Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

Cours à distance – Semaine 5 – Polynômes – Corrigé TD2

Exercice 1. *Donner la décomposition en facteurs irréductibles dans* $\mathbb{C}[X]$ *puis dans* $\mathbb{R}[X]$ *:*

1. *de* $X^3 - 3X - 2$ *;*

$$\begin{aligned} X^3 - 3X - 2 &= (X+1)(X^2 - X - 2) \\ &= (X+1)^2(X-2) \quad \text{dans } \mathbb{C}[X] \text{ et dans } \mathbb{R}[X] \end{aligned}$$

2. *de* $X^4 + X^2 + 1$ *;*

$$\begin{aligned} X^4 + X^2 + 1 &= (X^2 - e^{2i\pi/3})(X^2 - e^{4i\pi/3}) \\ &= (X - e^{i\pi/3})(X - e^{2i\pi/3})(X - e^{4i\pi/3})(X - e^{-i\pi/3}) \quad \text{dans } \mathbb{C}[X] \\ &= (X^2 + X + 1)(X^2 - X + 1) \quad \text{dans } \mathbb{R}[X] \end{aligned}$$

3. *de* $X^6 - 3X^5 + 2X^4 + X^2 - 3X + 2$ *;*

$$\begin{aligned} X^6 - 3X^5 + 2X^4 + X^2 - 3X + 2 &= (X^4 + 1)(X^2 - 3X + 2) \\ &= (X-1)^2(X+1)(X-i)(X+i)(X-2) \quad \text{dans } \mathbb{C}[X] \\ &= (X-1)^2(X+1)(X-2)(X^2+1) \quad \text{dans } \mathbb{R}[X] \end{aligned}$$

4. *de* $2X^4 - X^3 - 9X^2 + 13X - 5$ *;*

$$\begin{aligned} 2X^4 - X^3 - 9X^2 + 13X - 5 &= (X-1)(2X^3 + X^2 - 8X + 5) \\ &= (X-1)^2(2X^2 + 3X - 5) \\ &= (X-1)^3(2X+5) \quad \text{dans } \mathbb{C}[X] \text{ et dans } \mathbb{R}[X] \end{aligned}$$

5. *de* $2X^4 - 10X^3 + 6X^2 + 18X$*.*

$$\begin{aligned} 2X^4 - 10X^3 + 6X^2 + 18X &= 2X(X^3 - 5X^2 + 3X + 9) \\ &= 2X(X+1)(X^2 - 6X + 9) \\ &= 2X(X+1)(X-3)^2 \quad \text{dans } \mathbb{C}[X] \text{ et dans } \mathbb{R}[X] \end{aligned}$$

Exercice 2.

1. *Soit* $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Q}[X]$ *avec* $a_0, \dots, a_n \in \mathbb{Z}$*. Soient* $p, q \in \mathbb{Z}^*$ *des entiers premiers entre eux tels que* $P\big(\frac{p}{q}\big) = 0$*. Montrer que* p *divise* a_0 *et que* q *divise* a_n*.*

   On a $P\big(\frac{p}{q}\big) = \sum_{i=0}^{n} a_i \big(\frac{p}{q}\big)^i = 0$, donc, en multipliant par q^n, $\sum_{i=0}^{n} a_i p^i q^{n-i} = 0$. En isolant le terme en $i = 0$, cela donne $a_0 q^n + p\big(\sum_{i=1}^{n} a_i p^{i-1} q^{n-i}\big) = 0$. Comme tous les termes sont des entiers et que p est premier avec q (et donc avec q^n), on en déduit par le lemme de Gauss que p divise a_0. De même, en isolant le terme en $i = n$, on obtient $q\big(\sum_{i=0}^{n} a_i p^i q^{n-i-1}\big) + a_n p^n = 0$ et on en déduit que q divise a_n.

