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

Contrôle continu n°2
Jeudi 8 avril 2021, 16h15 – 17h45
Corrigé

Exercice 1

1. Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$. Rappeler la définition de « P est un élément irréductible de $\mathbf{K}[X]$ »
Solution *: Parmi les définitions équivalentes possibles, voici celle donnée dans le cours : un polynôme $P \in \mathbf{K}[X]$ est* irréductible *si et seulement s'il est non constant et toute factorisation $P = QR$, avec $Q, R \in \mathbf{K}[X]$, entraîne que soit Q, soit R est constant.*

2. Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ un polynôme de degré 2 ou 3 qui n'a pas de racine dans $\mathbf{K}$. Montrer que P est un élément irréductible de $\mathbf{K}[X]$.
Solution *: Comme P est de degré 2 ou 3, il est non constant. Soit $Q, R \in \mathbf{K}[X]$ tels que $P = QR$. Il s'agit de montrer que Q est constant ou R est constant. On a $\deg(P) = \deg(QR) = \deg(Q) + \deg(R)$. Ainsi $\deg(Q) + \deg(R) \in \{2, 3\}$. Par ailleurs on a $\deg(Q) \in \mathbf{N}$ et $\deg(R) \in \mathbf{N}$. Enfin, comme $\mathbf{K}$ est un corps, un polynôme de $\mathbf{K}[X]$ de degré 1 a toujours une racine dans $\mathbf{K}$. Comme Q et R divisent P et que P n'a pas de racine dans $\mathbf{K}$, on a $\deg(Q) \neq 1$ et $\deg(R) \neq 1$. La seule décomposition de 2 (resp. de 3) comme somme d'entiers naturels dont aucun ne vaut 1 est $2 = 0 + 2$ (resp. $3 = 0 + 3$). Donc $\deg(Q) = 0$ ou $\deg(R) = 0$, en d'autres termes Q est constant ou R est constant. Donc P est bien irréductible.*

3. Donner un exemple d'un corps $\mathbf{K}$ et d'un élément $P \in \mathbf{K}[X]$ de degré 4 qui n'a pas de racine dans $\mathbf{K}$ et n'est pas irréductible dans $\mathbf{K}[X]$ dans les cas suivants :
   (a) $\mathbf{K}$ est de caractéristique 0
   Solution *: Prenons $\mathbf{K} = \mathbf{R}$ (qui est bien de caractéristique 0) et $P = (X^2 + 1)^2$ qui est bien de degré 4. Pour tout $x \in \mathbf{R}$, on a $(x^2 + 1)^2 > 0$. Donc P n'a pas de racine dans $\mathbf{R}$. Posant $Q = R = X^2 + 1$, on voit que $P = QR$ alors que ni Q, ni R n'est constant. Donc P n'est pas irréductible dans $\mathbf{R}[X]$.*

   (b) $\mathbf{K}$ est de caractéristique 2
   Solution *: Prenons $\mathbf{K} = \mathbf{F}_2$ (qui est bien de caractéristique 2) et $P = (X^2 + X + [1]_2)^2$ qui est bien de degré 4. On a $\mathbf{F}_2 = \{[0]_2, [1]_2\}$ et par ailleurs*

$$P([0]_2) = ([0]_2^2 + [0]_2 + [1]_2)^2 = [1]_2^2 = [1]_2 \neq [0]_2,$$

$$P([1]_2) = ([1]_2^2 + [1]_2 + [1]_2)^2 = [3]_2^2 = [1]_2 \neq [0]_2.$$

   Donc P n'a pas de racine dans $\mathbf{F}_2$. Posant $Q = R = X^2 + X + [1]_2$, on voit que $P = QR$ alors que ni Q, ni R n'est constant. Donc P n'est pas irréductible dans $\mathbf{F}_2[X]$.

4. Dans toute la suite de l'exercice, on suppose que P est l'élément de $\mathbf{F}_3[X]$ donné par $P := X^3 + [2]_3 X + [1]_3$. On pose $\mathbf{K} := \mathbf{F}_3[X]/\langle P \rangle$. Justifier que $\mathbf{K}$ est un corps.

