UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille n°3 : anneaux, anneaux de polynômes

Exercices à savoir faire chez soi

Exercice 1

Soit $\mathbf{K}$ un corps, et $P \in \mathbf{K}[X]$. Les assertions suivantes sont elles vraies ou fausses ? On justifiera bien entendu la réponse.

1 Si P n'a pas de racine dans $\mathbf{K}$, alors P est irréductible dans $\mathbf{K}[X]$.

2 Si P est irréductible dans $\mathbf{K}[X]$, alors P n'a pas de racine dans $\mathbf{K}$.

Exercice 2

Relire soigneusement son cours si besoin, puis, sans le cours, écrire les définitions d'un groupe, d'un sous-groupe, d'un morphisme de groupes, de son noyau, d'un anneau, d'un idéal, d'un morphisme d'anneaux, de son noyau, d'un diviseur de zéro, d'un élément inversible, d'un anneau intègre. Donner le plus d'exemples possible pour chacune de ces notions. Rappeler également les définitions d'une application injective, puis surjective. Si $f : A \to B$ est une application, A' une partie de A et B' une partie de B, rappeler ce que sont $f(A')$ et $f^{-1}(B')$. Donner des exemples.

Exercice 3

Soit G, G', G'' des groupes, $f : G \to G'$ et $g : G' \to G''$ des morphismes de groupes. Montrer que $g \circ f$ est un morphisme de groupes. Mêmes questions avec des morphismes d'anneaux.

Exercice 4

Vrai ou faux ? Soit G et H des groupes notés multiplicativement, $\varphi : G \to H$ un isomorphisme de groupes. Alors pour tout $h \in H$, on a $\varphi^{-1}(h) = \varphi(h)^{-1}$.

Exercices à savoir faire

Exercice 5

Soit $D : \mathbf{R}[X] \to \mathbf{R}[X]$ l'application de dérivation.
Est-ce un morphisme de groupes ? Un morphisme d'anneaux ? Une application linéaire ?

Exercice 6

Déterminer les solutions de l'équation $x^2 - [1]_8 = 0, \quad x \in \mathbf{Z}/8\mathbf{Z}$. Comparer leur nombre au degré du polynôme $X^2 - [1]_8$. Commenter le résultat.

Exercice 7

Soit $P = X^4 + 1$.

1 Factoriser P en produit d'irréductibles dans $\mathbf{C}[X]$.

2 Factoriser P en produit d'irréductibles dans $\mathbf{R}[X]$.

3 Montrer que P ne peut pas se factoriser en produit de deux polynômes de degré 2 à coefficients rationnels (on pourra raisonner par l'absurde, et écrire la division euclidienne de P par l'un de ces facteurs).

4 En déduire que P est irréductible dans $\mathbf{Q}[X]$.

Exercice 8

Montrer que $X^3 + X + [1]_2$ est irréductible dans $\mathbf{F}_2[X]$. Écrire les tables d'adddition et de multiplication dans le corps $\mathbf{F}_2[X]/(X^3 + X + [1]_2)$ (on notera t l'image de X dans le quotient $\mathbf{F}_2[X]/(X^3 + X + [1]_2)$). Montrer que le groupe $(\mathbf{F}_2[X]/(X^3 + X + [1]_2))^\times$ est cyclique et en déterminer un générateur.

Exercice 9

1 Donner la liste des polynômes irréductibles de degré 2 et 3 sur $\mathbf{F}_3[X]$. Même question pour $\mathbf{F}_5[X]$.

2 Donner la liste des polynômes irréductibles de degré 4 dans $\mathbf{F}_2[X]$, puis dans $\mathbf{F}_3[X]$, puis dans $\mathbf{F}_5[X]$.

3 Pour chacun des polynômes P déterminés ci-dessus, donner la liste des éléments de $\mathbf{K}[X]/P$ (on notera t l'image de X dans le quotient), écrire les tables d'addition et de multiplication dans le corps $\mathbf{K}[X]/P$, pour $\mathbf{K} = \mathbf{F}_2$, $\mathbf{F}_3$ ou $\mathbf{F}_5$, vérifier que le groupe $(\mathbf{K}[X]/P)^\times$ est cyclique et en donner un générateur.

Exercice 10

1 Soit n un entier naturel et d un diviseur de n. Montrer que $X^d - 1$ divise $X^n - 1$ (on pourra travailler dans l'anneau quotient $k[X]/(X^d - 1)$).

2 Soit n un entier naturel. Soit d un entier naturel non nul et r le reste de la division euclidienne de n par d. Montrer que $X^r - 1$ est le reste de la division euclidienne de $X^n - 1$ par $X^d - 1$ (on pourra travailler dans $k[X]/(X^d - 1)$).

3 Soient m et n des entiers naturels, et $d = \text{pgcd}(m, n)$. Déduire de ce qui précède que $X^d - 1$ est un pgcd de $X^m - 1$ et $X^n - 1$.

Exercice 11

Soit G, G' des groupes et $f : G \to G'$ un morphisme.

