Polynômes

Dans tout le cours, K désigne un sous-corps de $\mathbb{C}$, le plus souvent $\mathbb{R}$ ou $\mathbb{C}$, quelquefois $\mathbb{Q}$ et plus rarement autre chose. Les éléments de K sont appelés les scalaires.

1 Ensemble $K[X]$

1.1 Définition

Définition. On appelle polynôme à coefficients dans K toute suite presque nulle d'éléments de K, c'est-à-dire toute suite nulle à partir d'un certain rang.

En particulier, la suite $(0, 1, 0, 0, \ldots)$ est notée X et est appelée l'indéterminée (c'est un polynôme particulier).

L'ensemble des polynômes est noté $K[X]$.

L'égalité de deux polynômes est l'égalité habituelle des suites : deux polynômes $P = (a_i)$ et $Q = (b_i)$ sont égaux si et seulement si pour tout $i \in \mathbb{N}$, $a_i = b_i$.

1.2 Degré

Si $P = (a_i) \in K[X]$ et $P \neq 0$, alors on pose $d = \max\{i \in \mathbb{N} \;/\; a_i \neq 0\}$: d est appelé le degré du polynôme P et est noté $d = \deg P$ ou $d = d^\circ P$. Le coefficient a_d est appelé le coefficient dominant de P (le monôme $a_d X^d$ est appelé le terme dominant : voir plus loin).

On a donc : pour tout $k \in \{0, \ldots, d\}$, $\operatorname{coeff}_k(P) = a_k$ et pour tout $k > d$, $\operatorname{coeff}_k(P) = 0$.

Par convention, on pose $\deg 0 = -\infty$. Tous les coefficients du polynôme nul sont nuls.

2 Opérations sur les polynômes

2.1 Multiplication par un scalaire

La multiplication d'un polynôme par un scalaire est la multiplication classique d'une suite par un scalaire.

Proposition 1. *Si P est un polynôme et λ un scalaire, alors*
$$\lambda P \text{ est un polynôme et } \deg(\lambda P) \leqslant \deg P.$$
Plus précisément, si $\lambda \neq 0$, alors $\deg(\lambda P) = \deg P$.
Pour tout $k \in \mathbb{N}$, $\operatorname{coeff}_k(\lambda.P) = \lambda \operatorname{coeff}_k(P)$.

2.2 Somme de polynômes

L'addition de deux polynôme est l'addition classique des suites.

Proposition 2. *Si P et Q sont deux polynômes, alors*
$$P + Q \text{ est un polynôme et } \deg(P + Q) \leqslant \max(\deg P, \deg Q).$$
Plus précisément,

si $\deg P \neq \deg Q$,	*alors* $\deg(P + Q) = \max(\deg P, \deg Q)$
si $\deg P = \deg Q$,	*alors* $\deg(P + Q) = \deg P = \deg Q$ *si et seulement si la somme des coefficients dominants de P et Q est non nulle, dans le cas contraire on a* $\deg(P + Q) < \deg P$

Pour tout $k \in \mathbb{N}$, $\operatorname{coeff}_k(P + Q) = \operatorname{coeff}_k(P) + \operatorname{coeff}_k(Q)$.

2.3 Produit de polynômes

En revanche, le produit de deux polynômes n'est pas le produit des suites.

Définition. Soit $P = (a_i)$ et $Q = (b_i)$ deux polynômes.

On note $P \times Q = PQ$ la suite (c_i) telle que pour tout $p \in \mathbb{N}$, $c_p = \sum_{k=0}^{p} a_k b_{p-k}$.

Proposition 3. *Si P et Q sont deux polynômes, alors*
$$P \times Q \text{ est un polynôme et } \deg(P \times Q) = \deg P + \deg Q.$$
Pour tout $k \in \mathbb{N}$, $\operatorname{coeff}_k(PQ) = \sum_{j=0}^{k} \operatorname{coeff}_j(P) \operatorname{coeff}_{k-j}(Q)$.

On définit de manière récurrente la notion de puissance k-ème d'un polynôme, car la loi $\times$ est associative. Pour éviter les cas particuliers, pour tout polynôme P, même nul, on convient que $P^0 = 1$.

2.4 Structure d'anneau

Proposition 4. *$K[X]$ est un anneau commutatif intègre pour les lois précédentes.*

Enfin, on donne l'écriture standard des polynômes.

