Corps, Anneaux, Algèbres

Jean Ludwig

1 Définitions basiques.

Définition 1.1. Un *corps* est un ensemble K muni de deux lois internes $(+, \cdot)$

$$K \times K \to K;\ (a, b) \mapsto a + b,$$

$$K \times K \to K;\ (a, b) \mapsto a \cdot b,$$

vérifiant les axiomes suivants.

1. $(K, +)$ est un groupe commutatif.
2. Soit 0 l'élément neutre de $(K, +)$ et soit $K^* = K \setminus \{0\}$. $(K^*, \cdot)$ est un groupe commutatif.
3.

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad \text{a, b, c } \in K.$$

Définition 1.2. Un *anneau* est un ensemble A muni de deux lois internes $(+, \cdot)$ tels que

1. $(A, +)$ est un groupe abélien
2. la multiplication est associative, c. à d.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),\ \forall a, b, c \in A.$$

3. La multiplication est distributive par rapport à l'addition, c. à d.

$$a \cdot (b + c) = a \cdot b + a \cdot c,\ \forall a, b, c \in A$$

Définition 1.3. On dit que l'anneau $(A, +, \cdot)$ est *commutatif*, si $a \cdot b = b \cdot a$ pour tout $a, b \in A$.

Définition 1.4. Nous disons que l'anneau $(A, +, \cdot)$ est *unitaire*, s'il existe un élément $\mathbb{I}$ dans A, tel que

$$\mathbb{I} \cdot a = a \cdot \mathbb{I},\ a \in A.$$

Définition 1.5. Un espace vectoriel sur un corps K est un groupe commutatif $(E, +)$ muni d'une loi externe

$$K \times E \to E;\ (\lambda, x) \mapsto \lambda \cdot x,$$

telle que pour tout $\lambda, \mu \in K$, $x, y \in E$,

1. $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$,
2. $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$
3. $(\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x)$.
4. $1_K \cdot x = x$

Proposition 1.6. *1. Un corps possède au moins deux éléments.*

2. Soit 0_A le "zéro" de l'anneau A. Alors

$$0_A \cdot x = x \cdot 0_A = 0_A,\ \forall x \in A.$$

3. *Si A est unitaire, alors*
$$(-\mathbb{I})\cdot x = -x,\ \forall x \in A.$$

Démonstration. 1. En effet, pour $x \in A$,
$$0_A \cdot x + 0_A \cdot x = (0_A + 0_A)\cdot x = 0_A \cdot x,$$
donc $0_A \cdot x = 0_A$. De même pour $x \cdot 0_A = 0_A$.

2. En effet,
$$x + (-\mathbb{I})\cdot x = \mathbb{I}\cdot x + (-\mathbb{I})\cdot x = (\mathbb{I}-\mathbb{I})\cdot x = 0_A \cdot x = 0_A.$$
Ainsi $(-\mathbb{I})\cdot x$ est l'opposé de x.

□

Proposition 1.7. *Soit E un K-espace vectoriel. Alors pour tout $x \in E, \lambda \in K$,*
$$0_K \cdot x = 0_E,\ (-1_K)\cdot x = -x,\ \lambda \cdot 0_E = 0_E.$$

Exemple 1.8. 1. L'ensemble $(\mathbb{Z}, +, \cdot)$ est un anneau unitaire commutatif.
2. L'ensemble $(\mathbb{Q}, +, \cdot)$ est un sous-corps du corps $(\mathbb{R}, +, \cdot)$.
3. L'ensemble $(\mathbb{R}, +, \cdot)$ est un sous-corps du corps $(\mathbb{C}, +, \cdot)$.
4. l'ensemble $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ muni de l'addition
$$(a,b) + (a',b') = (a+a', b+b')$$
et de la multiplication
$$(a,b)\cdot(a',b') = (aa' - bb', ab' + a'b),\ (a,b),(a',b') \in C.$$
On vérifie que la multiplication est associative et distributive par rapport à l'addition, que
$$(1,0)\cdot(a,b) = (a,b)\cdot(1,0) = (a,b),\ \forall (a,b) \in C,$$
que pour $(a,b) \neq (0,0)$,
$$(a,b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = (1,0) = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)\cdot(a,b).$$
En outre
$$(0,1)\cdot(0,1) = -(1,0) = -1_{\mathbb{C}}.$$
Posons
$$(0,1) = i,\ (1,0) = 1$$
et pour $x \in \mathbb{R}$, $(a,b) \in C$,
$$x(a,b) = (x,0)\cdot(a,b) = (xa, xb).$$
Alors
$$(a,b) = (a,0) + (0,b) = a(1,0) + b(0,1) = a + bi.$$

Définition: Pour $(a,b) = a + bi \in \mathbb{C}$, appelons *conjugué* de (a,b) le nombre complexe
$$\overline{(a,b)} = (a,-b) = a - bi.$$
Alors pour $z = a + bi, z' = a' + b'i \in \mathbb{C}$, on a que
$$\overline{(z+z')} = \overline{z} + \overline{z'},\ \overline{z\cdot z'} = \overline{z}\cdot\overline{z'}.$$

(la conjugaison $z \mapsto \overline{z}$ est donc un automorphisme de $\mathbb{C}$).

