Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 4

Exercice 1.
On pourra procéder en quotientant en deux temps pour répondre aux questions suivantes.

1. Montrer que $\mathbb{Z}[t]/(t^2+t+1,2)$ est un corps. Combien d'éléments il y a-t-il dans ce corps ?
2. Soit k un corps. Montrer que $k[x,y,z]/(x-y^3-y^2, y^3+z^4) \cong k[y,z]/(y^3+z^4)$.

Solution.

1. On procède par un quotient en deux temps. C'est à dire qu'on se ramène à étudier le quotient suivant
$$(\mathbb{Z}/2\mathbb{Z})[t]/(t^2+t+1).$$
Par division Euclidienne on voit que les classes des éléments de ce quotient sont les classes de $0, 1, t, t+1$. Donc il y a 4 éléments dans ce quotient. De plus pour vérifier que c'est un corps il suffit de montrer que t et $t+1$ ont un inverse multiplicatif. Mais
$$t(t+1) = t^2+t = -1 = 1$$
Donc t et $t+1$ sont inverses l'un de l'autre et on conclut.

2. On utilise le fait suivant déjà démontré en exercise. Si A est un anneau commutatif et $a \in A$ alors le noyau de l'évaluation en A, c'est à dire le morphisme $A[t] \to A$ qui envoie $p(t)$ sur $p(a)$, est l'idéal généré par $(t-a)$. En appliquant ce principe pour l'évaluation en y^3+y^2
$$k[y,z][x] \to k[y,z]$$
qui envoie $p(x,y,z) \mapsto p(y^2+y^3, y, z)$ on voit que
$$k[x,y,z]/(x-y^2-y^3) \cong k[y,z].$$
En utilisant maintenant le quotient en deux temps, on conclut à l'isomorphisme désiré.

Exercice 2.
Soit R un anneau commutatif. Les anneaux de gauche sont des anneaux de groupes.

(a) Montrer que $R[\mathbb{Z}/n\mathbb{Z}] \cong R[t]/(t^n-1)$.

(b) Montrer que $R[\mathbb{Z}] \cong R[x,y]/(xy-1) \cong R[t,t^{-1}]$.

Réfléchissez où doivent être envoyés les éléments des groupes/les variables.

Solution.

(a) Donnons deux preuves de ce fait:

(a) Soit $f\colon R[t] \to R[\mathbb{Z}/n\mathbb{Z}]$ le morphisme évaluant t en $e_{[1]}$ (i.e. l'élément correspondant à $[1] \in \mathbb{Z}/n\mathbb{Z}$). Ce morphisme est certainement surjectif: l'élément $\sum_{[j]\in\mathbb{Z}/n\mathbb{Z}} a([j])e_{[j]} \in R[\mathbb{Z}/n\mathbb{Z}]$ a par exemple comme préimage $\sum_{j=0}^{n-1} a([j])t^j$. Montrons que $\ker(f) = (t^n-1)$. Tout d'abord, comme
$$f(t^n-1) = e_{[1]}^n - 1 = e_{[n]} - 1 = e_{[0]} - 1 = 1 - 1 = 0,$$
on en déduit que $t^n - 1 \in \ker(f)$ (et donc $(t^n-1) \subseteq \ker(f)$).

Il nous reste à montrer l'autre inclusion, et donc soit $a(t) \in \ker(f)$. Vu que le coefficient dominant de $t^n - 1$ est inversible, on peut effectuer la division euclidienne de $a(t)$ par $t^n - 1$, i.e. on peut écrire $a(t) = b(t)(t^n - 1) + c(t)$, avec $\deg(c) < n$. Vu que $a(t) \in \ker(f)$ et $t^n - 1 \in \ker(f)$, on déduit de l'équation ci-dessus que $c(t) \in \ker(f)$. Nous allons montrer qu'en fait, $c(t) = 0$ (et donc $a(t) \in (t^n - 1)$!). Ecrivons $c(t) = \sum_{j=0}^{n-1} c_j t^j$. Alors son image est $\sum_{j=0}^{n-1} c_j e_{[j]}$. Comme $[i] \neq [j]$ pour tout $i \neq j$ dans $\{0, \ldots, n-1\}$, on en déduit que $c_j = 0$ pour tout j, et donc $c(t) = 0$. On rappelle que définition de l'anneau de groupe le groupe abélien sous-jacent de $R[\mathbb{Z}/n\mathbb{Z}]$ est

$$\bigoplus_{[i] \in \mathbb{Z}/n\mathbb{Z}} R[i]$$

Et qu'un élément est nul si et seulement si le coefficient devant chaque variable formelle $[i]$ est nul.

