Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 2

Exercice 1.
Soit K un corps et $R \subset K$ un sous-anneau.

1. Montrer que R est intègre.
2. Montrer que si pour tout élément de $k \in K$ il existe $r \in R$ non-nul tel que $rk \in R$, alors l'application naturelle $\mathrm{Frac}(R) \to K$ est un isomorphisme.
3. Les inclusions suivantes sont-elles l'inclusion d'un anneau dans son corps des fractions ? L'anneau R est supposé intègre.
   (a) $\mathbb{Z}[i] \subset \mathbb{Q}[i]$
   (b) $\mathbb{Z}[t] \subset \mathbb{Q}[t]$
   (c) $R[x, y] \subset K(x, y)$ si $K = \mathrm{Frac}(R)$.

Corrigé.

1. Si $a, b \in R$ satisfont que $ab = 0$, alors c'est aussi vrai dans K (qui est un corps, donc certainement intègre). Du coup, a ou b doivent être nuls.

2. Nommons cette application θ, et montrons tout d'abord qu'elle est injective. Vu que $\ker(\theta)$ est un idéal de K, on a que soit $\ker(\theta) = \mathrm{Frac}(R)$ ou $\ker(\theta) = 0$. Dans le deuxième cas on est bon, et le premier cas est absurde.

   Montrons maintenant la surjectivité: soit $k \in K$, et par hypothèse soit $0 \neq r \in R$ tq $rk \in R$. On a alors que
   $$r\theta\left(\frac{rk}{r}\right) = \theta\left(\frac{rk}{1}\right) = rk,$$
   et donc en divisant par $r \in R \subseteq K$ des deux cotés, on obtient que
   $$\theta\left(\frac{rk}{r}\right) = k.$$

3. (a) C'est le cas. On a vu en cours que $\mathbb{Q}[i]$ est en corps. Maintenant, si $s = \frac{a}{b} + \frac{c}{d}i$, alors $(bd)s \in \mathbb{Z}[i]$.
   (b) Non, car $\mathbb{Q}[t]$ n'est pas un corps (t n'a pas d'inverse).
   (c) C'est le cas. Montrons-le en deux temps. Disons qu'une inclusion d'anneaux intègres $A \subseteq B$ satisfait $(\star)$ si pour tout $b \in B$, alors il existe $a \in A$ non-nul tel que $ab \in A$. Notez que si $A \subseteq B$ et $B \subseteq C$ satisfont $(\star)$, alors $A \subseteq C$ le satisfait aussi.

   Par le point précédent, il suffit de montrer que $R[x, y] \subseteq K(x, y)$ satisfait $(\star)$, et donc que les deux inclusions $R[x, y] \subseteq K[x, y]$ et $K[x, y] \subseteq K(x, y)$ satisfont $(\star)$. Pour la première inclusion, si $f = \sum_{i,j} \frac{r_{ij}}{s_{ij}} x^i y^j \in K[x, y]$ est non-nul, et $s := \prod_{i,j} s_{i,j}$ (il y a un nombre fini de tels éléments par définition d'un polynôme), alors $sf \in R[x, y]$.

   Pour la deuxième inclusion, c'est en fait immédiat parce que $K(x, y)$ est par définition le corps des fractions de $K[x, y]$.

□

Exercice 2.
Prouvez les affirmations suivantes.

1. Un anneau A dans lequel $a = a^2$ pour tout $a \in A$, est commutatif.

2. Un anneau intègre et fini est un corps.

3. Soit K un corps et A un anneau commutatif.

   (a) Soit $K \to A$ un morphisme d'anneau. Montrez que multiplier par l'image des éléments de K fait de A un K-espace vectoriel avec son addition qui vient de la structure d'anneau de A.

   (b) Si maintenant A est intègre et de dimension finie en tant qu'espace vectoriel avec la structure ci-dessus, montrez que A est un corps.

Corrigé. La première assertion se prouve en dévellopant $(x+y)^2$ pour $x, y \in A$ quelconque. Pour la deuxième assertion: si A est fini et intègre pour tout $a \in A$ non-nul l'application $a \cdot A \to A$ est injective. Mais comme A est un ensemble fini, elle est donc bijective. Ainsi il existe $b \in A$ avec $ab = 1$, concluant. Pour 3.(b) le même type de raisonnement s'applique: un K-endormphisme injectif d'un espace vectoriel de dimension finie est bijectif. □

Exercice 3.
Dans chacun des cas suivants, déterminer si l'affirmation suivante est vraie ou fausse. Justifier la réponse par un raisonnement ou un contre-exemple.

