3 Polynômes et fractions rationnelles

3.1 Polynômes à une indéterminée sur un corps commutatif K

Soit K un corps commutatif. On sait très bien ce qu'est un polynôme à coefficients dans K : c'est une expression abstraite $P = \sum_{k=0}^{n} a_k X^k$ où les a_i sont des éléments de K appelés les coefficients de P. On sait ajouter et multiplier les polynômes, les multiplier par un scalaire : les polynômes forment une K-algèbre.

3.1 Quelques mots sur la définition de l'algèbre $K[X]$. Se donner un polynôme revient à se donner ses coefficients c'est à dire une suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de K qui sont nuls pour k assez grand : il existe $n \in \mathbb{N}$ satisfaisant $a_k = 0$ pour $k > n$. On peut formaliser cela en définissant un polynôme comme la suite abstraite de ses coefficients : l'ensemble des polynômes est alors l'ensemble $K^{(\mathbb{N})}$ des suites $(a_k)_{k\in\mathbb{N}}$ telles qu'il existe $n \in \mathbb{N}$ satisfaisant $a_k = 0$ pour $k > n$. Dans cette vision, le $k^{\text{ème}}$ coefficient du polynôme X^k est égal à 1, et tous les autres sont nuls. L'ensemble $K^{(\mathbb{N})}$ est naturellement un K-espace vectoriel de dimension infinie et $(X^k)_{k\in\mathbb{N}}$ en est une base.

L'algèbre $K[X]$ est donc l'espace vectoriel $K^{(\mathbb{N})}$ muni de l'unique produit tel que $X^k X^\ell = X^{k+\ell}$ (pour tous $k, \ell \in \mathbb{N}$). Enfin, on identifie K avec l'ensemble des polynômes constants (au moyen de $a \mapsto aX^{(0)}$).

Soit $P \in K[X]$ un polynôme non nul. On appelle *degré* de P l'entier $\partial P = n \in \mathbb{N}$ tel que $a_n \neq 0$ et, $a_k = 0$ pour $k > n$ (où les a_k sont les coefficients de P). Le coefficient non nul de plus haut degré (a_n si $\partial P = n$) s'appelle le *coefficient directeur* de P. On dit que P est *unitaire* (ou *monique*) si son coefficient directeur est 1.

3.2 Proposition. Pour $P, Q \in K[X]$ deux polynômes non nuls, on a $PQ \neq 0$, $\partial(PQ) = \partial P + \partial Q$, et le coefficient directeur de PQ est le produit des coefficients directeurs de P et de Q. En particulier, l'anneau $K[X]$ est intègre.

L'anneau $K[X]$ est euclidien de stathme ∂. Plus précisément on a (où l'on a convenu $\partial 0 < 0$) :

3.3 Proposition : Division euclidienne dans $K[X]$. Soient $A, B \in K[X]$ avec $B \neq 0$. Il existe un unique couple $Q, R \in K[X]$ tels que $A = BQ + R$ et $\partial R < \partial B$.

On en déduit que $K[X]$ est principal, c'est-à-dire que tous les idéaux de $K[X]$ sont de la forme $AK[X]$. On peut alors définir le plus grand commun diviseur (PGCD) et plus petit commun multiple (PPCM) de deux polynômes, établir un théorème de Bézout, un algorithme d'Euclide qui permet de trouver le PGCD et une relation de Bézout ainsi que la décomposition unique d'un polynôme en facteurs irréductibles.

3.4 Exercices. a) Soient L un corps commutatif et K un sous-corps de L. Soient $A, B \in K[X]$; Démontrer que leur PGCD est le même qu'on les considère comme éléments de $K[X]$ ou de $L[X]$.

b) Calculer $PGCD(X^m - 1, X^n - 1)$.

De l'égalité $\partial(PQ) = \partial P + \partial Q$ on déduit :

3.5 Proposition. a) Les éléments inversibles de $K[X]$ sont les polynômes non nuls de degré nul, *i.e.* les éléments de K.

b) Tout polynôme de degré 1 est irréductible.

3.2 Fonctions polynômes

3.2.1 Racines

Soit K un corps. Si $x \in K$ et $P = \sum_{k=0}^{n} a_k X^k \in K[X]$, on pose $P(x) = \sum_{k=0}^{n} a_k x^k$. L'application $x \mapsto P(x)$ s'appelle la fonction polynôme associée à P. L'application $P \mapsto P(x)$ est un homomorphisme d'anneaux de $K[X]$ dans K. On dit que x est une *racine* de P si $P(x) = 0$.

3.6 Proposition. Le reste de la division euclidienne de P par $X - a$ est $P(a)$. En particulier, $X - a$ divise P si et seulement si $P(a) = 0$.

En effet, écrivons $P = (X - a)Q + R$ avec $\partial R < 0$, donc $R \in K$. Comme $(X - a)(a) = 0$, on trouve $P(a) = R$.

