Université de Rennes 1 Année universitaire 2020-2021
Licence de mathématiques
Module Anneaux et arithmétique

Solution de l'exercice 3.4

Exercice

Soit d un entier supérieur à 2 et sans facteur carré, c'est-à-dire tel que pour tout nombre premier p, p^2 ne divise pas d.

1. Montrer que $\sqrt{d} \notin \mathbf{Q}$ et que le polynôme $X^2 - d$ est irréductible dans $\mathbf{Q}[X]$.
   Solution *: Pour tout nombre premier p, on note ν_p la valuation p-adique associée ; rappelons que $\nu_p(0) = +\infty$ et pour tout entier n non nul, $\nu_p(n)$ est le plus grand entier ν tel que p^ν divise n, en d'autres termes $\nu_p(n)$ est l'exposant de p dans la décomposition en facteurs premiers de n ; rappelons aussi que pour tous $n, m \in \mathbf{Z}$ on a $\nu_p(nm) = \nu_p(n) + \nu_p(m)$; en particulier d est sans facteur carré si et seulement si pour tout nombre premier p qui divise d on a $\nu_p(d) = 1$.* NB : *au lieu de raisonner avec les valuations p-adiques, on peut raisonner directement sur les décompositions en facteurs premiers ; cela ne change pas fondamentalement la nature des arguments ci-dessous ; l'avantage des valuations p-adiques est qu'elles permettent d'en donner une version condensée, à la fois plus facile à écrire et plus lisible.*

   Raisonnons par l'absurde et supposons qu'il existe $n, m \in \mathbf{Z} \setminus \{0\}$ tels que $\left(\frac{n}{m}\right)^2 = d$. On a donc $n^2 = d.m^2$. Soit p un facteur premier de d. Comme d est sans facteur carré, on a $\nu_p(d) = 1$. On a donc $\nu_p(n^2) = \nu_p(d.m^2)$ soit $2\nu_p(n) = \nu_p(d) + 2\nu_p(m)$. En particulier, $\nu_p(d) = 2(\nu_p(m) - \nu_p(n))$ est pair. Ceci contredit le fait que $\nu_p(d) = 1$. Donc $\sqrt{d} \notin \mathbf{Q}$. Ainsi on a également $-\sqrt{d} \notin \mathbf{Q}$. Remarque : *l'argument ci-dessus montre qu'au lieu de supposer d sans facteur carré, on aurait pu adopter l'hypothèse plus faible suivante : « il existe un nombre premier p tel que $\nu_p(d) = 1$ », voire même « il existe un nombre premier p tel que $\nu_p(d)$ est impair » ; on pourra d'ailleurs essayer de montrer que cette dernière propriété est équivalente au fait que d n'est pas un carré dans $\mathbf{Z}$; on notera que si d est un carré dans $\mathbf{Z}$, $\sqrt{d}$ est entier donc rationnel.*

   Les racines du polynôme $X^2 - d$ dans $\mathbf{R}$ sont $\sqrt{d}$ et $-\sqrt{d}$. Comme ces racines ne sont pas dans $\mathbf{Q}$, ceci montre que le polynôme $X^2 - d$ n'a pas de racine dans $\mathbf{Q}$. Comme c'est un polynôme de degré 2, et $\mathbf{Q}$ est un corps, on en déduit que ce polynôme est un élément irréductible de $\mathbf{Q}[X]$.

2. Soit $A = \{a + b\sqrt{d}, \quad (a, b) \in \mathbf{Q}^2\}$; montrer que A est un sous-corps de $\mathbf{R}$ isomorphe à $\mathbf{Q}[X]/\langle X^2 - d\rangle$. Si $(a, b) \in \mathbf{Q}^2 \setminus \{(0, 0)\}$, montrer que $a + b\sqrt{d}$ est inversible dans A et expliciter son inverse.
   Solution *:* Remarque préliminaire : *On utilise dans ce qui suit le résultat suivant, qui ne figure pas dans le cours et découle a priori facilement de l'unicité de l'inverse d'un élément inversible d'un anneau (*Mea culpa : *cette dernière propriété aurait pu figurer explicitement dans le cours). Soit B un anneau, A un sous-anneau de B, a un élément de A ; on suppose que $a \in B^\times$; soit a' l'inverse de a dans B ; alors $a \in A^\times$ si et seulement si $a' \in A$; et dans ce cas l'inverse de a dans A est a'.*

   Soit $\varphi\colon \mathbf{Q}[X] \to \mathbf{R}$ l'unique morphisme de $\mathbf{Q}$-algèbres qui envoie X sur $\sqrt{d}$. En d'autres termes, pour tout élément P de $\mathbf{Q}[X]$, on a $\varphi(P) = P(\sqrt{d})$.

