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

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

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

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

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* $\operatorname{pgcd}(m, n) = 1$*. En particulier l'application*

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

est une bijection.

Démonstration. Soit $m \in \mathbf{Z}$. Alors $[m]_n$ est inversible si et seulement s'il existe $x \in \mathbf{Z}/n\mathbf{Z}$ tel que $x[m]_n = [1]_n$ Ceci équivaut à l'existence de $r \in \mathbf{Z}$ tel que $[r]_n[m]_n = [1]_n$. Or, pour $r \in \mathbf{Z}$, on a $[r]_n[m]_n = [rm]_n$ et la condition $[rm]_n = [1]_n$ équivaut au fait que $rm - 1$ est un multiple de n. Ainsi la condition $[m]_n$ est inversible est équivalente à l'existence d'entiers $r, s \in \mathbf{Z}$ tels que $rm - 1 = sn$. D'après le théorème de Bezout, cette dernière condition équivaut au fait que m et n sont premiers entre eux. □

Remarque. Dans la pratique, si m est un entier premier avec n, le calcul de $r \in \mathbf{Z}$ tel que $[r]_n[m]_n = [1]_n$, autrement dit le calcul d'un inverse de m modulo n, se fait en déterminant une relation de Bezout pour m et n ; rappelons qu'on utilise pour cela l'algorithme d'Euclide (éventuellement étendu).

Remarque. Ce théorème décrit ensemblistement $(\mathbf{Z}/n\mathbf{Z})^\times$, mais ne dit rien a priori sur la structure de *groupe* du groupe $((\mathbf{Z}/n\mathbf{Z})^\times, \times)$

.

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

Démonstration. Notons c la caractéristique de A et φ_A l'unique élément de $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}, A)$ (*cf.* le théorème 15 du chapitre 2), qui est donc de noyau $c\mathbf{Z}$ (*cf.* la définition 29 du chapitre 2). D'après la propriété universelle de l'anneau quotient (théorème 47 du chapitre 2) l'ensemble $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}/n\mathbf{Z}, A)$ est en bijection avec $\{\varphi \in \mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}, A), n\mathbf{Z} \subset \mathrm{Ker}(\varphi)\}$. Comme $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}, A)$ possède un unique élément φ_A et que φ_A est de noyau $c\mathbf{Z}$, on en déduit que $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}/n\mathbf{Z}, A)$ est vide si $c\mathbf{Z}$ ne contient pas $n\mathbf{Z}$ et égal à $\{\varphi_A\}$ si $c\mathbf{Z}$ contient $n\mathbf{Z}$. $\square$

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 $\mathbf{Z}/m\mathbf{Z}$.

Remarque. Concrètement $\pi_{n,m}$ se décrit ainsi : soit $x \in \mathbf{Z}/n\mathbf{Z}$ et $y \in \mathbf{Z}$ tel que $x = [y]_n$; alors $\pi_{n,m}(x) = [y]_m$. On peut d'ailleurs vérifier « à la main » que cette application est bien définie et est l'unique morphisme d'anneaux de $\mathbf{Z}/n\mathbf{Z}$ vers $\mathbf{Z}/m\mathbf{Z}$

Plus généralement, si A est un anneau de caractéristique c divisant n, l'unique morphisme $\pi_{n,A} \colon \mathbf{Z}/n\mathbf{Z} \to A$ se décrit ainsi : soit $x \in \mathbf{Z}/n\mathbf{Z}$ et $y \in \mathbf{Z}$ tel que $x = [y]_n$. Alors $\pi_{n,A}(x) = y \cdot 1_A$.

Remarque. Si $n_1, \ldots, n_r$ sont premiers entre eux deux à deux, le morphisme

$$\prod_{i=1}^{r} \pi_{n,n_i} \colon \mathbf{Z}/n\mathbf{Z} \to \prod_{i=1}^{r} \mathbf{Z}/n_i\mathbf{Z}$$

est l'isomorphisme décrit par le théorème chinois (théorème 49 du chapitre 2)

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*
$$C_\mathbf{K} \colon \begin{array}{ccc}\mathbf{K}^\times & \longrightarrow & \mathbf{K}^\times \\ x & \longmapsto & x^2\end{array}$$
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 $x^{\frac{q-1}{2}} = 1_\mathbf{K}$.*

Démonstration. Rappelons qu'un corps n'est pas nul et que donc l'unique morphisme de $\mathbf{Z}$ dans $\mathbf{K}$, à savoir $\varphi_\mathbf{K} \colon n \mapsto n \cdot 1_\mathbf{K}$ n'a pas pour noyau $\mathbf{Z}$. Dire que 2 n'est pas la caractéristique de $\mathbf{K}$ est donc équivalent à dire que $2 \cdot 1_\mathbf{K} = 1_\mathbf{K} + 1_\mathbf{K} \neq 0_\mathbf{K}$.

