Université de Genève
Section de Mathématiques

Algèbre I
Session de printemps 2009
Série 10, corrigé

Ex.1

Soit $a = \sum_{i=0}^{n_a} a_i x^i$, $b = \sum_{j=0}^{n_b} b_j x^j$ et $c = \sum_{k=0}^{n_c} c_k x^k$ trois élèments de $A[x]$. On a

$$\begin{aligned}(ab)c &= \Big(\sum_{\substack{0\le i\le n_a\\0\le j\le n_b}} a_i b_j x^{i+j}\Big)\Big(\sum_{0\le k\le n_c} c_k x^k\Big) = \sum_{\substack{0\le i\le n_a\\0\le j\le n_b\\0\le k\le n_c}} \big((a_i b_j)c_k\big)x^{(i+j)+k}\\ &= \sum_{\substack{0\le i\le n_a\\0\le j\le n_b\\0\le k\le n_c}} \big(a_i(b_j c_k)\big)x^{i+(j+k)} = \Big(\sum_{0\le i\le n_a} a_i x^i\Big)\Big(\sum_{\substack{0\le j\le n_b\\0\le k\le n_c}} b_j c_k x^{j+k}\Big) = a(bc).\end{aligned}$$

Ex.2

Soit a et b deux éléments de $\mathbb{K}[x]$. Pour tout $i \in \mathbb{N}$, on note respectivement a_i, b_i, $(a+b)_i$ et $(ab)_i$ le coefficient, potentiellement nul, de x^i dans a, dans b, dans $a+b$ et dans ab. Si a et b sont non nuls, par définition du degré d'un polynôme, pour tout $i > \deg(a)$, on a $a_i = 0$ et pour tout $i > \deg(b)$, on a $b_i = 0$. De fait, pour tout $i > \max\big(\deg(a), \deg(b)\big)$, on a $(a+b)_i = a_i + b_i = 0$ et donc $\deg(a+b) \le \max\big(\deg(a), \deg(b)\big)$.

Concernant le produit, si a et b sont non nuls, on a

$$\begin{aligned}(ab)_{\deg(a)+\deg(b)} &= \sum_{i=0}^{\deg(a)+\deg(b)} a_i b_{\deg(a)+\deg(b)-i}\\ &= \sum_{i=0}^{\deg(a)-1} a_i b_{\deg(a)+\deg(b)-i} + a_{\deg(a)} b_{\deg(b)} + \sum_{i=\deg(a)+1}^{\deg(a)+\deg(b)} a_i b_{\deg(a)+\deg(b)-i}.\end{aligned}$$

Or, pour tout $i \in [\![0, \deg(a)-1]\!]$, $\deg(a)+\deg(b)-i > \deg(b)$ et donc $a_i b_{\deg(a)+\deg(b)-i} = a_i.0 = 0$ et pour tout $i \in [\![\deg(a)+1, \deg(a)+\deg(b)]\!]$, $a_i b_{\deg(a)+\deg(b)-i} = 0.b_{\deg(a)+\deg(b)-i} = 0$. Au final, $(ab)_{\deg(a)+\deg(b)} = a_{\deg(a)} b_{\deg(b)}$. Or, par définition du degré, $a_{\deg(a)} \neq 0$ et $b_{\deg(b)} \neq 0$ et comme $\mathbb{K}$ est intègre car c'est un corps, on a $(ab)_{\deg(a)+\deg(b)} \neq 0$.

Par le même raisonemment, pour tout $k > \deg(a) + \deg(b)$, on a

$$\begin{aligned}(ab)_k &= \sum_{i=0}^{k} a_i b_{k-i}\\ &= \sum_{i=0}^{k-deg(b)-1} a_i b_{k-i} + \sum_{i=k-deg(b)}^{k} a_i b_{k-i}\end{aligned}$$

$$\begin{aligned}(ab)_k &= \sum_{i=0}^{k-deg(b)-1} a_i.0 + \sum_{i=k-deg(b)}^{k} 0.b_{k-i} \\ &= 0.\end{aligned}$$

On a donc $\deg(ab) = \deg(a) + \deg(b)$.