Montrons que $\varphi(\mathbf{Q}[X]) = A$. *Montrons d'abord l'inclusion* $A \subset \varphi(\mathbf{Q}[X])$. *Soit* $(a,b) \in \mathbf{Q}^2$. *Soit* $P = a + bX \in \mathbf{Q}[X]$. *Alors* $\varphi(P) = a + b\sqrt{d}$, *et ainsi* $a + b\sqrt{d} \in \varphi(\mathbf{Q}[X])$. *Ceci montre l'inclusion* $A \subset \varphi(\mathbf{Q}[X])$. *Montrons à présent l'inclusion réciproque. Soit* $P \in \mathbf{Q}[X]$. *Comme* $\mathbf{Q}$ *est un corps et* $X^2 - d$ *est non nul, la division euclidienne de* P *par* $X^2 - d$ *existe : soit* $Q, R \in \mathbf{Q}[X]$ *tels que* $P = Q \cdot (X^2 - d) + R$ *et* $\deg(R) < \deg(X^2 - d) = 2$. *Comme* $\deg(R) \leqslant 1$, *il existe* $a, b \in \mathbf{Q}$ *tels que* $R = a + bX$. *Par ailleurs l'application de* φ *à l'égalité* $P = Q \cdot (X^2 - d) + R$ *donne l'égalité* $P(\sqrt{d}) = Q(\sqrt{d}) \cdot 0 + R(\sqrt{d})$ *soit* $P(\sqrt{d}) = a + b\sqrt{d}$. *Ainsi* $\varphi(P) = P(\sqrt{d})$ *est un élément de* A. *Ceci montre l'inclusion* $\varphi(\mathbf{Q}[X]) \subset A$.

Montrons à présent l'égalité $\mathrm{Ker}(\varphi) = \langle X^2 - d \rangle$. *On a* $\varphi(X^2 - d) = (\sqrt{d})^2 - d = 0$ *donc* $X^2 - d \in \mathrm{Ker}(\varphi)$. *Comme* $\mathrm{Ker}(\varphi)$ *est un idéal,* $\mathrm{Ker}(\varphi)$ *contient donc aussi l'idéal engendré par* $X^2 - d$, *c'est à dire* $\langle X^2 - d \rangle$. *Ceci montre l'inclusion* $\langle X^2 - d \rangle \subset \mathrm{Ker}(\varphi)$. *Montrons l'inclusion réciproque. Soit* $P \in \mathrm{Ker}(\varphi)$. *Soit* $Q, R \in \mathbf{Q}[X]$ *tels que* $P = Q \cdot (X^2 - d) + R$ *et* $\deg(R) < \deg(X^2 - d) = 2$ *(cf. ci-dessus). Soit* $a, b \in \mathbf{Q}$ *tels que* $R = a + bX$. *L'application de* φ *à l'égalité* $P = Q \cdot (X^2 - d) + R$ *donne l'égalité* $0 = Q(\sqrt{d}) \cdot 0 + R(\sqrt{d})$ *soit* $a + b\sqrt{d} = 0$. *Si* b *était non nul, on en déduirait que* $\sqrt{d} = -\frac{a}{b}$ *serait un élément de* $\mathbf{Q}$, *ce qui contredit le résultat de la question précédente. Donc* $b = 0$ *et il s'ensuit aussitôt que* $a = 0$. *Donc* $R = 0$ *et* $P = Q \cdot (X^2 - d)$. *En d'autres termes* $P \in \langle X^2 - d \rangle$. *Ceci montre l'inclusion* $\mathrm{Ker}(\varphi) \subset \langle X^2 - d \rangle$ *et achève de montrer l'égalité* $\mathrm{Ker}(\varphi) = \langle X^2 - d \rangle$.

