

Corrigé du contrôle continu n°2

Question de cours

Soit \mathbf{L} un corps, \mathbf{K} un sous-corps fini de \mathbf{L} , q le cardinal de \mathbf{K} . Montrer que $\mathbf{K} = \{x \in \mathbf{L}, x^q = x\}$.

Montrons l'inclusion $\mathbf{K} \subset \{x \in \mathbf{L}, x^q = x\}$. Comme \mathbf{K} est un corps de cardinal q , $\mathbf{K}^\times = \mathbf{K} \setminus \{0\}$ est un groupe de cardinal $q - 1$. Soit $x \in \mathbf{K}$. D'après le théorème de Lagrange, on a $x^{q-1} = 1$, d'où $x^q = x$. Par ailleurs $0^q = 0$. D'où l'inclusion annoncée.

Par ailleurs $A := \{x \in \mathbf{L}, x^q = x\}$ est l'ensemble des racines dans \mathbf{L} du polynôme $P = X^q - X \in \mathbf{L}[X]$. Comme \mathbf{L} est un corps, on a $\text{card}(A) \leq q$. Comme A contient \mathbf{K} qui est de cardinal q , on a nécessairement $A = \mathbf{K}$.

Exercice 1

Convaincre le correcteur en quelques lignes que vous savez décrire explicitement un corps à 9 éléments et (à l'aide de quelques exemples pertinents) y faire des calculs. Aucune justification n'est demandée, mais on introduira soigneusement les notations utilisées, et on ne négligera pas la présentation.

Soit $\mathbf{L} = \mathbf{F}_3[X]/\langle X^2 + [1]_3 \rangle$. Alors \mathbf{L} est un corps à 9 éléments, et, en notant α l'image de $X \in \mathbf{F}_3[X]$ par le morphisme quotient, l'application

$$\begin{aligned} \mathbf{F}_3^2 &\longrightarrow \mathbf{L} \\ (a, b) &\longmapsto a + b\alpha \end{aligned}$$

est une bijection, ce qui donne une représentation explicite des éléments de \mathbf{L} . Cette bijection est même un isomorphisme de groupes (en fait de \mathbf{F}_3 -espaces vectoriels), ce qui permet de calculer explicitement dans le groupe $(\mathbf{L}, +)$. Exemples :

$$([1]_3 + \alpha) + ([2]_3 + \alpha) = 2\alpha, \quad [2]_3 + ([2]_3 + \alpha) = [1]_3 + \alpha$$

La multiplication s'obtient en calculant dans la représentation ci-dessous selon les règles usuelles et en utilisant la relation $\alpha^2 = -[1]_3$ pour toujours se ramener à un élément de la forme $a + b\alpha$ avec $(a, b) \in \mathbf{F}_3$. Exemples :

$$([1]_3 + \alpha) \times ([2]_3 + \alpha) = [2]_3 + [3]_3\alpha + \alpha^2 = [1]_3$$

$$\alpha \times ([1]_3 + [2]_3\alpha) = \alpha + [2]_3\alpha^2 = [1]_3 + \alpha.$$

Exercice 2

Soit \mathbf{K} un corps et A l'anneau quotient $\mathbf{K}[X, Y]/\langle X^2 - Y^3 \rangle$. Soit x (respectivement y) l'image de X (respectivement Y) dans A .

1. Soit $\varphi: \mathbf{K}[X, Y] \rightarrow \mathbf{K}[T]$ l'unique morphisme de \mathbf{K} -algèbres qui envoie X sur T^3 et Y sur T^2 . Montrer que $\text{Ker}(\varphi) = \langle X^2 - Y^3 \rangle$.

On a $\varphi(X^2 - Y^3) = (T^3)^2 - (T^2)^3 = T^6 - T^6 = 0$, donc $X^2 - Y^3 \in \text{Ker}(\varphi)$, et comme $\text{Ker}(\varphi)$ est un idéal, on a l'inclusion $\langle X^2 - Y^3 \rangle \subset \text{Ker}(\varphi)$

Montrons l'inclusion opposée. Soit $P \in \text{Ker}(\varphi)$. En utilisant le résultat rappelé au début de l'énoncé du contrôle et en voyant P comme un polynôme en l'indéterminée X à coefficients dans $\mathbf{K}[X]$, on obtient qu'il existe $Q \in \mathbf{K}[X, Y]$, $R_1 \in \mathbf{K}[Y]$ et $R_0 \in \mathbf{K}[Y]$ tels que

$$P = Q(X^3 - Y^2) + R_1(Y)X + R_2(Y).$$

Or

$$0 = \varphi(P) = \varphi(Q)\varphi(X^3 - Y^2) + \varphi(R_1(Y)X + R_2(Y)) = 0 + R_1(T^2)T^3 + R_0(T^2).$$

