3 Étude des anneaux quotients $\mathbf{Z}/n\mathbf{Z}$ et $\mathbf{K}[X]/P\mathbf{K}[X]$ (K un corps)

3.1 Étude de $\mathbf{Z}/n\mathbf{Z}$

Soit n un entier positif. On rappelle à toutes fins utiles que le morphisme quotient

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ m & \longmapsto & [m]_n \end{array}$$

est surjectif de noyau $n\mathbf{Z}$ et que l'application

$$\begin{array}{ccc} \{m \in \mathbf{Z}, 0 \leqslant m \leqslant n-1\} & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ m & \longmapsto & [m]_n \end{array}$$

induite par restriction est une bijection.

3.1.1 Éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$

Théorème 1. *Soit n un entier positif et $m \in \mathbf{Z}$. Alors $[m]_n \in (\mathbf{Z}/n\mathbf{Z})^\times$ si et seulement si $\mathrm{pgcd}(m,n) = 1$. En particulier l'application*

$$\begin{array}{ccc} \{m \in \mathbf{Z}, 0 \leqslant m \leqslant n-1, \mathrm{pgcd}(m,n) = 1\} & \longrightarrow & (\mathbf{Z}/n\mathbf{Z})^\times \\ m & \longmapsto & [m]_n \end{array}$$

est une bijection.

.

3.1.2 Endomorphismes de $\mathbf{Z}/n\mathbf{Z}$

L'étude des endomorphisme de $\mathbf{Z}/n\mathbf{Z}$ figure explicitement sur le programme officiel du module. On va faire une étude un peu plus générale à moindres frais.

Théorème 2. *Soit n un entier positif et A un anneau. Alors l'ensemble $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}/n\mathbf{Z}, A)$ est non vide si et seulement si la caractéristique de A divise n, et alors $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}/n\mathbf{Z}, A)$ a un unique élément.*

En particulier $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}) = \mathrm{Id}_{\mathbf{Z}/n\mathbf{Z}}$.

Définition. Soit m, n des entiers positifs tels que m divise n. On note $\pi_{n,m}$ l'unique morphisme d'anneaux de $\mathbf{Z}/n\mathbf{Z}$ vers $\mathbf{Z}/m\mathbf{Z}$.

3.1.3 Les carrés dans $\mathbf{Z}/p\mathbf{Z}$, p premier

Définition 3. Soit A un anneau. On dit qu'un élément a de A est un carré (dans A) si l'équation

$$x^2 = a \quad x \in A$$

possède au moins une solution.

Théorème 4. *Soit p un nombre premier impair.*

1. *L'application*
$$\begin{array}{ccc} (\mathbf{Z}/p\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/p\mathbf{Z})^\times \\ x & \longmapsto & x^2 \end{array}$$
est un morphisme de groupes, de noyau $\{[1]_p, [-1]_p\}$.
2. *Il y a exactement $\frac{p+1}{2}$ éléments de $\mathbf{Z}/p\mathbf{Z}$ qui sont des carrés. En outre, soit $x \in (\mathbf{Z}/p\mathbf{Z})^\times$; alors x est un carré si et seulement si $x^{\frac{p-1}{2}} = [1]_p$.*

C'est en fait un cas particulier du théorème suivant.

Théorème 5. *Soit $\mathbf{K}$ un corps de caractéristique différente de 2.*

1. *On a $1_\mathbf{K} \neq -1_\mathbf{K}$.*
2. *L'application*
$$C_\mathbf{K} : \begin{array}{ccc} \mathbf{K}^\times & \longrightarrow & \mathbf{K}^\times \\ x & \longmapsto & x^2 \end{array}$$
est un morphisme de groupes, de noyau $\{1_\mathbf{K}, -1_\mathbf{K}\}$.
3. *En particulier si $\mathbf{K}$ est un corps fini de cardinal q impair, il y a $\frac{q+1}{2}$ carrés dans $\mathbf{K}$. Par ailleurs $x \in \mathbf{K}^\times$ est un carré si et seulement si $x^{\frac{q-1}{2}} = 1_\mathbf{K}$.*

3.2 Étude de la K-algèbre $\mathbf{K}[X]/P\mathbf{K}[X]$, où K est un corps et $P \in \mathbf{K}[X]$

3.2.1 Structure de K-espace vectoriel sur les quotients de $\mathbf{K}[X]$

Soit $\mathbf{K}$ un corps, et P un élément de $\mathbf{K}[X]$. Le morphisme $\mathbf{K} \to \mathbf{K}[X]$ induit par composition avec le morphisme quotient $\mathbf{K}[X] \to \mathbf{K}[X]/P\mathbf{K}[X]$ une structure de $\mathbf{K}$-algèbre (donc de $\mathbf{K}$-espace vectoriel) sur $\mathbf{K}[X]/P\mathbf{K}[X]$) (*cf.* la section 2.10 du chapitre 2).