Cette proposition nous conduit à dire que a est une racine d'ordre k (au moins) si $(X - a)^k$ divise P et d'ordre exactement k si de plus $(X - a)^{k+1}$ ne divise pas P. Si $k = 2, 3$, on dira que a est racine double, triple... de P. Si $k \geqslant 2$ on dira que a est *racine multiple* de P

3.7 Proposition. Soient $a_1, \ldots, a_k \in K$ des éléments deux à deux distincts et $m_1, \ldots, m_k \in \mathbb{N}$. Si un polynôme non nul P admet les racines a_j avec multiplicité m_j, il est divisible par $\prod_{j=1}^{k} (X - a_j)^{m_j}$. En particulier $\partial P \geqslant \sum m_j$ et si $\partial P = \sum m_j$, alors $P = a \prod_{j=1}^{k} (X - a_j)^{m_j}$ où $a \in K$ est le coefficient directeur de P.

Les polynômes $X - a_j$ sont premiers entre eux deux à deux, donc il en va de même pour $(X - a_j)^{m_j}$. Si P admet les racines a_j avec multiplicité m_j, il est divisible par $(X - a_j)^{m_j}$, donc par leur produit.

3.8 Exemple. Soit p un nombre premier. D'après le (petit) théorème de Fermat, pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, on a $x^p = x$. En d'autres termes, tout élément de $\mathbb{Z}/p\mathbb{Z}$ est racine du polynôme $X^p - X \in \mathbb{Z}/p\mathbb{Z}[X]$. On en déduit que $\prod_{x \in \mathbb{Z}/p\mathbb{Z}} (X - x) = X^p - X$.

3.9 Corollaire. Si K est infini, l'homomorphisme qui à un polynôme P associe la fonction polynôme $x \mapsto P(x)$ de K dans K est injectif.

En effet, un polynôme non nul ne peut avoir qu'un nombre fini de racines. Il ne peut s'annuler sur tout K.

A cause de ce corollaire, on confond souvent les polynômes avec les fonctions polynômes.

3.10 Remarque. Pour $K = \mathbb{Z}/p\mathbb{Z}$, le noyau de l'homomorphisme qui à un polynôme P associe la fonction polynôme $x \mapsto P(x)$ de K dans K est l'idéal engendré par $X^p - X$.

3.11 Exemple. Polynôme d'interpolation de Lagrange. Soient $x_1, x_2 \ldots, x_n$ des éléments distincts de K et $\lambda_1, \lambda_2, \ldots, \lambda_n$ des éléments de K. Il existe un unique polynôme P de degré au plus $n - 1$ tel que $P(x_i) = \lambda_i$ pour tout i.

Existence. Pour $i = 1, \ldots, n$, posons $Q_i = \prod_{1 \leqslant j \leqslant n;\ j \neq i} (X - x_j)$. On prend $P = \sum_{i=1}^{n} \frac{\lambda_i}{Q_i(x_i)} Q_i$.

Unicité. Si P et Q satisfont ces conditions alors $P - Q$ s'annule en les x_i ; comme $\partial(P - Q) < n$, il vient $P - Q = 0$.

3.2.2 Polynômes scindés ; relations entre coefficients et racines

On dit qu'un polynôme P est *scindé* s'il est produit de polynômes du premier degré. Alors P s'écrit $P = a\prod_{k=1}^{n}(X - x_k)$.

Soit $P = \prod_{k=1}^{n}(X - x_k)$ un polynôme unitaire scindé. Écrivons $P = X^n + \sum_{k=0}^{n-1} a_k X^k$. Alors on a

- somme des racines $\sum_{k=1}^{n} x_k = -a_{n-1}$;
- produit des racines $(-1)^n a_0 = \prod_{k=1}^{n} x_k$.
- Plus généralement, $(-1)^\ell a_{n-\ell} = \sum_{1\leqslant k_1<\ldots<k_\ell\leqslant n}\left(\prod_{j=1}^{\ell} x_{k_j}\right)$ est la somme de tous les produits de ℓ racines.
- Pour $n = 2$ on trouve $P = X^2 - SX + P$ où S est la somme et P le produit des racines.
- Pour $n = 3$ on trouve $P = X^3 - SX^2 + \Sigma_2 X - P$, où S est la somme, P le produit des racines et $\Sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$.

3.2.3 Dérivation des polynômes

Soit $P = \sum_{k=0}^{n} a_k X^k$. On définit sa dérivée : c'est le polynôme $P' = \sum_{k=1}^{n} k a_k X^{k-1}$.

