Chapitre 19. Arithmétique des polynômes

On fixe un corps K des scalaires.

Rappels :

* On dit que $P \in K[X]$ divise $Q \in K$ s'il existe $R \in K[X]$ tel que $Q = PR$
* Si $z \in K$, on a l'équivalence $P(z) = 0 \iff X - z \mid P$

1 Multiplicité des racines

1.1 Généralités

Définition 1.1. Soit $P \in K[X]$ not nul et $z \in K$ une racine de P
L'ordre de multiplicité de z en tant que racine de P, $\mu_z(P)$ est le plus grand entier $k \in \mathbb{N}^*$ tel que $(X - z)^k \mid P$
On étend cette notion en posant :

* $\mu_z(P) = 0$ si z n'est pas racine de P
* $\mu_z(P) = +\infty$ si P est le polynôme nul.

On dit que z est une racine simple (resp. double, triple, ... , n-uple) si $\mu_z(P) = 1$ (resp. 2, 3, ... , n), multiple si $\mu_z(P) \geq 2$

Lemme 1.2. Soit $P \in K[X]$, $z \in K$ et $n \in \mathbb{N}$
Alors $\mu_z(P) = n$ ss'il existe $P_0 \in K[X]$ tel que $P = (X - z)^n P_0$ et $P_0(z) \neq 0$

Proposition 1.3. Soit $P, Q \in K[X]$ et $z \in K$ On a :

* $\mu_z(P + Q) \geq \min(\mu_z(P),\ \mu_z(Q))$, avec égalité si $\mu_z(P) \neq \mu_z(Q)$
* $\mu_z(PQ) = \mu_z(P) + \mu_z(Q)$

Proposition 1.4. Soit $P \in \mathbb{R}[X]$ et $z \in \mathbb{C}$
On a alors $\mu_z(P) = \mu_{\bar{z}}(P)$

1.2 Critère radical de nullité

Théorème 1.5. Soit $P \in K[X]$, $z_1, ..., z_r \in K$ distincts et $n_1, ..., n_r \in \mathbb{N}$

* Si $\forall i \in [\![1, r]\!]$, $\mu_{z_i}(P) \geq n_i$, alors $\prod\limits_{i=1}^{r} (X - z_i)^{n_i} \mid P$
* Si en outre, $P \neq 0$, on a $\sum\limits_{i=1}^{r} n_i \leq \deg P$
* Si $P \in K[X]$ vérifie $\forall i \in [\![1, r]\!]$, $\mu_{z_i}(P) \geq n_i$ et que $\sum\limits_{i=1}^{r} n_i > n$, alors $P = 0$

1.3 Polynômes scindés

Définition 1.6. Soit $P \neq 0$. Les assertions suivantes sont équivalentes :

(i) Les racines $z_1, ..., z_r$ de P vérifient $\sum\limits_{i=1}^{r} \mu_{z_i}(P) = \deg P$

(ii) Il existe $\lambda \in K$ non nul, $z_1, ..., z_r \in K$ et $n_1, ..., n_r \in \mathbb{N}^*$ tels que $P = \lambda \prod\limits_{i=1}^{r} (X - z_i)^{n_i}$

Quand ces assertions sont vraies, on dit que le polynôme P est scindé.

Théorème 1.7 (Relation coefficients racines, ou formules de Viète)**.** Soit

$$P = \sum_{k=0}^{n} a_k X^k = \prod_{i=1}^{n} (X - z_i)$$

un polynôme scindé unitaire. On a alors

$$\forall k \in [\![1, n]\!],\ a_{n-k} = (-1)^k \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} z_{i_1} \ldots z_{i_k}$$

En particulier,

$$\begin{aligned} a_0 &= (-1)^n z_1 z_2 \ldots z_n && (k = n) \\ a_{n-1} &= -(z_1 + z_2 + \ldots + z_n) && (k = 1) \end{aligned}$$

1.4 Lien avec la dérivée

Théorème 1.8. Soit $P \in K[X]$ et $z \in K$
Alors $\mu_z(P)$ est le plus grand entier k tel que $P(z) = P'(z) = \ldots = P^{(k-1)}(z) = 0$ (k scalaires)

2 Décomposition en facteurs irréductibles

2.1 Polynômes associés

Proposition 2.1.
- On a $K[X]^\times = \{\lambda \mid \lambda \in K^*\}$ (rappel)
- Soit $P, Q \in K[X]$. On a $P \mid Q$ et $Q \mid P$ ssi $\exists \lambda \in K^* : P = \lambda Q$

Dans ce cas, on dit que P et Q sont associés.