On a donc montré que $\ker(f) = (t^n - 1)$ et que f est surjective, on conclut donc la preuve par le premier théorème d'isomorphisme.

(b) Soit $f\colon R[t] \to R[\mathbb{Z}/n\mathbb{Z}]$ le morphisme évaluant t en $e_{[1]}$. Comme avant, on calcule que $(t^n - 1) \subseteq \ker(f)$ (c'était l'inclusion facile), et donc que on obtient un morphisme $\overline{f}\colon R[t]/(t^n - 1) \to R[\mathbb{Z}/n\mathbb{Z}]$. Trouvons un inverse explicite.

Comme expliqué dans la preuve de l'exercise à propos de $\mathbb{Z}[S_3]$, trouver un morphisme $R[\mathbb{Z}/n\mathbb{Z}] \to R[t]/(t^n - 1)$ est équivalent à trouver un morphisme d'anneaux $R \to R[t]/(t^n - 1)$ et un morphisme de groupes $\mathbb{Z}/n\mathbb{Z} \to (R[t]/(t^n - 1))^\times$. Dans notre cas, on prend la composition $R \to R[t] \to R[t]/(t^n - 1)$, et le morphisme de groupes défini par envoyer $[1] \in \mathbb{Z}/n\mathbb{Z}$ sur $[t] \in (R[t]/(t^n - 1))^\times$ (notez que cela a du sens, car $[t]$ est inversible et d'ordre n dans cet anneau, vu que $[t]^n = [1]$). Ainsi, on a un morphisme d'anneaux explicite $g\colon R[\mathbb{Z}/n\mathbb{Z}] \to R[t]/(t^n - 1)$, qui "fixe" R et envoie $e_{[1]}$ sur t.

Montrons enfin que ces deux morphismes sont inverses l'un de l'autre. Le calcul peut se simplifier de la facon suivante: dans $R[t]/(t^n - 1)$ (resp. $R[\mathbb{Z}/n\mathbb{Z}]$), tout élément s'écrit comme somme et multiples des éléments de R et de t (resp. des éléments de R et de $e_{[1]}$). Ainsi, pour montrer que deux morphismes sont égaux, il suffit de montrer qu'ils envoient R et t (resp. R et $e_{[1]}$) au même endroit. Dans notre cas, on sait que $\overline{f}$ et g "fixent" R, et permutent t et $e_{[1]}$, donc ils sont bel et bien inverses de l'autre. Remarquez que cette méthode est plus conceptuelle que la précédente, et a permis d'éviter certains calculs.

(b) Nous allons précéder comme dans la deuxième preuve du point précédent. Soit $f\colon R[x, y] \to R[\mathbb{Z}]$ le morphisme défini en fixant R, et en envoyant x (resp. y) sur e_1 (resp. e_{-1}). Alors

$$f(xy - 1) = f(x)f(y) - 1 = e_1 e_{-1} - 1 = e_0 - 1 = 1 - 1 = 0,$$

et donc il se factorise en un morphisme $R[x, y]/(xy - 1) \to R[\mathbb{Z}]$.