Soit

$$h : \mathbb{R} \to \mathbb{R};\ h(x) = (x, 0).$$

On constate que

$$h(x+y) = h(x) + h(y),\ h(xy) = h(x) \cdot h(y),\ x, y \in \mathbb{R},$$

et que h est injectif. Donc h est un isomorphisme de $\mathbb{R}$ sur son image dans $\mathbb{C}$. Nous pouvons donc identifier le corps $\mathbb{R}$ avec le sous-corps $\mathbb{R} \times \{0\}$ de $\mathbb{C}$.

Définition 1.9. Un *homomorphisme* d'un anneau A dans un anneau B est une application telle que

$$h(a+b) = h(a) + h(b),$$
$$h(a \cdot b) = h(a) \cdot h(b),\ a, b \in A.$$

Définition 1.10. Soit A un anneau. Un sous-anneau B de A est sous-groupe de A, tel que

$$a \cdot b \in B,\ \forall a, b \in B.$$

Soit A un anneau *commutatif.* Nous disons que la partie I de A est un *idéal* de A, si I est un sous-groupe de $(A, +)$ et si

$$a \cdot b \in I,\ \forall a \in A, b \in B.$$

Exemple 1.11. nous prenons $x \in A$ et nous posons

$$I[x] = \{bx,\ b \in A\}.$$

On vérifie facilement, que $I[x]$ est un idéal de A. Si A est unitaire alors $x = \mathbb{I}_A \cdot x \in I$. Ces idéaux sont appelés idéaux *principaux* de A.

Proposition 1.12. *Soit $h : A \to B$ un homomorphisme d'anneau et suposons A commutatif. Alors $ker(h)$ est un idéal de A.*

Démonstration. Nous savons déjà que $\ker(h)$ est un sous-groupe de A. Soient $a \in A$ et $b \in \ker(h)$. Alors

$$h(a \cdot b) = h(a) \cdot h(b) = h(a) \cdot 0_B = 0_B.$$

Ainsi $a \cdot b \in \ker(h)$ et donc $\ker(h)$ est bien un idéal de A. □

2 Les polynômes

Définition 2.1. Soit K un corps. Nous appelons *polynôme* à coefficients dans K toute suite

$$P = (a_0, a_1, \cdots, a_j, \cdots)$$

dans K tel que a_j=0, pour j assez grand.

Nous appelons degré d'un polynôme $P \neq 0$ le plus grand indice d, tel que

$$a_d \neq 0.$$

Le degré du polynôme $P = 0 = (0, 0 \cdots, 0, \cdots)$ est par définition égal à $-\infty$. Le degré de P se note

$$\deg(P).$$

Définition 2.2. Nous écrivons $K[X]$ pour l'ensemble des polynômes à coefficients dans K. Soit $P = (a_j)_j \in K[X]$. Nous appelons le nombre a_j le j-ième coefficient de P et nous le notons parfois par le symbole

$$a_j = P(j),\ j \in \mathbb{N}.$$

Ainsi deux polynômes P, Q sont égaux, si et seulement si tous leurs coefficients coïncident.

Définition 2.3. Nous définissons la somme de deux polynômes $P = (a_j)$ et $Q = (b_j)$ par

$$P + Q = (a_0 + b_0, a_1 + b_1 \cdots, a_j + b_j, \cdots).$$

Nous définissons le produit $(c_j)_j = R = P \cdot Q$ de P par Q de la façon suivante,

$$c_j = \sum_{k+l=j} a_k b_l = \sum_{k=0}^{j} a_k b_{j-k},\ j \in \mathbb{N}.$$

En particulier

$$c_0 = a_0 b_0,\ c_1 = a_0 b_1 + a_1 b_0.$$

Remarque 2.4. Nous remarquons que le polynôme

$$1 = (1, 0, 0 \cdots, 0, \cdots)$$

est un élément unité pour le produit des polynômes :

$$1 \cdot P = P.$$

En effet,

$$1 \cdot P(j) = \sum_{k=0}^{j} 1(k) P(j-k) = \underbrace{1(0)}_{1} P(j) + \underbrace{1(1)}_{0} P(j-1) + \cdots$$
$$= P(j),\ j \in \mathbb{N}.$$