Solution : *On a* $\mathbf{F}_2 = \{[0]_3, [1]_3, [2]_3\}$ *et par ailleurs*

$$P([0]_3) = [0]_3^3 + [2]_3[0]_3 + [1]_3 = [1]_3 = [1]_3 \neq [0]_3,$$

$$P([1]_3) = [1]_3^3 + [2]_3[1]_3 + [1]_3 = [4]_3 = [1]_3 \neq [0]_3,$$

$$P([2]_3) = [2]_3^3 + [2]_3[2]_3 + [1]_3 = [13]_3 = [1]_3 \neq [0]_3.$$

Ainsi P *n'a pas de racine dans* $\mathbf{F}_3$*. Comme il est de degré* 3*, on sait d'après la question 2 que* P *est un élément irréductible de* $\mathbf{F}_3[X]$*. Comme* $\mathbf{F}_3$ *est un corps, on en déduit que* $\langle P\rangle$ *est un idéal maximal de* $\mathbf{F}_3[X]$*, et donc que* $\mathbf{K} = \mathbf{F}_3[X]/\langle P\rangle$ *est un corps.*
On note π le morphisme quotient $\mathbf{F}_3[X] \to \mathbf{K}$ et $\alpha := \pi(X)$. Donner, *sans justification*, le cardinal de $\mathbf{K}$ et une base du $\mathbf{F}_3$-espace vectoriel $\mathbf{K}$.
Solution : $\mathbf{K}$ *est de cardinal* $3^3 = 27$*. Une base du* $\mathbf{F}_3$*-espace vectoriel* $\mathbf{K}$ *est* $\{[1]_3, \alpha, \alpha^2\}$.
Dans toute la suite, le résultat des calculs dans $\mathbf{K}$ devront être exprimés dans cette base.

5. Calculer α^2, α^4, α^8.
Solution : *Comme* P *est dans le noyau de* π *et* $\pi(X) = \alpha$*, on a* $\alpha^3 + [2]_3\alpha + [1]_3 = [0]_3$*, soit* $\alpha^3 = \alpha + [2]_3$.
L'élément α^2 *est déjà décomposé dans la base* $\{[1]_3, \alpha, \alpha^2\}$.
Comme $\alpha^3 = \alpha + [2]_3$*, on a*

$$\alpha^4 = \alpha.\alpha^2 = \alpha^2 + [2]_3\alpha.$$

On en déduit

$$\alpha^8 = (\alpha^4)^2 = (\alpha^2 + [2]_3\alpha)^2 = \alpha^4 + [4]_3\alpha^3 + \alpha^2.$$

Ainsi

$$\alpha^8 = (\alpha^2 + [2]_3\alpha) + (\alpha + [2]_3) + \alpha^2 = [2]_3\alpha^2 + [2]_3.$$

En déduire α^{13}. On vérifiera que $\alpha^{13} = [2]_3$.
Solution : *On a*

$$\alpha^{13} = \alpha^8 \cdot \alpha^4 \cdot \alpha$$

soit

$$\alpha^{13} = ([2]_3\alpha^2 + [2]_3) \cdot (\alpha^2 + [2]_3) \cdot \alpha.$$

Or

$$([2]_3\alpha^2 + [2]_3) \cdot (\alpha^2 + [2]_3\alpha) = [2]_3\alpha^4 + \alpha^3 + [2]_3\alpha^2 + \alpha$$

d'où

$$([2]_3\alpha^2 + [2]_3) \cdot (\alpha^2 + [2]_3\alpha) = ([2]_3\alpha^2 + \alpha) + (\alpha + [2]_3) + [2]_3\alpha^2 + \alpha.$$

soit

$$([2]_3\alpha^2 + [2]_3) \cdot (\alpha^2 + [2]_3\alpha) = \alpha^2 + [2]_3$$

On en tire

$$\alpha^{13} = (\alpha^2 + [2]_3)\alpha = \alpha^3 + [2]_3\alpha$$

soit

$$\alpha^{13} = (\alpha + [2]_3) + [2]_3\alpha) = [2]_3.$$

6. Déduire de la question précédente un générateur de $\mathbf{K}^\times$.
Solution *: Comme* $\mathbf{K}$ *est de cardinal* 27 *et* $\mathbf{K}$ *est un corps, le groupe* $\mathbf{K}^\times$ *est de cardinal* 26*, qui se décompose en facteurs premiers comme* $26 = 2 \cdot 13$*. Comme* $\{[1]_3, \alpha, \alpha^2\}$ *est une base du* $\mathbf{F}_3$*-espace vectoriel* $\mathbf{K}$*, les éléments* α *et* α^2 *sont distincts de* $[1]_3$*. Par ailleurs la question précédente montre que* α^{13} *est distinct de* $[1]_3$*. Comme* $\mathbf{K}^\times$ *est de cardinal* 26*, l'ordre de* α *est un diviseur positif de* 26*, mais par ailleurs on sait que cet ordre n'est pas dans l'ensemble* $\{1, 2, 13\}$*. Donc* α *est d'ordre* 26 *et est donc un générateur de* $\mathbf{K}^\times$*.*