Si a est nul, alors $\deg(a+b) = \deg(b) = \max\big(-\infty, \deg(b)\big)$ et $\deg(ab) = \deg(0) = -\infty = -\infty + \deg(b)$. Il est en de même si b est nul.

Ex.3
Dans ce qui suit, tous les entiers sont considérés modulo 4. Notamment, on a $2 = -2$ ce qui pousse à croire que nous allons obtenir quatre fois le même résultat. De plus, l'anneau $\mathbb{Z}/4\mathbb{Z}[x]$ est commutatif, on peut donc utiliser le binôme de Newton[1].
(1) $(x-2)^2 = x^2 - 2.2.x + 2^2 = x^2 - 4x + 4 = x^2$.
(2) $(x+2)^2 = x^2 + 2.2.x + 2^2 = x^2 + 4x + 4 = x^2$.
(3) $(x-2)(x+2) = x^2 - 2^2 = x^2 - 4 = x^2$.

Ex.4
Pour $p = 2$, on a

$$\prod_{a\in\mathcal{F}_2}(x-a) \;=\; x(x-1) \;=\; x^2 - x.$$

Pour $p = 3$,

$$\prod_{a\in\mathcal{F}_3}(x-a) \;=\; x(x-1)(x-2) \;=\; x(x-1)(x+1) \;=\; x(x^2-1) \;=\; x^3 - x.$$

Pour $p = 5$,

$$\begin{aligned}\prod_{a\in\mathcal{F}_5}(x-a) &= x(x-1)(x-2)(x-3)(x-4) \;=\; x(x-1)(x+1)(x-2)(x+2) \\ &= x(x^2-1)(x^2-4) \;=\; x(x^2-1)(x^2+1) \;=\; x(x^4-1) \;=\; x^5 - x.\end{aligned}$$

En utilisant récursivement la formule de l'exercice (2).(2), on montre que pour tout entier $k \geq 2$ et tous polynômes $a_1, \ldots, a_k$ à coefficients dans un corps, on a $\deg\left(\prod_{i=1}^{k} a_i\right) = \sum_{i=1}^{k}\deg(a_i)$. De fait, on a $\deg\big(G(x)\big) = \sum_{i=0}^{p-1}\deg(x-i) = \sum_{i=0}^{p-1} 1 = p$.
Puisque $\mathcal{F}_p$ est intègre, le coefficient dominant d'un produit de polynômes et égal au produit des coefficients dominant. Le coefficient dominant de $G(x)$ est donc égal à 1. Enfin, x étant en facteur dans $G(x)$, le terme constant de ce dernier est nul.
Cela n'était pas demandé, mais le coefficient en x est égal au produit des éléments non nuls de $\mathcal{F}_p$. D'après l'exercice 5 de la série 6, il est donc égal à -1.

[1] le "2" du second facteur dans $(a+b)^2 = a^2 + 2ab + b^2$ est un vrai élément de $\mathbb{N}$, mais on a

$$2ab = ab + ab = \overline{1}ab + \overline{1}ab = (\overline{1} + \overline{1})ab = \overline{2}ab$$

Ex.5

Soit A un anneau et $A[X]$ son anneau de polynômes. Si 1_A est l'élément unitaire de A, alors celui de $A[X]$ est le polynôme constant égal à 1_A. On note maintenant $\phi_A\colon \mathbb{Z} \longrightarrow A$ et $\phi_{A[X]}\colon \mathbb{Z} \longrightarrow A[X]$ les morphismes d'anneaux envoyant un entier positif n sur la somme de n fois l'élément unitaire. Ce sont les morphismes grâce auxquels on définit la caractéristique des anneaux concernés. On note enfin $\psi\colon A \longrightarrow A[X]$ le morphisme d'anneaux qui envoit un élément $a \in A$ sur le polynôme constant égal à a.