Proposition 2.5. *Le produit des polynômes est associatif.*

Démonstration. En effet, si P, Q, R sont des polynômes à coefficients dans K, alors pour $j \in \mathbb{N}$

$$P \cdot (Q \cdot R)(j) = \sum_{k+l=j} P(k)(Q \cdot R)(l)$$

$$= \sum_{k+l=j} P(k)\Big(\sum_{m+n=l} Q(m)R(n)\Big)$$

$$= \sum_{k+m+n=j} P(k)Q(m)R(n)$$

$$= \sum_{l+n=j} \left(\sum_{k+m=l} P(k)Q(m)\right) R(n)$$

$$= \sum_{l+n=j} (P \cdot Q)(l)R(n) = (P \cdot Q) \cdot R(j).$$

Ainsi

$$P \cdot (Q \cdot R) = (P \cdot Q) \cdot R.$$

□

Définition 2.6. Nous avons une loi naturelle externe :

$$K \times K[X] \to K[X];\ (\lambda, P) \mapsto \lambda P,$$

où

$$(\lambda P)(j) = \lambda(P(j)),\quad \text{c. à d. } \lambda P = (\lambda a_0, \lambda a_1, \cdots, \lambda a_j, \cdots).$$

Définition 2.7. Une *algèbre* sur un corps K est un K-espace vectoriel A qui est en même temps un anneau tel que pour tout $\lambda \in K, a, b \in A$ on ait

$$\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b) \tag{2.1}$$

On vérifie facilement que

Proposition 2.8. *L'ensemble $K[X]$ muni de l'addition, du produit interne et de la loi externe définis en haut est une K-algèbre.*

et que

Proposition 2.9. *Pour tout polynômes $P, Q \in K[X]$ on a*

$$deg(P+Q) \leq \max(\deg P, \deg Q),\ \deg P \cdot Q = \deg P + \deg Q.$$

En effet , nous pouvons supposer que $p = \deg P \geq \deg Q = q$ et donc

$$P + Q = (P(0) + Q(0), P(1) + Q(1), \cdots, P(q) + P(q),$$

$$\cdots, P(d) + Q(d), 0, \cdots).$$

Ainsi $\deg(P+Q) \leq p = \max(\deg P, \deg Q)$. D'autre part, pour $j = p + q$ nous avons que

$$P \cdot Q(p+q) = \sum_{k+l=p+q} P(k)Q(l) = \sum_{k=0}^{p+q} P(k)Q(p+q-k)$$

$$= \sum_{k=0}^{p} P(k)Q(p+q-k)$$

$$= 0 + P(p)Q(p+q-p) = P(p)Q(q) \neq 0.$$

Pour $j > p + q$ nous avons

$$P \cdot Q(j) = \sum_{k=0}^{p} P(k)Q(j-k) = \sum_{k=0}^{p} P(k)0 = 0,$$

car $j - k > p + q - p = q$ et donc $Q(j-k) = 0$, pour $k \leq p$. Ainsi

$$\deg P \cdot Q = \deg P + \deg Q.$$

□

Définition 2.10. Soit X le polynôme dans $K[X]$ défini par

$$X = (\delta_{1,j})_j = (0, 1, 0, \cdots, 0, \cdots)$$

Ici $\delta_{i,j}$ désigne le symbole de Kronecker

$$\delta_{i,j} = \begin{cases} 0 & \text{si } j \neq i \\ 1 & \text{si } i = j \end{cases}$$

X s'appelle l'indéterminée.

Proposition 2.11. *Pour chaque $n \in \mathbb{N}$, X^n est alors le polynôme*

$$X^n = (\delta_{n,j})_j = (0, 0, \cdots, 0, 1, 0 \cdots)$$

où 1 apparaît à la position n.

Démonstration. Par récurrence sur n, on a

$$X^{n+1}(j) = X^n \cdot X(j) = \sum_{k=0}^{j} \delta_{1,k}\delta_{n,j-k}$$

$$= 0 + \delta_{n,j-1}.$$

Ainsi

$$X^{n+1}(j) = \begin{cases} 0 & , \text{ si } j \neq n+1 \\ 1 & , \text{ si } j = n+1. \end{cases}$$

Donc $X^{n+1} = (\delta_{n+1,j})_j$. □

Remarque 2.12. Soit $P = (a_j)_j \in K[X]$ de degré d. Alors

$$P = (a_0, a_1, \cdots, a_j, \cdots, a_d, 0, \cdots)$$

$$= a_0(\delta_{0,j})_j + a_1(\delta_{1,j})_j + \cdots + a_d(\delta_{d,j})_j$$

$$= a_0 + a_1 X + \cdots + a_d X^d$$

$$= \sum_{j=0}^{d} a_j X^j,$$

si nous posons encore

$$X^0 = 1 = (\delta_{0,j})_j.$$

Tout polynôme s'écrit donc de façon unique comme

$$P = \sum_{j}^{\infty} a_j X^j,$$

où $a_j = 0$ pour $j > \deg P$.