7. *Pour cette question, on demande de ne pas utiliser les résultats du cours sur les cardinaux des sous-corps des corps finis.* Existe-t-il un élément β de $\mathbf{K}$ tel que $\beta^8 = [1]_3$?
Solution *: Bien sûr ! On prend* $\beta = [1]_3$ *(l'énoncé aurait du être : existe-t-il un élément* β *de* $\mathbf{K}^\times$ *d'ordre* 8 *?)*
Existe-t-il un sous-corps de $\mathbf{K}$ de cardinal 3 ?
Solution *: Oui :* $\mathbf{F}_3$ *est un sous-corps de* $\mathbf{K}$ *de cardinal* 3*.*
de cardinal 9 ?
Solution *: Non : si un tel sous-corps* $\mathbf{L}$ *existait, comme* $\mathbf{L}^\times$ *est cyclique, il existerait dans* $\mathbf{K}^\times$ *un élément d'ordre* $9 - 1 = 8$*. Mais* $\mathbf{K}^\times$ *est de cardinal* 26 *et* 8 *ne divise pas* 26*, donc l'existence d'un tel élément contredirait le théorème de Lagrange.*
Autre argument : on peut invoquer le fait que si $\mathbf{L}$ *est un sous-corps de* $\mathbf{K}$*,* $\mathbf{K}$ *est muni d'une structure de* $\mathbf{L}$*-espace vectoriel (c'est un fait général) pour laquelle il est de dimension finie (car il est fini de toute façon). Ainsi le cardinal de* $\mathbf{K}$ *est nécessairement une puissance du cardinal de* $\mathbf{L}$*, ce qui impose* $card(\mathbf{L}) \in \{3, 27\}$*.*
de cardinal n, pour $n \in \mathbf{N} \setminus \{3, 9\}$?
Solution *: Oui pour* $n = 27$ *:* $\mathbf{K}$ *lui-même...*
Non pour $n \in \mathbf{N} \setminus \{3, 9, 27\}$ *(déjà vu ci-dessus).*

8. **(*)** Soit $Q \in \mathbf{F}_3[X]$ de degré 2 et vérifiant $\forall a \in \mathbf{F}_3$, $Q(a) \neq 0$. Montrer que Q est un élément irréductible de $\mathbf{K}[X]$.
Solution *: Comme* Q *est de degré* 2 *et n'a pas de racine dans* $\mathbf{F}_3$*,* Q *est un élément irréductible de* $\mathbf{F}_3$*. En particulier,* $\mathbf{L} := \mathbf{F}_3[X]/\langle P \rangle$ *est un corps de cardinal* $3^{\deg(Q)} = 3^2$*. Toujours comme* Q *est de degré* 2*, pour montrer que* Q *est un élément irréductible de* $\mathbf{K}[X]$ *il suffit de montrer que* Q *n'a pas de racine dans* $\mathbf{K}$*. Supposons qu'il existe* $\beta \in \mathbf{K}$ *qui vérifie* $Q(\beta) = 0$*. Soit* φ *l'unique morphisme de* $\mathbf{F}_3$*-algèbre de* $\mathbf{F}_3[X]$ *vers* $\mathbf{K}$ *qui envoie* X *sur* β*. Comme* $Q(\beta) = 0$*, le noyau de* φ *contient* Q *et donc l'idéal* $Q \cdot \mathbf{F}_3[X]$*. Ainsi* φ *induit un morphisme* $\psi \colon \mathbf{L} = \mathbf{F}_3[X]/\langle Q \rangle \to \mathbf{K}$*. Comme* $\mathbf{L}$ *est un corps et* $\mathbf{K}$ *n'est pas l'anneau nul,* ψ *est injectif, et son image est donc un sous-corps de* $\mathbf{K}$ *de cardinal* 9 *ce qui contredit un résultat de la question précédente.*

Exercice 2

Soit A un anneau. Pour tout idéal I de A, on pose $\sqrt{I} := \{a \in A, \quad \exists n \in \mathbf{N} \setminus \{0\}, \quad a^n \in I\}$.