3.12 Proposition. a) Pour $P, Q \in K[X]$, on a $(PQ)' = P'Q + PQ'$.

b) Soient $P \in K[X]$ et $a \in K$ une racine de P. Alors a est une racine double de P si et seulement si $P'(a) = 0$.

a) se vérifie pour $P = X^k$ et $Q = X^\ell$ et s'étend par linéarité.
Pour b), écrivons $P = (X-a)Q$ de sorte que (d'après a) $P' = Q+(X-a)Q'$, donc $Q(a) = P'(a)$. Alors a est racine double de P, si et seulement si c'est une racine de Q, *i.e.* si et seulement si $P'(a) = Q(a) = 0$.

3.13 Dérivées successives ; identité de Taylor. On définit aussi les dérivées successives en posant $P'' = (P')'$ *etc.* La dérivée k-ième se note $P^{(k)}$. On a $P^{(k)}(0) = k!a_k$, de sorte que, si K est de caractéristique nulle (et $\partial P \leqslant n$),

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k.$$

Plus généralement, soit $a \in K$. Les polynômes $(X - a)^k$ forment une base de $K[X]$ (car ils sont échelonnés). Posons $Q_k = \dfrac{(X-a)^k}{k!}$. On a $Q_k^{(j)} = Q_{k-j}$ si $k \geqslant j$ et $Q_k^{(j)} = 0$ si $k < j$. En particulier, $Q_k^{(j)}(a) = \delta_k^j$, et si P s'écrit $\sum_k b_k Q_k$, il vient $b_j = P^{(j)}(a)$, donc

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X - a)^k.$$

3.2.4 Polynômes irréductibles sur $\mathbb{R}$ et $\mathbb{C}$

Donnons sans démonstration le théorème fondamental suivant :

3.14 Théorème de d'Alembert-Gauss. Tout polynôme non constant à coefficients complexes admet au moins une racine dans $\mathbb{C}$.

Tout polynôme non constant est donc divisible par un $X - a$. Il en résulte immédiatement que les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes du premier degré : tout polynôme à coefficients complexes est donc scindé.

Soit maintenant $P \in \mathbb{R}[X]$ un polynôme irréductible. Considérons le comme polynôme à coefficients complexes. Il a une racine $z \in \mathbb{C}$. Si $z \in \mathbb{R}$, P est du premier degré. Si $z = a + ib \notin \mathbb{R}$, alors écrivons $P = BQ + R$ la division euclidienne de P par $B = (X - z)(X - \overline{z}) = X^2 - 2aX + (a^2 + b^2)$ (dans $\mathbb{R}[X]$). Alors $R \in \mathbb{R}[X]$ est de degré au plus 1 et s'annule en z : c'est le polynôme nul.

On trouve :

3.15 Corollaire. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes du premier degré et ceux du deuxième degré de discriminant strictement négatif.

3.2.5 Racines et extensions de corps

Soient K un corps commutatif et $P \in K[X]$. Si L est une extension de K, on peut considérer P comme polynôme à coefficients dans L : en d'autres termes on identifie $K[X]$ à un sous-anneau de $L[X]$. En particulier, on peut définir

On note (P) l'idéal $PK[X]$ de $K[X]$. Puisque $K[X]$ est principal, tout idéal de $K[X]$ est de cette forme. Nous utiliserons le résultat suivant.

3.16 Proposition. Soit $P \in K[X]$ un polynôme non nul. On a l'équivalence entre :

(i) Le polynôme P est irréductible ;

(ii) L'anneau quotient $K[X]/(P)$ est intègre ;

(iii) L'anneau quotient $K[X]/(P)$ est un corps. □

Soit $P \in K[X]$ un polynôme irréductible. Notons $L = K[X]/(P)$ l'anneau quotient.

- On considère l'application $i : K \to L$ qui à un scalaire $a \in K$ associe la classe du polynôme constant $a \in K[X]$ dans le quotient. L'application i est un morphisme de corps (injectif) au moyen duquel on identifie K à un sous-corps de L et donc L à une extension de K.
- Notons aussi x la classe dans L du polynôme X dans le quotient $L = K[X]/(P)$. En d'autres termes, on a $x = \pi(X)$ où $\pi : K[X] \to L = K[X]/(P)$ est l'application quotient.
- Comme π est un homomorphisme d'anneaux, on $\pi(X^2) = x^2$ et plus généralement $\pi(X^n) = x^n$.
- Pour $a \in K$, on a $\pi(aX^0) = i(a)$, en d'autres termes, avec les identifications de $K \subset K[X]$ et $K \subset L$, la restriction de π à K est l'identité.
- On a donc $\pi(\sum_{k=0}^{n} a_k X^k) = \sum_{k=0}^{n} a_k x^k$; autrement dit, pour tout polynôme $Q \in K[X]$, on a $\pi(Q) = Q(x)$.
- En particulier, puisque $P \in \ker \pi = (P)$, on a $P(x) = 0$.

On a démontré :

3.17 Théorème. Soient K un corps et $P \in K[X]$ un polynôme irréductible sur K. Il existe une extension L de K dans laquelle P a une racine.