On en déduit $\deg_T(R_1(T^2)T^3) = \deg_T(R_0(T^2))$ soit

$$3 + 2 \deg_Y(R_1) = 2 \deg_Y(R_0).$$

Or $\deg_Y(R_1), \deg_Y(R_0) \in \mathbf{N} \cup \{-\infty\}$ et comme 2 ne divise pas 3, l'égalité ci-dessus n'est possible que si $\deg_Y(R_1) = \deg_Y(R_0) = -\infty$, soit $R_0 = R_1 = 0$. Ainsi $P = Q(X^3 - Y^2)$ est bien un élément de $\langle X^3 - Y^2 \rangle$.

2. *En déduire que A est un anneau intègre.*

Par le théorème de factorisation, φ induit un isomorphisme de $\mathbf{K}[X, Y]/\text{Ker}(\varphi) = A$ sur $\text{Im}(\varphi)$ qui est un sous-anneau de $\mathbf{K}[T]$. Or comme \mathbf{K} est un corps, $\mathbf{K}[T]$ est intègre, donc tout sous-anneau de $\mathbf{K}[T]$ est intègre. Donc A est un anneau intègre.

3. *Soit $\pi: \mathbf{K}[X, Y] \rightarrow A$ le morphisme quotient. Justifier que le corps \mathbf{K} est isomorphe à $\pi(\mathbf{K})$.* L'application $\theta: \mathbf{K} \rightarrow \pi(\mathbf{K})$ induite par π est un morphisme d'anneaux surjectif. Comme $\pi(\mathbf{K})$ est un sous-anneau de A , $\pi(\mathbf{K})$ est intègre, en particulier non nul, donc $\text{Ker}(\theta)$ est un idéal propre de \mathbf{K} . Comme \mathbf{K} est un corps, $\text{Ker}(\theta) = \{0\}$, et finalement θ est un isomorphisme.

On identifie désormais \mathbf{K} et $\pi(\mathbf{K})$. Montrer que $A^\times = \mathbf{K}^\times$.

En fait si on identifie A à $\text{Im}(\varphi) = \{P(T^2, T^3)\}_{P \in \mathbf{K}[X, Y]}$, $\pi(\mathbf{K})$ s'identifie à $\mathbf{K} \subset \mathbf{K}[T]$. On sait par ailleurs que A^\times est inclus dans $\mathbf{K}[T]^\times$ (car A est un sous-anneau de $\mathbf{K}[T]$) et que $\mathbf{K}[T]^\times = \mathbf{K}^\times$ (car \mathbf{K} est intègre). Comme \mathbf{K} est un sous-anneau de A , l'inclusion $\mathbf{K}^\times \subset A^\times$ est également vérifiée, et on a bien $\mathbf{K}^\times = A^\times$.

4. *Montrer que x et y sont des éléments irréductibles de A .*

Commençons par la remarque suivante. Soit $P \in \mathbf{K}[X, Y]$. Alors $P(T^3, T^2)$ est une combinaison \mathbf{K} -linéaire de monômes de la forme T^{3i+2j} avec $i, j \in \mathbf{N}$. Pour $i, j \in \mathbf{N}$, $3i + 2j$ est soit nul, soit supérieur à 2, d'où il ressort que $P(T^3, T^2)$ est soit constant, soit de degré supérieur à 2.

Via l'identification de la question précédente, on a $x = T^3$. En particulier x est non nul, et, d'après la question précédente, non inversible. Soit $x_1, x_2 \in A$ tel que $x = x_1 x_2$. Il existe $P_1, P_2 \in \mathbf{K}[X, Y]$ tel que $x_1 = P_1(T^3, T^2)$ et $x_2 = P_2(T^3, T^2)$. On a donc

$$T^3 = P_1(T^3, T^2)P_2(T^3, T^2)$$

$$\text{d'où } 3 = \deg_T(P_1(T^3, T^2)) + \deg_T(P_2(T^3, T^2))$$

ce qui montre que nécessairement on a (quitte à échanger P_1 et P_2) $\deg_T(P_1(T^3, T^2)) \leq 1$ d'où $P_1(T^3, T^2) \in \mathbf{K}$ d'après la remarque ci-dessus. Ainsi $x_1 \in \mathbf{K}^\times = A^\times$, ce qui achève de montrer que x est irréductible.

