Recasages possibles : 122, 141, 142.
Référence : Cours d'algèbre, Perrin (p. 51-53).

Développement 1 (Transfert de la factorialité de Gauss)

Soit A un anneau factoriel de corps des fractions $\mathbb{K}$.

Lemme 1 (Gauss) Si $P, Q \in A[X]$, alors $c(PQ) = c(P)c(Q)$.

Proposition 2 Les irréductibles de $A[X]$ sont :
(i) Les polynômes constants $p \in A$ irréductibles dans A ;
(ii) Les polynômes primitifs de degré $\geqslant 1$ et irréductibles dans $\mathbb{K}[X]$.

Théorème 3 (Gauss) L'anneau $A[X]$ est factoriel.

- *Preuve du Lemme 1* : Rappelons tout d'abord que le contenu $c(P)$ du polynôme $P \in A[X]$ est un pgcd de ses coefficients, et est donc défini modulo les inversibles de A. Ainsi, l'égalité à prouver est une égalité modulo $A^\times$. Commençons par montrer que le produit de deux polynômes primitifs est primitif, *i.e.* montrer le lemme pour $c(P) = c(Q) = 1$. On écrit

$$P(X) = a_r X^r + \cdots + a_0 \; ; \; Q(X) = b_s X^s + \cdots + b_0 \;\text{ et }\; PQ(X) = c_{r+s}X^{r+s} + \cdots + c_0.$$

Supposons $c(PQ) \neq 1$ et soit $p \in A$ irréductible tel que $p \mid c(PQ)$ (qui existe puisque A est factoriel). Comme P et Q sont primitifs, il existe $i_0 \leqslant r$, $j_0 \leqslant s$ tels que

$$\forall i < i_0,\ p \mid a_i \;\text{ et }\; p \nmid a_{i_0} \quad ; \quad \forall j < j_0,\ p \mid b_j \;\text{ et }\; p \nmid b_{j_0}.$$

Par produit on a

$$c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0}b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j.$$

Or, $p \mid c_{i_0+j_0}$ et p divise tous les termes de la somme de droite, donc par différence $p \mid a_{i_0}b_{j_0}$ ce qui contredit le lemme d'Euclide. Ainsi, on a $c(PQ) = 1$.

Pour P et Q quelconques, on pose $\alpha = c(P)$, $\beta = c(Q)$ et on note $\widetilde{P}$, $\widetilde{Q}$ les polynômes primitifs de $A[X]$ tels que $P = \alpha\widetilde{P}$ et $Q = \beta\widetilde{Q}$. On a d'après ce qui précède $c(\widetilde{P}\widetilde{Q}) = 1$ donc

$$c(PQ) = c(\alpha\beta\widetilde{P}\widetilde{Q}) = \alpha\beta c(\widetilde{P}\widetilde{Q}) = \alpha\beta = c(P)c(Q),$$

et le **Lemme 1** de Gauss est démontré.

- *Preuve de la Proposition 2* : Montrons d'abord que les éléments (i) et (ii) sont irréductibles :
  (i) Soit $p \in A$ irréductible et $P, Q \in A[X]$ tels que $p = PQ$. Comme A est intègre, on a $0 = \deg(p) = \deg(P) + \deg(Q)$, donc P et Q sont constants. Par irréductibilité de p dans A, P ou Q est inversible dans A, donc dans $A[X]$ et p est bien irréductible dans $A[X]$.
  (ii) Soit $P \in A[X]$ primitif de degré $\geqslant 1$ et irréductible dans $\mathbb{K}[X]$. Soient $Q, R \in A[X]$ tels que $P = QR$. Cette égalité vue dans $\mathbb{K}[X]$ donne Q ou R dans $\mathbb{K}[X]^\times$. Supposons quitte à échanger que $Q \in \mathbb{K}[X]^\times$. On a alors $\deg(Q) = 0$, puis $Q = q \in A$. On en déduit $P = qR$ donc $q \mid c(P) = 1$, d'où $q \in A^\times$. Ainsi, P est bien irréductible dans $A[X]$.

