

# Corps, Anneaux, Algèbres

## 1 Définitions basiques.

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

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

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

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.

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

**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.

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

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

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

**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  $\mathbb{1}$  dans  $A$ , tel que

$$\mathbb{1} \cdot a = a \cdot \mathbb{1}, \quad a \in A.$$

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

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

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

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

3. Si  $A$  est unitaire, alors

$$(-\mathbb{1}) \cdot x = -x, \forall x \in A.$$

*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,

$$x + (-\mathbb{1}) \cdot x = \mathbb{1} \cdot x + (-\mathbb{1}) \cdot x = (\mathbb{1} - \mathbb{1}) \cdot x = 0_A \cdot x = 0_A.$$

Ainsi  $(-\mathbb{1}) \cdot x$  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

$$\overline{(z + z')} = \bar{z} + \bar{z}', \overline{z \cdot z'} = \bar{z} \cdot \bar{z}'.$$

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

Soit

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

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

$$\begin{aligned} h(a + b) &= h(a) + h(b), \\ h(a \cdot b) &= h(a) \cdot h(b), a, b \in A. \end{aligned}$$

**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

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

**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  $x = \mathbb{1}_A \cdot x \in I$ . Ces idéaux sont appelés idéaux *principaux* de  $A$ .

**Proposition 1.12.** Soit  $h : A \rightarrow B$  un homomorphisme d'anneau et supposons  $A$  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  $A$ . ■

**Définition 1.13.** Soit  $K$  un corps. Nous appelons *polynôme* à coefficients dans  $K$  toute suite

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

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

$$\deg(P).$$

**Définition 1.14.** 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

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

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

**Définition 1.15.** Nous définissons la somme de deux polynômes  $P = (a_j)$  et  $Q = (b_j)$  par

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

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

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

En particulier

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

**Remarque 1.16.** Nous remarquons que le polynôme

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

est un élément unité pour le produit des polynômes :

$$1 \cdot P = P.$$

En effet,

$$\begin{aligned} 1 \cdot P(j) &= \sum_{k=0}^j 1(k)P(j-k) = \underbrace{1(0)}_1 P(j) + \underbrace{1(1)}_0 P(j-1) + \dots \\ &= P(j), \quad j \in \mathbb{N}. \end{aligned}$$

**Proposition 1.17.** *Le produit des polynômes est associatif.*

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

$$\begin{aligned} P \cdot (Q \cdot R)(j) &= \sum_{k+l=j} P(k)(Q \cdot R)(l) \\ &= \sum_{k+l=j} P(k) \left( \sum_{m+n=l} Q(m)R(n) \right) \\ &= \sum_{k+m+n=j} P(k)Q(m)R(n) \\ &= \sum_{l+n=j} \left( \sum_{k+m=l} P(k)Q(m) \right) R(n) \\ &= \sum_{l+n=j} (P \cdot Q)(l)R(n) = (P \cdot Q) \cdot R(j). \end{aligned}$$

Ainsi

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

■

**Définition 1.18.** Nous avons une loi naturelle externe :

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

où

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

**Définition 1.19.** 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

$$(1) \quad \lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$$

On vérifie facilement que

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

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

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

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

$$P + Q = (P(0) + Q(0), P(1) + Q(1), \dots, P(q) + Q(q), \dots, P(d) + Q(d), 0, \dots).$$

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

$$\begin{aligned} P \cdot Q(p + q) &= \sum_{k+l=p+q} P(k)Q(l) = \sum_{k=0}^{p+q} P(k)Q(p+q-k) \\ &= \sum_{k=0}^p P(k)Q(p+q-k) \\ &= 0 + P(p)Q(p+q-p) = P(p)Q(q) \neq 0. \end{aligned}$$

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

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

**15 Définition:** Soit  $X$  le polynôme dans  $K[X]$  défini par

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

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

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

où 1 apparaît à la position  $n$ .

*Démonstration.* Par récurrence sur  $n$ , on a

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

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

$$\begin{aligned} P &= (a_0, a_1, \dots, a_j, \dots, a_d, 0, \dots) \\ &= a_0(\delta_{0,j})_j + a_1(\delta_{1,j})_j + \dots + a_d(\delta_{d,j})_j \\ &= a_0 + a_1X + \dots + a_dX^d \\ &= \sum_{j=0}^d a_j X^j, \end{aligned}$$

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 1.22.** (*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

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

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

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

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

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

Donc si nous procédons par récurrence sur  $m$

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

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 1.23.** *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

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

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

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

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 1.24.** (le p.g.c.d.) Soit  $A_1, \dots, A_n$  une famille finie de polynômes non tous nuls. Soit

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

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 éléments de  $J$  et donc aussi  $D$ . Ainsi  $D$  est le diviseur commun de plus haut degré de la famille  $(A_1, \dots, A_n)$ . Nous disons que  $D$  est le p.g.c.d. de cette famille de polynômes.

**Définition 1.25.** On dit que les polynômes  $A_1, \dots, A_n$  sont *premiers entre eux dans leur ensemble* si le p.g.c.d. est une constante non nulle.

