Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

Cours à distance – Semaine 4 – Polynômes – Arithmétique

On fixe $\mathbb{K}$ un corps commutatif, par exemple $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

3 Arithmétique des polynômes

Grâce à la division euclidienne, nous allons maintenant développer toute une arithmétique pour les polynômes, très similaire à celle des nombres entiers.

3.1 Idéaux de polynômes

Nous allons établir un parallèle entre polynômes et nombres entiers. Certaines notions seront toutefois modifiées par ce parallèle. La notion de valeur absolue, par exemple, sera remplacée la notion de degré. Ainsi, pour les polynômes, l'implication $a|b \Rightarrow |a| \leq |b|$ vue pour les entiers donnera :

Lemme 3.1.1. Soient $P, Q \in \mathbb{K}[X]^*$. Si P divise Q, alors $\deg(P) \leq \deg(Q)$.

Démonstration. Si P divise Q, alors il existe $S \in \mathbb{K}[X]^*$ tel que $Q = P.S$ et on a donc $\deg(Q) = \deg(P) + \deg(Q) \geq \deg(P)$. □

Enonçons maintenant deux résultats sur les nombres entiers, passés jusqu'à maintenant sous silence car totalement élémentaires.

Proposition 3.1.2.

- Deux entiers $a, b \in \mathbb{Z}^*$ se divisent mutuellement si et seulement si $b = \pm a$, c'est-à-dire si l'un est le produit de l'autre par un élément de $\mathbb{Z}^\times = \{\pm 1\}$.
- Tout entier non nul s'écrit de manière unique comme produit d'un élément inversible (1 ou -1) et d'un entier strictement positif.

Ces résultats possèdent également un équivalent pour les polynômes.

Proposition 3.1.3.

- Deux polynômes non nuls $P_1, P_2 \in \mathbb{K}[X]^*$ se divisent mutuellement si et seulement si $P_2 = \alpha.P_1$ avec $\alpha \in \mathbb{K}^*$, c'est-à-dire si l'un est le produit de l'autre par un élément de $\mathbb{K}[X]^\times = \big\{A \in \mathbb{K}[X] \mid \deg(A) = 0\big\}$.
- Tout polynôme non nul $P \in \mathbb{K}[X]^*$ s'écrit de manière unique sous la forme $\alpha.\widetilde{P}$, avec $\alpha \in \mathbb{K}^*$ et $\widetilde{P} \in \mathbb{K}[X]$ unitaire.

On pourra remarquer que la notion de positivité pour les entiers est remplacée, pour les polynômes, par le caractère unitaire.

Démonstration. Pour le premier point, on sait par le lemme précédent que, simultanément, $\deg(P_1) \leq \deg(P_2)$ et $\deg(P_2) \leq \deg(P_1)$. On a donc $\deg(P_1) = \deg(P_2)$. Mais puisque $P_2 \in (P_1)$, on sait également

qu'il existe $Q \in \mathbb{K}[X]$ tel que $P_2 = Q.P_1$. On a alors $\deg(Q) = \deg(P_2) - \deg(P_1) = 0$, ce qui montre le résultat.

Concernant le second point, on note $\alpha \in \mathbb{K}^*$ le coefficient dominant de P, alors $\widetilde{P} := \alpha^{-1}.P$ est unitaire et vérifie bien $P = \alpha.\widetilde{P}$. Considérons maintenant une autre paire $(\beta, \overline{P}) \in \mathbb{K}^* \times \mathbb{K}[X]$ avec $\overline{P}$ unitaire et $\beta.\overline{P} = P$. Alors $\alpha^{-1}\beta\overline{P} = \alpha^{-1}.P = \widetilde{P}$ est unitaire et son coefficient dominant vaut donc 1. Mais comme $\overline{P}$ est lui aussi unitaire, le coefficient dominant de $\alpha^{-1}\beta\overline{P}$ vaut $\alpha^{-1}\beta$, et on a donc $\alpha^{-1}\beta = 1$. On en déduit, d'une part, que $\beta = \alpha$ et, d'autre part, que $\overline{P} = \widetilde{P}$. □

Enfin, il a été vu en TD que les seuls idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$, c'est-à-dire les idéaux engendrés par un unique entier positif ou nul. Là aussi, il existe un résultat similaire pour les polynômes.