(a) Si A est un anneau intègre, et I et J sont deux idéaux non nuls de A, alors $I \cap J$ est aussi un idéal non nul de A.

(b) Si K est un corps, alors les deux seuls idéaux de K sont $\{0\}$ et K.

(c) Si K est un anneau n'ayant que deux idéaux bilatères, alors tout élément non-nul de K possède un inverse à gauche et à droite.

(d) Si K est un anneau commutatif n'ayant que deux idéaux, alors K est un corps.

(e) Si K est un anneau tel que les seuls idéaux à gauche sont $\{0\}$ et K, alors tout élément non-nul de K possède un inverse à gauche et à droite.

(f) Si K est un anneau tel que les seuls idéaux à droite sont $\{0\}$ et K, alors tout élément non-nul de K possède un inverse à gauche et à droite.

Corrigé. (a) Let $0 \neq x \in I$ and let $0 \neq y \in J$. Then $xy \neq 0$, as A is integral, and $xy \in I \cap J$;

(b) Oui, si $x \neq 0$ alors x est inversible et donc $(x) = K$ car $1 \in (x)$ car $1 = x^{-1}x$.

Pour les points (e) et (f), l'argument suivant s'applique. Soit $x \in K$ non-nul. Alors $Kx = K$. En particulier, il existe $y \in K$ tel que $yx = 1$. Comme $Ky = K$, il existe $z \in K$ tel que $zy = 1$. En multipliant par x à droite, on obtient, $zyx = x$, et donc $z = x$. Ainsi y est un inverse à droite et à gauche de x.

□

Exercice 4.
Soit G un groupe fini non-trivial. Considérons l'anneau $\mathbb{Z}[G]$.

1. Supposons que $g \in G$ soit non-trivial et que $g^2 = e$. Montrez que $1 - g$ et $1 + g$ sont des diviseurs de zéro.

2. Plus généralement, montrez que si $g \in G$ est non-trivial, alors $1 - g$ est un diviseur de zéro.

Corrigé. Notons G multiplicativement, et les éléments de $\mathbb{Z}[G]$ comme des sommes $\sum_{g \in G} a(g)e_g$ où $a(g) \in \mathbb{Z}$. Nous noterons ϵ l'élément neutre de G (donc en particulier $\epsilon = 1$ dans $\mathbb{Z}[G]$).

1. On a que $(1 - e_g)(1 + e_g) = 1 - e_g + e_g - e_{g^2} = 1 - e_\epsilon = 0$, alors que vu que $g \neq \epsilon$, ni $1 - e_g$ ni $1 + e_g$ ne sont triviaux.

2. Prenons $g \in G$ distinct de l'élément neutre $\epsilon \in G$. Puisque G est fini et que g n'est pas l'élément neutre, il existe $n > 1$ tel que $g^n = \epsilon$. On a alors :

$$0 = e_\epsilon - e_{g^n} = (e_\epsilon - e_g)(e_\epsilon + e_g + e_{g^2} + \cdots + e_{g^{n-1}})$$

et ni $e_\epsilon - e_g$ ni $e_\epsilon + e_g + \cdots + e_{g^{n-1}}$ ne sont égaux à zéro.

□

Exercice 5.
Montrez qu'il existe exactement 4 morphismes d'anneaux $\mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$.
Indication : si $f\colon \mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$ est un homomorphisme, étudiez les images possibles des éléments de S_3.

Corrigé. Par souci de clarté, si G est un groupe fini nous écrirons les éléments de $\mathbb{Z}[G]$ sous la forme $\sum_{g \in G} a(g)e_g$, où $a(g) \in \mathbb{Z}$.

Soit $f\colon \mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$ un homomorphisme. Puisque $(123)^3$ est l'élément neutre de S_3, on doit avoir

$$f(e_{(123)})^3 = (1,1).$$

On peut écrire $f(e_{(123)}) = (n,m)$ pour certains $n, m \in \mathbb{Z}$, et donc il faut que $n^3 = m^3 = 1$. Ainsi, on a que

$$f(e_{(123)}) = (1,1).$$

Faisons le même raisonemment pour $e_{(12)}$. Si $f(e_{(12)}) = (a,b)$, alors on obtient que $a^2 = b^2 = 1$, et ainsi (a,b) vaut $(1,1), (1,-1), (-1,1)$ ou $(-1,-1)$.

