UNSA 2004-2005, Algèbre III, L2 maths
Feuille d'exercices n^o 4

1. On considère l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients entiers ainsi que l'anneau $\mathbb{Z}[i]$ des "entiers de Gauss".

1.a. Montrer que $I = \{a(X) \in \mathbb{Z}[X] \,|\, a(0) \text{ pair}\}$ est un idéal de $\mathbb{Z}[X]$.

1.b. Montrer que I est le plus petit idéal de $\mathbb{Z}[X]$ contenant à la fois la constante 2 et le monôme X, donc $I = 2\mathbb{Z}[X] + X\mathbb{Z}[X]$.

1.c. Montrer que l'idéal I n'est pas l'ensemble $a(X)\mathbb{Z}[X]$ des multiples d'un seul polynôme $a(X) \in \mathbb{Z}[X]$, donc l'anneau $\mathbb{Z}[X]$ n'est pas principal.

1.d. Montrer qu'il existe un et un seul morphisme d'anneaux $\phi : \mathbb{Z}[X] \to \mathbb{Z}[i]$ qui applique X sur i. Quel est son noyau ? Montrer que l'image $J = \phi(I)$ est un idéal de $\mathbb{Z}[i]$. Trouver $a + bi \in \mathbb{Z}[i]$ tel que $J = (a + bi)\mathbb{Z}[i]$.

2. Soient A un anneau principal et $a, b \in A$.

2.a. Montrer que $a|b$ dans A si et seulement si $aA \supseteq bA$.

2.b. En déduire que dans un anneau principal $aA + bA = pgcd(a, b)A$.

2.c. De même, montrer que $aA \cap bA = ppcm(a, b)A$.

2.d. Quels sont les anneaux principaux que vous connaissez ?

3. Soit $R_n = \{P(X) \in \mathbb{R}[X] \,|\, deg(P(X)) \leq n\}$.

3.a. Montrer que $P(X) \mapsto P'(X)$ définit une application linéaire $R_n \to R_{n-1}$. Déterminer son image et son noyau, et vérifier la formule du rang.

3.b. Soient $P(X), Q(X) \in \mathbb{R}[X]$ deux polynômes premiers entre eux avec $deg(P(X)) = n$, $deg(Q(X)) = m$. Montrer que l'application

$$\begin{array}{rcl} \phi : R_{m-1} \times R_{n-1} & \to & R_{m+n-1} \\ (A(X), B(X)) & \mapsto & A(X)P(X) + B(X)Q(X) \end{array}$$

est linéaire et injective.

3.c. À l'aide de la formule du rang déduire de 3.b que ϕ est également surjective. Interpréter le résultat comme théorème de Bézout "raffiné".

4.a. Déterminer dans $\mathbb{R}[X]$ la somme $p(X)\mathbb{R}[X] + q(X)\mathbb{R}[X]$ et l'intersection $p(X)\mathbb{R}[X] \cap q(X)\mathbb{R}[X]$ pour $p(X) = X^3 + 2X + 3$, $q(X) = X^2 + X + 1$ et pour $p(X) = X^3 - X^2 - X - 2$, $q(X) = X^4 + X^2 + 1$.

4.b. En remontant l'algorithme d'Euclide trouver des polynômes $u(X), v(X)$ tels que $(X^3 + 2X + 3)u(X) + (X^2 + X + 1)v(X) = 1$.

5.a. Montrer que dans $\mathbb{R}[X]$, $(X - 1)^2$ divise $X^{n+1} - X^n - X + 1$ $(n \geq 2)$.

5.b. Trouver l'ensemble des $(a, b) \in \mathbb{R}^2$ tels que $X^2 + 1$ divise $aX^3 + bX^2 - X + 1$ dans $\mathbb{R}[X]$.

6.a. Décomposer les polynômes $p(X) = X^4 + 1$ et $q(X) = X^4 - X^2 - 2$ en facteurs irréductibles en les considérant successivement comme éléments de $\mathbb{C}[X]$, de $\mathbb{R}[X]$ et de $\mathbb{Q}[X]$.

6.b. Ecrire la fraction rationnelle $\frac{p(X)}{q(X)}$ sous forme $1+\frac{a(X)}{r(X)}+\frac{b(X)}{s(X)}+\frac{c(X)}{t(X)}$, où les $r(X), s(X), t(X)$ sont les facteurs irréductibles de $q(X)$ sur $\mathbb{R}$ et où les degrés des numérateurs sont strictement inférieurs aux degrés des dénominateurs.

6.c. Déduire de 6.b une primitive de la fraction rationnelle $\frac{p(X)}{q(X)}$.

7. On considère les deux polynômes $p(X), q(X) \in \mathbb{Q}[X]$ définis par

$$p(X) = X^4 - 7X^2 + 12$$
$$q(X) = X^4 - 3X^3 + X^2 + 4.$$

7.a. Montrer que $p(X)$ et $q(X)$ ont une racine en commun. On pourra d'abord déterminer les racines de $p(X)$.

7.b. Déterminer les racines doubles de $q(X)$. On pourra utiliser que ce sont les racines simples du $pgcd(q(X), q'(X))$.

7.c. Décomposer $p(X)$ et $q(X)$ en facteurs irréductibles sur $\mathbb{Q}$.

7.d. Écrire $\frac{p(X)}{q(X)}$ sous forme $e(X)+\frac{p_1(X)}{q_1(X)}+\cdots+\frac{p_r(X)}{q_r(X)}$ telle que pour $1 \leq i \leq r$, $q_i(X)$ soit irréductible sur $\mathbb{Q}$ et $deg(p_i(X)) < deg(q_i(X))$.

8. Soit p un nombre premier et notons $\mathbb{F}_p$ le corps fini à p éléments.

8.a. Montrer que dans l'anneau des polynômes $\mathbb{F}_p[X]$, on a la décomposition en facteurs irréductibles $X^{p-1} - [1] = (X - [1])(X - [2]) \cdots (X - [p-1])$.

8.b. En déduire la congruence de Wilson : $(p-1)! \equiv -1 \mod p$. Vérifier pour $p = 2, 3, 5, 7, 11$.

8.c. Les polynômes $X^4 + [1], X^4 + X + [1], X^4 + X^2 + [1], X^4 + X^3 + [1]$ sont-ils irréductibles dans $\mathbb{F}_2[X]$? Même question en les considérant comme éléments de $\mathbb{F}_3[X]$.

Mots-Clés : Anneaux principaux, anneaux de polynômes, fractions rationnelles, racines, irréductibilité sur $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_p$.