TD - Théorie des corps

23 septembre 2022

Exercice 1

Soit L un corps et soit $\varphi : L \to L$ un morphisme de corps.

1. Soit $K = \{x \in L \mid \varphi(x) = x\}$. Vérifier que K est un sous-corps de L.
2. Soit $P \in K[X]$ non nul.
   a) Démontrer que pour tout $\alpha \in L$ racine de P, $\varphi(\alpha)$ est racine de P.
   b) En déduire que φ induit une permutation de l'ensemble des racines de P dans L.
3. On suppose que L/K est algébrique.
   a) Démontrer que φ est surjectif.
   b) En déduire que l'extension de corps L/L définie par φ est de degré 1.

Correction de l'exercice 1

1. On a bien $0, 1 \in K$. Soient $x, y \in K$, alors $\varphi(x - y) = \varphi(x) - \varphi(y) = x - y$, et $\varphi(xy) = \varphi(x)\varphi(y) = xy$. Ainsi, K est un sous-anneau. Comme $\varphi(1) = 1$, on a de plus, si $x \neq 0$, $\varphi(x^{-1}) = x^{-1}$.
2. a) Soit $\alpha \in L$. Si on écrit $P = \sum_{k=0}^{d} a_k X^k \in K[X]$, alors :

$$\varphi(P(\alpha)) = \sum_{k=0}^{d} a_k \varphi(\alpha)^k = P(\varphi(\alpha)).$$

   En particulier, si α est racine de P, alors $\varphi(\alpha)$ aussi.
   b) Comme $P \neq 0$, l'ensemble Ω des racines de P dans L est fini. D'après la question précédente, $\varphi(\Omega) \subset \Omega$. Comme φ est injectif, sa restriction à Ω l'est, et comme Ω est fini, φ induit une permutation de Ω.
3. a) Soit $x \in L$. Comme L/K est algébrique, on dispose de $P \in K[X]$ tel que $P(x) = 0$. D'après la question précédente, on dispose de $y \in L$ tel que $\varphi(y) = x$. Cela montre la surjectivité de φ.
   b) L'endomorphisme K-linéaire de L φ est bijectif. En particulier, $\{1_L\}$ est une base du L-espace vectoriel L, d'où $\dim_L(L) = 1$.

Exercice 2 Soit K un corps, et soient $P, Q \in K[X]$ premiers entre eux et non constants. On pose $f = P/Q \in K(X)$ et on s'intéresse à l'extension $K(X)/K(f)$.

1. On pose $A = P(T) - fQ(T) \in K[f][T]$

a) Démontrer que X est algébrique sur $K(f)$.
b) En déduire que $K[f]$ est factoriel.

2. On veut montrer que A est irréductible dans $K[f][T]$
   a) On suppose que A s'écrit $A = F(T)G(f,T)$ avec $F(T) \in K[T]$. Démontrer que F est constant.
   b) En déduire que A est primitif dans $K[T][f]$, puis qu'il est irréductible.
3. Démontrer que $[K(X) : K(\alpha)] = \max\{\deg P, \deg Q\}$.

Exercice 3 Le but de cet exercice est de démontrer le théorème de Lüroth :

Théorème (Lüroth).
Soit K un corps, $K \subsetneq F \subset K(X)$ un sous-corps de $K(X)$. Alors il existe $\alpha \in K(X) \setminus K$ tel que $F = K(\alpha)$.

Soit K un corps, $K \subsetneq F \subset K(X)$ un sous-corps de $K(X)$.

1. Démontrer que $K(X)/F$ est algébrique. On note $M(T) \in F[T]$ le polynôme minimal de X sur F.
2. Pour $\alpha \in F \setminus K$, on peut écrire $\alpha = P(X)/Q(X)$ avec P, Q premiers entre eux et non constants, et on définit la *hauteur* de α par : $\mathrm{ht}(\alpha) = \max\{\deg P, \deg Q\}$. Justifier que l'on dispose d'un élément $\alpha \in F \setminus K$ de hauteur minimale.
3. Justifer que M divise N dans $F[T]$ et en déduire qu'il existe $M_0, N_0, R_0 \in K[X][T]$ primitifs en X tels que $N_0 = M_0 R_0$.
4. Démontrer que $\deg_X M_0 \geq \deg_X N_0$ et en déduire que R_0 est constant.
5. Conclure.