Proposition 2.13. *(Division euclidienne dans $K[X]$) Soit K un corps et P, Q des polynômes sur K, $Q \neq 0$. Il existe des polynômes A, R déterminés de façon unique, tels que*

$$P = AQ + R, \ \deg R < \deg Q.$$

Démonstration. Unicité : S'il existe un autre couple (A', R') vérifiant

$$P = A'Q + R', \ \deg R' < \deg Q,$$

alors

$$(A - A')Q = R - R'.$$

Or si $A - A' \neq 0$, alors $\deg(R - R') = \deg(A - A')Q \geq \deg Q$ et donc

$$\deg Q \leq \deg(R - R') \leq \max(\deg R, \deg R') < \deg Q,$$

ce qui est absurde. Existence : Si $P = 0$, on a $A = 0 = R$. Si $\deg P < \deg Q$, on a

$$A = 0, \ R = P.$$

Si $\deg P \geq \deg Q$, on a

$$P = \sum_{j=0}^{m} a_j X^j,\ Q = \sum_{j=0}^{n} b_j X^j,$$

avec $m = \deg P \geq \deg Q = n$. Alors

$$\begin{aligned} & P - \frac{a_m}{b_n} X^{m-n} Q \\ &= a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0 \\ &- \frac{a_m}{b_n} X^{m-n} (b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0) \\ &= c_{m-1} X^{m-1} + \cdots + c_0 = S. \end{aligned}$$

Donc si nous procédons par récurrence sur m

$$P - \frac{a_m}{b_n} X^{m-n} Q = S = A'Q + R',\ \deg R' < \deg Q,$$

Donc

$$P = \frac{a_m}{b_n} X^{m-n} Q + A'Q + R' = AQ + R,$$

où $A = \frac{a_m}{b_n} X^{m-n} + A',\ R = R'$. □

Théorème 2.14. *Tout idéal I de $K[X]$ est principal, c. à d. de la forme*

$$I = I(P) = K[X]Q$$

pour un certain $Q \in K[X]$.

Démonstration. Soit I un idéal de $K[X]$. Si $I = \{0\}$, alors

$$I = K[X] \cdot 0.$$

Sinon, il existe un élément Q non nul dans I de degré *minimal*. Alors

$$K[X] \cdot Q \subset I.$$

Soit $P \in I$. Ecrivons

$$P = AQ + R,\ \deg R < \deg Q.$$

Comme alors $R = P - AQ \in I$, nous devons avoir $R = 0$ par la minimalité du degré de Q. Ainsi $P = AQ \in K[X] \cdot Q$. □

Remarque:

L'élément Q qui engendre I est unique à un facteur multiplicatif non nul de K près. En effet si

$$K[X]Q = I = K[X]Q,'$$

on a

$$Q = BQ',\ Q' = CQ,$$

pour certains $C, B \in K[X]$ et alors

$$Q = BCQ$$

ce qui implique que $\deg BC = 0$ et donc $B, C \in K$.

Définition: Nous disons qu'un polynôme P est *unitaire* si

$$P = a_0 + a_1 + \cdots + a_{d-1} X^{d-1} + X^d,$$

c. à d. si son coefficient de plus haut degré vaut 1.

19 Définition: Nous disons qu'un polynôme Q divise un polynôme P s'il existe $A \in K[X]$ tel que

$$P = AQ.$$

□

Définition 2.15. (le p.g.c.d.) Soit $A_1, \cdots, A_n$ une famille finie de polynômes non tous nuls. Soit

$$J = J(A_1, \cdots, A_n) = K[X]A_1 + \cdots + K[X]A_n$$

l'idéal engendré par les A_i. Alors

$$J = K[X]D$$

pour un polynôme $D \neq 0$ unitaire unique. Alors $A_i = S_i D$, pour tout i ($S_i \in K[X]$), et D est donc un diviseur commun de tous les A_i. Si le polynôme E divise tous les A_i, alors E divise tous les élément s de J et donc aussi D. Ainsi D est le diviseur commun de plus haut degré de la famille $(A_1, \cdots, A_n)$. Nous disons que D est le p.g.c.d. de cette famille de polynômes.

Définition 2.16. On dit que les polynômes $A_1, \cdots, A_n$ sont *premiers entre eux dans leur ensemble* si le p.g.c.d. est une constante non nulle.