Théorème 6. *Soit* $\mathbf{K}$ *un corps, et* P *un élément de* $\mathbf{K}[X]$*. Supposons* P *non constant. Soit* $\pi\colon \mathbf{K}[X] \to \mathbf{K}[X]/P\mathbf{K}[X]$ *le morphisme quotient et* $x := \pi(X)$*. Alors* $\{1, x, \ldots, x^{\deg(P)-1}\}$ *est une base du* $\mathbf{K}$*-espace vectoriel* $\mathbf{K}[X]/P\mathbf{K}[X]$

En particulier l'application

$$\begin{array}{ccc} \{Q \in \mathbf{K}[X], \deg(Q) < \deg(P)\} & \longrightarrow & \mathbf{K}[X]/P\mathbf{K}[X] \\ Q & \longmapsto & \pi(Q) \end{array}$$

est bijective.

3.2.2 Éléments inversibles des quotients de $\mathbf{K}[X]$

Théorème 7. *Soit* $\mathbf{K}$ *un corps, et* P *un élément de* $\mathbf{K}[X]$*. Supposons* P *non constant. Soit* $\pi\colon \mathbf{K}[X] \to \mathbf{K}[X]/P\mathbf{K}[X]$ *le morphisme quotient.*

Soit $Q \in \mathbf{K}[X]$*. Alors* $\pi(Q) \in (\mathbf{K}[X]/P\mathbf{K}[X])^\times$ *si et seulement si* P *et* Q *sont premiers entre eux.*

En particulier l'application

$$\begin{array}{ccc} \{Q \in \mathbf{K}[X], \deg(Q) < \deg(P), \mathrm{pgcd}(P, Q) = 1\} & \longrightarrow & (\mathbf{K}[X]/P\mathbf{K}[X])^\times \\ Q & \longmapsto & \pi(Q) \end{array}$$

induite par restriction de π *est une bijection.*

3.2.3 Endomorphismes des quotients de $\mathbf{K}[X]$

Comme pour les endomorphismes de $\mathbf{Z}/n\mathbf{Z}$, on va faire une étude un peu plus générale (et on va dévier un peu). À toutes fins utiles, on fait le rappel suivant. Soit $\mathbf{K}$ un corps. Soit A une $\mathbf{K}$-algèbre et $a \in A$. Le morphisme d'évaluation $\mathrm{ev}_a\colon \mathbf{K}[X] \to A$ est l'unique morphisme de $\mathbf{K}$-alèbres $\mathbf{K}[X] \to A$ qui envoie X sur a.

Théorème 8. *Soit* $\mathbf{K}$ *un corps. Soit* A *une* $\mathbf{K}$*-algèbre Alors l'application*

$$\begin{array}{ccc} A & \longrightarrow & \mathrm{Hom}_{\mathbf{K}-Alg}(\mathbf{K}[X], A) \\ a & \longmapsto & \mathrm{ev}_a \end{array}$$

est une bijection qui pour tout élément $P \in \mathbf{K}[X]$ induit une bijection de l'ensemble $\{a \in A, \quad \mathrm{ev}_a(P) = 0\}$ (ie l'ensemble des zéros de P dans A) sur l'ensemble $\mathrm{Hom}_{\mathbf{K}-Alg}(\mathbf{K}[X]/\langle P\rangle, A)$.

On en profite pour introduire les quelques définitions et propriétés suivantes. La démonstration des propriétés fait l'objet d'exercices de TD.

Définition 9. Soit $\mathbf{K}$ un corps, A une $\mathbf{K}$-algèbre et $a \in A$. On dit que a est transcendant sur $\mathbf{K}$ si ev_a est injectif. De manière équivalente, a n'est racine d'aucun polynôme non nul à coefficient dans A. Dans le cas contraire, a est dit algébrique sur $\mathbf{K}$, et le générateur unitaire de $\mathrm{Ker}(\mathrm{ev}_a)$ est appelé polynôme minimal de A (sur $\mathbf{K}$).

Proposition 10. *Soit $\mathbf{K}$ un corps et A une $\mathbf{K}$-algèbre qui est un $\mathbf{K}$-espace vectoriel de dimension finie. Alors tout élément de A est algébrique sur $\mathbf{K}$.*

Proposition 11. *Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X] \setminus \{0\}$, $A = \mathbf{K}[X]/P\mathbf{K}[X]$. Alors tout élément de A est algébrique sur $\mathbf{K}$. En outre le polynôme minimal de x est P.*

Proposition 12. *Soit $\mathbf{K}$ un corps, A une $\mathbf{K}$-algèbre* intègre *et $a \in A$ un élément algébrique. Alors le polynôme minimal de a sur $\mathbf{K}$ est irréductible.*

Définition 13. Soit $\mathbf{K}$ un corps. Une $\mathbf{K}$-extension (ou extension de $\mathbf{K}$) est une $\mathbf{K}$-algèbre qui est un corps. En d'autres termes, une $\mathbf{K}$-extension est la donnée d'un corps $\mathbf{L}$ et d'un morphisme d'anneaux $\mathbf{K} \to \mathbf{L}$.

Le degré d'une $\mathbf{K}$-extension $\mathbf{L}$ est la dimension de $\mathbf{L}$ en tant que $\mathbf{K}$-espace vectoriel. Il est noté $[\mathbf{L} : \mathbf{K}]$.