TD 2 – Anneaux de fractions et résultant

Exercice 1. Soit A un anneau intègre et S une partie multiplicative de A. Montrer que l'opération $o_+ : (S \times A)^2 \to S \times A$ donnée par

$$o_+((s_1, a_1), (s_2, a_2)) = (s_1\, s_2, s_1\, a_2 + s_2\, a_1),$$

est compatible avec la relation d'équivalence $\sim$ définie sur $S \times A$ par

$$(s_1, a_1) \sim (s_2, a_2) \Leftrightarrow s_2 a_1 = a_2 s_1.$$

Ceci termine la démonstration du Lemme 2 du cours.

Exercice 2. Soit A un anneau commutatif intègre et S une partie multiplicative de A. Montrer que l'ensemble $S^{-1}A$ muni des opérations $+_{S^{-1}A}$ et $\times_{S^{-1}A}$ est un anneau commutatif. Ceci termine la démonstration du Théorème 4 du cours.

Exercice 3. Soit A un anneau factoriel. On note $\mathbb{K}$ le corps de fraction de A. Soient (n, m) un couple d'entiers naturels non nuls et

$$F = \sum_{i=0}^{n} a_i X^i \quad \text{et} \quad G = \sum_{j=0}^{m} b_j X^j,$$

deux polynômes de $A[X]$ vérifiant $a_n \neq 0$ et $a_m \neq 0$. On note $\mathrm{Syl}(F, G)$ la matrice de Sylvester de F et G et $\mathrm{Res}(F, G)$ le résultant de F et G, i.e, $\mathrm{Res}(F, G) = \det(\mathrm{Syl}(F, G))$.

On pose $\mathcal{B} = \big((X^{m-1}, 0), (X^{m-2}, 0), ..., (1, 0), (0, X^{n-1}), ..., (0, 1)\big)$ et $\mathcal{B}' = \big(X^{n+m-1}, ..., X, 1\big)$. On considère enfin l'application

$$\begin{array}{rcl} \varphi : \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] & \to & \mathbb{K}_{n+m-1}[X] \\ (U, V) & \mapsto & FU + GV \end{array}$$

a. Montrer que $\mathcal{B}$ est une base de $K_{n-1}[X] \times \mathbb{K}_{m-1}[X]$.

b. Montrer que φ est une application linéaire.

c. Expliciter la matrice représentative de φ relativement aux bases $\mathcal{B}$ et $\mathcal{B}'$.

d. On suppose que $F \wedge G = 1$.

i. Montrer que φ est injective.

ii. En déduire que $\mathrm{Res}(F, G) \neq 0$.

e. On suppose que $F \wedge G \neq 1$. Montrer que φ n'est pas injective, puis que $\mathrm{Res}(F, G) = 0$.

f. En déduire une démonstration du Théorème 11 du cours.

On suppose maintenant $n \geq 2$. On note F' le polynôme dérivée de F. Le discriminant $\Delta(F)$ est donnée par

$$\Delta(F) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n} \mathrm{Res}(F, F').$$

g. On suppose ici que F est de degré 2 et on pose $F = aX^2 + bX + c$. Calculer $\Delta(F)$.

h. Donner une démonstration du Corollaire 13 du cours.

Exercice 4. Soit A un anneau commutatif unitaire intègre, S une partie multiplicative de A et $i : A \to S^{-1}A$ l'homomorphisme canonique de A dans $S^{-1}A$ (donné par le Théorème 4).

a. Soit I un idéal de A. On note $S^{-1}I$ l'idéal de $S^{-1}A$ engendré par $i(I)$. Démontre que $S^{-1}I$ est l'ensemble des fractions a/s avec $a \in I$ et $s \in S$.

b. Démontrer que $S^{-1}I = S^{-1}A$ si et seulement si $S \cap I \neq \emptyset$.

c. Soit J un idéal de $S^{-1}A$. Posons $I = i^{-1}(J)$. Montrer que l'on a $S^{-1}I = J$.

d. Soit $\mathfrak{p}$ un idéal premier de A tel que $\mathfrak{p} \cap S = \emptyset$. Démontrer que $S^{-1}\mathfrak{p}$ est un idéal premier de $S^{-1}A$.

e. Soit $\mathfrak{q}$ un idéal premier de $S^{-1}A$. Démontrer que $\mathfrak{p} = i^{-1}(\mathfrak{q})$ est l'unique idéal premier de A tel que $S^{-1}\mathfrak{p} = \mathfrak{q}$.

f. On suppose $S = A - \mathfrak{p}$, où $\mathfrak{p}$ est un idéal premier de A. Démontrer que tout idéal propre de $S^{-1}A$ est contenu dans $S^{-1}\mathfrak{p}$. En déduire que $S^{-1}\mathfrak{p}$ est l'unique idéal maximal de $S^{-1}A$.

Exercice 5. Soit le polynôme $X^3 + pX + q \in \mathbb{C}[X]$. Quelle condition doivent vérifier p et q pour qu'il admette une racine double ?

Exercice 6. Soit p un nombre premier et $P = X^{p-1} + X^{p-2} + \cdots + X + 1$.

a. Réécrire P en tenant compte de la somme d'une progression géométrique.

b. Calculer $P(Y + 1)$.

c. En déduire que P est irréductible sur $\mathbb{Q}[X]$.

Exercice 7. Soit p un nombre premier. Pour tout polynôme $F \in \mathbb{Z}[X]$, on note $\overline{F}$ son image dans $\mathbb{F}_p[X]$.

a. Soit $F \in \mathbb{Z}[X]$ unitaire. Montrer que si $\overline{F}$ est irréductible dans $\mathbb{F}_p[X]$ alors F est irréductible dans $\mathbb{Z}[X]$.

b. Posons $F = X^4 + 1$.

i. Montrer que F est irréductible dans $\mathbb{Z}[X]$.

ii. Montrer que F est réductible dans $\mathbb{F}_2[X]$.

On rappel, que pour $p \geq 3$, l'élément a est un carré dans $\mathbb{F}_p^*$ si et seulement si $a^{\frac{p-1}{2}} = 1$. Et que de plus $a^{\frac{p-1}{2}} = \pm 1$ pour tout $a \in \mathbb{F}_p^*$ (voir **2.d** du TD1).

iii. Trouver une factorisation de $X^4 + 1$ dans le cas où -1 est un carré modulo p.

iv. Trouver une factorisation de $X^4 + 1$ dans le cas où 2 est un carré modulo p.

v. Trouver une factorisation de $X^4 + 1$ dans le cas où -2 est un carré modulo p.

vi. Montrer qu'au moins l'un des entiers $-1, 2, -2$ est un carré modulo p.

vii. Conclure.

c. Démontrer que le polynôme $X^4 + X + 1$ est irréductible dans $\mathbb{Q}[X]$.