□

3.18 Corollaire. Soient K un corps et $P \in K[X]$ un polynôme non constant.

a) Il existe une extension L de K dans laquelle P a une racine.

b) Il existe une extension L de K dans laquelle P est scindé.

Démonstration. a) Soit $P_0 \in K[X]$ un polynôme irréductible dans K divisant P. Par le théorème ci-dessus, il existe une extension L de K dans laquelle P_0 admet une racine ; celle-ci sera une racine de P.

b) On procède par récurrence sur le degré de P. On démontre par récurrence sur n l'énoncé suivant : $S(n)$: pour tout corps commutatif K et tout polynôme $P \in K[X]$ de degré n, il existe une extension L de K telle que P est scindé sur L.
- Pour $n = 1$: tout polynôme de degré 1 est scindé donc $S(1)$ est vraie.
- Supposons $S(n)$ démontrée et soit P un polynôme de degré $n+1$ sur un corps commutatif K. Par (a), il existe une extension L_1 de K dans laquelle P admet une racine α. Alors P vu comme polynôme de $L_1[X]$ s'écrit $P = (X-\alpha)Q$ où $Q \in L_1[X]$ est de degré n. Puisque $S(n)$ est vraie (hypothèse de récurrence), il existe une extension L de L_1 dans laquelle le polynôme Q est scindé. Alors L est une extension de K et le polynôme $P = (X-\alpha)Q$ est scindé dans L. □

3.3 Fractions rationnelles sur un corps commutatif K

3.19 Définition. Le corps des fractions de $K[X]$ se note $K(X)$. Ses éléments s'appellent des *fractions rationnelles.*

Si A, B, D sont des polynômes avec $BD \neq 0$, on a $\dfrac{AD}{BD} = \dfrac{A}{B}$. Donc pour chaque fraction rationnelle F il existe des polynômes A, B premiers entre eux $B \neq 0$ tels que $F = \dfrac{A}{B}$. Une écriture de $F = \dfrac{A}{B}$ avec A, B premiers entre eux s'appelle une *forme irréductible* de F.

Soit F une fraction rationnelle et $F = \dfrac{A}{B}$ une forme irréductible. Les racines de A s'appellent les *zéros* ou *racines* de F ; les racines de B s'appellent les *pôles* de F. L'*ordre de multiplicité* d'un zéro (*resp.* pôle) a est l'ordre de multiplicité de la racine a de A (*resp.* B).

Soit $F \in K(X)$. Notons $\mathcal{P} \subset K$ l'ensemble de ses pôles. Soit $x \in K - \mathcal{P}$. Il existe une écriture $F = \dfrac{A}{B}$ telle que $B(x) \neq 0$. On pose alors $F(x) = A(x)B(x)^{-1}$. Cet élément de K ne dépend pas de l'écriture $F = \dfrac{A}{B}$ (avec $B(x) \neq 0$).
L'application $x \mapsto F(x)$ de $K - \mathcal{P}$ dans K s'appelle la *fonction rationnelle* associée à F.

Décomposition en éléments simples

On va peu à peu essayer de décomposer une fraction rationnelle en une somme de termes plus simples.

a) ***Partie entière*** Le degré d'une fraction rationnelle $F = \dfrac{A}{B}$ est le nombre $\partial F = \partial A - \partial B (\in \mathbb{Z})$. Ce nombre est indépendant de l'écriture. On a $\partial(FG) = \partial F + \partial G$ et $\partial(F+G) \leqslant \max\{\partial F, \partial G\}$ (avec la convention $\partial 0 = -\infty$).
Soit $F = \dfrac{A}{B}$ une fraction rationnelle. Écrivons $A = BQ + R$ la division euclidienne de A par B. On trouve $F = Q + \dfrac{R}{B}$, où $Q \in K[X] \subset K(X)$ et $\dfrac{R}{B}$ est une fraction rationnelle de degré < 0 (ou nulle). Donc :
Toute fraction rationnelle $F \in K(X)$ se décompose de façon unique en une somme d'un polynôme Q et d'une fraction rationnelle F_1 de degré strictement négatif. Le polynôme Q de cette décomposition s'appelle la partie entière *de F.*

b) ***Parties primaires.*** Soit à présent $F = \dfrac{A}{B}$ une fraction rationnelle de degré < 0. Supposons que B s'écrive $B = B_1B_2$ où B_1 et B_2 sont des polynômes premiers entre eux. D'après le théorème de Bézout, il existe des polynômes C_1 et C_2 tels que $A = B_1C_2 + B_2C_1$. Écrivons $C_1 = QB_1 + A_1$ la division euclidienne de C_1 par B_1 et posons $A_2 = C_2 + QB_2$, de sorte que $A = A_2B_1 + A_1B_2$ avec $\partial A_1 < \partial B_1$. Notons qu'alors $A_2B_1 = A - A_1B_2$, de sorte que $\partial(A_2B_1) < \partial B$; il vient $\dfrac{A}{B} = \dfrac{A_1}{B_1} + \dfrac{A_2}{B_2}$ avec $\partial A_1 < \partial B_1$ et $\partial A_2 < \partial B_2$. On vérifie que cette décomposition est unique.

