# Le théorème fondamental de l'algèbre

**Leçons**

**125** (ex) Extensions de corps. Exemples et applications.

**142** (dev) Algèbre des polynômes à plusieurs indéterminées.

**144** (dev) Racines d'un polynôme. Polynômes symétriques élémentaires

**Source** Pierre Samuel [Sam67, P.53]. Attention coquille, $y_j$ à la place de $x_j$.

**Pré-requis**

1. Théorème des polynômes symétriques.
2. L'équation de degré 2 dans $\mathbb{C}$.
3. Théorème des valeurs intermédiaires.

---

**Théorème 1.** *Soit $P \in \mathbb{C}[X]$ non constant. Alors $P$ admet une racine dans $\mathbb{C}$.*

---

Soit $P \in \mathbb{C}[X]$ unitaire. On procède par récurrence sur la valuation 2-adique du degré de $P$.

**(a) Coefficients réels.** On introduit un nouveau polynôme $F \in \mathbb{C}[X]$ par

$$F(X) = P(X)\,\overline{P}(X).$$

Alors $F = \overline{F}$ et donc $F \in \mathbb{R}[X]$ (la sous-$\mathbb{R}$-algèbre des invariants) ; par ailleurs si $F$ possède une racine complexe $\rho$, alors $\rho$ ou $\overline{\rho}$ est racine de $P$. On supposera donc $P$ à coefficients réels dans la suite.

**(b) Initialisation : degré impair** Soit $P \in \mathbb{R}[X]$ de degré impair, $\widetilde{P}$ la fonction polynômiale associée. Alors $\widetilde{P}$ est continue sur $\mathbb{R}$, de limite $-\infty$ (resp. $+\infty$) en $-\infty$ (resp. $+\infty$). D'après le théorème des valeurs intermédiaires, $\widetilde{P}$ s'annule et $P$ possède une racine réelle.

**(c) Un polynôme auxiliaire** Ecrivons $\deg P = d = 2^n q$ avec $q$ impair (une telle écriture est unique). Pour tout $c \in \mathbb{Z}$, posons

$$G_c(X_1, \dots X_d, X) = \prod_{1 \leqslant i \leqslant j \leqslant d} (X - X_i - X_j - cX_iX_j).$$

Alors $G_c \in \mathbb{Z}[X_1, \dots X_d]^{\mathfrak{S}_d}[X]$. D'après le théorème des polynômes symétriques, on a donc

$$G_c \in \mathbb{Z}[\sigma_1, \dots \sigma_d][X].$$

En particulier, si $x_1, \dots x_d$ sont les racines de $P$ (éventuellement non distinctes) dans un corps de décomposition $K$ de $P$ sur $\mathbb{C}$,

$$\begin{aligned} G_c(x_1, \dots x_d, X) &\in \mathbb{Z}[\sigma_1(x_1, \dots x_d), \dots \sigma_d(x_1, \dots x_d)][X] \\ &= \mathbb{Z}[a_{d-1}, \dots a_0][X] \\ &\subseteq \mathbb{R}[X]. \end{aligned}$$

**(d) Réduction de degré** Le degré en $X$ de $G_c$ est

$$\deg_X G_c = \frac{d(d+1)}{2} = 2^{n-1} q (d+1).$$

Par hypothèse de réccurence, $G_c(x_1, \dots x_d, X)$ possède une racine $z$ dans $\mathbb{C}$, pour tout $c \in \mathbb{Z}$. Il s'agit de l'un des $y_{ij}(c) = x_i + x_j + cx_ix_j$ ; notons le $y_{i(c)j(c)}(c)$. Puisque $\mathbb{Z}$ est infini, il existe $c$ et $c'$ distincts dans $\mathbb{Z}$ tels que

$$\begin{aligned} i(c) &= i(c') = r \\ j(c) &= j(c') = s. \end{aligned}$$

On sait alors que $y_{rs}(c)$ et $y_{rs}(c')$ sont dans $\mathbb{C}$. Par conséquent, la somme et le produit de $x_r$ et $x_s$ sont dans $\mathbb{C}$. Or $x_r$ et $x_s$ sont racines de

$$X^2 - (x_r + x_s) X + x_r x_s,$$

et tout polynôme de degré 2 à coefficients complexes admet [1] une racine dans $\mathbb{C}$. Conclusion, $x_r$ et $x_s$ sont dans $\mathbb{C}$.

---

*Remarque* 2. La preuve qu'on présente ici peut être retracée jusqu'à Lagrange en 1772. Voir [Suz06] pour sa place dans l'histoire du théorème fondamental de l'algèbre. La seule objection de Gauss concernait le lieu a priori des racines ; avec le point de vue de l'algèbre moderne ce n'est plus un problème.

*Remarque* 3 (Ariles Remaki). On a utilisé l'axiome du choix (à cause du choix des $z_c$) si on veut l'éviter on fait simplement varier $c$ dans un ensemble fini assez grand pour appliquer le principe des tiroirs.

1. En caractéristique $\neq 2$ rajouter simplement une racine de $-1$ (i.e. se placer dans le corps de rupture de $X^2 + 1$) suffit pour résoudre toutes les équations du second degré. Attention, la réduction aux coefficients réels du (a) n'est pas susceptible de s'appliquer ici puisqu'elle double le degré.

**Applications du théorème fondamental de l'algèbre** On mentionne les applications directes de l'énoncé « minimaliste » (existence d'une racine)

— (Algèbre linéaire) Soit $E$ un $\mathbb{C}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$. Alors $u$ admet un vecteur propre.

— (Géométrie) Soit $\mathcal{F}$ un faisceau de quadriques complexe. Alors une quadrique de $\mathcal{F}$ au moins est dégénérée.

— (Groupes) $\mathbb{C}^\times$ est un groupe divisible (pour tout $Z \in \mathbb{C}^\times$, pour tout $n \in \mathbb{N}$, il existe $z \in \mathbb{C}^\times$ tel que $Z = z^n$) ; sans requérir l'exponentielle complexe. Ceci permet notamment le lemme de prolongement des caractères.

**Autres applications du théorème des polynômes symétriques**

— Dans le lemme de Kronecker (voir le développement **??**)

— Polynômes palindromiques (voir le développement **??**)

— Soit $f : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}$ une fonction polynômiale telle que $f(AB) = f(BA)$ pour toutes $A, B \in \mathcal{M}_n(\mathbb{C})$. Alors $f$ est un polynôme en les coefficients de $\chi_-$.

## Références

[Sam67] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

[Suz06] Jeff Suzuki. Lagrange's proof of the fundamental theorem of algebra. *The American Mathematical Monthly*, 113(8) :705–714, 2006.