1 Soit H un sous-groupe de G. Montrer que $f(H)$ est un sous-groupe de G'.

2 Soit H' un sous-groupe de G'. Montrer que $f^{-1}(H')$ est un sous-groupe de G.

Exercice 12

$(A, +, \times)$ désigne un anneau supposé distinct de l'anneau nul.

1 Soient I et J deux idéaux de A. Montrer que $I \cap J$ et $I + J \overset{\text{déf}}{=} \{a + b, \quad a \in I,\, b \in J\}$ sont des idéaux de A.

2 Soit $a \in A$. Montrer que $a\,A \overset{\text{déf}}{=} \{a\,b,\, b \in A\}$ est un idéal de A. Soit I un idéal de A contenant a. Montrer que I contient $a\,A$. On dit que aA est l'idéal de A engendré par a.
3 Montrer que $\{0_A\}$ et A sont des idéaux de A. Soit I un idéal de A qui contient un élément inversible. Montrer que $1_A \in I$, puis que $I = A$. Montrer qu'un élément a de A est inversible si et seulement si $a\,A = A$. On suppose A différent de l'anneau nul. Montrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0_A\}$ et A.
4 Soit $(B, \oplus, \otimes)$ un anneau et $f : A \to B$ un morphisme d'anneaux. Soit J un idéal de B. Montrer que $f^{-1}(J)$ est un idéal de A. Soit I un idéal de A. Montrer que si f est surjectif, $f(I)$ est un idéal de B. Ceci est-il encore vrai si f n'est pas surjectif ? (on pourra regarder l'inclusion $\mathbf{Z} \subset \mathbf{Q}$)
5 *(plus délicat).* Soient $a_1, \ldots, a_n$ des éléments de A. Décrire l'idéal engendré par $a_1, \ldots, a_n$. Plus généralement, définir l'idéal engendré par une partie de A (et montrer son existence).
6 *(plus délicat).* Si A est $\mathbf{Z}$ ou $k[X]$, le cours montre que tout idéal de A est engendré par un élément, en d'autres termes est de la forme aA pour un certain $a \in A$. En considérant l'idéal engendré par X et Y dans $k[X, Y]$, montrer que cette propriété n'est plus vérifiée pour $A = k[X, Y]$.

Exercice 13
Soient A et B des anneaux. Montrer qu'on a $(A \times B)^\times = A^\times \times B^\times$.

Exercices à chercher

Exercice 14
1 Déterminer la liste des inversibles de $\mathbf{Z}/15\mathbf{Z}$.
2 Déterminer l'ordre de chaque élément de $(\mathbf{Z}/15\mathbf{Z})^\times$.
3 Déterminer la liste des inversibles de $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$. Déterminer l'ordre de chaque élément dans $(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z})^\times$.
4 Expliciter un isomorphisme de groupes de $(\mathbf{Z}/15\mathbf{Z})^\times$ sur $(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z})^\times$.

Exercice 15
Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbf{Z}[X]$. On veut déterminer toutes les racines rationnelles de P.
1 On suppose que P a une racine rationnelle non nulle x, avec $x = \frac{p}{q}$ et $\text{pgcd}(p, q) = 1$. Montrer que p divise a_0 et q divise a_n.
2 Le polynôme $7X^3 - 5X^2 - 9X + 4$ a-t-il des racines rationnelles ? et $X^4 - 2X^2 - 3$?
3 Soit n un entier naturel. Montrer que $\sqrt{n}$ est soit un entier, soit un irrationnel.

Exercice 16
Montrer que $X^2 + 4$ est irréductible dans $\mathbf{Z}[X]$ mais réductible dans $\mathbf{Z}/2\mathbf{Z}[X]$; en toute rigueur, la deuxième question s'énonce : montrer que l'image de $X^2 + 4$ dans $\mathbf{Z}/2\mathbf{Z}[X]$ par le morphisme naturel $\mathbf{Z}[X] \to \mathbf{Z}/2\mathbf{Z}[X]$ (obtenu en appliquant $n \mapsto [n]_2$ aux coefficients) est réductible.

Exercice 17

Soit p un nombre premier. On s'intéresse aux polynômes irréductibles sur $\mathbf{F}_p$. Expliquer comment déterminer facilement les polynômes irréductibles de degré 2 et 3 sur $\mathbf{F}_p$. Expliquer ensuite comment en déduire les polynômes irréductibles de degré 4, puis 5. Expliquer enfin une procédure générale permettant de déterminer les polynômes irréductibles de degré n sur $\mathbf{F}_p$ avec n quelconque.

Exercice 18

On considère l'application φ : $\begin{array}{ccc} \mathbf{R}[X] & \to & \mathbf{C} \\ P & \mapsto & P(i) \end{array}$

1 Montrer que φ est un morphisme d'anneaux surjectif.

2 Soit $P \in \ker \varphi$. Montrer que P est divisible par X^2+1 (on pourra utiliser une division euclidienne).

3 En déduire que le noyau de φ est l'idéal de $\mathbf{R}[X]$ engendré par X^2+1.

4 Montrer que φ se factorise en une application $\tilde{\varphi}$: $\mathbf{R}[X]/(X^2+1) \to \mathbf{C}$ et que $\tilde{\varphi}$ est un isomorphisme.