Théorème 2.17. *(Bezout) Pour que les polynômes $A_1, \cdots, A_n$ soient premiers entre eux dans leur ensemble, il faut et il suffit qu'il existent des polynômes $U_1, \cdots, U_n$, tels que*

$$\sum_{i=1}^{n} U_i P_i = 1.$$

Démonstration. Si les A_i sont premiers entre eux dans leur ensemble, alors

$$J = J(A_1, \cdots, A_n) = K[X] \cdot 1 = K[X]$$

ce qui implique que la constante 1 est dans J et donc pour tout i il existe $U_i \in K[X]$, tels que

$$\sum_{i=1}^{n} U_i A_i = 1.$$

Réciproquement si

$$\sum_{i=1}^{n} U_i A_i = 1$$

pour certains U_i, alors $1 \in J(A_1, \cdots, A_n)$. Donc

$$J(A_1, \cdots, A_n) = K[X] = K[X] \cdot 1$$

et 1 est le p.g.c.d des A_i, qui sont alors premiers entre eux. □

Théorème 2.18. *Soit $n \in \mathbb{N}^*$.*

- *a_n) Si le polynôme C divise le produit $A_1 A_2 \cdots A_n$ et s'il est premier avec chacun des polynômes $A_1, \cdots, A_{n-1}$, alors C divise A_n.*
- *b_n) Si les polynômes $A_1, A_2, \cdots, A_n$ sont premiers entre eux deux à deux et si le polynôme C est divisible par chacun d'eux, alors C est divisible par leur produit.*
- *c_n) Si le polynôme A est premier avec chacun des polynômes $B_1, \cdots, B_n$, alors A est premier avec le produit $B_1 \cdots B_n$.*

Démonstration. (récurrence sur n.) $n = 2$. a_2)

$$A_1A_2 = LC,\ UA_1 + VC = 1.$$

Donc

$$UA_1A_2 + VA_2C = A_2.$$

Ainsi

$$(LU + VA_2)C = LCU + VA_2C = A_2.$$

b_2)On a

$$C = L_1A_1,\ C = L_2A_2,\ U_1A_1 + U_2A_2 = 1.$$

Donc

$$C = CU_1A_1 + CU_2A_2 = L_2A_2U_1A_1 + L_1A_1U_2A_2$$
$$= (L_2U_1 + L_1U_1)A_1A_2.$$

Donc A_1A_2 divise C. c_2)On a

$$U_1A + V_1B_1 = 1,\ U_2A + V_2B_2 = 1.$$

Ainsi

$$1 = (U_1A + V_1B_1)(U_2A + V_2B_2)$$
$$= (U_1U_2A + U_1V_1B_2 + V_1U_2B_1)A + V_1V_1(B_1B_2).$$

Supposons les formules vraies pour tout $2 \leq n' < n$. a_n) Donc si C est premier avec $A_1, \cdots, A_{n-1}$, C est, d'après c_{n-1}, premier avec $A_1 \cdots A_{n-1}$ et comme C divise $(A_1 \cdots A_{n-1})A_n$, C divise A_n d'après a_2. b_n) C est divisible par $A_1 \cdots A_{n-1}$ d'après b_{n-1}, d'autre part A_n est premier avec $A_1 \cdots A_{n-1}$, donc C est divisible par $(A_1 \cdots A_{n-1})A_n$ d'après b_2. c_n) A est premier avec $B_1 \cdots B_{n-1}$ d'après c_{n-1}, A est premier avec A_n, donc A est premier avec $(A_1 \cdots A_{n-1})A_n$, d'après c_2. □

Définition 2.19. Un polynôme de degré ≥ 1 est dit *irréductible*, si les seuls diviseurs de P sont P et 1(à des facteurs multiplicatifs constants non nul près)

Exemple 2.20. Nous avons les trois exemples suivants :

1. Les polynômes linéaires $P = X - \lambda,\ \lambda \in K$, sont irréductibles
2. le polynôme $P = X^2 + bX + c \in \mathbb{R}[X]$ est irréductible si et seulement si le discriminant $b^2 - 4c$ est strictement négatif. En effet, si P n'est pas irréductible si et seulement si P admet un diviseur non trivial, donc un diviseur de degré 1, c. à d. $P = (X - \alpha)(X - \beta)$ pour certains $\alpha, \beta \in \mathbb{R}$. Ceci est équivalent à dire que $b^2 - 4c \geq 0$.
3. $P = X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$.