Décomposant B en produit $\displaystyle\prod_{i=1}^{k} P_i^{m_i}$ où les P_i sont des polynômes irréductibles distincts on obtient (par récurrence sur k) une décomposition unique

$$\frac{A}{B} = \sum_{i=1}^{k} \frac{A_i}{P_i^{m_i}}$$

avec $\partial A_i < m_i \partial P_i$.

c) ***Éléments simples.*** Considérons enfin le cas où $F = \dfrac{A}{P^m}$ où P est irréductible, $\partial A < m\partial P$. Supposons que $m \geqslant 2$, et notons $A = PQ + R$ la division euclidienne de A par P. On trouve $F = \dfrac{R}{P^m} + \dfrac{Q}{P^{m-1}}$. Par récurrence sur m, on trouve donc que F s'écrit

$$\sum_{k=1}^{m} \frac{R_k}{P^k}$$

avec $\partial R_k < \partial P$. Cette décomposition est encore unique.

d) Mettant tout cela ensemble, on trouve que toute fraction rationnelle $F = \dfrac{A}{B}$ s'écrit de façon unique sous la forme :

$$F = E + \sum_{i=1}^{k} \sum_{j=1}^{m_i} \frac{R_{i,j}}{P_i^j}$$

où $B = b\prod P_i^{m_i}$ est la décomposition de B en facteurs irréductibles (et $b \in K^*$), E et $R_{i,j}$ sont des polynômes avec $\partial R_{i,j} < \partial P_i$.
Cette décomposition s'appelle la *décomposition* de F *en éléments simples.*

Lorsque P_i est un polynôme du premier degré - c'est toujours le cas si $K = \mathbb{C}$ - les $R_{i,j}$ sont de degré nul, donc des éléments de K.

Dans le cas où $K = \mathbb{R}$, on peut avoir des P_i du deuxième degré ; on aura alors des termes du premier degré au numérateur.

3.4 Exercices

3.1 Exercice. *Racines rationnelles*
Soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients entiers. Soit $x = \dfrac{p}{q}$ une racine rationnelle de P écrite sous forme irréductible. Démontrer que $p|a_0$ et $q|a_n$.

3.2 Exercice. Factoriser le polynôme $P = X^5 - 4X^4 + 9X^3 - 21X^2 + 20X - 5$ sachant qu'il s'écrit comme un produit de trois polynômes à coefficients entiers.

3.3 Exercice. [Contenu d'un polynôme]

1. Soient $A, B \in \mathbb{Z}[X]$.
   Écrivons $A = \sum_{k=0}^{m} a_k X^k$, $B = \sum_{k=0}^{n} b_k X^k$ et $AB = \sum_{k=0}^{m+n} c_k X^k$. Soit p un nombre premier. On suppose que p divise tous les c_k. Démontrer que p divise tous les a_k ou tous les b_k.
   On appelle *contenu* d'un polynôme $P = \sum_{k=0}^{n} p_k X^k$ à coefficients dans $\mathbb{Z}$ et on note $c(P)$ le PGCD de ses coefficients $p_0, \ldots, p_n$.
2. Soient $A, B \in \mathbb{Z}[X]$. Démontrer que si $c(A) = c(B) = 1$, alors $c(AB) = 1$. En déduire que l'on a toujours $c(AB) = c(A)c(B)$.
3. Soit $P \in \mathbb{Z}[X]$ un polynôme non constant. Démontrer que si P est irréductible dans $\mathbb{Z}[X]$ il est irréductible dans $\mathbb{Q}[X]$.

3.4 Exercice. [Critère d'Eisenstein] Soient P un polynôme unitaire à coefficients entiers et p un nombre premier. On suppose que p divise tous les coefficients de P - sauf le coefficient dominant - et que $P(0)$ n'est pas divisible par p^2. Démontrer que P est irréductible sur $\mathbb{Z}$ - donc sur $\mathbb{Q}$.

Application. Démontrer que pour tout nombre premier p le polynôme $\Phi_p = \sum_{k=0}^{p-1} X^k$ est irréductible sur $\mathbb{Q}$.

3.5 Exercice. Décomposer en éléments simples dans $\mathbb{R}[X]$ la fraction rationnelle $F = \dfrac{X^2+2}{X^3(X-1)^2}$.
En déduire une primitive de l'application $t \mapsto \dfrac{t^2+2}{t^3(t-1)^2}$.

3.6 Exercice. Soit K un corps et $a, b \in \mathbb{N}$. On considère les polynômes $A = X^a - 1$ et $B = X^b - 1$ de $K[X]$.