La démonstration du fait que l'application $C_\mathbf{K}$ est un morphisme de groupes est a priori facile et laissée à titre d'exercice.

Étudions le noyau de $C_\mathbf{K}$. Par définition c'est $\{x \in \mathbf{K}, x^2 = 1_\mathbf{K}\}$ soit encore $\{x \in \mathbf{K}, (x - 1_\mathbf{K})(x + 1_\mathbf{K}) = 0_\mathbf{K}\}$. Comme un corps est anneau intègre, pour tout $x \in \mathbf{K}$, la relation $(x - 1_\mathbf{K})(x + 1_\mathbf{K}) = 0_\mathbf{K}$ équivaut à $x - 1_\mathbf{K} = 0_\mathbf{K}$ ou $x + 1_\mathbf{K} = 0_\mathbf{K}$. Donc $\mathrm{Ker}(C_\mathbf{K}) = \{1_\mathbf{K}, -1_\mathbf{K}\}$.

Supposons à présent que $\mathbf{K}$ est un corps fini de cardinal q impair. Soit $\mathcal{C}_\mathbf{K}^*$ l'ensemble des carrés non nuls de $\mathbf{K}$. Comme $\mathcal{C}_\mathbf{K}^*$ est l'image de $\mathbf{K}^\times$ par le morphisme de groupes $C_\mathbf{K}$ et que $\mathrm{card}(\mathrm{Ker}(C_\mathbf{K})) = 2$, le cardinal de $\mathcal{C}_\mathbf{K}^*$ est $\frac{\mathrm{card}(\mathbf{K}^\times)}{2} = \frac{q-1}{2}$. Comme $0_\mathbf{K} = 0_\mathbf{K}^2$ est également un carré dans $\mathbf{K}$, on en déduit qu'il y a $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ carrés dans $\mathbf{K}$.

Soit x un élément de $\mathcal{C}_\mathbf{K}$ et $y \in \mathbf{K}$ tel que $y^2 = x$. En particulier y est non nul. Comme le groupe $\mathbf{K}^\times = \mathbf{K} \setminus \{0_\mathbf{K}\}$ possède $q - 1$ élément, le théorème de Lagrange (théorème 32 du chapitre 1) montre que $y^{q-1} = 1_{\mathbf{K}}$. Donc $x^{\frac{q-1}{2}} = y^{q-1} = 1_{\mathbf{K}}$. Ainsi $\mathcal{C}_{\mathbf{K}}^*$ est inclus dans l'ensemble $\mathcal{R}_{\mathbf{K}}$ des racines dans $\mathbf{K}$ du polynôme $X^{\frac{q-1}{2}} - 1_{\mathbf{K}}$. Or, d'après le corollaire 43 du chapitre 2, le cardinal de $\mathcal{R}_{\mathbf{K}}$ est majoré par $\frac{q-1}{2}$. Comme $\mathrm{card}(\mathcal{C}_{\mathbf{K}}^*) = \frac{q-1}{2}$ on en déduit que $\mathcal{C}_{\mathbf{K}}^* = \mathcal{R}_{\mathbf{K}}$. □

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

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

est bijective.

Démonstration. Soit$A \in \mathbf{K}[X]$. Soit $Q, R \in \mathbf{K}[X]$, avec $\deg(R) < \deg(P)$, tels que $A = PQ + R$ est la division euclidienne de A par P (P est non constant donc non nul). On voit alors que $\pi(A) = \pi(R)$. Écrivons $R = \sum_{i=0}^{\deg(P)-1} a_i \cdot X^i$ avec $(a_i) \in \mathbf{K}^{\deg(P)}$. Comme π est un morphisme de $\mathbf{K}$-algèbres, on obtient

$$\pi(R) = \sum_{i=0}^{\deg(P)-1} a_i \cdot x^i$$

ce qui montre que la famille $\{1, x, \ldots, x^{\deg(P)-1}\}$ engendre le $\mathbf{K}$-espace vectoriel $\mathbf{K}[X]/P\mathbf{K}[X]$.

Soit à présent $(a_i)_{0 \leqslant i \leqslant \deg(P)-1} \in \mathbf{K}^{\deg(P)}$ tel que

$$\sum_{i=0}^{\deg(P)-1} a_i \cdots x^i = 0$$

Si on note $R := \sum_{i=0}^{\deg(P)-1} a_i \cdots X^i$, on a donc

$$\sum_{i=0}^{\deg(P)-1} a_i \cdots x^i = \pi(R).$$

Ainsi le polynôme R est dans $\mathrm{Ker}(\pi)$, en d'autres termes, P divise R. Pour des raisons de degré, on a donc $R = 0$. Aisni, pour tout $i \in \{0, \dots, \deg(P) - 1\}$,on a $a_i = 0$. Ceci montre que la famille $\{1, x, \dots, x^{\deg(P)-1}\}$ est une famille libre du $\mathbf{K}$-espace vectoriel $\mathbf{K}[X]/P\mathbf{K}[X]$. □

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

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

induite par restriction de π *est une bijection.*

Démonstration. La démonstration est formellement quasi-identique à la démonstration de la propriété analogue pour les quotients de $\mathbf{Z}$. Faites là ! □

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*

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

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* $\mathrm{Hom}_{\mathbf{K}-Alg}(\mathbf{K}[X]/\langle P\rangle, A)$.