Proposition 5. *Tout polynôme $P = (a_i) \in K[X]$ s'écrit sous la forme $\sum_{k=0}^{n} a_k X^k$, où n est un entier quelconque au moins égal au degré de P.*
Plus précisément, si $P \neq 0$ et si on choisit $n = \deg P$, alors l'écriture précédente est unique.

2.5 Lien avec les fonctions polynômes

À tout polynôme $P = (a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$, on associe l'application $\tilde{P}$ de K dans K définie de la façon suivante : pour tout $x \in K$, $\tilde{P}(x) = \sum_{k=0}^{n} a_k x^k$.

On montre plus loin que toute fonction polynôme est associée à un unique polynôme. Mais il ne faut pas croire que cette idée est toujours vraie ! Si K est un corps fini, alors deux polynômes formellement distincts peuvent avoir la même fonction polynôme associée.

Autrement dit, si K est un corps infini, l'application $P \mapsto \tilde{P}$ est une bijection, mais si K est un corps fini, alors elle est surjective et non injective.

Définition. Soit $t \in K$. On appelle évaluation en t l'application $\begin{array}{ccc} K[X] & \longrightarrow & K \\ P & \longmapsto & P(t) \end{array}$.

Proposition 6. *Soit $t \in K$. L'évaluation en t est linéaire et compatible avec les produits : pour tout $(P, Q) \in K[X]^2$, $\lambda \in K$,*
- $(P + Q)(t) = P(t) + Q(t)$;
- $(\lambda P)(t) = \lambda P(t)$;
- $(PQ)(t) = P(t)Q(t)$.

2.6 Composition de polynômes

Définition. Soit $P = \sum_{k=0}^{n} a_k X^k$ et Q deux polynômes. On pose $P \circ Q = \sum_{k=0}^{n} a_k Q^k$.

Proposition 7. *Si P et Q sont deux polynômes, alors*
$P \circ Q$ *est un polynôme et si* $\deg Q \geqslant 1$, $\deg(P \circ Q) = \deg P \times \deg Q$.

Le polynôme $P \circ Q$ est plus souvent noté $P(Q)$. Avec cette notation, $P = P \circ X = P(X) \dots$

Proposition 8. *Soit $A \in K[X]$. La composition par A est linéaire et compatible avec les produits : pour tout $(P, Q) \in K[X]^2$, $\lambda \in K$,*
- $(P + Q)(A) = P(A) + Q(A)$;
- $(\lambda P)(A) = \lambda P(A)$;
- $(PQ)(A) = P(A)Q(A)$.

2.7 Polynômes constants

Un polynôme de degré inférieur ou égal à 0 est appelé polynôme constant.

Si on considère l'application φ de K dans $K[X]$ qui associe à a le polynôme constant $(a, 0, 0, \dots)$, on remarque qu'elle vérifie :
- φ est injective
- pour tout $(a, b) \in K^2$, $\varphi(a + b) = \varphi(a) + \varphi(b)$ et $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1) = (1, 0, 0, \dots)$

Par conséquent, tout calcul effectué sur les nombres revient à un calcul sur les polynômes constants. Par abus, on identifie les scalaires et les polynômes constants : avec cet abus de notation, on se permet d'écrire $P = 2$ au lieu de $P = 2X^0$ le polynôme constant égal à 2, donc en quelque sorte, on se permet de penser que $K \subset K[X]$.

3 Racines d'un polynôme

3.1 Diviseurs dans $K[X]$

Définition. Soit P, Q deux polynômes de $K[X]$. On dit que P divise Q si et seulement si il existe $R \in K[X]$ tel que $Q = PR$, autrement dit si on peut factoriser P dans le polynôme Q.

On va voir que cette définition et toutes celles qui s'y rapportent permettent de faire dans $K[X]$ les mêmes raisonnements que dans $K[X]$, c'est-à-dire de l'arithmétique.

3.2 Factorisation par $X - a$

Définition. Soit $P \in K[X]$ et $a \in K$. On dit que a est une racine (ou un zéro) de P dans K si et seulement si $P(a) = 0$.

Dans cette définition, $P(a)$ désigne aussi bien la composée du polynôme P par le polynôme constant a que la valeur en a de la fonction polynôme associée $\tilde{P}$: par l'identification des constantes et des polynômes constants, c'est la même chose.

Proposition 9. *Soit $P \in K[X]$ et $a \in K$. Alors $X - a$ divise P si et seulement si $P(a) = 0$.*

On en déduit le résultat suivant par récurrence sur k, nombre de racines distinctes de P.