Il est clair que, pour tout $k \in \mathbb{Z}$, $\psi\big(\phi_A(k)\big) = \phi_{A[X]}(k)$. On en déduit que $\mathrm{Ker}(\phi_A) \subset \mathrm{Ker}(\phi_{A[X]})$. Mais puisque ψ est clairement injective, on en déduit l'inclusion inverse et on obtient $\mathrm{Ker}(\phi_A) = \mathrm{Ker}(\phi_{A[X]})$. Par définition de la caractéristique d'un anneau, on a donc $\mathrm{Car}(A[X]) = \mathrm{Car}(A)$. Notamment, $\mathrm{Car}(\mathbb{Z}[X]) = \mathrm{Car}(\mathbb{Z}) = 0$, $\mathrm{Car}(\mathbb{R}[X]) = \mathrm{Car}(\mathbb{R}) = 0$ et $\mathrm{Car}(\mathcal{F}_p[X]) = \mathrm{Car}(\mathcal{F}_p) = p$.

Ex.6

Soit $a = \displaystyle\sum_{i=0}^{\deg(a)} a_i x^i \in (d\mathbb{Z})[x]$. Alors, pour tout $i \in [\![0, d]\!]$, il existe $a'_i \in \mathbb{Z}$ tel que $a_i = da'_i$. Mais alors, en posant $a' = \displaystyle\sum_{i=0}^{\deg(a)} a'_i x^i \in \mathbb{Z}[x]$, on a $a = d.a'$ et donc $a \in (d) = \{d.P(x) | P(x) \in \mathbb{Z}[x]\}$ l'idéal de $\mathbb{Z}[x]$ engendré par d, le polynôme constant égal à d. On a donc $(d\mathbb{Z})[x] \subset (d)$. Réciproquement, en distribuant d, il est clair que tout élément de (d) est dans $(d\mathbb{Z})[x]$. On a donc $(d\mathbb{Z})[x] = (d)$ qui est donc bien un idéal.

On considère maintenant l'application

$$\phi\colon \begin{array}{ccc} \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}/_{d\mathbb{Z}}[x] \\ \displaystyle\sum_{i=0}^{n} a_i x^i & \longmapsto & \displaystyle\sum_{i=0}^{n} \overline{a_i} x^i \end{array}$$

où, pour tout entier k, $\overline{k}$ est la classe de k modulo d. La multiplication et l'addition étant compatible avec la prise de modulo, on vérifie que ϕ est un morphisme d'anneaux. Il est, de plus, clair que ϕ est surjective et enfin

$$\begin{aligned} a = \sum_{i=0}^{n} a_i x^i \in \mathrm{Ker}(\phi) \quad &\Leftrightarrow \quad \sum_{i=0}^{n} \overline{a_i} x^i = 0 \\ &\Leftrightarrow \quad \forall i \in [\![0, n]\!], \overline{a_i} = 0 \\ &\Leftrightarrow \quad \forall i \in [\![0, n]\!], a_i \in d\mathbb{Z} \\ &\Leftrightarrow \quad a \in (d\mathbb{Z})[x] \end{aligned}$$

Donc $\mathrm{Ker}(\phi) = (d\mathbb{Z})[x]$. Or, d'après le théorème d'isomorphisme, $\mathbb{Z}[x]/_{\mathrm{Ker}(\phi)} \cong \mathrm{Im}(\phi)$. On en conclut que $\mathbb{Z}[x]/_{(d\mathbb{Z})[x]} \cong \mathbb{Z}/_{d\mathbb{Z}}[x]$.

Ex.7

On pose $x = 11 - \sqrt{\frac{3}{11}}$. On a alors $11 - x = \sqrt{\frac{3}{11}}$ et donc $(11 - x)^2 = \frac{3}{11}$. Le nombre réel $11-\sqrt{\frac{3}{11}}$ est donc racine du polynôme à coefficients dans $\mathbb{Q}$ [2] $P(X)=(X-11)^2-\frac{3}{11}$, il s'agit donc d'un nombre algébrique.

[2] en multipliant P par 11, on voit qu'il est même racine d'un polynôme à coefficients entiers