La démonstration pour y est strictement similaire.

Exercice 3

Soit A un anneau, \mathcal{I} un idéal de A , S une partie multiplicative de A , $\iota: A \rightarrow S^{-1}A$ le morphisme de localisation.

1. Montrer que l'ensemble $\{\frac{a}{s}\}_{a \in \mathcal{I}, s \in S}$ est l'idéal de $S^{-1}A$ engendré par $\iota(\mathcal{I})$; on le note $S^{-1}\mathcal{I}$.

Notons donc $S^{-1}\mathcal{I}$ l'ensemble $\{\frac{a}{s}\}_{a \in \mathcal{I}, s \in S}$. On a $\iota(\mathcal{I}) = \{\frac{a}{1}\}_{a \in \mathcal{I}}$. On sait que l'idéal \mathcal{J} engendré par $\iota(\mathcal{I})$ est exactement l'ensemble des éléments x de $S^{-1}A$ tel qu'il existe un entier positif n , $(b_i) \in (S^{-1}A)^n$ et $(a_i) \in \mathcal{I}^n$ tels que

$$x = \sum_{i=1}^n b_i \frac{a_i}{1}.$$

Le cas $n = 1$, $a_1 = a \in \mathcal{I}$ et $b_1 = \frac{1}{s}$ où $s \in S$ montre que $S^{-1}\mathcal{I}$ est inclus dans \mathcal{J} .

En général, prenant un élément $x \in \mathcal{J}$ qui s'écrit comme ci-dessus et notant $b_i = \frac{c_i}{s_i}$ avec $c_i \in A$ et $s_i \in S$, on obtient

$$x = \frac{\sum_{i=1}^n a_i c_i \prod_{j \neq i} s_j}{\prod_{i=1}^n s_i}.$$

Pour tout $i \in \{1, \dots, n\}$, comme $a_i \in \mathcal{I}$ et \mathcal{I} est un idéal de A , on a $a_i c_i \prod_{j \neq i} s_j \in \mathcal{I}$, d'où on déduit ensuite que le numérateur dans l'expression de x ci-dessus est dans \mathcal{I} . Comme S est une partie multiplicative, le dénominateur est un élément de S , donc $x \in S^{-1}\mathcal{I}$. Ainsi \mathcal{J} est inclus dans $S^{-1}\mathcal{I}$, ce qui conclut.

Autre démonstration possible : montrer que

- (a) $S^{-1}\mathcal{I}$ est un idéal de $S^{-1}A$;
- (b) $S^{-1}\mathcal{I}$ contient $\iota(\mathcal{I})$;
- (c) tout idéal de $S^{-1}A$ qui contient $\iota(\mathcal{I})$ contient $S^{-1}\mathcal{I}$

ce qui permet de conclure par définition d'un idéal engendré.

2. Donner un exemple explicite où \mathcal{I} est strictement inclus dans $\iota^{-1}(S^{-1}\mathcal{I})$.

Prenons par exemple $A = \mathbf{Z}$, $S = \mathbf{Z} \setminus \{0\}$ et $\mathcal{I} = 2\mathbf{Z}$. Alors $S^{-1}A = \mathbf{Q}$ est un corps et l'idéal $S^{-1}\mathcal{I}$, qui n'est pas réduit à 0 car il contient 2, est donc égal à \mathbf{Q} . Donc $\iota^{-1}(S^{-1}\mathcal{I}) = \mathbf{Z}$, et on a bien que \mathcal{I} est strictement inclus dans \mathbf{Z} .

3. Donner un exemple explicite où $\mathcal{I} \cap S = \emptyset$ et \mathcal{I} est strictement inclus dans $\iota^{-1}(S^{-1}\mathcal{I})$.

De manière générale, comme $\iota(\mathcal{I})$ est contenu dans $S^{-1}\mathcal{I}$, \mathcal{I} est toujours inclus dans $\iota^{-1}(S^{-1}\mathcal{I})$.

Prenons par exemple $A = \mathbf{Z}$, $S = \{2^n\}_{n \in \mathbf{N}}$ et $\mathcal{I} = 6\mathbf{Z}$. Alors $3 = \frac{6}{2}$ est un élément de $\iota^{-1}(S^{-1}\mathcal{I})$, mais $3 \notin \mathcal{I}$.