Proposition 3.1.4. Pour tout idéal I de $\mathbb{K}[X]$, il existe un unique $P \in \mathbb{K}[X]$ unitaire ou nul tel que $I = (P)$.

Démonstration. Soit $I \subset \mathbb{K}[X]$ un idéal. Si $I = \{0\}$, alors $I = (0)$. Autrement I^* est non vide et on peut considérer $n_0 := \min\{\deg(P) \mid P \in I^*\}$ ainsi que $P_0 \in I^*$ tel que $\deg(P_0) = n_0$. Montrons que $I = (P_0)$. Par stabilité par produit, on a bien entendu $(P_0) \subset I$. Réciproquement, considérons $P \in I$. Par division euclidienne de P par P_0, on sait qu'il existe $Q, R \in \mathbb{K}[X]$ avec $\deg(R) < \deg(P_0)$ tels que $P = Q.P_0 + R$. Mais alors $R = P - Q.P_0 \in I$ et, par minimalité de $\deg(P_0)$ parmi les degrés d'éléments non nuls de I, on a $R = 0$. On en déduit que $P \in (P_0)$, montrant ainsi que $I \subset (P_0)$ et donc que $I = (P_0)$. Enfin, d'après le second point de la proposition précédente, il existe $\alpha \in \mathbb{K}^*$ et $P \in \mathbb{K}[X]$ unitaire tels que $P_0 = \alpha.P$. On a alors $(P) = (P_0) = I$. Cela montre l'existence.

L'unicité est claire lorsque $I = (0)$. Dans les autres cas, supposons que $(P_1) = (P_2)$ avec $P_1, P_2 \in \mathbb{K}[X]$ unitaires. Alors P_1 et P_2 se divisent mutuellement et, d'après le premier point de la proposition précédente, il existe $\alpha \in \mathbb{K}^*$ tel que $P_2 = \alpha.P_1$. En comparant les coefficients dominants, on obtient enfin que $\alpha = 1$ et donc que $P_1 = P_2$. □

3.2 Polynômes premiers entre eux

Comme pour les entiers, on peut définir une notion de plus petit multiple et de plus grand diviseur communs à deux polynômes non nuls. Mais par rapport aux entiers, il est toutefois moins aisé de les définir directement car, s'il existe un unique entier strictement positif ayant une valeur absolue donnée, il peut exister plusieurs polynômes unitaires ayant un degré donné. Nous allons donc d'abord les définir de manière ad-hoc et vérifier ensuite qu'ils correspondent à ce qu'on peut en attendre.

Définition 3.2.1. Soit $P_1, P_2 \in \mathbb{K}[X]^*$.

- On définit le *plus petit multiple commun* de P_1 et P_2, noté $\mathrm{ppcm}(P_1, P_2)$, comme l'unique générateur unitaire de l'idéal $(P_1) \cap (P_2)$.
- On définit le *plus grand diviseur commun* de P_1 et P_2, noté $\mathrm{pgcd}(P_1, P_2)$, comme l'unique générateur unitaire de l'idéal $(P_1) + (P_2)$.

Proposition 3.2.2. Soit $P_1, P_2 \in \mathbb{K}[X]^*$. Alors :

- $\mathrm{ppcm}(P_1, P_2)$ est le plus petit, au sens de la divisibilité, multiple de P_1 et P_2 dans le sens où c'est un multiple commun à P_1 et P_2, et que tout multiple commun à P_1 et P_2 est un multiple de $\mathrm{ppcm}(P_1, P_2)$;
- $\mathrm{pgcd}(P_1, P_2)$ est le plus grand, au sens de la divisibilité, diviseur de P_1 et P_2 dans le sens où c'est un diviseur commun à P_1 et P_2, et que tout diviseur commun à P_1 et P_2 est un diviseur de $\mathrm{pgcd}(P_1, P_2)$.