1. On suppose $b \neq 0$. Quel est le reste de la division euclidienne de A par B ?
2. Quel est le PGCD D de A et B ?
3. Écrire une relation de Bézout $D = AU + BV$.
4. Autre méthode : décomposer A et B en facteurs irréductibles dans $\mathbb{C}$. Pourquoi cela donne-t-il le PGCD de A et B vus comme éléments de $\mathbb{Q}[X]$?

3.7 Exercice. Trouver un polynôme $P \in K[X]$ de degré 3 tel que $P(0) = 1$, $P'(0) = 0$, $P(1) = 0$ et $P'(1) = 1$. Quels sont les polynômes $Q \in K[X]$ qui vérifient $Q(0) = 1$, $Q'(0) = 0$, $Q(1) = 0$ et $Q'(1) = 1$?

3.8 Exercice. Calculer des primitives des fonctions
a) $x \mapsto \dfrac{1}{x^4 - x^2 - 2}$; b) $x \mapsto \dfrac{x+1}{(x^2+1)^2}$; c) $x \mapsto \dfrac{x+1}{x(x-1)^6}$; d) $x \mapsto \dfrac{1}{\cos^3 x}$.

3.9 Exercice. *Résolution des équations du quatrième degré*

1. Soit $P \in K[X]$ un polynôme scindé unitaire de degré 4. Notons z_1, z_2, z_3, z_4 ses racines. Trouver un polynôme de degré 3 dont les racines sont $u_1 = z_1z_2 + z_3z_4$, $u_2 = z_1z_3 + z_2z_4$, $u_3 = z_1z_4 + z_1z_4$.
2. Si on sait résoudre les équations du troisième degré, on peut trouver u_1, u_2, u_3. Comment trouver alors les z_i ?

3.10 Exercice. Résoudre le système d'équations $\begin{cases} x+y+z=3 \\ xy+yz+zx=1 \\ x^3+y^3+z^3=15 \end{cases}$ d'inconnues $x, y, z \in \mathbb{C}$.

3.11 Exercice. Soit p un nombre premier.

1. Démontrer que dans $\mathbb{F}_p[X]$ on a l'égalité $X^p - X = \prod_{x \in \mathbb{F}_p} (X - x)$.
2. Démontrer le *théorème de Wilson* : $(p-1)! + 1 \equiv 0 \ \ [p]$.

3.12 Exercice. Soit $P \in \mathbb{R}[X]$ un polynôme sans racines réelles.

1. Démontrer qu'il existe un polynôme $A \in \mathbb{C}[X]$ tel que $P = \overline{A}\,A$ et A et $\overline{A}$ soient premiers entre eux.

   Notons k le degré de A.
2. Démontrer qu'il existe un unique polynôme $J \in \mathbb{C}[X]$ de degré $< 2k$ tel que $J \equiv i \ [A]$ et $J \equiv -i \ [\overline{A}]$.
3. Démontrer que $J \in \mathbb{R}[X]$ et $J^2 \equiv -1 \ [P]$.
4. Un espace vectoriel complexe peut être considéré comme $\mathbb{R}$-espace vectoriel. Inversement, soient E un $\mathbb{R}$-espace vectoriel et j un endomorphisme de E tel que $j^2 = -\mathrm{id}_E$.
   a) Démontrer qu'il existe une unique structure d'espace vectoriel sur E telle que, pour $s, t \in \mathbb{R}$ et $x \in E$ on ait $(s + it)x = sx + tj(x)$.
   b) Munissons E de cette structure. Démontrer que les endomorphismes du $\mathbb{C}$-espace vectoriel E sont les endomorphismes f du $\mathbb{R}$ espace vectoriel E tels que $j \circ f = f \circ j$.
5. Soit E un $\mathbb{R}$ espace vectoriel de dimension finie et f un endomorphisme de E sans valeurs propres réelles. Démontrer qu'il existe sur E une structure d'espace vectoriel complexe telle que f soit $\mathbb{C}$-linéaire.

3.13 Exercice. *Comment trouver les racines d'un polynôme dans $\mathbb{F}_p$?*
On se donne $P \in K[X]$ dont on veut trouver les racines dans K.

1. Trouver une méthode pour isoler les racines multiples.

   Indication : On pourra utiliser la dérivée de P.
2. On suppose que $K = \mathbb{F}_p$ où p est un (grand !) nombre premier. Donner une méthode pour trouver un polynôme scindé à racines simples ayant les mêmes racines que P.