Théorème 2.21. *Tout polynôme $A \in K[X]$ de degré > 0 possède un diviseur irréductible.*

Démonstration. Soit $\mathcal{D}$ l'ensemble des diviseurs de degré ≥ 1 de A. Alors $A \in \mathcal{D}$, donc $\mathcal{D}$ n'est pas vide. Soit $P \in \mathcal{D}$ de degré minimum. Si P n'est pas irréductible alors $P = QR$ avec $\deg P > \deg Q \geq 1$. Alors Q divise aussi A, donc $Q \in \mathcal{D}$, ce qui est impossible à cause de la minimalité du degré de P. □

Notation : Soit $(P_i)_{i \in I}$ la famille des polynômes irréductibles de $K[X]$, indexés arbitrairement (mais de façon que $P_i \neq P_j$ si $i \neq j$.)

Exemple 2.22. Nous verrons que tous les polynômes irréductibles dans $\mathbb{C}[X]$ sont linéaires. Nous pouvons donc indexer les polynômes irréductibles unitaires par les élément s de $\mathbb{C}$.

$$P_\alpha = X - \alpha,\ \alpha \in \mathbb{C}.$$

Théorème 2.23. *Soit P un élément non nul de $K[X]$. Alors P se met de manière unique sous la forme*

$$P = \lambda \prod_{i \in I} P_i^{\alpha_i},$$

où $\lambda \in K$ et où les α_i sont des entiers ≥ 0, nuls sauf pour un nombre fini d'indices.

Démonstration. Si $\deg P = 0$, alors $P = \lambda \prod_{i \in I} P_i^0$. Soit $n > 0$. Supposons le théorème établi pour les polynômes de degré $< n$. Nous savons (voir (25)) que $P = LP_{i_0}$ pour un certain $i_0 \in I$. Comme $\deg L < \deg P$ on a que

$$L = \lambda \prod_{i \in I} P_i^{\alpha_i'},$$

donc

$$P = \lambda \prod_{i \in I} P_i^{\alpha_i}$$

avec

$$\alpha_i = \begin{cases} \alpha_i' & \text{pour } i \neq i_0 \\ \alpha_{i_0'} + 1 & \text{pour } i = i_0 \end{cases}$$

Si

$$P = \lambda \prod_{i \in I} P_i^{\alpha_i} = \mu \prod_{i \in I} P_i^{\beta_i},$$

alors $\beta_i = 0$ entraîne que P_i est premier avec P, car P_i est premier avec P_j^α pour tout $j \neq i$ ($\alpha \in \mathbb{N}$). Donc $\alpha_i = 0$. Ainsi $\alpha_i = 0$ si et seulement β_i. Comme $\alpha_{i_0} \neq 0$ on a aussi que $\beta_{i_0} \neq 0$. Divisons P par P_{i_0}. L'hypothèse de récurrence appliquée à

$$P/P_{i_0} = \lambda P_{i_0}^{\alpha_{i_0}-1} \prod_{i \in I, i \neq i_0} P_i^{\alpha_i} = \mu P_{i_0}^{\beta_{i_0}-1} \prod_{i \in I, i \neq i_0} P_i^{\beta_i}$$

implique que

$$\alpha_i = \beta_i\ (i \neq i_0),\ \alpha_{i_0} - 1 = \beta_{i_0} - 1,\ \lambda = \mu.$$

□

Théorème 2.24. *Soient $P = \lambda \prod_{i \in I} P_i^{\alpha_i}, Q = \mu \prod_{i \in I} P_i^{\beta_i}$ deux polynômes sur K. Pour que Q divise P il faut et il suffit que $\beta_i \leq \alpha_i,\ \forall i$.*

Démonstration. Si $\alpha_i - \beta_i \geq 0$ pour tout i, alors

$$P = (\frac{\lambda}{\mu} \prod_{i \in I} P_i^{\alpha_i - \beta_i})Q.$$

Réciproquement, si $P = LQ$ pour un $L \in K[X]$, alors, comme

$$L = \nu \prod_{i \in I} P_i^{\gamma_i}$$

on a

$$P = \mu\nu \prod_{i \in I} P_i^{\gamma_i + \beta_i}$$

et donc

$$\alpha_i = \gamma_i + \beta_i \geq \beta_i,\ i \in I.$$

□

Définition 2.25. Soit A une K-algèbre unitaire. Soit $a \in A$. Posons $x^0 = \mathbb{I}_A$ et définissons une application

$$h_a : K[X] \to A;\ h_a(\sum_{i\in\mathbb{N}} \alpha_i X^i) = \sum_{i\in} \alpha_i a^i$$

pour $P = \sum_{i\in\mathbb{N}} \alpha_i X^i \in K[X]$.