Exercice 4

Soit A un anneau factoriel. Soit I un idéal premier de A, $R = A/I$ et $\pi_0 : A \to R$ la projection canonique, que l'on étend naturellement en $\pi : A[X] \to R[X]$.

1. Soit $P = \sum_{k=0}^{d} a_k X^k \in A[X]$ de degré d, tel que $a_d \notin I$. On suppose que $P = P_1 P_2$ avec $P_1, P_2 \in A[X]$ unitaires et que $\pi(P) = \pi(a_d)X^n$.
   a) Démontrer qu'il existe $0 \leq j \leq n$ et $\alpha_1, \alpha_2 \in A/I$ tels que $\pi(P_1) = \alpha_1 X^j$, $\pi(P_2) = \alpha_2 X^{n-j}$.
   b) En déduire que $P(0) \in I^2$.
2. Soit $K = \mathrm{Frac}(A)$. Soit $P \in A[X]$ unitaire, tel que tous les coefficients de P soient dans I et tel que $P(0) \notin I^2$.
   a) Démontrer que P est irréductible dans $A[X]$.
   b) En déduire que P est irréductible dans $K[X]$.
3. Soit $p \in \mathbf{N}$ premier, et soit $P(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.
   a) Démontrer que tous les coefficients (hormis le coefficient dominant) de $P(X+1)$ sont divisibles par p.
   b) Démontrer que P est irréductible dans $\mathbf{Q}[X]$.

Exercice 5

Soit K un corps de caractéristique 0 et soit L une extension finie de K. Le but de l'exercice est de démontrer qu'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

1. On traite d'abord le cas où il existe $x, y \in L$ tels que $L = K(x, y)$. On veut prouver qu'il existe $t \in K$ tel que $L = K(x + ty)$. Soit M/L un corps de décomposition de $P = \pi_x \pi_y$. On note $x = x_1, \ldots, x_n$ (resp. $y = y_1, \ldots, y_m$) les racines de P dans M.
   a) Pour $t \in K$, on note $\alpha = x + ty$ et $P_t(X) = \pi_x(\alpha - tX)$. Justifier que, hormis pour un nombre fini de valeurs de t, y est la seule racine commune de P_t et de π_y dans M.
   b) En déduire qu'il existe $t \in K$ tel que $\mathrm{pgcd}(\pi_y, P_t)$ soit scindé dans $M[X]$ avec pour seule racine y.
   c) Démontrer que pour un tel t, on a $K(x, y) = K(x + ty)$.
2. Traiter le cas général.
3. Soit G le groupe des automorphismes de corps K-linéaires de L. Démontrer que $|G| = [L : K]$.

Exercice 6

Soit $L = \mathbf{F}_p(X, Y)$ le corps des fractions rationnelles à deux indéterminées à coefficients dans $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, et $K = \mathbf{F}_p(X^p, Y^p) \subset L$ le sous-corps engendré par $\mathbf{F}_p, X^p$ et Y^p. On veut montrer qu'il n'existe pas d'élément primitif pour l'extension L/K.

1. Justifier que $[L : K] = p^2$.
2. Soit $a \in L$. Démontrer que $a^p \in K$.
3. En déduire que pour tout $a \in L$, $[K(a) : K] < p^2$ et conclure.

Exercice 7

Soit K un corps et $P \in K[X]$. Soit E une extension de K telle que P soit scindé dans $E[X]$, de racines $\alpha_1, \ldots, \alpha_n$, et telle que $E = K(\alpha_1, \ldots, \alpha_n)$. Soit L une extension de K telle que P soit scindé dans $L[X]$. On veut montrer par récurrence sur $\deg P$ qu'il existe un morphisme K-linéaire $\varphi : E \to L$.