Puisque (12) et (123) génèrent S_3, la connaissance de $f(e_{(123)})$ et de $f(e_{(12)})$ permet de déterminer f entièrement. On voit donc qu'il existe au plus 4 possibilités pour f.

Pour montrer qu'il existe exactement 4 morphismes, on peut montrer à la main avec les formules qu'envoyer les 2-cycles sur $(a,b) \in \{(1,1), (-1,1), (1,-1), (-1,-1)\}$ et les 3-cycles ainsi que l'élément neutre sur $(1,1)$ se prolonge en unique morphisme. Pour démontrer cela on peut passer par l'argument suivant, qui met en situation ce "prolongement".

L'idée est la suivante: de manière similare au cas des polynômes, la donnée d'un morphisme $R[G] \to S$ pour S un anneau commutatif est *exactement* la même chose que la donnée d'un morphism d'anneaux $R \to S$ et celle d'un morphisme de groupes $G \to (S^\times, \cdot)$. Expliquons cela un peu plus.

Si l'on a un morphisme d'anneaux $f\colon R[G] \to S$, alors on peut précomposer par l'injection canonique $R \to R[G]$ pour obtenir un morphisme d'anneaux $R \to S$. De plus, les éléments de G sont nécessairement envoyés sur des unités de S. En effet, $f(e_g)f(e_{g^{-1}}) = f(e_g e_{g^{-1}}) = f(1) = 1$. Ainsi, on voit que l'on obtient un morphisme de groupes $G \to (S^\times, \cdot)$ donné par $g \mapsto f(e_g)$.

Voyons l'autre sens de la bijection. Si l'on a un morphisme d'anneaux $\theta\colon R \to S$ et un morphisme de groupes $\phi\colon G \to (S^\times, \cdot)$, alors on peut définir $f\colon R[G] \to S$ par

$$f\left(\sum_{g \in G} a(g)e_g\right) = \sum_{g \in G} \theta(a(g))\phi(g) \in S.$$

En utilisant la commutativité de S, on peut montrer que cela est bien un morphisme d'anneaux.

Revenons maintenant à notre cas. On veut comprendre les morphismes d'anneaux $\mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$. Par ce que l'on a dit précédemment, il suffit donc de comprendre les morphismes d'anneaux $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ et les morphismes de groupes $S_3 \to (\mathbb{Z} \times \mathbb{Z})^\times$.

Pour les morphismes d'anneaux, vu que 1 doit être préservé (et donc ici envoyé sur $(1,1)$), on en déduit par la compatibilité avec l'addition que pour tout $n \in \mathbb{Z}$, son image est obligatoirement

$(n, n) \in \mathbb{Z} \times \mathbb{Z}$. Ainsi, il y a bien un unique morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ (notez que cet argument montre que pour *tout* anneau R, il y a un unique morphisme $\mathbb{Z} \to R$).

Etudions maintenant les morphisme de groupes $S_3 \to (\mathbb{Z} \times \mathbb{Z})^\times$. Vu que $(\mathbb{Z} \times \mathbb{Z})^\times = \mathbb{Z}^\times \times \mathbb{Z}^\times$ et que $\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$, on en déduit qu'un morphisme de groupes $S_3 \to (\mathbb{Z} \times \mathbb{Z})^\times$ est la même chose que deux morphismes de groups $S_3 \to \mathbb{Z}/2\mathbb{Z}$.

Nous allons montrer qu'il n'y a en fait que 2 tels morphismes (et donc bien quatre morphismes $\mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$ par notre discussion précédente). Donnons deux preuves:

- Vu que $\mathbb{Z}/2\mathbb{Z}$ est abélien, un morphisme $S_3 \to \mathbb{Z}/2\mathbb{Z}$ doit nécessairement contenir $[S_3, S_3] = \langle (123) \rangle$ dans son noyau. Ainsi, il se factorise automatiquement par $S_3/\langle (123) \rangle \cong \mathbb{Z}/2\mathbb{Z}$, et il suffit donc d'étudier les morphismes $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Il n'y a que deux tels morphismes: le morphisme trivial et l'identité.

- Vu que $(123) \in S_3$ est d'ordre 3, l'ordre de son image doit diviser 3. Etant donné que $\mathbb{Z}/2\mathbb{Z}$ n'a aucun élément d'ordre 3, on obtient que le noyau d'un morphisme $g\colon S_3 \to \mathbb{Z}/2\mathbb{Z}$ doit contenir (123). Ainsi, il se factorise par $S_3/\langle (123) \rangle \cong \mathbb{Z}/2\mathbb{Z}$. On conclut comme juste au-dessus.

□