Proposition 4.6 (Caractérisation du PGCD par divisibilité)**.** *Soit $n \geq 2$ et $P_1, \ldots, P_n$ des polynômes non tous nuls de $\mathbb{K}[X]$. Alors*

- *$Q = P_1 \wedge \cdots \wedge P_n$ est l'unique polynôme unitaire de plus petit degré divisant chacun des P_i;*
- *Tout autre polynôme D divisant chaque P_i vérifie $D \mid Q$.*

Exercise 4.7. *Soit K un corps, et L une extension de K (ainsi L est un corps dont K est un sous-corps). Soit $P, Q \in \mathbb{K}[X]$. Montrer que P et Q ont même PGCD dans $\mathbb{K}[X]$ et dans $L[X]$.*

4.2 Décomposition en facteurs irréductibles

Définition 4.8 (Polynôme irréductible)**.** *Un polynôme non constant P de $\mathbb{K}[X]$ est irréductible si et seulement s'il n'est, à une constante multiplicative non nulle près, divisible que par lui-même et par 1.*

Exercise 4.9.
1. *Soit P un polynôme irréductible de $\mathbb{Q}[X]$. Montrer que P n'a pas de racine double dans $\mathbb{C}$.*
2. *Soit $P \in \mathbb{Q}[X]$ de degré 5. On suppose que P admet une racine double dans $\mathbb{C}$. Montrer que P possède une racine dans $\mathbb{Q}$.*

Exemple 4.10.
1. *Les polynômes $X - \lambda$ sont irréductibles ($\lambda \in \mathbb{K}$).*
2. *Dans $\mathbb{R}[X]$, tout polynôme $aX^2 + bX + c$ tel que $\Delta < 0$ est irréductible.*
3. *Ces polynômes ne sont pas irréductibles dans $\mathbb{C}[X]$.*

Théorème 4.11 (Polynômes irréductibles de $\mathbb{C}[X]$. *et $\mathbb{R}[X]$]*

(i) Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1 (théorème de d'Alembert-Gauss).

(ii) Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Lemme 4.12 (Existence d'un diviseur irréductible)**.** *Tout polynôme non constant $P \in \mathbb{K}[X]$ admet un diviseur irréductible.*

Éléments de preuve. Considérer un diviseur non constant de degré minimal. □

Lemme 4.13 (Euclide)**.** *Soit A et B deux polynômes de $\mathbb{K}[X]$ et P un polynôme irréductible. Alors si P divise AB, P divise A ou P divise B. Le lemme d'Euclide se généralise facilement à davantage de facteurs, par récurrence immédiate.*

Éléments de preuve. Si P ne divise pas A, $P\mathbb{K}[X] + A\mathbb{K}[X] = \mathbb{K}[X]$. Multiplier par B pour obtenir $B\mathbb{K}[X] \subset P\mathbb{K}[X]$. □

Exercise 4.14. *Soit $n \geq 2$ et $a_1, \ldots, a_n$ des éléments de $\mathbb{Z}$ deux à deux distincts. Montrer que le polynôme $P = (X - a_1) \cdots (X - a_n) - 1$ est irréductible dans $\mathbb{Z}[X]$.*

Théorème 4.15 (Décomposition en facteurs irréductibles)**.** *Soit P un polynôme non nul de $\mathbb{K}[X]$. Il existe un unique élément $\lambda \in \mathbb{K}^*$ et des polynômes irréductibles unitaires $P_1, \ldots, P_k$, uniques à permutation près, tels que*

$$P = \lambda P_1 \cdots P_k.$$

Éléments de preuve**.** Par récurrence, en divisant par un facteur irréductible unitaire. Pour l'unicité, aussi par récurrence, en remarquant qu'un facteur irréductible unitaire de P se retrouve dans toute décomposition, d'après le lemme d'Euclide. □

Exercise 4.16. *Soit P un polynôme scindé de $\mathbb{R}[X]$ à racines simples, de degré $n \geq 2$.*

1. *Montrer que P' est scindé à racines simples.*
2. *Montrer que $P = \sum_{k=0}^{n} a_k X^k$ ne peut pas avoir deux coefficients successifs nuls.*
3. *Montrer que P ne peut pas avoir un coefficient nul entouré de deux coefficients non nuls de même signe.*