Corollaire 1. *Soit $P \in K[X]$ et $a_1, \dots, a_k$ k scalaires distincts.*
Si $a_1, \dots, a_k$ sont k racines de P dans K, alors P est divisible par $(X - a_1) \dots (X - a_k)$.

Exercices :

1) Donnez un polynôme A tel que $A(2) = A(3) = 0$ et $A(4) = 1$.

3.3 Nombre de racines distinctes

Théorème 1. *Si P est un polynôme non nul de $K[X]$ et si P de degré n, alors P a au maximum n racines distinctes dans K.*

Le corollaire est un moyen très puissant de prouver qu'un polynôme est nul, **sans** chercher à calculer ses coefficients.

Corollaire 2. *Soit $P \in K[X]$.*

- ▷ *Si $\deg P \leqslant n$ et si P a $n+1$ racines distinctes, alors $P = 0$.*
- ▷ *Si P a une infinité de racines, alors $P = 0$.*

On en déduit une bijection entre l'ensemble des polynômes et celui des fonctions polynômes.

Corollaire 3. *Si K est un corps infini, alors l'application $P \mapsto \tilde{P}$ est une bijection.*

4 Division euclidienne dans $K[X]$

Théorème 2. *Soit $(A, B) \in K[X]^2$, $B \neq 0$. Alors il existe un unique couple $(Q, R) \in K[X]^2$ tel que $A = BQ + R$ et $\deg R < \deg B$.*

Q est le quotient de la division euclidienne de A par B, R est le reste.

Un cas particulier : si $P \in K[X]$ et $a \in K$, alors le reste de la division euclidienne de P par $X - a$ est $P(a)$.

5 Dérivation des polynômes

5.1 Généralités

Définition. Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme.

On appelle polynôme dérivé de P le polynôme $P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$.

Puis par récurrence, on définit les polynômes dérivés successifs $P^{(m)}$ de manière évidente.

On note que la dérivation des polynômes ressemble à celle des fonctions polynômes dans le cas des polynômes réels. En fait, toutes les propriétés calculatoires de la dérivation restent vraies.

Proposition 10. *Soit $\lambda \in K$, $(P, Q) \in K[X]^2$. Alors*

- $(\lambda P)' = \lambda P'$
- $(P + Q)' = P' + Q'$
- $(PQ)' = P'Q + PQ'$
- $(P \circ Q)' = P' \circ Q \times Q'$.
- $P' = 0$ *si et seulement si P est constant*

De même, la formule de Leibniz reste valable pour dériver n fois des produits (voir chapitre sur la dérivation).

5.2 Racines simples ou multiples

Définition. Soit $P \in K[X]$ et a une racine de P, alors P est factorisable par $X - a$: $P = (X - a)Q$.

On dit que a est une racine simple de P si et seulement si a n'est pas racine de Q, c'est-à-dire si $Q(a) \neq 0$, sinon a est dite racine multiple de P.

Autrement dit,

- a est une racine simple si et seulement si on ne peut factoriser $X - a$ qu'une seule fois dans P,
- a est une racine multiple si et seulement si on peut factoriser $X - a$ au moins deux fois dans P, c'est-à-dire si $(X - a)^2$ divise P.

Proposition 11. *Soit $P \in K[X]$ et a une racine de P.*
Alors a est racine simple de P si et seulement si $P'(a) \neq 0$.
Les racines multiples de P sont donc les racines communes à P et à P'.

6 Espace vectoriel $K_n[X]$

6.1 Définitions

Soit $n \in \mathbb{N}$, on note $K_n[X]$ l'ensemble des polynômes de degrés inférieurs ou égaux à n

$$K_n[X] = \{P \in K[X] \ / \ \deg P \leqslant n\}$$

On remarque que :
— si $(P, Q) \in K_n[X]^2$, alors $P + Q \in K_n[X]$;
— si $P \in K_n[X]$ et $\lambda \in K$, alors $\lambda P \in K_n[X]$.
On dit que $K_n[X]$ est un K-espace vectoriel.

6.2 Bases de $K_n[X]$

Tout polynôme de $K_n[X]$ s'écrit de manière unique sous la forme $P = \sum_{k=0}^{n} a_k X^k$: on dit que la famille de polynômes $(1, X, X^2, \ldots, X^n)$ est une base de $K_n[X]$.
De manière générale, on dit qu'une famille de polynômes de $K_n[X]$ $(P_0, P_1, \ldots, P_m)$ est une base de $K_n[X]$ si et seulement si tout polynôme P de $K_n[X]$ s'écrit de manière unique sous la forme $\sum_{k=0}^{m} \lambda_k P_k$.