2. *Montrer que, pour tout $a \neq b \in \mathbb{Z}$ tels que $a+b \neq -2$, le polynôme $P = X^3 + aX^2 + bX + 1$ est irréductible dans $\mathbb{Q}[X]$.*
   Supposons que P n'est pas irréductible. Comme P est de degré 3, il a alors au moins un facteur de degré 1. On peut donc écrire $P = (X - \frac{p}{q})\,Q$, avec $p, q \in \mathbb{Z}^*$ premiers entre eux (notons que $p \neq 0$ car X ne divise pas P). On a donc $P\big(\frac{p}{q}\big) = 0$, donc, d'après la question précédente, p et q divisent 1. Ainsi $p = \pm 1$ et $q = \pm 1$, donc $\frac{p}{q} = \pm 1$. On en déduit que $X - 1$ ou $X + 1$ divise P, c'est-à-dire que le reste de la division euclidienne de P par un de ces deux polynômes est nul. Effectuons ces deux divisions euclidiennes.

$$P = (X-1)\big(X^2 + (a+1)X + (a+b+1)\big) + (a+b+2)$$
$$P = (X+1)\big(X^2 + (a-1)X + (b-a+1)\big) + (a-b)$$

   On obtient $a+b+2 = 0$ **ou** $a-b = 0$. Par contraposée, si $a+b+2 \neq 0$ **et** $a-b \neq 0$, alors P est irréductible.

Exercice 3. *Dans cet exercice, quand bien même $\mathbb{Z}$ n'est pas un corps, on considérera $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, l'anneau des polynômes à coefficients entiers.*
Pour tout polynôme $P \in \mathbb{Z}[X]^*$, on appelle contenu de P, noté $c(P)$, le pgcd des coefficients de P. On dit que P est primitif si $c(P) = 1$.

1. *Calculer le contenu des polynômes suivants et dire s'ils sont primitifs : $P = 6X^3 - 15X^2 + 9$, $Q = 5X^2 + 3X - 15$, $R = 4X^3 + 8X - 14$.*
   On a $c(P) = 3$, $c(Q) = 1$ et $c(R) = 2$. Parmi les trois, seul Q est primitif.

2. (a) *Pour tout entier premier p, on définit l'application*

$$\varphi_p : \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}/p\mathbb{Z}[X] \\ \sum_{i=0}^n a_i X^i & \longmapsto & \sum_{i=0}^n \overline{a}_i X^i \end{array}.$$

   Montrer que φ_p est un morphisme d'anneaux. Déterminer son noyau.
   On vérifie par calcul direct que $\varphi_p(P+Q) = \varphi_p(P) + \varphi_p(Q)$, $\varphi_p(PQ) = \varphi_p(P).\varphi_p(Q)$ et $\varphi_p(1) = 1$.
   Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$. Fixons un entier premier p. On a

$$\begin{aligned} P \in \ker(\varphi_p) &\iff \overline{a}_i = 0 \text{ pour tout } i \in \{1, \dots, n\} \\ &\iff p | a_i \text{ pour tout } i \in \{1, \dots, n\} \\ &\iff p | c(P) \end{aligned}$$

   Ainsi $\ker(\varphi_p) = \{P \in \mathbb{Z}[X] \,|\, p \text{ divise } c(P)\}$.

   (b) *Montrer qu'un produit de polynômes primitifs est primitif.*
   Soient $P, Q, R \in \mathbb{Z}[X]^*$ tels que $P = QR$. Si P n'est pas primitif, il existe un entier premier p tel que p divise $c(P)$. Donc $\varphi_p(P) = 0$, ce qui implique $\varphi_p(Q).\varphi_p(R) = 0$. Comme $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre, on a soit $\varphi_p(Q) = 0$, soit $\varphi_p(R) = 0$, donc p divise $c(Q)$ ou $c(R)$. Ainsi Q ou R n'est pas primitif. Par contraposée, si Q et R sont primitifs, alors P est primitif.

   (c) *En déduire que, pour tous polynômes $P, Q \in \mathbb{Z}[X]^*$, on a $c(P.Q) = c(P).c(Q)$.*
   Par définition du contenu, tout polynôme $P \in \mathbb{Z}[X]^*$ s'écrit $P = c(P)\widetilde{P}$ pour un polynôme primitif $\widetilde{P}$ —notons que cette écriture est unique. On a donc $PQ = \big(c(P)\widetilde{P}\big)\big(c(Q)\widetilde{Q}\big) = c(P)c(Q)\widetilde{P}\widetilde{Q}$, où $\widetilde{P}\widetilde{Q}$ est primitif comme produit de polynômes primitifs. On en déduit $c(PQ) = c(P)c(Q)$.