Trouvons le morphisme dans l'autre sens. Notez que $[x]$ en inversible dans $R[x, y]/(xy - 1)$. En effet,

$$[x][y] = [xy] = [xy] - [xy - 1] = [1].$$

Ainsi, on peut définir un morphisme de groupes $\mathbb{Z} \to (R[x, y]/(xy - 1))^\times$ envoyant 1 sur $[x]$. On a aussi un morphisme d'anneaux $R \to R[x, y]/(xy - 1)$ défini par la composition $R \to R[x, y] \to R[x, y]/(xy - 1)$, et donc on obtient un morphisme $g\colon R[\mathbb{Z}] \to R[x, y]/(xy - 1)$. Notez que vu que $[x]^{-1} = [y]$ (c.f. le calcul précédent) et que $e_{-1} = e_1^{-1}$, on en déduit que e_{-1} est envoyé sur y.

La preuve que $\overline{f}$ et g sont inverses l'un de l'autre est exactement la même que dans le point précédent (tout élément de $R[\mathbb{Z}]$ (resp. $R[x, y]/(xy - 1)$) est somme et multiple d'éléments de R et de e_1 et e_{-1} (resp. d'éléments de R et de $[x]$ et $[y]$)).

On montre maintenant que $R[\mathbb{Z}] \to R[t, t^{-1}]$ induit par l'identité de R et le morphisme de groupe $\mathbb{Z} \to R[t, t^{-1}]^\times$ qui envoie 1 sur t est un isomorphisme. Ce morphisme est surjectif car il atteint toutes les constantes et t. Pour montrer que ce morphisme est injectif, on remarque qu'une section (il suffit de donner une fonction ensembliste qui est une section pour montrer l'injectivité*) est donné par la fonction

$$\sum_{i\in\mathbb{Z}} a_i t^i \mapsto \sum_{i\in\mathbb{Z}} a_i[i].$$

Cela conclut car le morphisme $R[\mathbb{Z}] \to R[t, t^{-1}]$ et alors un isomorphisme.

Exercice 3.
Soit A un anneau commutatif. Montrer que $\mathbb{Z}[\sqrt{7}]/(5 + 2\sqrt{7}) \cong \mathbb{Z}/3\mathbb{Z}$.

On pourra commencer par identifier le noyau de l'unique homomorphisme d'anneaux $\varphi\colon \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]/(5 + 2\sqrt{7})$.

Solution.
On présente deux solutions.

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]/I$, where $\varphi(n) = [n]$, for all $n \in \mathbb{Z}$. Clearly, φ is a ring homomorphism and $\ker(\varphi) = \{n \in \mathbb{Z} \mid n \in I\}$. Let $n \in \ker(\varphi)$. Then there exist $a, b \in \mathbb{Z}$ such that $n = (5 + 2\sqrt{7})(a + b\sqrt{7})$. We make the computations and arrive at $2n = 3b$. As $\gcd(2, 3) = 1$, we have $n \in (3)$, hence $\ker(\varphi) \subseteq (3)$. Conversely, let $n \in (3)$. Note that $(5-2\sqrt{7})(5+2\sqrt{7}) = -3$, then as $n = 3m$, for some $m \in \mathbb{Z}$, and $\varphi(n) = \varphi(3)\varphi(m) = 0$. We deduce that $\ker(\varphi) = (3)$.

   The only thing left to prove is that φ is surjective. Before we proceed, we remark that $\sqrt{7}(5 + 2\sqrt{7}) = 14 + 5\sqrt{7} \in I$ and $(14 + 5\sqrt{7}) - 2(5 + 2\sqrt{7}) = 4 + \sqrt{7} \in I$. Now, let $[a + b\sqrt{7}] \in \mathbb{Z}[\sqrt{7}]/I$. We have that

$$[a + b\sqrt{7}] = [a] + [b\sqrt{7}] = [a] + [-4b] = \varphi(a) + \varphi(-4b) = \varphi(a - 4b).$$

   We use the isomorphism theorem to conclude that $\mathbb{Z}/(3) \cong \mathbb{Z}[\sqrt{7}]/(5 + 2\sqrt{7})$.