Proposition 12. *Soit $a \in K$. La famille $(1, X - a, (X - a)^2, \ldots, (X - a)^n)$ est une base de $K_n[X]$.*
Plus précisément, si $P \in K_n[X]$, alors $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X - a)^k$ (égalité de Taylor).

6.3 Application aux racines multiples

Définition. Soit $P \in K[X]$ et a une racine de P. On dit que a est une racine d'ordre (de multiplicité) k de P si et seulement si on peut factoriser $(X - a)^k$ dans P mais pas $(X - a)^{k+1}$.

Les racines simples sont les racines d'ordre 1, les racines multiples sont celles d'ordre au moins 2.

Proposition 13. *Soit $P \in K[X]$ et $a \in K$.*
Alors a est racine d'ordre k de P si et seulement si $P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

7 Factorisation dans $\mathbb{C}[X]$

Théorème 3 (d'Alembert-Gauss)**.** *Tout polynôme de $\mathbb{C}[X]$ non constant a au moins une racine dans $\mathbb{C}$.*

Corollaire 4. *Soit $P \in \mathbb{C}[X]$, de degré $n \geqslant 1$.*

▷ *P possède exactement n racines complexes, chacune étant comptée selon son ordre de multiplicité :*
si P a pour racines distinctes $a_1, \ldots, a_k$ d'ordres de multiplicité $\alpha_1, \ldots, \alpha_k$,
alors $\alpha_1 + \cdots + \alpha_k = n$

▷ *P est factorisable en produits de facteurs de degré 1 :*
si P a pour racines distinctes $a_1, \ldots, a_k$ d'ordres de multiplicité $\alpha_1, \ldots, \alpha_k$ et si λ est le coefficient dominant de P, alors

$$P = \lambda \prod_{p=0}^{k} (X - a_p)^{\alpha_p}$$

La décomposition précédente s'appelle « décomposition en facteurs irréductibles de P dans $\mathbb{C}[X]$ » : elle est unique à l'ordre des facteurs près.

***Exercices* :**

1) Factorisez $X^3 - 8i$ dans $\mathbb{C}[X]$
2) Factorisez $(X+1)^5 - 32X^5$ dans $\mathbb{C}[X]$.

8 Factorisation dans $\mathbb{R}[X]$

Un polynôme à coefficients réels est en particulier un polynôme à coefficients complexes : $\mathbb{R}[X] \subset \mathbb{C}[X]$. Les résultats précédents s'appliquent donc. Si on veut ne manipuler que des réels et aucun complexe non réel, alors il faut être plus précis.

Proposition 14. *Si $P \in \mathbb{R}[X]$ et si a est une racine complexe de P d'ordre de multiplicité α, alors $\overline{a}$ est aussi racine de P, avec le même ordre de multiplicité α.*

Corollaire 5.

Tout polynôme de $\mathbb{R}[X]$ non constant est factorisable en produit de facteurs dans $\mathbb{R}[X]$:
- *de degré 1 ou*
- *de degré 2 à discriminant strictement négatif.*

Si $P \in \mathbb{R}[X]$ est non constant de coefficient dominant λ, alors

$$P = \lambda \prod_{p=1}^{r} (X - a_p)^{\alpha_p} \prod_{q=1}^{k} (X^2 + b_q X + c_q)^{\beta_q}$$

où $a_1, \ldots, a_r$ sont les r racines réelles de P d'ordre de multiplicité $\alpha_1, \ldots, \alpha_r$ et $b_1, \ldots, b_k, c_1, \ldots, c_k$ sont $2k$ réels tels que pour tout $q \in \{1, \ldots, k\}$, $\Delta_q = b_q^2 - 4c_q < 0$.

La décomposition précédente s'appelle « décomposition en facteurs irréductibles de P dans $\mathbb{R}[X]$ » : elle est unique à l'ordre des facteurs près.

***Exercices* :**

1) Factorisez $X^4 + 1$ dans $\mathbb{R}[X]$.
2) Factorisez $(X+1)^5 - 32X^5$ dans $\mathbb{R}[X]$.