   Indication : Penser au polynôme $X^p - X$.
3. On suppose que P est scindé à racines simples.
   a) Ecrire $P = AB$ où les racines de A sont des carrés dans $\mathbb{F}_p$ et celles de B ne le sont pas.
   b) Soient a, b deux racines (qu'on ne connait pas). On veut les séparer, c'est à dire écrire $P = AB$ avec a racine de A et b de B. Pour cela, on cherche un polynôme Q dont a ou b est racine mais pas l'autre, puis on prend le PGCD de P et Q. (On dit que Q sépare a et b.) Soit $c \in \mathbb{F}_p$ - distinct de a et de b. On pose $Q = (X - c)^{\frac{p-1}{2}} - 1$. Démontrer que Q sépare a et b si et seulement si $\dfrac{c-a}{c-b}$ n'est pas un carré.

      En choisissant c au hasard, on a donc une chance sur 2 de séparer a et b.
   c) Esquisser une méthode qui va nous permettre de trouver toutes les racines de P (le degré de P est ici supposé petit par rapport à p).

3.14 Exercice. *Polynômes irréductibles dans $\mathbb{F}_p[X]$.*

1. *Fonction de Moebius.* On définit la fonction de Moebius $\mu : \mathbb{N}^* \to \mathbb{Z}$ en posant $\mu(n) = 0$ si n a des facteurs carrés, $\mu(1) = 1$ et $\mu(p_1 p_2 \dots p_n) = (-1)^n$ si les p_i sont des nombres premiers distincts.
   a) Démontrer que si m, n sont premiers entre eux, on a $\mu(mn) = \mu(m)\mu(n)$.
   b) Soient $(a_n)_{n \in \mathbb{N}^*}$ et $(b_n)_{n \in \mathbb{N}^*}$ des suites de nombres réels. Démontrer que l'on a $a_n = \sum_{d|n} b_d$ pour tout n si et seulement si on a $b_n = \sum_{d|n} \mu(\frac{n}{d}) a_d$ pour tout n.

2. On note Q l'ensemble des polynômes unitaires à coefficients dans $\mathbb{F}_p$ et P l'ensemble des polynômes unitaires irréductibles. On note N_n le nombre de polynômes unitaires irréductibles de degré n.
   a) Démontrer que pour $t \in]-1/p, 1/p[$ on a
   $$\frac{1}{1-pt} = \sum_{A\in Q} t^{\partial A} = \prod_{R\in P} \frac{1}{1-t^{\partial R}} = \prod_{n=1}^{+\infty} (1-t^n)^{-N_n}.$$
   b) Démontrer que $p^n = \sum_{d|n} dN_d$.

   Indication : Prendre le logarithme - ou la dérivée logarithmique.
   c) En déduire que $nN_n = \sum_{d|n} \mu(\frac{n}{d}) p^d$.
   d) Remarquant que n a au plus $\frac{n}{2}$ diviseurs distincts de n tous $\leqslant \frac{n}{2}$, en déduire que $nN_n \geqslant p^{n/2}(p^{n/2} - n/2)$, puis que $N_n > 0$ pour tout $n > 0$.
   e) En déduire l'existence d'un corps à p^n éléments.

3.15 Exercice. *Hyperbole et triangle équilatère.* Dans le plan affine euclidien on considère une hyperbole équilatère H. Notons O son centre de symétrie. Soient P un point de H, P' son symétrique par rapport à O et $\mathcal{C}$ le cercle de centre P et de rayon PP'.

1. Démontrer que $\mathcal{C}$ et H se coupent en quatre points (avec la possibilité que P' soit un point double).
2. On note A, B, C les trois autres points d'intersection de $\mathcal{C}$ avec H. Démontrer que le centre de gravité du triangle ABC est P ; en déduire que c'est un triangle équilatéral.

3.16 Exercice. Soit $P \in K[X]$.

1. Décomposer $\frac{P'}{P}$ en éléments simples.
2. *Théorème de Lucas.* On suppose $K = \mathbb{C}$. Démontrer que l'ensemble des zeros de P' est inclus dans l'enveloppe convexe de l'ensemble des zéros de P.

3.17 Exercice. *Polynômes à racines de module* 1
Soit P un polynôme unitaire à coefficients entiers. Notons $x_1, \ldots, x_n$ les racines de P (comptées avec leur multiplicité).

1. On suppose que pour tout k, on a $|x_k| = 1$.
   a) Soit $\ell \in \mathbb{N}$. Démontrer qu'il existe un polynôme unitaire P_ℓ à coefficients entiers dont les racines sont les x_k^ℓ.
   b) Soit $Q = X^n + \sum_{j=0}^{n-1} a_j X^j$ un polynôme dont toutes les racines sont de module 1. Démontrer que $|a_j| \leqslant C_n^j$.
   c) En déduire qu'il existe ℓ et m tels que tels que $\ell \neq m$ et $P_\ell = P_m$.
   d) Démontrer qu'il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que, pour tout k on ait $x_k^\ell = x_{\sigma(k)}^m$.
   e) En déduire que pour tout $r \in \mathbb{N}$, on a $x_k^{\ell^r} = x_{\sigma^r(k)}^{m^r}$.
   f) Démontrer que toutes les racines de P sont des racines de 1.
2. On suppose que toutes les racines de P sont réelles comprises entre -2 et 2. Démontrer qu'elles sont de la forme $2\cos q\pi$ avec $q \in \mathbb{Q}$. (Considérer un polynôme Q tel que $Q(x) = x^n P(x + 1/x)$).