3. *Soit $P \in \mathbb{Z}[X]$ un polynôme non irréductible dans $\mathbb{Q}[X]$. Montrer que P est le produit de deux polynômes de $\mathbb{Z}[X]$ de degré strictement positif.*
Comme P n'est pas irréductible dans $\mathbb{Q}[X]$, il s'écrit $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ des polynômes non inversibles, c'est-à-dire de degré strictement positif. Soit q (respectivement r) un dénominateur commun des coefficients de Q (respectivement R). On a alors $qrP = (qQ)(rR)$ avec $qQ \in \mathbb{Z}[X]$ et $rR \in \mathbb{Z}[X]$. Notons n le plus petit entier dans $\mathbb{N}^*$ tel que nP s'écrit $nP = ST$ avec $S, T \in \mathbb{Z}[X]$ de degré strictement positif. Par l'absurde, supposons que $n > 1$. Alors il existe un entier premier p qui divise n. Maintenant, l'égalité $nP = ST$ donne $n.c(P) = c(S).c(T)$. Ainsi, p divise $c(S)$ ou $c(T)$. Par symétrie, on peut supposer que p divise $c(S)$, c'est-à-dire que p divise tous les coefficients de S. Mais alors $\frac{1}{p}S \in \mathbb{Z}[X]$. Ainsi, en notant $m = \frac{n}{p} \in \mathbb{N}^*$, on a $mP = (\frac{1}{p}S)T$ avec $\frac{1}{p}S, T \in \mathbb{Z}[X]$ et $m < n$, ce qui contredit la minimalité de n. On a donc $n = 1$ et $P = ST$ avec $S, T \in \mathbb{Z}[X]$ de degré strictement positif.

Remarque : Dans $\mathbb{Z}[X]$, tous les entiers différents de 0 et ± 1 sont des polynômes de degré 0 non inversibles. Ainsi, dire que P est le produit de deux polynômes de $\mathbb{Z}[X]$ de degré strictement positif est plus fort que dire qu'il n'est pas irréductible dans $\mathbb{Z}[X]$. Par exemple, $2X$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.

4. *Soit $P \in \mathbb{Z}[X]$ de degré strictement positif. Montrer que P est irréductible dans $\mathbb{Z}[X]$ si et seulement si $c(P) = 1$ et P est irréductible dans $\mathbb{Q}[X]$.*
Si $c(P) > 1$, alors $P = c(P)\widetilde{P}$ avec $\widetilde{P} \in \mathbb{Z}[X]$ et $\deg(\widetilde{P}) > 0$. Ni $c(P)$ ni $\widetilde{P}$ n'est inversible dans $\mathbb{Z}[X]$, donc P n'est pas irréductible dans $\mathbb{Z}[X]$. Si P n'est pas irréductible dans $\mathbb{Q}[X]$, alors d'après la question précédente, P est le produit de deux polynômes de $\mathbb{Z}[X]$ de degré strictement positif, donc il n'est pas irréductible dans $\mathbb{Z}[X]$. Finalement, P irréductible dans $\mathbb{Z}[X]$ implique $c(P) = 1$ et P irréductible dans $\mathbb{Q}[X]$.
Supposons maintenant que $c(P) = 1$ et que P est irréductible dans $\mathbb{Q}[X]$. Alors, d'après la question précédente, P n'est pas le produit de deux polynômes de $\mathbb{Z}[X]$ de degré strictement positif. Donc les seules décompositions possibles de P dans $\mathbb{Z}[X]$ sont de la forme $P = qR$ avec $q \in \mathbb{Z}$ et $R \in \mathbb{Z}[X]$. Mais alors q divise $c(P) = 1$, donc $q = \pm 1$ est inversible. Finalement P est irréductible dans $\mathbb{Z}[X]$.