  Montrons que ce sont bien les seuls irréductibles de $A[X]$: soit $P \in A[X]$ irréductible sur A.
  · Si $\deg(P) = 0$, alors $P = p \in A$ est irréductible dans A car si $q, r \in A$ sont tels que $p = qr$, alors voyant cette égalité dans $A[X]$, on en déduit quitte à échanger que $q \in A[X]^\times = A^\times$.
  · Si $\deg(P) \geqslant 1$, P est nécessairement primitif. En effet, si $c(P) \neq 1$, alors il existe $p \in A$ irréductible tel que $p \mid c(P)$ (par factorialité de A) et donc $P = p\frac{P}{p}$ est une factorisation non triviale de P dans $A[X]$. Montrons alors que P est irréductible dans $\mathbb{K}[X]$. Soient $Q, R \in \mathbb{K}[X]$ tels que $P = QR$. En considérant b un ppcm des dénominateurs des coefficients de Q, on écrit $Q = \frac{1}{b}\overline{Q}$ avec $\overline{Q} \in A[X]$. Ensuite, en notant $a = c(\overline{Q})$, on écrit $Q = \frac{a}{b}\widetilde{Q}$ avec $\widetilde{Q} \in A[X]$ primitif. On écrit de même $R = \frac{c}{d}\widetilde{R}$ avec $c, d \in A$, $\widetilde{R} \in A[X]$ primitif. On obtient

$$P = QR = \frac{ac}{bd}\widetilde{Q}\widetilde{R} \quad \text{d'où} \quad bdP = ac\widetilde{Q}\widetilde{R}.$$

En prenant les contenus, on obtient $bd = ac$ (modulo $A^\times$) d'après le **Lemme**

1, d'où l'existence de $u \in A^\times$, tel que $P = u\widetilde{Q}\widetilde{R}$. Or, par irréductibilité de P dans $A[X]$, on en déduit (quitte à échanger blablabla) $\widetilde{Q} \in A[X]^\times = A^\times$ d'où $\deg(\widetilde{Q}) = \deg(Q) = 0$. Ainsi, $Q \in \mathbb{K}[X]^\times$ et on a bien montré l'irréductibilité de P dans $\mathbb{K}[X]$, ce qui conclut la preuve de la **Proposition 2**.

- *Preuve du Théorème 3* : Commençons par montrer l'existence de la décomposition en produit de facteurs irréductibles dans $A[X]$. Considérons pour commencer $P \in A[X]$ primitif. Dans l'anneau $\mathbb{K}[X]$ (euclidien donc principal donc factoriel), on écrit $P = P_1 \cdots P_r$ avec les $P_i \in \mathbb{K}[X]$ irréductibles dans $\mathbb{K}[X]$. En procédant de même que précédemment, on écrit pour tout $i \in [\![1, r]\!]$,

$$P_i = \frac{a_i}{b_i}\widetilde{P}_i \quad \text{avec} \quad \widetilde{P}_i \in A[X] \ \text{ primitif.}$$

On a $\widetilde{P}_i = \frac{b_i}{a_i}P_i$ et $\frac{b_i}{a_i} \in \mathbb{K}^\times$, donc $\widetilde{P}_i$ est irréductible dans $\mathbb{K}[X]$, et étant primitif, il est irréductible dans $A[X]$ d'après la **Proposition 2**. On a donc

$$\left(\prod_{i=1}^{r} b_i\right) P = \prod_{i=1}^{r} a_i \widetilde{P}_i.$$

En prenant les contenus et en utilisant le **Lemme 1**, comme P a été choisi primitif, on voit à nouveau que

$$\prod_{i=1}^{r} b_i = \prod_{i=1}^{r} a_i \quad \text{modulo} \ \ A^\times.$$

Ainsi, il existe $u \in A^\times$ tel que $P = u\widetilde{P_1} \cdots \widetilde{P_r}$, ce qui fournit une décomposition en produit de facteurs irréductibles de P dans $A[X]$. Si maintenant P n'est pas primitif, on écrit $P = c(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ primitif et on applique ce qui précède à $\widetilde{P}$. On obtient donc $u \in A^\times$ et $\widetilde{P_1}, \ldots, \widetilde{P_r} \in A[X]$ irréductibles dans $A[X]$ tels que

$$P = uc(P)\widetilde{P_1} \cdots \widetilde{P_r}.$$

Comme $c(P) \notin A^\times \cup \{0\}$, il existe $v \in A^\times$ et $p_1, \ldots, p_s \in A$ irréductibles tels que

$$c(P) = vp_1 \cdots p_s.$$

La **Proposition 2** dit que les p_i sont irréductibles dans $A[X]$, et $uv \in A^\times$ donc l'écriture

$$P = uvp_1 \cdots p_s \widetilde{P_1} \cdots \widetilde{P_r}$$

est une décomposition en produit de facteurs premiers de P dans $A[X]$, ce qui termine la preuve de l'existence.