3. Soit A une matrice symétrique à coefficients entiers de norme < 2. Démontrer que les valeurs propres de A sont de la forme $2\cos q\pi$ avec $q \in \mathbb{Q}$. (*Variante difficile :* ... que $\|A\|$ est de la forme $2\cos \pi/n$).

3.18 Exercice. *Résultant de deux polynômes*
Soit K un corps. Pour $n \in \mathbb{N}$, notons E_n l'espace vectoriel des polynômes de degré $< n$.

Soient $A, B \in K[X]$ des polynômes non nuls. Posons $m = \partial A$ et $n = \partial B$ et écrivons $A = \sum_{k=0}^{m} a_k X^k$, $B = \sum_{k=0}^{n} b_k X^k$. On considère l'application linéaire $f : E_n \times E_m \to E_{m+n}$ définie par $f(P,Q) = AP + BQ$.
Pour $k = 0, \ldots, n-1$, notons C_k la matrice colonne à $n+m$ lignes :

$$C_0 = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad C_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad C_{n-1} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}.$$

De même, pour $k = 0, \ldots, m-1$, notons D_k la matrice colonne à $n+m$ lignes :

$$D_0 = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad D_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad D_{m-1} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

(La matrice C_k commence par k lignes nulles et se termine par $n-1-k$ lignes nulles ; la matrice D_k commence par k lignes nulles et se termine par $m-1-k$ lignes nulles.)

1. Démontrer l'équivalence :
   (i) les polynômes A et B sont premiers entre eux (pour $K = \mathbb{C}$ les polynômes A et B n'ont pas de racine commune) ;
   (ii) l'application f est bijective ;
   (iii) le déterminant $R_{A,B}$ (appelé *résultant* de A et B) de la matrice carrée de colonnes $C_0, \ldots, C_{n-1}, D_0, \ldots$ n'est pas nul.
2. Pour $K = \mathbb{C}$ écrire une relation nécessaire et suffisante pour qu'un polynôme A possède des racines multiples.
3. Applications : calculer le résultant de A et B dans les cas suivant

a) $A = aX^2 + bX + c$ et $B = A'$;

b) $A = X^3 + pX + q$ et $B = A'$;

c) A quelconque $B = X - b$.

3.19 Exercice. On se propose de démontrer le :

Théorème de Sturm. Soit $P \in \mathbb{R}[X]$ un polynôme sans racines multiples dans $\mathbb{C}$. Posons $P_0 = P$, $P_1 = P'$ et pour $k \geqslant 2$, supposant P_{k-2} et P_{k-1} construits, on écrit la division euclidienne de P_{k-2} par P_{k-1} sous la forme $P_{k-2} = Q_k P_{k-1} - P_k$. On note P_m le dernier P_k non nul. Notons A l'ensemble des nombres réels qui sont racine d'un P_k pour $0 \leqslant k \leqslant m$. Pour $x \in \mathbb{R} \setminus A$, notons $n(x)$ le nombre de changements de signes de la suite $P_0(x), P_1(x), \ldots, P_m(x)$, c'est-à-dire le nombre de $i \in \{1, \ldots, m\}$ tels que $P_i(x)$ et $P_{i-1}(x)$ soient de signes contraires. Pour tous $a, b \in \mathbb{R} \setminus A$ tels que $a < b$, le nombre de racines de P dans l'intervalle $[a, b]$ est $n(a) - n(b)$.

1. Démontrer que, pour tout $k < m$, P_k et P_{k+1} sont premiers entre eux. Démontrer que P_m est constant et non nul.
2. Démontrer que l'application $x \mapsto n(x)$ est constante sur tout intervalle contenu dans le complémentaire de A.

   Pour $x \in A$, on note $n_g(x)$ la limite à gauche de n en x et $n_d(x)$ sa limite à droite.
3. Soit x une racine de P_k avec $k > 0$. Démontrer que P_{k-1} et P_{k+1} ne s'annulent pas en x et sont de signes contraires. Démontrer qu'il existe un intervalle ouvert J contenant x tel que, pour $y \in J \setminus \{x\}$, le nombre de changements de signe dans la suite $P_{k-1}(y), P_k(y), P_{k+1}(y)$ soit égal à 1.
4. Démontrer que si $x \in A$ n'est pas racine de $P_0 = P$, alors $n_g(x) = n_d(x)$.
5. Soit x une racine de P. Démontrer que $n_g(x) = n_d(x) + 1$.

   Indication : Les polynômes P et P' ont le même signe à droite de x et des signes contraires à gauche de x.
6. Établir le théorème de Sturm.