2.2 PGCD

Définition 2.2. Soit $P, Q \in K[X]$ non tous deux nuls.
- On définit un PGCD de P et Q comme un diviseur commun à P et Q de degré maximal.
- Le PGCD de P et Q, noté $P \wedge Q$ sera l'unique PGCD unitaire de P et Q.

Théorème 2.3. Soit $P, Q \in K[X]$ deux polynômes non nuls.
Alors il existe $D \in K[X]$ tel que $\{PU + QV \mid U, V \in K[X]\} = \{DW \mid W \in K[X]\}$

Définition 2.4. On dit que I est un idéal de $K[X]$ si :
- I est un sous-groupe de $(K[X], +)$
- On a $\forall R \in I, \forall S \in K[X], RS \in I$

Lemme 2.5. Tout idéal de $K[X]$ est de la forme $DK[X] = \{DW \mid W \in K[X]\}$ pour un certain $D \in K[X]$
(On dit que $K[X]$ est un anneau principal.)

Corollaire 2.6. Soit $P, Q \in K[X]$ et D comme dans le théorème. Alors :

(i) D divise à la fois P et Q : Il suffit de remarquer que $P = P \cdot 1 + Q \cdot 0 \in DK[X]$, et idem pour Q

(ii) D est un multiple de tout diviseur commun Δ de P et Q.
En effet, on peut trouver $U, V \in K[X]$ tels que l'on ait une relation de Bézout : $PU + QV = D$. Comme $\Delta \mid P$ et $\Delta \mid Q$, on doit avoir $\Delta \mid D$. En particulier, $\deg \Delta \leq \deg D$
On en déduit que D est un PGCD de P et Q. En particulier, si Δ est un PGCD de P et Q, on a $\Delta \mid D$ et $\deg \Delta = \deg D$: On en déduit que Δ et D sont associés.

2.3 Lemme de Gauss et conséquences

Théorème 2.7 (Lemme de Gauss)**.** Soit $P, Q, R \in K[X]$
Si $P \mid QR$ et $P \perp Q$, alors $P \mid Q$

Corollaire 2.8.
- Soit $P \in K[X]$. L'ensemble des polynômes premiers avec P est stable par produit.
- Soit $P, Q \in K[X]$ premiers entre eux et $n, m \in \mathbb{N}$. Alors P^n et Q^m sont premiers entre eux.

2.4 Polynômes irréductibles

Définition 2.9. Un polynôme $P \in K[X]$ non constant est dit irréductible si
$\forall Q, R \in K[X], P = QR \implies \deg Q = 0$ ou $\deg R = 0$

2.5 Décomposition en facteurs irréductibles

Théorème 2.10. Soit $P \in K[X]$ non nul.
Alors il existe $u \in K[X]$, $Q_1, ..., Q_r \in K[X]$ irréductibles distincts et $\alpha_1, ..., \alpha_r \in \mathbb{N}^*$ tels que

$$P = u \prod_{i=1}^{r} Q_i^{\alpha_i}$$

Par ailleurs, cette décomposition est unique : Si

$$P = u \prod_{i=1}^{r} Q_i^{\alpha_i} = v \prod_{j=1}^{s} R_j^{\beta_j}$$

sont deux telles décompositions, on a $u = v$, $r = s$, et, quitte à permuter les R_j,
on a $\forall i \in [\![1, r]\!], (Q_i = R_i$ et $\alpha_i = \beta_i)$

3 Quelques corps particuliers

3.1 $\mathbb{C}$

Théorème 3.1 (D'Alembert-Gauss)**.** Tout polynôme de $\mathbb{C}[X]$ possède une racine.