Remarque. Un polynôme est dit scindé dans $K[X]$ quand il peut s'écrire comme un produit de facteurs de degré 1 à coefficients dans K. Dans $\mathbb{C}[X]$, tous les polynômes sont scindés. Dans $\mathbb{R}[X]$, ça dépend du polynôme : il est scindé si et seulement si il n'a aucune racine non réelle.

9 Relations entre les racines et les coefficients

Soit P un polynôme scindé de degré n. On a deux écritures pour P :

— en somme : $P = \sum_{k=0}^{n} a_k X^k$

— en produit : $P = a_n \prod_{p=1}^{n} (X - r_p)$ (donc $a_n \neq 0$).

Si on développe le produit et qu'on réécrit le polynôme en somme, alors en identifiant les coefficients, on obtient des relations entre les racines et les coefficients.

Exemples.

— la somme des racines $r_1 + \cdots + r_n$ vaut $-\dfrac{a_{n-1}}{a_n}$

— le produit des racines $r_1 \times \cdots \times r_n$ vaut $(-1)^n \dfrac{a_0}{a_n}$

Dans le cas d'un polynôme de degré deux $P = aX^2 + bX + c$, on retrouve les relations bien connues : la somme de deux racines est $\dfrac{-b}{a}$ et le produit $\dfrac{c}{a}$.

D'une manière générale, pour $k \in \{1, \ldots, k\}$, on note $\sigma_k(r_1, \ldots, r_n)$ ou plus simplement σ_k s'il n'y a pas d'ambiguïté la somme de tous les produits de k racines prises par les n.

Alors

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Exercices **:**

1) Soit a, b, c les trois racines du polynôme $X^3 - 3X^2 + X + 2$. Que vaut $a^2 + b^2 + c^2$?
2) Soit p, q deux entiers. Déterminez un polynôme unitaire à coefficients entiers dont les racines sont les carrés de celles du polynôme $X^3 + pX + q$.

10 Arithmétique dans $K[X]$

L'existence d'une division euclidienne dans $K[X]$ permet de retrouver quasiment à l'identique les résultats obtenus dans $K[X]$.

10.1 Polynômes associés

Définition. Deux polynômes A et B de $K[X]$ sont dits associés quand A divise B et B divise A.

Il est très simple de déterminer les associés d'un polynôme.

Proposition 15. *Le seul polynôme associé au polynôme nul est le polynôme nul.*
Si A et B sont associés et non nuls, alors il existe $\lambda \in K^*$ tel que $A = \lambda B$.

Parmi tous les polynômes associés, l'un est en général privilégié : celui qui est unitaire.

Pour tout polynôme A, on note $\mathrm{Div}(A)$ l'ensemble des diviseurs de A.

Proposition 16. *Soit A, B deux polynômes.*
$\mathrm{Div}(A) = \mathrm{Div}(B)$ *si et seulement si A et B sont associés.*

10.2 Diviseurs communs

Proposition 17. *(Lemme d'Euclide)*
Soit A, B deux polynômes, B non nul. On note R le reste de la division euclidienne de A par B.
Alors $\mathrm{Div}(A) \cap \mathrm{Div}(B) = \mathrm{Div}(B) \cap \mathrm{Div}(R)$

On considère l'algorithme suivant :

```
entrée : A, B deux polynômes non nuls
sortie : S un polynôme
----------
S <- A
T <- B
tant que T != 0 faire
  R <- reste de la division euclidienne de S par T
  S <- T
  T <- R
finfaire
```

Proposition 18. *L'algorithme précédent termine et la valeur finale de S est un polynôme tel que* $\mathrm{Div}(A) \cap \mathrm{Div}(B) = \mathrm{Div}(S)$.

S est appelé **un** p.g.c.d. de A et B. Tout autre polynôme associé à S vérifie la même propriété. En général, on privilégie parmi tous les p.g.c.d. de A et B celui qui est unitaire, mais ce n'est nullement une obligation.

Par abus de notation, on écrit $S = \mathrm{pgcd}(A, B)$ pour signifier que S est un p.g.c.d. de A et B. Quand on note $A \wedge B$, on considère le p.g.c.d. unitaire.

De plus, si on modifie légèrement l'algorithme précédent, on peut prouver comme dans le cas des entiers l'existence de coefficients de Bézout.

Théorème 4. *Soit $(A, B) \in K[X]^2$ et $D = \mathrm{pgcd}(A, B)$.*
Alors il existe $(U, V) \in K[X]^2$ tel que $D = AU + BV$.