Démonstration. (esquisse) Le fait que la première application est une bijection vient de la propriété universelle de la $\mathbf{K}$-algèbre $\mathbf{K}[X]$ (théorème 75 du chapitre 2) compte tenu de la définition 76 du chapitre 2.

Par ailleurs la propriété universelle des algèbres quotients (*cf.* le théorème 77 du chapitre 2 et la remarque qui suit) montre que $\mathrm{Hom}_{\mathbf{K}-\mathrm{Alg}}(\mathbf{K}[X]/\langle P\rangle, A)$ est en bijection avec l'ensemble

$$\{\varphi \in \mathrm{Hom}_{\mathbf{K}-\mathrm{Alg}}(\mathbf{K}[X], A), \quad \langle P\rangle \subset \mathrm{Ker}(\varphi)\}$$

qui n'est autre que l'ensemble

$$\{\varphi \in \mathrm{Hom}_{\mathbf{K}-\mathrm{Alg}}(\mathbf{K}[X], A), \quad \varphi(P) = 0\}$$

□

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 $\mathbf{K}$).

Remarque. La notion de polynôme minimal ne s'étend pas directement au cas d'un élément d'une A-algèbre où A n'est plus un corps. Le problème est qu'il n'est plus vrai que tout idéal de $A[X]$ est engendré par un élément. Considérons par exemple la $\mathbf{Z}$-algèbre $\mathbf{Z}/2\mathbf{Z}$ et le morphisme d'évaluation en $0_{\mathbf{Z}/2\mathbf{Z}}$. Ce morphisme envoie $P \in \mathbf{Z}[X]$ sur $[P(0)]_2$ et on montre que son noyau est $\langle 2, X\rangle$ et que ce noyau n'est pas engendré par un élément. Ainsi « le polynôme minimal de $0_{\mathbf{Z}/2\mathbf{Z}}$ sur $\mathbf{Z}$ » ne fait pas vraiment sens.

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 $[\mathbf{L} : \mathbf{K}]$.

Remarque. Si $\mathbf{L}$ est une extension de $\mathbf{K}$, $\mathbf{K}$ est isomorphe à un sous-corps de $\mathbf{L}$.

Si $P \in \mathbf{K}[X]$ est un polynôme irréductible, le corps $\mathbf{L} = \mathbf{K}[X]/\langle P \rangle$ est une extension de $\mathbf{K}$ de degré $\deg(P)$.

Exemple. Soit $\mathbf{K}$ un corps. Regardons l'exemple de $\mathrm{Hom}_{\mathbf{K}-\mathrm{alg}}(\mathbf{L}, \mathbf{L})$ où $\mathbf{L}$ est la $\mathbf{K}$-algèbre $\mathbf{K}[X]/P\mathbf{K}[X]$, avec $P \in \mathbf{K}[X]$ irréductible (donc $\mathbf{L}$ est un corps). On a donc

$$\mathrm{Hom}_{\mathbf{K}-\mathrm{alg}}(\mathbf{L}, \mathbf{L}) = \{y \in \mathbf{L}, \quad P(y) = 0\}$$

Comme tout élément de $\mathrm{Hom}_{\mathbf{K}-\mathrm{alg}}(\mathbf{L}, \mathbf{L})$ est une application linéaire injective et que $\mathbf{L}$ est un $\mathbf{K}$-espace vectoriel de dimension finie, tout élément de $\mathrm{Hom}_{\mathbf{K}-\mathrm{alg}}(\mathbf{L}, \mathbf{L})$ est en fait un automorphisme de la $\mathbf{K}$-algèbre $\mathbf{L}$. Le groupe d'automorphismes $\mathrm{Hom}_{\mathbf{K}-\mathrm{alg}}(\mathbf{L}, \mathbf{L})$ est appelé le *groupe de Galois* de $\mathbf{L}/\mathbf{K}$. D'après le corollaire 43 du chapitre 2 et l'égalité ci-dessus, son cardinal est majoré par $\deg(P) = [\mathbf{L} : \mathbf{K}]$. L'extension $\mathbf{L}/\mathbf{K}$ est dite *galoisienne* si le cardinal de son groupe de Galois est égal au degré $[\mathbf{L} : \mathbf{K}]$

Prenons par exemple $\mathbf{K} = \mathbf{Q}$. Si $P = X^2 - 2$, on peut montrer que l'extension obtenue est galoisienne, alors que ce n'est pas le cas pour $P = X^3 - 2$.