2. On utilise d'abord que l'évaluation en $\sqrt{7}$ induit un isomorphisme

$$\mathbb{Z}[t]/(t^2 - 7) \to \mathbb{Z}[\sqrt{7}].$$

   Cela se démontre par division Euclidienne par $t^2 - 7$ et en utilisant $\sqrt{7} \notin \mathbb{Z}$. Après avoir utilisé cet isomorphisme, on s'intéresse donc au quotient suivant,

$$\mathbb{Z}[t]/(t^2 - 7, 5 + 2t).$$

   On commence par quotienter par $5 + 2t$. On considère l'anneau

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^n} \in \mathbb{Q} \mid a \in \mathbb{Z} \quad n \in \mathbb{N}\right\}.$$

   On voit que l'évaluation en $-\frac{5}{2}$ donne un isomorphisme

$$\mathbb{Z}[t]/(5 + 2t) \to \mathbb{Z}\left[\frac{1}{2}\right].$$

   En effet comme $3 - \frac{5}{2} = \frac{1}{2}$ on voit que $\frac{1}{2}$ est atteint par ce morphisme et donc que le morphisme est surjectif, et par division euclidienne et en utilisant que $-\frac{5}{2} \notin \mathbb{Z}$ on conclut avec le théorème

*Même si a posteriori cet inverse ensembliste et forcément un morphisme d'anneau car tout inverse ensembliste a un morphisme d'anneau est un morphisme d'anneau.

d'isomorphismed. En utilisant cet isomorphisme et le principe du quotient en deux temps on voit qu'on s'intéresse donc au quotient

$$\mathbb{Z}\left[\frac{1}{2}\right]/(\frac{25}{4}-7).$$

Mais on note que comme 2 est inversible, l'idéal $(\frac{25}{4}-7)$ est égal à l'idéal (3) (en multipliant par l'élément inversible -4). Alors on s'intéresse au quotient

$$\mathbb{Z}\left[\frac{1}{2}\right]/(3).$$

On argumente maintenant que $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}\left[\frac{1}{2}\right]/(3)$ est un isomorphisme. On montre que c'est surjectif. Pour cela, on voit que comme $\frac{1}{2}+\frac{3}{2}=2$, l'application est surjective car la classe de $\frac{1}{2}$ dans $\mathbb{Z}\left[\frac{1}{2}\right]/(3)$ est égale à la classe de 2. On montre maintenant que cette application est injective. Si $m \in \mathbb{Z}$ est égal $m = \frac{3a}{2^n}$, alors $\frac{3a}{2^n} \in \mathbb{Z}$. Ainsi $2^n \mid 3a$. Mais comme 2 et 3 sont premiers entre eux on a $2^n \mid a$. Alors $3 \mid m$ dans $\mathbb{Z}$ et cela démontre que l'application est injective, concluant.

Exercice 4.
Soit $1 \neq \epsilon \in \mathbb{C}$ une racine cubique de l'unité.

(a) Montrer que $\mathbb{Z}[\varepsilon] \cong \mathbb{Z}[t]/(t^2+t+1)$.

(b) Montrer que $\mathbb{Q}[\varepsilon] = \mathrm{Frac}(\mathbb{Z}[\varepsilon])$.

(c) Montrer que la dimension de $\mathbb{Q}[\varepsilon]$ en tant que $\mathbb{Q}$-espace vectoriel est 2.

Solution.

(a) Soit le morphisme $f\colon \mathbb{Z}[t] \to \mathbb{Z}[\varepsilon]$ définit par l'évaluation de t en ε. Ce morphisme est surjectif, et donc il suffit de montrer que $\ker(f) = (t^2+t+1)$. Vu que