Démonstration. On a $\mathrm{ppcm}(P_1, P_2) \in \big(\mathrm{ppcm}(P_1, P_2)\big) = (P_1) \cap (P_2)$. Donc, en particulier, $\mathrm{ppcm}(P_1, P_2) \in (P_1)$, c'est donc un multiple de P_1, et $\mathrm{ppcm}(P_1, P_2) \in (P_2)$, c'est donc également un multiple de P_2. Par

ailleurs, tout multiple commun à P_1 et P_2 est, par essence, dans $(P_1) \cap (P_2) = \big(\text{ppcm}(P_1, P_2)\big)$, c'est donc un multiple de $\text{ppcm}(P_1, P_2)$.

On a $P_1 \in (P_1) \subset (P_1) + (P_2) = \big(\text{pgcd}(P_1, P_2)\big)$, donc $\text{pgcd}(P_1, P_2)$ est un diviseur de P_1. De la même manière, $\text{pgcd}(P_1, P_2)$ est également un diviseur de P_2. Considérons maintenant $D \in \mathbb{K}[X]$, un diviseur commun à P_1 et P_2. On a alors $P_1, P_2 \in (D)$. On en déduit que $(P_1), (P_2) \subset (D)$ et donc, par stabilité par somme, $\big(\text{pgcd}(P_1, P_2)\big) = (P_1) + (P_2) \subset (D)$. De fait, $\text{pgcd}(P_1, P_2) \in (D)$, ce qui signifie que D divise $\text{pgcd}(P_1, P_2)$. □

On peut maintenant définir une notion de polynômes premiers entre eux.

Définition 3.2.3. On dit que deux polynômes $P_1, P_2 \in \mathbb{K}[X]^*$ sont *premiers entre eux* si $\text{pgcd}(P_1, P_2) = 1$.

L'équivalent du théorème de Bachet–Bézout devient alors un corollaire immédiat de la définition de plus grand diviseur commun.

Théorème 3.2.4.

- Pour tout $P_1, P_2 \in \mathbb{K}[X]^*$, il existe $Q_1, Q_2 \in \mathbb{K}[X]$ tels que $P_1.Q_1 + P_2.Q_2 = \text{pgcd}(P_1, P_2)$.
- Deux polynômes $P_1, P_2 \in \mathbb{K}[X]^*$ sont premiers entre eux si et seulement si il existe $Q_1, Q_2 \in \mathbb{K}[X]$ tels que $P_1.Q_1 + P_2.Q_2 = 1$.

Remarque 3.2.5. Comme pour les entiers, on peut définir un algorithme d'Euclide par divisions euclidiennes successives, lequel permet non seulement de déterminer le plus grand diviseur commun de deux polynômes non nuls, mais aussi une relation de Bézout entre eux.

Enfin, on pourra reprendre à l'identique les preuves données dans le cas des entiers pour démontrer les propositions suivantes :

Proposition 3.2.6. Soit $P, Q_1, Q_2 \in \mathbb{K}[X]^*$.

- Si P est simultanément premier avec Q_1 et Q_2, alors il est premier avec $Q_1.Q_2$.
- Si P divise $Q_1.Q_2$ et que P est premier avec Q_1, alors P divise Q_2.
- Si Q_1 et Q_2 sont premiers entre eux et qu'ils divisent simultanément P, alors $Q_1.Q_2$ divise P.

Démonstration. Laissée en exercice ! □

3.3 Décomposition en produit de polynômes irréductibles

Toujours à l'instar des entiers, les polynômes ont une unique décomposition en facteurs "indécomposables". Dans le cas des polynômes, ces derniers ne seront toutefois pas appelés *premiers* comme pour les entiers, mais *irréductibles*. Nous verrons plus en détails cette distinction premier/irréductible dans le chapitre sur les anneaux factoriels.