5. *(Critère d'Eisenstein) Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ tel qu'il existe un nombre premier p vérifiant les propriétés suivantes :*
   - *p ne divise pas a_n ;*
   - *p divise a_i pour tout $i \in [\![0, n-1]\!]$;*
   - *p^2 ne divise pas a_0.*

   Montrer que P est irréductible dans $\mathbb{Q}[X]$. (On pourra utiliser l'application φ_p.)
   Supposons que P s'écrit $P = QR$ avec $Q, R \in \mathbb{Q}[X]^*$ (P est non nul car p ne divise pas a_n, donc $a_n \neq 0$). Notons $Q = \sum_{i=0}^{k} b_k X^k$ et $R = \sum_{i=0}^{\ell} c_\ell X^\ell$ avec $b_k, c_\ell \neq 0$, et donc $k + \ell = n$. On a d'une part $\varphi_p(P) = \overline{a}_n X^n$ et d'autre part $\varphi_p(P) = \varphi_p(Q).\varphi_p(R)$, donc $\left(\sum_{i=0}^{k} \overline{b}_i X^i\right)\left(\sum_{i=0}^{\ell} \overline{c}_i X^i\right) = \overline{a}_n X^n$. On en déduit $\varphi_p(Q) = \overline{b}_k X^k$ et $\varphi_p(R) = \overline{c}_\ell X^\ell$. Ainsi, si $k > 0$ et $\ell > 0$, alors pour $0 \leq i < k$ et $0 \leq j < \ell$, on a $\overline{b}_i = 0$ et $\overline{c}_j = 0$, c'est-à-dire p divise b_i et c_j. Mais alors p divise b_0 et c_0, donc p^2 divise $a_0 = b_0 c_0$, ce qui contredit l'hypothèse. Ainsi k ou ℓ est nul, c'est-à-dire que Q ou R est inversible. Donc P est inversible.

6. (a) *Le polynôme* $5X^3 + 45X^2 - 15X + 15$ *est-il irréductible dans* $\mathbb{Q}[X]$ *?*
D'après le critère d'Eisenstein avec $p = 3$, le polynôme $5X^3+45X^2-15X+15$ est irréductible dans $\mathbb{Q}[X]$.

   (b) *Soit* p *un entier premier et* $n \in \mathbb{N}^*$*. Le polynôme* $X^n - p$ *est-il irréductible dans* $\mathbb{Q}[X]$ *?*
D'après le critère d'Eisenstein, le polynôme $X^n - p$ est irréductible dans $\mathbb{Q}[X]$.

   (c) *Le polynôme* $P = X^2 + X + 2$ *est-il irréductible dans* $\mathbb{Q}[X]$ *? (On pourra s'intéresser au polynôme* $P(X + 3)$*.)*
On a $P(X+3) = X^2+7X+14$. D'après le critère d'Eisenstein pour $p = 7$, le polynôme $P(X+3)$ est irréductible dans $\mathbb{Q}[X]$. Si $P = QR$ avec $Q, R \in \mathbb{Q}[X]^*$, alors $P(X+3) = Q(X+3).R(X+3)$. Comme $P(X + 3)$ est irréductible, cela implique que $Q(X + 3)$ ou $R(X + 3)$ est inversible dans $Q[X]$, c'est-à-dire est un polynôme constant. Par suite, Q ou R est un polynôme constant (Q et $Q(X + 3)$ ont le même degré), donc inversible. Ainsi P est irréductible dans $\mathbb{Q}[X]$.

   (d) *Reprendre les trois questions précédentes dans* $\mathbb{Z}[X]$*.*
   - On a $5X^3+45X^2-15X+15 = 5(X^3+9X^2-3X+3)$ et les polynômes 5 et X^3+9X^2-3X+3 ne sont pas inversibles dans $\mathbb{Z}[X]$, donc $5X^3 + 45X^2 - 15X + 15$ n'est pas irréductible dans $\mathbb{Z}[X]$. (En utilisant la question 4 : on a $\deg(P) > 0$ et $c(P) = 5$.)
   - On a $\deg(X^n - p) > 0$, $c(X^n - p) = 1$ et $X^n - p$ est irréductible dans $\mathbb{Q}[X]$, donc $X^n - p$ est irréductible dans $\mathbb{Z}[X]$.
   - On a $\deg(P) > 0$, $c(P) = 1$ et P est irréductible dans $\mathbb{Q}[X]$, donc P est irréductible dans $\mathbb{Z}[X]$.