Corollaire 3.2.
- Tout polynôme non nul de $\mathbb{C}[X]$ est scindé.
- Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.
- Deux polynômes $P, Q \in \mathbb{C}[X]$ sont premiers entre eux ss'ils n'ont pas de racine commune.

3.2 Polynômes minimaux des nombres algébriques

On fixe une extension de corps L/K. (Par exemple, $K = \mathbb{Q}$ ou $K = \mathbb{R}$ et $L = \mathbb{C}$)

Définition 3.3. Un élément $x \in L$ est dit algébrique sur K s'il est racine d'un certain polynôme non nul $P \in K[X]$. Il est transcendant sur K sinon.

Proposition 3.4. Soit $z \in L$ algébrique sur K. Alors il existe un unique polynôme unitaire $P \in K[X]$ tel que :
- $P(z) = 0$
- $\forall Q \in K[X], Q(z) = 0 \implies P \mid Q$

Ce polynôme P est irréductible dans $K[X]$. On l'appelle le polynôme minimal de z (sur K).

3.3 $\mathbb{R}$

Dans toute cette section, si $z \in \mathbb{C} \setminus \mathbb{R}$, on note

$$P_z = (X - z)(X - \bar{z}) = X^2 - 2\text{Ré}(z)X + |z|^2$$

son polynôme minimal. Il est irréductible :

* D'après la proposition générale de la section 2.
* Variant : si P_z admettait une décomposition $P_z = QR$, où $\deg Q, \deg R \geq 1$. On aurait $\deg Q = \deg R = 1$ donc Q et R auraient des racines réelles et donc P aussi, ce qui n'est pas.

Les polynômes de second degré à discriminant < 0 sont exactement les uP_z, pour $u \in \mathbb{R}^*$ (un tel polynôme a forcément z et $\bar{z}$ comme racines).

Théorème 3.5. Les polynômes irréductibles sur $\mathbb{R}$ sont :

* Les polynômes de degré 1.
* Les polynômes du seconde degré à discriminant < 0.

Corollaire 3.6. Tout polynôme de $\mathbb{R}[X]$ possède une décomposition en facteurs irréductibles

$$P = u \prod_{i=1}^{r} (X - t_i)^{\alpha_i} \prod_{j=1}^{s} P_{z_j}^{\beta_j}$$

où :

* u est le coefficient dominant de P.
* Les t_i sont les racines de P et les α_i leur multiplicités.
* Les z_i sont les racines de P dans le demi-plan $\mathbb{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$ et $\beta_j = \mu_{z_j}(P) = \mu_{\bar{z}_j}(P)$

Proposition 3.7 (Hors programme mais à savoir faire absolument)**.** Soit $P \in \mathbb{R}[X]$ non constant.

* Si P est <u>simplement scindé</u> (scindé et toutes ses racines sont simples), alors P' aussi.
* Si P est scindé, P' aussi.

3.4 $\mathbb{Q}$ (hors-programme)

On va montrer qu'il existe des irréductibles de tout degré dans $\mathbb{Q}[X]$.

Lemme 3.8 (Gauss)**.** Soit $P \in \mathbb{Z}[X]$
On suppose que toute décomposition $P = QR$, où $Q, R \in \mathbb{Z}[X]$ est triviale (càd $\deg P = 0$ ou $\deg Q = 0$).
Alors P est irréductible dans $\mathbb{Q}[X]$.

Théorème 3.9 ("critère" d'Eisenstein)**.** Soit $P \in \mathbb{Z}[X]$ unitaire de degré $d \in \mathbb{N}^*$ et p un nombre premier tel que :

* On a $\forall k \in [\![0, d-1]\!]$, $p \mid \text{coeff}_k(P)$
* On a $p^2 \nmid \text{coeff}_0(P) = P(0)$

Alors P est irréductible dans $\mathbb{Q}[X]$