Exercices **:**

1) Déterminez le p.g.c.d des polynômes $P = X^5 + X^3 + X^2 - 2X + 2$ et $Q = X^4 + 3X^3 + 3X^2 + 6X + 2$, ainsi que des coefficients de Bézout associés.

On dispose bien sûr d'un résultat presque réciproque.

Proposition 19. *Soit A, B deux polynômes non nuls.*
Si D divise A et B et s'il existe $(U, V) \in K[X]^2$ tel que $D = AU + BV$, alors $D = \mathrm{pgcd}(A, B)$.

10.3 Polynômes premiers entre eux

Définition. Deux polynômes sont dits premiers entre eux ou étrangers (ou encore copremiers, comme on le dit au Québec) quand un p.g.c.d. est égal à 1.

On a alors le th. de Bézout.

Théorème 5. *Soit $(A, B) \in K[X]^2$.*
A et B sont premiers entre eux si et seulement si il existe $(U, V) \in K[X]^2$ tel que $1 = AU + BV$.

Puis divers résultats.

Proposition 20. *Soit A, B, C trois polynômes. Si $A \wedge B = 1$ et $A \wedge C = 1$, alors $A \wedge (BC) = 1$.*

Corollaire 6. *Soit A, B deux polynômes. Si $A \wedge B = 1$, alors pour tout $(m, n) \in \mathbb{N}^2$, $A^m \wedge B^n = 1$.*

Enfin le fameux théorème de Gauss.

Théorème 6. *Soit A, B, C trois polynômes.*
Si A divise BC et A est premier avec B, alors A divise C.

Ce résultat est faux si on ne suppose pas que A est premier avec B, par exemple si on suppose seulement (erreur classique) que A ne divise pas B.

Proposition 21. *Soit A, B, C trois polynômes.*
Si $A \mid C$, $B \mid C$ et $A \wedge B = 1$, alors $(AB) \mid C$.

Là encore, le résultat est faux si on ne suppose pas que A est premier avec B.

10.4 Multiples communs

Proposition 22. *Soit A, B deux polynômes non nuls. On pose M le quotient de AB par $A \wedge B$.*
Alors l'ensemble des multiples communs à A et à B est l'ensemble des multiples de M.

M est appelé un p.p.c.m. de A et B : les autres p.p.c.m. sont les associés de celui-ci. Par abus de notation, on note $M = \text{ppcm}(A, B)$ pour signifier que M est un p.p.c.m. de A et B.

10.5 Généralisation à plusieurs polynômes

Proposition 23. *Soit $n \in \mathbb{N}^*$.*
Pour tout $(A_1, \dots, A_n) \in K[X]^n$, il existe un polynôme D tel que
pour tout $P \in K[X]$, $(P \mid D)$ si et seulement si (pour tout $i \in [\![1, n]\!]$, $P \mid A_i$).

D est appelé un p.g.c.d. de $A_1, \dots, A_n$ et noté $\text{pgcd}(A_1, \dots, A_n)$. D est défini à une constante multiplicative près.

Proposition 24. *Avec les mêmes hypothèses, on vérifie que*
$$\text{pgcd}(A_1, \dots, A_n) = \text{pgcd}(A_1, \text{pgcd}(A_2, \dots, A_n)).$$
Autrement dit, la l.c.i. $\wedge$ est associative : on peut donc noter aussi $A_1 \wedge \dots \wedge A_n$ le p.g.c.d. unitaire de $A_1, \dots, A_n$.

L'égalité de Bezout reste vraie.

Proposition 25. *Avec les mêmes hypothèses,*
si $D = \text{pgcd}(A_1, \dots, A_n)$, alors il existe $(U_1, \dots, U_n) \in K[X]^n$ tel que $D = \sum_{i=1}^{n} U_i A_i$.
Réciproquement, si D est un diviseur commun à $A_1, \dots, A_n$ et s'il existe $(U_1, \dots, U_n) \in K[X]^n$ tel que $D = \sum_{i=1}^{n} U_i A_i$, alors $D = \text{pgcd}(A_1, \dots, A_n)$.

Définition. On dit de même que $A_1, \dots, A_n$ sont premiers entre eux (dans leur ensemble) quand leur p.g.c.d. est égal à 1.

