple (s,t) : Notons q_i le quotient de la division euclidienne de a_{i-1} par a_i. Ainsi, $a_{i+1} = a_{i-1} - q_i ai$.
En particulier, avec $i = N-2$, on obtient $1 = a_{N-3} - q_{N-2}a_{N-2}$.
Supposons que, pour un entier $i \in \{1, \ldots, N-3\}$, on dispose d'entiers s_i et t_i tels que $1 = s_i a_i + t_i a_{i+1}$. Alors $1 = s_i a_i + t_i(a_{i-1} - a_i q_i) = (s_i - t_i q_i)a_i + t_i a_{i-1}$, ce qui donne des entiers s_{i-1} et t_{i-1} tels que $1 = s_{i-1}a_{i-1} + t_{i-1}a_i$.
Par récurrence descendante, on peut donc calculer des entier s_0 et t_0 tels que $1 = s_0 a_0 + t_0 a_1$.

Corollaire. Supposons que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ et soit $(A,B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$.
Les PGCD et PPCM de A et B sont les mêmes, que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

Exercice. Soit $a, b, c \in A$ avec a et b non nuls.
Résoudre l'équation de Bézout (B) : $au + bv = c$ en l'inconnue $(u,v) \in A^2$.

Il faut savoir le démontrer.

2 Identification entre polynômes formels et applications polynomiales

Notation. On fixe un corps $\mathbb{K}$ quelconque.

Propriété. Soit $P \in \mathbb{K}[X]$ et $a_1, \ldots, a_k$ k éléments de $\mathbb{K}$ deux à deux distincts :
$a_1, \ldots, a_k$ sont toutes racines de P si et seulement si P est un multiple de $(X - a_1) \times \cdots \times (X - a_k)$.
Il faut savoir le démontrer.

Corollaire. Un polynôme non nul admet au plus $\deg(P)$ racines.

Principe de rigidité des polynômes : si $P \in \mathbb{K}[X]$ possède une infinité de racines, alors $P = 0$.

Propriété. Soit $n \in \mathbb{N}$ et $P, Q \in \mathbb{K}_n[X]$.
Si $\{x \in \mathbb{K} \ / \ \tilde{P}(x) = \tilde{Q}(x)\}$ contient au moins $n+1$ scalaires, alors $P = Q$.

Théorème. On peut identifier l'ensemble $\mathbb{K}[X]$ des polynômes formels avec l'ensemble $\mathcal{P}_{\mathbb{K}}$ des applications polynomiales de $\mathbb{K}$ dans $\mathbb{K}$ si et seulement si $\mathbb{K}$ est de cardinal infini.

Remarque. Si $\mathbb{K}$ est fini de cardinal q, alors $\displaystyle\prod_{a \in \mathbb{K}} (X - a) = X^q - X$.

Il faut savoir le démontrer.

3 Polynôme d'interpolation de Lagrange

Notation. Dans tout ce paragraphe, on fixe un corps quelconque $\mathbb{K}$, $n \in \mathbb{N}$ et une famille $a_0, \ldots, a_n \in \mathbb{K}$ de $n+1$ scalaires deux à deux distincts.
Pour tout $i \in \{0, \ldots, n\}$, posons $L_i = \displaystyle\prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - a_j}{a_i - a_j}$.
Les L_i sont appelés les polynômes de Lagrange associés à $(a_0, \ldots, a_n)$.

Propriété. Pour tout $i, k \in \{0, \ldots, n\}$, $\widetilde{L_i}(a_k) = \delta_{i,k}$.

Propriété. Pour tout $P \in \mathbb{K}_n[X]$, $P = \sum_{i=0}^{n} \tilde{P}(a_i) L_i$.

Il faut savoir le démontrer.

Théorème. Soit $(b_0, b_1, \ldots, b_n) \in \mathbb{K}^{n+1}$ une famille quelconque de scalaires. Il existe un unique polynôme P_0 de degré inférieur ou égal à n tel que, pour tout $i \in \{0, \ldots, n\}$, $\widetilde{P_0}(a_i) = b_i$. P_0 est appelé le polynôme d'interpolation de Lagrange (associé aux deux familles $(a_0, a_1, \ldots, a_n)$ et $(b_0, b_1, \ldots, b_n)$).

On dispose de la formule suivante : $P_0 = \sum_{i=0}^{n} \left(b_i \prod_{\substack{0 \le j \le n \\ j \ne i}} \frac{X - a_j}{a_i - a_j} \right)$. Enfin, l'ensemble des polynômes P vérifiant, pour tout $i \in \{0, \ldots, n\}$, $\tilde{P}(a_i) = b_i$, est égal à $P_0 + \left(\prod_{i=0}^{n} (X - a_i)\right) \mathbb{K}[X]$.

4 Polynôme dérivé

Notation. Dans ce paragraphe, on suppose que $\mathbb{K}$ est un corps de caractéristique nulle.