Théorème 2.26. *L'application $h_a : K[X] \to A$ est un homomorphisme de K-algèbre*

Démonstration. Il faut vérifier que

$$h_a(P + P') = h_a(P) + h_a(Q),\ h_a(PP') = h_a(P)h_a(P'),$$

$\forall P, P' \in K[X]$. Or

$$\begin{aligned} h_a(\sum_{i\in\mathbb{N}} \alpha_i X^i + \sum_{i\in\mathbb{N}} \alpha'_i X^i) &= h_a(\sum_{i\in\mathbb{N}} (\alpha_i + \alpha'_i) X^i) \\ &= \sum_{i\in\mathbb{N}} (\alpha_i + \alpha'_i) a^i \\ &= \sum_{i\in\mathbb{N}} \alpha_i a^i + \sum_{i\in\mathbb{N}} \alpha'_i a^i \\ &= h_a(P) + h_a(P'). \end{aligned}$$

D'autre part

$$\begin{aligned} h_a(PP') &= h_a((\sum_{i\in\mathbb{N}} \alpha_i X^i)(\sum_{i\in\mathbb{N}} \alpha'_i X^i)) \\ &= h_a(\sum_{i\in\mathbb{N}} (\sum_{k+l=i} \alpha_l \alpha'_k) X^i) \\ &= \sum_{i\in\mathbb{N}} (\sum_{k+l=i} \alpha_l \alpha'_k) a^i \\ &= (\sum_{k\in\mathbb{N}} \alpha_k a^k)(\sum_{l\in\mathbb{N}} \alpha'_l a^l) \\ &= h_a(P) h_a(P'). \end{aligned}$$

□

Définition 2.27. Si $P = \alpha_0 + a_1 X + \cdots + \alpha_n X^n \in K[X]$, alors notons

$$h_a(P) = P(a), \quad (a \in A),$$

c. à d. on substitue l'indéterminée X par l'élément $a \in A$. On a donc les formules :

$$(P + P')(a) = P(a) + P(a'), \quad PP'(a) = P(a)P'(a).$$

Dans le cas où $A = K$, nous obtenons la fonction polynômiale $\lambda \mapsto P(\lambda)$ de K dans K.

Définition 2.28. Soit K un corps. Soient $P \in K[X]$ et $\lambda \in K$. Si $P(\lambda) = 0$, on dit que λ est une *racine* de P.

Théorème 2.29. *Soient $P \in K[X]$ et $\lambda \in K$. Pour que λ soit une racine de P, il faut et il suffit que P soit divisible par $X - \lambda$.*

Démonstration. Si $P = L(X - \lambda)$ alors

$$P(\lambda) = L(\lambda)(\lambda - \lambda) = 0.$$

Réciproquement, si nous effectuons la division euclidienne de P par $(X - \lambda)$, alors

$$P = L(X - \lambda) + R$$

avec $\deg R < 1$. Comme

$$0 = P(\lambda)(\lambda - \lambda) + R = 0 + R,$$

nous voyons que $R = 0$ et donc P est divisible par $X - \lambda$. □

Théorème 2.30. *Soient $P \in K[X], \lambda \in K,\ h \in \mathbb{N}^*$. Les conditions suivantes sont équivalentes :*

1. *P est divisible par $(X - \lambda)^h$, mais pas par $(X - \lambda)^{h+1}$.*
2. *$P = (X - \lambda)^h Q$, où $Q(\lambda) \neq 0$*

Démonstration. $\Rightarrow$ On a $P = (X - \lambda)^h Q$ pour un certain $Q \in K[X]$. Si Q admet λ comme racine, alors $Q = Q'(X - \lambda)$ et donc $P = (X - \lambda)^{h+1} Q'$ est divisible par $(X - \lambda)^{h+1}$, ce qui est absurde. $\Leftarrow$ Réciproquement, P est divisible par $(X - \lambda)^h$. Si P est divisible par $(X - \lambda)^{h+1}$, alors

$$P = (X - \lambda)^{h-1} Q' = (X - \lambda)^h Q$$

et donc

$$(X - \lambda)^h (Q'(X - \lambda) - Q) = 0$$

ce qui implique que

$$Q = (X - \lambda) Q'$$

admet λ comme racine, ce qui est impossible. □

Corollaire 2.31. *Soit P un polynôme sur K de degré n. Alors P admet au plus n racines.*

Démonstration. Si P a $n+1$ racines distinctes $\lambda_1, \cdots, \lambda_{n+1}$, alors P est divisible par $\prod_{i=1}^{n+1}(X - \lambda_i)$ et le degré de P est $\geq n + 1$. □

Théorème 2.32. *Le corps $\mathbb{C}$ est algébriquement clos, c. à d. tout polynôme admet au moins une racine dans $\mathbb{C}$.*