1. Soit I un idéal de A. Montrer que $\sqrt{I}$ est un idéal de A qui contient I. L'idéal I est dit *radical* s'il vérifie $\sqrt{I} = I$.
Solution *: (tirée de la correction du CC1 d'ANAR de 2019) Montrons que* $\sqrt{I}$ *est un sous-groupe de* A*.*
On a $0^1 = 0$ *or* $0 \in I$ *car* I *est un idéal de* A*, donc* $0 \in \sqrt{I}$
Soit $x \in \sqrt{I}$ *et* $n \in \mathbf{N} \setminus \{0\}$ *tel que* $x^n \in I$*. Alors* $(-x)^n = (-1)^n x$*. Comme* I *est un sous-groupe de* A *et* $x^n \in I$*, on a* $(-1)^n x \in I$*. Donc* $-x \in \sqrt{I}$*.*
Soit $x, y \in \sqrt{I}$*,* $n \in \mathbf{N} \setminus \{0\}$ *tel que* $x^n \in I$ *et* $m \in \mathbf{N} \setminus \{0\}$ *tel que* $y^m \in I$*.*
Notons que si $r \in \mathbf{N}$*, comme* $x^{n+r} = x^n x^r$ *et* I *est un idéal, on a* $x^{n+r} \in I$*. De même*

$y^{m+r} \in I$.
D'après la formule du binôme de Newton, on a

$$(x+y)^{n+m} = \sum_{\substack{p,q\in\mathbf{N}\\ p+q=n+m}} \binom{n}{p} x^p y^q.$$

Soit $p, q \in \mathbf{N}$ tel que $p+q = n+m$. Si $p < n$ et $q < m$, on a $p+q < n+m$ ce qui est absurde. Donc soit $p \geqslant n$, soit $q \geqslant m$. Si $p \geqslant n$, d'après la remarque ci-dessus, on a $x^p \in I$. Comme I est un idéal, on a alors $\binom{n}{p}x^p y^q \in I$. Si $q \geqslant m$, on a $y^q \in I$ et donc là encore $\binom{n}{p}x^p y^q \in I$.
Ainsi $(x+y)^{n+m}$ s'écrit comme une somme d'éléments de I, donc est dans I. Donc $x+y \in \sqrt{I}$.
Ainsi $\sqrt{I}$ est bien un sous-groupe de A.
Soit $x \in \sqrt{I}$, $n \in \mathbf{N}\setminus\{0\}$ tel que $x^n \in I$ et $y \in A$. Alors $(xy)^n = x^n y^n$. Comme $x^n \in I$ et I est un idéal, on a $x^n y^n \in I$. Donc $xy \in \sqrt{I}$.
Ceci achève de montrer que $\sqrt{I}$ est un idéal de A.
Montrons que $I \subset \sqrt{I}$. Soit $x \in I$. On a $x^1 = x$ donc $x^1 \in I$ et donc $x \in \sqrt{I}$, ce qui conclut.
Notons que ce dernier résultat montre que pour établir qu'un idéal I est radical, il suffit de montrer l'inclusion $\sqrt{I} \subset I$, cette inclusion étant équivalente à la propriété :

$$\forall a \in A, \quad (\exists n \in \mathbf{N}\setminus\{0\}, a^n \in I) \Rightarrow a \in I$$

2. Soit I un idéal de A. Montrer que l'idéal $\sqrt{I}$ est radical.
Solution *: Soit $a \in A$ et $n \in \mathbf{N}\setminus\{0\}$ tel que $a^n \in \sqrt{I}$. Il s'agit de montrer que $a \in \sqrt{I}$. Par définition de $\sqrt{I}$ il existe $m \in \mathbf{N}\setminus\{0\}$ tel que $(a^n)^m \in I$. Ainsi $a^{nm} \in I$. Toujours par définition de $\sqrt{I}$, on en déduit que $a \in \sqrt{I}$, ce qui conclut.*