Propriété. Pour tout $P \in \mathbb{K}[X]$ tel que $\deg(P) \ge 1$, $\deg(P') = \deg(P) - 1$.

Corollaire. Soit $P \in \mathbb{K}[X]$. P est un polynôme constant si et seulement si $P' = 0$.

Corollaire. Si $P \in \mathbb{K}[X]$, $\deg(P) \ge n \Longrightarrow \deg(P^{(n)}) = \deg(P) - n$ et $P^{(n)} = 0 \Longleftrightarrow \deg(P) < n$.

Formule de Taylor : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors $P = \sum_{n \in \mathbb{N}} \frac{(X - a)^n}{n!.1_{\mathbb{K}}} P^{(n)}(a)$.

Il faut savoir le démontrer.

Corollaire. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $k \in \mathbb{N}$. Alors
le reste de la division euclidienne de P par $(X - a)^k$ est égal à $\sum_{h=0}^{k-1} \frac{(X - a)^h}{h!.1_{\mathbb{K}}} P^{(h)}(a)$.

5 Racines multiples

Notation. $\mathbb{K}$ désigne un corps quelconque.

Définition. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est une racine de P de multiplicité m si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X - a)^m Q(X)$ avec $\tilde{Q}(a) \ne 0$.

Remarque. a n'est pas racine de P si et seulement si a est racine de P de multiplicité nulle.

Définition. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$.
a est racine de P de multiplicité au moins m si et seulement si $(X - a)^m \mid P$.
Ainsi, a est racine de P de multiplicité m si et seulement si elle est racine de P de multiplicité au moins m, mais n'est pas racine de P de multiplicité au moins $m + 1$.

Définition. On dit que $a \in \mathbb{K}$ est une racine simple (resp : double, triple) de $P \in \mathbb{K}[X]$ si et seulement si a est une racine de P de multiplicité 1 (resp : 2, 3).

Définition. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Posons $\{a_1, \ldots, a_k\} = \{x \in \mathbb{K} / \tilde{P}(x) = 0\}$. Pour tout $h \in \mathbb{N}_k$, notons m_h la multiplicité de a_h pour le polynôme P. On dit alors que le nombre de racines de P, **comptées avec multiplicité**, est égal à $\sum_{h=1}^{k} m_h$.

Et k est le nombre de racines de P comptées sans multiplicité.

Propriété. Soit $P \in \mathbb{K}[X]$, $a_1, \ldots, a_k \in \mathbb{K}$ et $m_1, \ldots, m_h \in \mathbb{N}$. Pour tout $h \in \{1, \ldots, k\}$, a_h est racine de P de multiplicité au moins m_h si et seulement si P est un multiple de $\prod_{h=1}^{k} (X - a_h)^{m_h}$.

Propriété. Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Le nombre de racines de P, comptées avec multiplicité est inférieur ou égal au degré de P.

Hypothèse : Pour la suite de ce paragraphe, on suppose que $\text{car}(\mathbb{K}) = 0$.

Théorème. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est racine de P de multiplicité au moins m si et seulement si $\forall i \in \{0, \ldots, m-1\},\ \ P^{(i)}(a) = 0$.
Il faut savoir le démontrer.

Corollaire. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est racine de P de multiplicité m si et seulement si $\forall i \in \{0, \ldots, m-1\},\ \ P^{(i)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Corollaire. Si $a \in \mathbb{K}$ est racine de $P \in \mathbb{K}[X]$ de multiplicité $m \in \mathbb{N}^*$, alors a est racine de P' de multiplicité $m - 1$.

6 Polynômes scindés

Notation. $\mathbb{K}$ désigne un corps quelconque.

Définition. $P \in \mathbb{K}[X] \setminus \{0\}$ est scindé dans $\mathbb{K}[X]$ si et seulement si sa décomposition en polynômes irréductibles dans $\mathbb{K}[X]$ ne fait intervenir que des polynômes de degré 1.

Propriété. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. P est scindé dans $\mathbb{K}[X]$ si et seulement si le nombre de racines de P dans $\mathbb{K}$, comptées avec multiplicité, est égal au degré de P.
Il faut savoir le démontrer.

Définition. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. On dit que P est simplement scindé dans $\mathbb{K}[X]$ si et seulement si P est scindé dans $\mathbb{K}$ et si toutes ses racines sont simples.