1. Montrer qu'il existe une racine β_1 de P dans L' et un isomorphisme K-linéaire $\varphi_1 : K(\alpha_1) \to K(\beta_1)$ qui envoie α_1 sur β_1.
2. On écrit $P = (X - \alpha_1)Q$ avec $Q \in K(\alpha_1)[X]$. En appliquant l'hypothèse de récurrence à Q, démontrer que L est extension K-linéaire de E.
3. On suppose que pour toute extension L' de K telle que P soit scindé dans $L'[X]$, L' est une extension K-linéaire de L. Démontrer qu'il existe un isomorphisme K-linéaire de E vers L.

Exercice 8

1. Soit K un corps et soit $P \in K[X_1, \ldots, X_n]$. On suppose qu'il existe des parties infinies de $V_1, \ldots, V_n$ de K telles que

$$\forall (x_1, \ldots, x_n) \in V_1 \times \cdots \times V_n,\ P(x_1, \ldots, x_n) = 0.$$

   Démontrer que $P = 0$.
2. Soit K un corps. Soit L/K une extension.
   a) On suppose que K est infini et qu'il existe $(z_1, \ldots, z_n) \in L^n$ tel que $P(x_1, \ldots, x_n) \neq 0$. Montrer qu'il existe $(x_1, \ldots, x_n) \in K^n$ tel que $P(x_1, \ldots, x_n) \neq 0$.

b) Proposer un contre-exemple dans le cas où K est fini.

3. Soit K un corps infini. Démontrer que K^n n'est pas une réunion finie d'hyperplans.

Exercice 9

Soit K un corps et $M, M' \in \mathcal{M}_n(K)$. Soit E un corps de décomposition de $\chi_M \chi_{M'}$. On suppose que M et M' sont semblables dans $\mathcal{M}_n(E)$. On fixe une base $\alpha_1, \ldots, \alpha_d$ de E sur K.

1. Soit $P \in GL_n(E)$ telle que $P^{-1}MP = M'$.
   a) Justifier l'existence de matrices $P_1, \ldots, P_d \in \mathcal{M}_n(K)$ telles que $P = \sum_{1 \leq i \leq d} \alpha_i P_i$.
   b) Démontrer que pour tout $1 \leq i \leq d$, $MP_i = P_i M'$.
2. Démontrer qu'il existe $(x_1, \ldots, x_d) \in K^d$ tel que $\sum_{1 \leq i \leq d} x_i P_i \in GL_n(K)$
3. En déduire que M et M' sont semblables dans $\mathcal{M}_n(K)$.

Exercice 10

Soit K un corps de caractéristique différente de 2.

1. Soit $a \in K$ non carré. Démontrer que $[K(\sqrt{a}) : K] = 2$.
2. Soient $a, b \in K$ avec a non carré. Démontrer que b est un carré dans $K(\sqrt{a})$ si et seulement si b ou ab est un carré dans K.
3. Soient $a_1, \ldots, a_n \in K$. Pour $I \subset \{1, \ldots, n\}$, on note $a_I = \prod_{i \in I} a_i$.
   a) Démontrer que la famille $(\sqrt{a_I})_{I \subset \{1,\ldots,n\}}$ engendre $K(\sqrt{a_1}, \ldots, \sqrt{a_n})$ comme K-espace vectoriel.
   b) En déduire que $[K(\sqrt{a_1}, \ldots, \sqrt{a_n}) : K] \leq 2^n$.
4. On se propose de montrer que le cas d'égalité dans l'inégalité précédente correspond au cas où aucun des a_I n'est un carré dans K.
   a) Supposons que $[K(\sqrt{a_1}, \ldots, \sqrt{a_n}) : K] = 2^n$, montrer qu'aucun des a_I n'est un carré.
   b) Supposons qu'aucun des a_I n'est un carré.