**Théorème 1.26.** (Bezout) Pour que les polynômes  $A_1, \dots, A_n$  soient premiers entre eux dans leur ensemble, il faut et il suffit qu'il existent des polynômes  $U_1, \dots, U_n$ , tels que

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

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

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

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  $1 \in J(A_1, \dots, A_n)$ . Donc

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

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

■

**Théorème 1.27.** 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  $A_1, \dots, A_{n-1}$ , alors  $C$  divise  $A_n$ .
- $b_n$ ) Si les polynômes  $A_1, A_2, \dots, A_n$  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  $B_1, \dots, B_n$ , alors  $A$  est premier avec le produit  $B_1 \cdots B_n$ .

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

$$A_1 A_2 = LC, \quad UA_1 + VC = 1.$$

Donc

$$UA_1 A_2 + VA_2 C = A_2.$$

Ainsi

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

$b_2$ ) On a

$$C = L_1 A_1, \quad C = L_2 A_2, \quad U_1 A_1 + U_2 A_2 = 1.$$

Donc

$$\begin{aligned} C &= CU_1 A_1 + CU_2 A_2 = L_2 A_2 U_1 A_1 + L_1 A_1 U_2 A_2 \\ &= (L_2 U_1 + L_1 U_2) A_1 A_2. \end{aligned}$$

Donc  $A_1 A_2$  divise  $C$ .  $c_2$ ) On a

$$U_1 A + V_1 B_1 = 1, \quad U_2 A + V_2 B_2 = 1.$$

Ainsi

$$\begin{aligned} 1 &= (U_1 A + V_1 B_1)(U_2 A + V_2 B_2) \\ &= (U_1 U_2 A + U_1 V_1 B_2 + V_1 U_2 B_1) A + V_1 V_1 (B_1 B_2). \end{aligned}$$

Supposons les formules vraies pour tout  $2 \leq n' < n$ .  $a_n$ ) Donc si  $C$  est premier avec  $A_1, \dots, A_{n-1}$ ,  $C$  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 1.28.** Un polynôme de degré  $\geq 1$  est dit *irréductible*, si les seuls diviseurs de  $P$  sont  $P$  et 1 (à des facteurs multiplicatifs constants non nul près)

**Exemple 1.29.** 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  $b^2 - c \geq 0$ .
3.  $P = X^2 - 2$  est irréductible dans  $\mathbb{Q}[X]$ .

**Théorème 1.30.** *Tout polynôme  $A \in K[X]$  de degré  $> 0$  possède un diviseur irréductible.*

*Démonstration.* Soit  $\mathcal{D}$  l'ensemble des diviseurs de degré  $\geq 1$  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 1.31.** Nous verrons que tous les polynômes irréductibles dans  $\mathbb{C}[X]$  sont linéaires. Nous pouvons donc indexer les polynômes irréductibles unitaires par les éléments de  $\mathbb{C}$ .

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

**Théorème 1.32.** 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  $\alpha_i$  sont des entiers  $\geq 0$ , 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  $P_j^\alpha$  pour tout  $j \neq i$  ( $\alpha \in \mathbb{N}$ ). Donc  $\alpha_i = 0$ . Ainsi  $\alpha_i = 0$  si et seulement  $\beta_i = 0$ . 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

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

■

**Théorème 1.33.** 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

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

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

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

■

**Définition 1.34.** Soit  $A$  une  $K$ -algèbre unitaire. Soit  $a \in A$ . Posons  $x^0 = \mathbb{1}_A$  et définissons une application

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

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

**Théorème 1.35.** L'application  $h_a : K[X] \rightarrow A$  est un homomorphisme de  $K$ -algèbre

*Démonstration.* Il faut vérifier que

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

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

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

D'autre part

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

■

**Définition 1.36.** Si  $P = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n \in K[X]$ , 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 1.37.** Soit  $K$  un corps. Soient  $P \in K[X]$  et  $\lambda \in K$ . Si  $P(\lambda) = 0$ , on dit que  $\lambda$  est une racine de  $P$ .

**Théorème 1.38.** Soient  $P \in K[X]$  et  $\lambda \in K$ . Pour que  $\lambda$  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 1.39.** 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  $\lambda$  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  $\lambda$  comme racine, ce qui est impossible. ■

**Corollaire 1.40.** Soit  $P$  un polynôme sur  $K$  de degré  $n$ . Alors  $P$  admet au plus  $n$  racines.

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

**Théorème 1.41.** 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

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

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

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

Pour  $z \neq 0$ ,

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

Donc

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

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

$$= \infty.$$

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

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

Ainsi

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

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

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

Alors  $P$  est un polynôme de degré  $d$ , tel que

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

Montrons que ceci est impossible. Ecrivons

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

où  $a_m \neq 0$ . On a que

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

Prenons  $\phi$  tel que

$$a_m e^{m\phi} = -|a_m|.$$

Alors

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

où

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

En particulier

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

Finalement

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

Pour  $r$  assez petit on voit que

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

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 1.42.** *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

$$P = a_0 + a_1X + a_2X^2 = \alpha\beta - (\alpha + \beta)X + X^2$$

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  $\geq 2$  irréductible. Comme  $P \in \mathbb{C}[X]$ ,  $P$  admet au moins une racine  $\lambda = a + bi$  dans  $\mathbb{C}$ , et donc aussi

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

Ainsi  $P$  est divisible par  $(X - \lambda)(X - \bar{\lambda}) = X^2 + uX + v$ , où  $u = -\lambda - \bar{\lambda} \in \mathbb{R}$  et  $v = \lambda\bar{\lambda} \in \mathbb{R}$ . 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. ■