Définition 3.3.1. On dit qu'un polynôme $P \in \mathbb{K}[X]$ de degré strictement positif est *irréductible* s'il n'est pas produit de deux polynômes de degré strictement positif. Autrement dit, si P est irréductible et que $P = P_1.P_2$ avec $P_1, P_2, \mathbb{K}[X]$, alors l'un des polynômes P_1 ou P_2 est un polynôme constant (non nul), c'est-à dire de degré 0.

Exemples 3.3.2.

- Un polynôme $P \in \mathbb{K}[X]$ de degré 1 est toujours irréductible. En effet, si $P = P_1.P_2$ avec $P_1, P_2 \in \mathbb{K}[X]$, alors $\deg(P_1) + \deg(P_2) = \deg(P) = 1$; les seules possibilités sont donc $\deg(P_1) = 1$ et $\deg(P_2) = 0$, ou $\deg(P_1) = 0$ et $\deg(P_2) = 1$.

- Le polynôme X^2+3X+2 n'est pas irréductible dans $\mathbb{R}[X]$ car il peut s'écrire comme $X^2+3X+2 = (X+1)(X+2)$.
- Le polynôme X^4+X^2+1 n'est pas irréductible dans $\mathbb{R}[X]$ car il peut s'écrire comme $X^4+X^2+1 = (X^2+X+1)(X^2-X+1)$.
- Le polynôme X^2+X+1 est irréductible dans $\mathbb{R}[X]$. En effet, au vu de son degré et de son coefficient dominant, les seules décompositions envisageables sont de la forme $(X-a)(X-b)$ avec $a, b \in \mathbb{R}$. Or $(X-a)(X-b) = X^2-(a+b)X+ab$ et on aurait alors $ab = 1$ et $a+b = -1$; ceci est pourtant impossible car a et b seraient alors de même signe (puisque leur produit vaut 1) et on aurait donc $a, b \in]-1, 0[$ (puisque leur somme vaut -1) et donc $ab \in]0, 1[$ dont 1 ne fait pas partie. Par contre, ce même polynôme n'est pas irréductible dans $\mathbb{C}[X]$ puisque $X^2+X+1 = (X-e^{\frac{2i\pi}{3}})(X-e^{-\frac{2i\pi}{3}})$. Cela illustre le fait que le caractère irréductible ou non d'un polynôme dépend de l'anneau de polynôme considéré, nommément du corps dans lequel on prend les coefficients.
- Si $P \in \mathbb{K}[X]$ est irréductible, alors pour tout $\alpha \in \mathbb{K}^*$, αP l'est aussi. En effet, si αP ne l'était pas, alors on aurait $\alpha P = P_1.P_2$ avec $P_1, P_2 \in \mathbb{K}[X]$ et $\deg(P_1), \deg(P_2) > 0$ et donc $P = \alpha^{-1}P_1.P_2$ avec $\deg(\alpha^{-1}P_1), \deg(P_2) > 0$.

Avant de montrer le théorème de décomposition des polynômes en facteurs irréductibles, commençons par un petit lemme, utile dans la preuve du dit théorème, mais dont l'énoncé est également intéressant en soi.

Lemme 3.3.3. Soit $P_1, P_2 \in \mathbb{K}[X]$ unitaires et irréductibles. Alors P_1 et P_2 sont soit égaux, soit premiers entre eux.

Démonstration. Puisque $\text{pgcd}(P_1, P_2)$ est un diviseur commun à P_1 et P_2, il existe $Q_1, Q_2 \in \mathbb{K}[X]^*$ tels que $P_1 = Q_1.\text{pgcd}(P_1, P_2)$ et $P_2 = Q_2.\text{pgcd}(P_1, P_2)$. Par irréductibilité de P_1, on a donc $\deg(Q_1) = 0$ ou $\deg\big(\text{pgcd}(P_1, P_2)\big) = 0$. Si $\deg\big(\text{pgcd}(P_1, P_2)\big) = 0$, alors c'est que $\text{pgcd}(P_1, P_2) = 1$ et P_1 et P_2 sont premiers entre eux. Sinon, par l'unicité du second point de la proposition 3.1.3, on a $\text{pgcd}(P_1, P_2) = P_1$, qui est notamment de degré strictement positif. Or par irréductibilité de P_2, cela signifie que $\deg(Q_2) = 0$ et que, par l'unicité du second point de la proposition 3.1.3, $P_2 = \text{pgcd}(P_1, P_2) = P_1$. □

Théorème 3.3.4. A ordre des facteurs près, tout polynôme $P \in \mathbb{K}[X]$ de degré strictement positif admet une unique décomposition

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

avec $\alpha \in \mathbb{K}^*$ et $P_1, \ldots, P_k \in \mathbb{K}[X]$ des polynômes unitaires irréductibles.