Relations de Viète entre coefficients et racines : Soit $P \in \mathbb{K}[X]$ un polynôme **scindé** dans $\mathbb{K}[X]$ de degré n, avec $n \geq 1$. Alors P peut s'écrire sous les deux formes suivantes :
- $P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, avec $a_0, \ldots, a_n \in \mathbb{K}$ et $a_n \neq 0$;
- $P(X) = a_n (X - \beta_1) \times \cdots \times (X - \beta_n)$, où $\beta_1, \ldots, \beta_n$ est la liste des racines de P, comptées avec multiplicité. Alors, pour tout $p \in \{1, \ldots, n\}$,
$$\sigma_p = (-1)^p \frac{a_{n-p}}{a_n}, \text{ où } \sigma_p = \sum_{1 \leq i_1 < \cdots < i_p \leq n} \beta_{i_1} \times \cdots \times \beta_{i_p}.$$

Les σ_p s'appellent les fonctions symétriques élémentaires des racines. En particulier,
- Pour $p = 1$, $\sum_{i=1}^{n} \beta_i = -\frac{a_{n-1}}{a_n}$. Il s'agit de la somme des racines de P, comptées avec multiplicités.
- Pour $p = n$, $\prod_{i=1}^{n} \beta_i = (-1)^n \frac{a_0}{a_n}$. Il s'agit du produit des racines de P, comptées avec multiplicités.

Cette fin de paragraphe est hors programme.

Définition. Soit $n \in \mathbb{N}^*$ et $A \in \mathbb{K}[X_1, \ldots, X_n]$ un polynôme à n indéterminées. On dit que A est symétrique si et seulement si, pour tout $\sigma \in \mathcal{S}_n$, $A(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = A(X_1, \ldots, X_n)$.

Exemples. Les polynômes de Newton : $X_1^p + \cdots + X_n^p$, où $n, p \in \mathbb{N}^*$ sont symétriques.
Les polynômes symétriques élémentaires : pour tout $p \in \{1, \ldots, n\}$,

$\Sigma_p(X_1, \dots, X_n) = \displaystyle\sum_{1 \le i_1 < i_2 < \cdots < i_p \le n} X_{i_1} \times \cdots \times X_{i_p}$ est bien un polynôme symétrique.

Propriété. (Admise) Soit $n \in \mathbb{N}^*$. On suppose que A est un polynôme symétrique de $\mathbb{L}[X_1, \dots, X_n]$ (où $\mathbb{L}$ est un corps). Alors il existe $B \in \mathbb{L}[X_1, \dots, X_n]$ tel que $A = B(\Sigma_1, \dots, \Sigma_n)$.

Corollaire. Avec ces notations, si $\mathbb{K}$ est un sur-corps de $\mathbb{L}$ et si $P \in \mathbb{L}[X]$ est scindé dans $\mathbb{K}[X]$, alors en notant $\beta_1, \dots, \beta_n$ les racines de P comptées avec multiplicité, $A(\beta_1, \dots, \beta_n) \in \mathbb{L}$.

Exemple. Soit $P \in \mathbb{Q}[X]$ un polynôme dont les racines complexes comptées avec multiplicité sont notées $\beta_1, \dots, \beta_n$. Alors pour tout $p \in \mathbb{N}^*$, $\beta_1^p + \cdots + \beta_n^p \in \mathbb{Q}$.

7 Polynômes de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$

Définition. Si $P = \displaystyle\sum_{k \in \mathbb{N}} a_k X^k \in \mathbb{C}[X]$, on note $\overline{P} = \displaystyle\sum_{k \in \mathbb{N}} \overline{a_k} X^k$.

Propriété. L'application $\begin{array}{ccc} \mathbb{C}[X] & \longrightarrow & \mathbb{C}[X] \\ P & \longmapsto & \overline{P} \end{array}$ est un isomorphisme d'anneaux.

Propriété. Soit $P \in \mathbb{C}[X]$, $\alpha \in \mathbb{C}$ et $m \in \mathbb{N}$. α est racine de P de multiplicité m si et seulement si $\overline{\alpha}$ est racine de $\overline{P}$ de multiplicité m.
Il faut savoir le démontrer.

Corollaire. Si $P \in \mathbb{R}[X]$ et si α est racine de P (resp : racine de multiplicité m), alors $\overline{\alpha}$ est aussi une racine de P (resp : racine de multiplicité m).

Théorème de d'Alembert : Tout polynôme à coefficients complexes de degré supérieur ou égal à 1 possède au moins une racine complexe.

Corollaire. Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Corollaire. Dans $\mathbb{C}[X]$, deux polynômes sont premiers entre eux si et seulement si ils n'ont aucune racine complexe commune.

Corollaire. Dans $\mathbb{C}[X]$, tout polynôme non nul est scindé.
Dans $\mathbb{C}[X]$, le nombre de racines, comptées avec multiplicité, de tout polynôme non nul est égal à son degré.

Propriété. Soit $P, Q \in \mathbb{C}[X] \setminus \{0\}$. Alors $P \mid Q$ si et seulement si toute racine de P est racine de Q avec une multiplicité pour Q supérieure ou égale à celle pour P.

Propriété. Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.
Il faut savoir le démontrer.

Propriété. Soit $P \in \mathbb{R}[X] \setminus \{0\}$. P est scindé dans $\mathbb{R}[X]$ si et seulement si toutes ses racines sont réelles.