Terminons la preuve du théorème de Gauss par l'unicité d'une telle décomposition. Prouvons pour cela que si $P \in A[X]$ est irréductible, alors l'idéal $\langle P \rangle_A := PA[X]$ est premier (ce qui correspond à montrer le lemme d'Euclide dans l'anneau $A[X]$).

· Si $P = p \in A$ est une constante irréductible dans A, alors la réduction des coefficients modulo pA fournit un isomorphisme d'anneau

$$A[X]/\langle p \rangle_A \simeq (A/pA)[X].$$

Or, A/pA est intègre car p est irréductible dans A factoriel donc pA est premier. Ainsi, $A[X]/\langle p \rangle_A$ est intègre, ce qui signifie bien que $\langle P \rangle_A$ est premier.

· Sinon, $\deg(P) \geqslant 1$. On considère alors les morphismes canoniques

$$\iota : A[X] \hookrightarrow \mathbb{K}[X] \quad ; \quad \pi_{\mathbb{K}} : \mathbb{K}[X] \twoheadrightarrow \mathbb{K}[X]/\langle P \rangle_{\mathbb{K}}$$

puis on pose $\varphi = \pi_{\mathbb{K}} \circ \iota : A[X] \to \mathbb{K}[X]/\langle P \rangle_{\mathbb{K}}$. Montrons que $\mathrm{Ker}(\varphi) = \langle P \rangle_A$. On a *a priori* $\mathrm{Ker}(\varphi) = A[X] \cap \langle P \rangle_{\mathbb{K}}$ donc il suffit de montrer

$$A[X] \cap \langle P \rangle_{\mathbb{K}} \subseteq \langle P \rangle_A,$$

l'autre inclusion étant triviale. Soit $Q \in A[X] \cap \langle P \rangle_{\mathbb{K}}$ et $R \in \mathbb{K}[X]$ tel que $Q = PR$. On érit à nouveau $R = \frac{a}{b}\widetilde{R}$ avec $a, b \in A$ premiers entre eux et $\widetilde{R} \in A[X]$ primitif. On écrit également $Q = c(Q)\widetilde{Q}$ avec $\widetilde{Q} \in A[X]$ primitif. On a donc

$$bc(Q)\widetilde{Q} = aP\widetilde{R},$$

ce qui donne par passage aux contenus $bc(Q) = a$ puisque P est primitif par la **Proposition 2**. Ainsi, $b \mid a$ dans A, ce qui signifie que $\frac{a}{b} \in A$, puis que $R \in A[X]$ et enfin que $Q \in \langle P \rangle_A$. Ainsi, on a bien $\mathrm{Ker}(\varphi) = \langle P \rangle_A$, donc φ induit par factorisation un morphisme injectif

$$\overline{\varphi} : A[X]/\langle P \rangle_A \hookrightarrow \mathbb{K}[X]/\langle P \rangle_{\mathbb{K}}.$$

Or, d'après la **Proposition 2**, P est irréductible dans $\mathbb{K}[X]$, donc cet anneau étant factoriel $\langle P\rangle_{\mathbb{K}}$ est un idéal premier et le quotient $\mathbb{K}[X]/\langle P\rangle_{\mathbb{K}}$ est intègre. Ainsi, $A[X]/\langle P\rangle_A$ est intègre en tant que sous-anneau d'un anneau intègre et par suite, $\langle P\rangle_A$ est un idéal premier de $A[X]$, ce qu'on voulait montrer. La preuve de l'unicité de la décomposition en produit de facteurs irréductibles est alors la même que dans $\mathbb{Z}$: soient $u, v \in A^\times$, $P_1, \dots, P_r, Q_1, \dots, Q_s \in A[X]$ irréductibles tels que

$$uP_1 \cdots P_r = vQ_1 \cdots Q_s. \qquad (*)$$

Alors, $P_1 \mid vQ_1 \cdots Q_s$ donc comme $\langle P_1\rangle_A$ est premier, il existe $j \in [\![1, s]\!]$ tel que $P_1 \mid Q_j$. Or, Q_j étant irréductible dans $A[X]$, et comme $P_1 \notin A[X]^\times$, il existe $\lambda \in A^\times$ tel que $P_1 = \lambda Q_j$. Ainsi, on peut simplifier l'égalité $(*)$ par intégrité et on obtient

$$u\lambda P_2 \cdots P_r = vQ_1 \cdots \widehat{Q_j} \cdots Q_s,$$

où la notation $\widehat{Q_j}$ signifie que le facteur Q_j n'apparaît pas dans le produit. Ainsi, on a réduit strictement le nombre de facteurs irréductibles apparaissant dans l'égalité, donc en reitérant le raisonnement, on voit que $r = s$ et que les facteurs P_i sont deux à deux associés aux facteurs Q_j, ce qui termine la preuve de l'unicité de la décomposition, unicité à association près et à l'ordre des facteurs près bien sûr.