Démonstration. Commenons par montrer que P s'écrit comme produit de polynômes irréductibles par récurrence généralisée sur $n := \deg(P) \in \mathbb{N}^*$. Pour $n = 1$, le résultat est clair puisque nous avons vu que tout polynôme de degré 1 est irréductible. Considérons maintenant le résultat vrai pour les polynômes de degré entre 1 et $n-1$, avec $n > 1$. Si P est irréductible, alors il est sa propre décomposition. Sinon, c'est qu'il existe $Q_1, Q_2 \in \mathbb{K}[X]$ avec $\deg(Q_1), \deg(Q_2) > 0$ tels que $P = Q_1.Q_2$. Mais alors $\deg(Q_1) + \deg(Q_2) = \deg(P) = n$ et donc $0 < \deg(Q_1), \deg(Q_2) < n$. Par HR, Q_1 et Q_2 sont tous les deux produits de polynômes irréductibles, et $P = Q_1.Q_2$ l'est donc lui aussi.

On a donc $P = \widetilde{P}_1 \ldots \widetilde{P}_k$ avec $\widetilde{P}_1, \ldots, \widetilde{P}_k \in \mathbb{K}[X]$ irréductibles. D'après le second point de la proposition 3.1.3, il existe $\alpha_1, \ldots, \alpha_k \in \mathbb{K}^*$ et $P_1, \ldots, P_k \in \mathbb{K}[X]$ unitaires tels que $P_i = \alpha_i P_i$ pour tout $i \in [\![1, k]\!]$. En posant $\alpha := \alpha_1 \ldots \alpha_k$, on a bien $P = \alpha P_1 \cdots P_k$.

Montrons maintenant l'unicité. En remarquant que α est déterminé comme le coefficient dominant de P, celui-ci est bien unique et, quitte à multiplier le tout par α^{-1}, on peut supposer que P est lui-aussi unitaire. Le reste se fait par récurrence sur le nombre $k \in \mathbb{N}^*$ de facteurs. Si $k = 1$, alors P est irréductible, ce qui serait contredit par tout autre décomposition en plusieurs facteurs irréductibles. Supposons l'unicité vraie pour un produit de $k-1$ facteurs irréductibles, avec $k > 1$ et considérons une décomposition alternative

$P'_1 \cdots P'_{k'}$ de $P = P_1 \cdots P_k$. Alors P_k divise $P'_1 \cdots P'_{k'}$. On remarque alors que P_k est égal à l'un des P'_i, car sinon, l'usage répété du troisième point de la proposition 3.2.6 montrerait que P_k divise 1, ce qui n'est pas possible car $\deg(P_k) > 0$. Quitte à permuter les indices, on peut donc supposer $P_k = P'_{k'}$ et alors, par intégrité de $\mathbb{K}[X]$, on a $P_1 \cdots P_{k-1} = P'_1 \cdots P'_{k'-1}$. Par HR, et quitte à permuter les indices, on a dès lors $k' = k$ et $P'_i = P_i$ pour tout $i \in [\![1, k]\!]$. □

Au même titre que les nombres premiers, les polynômes irréductibles sont donc des briques élémentaires pour construire les polynômes. Il est de fait pertinent de savoir quels polynômes sont irréductibles. Dans le premier point des exemples 3.3.2, nous avons vu que tout polynôme de degré 1 est irréductible. Malgré la simplicité de sa preuve, c'est un résultat important que nous élevons maintenant au rang de proposition.

Proposition 3.3.5. Tout polynôme de degré 1 est irréductible.