Démonstration. Supposons qu'il existe un polynôme Q dans $\mathbb{C}[X]$ tel que $Q(z) \neq 0$ pour tout $z \in \mathbb{C}$. Soit

$$m = \inf_{z \in \mathbb{C}} |Q(z)|.$$

Montrons que $m \neq 0$. Nous avons que $d = \deg Q > 1$ et écrivons

$$Q(z) = \sum_{j=0}^{d} b_j z^j,\ z \in \mathbb{C}$$

Pour $z \neq 0$,

$$Q(z) = z^d \left(\frac{b_0}{z^d} + \frac{b_1}{z^{d-1}} + \cdots \frac{b_{d-1}}{z} + b_d\right).$$

Donc

$$\lim_{z \to \infty} |Q(z)|$$

$$= \lim_{z \to \infty} |z^d| \left(\left|\frac{b_0}{z^d}\right| + \left|\frac{b_1}{z^{d-1}}\right| + \cdots \left|\frac{b_{d-1}}{z}\right| + |b_d|\right)$$

$$= \infty.$$

Il existe donc un $R > 0$, tel que

$$|Q(z)| > m + 1, \ \forall z \text{ tel que } |z| > R.$$

Ainsi

$$m = \inf_{|z| \leq R} |Q(z)| \neq 0.$$

Comme la boule fermée de rayon R est compacte, il existe un z_0 dans cette boule tel que

$$m = |Q(z_0)| \neq 0.$$

Soit

$$P(z) = \frac{Q(z + z_0)}{Q(z_0)}, \ z \in \mathbb{C}.$$

Alors P est un polynôme de degré d, tel que

$$|P(z)| = |\frac{Q(z + z_0)}{Q(z_0)}| \geq \frac{m}{m} = 1 = P(0), \ z \in \mathbb{C}.$$

Montrons que ceci est impossible. Ecrivons

$$P(z) = 1 + a_m z^m + a_{m+1} z^{m+1} + \cdots + a_d z^d, \ z \in \mathbb{C},$$

où $a_m \neq 0$. On a que

$$z = re^{i\omega}, \quad \text{où } r = |z| \text{ et } \omega \in \mathbb{R}.$$

Prenons ω tel que

$$a_m e^{im\omega} = -|a_m|.$$

Alors

$$P(re^{i\omega}) = 1 - |a_m| r^m + r^{m+1} T(r, \omega), \ r \in \mathbb{R},$$

où

$$T(r, \omega) = a_{m+1} e^{i(m+1)\omega} + \cdots + a_d r^{d-m-1} e^{id\omega}.$$

En particulier

$$|T(r, \omega)| \leq \sum_{i>m} |a_i| =: C, 0 < r \leq 1.$$

Finalement

$$|P(re^{i\omega})| \leq |1 - r^m |a_m|| + r^{m+1} |C|, \ 0 < r \leq 1.$$

Pour r assez petit on voit que

$$|P(re^{i\omega})| \leq 1 - r^m |a_m| + r^{m+1} |C| = 1 - r^m (|a_m| - r|C|) < 1,$$

ce qui est en contradiction avec le fait que $|P(z)| \geq 1$ pour tout $z \in \mathbb{C}$. Ainsi un tel Q n'existe pas. □

Théorème 2.33. *Les polynômes irréductibles à coefficients dans $\mathbb{R}$ sont les polynômes linéaires et les polynômes de degré 2 à discriminant négatif.*

Démonstration. Il est clair qu'un polynôme P de degré 2 à discriminant négatif est irréductible. Car si P est réductible, alors $P = (X - \alpha)(X - \beta)$ avec $a, b \in \mathbb{R}$ et donc

$$P = a_0 + a_1 X + a_2 X^2 = \alpha\beta - (\alpha + \beta) X + X^2$$

et ainsi

$$a_1^2 - 4a_0 = (\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2 \geq 0.$$

Soit $P \in \mathbb{R}[X]$ un polynôme de degré ≥ 2 irréductible. Comme $P \in \mathbb{C}[X]$, P admet au moins une racine $\lambda = a + bi$ dans $\mathbb{C}$, et donc aussi

$$P(\overline{\lambda}) = \overline{P(\lambda)} = \overline{0} = 0.$$

Ainsi P est divisible par $(X - \lambda)(X - \overline{\lambda}) = X^2 + uX + v$, où $u = -\lambda - \overline{\lambda} \in \mathbb{R}$ et $v = \lambda\overline{\lambda} \in \mathbb{R}$. Donc P est divisible par un polynôme réel de degré 2 et comme P est irréductible, nous avons que

$$P = c(X^2 + uX + v),$$

où c est une constante. Finalement,

$$u^2 - 4v = (2a)^2 - 4(a^2 + b^2) = -4b^2 < 0.$$

Le discriminant de P est donc négatif. □