Finalement, l'existence et l'unicité de la décomposition en produit de facteurs premiers est bien vérifiée dans $A[X]$, ce qui fait de $A[X]$ un anneau factoriel, et conclut la preuve du **Théorème 3** de Gauss.

Commentaires et prolongements :

- Détaillé comme cela, le développement est sans doute trop long pour tenir en 15 minutes. Il faut donc passer sous silence, ou en tout cas rapidement, certains passages. Par exemple les nombreuses fois où l'on ramène une factorisation dans $\mathbb{K}[X]$ à une factorisation dans $A[X]$ peuvent être éludées, quitte à expliquer une fois le procédé à l'oral. Il me semble pertinent d'appuyer tout au long du développement sur l'utilisation du contenu, notamment dans la leçon 142.

- On peut écourter la preuve du **Lemme 1** de Gauss à l'aide d'une approche naturelle utilisant plus explicitement les propriétés d'un anneau factoriel comme suit : On considère à nouveau $P, Q \in A[X]$ primitifs. Si $p \in A$ est irréductible, A étant factoriel, pA est un idéal premier de A et donc A/pA est un anneau intègre. Par suite, $A/pA[X]$ est intègre. Considérons le morphisme d'anneaux

$$\pi : \left| \begin{array}{ccc} A[X] & \longrightarrow & A/pA[X] \\ R & \longmapsto & \pi(R) = \overline{R} \end{array} \right.$$

où $\overline{P}$ est le polynôme obtenu par réduction des coefficients de P dans A/pA. Si $p \mid c(PQ)$, alors $\overline{P}\,\overline{Q} = \overline{PQ} = \overline{0}$ donc $A/pA[X]$ étant intègre, on a $\overline{P} = \overline{0}$ ou $\overline{Q} = \overline{0}$. Ainsi, $p \mid c(P)$ ou $q \mid c(Q)$, ce qui est absurde puisque P et Q sont primitifs. Ainsi, $c(PQ)$ n'admet pas de facteurs irréductibles, ce qui signifie bien que PQ est primitif, et on conclut la preuve du **Lemme 1** de la même manière.

- Remarquons que par récurrence immédiate, on en déduit que pour tout $n \in \mathbb{N}$, l'anneau $A[X_1, \dots, X_n]$ est factoriel. Ceci permet notamment de justifier que l'anneau $\mathbb{K}[X, Y]$ est un anneau factoriel mais non principal, en utilisant le fait que $\langle X, Y\rangle$ ne saurait être engendré par un unique élément. De même, l'exemple direct du théorème de Gauss d'un tel exemple d'anneau factoriel mais non principal est bien sûr $\mathbb{Z}[X]$. Pour celui-ci, on peut vérifier que l'idéal $\langle 2, X\rangle$ n'est pas principal, ou encore montrer que $\langle X\rangle$ est un idéal premier non maximal, puisque $\mathbb{Z}[X]/\langle X\rangle \simeq \mathbb{Z}$, ce qui est impossible dans un anneau principal.

- En poussant encore plus loin, on peut voir que l'anneau $B = A[X_1, \dots, X_n, \dots]$ (en une infinité dénombrable de variables) est encore factoriel. En effet, si $P \in B$, alors il existe $n \in \mathbb{N}$ tel que $B \in A[X_1, \dots, X_n]$ donc en utilisant la factorialité de ce dernier, on peut décomposer P en produit d'irréductibles de $A[X_1, \dots, X_n]$, qui sont bien sûr des irréductibles de B. L'unicité est aussi claire puisque tout se passe avec un nombre fini de variables. En particulier, on obtient ici un exemple d'anneau factoriel mais non noetherien, puisque la suite $\left(\langle X_1, \dots, X_n\rangle\right)_{n\in\mathbb{N}*}$ est une suite strictement croissante d'idéaux et non stationnaire.