Définition 3.3.6. On dit qu'un polynôme non nul et non inversible est *scindé* si tous ses facteurs irréductibles sont de degré un.

Savoir s'il existe des polynômes irréductibles de degré strictement plus grand que 1, autrement dit savoir s'il existe des polynômes non nuls, non inversibles et non scindés, est une question dont la réponse dépend du corps $\mathbb{K}$.

Définition 3.3.7. On dit qu'un corps $\mathbb{K}$ est *algébriquement clos* si tout polynôme de degré au moins un dans $\mathbb{K}[X]$ est scindé, autrement dit si les polynômes de degré 1 sont les seuls à être irréductibles.

Théorème 3.3.8. Le corps $\mathbb{C}$ est algébriquement clos.

Démonstration. Nous admettrons ce résultat. Vous pourrez toutefois en trouver une preuve dans l'appendice des notes de cours. □

Corollaire 3.3.9. Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1. En particulier, pour tout polynôme $P \in \mathbb{C}[X]$ de degré strictement positif, il existe $\alpha \in \mathbb{C}^*$ et $z_1, \ldots, z_{\deg(P)} \in \mathbb{C}$ tels que

$$P = \alpha(X - z_1) \cdots (X - z_{\deg(P)}).$$

Dans $\mathbb{C}$, tout se passe donc relativement bien. Ça n'est pas aussi vrai dans $\mathbb{R}$!

Théorème 3.3.10. Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et les polynômes de degré 2 de la forme $a_0 + a_1 X + a_2 X^2$ avec $a_1^2 < 4a_0 a_2$.

Démonstration. Considérons un polynôme $P \in \mathbb{R}[X]$ irréductible et de degré au moins 2. Puisque $\mathbb{R} \subset \mathbb{C}$, on peut voir P comme un élément de $\mathbb{C}[X]$, et en tant que tel, il existe $\alpha \in \mathbb{C}^*$ et $z_1, \ldots, z_k \in \mathbb{C}$ tels que $P = \alpha(X - z_1) \cdots (X - z_k)$. Mais en développant ce produit, on observe que α est égal au coefficient dominant de $P \in \mathbb{R}[X]$, on a donc $\alpha \in \mathbb{R}^*$. De plus, si z_1 était réel, alors d'après le corollaire 2.2.7, le reste de la division euclidienne de P par $X - z_1$ dans $\mathbb{R}[X]$ serait le même que dans $\mathbb{C}[X]$, à savoir 0, et P serait donc divisible par $X - z_1$, ce qui contredirait son irréductibilité. On en déduit que $z_1 \in \mathbb{C} \setminus \mathbb{R}$, et donc que $\overline{z_1} \neq z_1$. Or, en notant $\overline{Q} \in \mathbb{C}[X]$ le polynôme obtenu à partir de $Q \in \mathbb{C}[X]$ en remplaçant chaque coefficient par son conjugué, on a

$$\alpha(X - \overline{z}_1) \cdots (X - \overline{z}_k) = \overline{\alpha}(X - \overline{z}_1) \cdots (X - \overline{z}_k) = \overline{P} = P = \alpha(X - z_1) \cdots (X - z_k),$$

puisque α et tous les coefficients de P sont réels. Par unicité de la décomposition en facteurs irréductibles (dans $\mathbb{C}$), on en déduit qu'il existe $i \in [\![2, k]\!]$ tel que $\overline{z}_1 = z_i$ et, quitte à permuter les indices, on peut supposer $z_2 = \overline{z}_1$. On a donc $P = \alpha(X - z_1)(X - \overline{z}_1) . \prod_{k=3}^{\deg(P)} (X - z_k) = \alpha(X^2 - 2\mathfrak{Re}(z_1) + |z_1|^2) . \prod_{k=3}^{\deg(P)} (X - z_k)$. Or $Q := \alpha(X^2 - 2\mathfrak{Re}(z_1) + |z_1|^2) \in \mathbb{R}[X]$ et, l'algorithme de division euclidienne

de P par Q étant le même dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$, son résultat est le même et on en déduit que Q divise P. Cela implique que $P = Q$ par irréductibilité de P et égalité des coefficients dominants. De plus, on a $\big(-2\alpha\mathfrak{Re}(z_1)\big)^2 \leq \big(-2\alpha\mathfrak{Re}(z_1)\big)^2 + \big(-2\alpha\mathfrak{Im}(z_1)\big)^2 = 4.\alpha.\alpha|z_1|^2$.

