Éléments de preuve. En passant aux inversibles dans le théorème chinois, sachant qu'un isomorphisme préserve l'inversibilité. □

Lemme 3.16 ($\varphi(p^k)$). *Soit $p \in \mathbb{P}$ et $k \in \mathbb{N}^*$. Alors $\varphi(p^k) = p^{k-1}(p-1)$.*

Éléments de preuve. Dénombrement direct, sachant que k n'est pas premier avec $p \in \mathbb{P}$ si et seulement s'il est multiple de p. □

Théorème 3.17 (Expression de $\varphi(n)$). *Soit $n \in \mathbb{N}^*$, et $n = p_1^{a_1} \cdots p_r^{a_r}$ sa décomposition en facteurs premiers, avec $a_i > 0$. Alors*

$$\varphi(n) = \prod_{\ell=1}^{r} p_\ell^{a_\ell - 1}(p_\ell - 1) = n \prod_{\ell=1}^{r} \left(1 - \frac{1}{p_\ell}\right).$$

4. Arithmétique dans l'anneau $\mathbb{K}[X]$

Conformément au programme, soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$ (mais tous les résultats de cette section restent valides si $\mathbb{K}$ est un corps quelconque).

4.1 Idéaux de $\mathbb{K}[X]$

Théorème 4.1 (Description des idéaux de $\mathbb{K}[X]$.] *Soit $\mathbb{K}$ un corps. Alors :*

(i) *$\mathbb{K}[X]$ est un anneau principal.*

(ii) *De plus, deux polynômes P et Q engendrent le même idéal si et seulement s'il existe un $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.*

(iii) *En particulier, tout idéal non nul I de $\mathbb{K}[X]$ s'écrit de manière unique sous la forme $I = P \cdot \mathbb{K}[X]$, où P est un polynôme unitaire.*

Éléments de preuve. S'aider de la division euclidienne, comme pour montrer que $\mathbb{Z}$ est principal. C'est une propriété générale de tout anneau muni d'une division euclidienne (anneau euclidien). La deuxième partie provient de la description des inversibles de $\mathbb{K}[X]$. □

Définition 4.2 (Divisibilité dans $\mathbb{K}[X]$.] *Soit A et B deux polynômes de $\mathbb{K}[X]$. On dit que B divise A s'il existe un polynôme Q tel que $A = BQ$. Inversement, on dit que A est un multiple de B.*

Exercise 4.3. *Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que P' divise P.*

Proposition 4.4 (Caractérisation en termes d'idéaux). *Soit A et B deux polynômes de $\mathbb{K}[X]$. Alors A divise B si et seulement si $B \in (A)$, ou encore si et seulement si $(B) \subset (A)$.*

Définition 4.5 ((Re)définition du PGCD de n polynômes). *Soit $n \geq 2$ et $P_1, \ldots, P_n$ des polynômes non tous nuls de $\mathbb{K}[X]$. Le PGCD Q de $P_1, \ldots, P_n$, noté $Q = P_1 \wedge P_2 \wedge \cdots \wedge P_n$, est l'unique polynôme unitaire tel que*

$$Q \cdot \mathbb{K}[X] = P_1 \cdot \mathbb{K}[X] + \cdots + P_n \cdot \mathbb{K}[X].$$

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 $\mathbb{Z}[X]$.*