$$0 = \varepsilon^3 - 1 = (\varepsilon-1)(\varepsilon^2+\varepsilon+1)$$

et que $\varepsilon \neq 1$, on en déduit que

$$\varepsilon^2+\varepsilon+1 = 0.$$

Ainsi, $t^2+t+1 \in \ker(f)$, et donc $(t^2+t+1) \subseteq \ker(f)$. Soit maintenant $g \in \ker(f)$. Vu que t^2+t+1 est unitaire, on peut effectuer la division euclidienne de g par t^2+t+1: on peut alors écrire $g = (t^2+t+1)q + r$, où $q, r \in \mathbb{Z}[t]$ et $\deg(r) < 2$. Vu que g et $t^2+t+1 \in \ker(f)$, on en déduit qu'aussi $r \in \ker(f)$. Montrons qu'en fait $r = 0$ (et donc que $g \in (t^2+t+1)$). Si l'on écrit $r = at+b$, alors on obtient que $a\varepsilon + b = 0$. Si $a = 0$, alors $b = 0$ et on est bon. Si $a \neq 0$, alors on a que $\varepsilon = \frac{b}{a}$, et donc en particulier $\varepsilon \in \mathbb{Q}$. Ceci est impossible, car l'unique racine cubique de l'unité rationelle (même réelle) est 1, et que $\epsilon \neq 1$.

Ainsi, on a bel est bien montré que $\ker(f) = (t^2+t+1)$, et donc on conclut par le premier théorpme d'isomorphisme.

(b) Tout d'abord, rappelons que $\mathbb{Q}[\varepsilon]$ est l'anneau engendré par $\mathbb{Q}$ et ε dans $\mathbb{C}$ les nombres complexes. Autrement dit ce sont éléments de $\mathbb{C}$ de la forme

$$\mathbb{Q}[\varepsilon] = \left\{ \sum_{i=0}^{n} q_i \varepsilon^i \mid q_i \in \mathbb{Q} \right\}.$$

Mais comme $\varepsilon^2 = -(\varepsilon+1)$, ce sont les éléments de la forme

$$\mathbb{Q}[\varepsilon] = \{q_0 + q_1\varepsilon \mid q_0, q_1 \in \mathbb{Q}\}.$$

Mais comme $\varepsilon = \cos(2\pi/3) + i\sin(2\pi/3) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, on peut encore reformuler cet anneau comme

$$\mathbb{Q}[\varepsilon] = \left\{ q_0 + q_1 i\sqrt{3} \mid q_0, q_1 \in \mathbb{Q} \right\}.$$

Maintenant, on peut montrer que aisément que c'est un corps. En effet, l'inverse de $q_0 + q_1 i\sqrt{3}$ est $\frac{q_0 - q_1 i\sqrt{3}}{q_0^2 + 3q_1^2} \in \mathbb{Q}[\varepsilon]$.

Maintenant, notons qu'on a une inclusion $\mathbb{Z}[\varepsilon] \subset \mathbb{Q}[\varepsilon]$. Si on prend un élément $q_0 + q_1\varepsilon$ en multipliant par les dénominateurs de q_0 et q_1, on se retrouve dans $\mathbb{Z}[\varepsilon]$. Dès lors, en utilisant le critère vu dans une série précédente, on conclut.

(c) On prétend qu'une base est $(1, \varepsilon)$. La génération suit de la discussion ci-dessus. La liberté de la famille suit par exemple de l'observation suivante: si $a + b\epsilon = 0$ pour $a, b \in \mathbb{Q}$ alors $a - \frac{1}{2}b + i\frac{\sqrt{3}}{2}b = 0$. Alors comme on sait que $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2 de base $(1, i)$ on voit que $b = 0$, et donc par suite que $a = 0$.

Exercice 5.
Considérons l'homomorphisme

$$\xi_p : \begin{array}{ccc} \mathbb{Z}[t] & \to & \mathbb{F}_p[t] \\ \sum_{i=0}^n a_i t^i & \mapsto & \sum_{i=0}^n [a_i] t^i \end{array}$$

qui envoie un polynôme à coefficients dans $\mathbb{Z}$ au polynôme obtenu par réduction des coefficients mod p. Soit $f(t)$ un polynôme dans $\mathbb{F}_p[t]$ et $g(t)$ une pré-image par ξ_p. Montrez que la pré-image de l'idéal $((f(t)))$ est $(p, g(t))$.

Solution. Nous allons procéder de deux manières différentes.

1. Non-explicite: Cet homomorphisme est surjectif de noyau (p). Comme la pré-image de $(f(t))$ et $(p, g(t))$ contiennent les deux (p), on sait par le théorème de correpondance qu'il suffit de montrer que leur image via $\mathbb{Z}[t] \to \mathbb{F}_p[t]$ sont les mêmes. Comme elles sont les deux $(f(t))$ par construction, on est bon.