Exercice 19

Soit k un corps et $P, Q \in k[X]$.

1 Rappeler comment on peut utiliser l'algorithme d'Euclide pour déterminer $\Pi = \operatorname{pgcd}(P,Q)$.

2 Soient K un corps avec $k \subset K$. On a donc $k[X] \subset K[X]$. On suppose que Q divise P dans $k[X]$. Montrer que Q divise P dans $K[X]$.

3 Montrer que la réciproque est vraie (on pourra considérer une division euclidienne). Ainsi on pourra simplement dire « Q divise P » sans préciser si on voit P et Q comme des éléments de $k[X]$ ou de $K[X]$.

4 On voit P et Q comme des éléments de $K[X]$. Montrer que leur pgcd est égal à Π. Ainsi on pourra parler du pgcd de P et Q sans préciser si l'on considère P et Q comme des éléments de $k[X]$ ou comme des éléments de $K[X]$.

5 Soit $P \in \mathbf{R}[X]$ tel que $(X-i)$ divise P dans $\mathbf{C}[X]$. En utilisant la conjugaison complexe, montrer que $X+i$ divise aussi P dans $\mathbf{C}[X]$. En déduire que X^2+1 divise P (dans $\mathbf{C}[X]$ ou dans $\mathbf{R}[X]\ldots$).

6 Montrer que si P est irréductible dans $K[X]$, alors P est irréductible dans $k[X]$ (on pourra raisonner par contraposition). Montrer par des exemples que la réciproque est fausse. Ainsi, lorsque l'on parle d'irréductibilité, il est très important de préciser si l'on voit P comme un élément de $k[X]$ ou comme un élément de $K[X]$.

Exercice 20

Soit E un ensemble et $\star$ une loi de composition interne sur E. On suppose qu'on a

$$\forall x \in E, \quad \exists e \in E, \quad x \star e = e \star x = x.$$

$(E, \star)$ admet-t-il nécessairement un élément neutre ?

Exercice 21

Pour tout polynôme $P \in \mathbf{C}[X]$ non nul, on note $N_0(P)$ le nombre de racines de P *comptées sans multiplicité*. Par exemple $N_0(X^3) = 1$, $N_0(X^2(X-1)) = 2$. Le but de cet exercice est de démontrer le théorème suivant.

Théorème 0.1 *Soit A, B, C des éléments de $\mathbf{C}[X]$ vérifiant $A+B=C$. On les suppose en outre premiers entre eux et non constants tous les trois. Alors on a l'inégalité*

$$\mathrm{Max}(\deg(A), \deg(B), \deg(C)) \leqslant N_0(ABC) - 1.$$

Ce théorème a été démontré par Stothers en 1981 et indépendamment par Mason en 1983. Ce résultat a été à l'origine d'une célèbre (et toujours largement ouverte) conjecture d'arithmétique, la « conjecture *abc* ». La conjecture *abc* est un énoncé analogue au théorème de Mason-Stothers où $\mathbf{Z}$ joue le rôle de $\mathbf{C}[X]$. Nous verrons également comment le théorème de Mason-Stothers implique facilement le grand théorème de Fermat pour les polynômes (le grand théorème de Fermat pour les entiers a été démontré par Wiles en 1994, mais la démonstration est infiniment moins élémentaire que dans le cas des polynômes !). La démonstration proposée ici du théorème de Mason-Stothers est dûe à Noah Snyder, qui l'a trouvée à la fin des années 90 alors qu'il était encore au lycée.

1 Montrer qu'on peut supposer qu'on a $\mathrm{Max}(\deg(A), \deg(B), \deg(C)) = \deg(C)$.

2 Vérifier la relation

$$A'B - AB' = AC' - A'C$$

En déduire

$$\mathrm{pgcd}(A, A')\,\mathrm{pgcd}(B, B')\,\mathrm{pgcd}(C, C') | (A'B - AB')$$

puis

$$\deg(\mathrm{pgcd}(A, A')) + \deg(\mathrm{pgcd}(B, B')) + \deg(\mathrm{pgcd}(C, C')) \leqslant \deg(A) + \deg(B) - 1.$$

3 Soit $P \in \mathbf{C}[X]$ non nul. Montrer la relation

$$\deg(\mathrm{pgcd}(P, P')) = \deg(P) - N_0(P)$$

(décomposer P en produit de facteurs irréductibles).

4 Montrer qu'on a $N_0(ABC) = N_0(A) + N_0(B) + N_0(C)$.

5 Déduire de ce qui précède le théorème de Mason-Stothers.

6 Déduire du théorème de Mason-Stothers le grand théorème de Fermat pour les polynômes : soit $n \geqslant 3$ un entier, et A, B, C des polynômes vérifiant $A^n + B^n + C^n = 0$; alors A, B et C sont des constantes (raisonner par l'absurde, et appliquer Mason-Stothers à A^n, B^n et C^n).