Comme φ *est un morphisme d'anneaux,* $A = \varphi(\mathbf{Q}[X])$ *est un sous-anneau de* $\mathbf{R}$. *Par ailleurs* φ *induit par corestriction un morphisme d'anneaux surjectif* $\mathbf{Q}[X] \to A$ *de même noyau que* φ. *Un tel morphisme induit donc un isomorphisme de* $\mathbf{Q}[X]/\langle X^2 - d \rangle$ *sur* A. *Comme* $X^2 - d$ *est irréductible dans* $\mathbf{Q}[X]$ *(question précédente) et* $\mathbf{Q}$ *est un corps,* $\langle X^2 - d \rangle$ *est un idéal maximal de* $\mathbf{Q}[X]$. *Donc* $\mathbf{Q}[X]/\langle X^2 - d \rangle$ *est un corps, et ainsi au vu l'isomorphisme ci-dessus* A *est également un corps. Finalement* A *est bien un sous-corps de* $\mathbf{R}$.

Soit $(a,b) \in \mathbf{Q}^2 \setminus \{(0,0)\}$. *Alors* $a + b\sqrt{d} \neq 0$ *et* $a - b\sqrt{d} \neq 0$ *(cf. argument ci-dessus) et comme* A *est un corps,* $a + b\sqrt{d}$ *est inversible dans* A. *Pour calculer son inverse, il suffit de calculer son inverse dans* $\mathbf{R}$ *(ici par « calculer » on entend : expliciter* $\alpha, \beta \in \mathbf{Q}$ *tels que l'inverse s'écrit* $\alpha + \beta\sqrt{d}$*). On peut écrire*

$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{(a + b\sqrt{d})(a - b\sqrt{d})} = \frac{a - b\sqrt{d}}{a^2 - d \cdot b^2} = \underbrace{\frac{a}{a^2 - d \cdot b^2}}_{\in \mathbf{Q}} + \underbrace{\left(-\frac{b}{a^2 - d \cdot b^2}\right)}_{\in \mathbf{Q}} \sqrt{d}.$$

Remarque : *ce calcul redémontre en fait que pour tout* $(a,b) \in \mathbf{Q}^2 \setminus \{(0,0)\}$, $a + b\sqrt{d}$ *est inversible dans* A *; en d'autres termes il redémontre que tout élément non nul de* A *est inversible. Ainsi on pouvait démontrer que* A *est un corps sans utiliser l'isomorphisme entre* A *et* $\mathbf{Q}[X]/\langle X^2 - d \rangle$.

Remarque finale : *la stratégie utilisée pour montrer que* A *et* $\mathbf{Q}[X]/\langle X^2 - d \rangle$ *sont isomorphes, dont la clef de voute est le fameux mantra « pour montrer que* B *et* A/I *sont isomorphes, il suffit de construire un morphisme de* A *vers* B *surjectif de noyau* I *», est très semblable à celle utilisée dans d'autres exercices pour montrer par exemple que* $\mathbf{Z}[i]$ *et* $\mathbf{Z}[X]/\langle X^2 + 1 \rangle$ *(ou encore* $\mathbf{Z}[i\sqrt{3}]$ *et* $\mathbf{Z}[X]/\langle X^2 + 3 \rangle$*) sont isomorphes. On notera cependant la différence fondamentale qui suit : dans le cas présent l'anneau de coefficients* $\mathbf{Q}$ *est un corps ; ainsi le fait que* $X^2 - d$ *est unitaire ne joue pas de rôle particulier dans l'argument,*

alors que c'était crucial dans le cas de $\mathbf{Z}[i]$ *et* $\mathbf{Z}[i\sqrt{3}]$*. En outre, même s'il est vrai que* X^2+1 *et* X^2+3 *sont des éléments irréductibles de* $\mathbf{Z}[X]$ *(attention, on ne peut pas raisonner ici uniquement sur les racines ;* $2(X^2+1)$ *n'est pas un élément irréductible de* $\mathbf{Z}[X]$ *; on en dira un peu plus à ce sujet dans le dernier chapitre du cours), on ne peut pas en déduire que* $\mathbf{Z}[i]$ *et* $\mathbf{Z}[i\sqrt{3}]$ *sont des corps. De fait, ce n'en sont pas. Par exemple* $2+2i$ *est un élément non nul mais non inversible dans* $\mathbf{Z}[i]$ *; pour le montrer, il suffit de constater que son inverse dans* $\mathbf{C}$*, à savoir* $\frac{1}{2}(1-i)$*, n'est pas un élément de* $\mathbf{Z}[i]$*.*