Réciproquement, considérons $P = a_0 + a_1X + a_2X^2$ avec $a_1^2 < 4a_0a_2$ et supposons par l'absurde qu'il n'est pas irréductible. Alors ses facteurs irréductibles sont nécessairement de degré 1, et on a $P = \alpha(X - \beta_1)(X - \beta_2)$ avec $\alpha, \beta_1, \beta_2 \in \mathbb{R}$. En développant, on trouve alors $P = \alpha X^2 - \alpha(\beta_1 + \beta_2)X + \alpha\beta_1\beta_2$ et donc $a_0 = \alpha\beta_1\beta_2$, $a_1 = -\alpha(\beta_1 + \beta_2)$ et $a_2 = \alpha$. Mais alors

$$a_1^2 - 4a_0a_2 = \alpha^2(\beta_1+\beta_2)^2 - 4\alpha^2\beta_1\beta_2 = \alpha^2(\beta_1^2+2\beta_1\beta_2+\beta_2^2-4\beta_1\beta_2) = \alpha^2(\beta_1^2-2\beta_1\beta_2+\beta_2^2) = \alpha^2(\beta_1-\beta_2)^2 \geq 0,$$

ce qui contredit l'hypothèse de départ. On en déduit donc que P est irréductible. □

L'intérêt des polynômes irréductibles va au-delà de la simple décomposition en facteurs.

Proposition 3.3.11. Si $P \in \mathbb{K}[X]$ est irréductible, alors $\mathbb{K}[X]/(P)$ est un corps.

Démonstration. Soit $\widetilde{Q} \in \left(\mathbb{K}[X]/(P)\right)^*$, alors tout représentant $Q \in \mathbb{K}[X]$ de $\widetilde{Q}$ est premier avec P. En effet, si $D \in \mathbb{K}[X]^* \setminus \mathbb{K}[X]^\times$ est un diviseur commun à P et Q, alors $D = \alpha.P$ avec $\alpha \in \mathbb{K}[X]^\times$ car P est irréductible, et donc $P = \alpha^{-1}.D$ divise Q, ce qui implique que $Q \in (P)$, contredisant la non trivialité de $\widetilde{Q}$. Par le thèorème de Bachet–Bézout, il existe donc $R, S \in \mathbb{K}[X]$ tels que $R.Q + S.P = 1$. On en déduit que $1 - R.Q \in (P)$ et donc que $1 - \widetilde{R}.\widetilde{Q} = 0$, en notant $\widetilde{R}$ l'image de R dans $\mathbb{K}[X]/(P)$. Cela fournit un inverse $\widetilde{R}$ pour $\widetilde{Q}$, qui est donc inversible. □

Exemple 3.3.12. En tant que corps, on a $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$. On peut en effet considérer l'application

$$f : \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ \sum_{k=0}^n a_k X^k & \longmapsto & \sum_{k=0}^n a_k i^k \end{array},$$

qui est un épimorphisme d'anneaux. Son noyau $\mathrm{Ker}(f)$ est un idéal, donc, d'après la proposition 3.1.4, il est engendré par un polynôme P unitaire. Or, clairement, $X^2 + 1 \in \mathrm{Ker}(f) = (P)$. Par irréductibilité de $X^2 + 1$ dans $\mathbb{R}[X]$, on en déduit que $P = X^2 + 1$ ou $P = 1$. Mais on ne peut pas avoir $P = 1$, car $1 \notin \mathrm{Ker}(f)$. On a donc $P = X^2 + 1$ et, par le théorème d'isomorphisme pour les anneaux, on obtient que $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$ en tant qu'anneaux.