Remarque. On prendra bien soin de distinguer les propriétés « être premiers dans leur ensemble » et « être premiers deux à deux », la seconde impliquant naturellement la première, mais la réciproque est fausse. Par exemple, $X(X-1), (X-1)(X-2), X(X-2)$ sont premiers dans leur ensemble, mais pourtant ni $X(X-1)$ et $X(X-2)$ ne sont premiers entre eux, ni $X(X-1)$ et $(X-1)(X-2)$, ni $X(X-2)$ et $(X-1)(X-2)$.

On retrouve bien sûr le même résultat qu'avec deux polynômes.

Proposition 26. *Avec les mêmes hypothèses,*
$A_1, \dots, A_n$ sont premiers entre eux si et seulement si il existe $(U_1, \dots, U_n) \in K[X]^n$ tel que $\sum_{i=1}^{n} U_i A_i = 1$.

10.6 Polynômes irréductibles

Définition. Un polynôme de $K[X]$ non constant est dit irréductible dans $K[X]$ quand ses seuls diviseurs dans $K[X]$ sont les constantes ou ses associés.

Les polynômes irréductibles vont jouer le même rôle que les nombres premiers. Voici quelques irréductibles simples.

Proposition 27.

- ▷ *Tout polynôme de degré* 1 *est irréductible.*
- ▷ *Tout polynôme de degré* 2 *ou* 3 *sans racine dans* K *est irréductible*

Remarque. Attention ! La notion d'irréductibilité est une notion relative : elle dépend de K. Par exemple, X^2+1 est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Une conséquence du th. de d'Alembert-Gauss :

Proposition 28. *Dans* $\mathbb{C}[X]$*, les seuls polynômes irréductibles sont les polynômes de degré* 1*.*
Dans $\mathbb{R}[X]$*, les polynômes irréductibles sont les les polynômes de degré* 1 *et ceux de degré* 2 *à discriminant strictement négatif.*

Dans $\mathbb{Q}[X]$, c'est plus compliqué (mais aussi plus intéressant) car on peut montrer qu'il existe des polynômes irréductible de tout degré.

Proposition 29. *Soit* P *un polynôme irréductible. Alors* P *est premier avec tous les polynômes qu'il ne divise pas ; en particulier, avec tous les polynômes non nuls de degré strictement inférieur.*

On en déduit le résultat suivant.

Proposition 30. *Un polynôme irréductible divise un produit de polynômes si et seulement si il divise l'un d'entre eux.*

Ce résultat est faux si on ne suppose pas le polynôme irréductible.

10.7 Décomposition en facteurs irréductibles

Proposition 31. *Tout polynôme non constant est divisible par au moins un polynôme irréductible.*

Corollaire 7. *Deux polynômes sont premiers entre eux si et seulement si ils n'ont aucun diviseur irréductible commun.*

Corollaire 8. *Deux polynômes de* $\mathbb{C}[X]$ *sont premiers entre eux si et seulement si ils n'ont aucune racine commune dans* $\mathbb{C}$*.*

Remarque. Attention ! Dans le corollaire précédente, on parle bien de racines complexes ! Le corollaire précédent est faux si on remplace $\mathbb{C}$ par $\mathbb{R}$: les polynômes (X^2+1) et $(X^2+1)^2$ sont des polynômes de $\mathbb{R}[X]$ qui n'ont aucune racine commune **dans** $\mathbb{R}$ et pourtant ils ne sont pas premiers entre eux.

Le théorème qui suit est souvent appelé théorème fondamental de l'arithmétique dans $K[X]$.

Théorème 7. *Tout polynôme non constant* P *s'écrit de manière unique comme un produit de polynômes irréductibles (à l'ordre près des facteurs et aux associés près des polynômes irréductibles).*
Autrement dit, pour tout $P \in K[X]-K$*, il existe* $k \in \mathbb{N}^*$*, un* k*-uplet* $(P_1,\dots,P_k) \in K[X]^k$ *tel que* $P_1,\dots,P_k$ *soient irréductibles et* $(\alpha_1,\dots,\alpha_k) \in \mathbb{N}^{*k}$ *tels que* $P = P_1^{\alpha_1}P_2^{\alpha_2}\dots P_k^{\alpha_k}$*.*
Cette écriture s'appelle la décomposition en facteurs irréductibles de P*.*
On peut choisir les polynômes irréductibles unitaires, mais dans ce cas, il faut ajouter le coefficient dominant λ *:* $P = \lambda P_1^{\alpha_1}P_2^{\alpha_2}\dots P_k^{\alpha_k}$*.*