2. Explicite: tout d'abord, vu que p et $g(t)$ sont dans $\xi_p^{-1}((f(t))$, alors automatiquement

$$(p, g(t)) \subseteq \xi_p^{-1}((f(t)).$$

Soit maintenant $h \in \xi_p^{-1}((f(t))$, et écrivons $\xi_p(h(t)) = \lambda(t)f(t)$, avec $\lambda(t) \in \mathbb{F}_p[t]$. Soit de plus $\mu(t)$ tel que $\xi_p(\mu(t)) = \lambda(t)$. Alors on obtient que

$$\xi_p(\mu(t)g(t)) = \lambda(t)f(t) = \xi_p(h(t)),$$

te donc que $\mu(t)g(t) - h(t) \in \ker(\xi_p) = (p)$. Ainsi, il exists $w(t)$ tel que

$$h(t) = \mu(t)g(t) - pw(t) \in (p, g(t)),$$

et donc on a bel et bien que

$$\xi_p^{-1}((f(t))) \subseteq (p, g(t)).$$

Exercice 6 (Fonctions polynomiales.)**.**
Soit A un anneau commutatif et $\mathcal{F}(A)$ l'anneau des fonctions $\varphi\colon A \to A$ où la somme et le produit sont définis dans l'ensemble d'arrivée (par exemple $(\varphi \cdot \phi)(a) = \varphi(a) \cdot \phi(a)$). On considère l'évaluation comme application $\mathrm{ev}\colon A[t] \to \mathcal{F}(A)$. L'évaluation d'un polynôme f est donc la fonction polynomiale $\mathrm{ev}(f)$ définie par $\mathrm{ev}(f)(a) = \mathrm{ev}_a(f) = f(a)$.

(a) Montrer que l'évaluation est un homomorphisme d'anneaux.

(b) Montrer que si A est fini, alors l'évaluation n'est pas injective.

(c) Montrer que si A est intègre et infini, alors l'évaluation est injective.

Solution.

(a) Let $f(t), g(t) \in A[t]$. We have that

$$\mathrm{ev}(f+g)(a) = (f+g)(a) = f(a) + g(a) = \mathrm{ev}(f)(a) + \mathrm{ev}(g)(a) = (\mathrm{ev}(f) + \mathrm{ev}(g))(a)$$

for all $a \in A$. Therefore $\mathrm{ev}(f+g) = \mathrm{ev}(f) + \mathrm{ev}(g)$.

Similarly,

$$\mathrm{ev}(fg)(a) = (fg)(a) = f(a)g(a) = \mathrm{ev}(f)(a)\,\mathrm{ev}(g)(a) = (\mathrm{ev}(f)\,\mathrm{ev}(g))(a)$$

for all $a \in A$. Therefore $\mathrm{ev}(fg) = \mathrm{ev}(f)\,\mathrm{ev}(g)$.

Lastly, we have that $\mathrm{ev}(1)(a) = 1$ for all $a \in A$ and thus $\mathrm{ev}(1) = 1$, where the constant polynomial function 1 is the unity of $\mathcal{F}(A)$.

(b) Consider the polynomial $f(t) = \prod_{a \in A}(t-a)$. Then $f \neq 0 \in A[t]$, but $f(a) = 0$ for all $a \in A$.

(c) Supposons que A est intègre et infini. Soit f dans le noyau. Alors f s'annule en tous les $a \in A$. Prenons une suite infinie d'éléments distincts $a_1, \ldots, a_n, \ldots$. Notons que $(t-a_1) \mid f$. Donc

$$f = g(t-a_1).$$

Donc $f(a_2) = g(a_2)(a_2 - a_1)$. Comme $a_2 \neq a_1$ et A est intègre, on a $g(a_2) = 0$. Alors $(t-a_2) \mid g$. Par récurence, on voit que $(t-a_n) \mid f$ pour tout n. Ainsi on voit que forcément $f = 0$, sans quoi le degré de ce polynôme ne serait pas borné.