3. Soit B un anneau, $\varphi\colon A \to B$ un morphisme d'anneaux et J un idéal radical de B. L'idéal $\varphi^{-1}(J)$ est-il nécessairement un idéal radical de A ?
Solution *: Soit $a \in A$ et $n \in \mathbf{N}\setminus\{0\}$ tel que $a^n \in \varphi^{-1}(J)$. Ainsi $\varphi(a^n) \in J$. Comme φ est un morphisme d'anneaux, on a $\varphi(a^n) = \varphi(a)^n$. Donc $\varphi(a)^n \in J$. Comme J est radical, on en déduit $\varphi(a) \in J$, soit $a \in \varphi^{-1}(J)$. Ainsi $\varphi^{-1}(J)$ est bien un idéal radical de A.*

4. L'idéal $6\mathbf{Z}$ est-il un idéal radical de $\mathbf{Z}$?
Solution *: Oui. Montrons-le. Soit $a \in \mathbf{Z}$ et $n \in \mathbf{N}\setminus\{0\}$ tel que $a^n \in 6\mathbf{Z}$, c'est-à-dire tel que 6 divise a^n. Comme $6 = 2\times 3$, on en déduit que 2 divise a^n et 3 divise a^n. Comme 2 et 3 sont premiers, on en déduit par le lemme d'Euclide que 2 divise a et 3 divise a. Comme 2 et 3 sont premiers entre eux, on en déduit que $6 = 2\times 3$ divise a. Ainsi $a \in 6\mathbf{Z}$. Ceci achève de montrer que $6\mathbf{Z}$ est radical.*
Donner une infinité d'exemples d'idéaux de $\mathbf{Z}$ qui sont radicaux mais pas premiers.
Solution *: Le raisonnement précédent montre que pour n'importe quel nombre premier impair p, l'idéal $2p\mathbf{Z}$ est radical (remplacer 6 par $2p$ et 3 par p). Cet idéal n'est pas premier car $2p$ n'est pas un nombre premier. Et si p et q sont deux nombres premiers impairs deux à deux distincts, $2p$ et $2q$ sont des entiers naturels distincts, donc les idéaux $2p\mathbf{Z}$ et $2q\mathbf{Z}$ sont distincts. Par ailleurs on sait qu'il existe une infinité de nombres premiers impairs. Ainsi la famille $\{2p\mathbf{Z}\}_{p \text{ nombre premier impair}}$ est une famille infinie d'idéaux radicaux non*

premiers de $\mathbf{Z}$.

5. Soit B et C des anneaux non nuls. Montrer que $\sqrt{0}$ (le radical de l'idéal nul) n'est *pas* un idéal premier de $B \times C$.
Solution *: (tirée de la correction du CC1 d'ANAR de 2019) On a* $(0_B, 1_C)(1_B, 0_C) = (0_B, 0_C)$ *et* $(0_B, 0_C) \in \sqrt{0}$*. Cependant, ni* $(0_B, 1_C)$ *ni* $(1_B, 0_C)$ *ne sont des éléments de* $\sqrt{0}$*. En effet, si* n *est un entier strictement positif, on a* $(0_B, 1_C)^n = (0_B^n, 1_C^n) = (0_B, 1_C)$ *et* $(0_B, 1_C) \neq (0_B, 0_C)$ *car* C *n'est pas l'anneau nul. Même raisonnement pour* $(1_B, 0_C)$*. Donc* $\sqrt{0}$ *n'est pas un idéal premier de* $B \times C$*.*

6. **(*)** Donner un exemple d'un anneau A non intègre tel que $\sqrt{0}$ est un idéal premier de A.
Solution *: (tirée de la correction du CC1 d'ANAR de 2019) Prenons* $A = \mathbf{Z}/4\mathbf{Z}$*. On a* $[2]_2^2 = [0]_2$*. Par ailleurs, pour tout entier* n *strictement positif* $[1]_2^n = [1]_2 \neq [0]_2$ *et* $[3]_2^n = [-1]_2^n = [(-1)^n]_2 \neq [0]_2$*.*
Donc $\sqrt{0} = \{[0]_2, [2]_2\}$*, qui est bien un idéal premier : en effet il est propre et on vérifie aussitôt que si* $\{a, b\} = \mathbf{Z}/4\mathbf{Z} \setminus \sqrt{0}$ *on a* $\{a^2, b^2, ab\} \cap \sqrt{0} = \varnothing$*. Plus conceptuellement, on pouvait montrer que* $(\mathbf{Z}/4\mathbf{Z})/\sqrt{0}$ *est isomorphe à* $\mathbf{Z}/2\mathbf{Z}$*. En effet on vérifie facilement que l'unique morphisme d'anneaux* $\mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ *est surjectif et de noyau* $\sqrt{0}$*.*