université PARIS DIDEROT PARIS 7

Licence (L3) *Année 2016/2017*

ALGÈBRE

Exercices sur les corps et la théorie de Galois

A. CHAMBERT-LOIR

EXERCICE 1

Soit A un anneau commutatif et soit n un entier $\geqslant 1$.

1 Pour tout $\sigma \in \mathfrak{S}_n$, démontrer qu'il existe un unique automorphisme σ' de la A-algèbre $A[T_1,\dots,T_n]$ tel que $\sigma'(T_i) = T_i$. Vérifier que l'application $\sigma \mapsto \sigma'$ est un homomorphisme de groupes de $\mathfrak{S}_n$ dans $\mathrm{Aut}_A(A[T_1,\dots,T_n])$.

2 On dit qu'un polynôme $P \in A[T_1,\dots,T_n]$ est symétrique si l'on a $\sigma'(P) = P$ pour tout $\sigma \in \mathfrak{S}_n$. Pour tout $p \in \{1,\dots,n\}$, on pose

$$S_p = \sum_{1\leqslant i_1<\dots<i_p\leqslant n} T_{i_1}\dots T_{i_p}.$$

Démontrer que les polynômes $S_1,\dots,S_n$ sont symétriques.

3 Soit $P \in A[T_1,\dots,T_n]$ un polynôme symétrique. Démontrer que le polynôme $P_0 \in A[T_1,\dots,T_{n-1}]$ défini par $P_0 = P(T_1,\dots,T_{n-1},0)$ est symétrique. Que deviennent les polynômes $S_1,\dots,S_n$ lorsqu'on remplace T_n par 0 ?

4 Soit $P \in A[T_1,\dots,T_n]$ un polynôme symétrique. Démontrer qu'il existe un unique polynôme $Q \in A[T_1,\dots,T_n]$ tel que $P = Q(S_1,\dots,S_n)$. (Pour l'existence, raisonner par récurrence sur n, puis sur $\deg(P)$; pour l'unicité, raisonner par récurrence sur n, puis sur $\deg(Q)$.)

EXERCICE 2 (Nullstellensatz combinatoire [?])

Soit K un corps commutatif, soit n un entier $\geqslant 1$, et soit $f \in K[T_1,\dots,T_n]$. Pour $i \in \{1,\dots,n\}$, soit A_i une partie de K et soit $g_i = \prod_{a\in A_i} (T_i - a)$.

1 On suppose que f s'annule en tout point de $A_1\times\cdots\times A_n$. On suppose que $\mathrm{Card}(A_i) > \deg_{T_i}(f)$ pour tout i, alors $f = 0$. (Traiter d'abord le cas $n = 1$ puis raisonner par récurrence sur n.)

2 On suppose encore que f s'annule en tout point de $A_1\times\cdots\times A_n$. Démontrer qu'il existe des polynômes $h_1,\dots,h_n \in K[T_1,\dots,T_n]$ tels que $f = \sum_{i=1}^{n} g_i h_i$ et $\deg(g_i)+\deg(h_i) \leqslant \deg(f)$ pour tout i.

3 Soit $m = (m_1,\dots,m_n) \in \mathbf{N}^n$ tel que le coefficient de T^m dans f soit non nul et tel que $\deg(f) = m_1+\cdots+m_n$. On suppose que $\mathrm{Card}(A_i) > m_i$ pour tout i. Démontrer qu'il existe $a \in A_1\times\cdots\times A_n$ tel que $f(a) \neq 0$.

EXERCICE 3

Soit p un nombre premier.

1 Soit C une partie de $\mathbf{Z}/p\mathbf{Z}$, distincte de $\mathbf{Z}/p\mathbf{Z}$, et soit $f_C \in (\mathbf{Z}/p\mathbf{Z})[X,Y]$ le polynôme $\prod_{c\in C}(X+Y-c)$. Soit $m,n \in \mathbf{N}$ tels que $\mathrm{Card}(C) = m+n$. Démontrer que le coefficient de $X^m Y^n$ dans f n'est pas nul.

2 Soit A,B des sous-ensembles non vides de $\mathbf{Z}/p\mathbf{Z}$; on pose $C = A+B$. On suppose que $\mathrm{Card}(A)+\mathrm{Card}(B) > p$; démontrer que $C = \mathbf{Z}/p\mathbf{Z}$.

3 On suppose que $\mathrm{Card}(A)+\mathrm{Card}(B) \leqslant p$. Observer que $f_C(a,b) = 0$ pour tout $(a,b) \in A\times B$. Utiliser le résultat de l'exercice 2 pour démontrer l'*inégalité de Cauchy–Davenport :*

$$\mathrm{Card}(A+B) \geqslant \mathrm{Card}(A)+\mathrm{Card}(B)-1.$$

EXERCICE 4

Soit E un corps fini, soit p sa caractéristique et soit q son cardinal. Pour tout polynôme $P \in E[T_1,\dots,T_n]$, on pose $s(P) = \sum_{a\in E^n} P(a)$.

1 Calculer $s(T^m)$ pour tout entier m.

2 Soit $P \in E[T_1,\dots,T_n]$ tel que $\deg(P) < n(q-1)$. Démontrer que $s(P) = 0$.

3 Soit $P_1,\dots,P_r$ des polynômes de $E[T_1,\dots,T_n]$. Soit $V = \{a \in E^n ; P_1(a) = \cdots = P_r(a) = 0\}$. On pose $P = \prod_{i=1}^{r}(1-P_i^{q-1})$. Démontrer que $\mathrm{Card}(V)\cdot 1_E = s(P)$. En déduire que $\mathrm{Card}(V)$ est multiple de p si $\sum_{i=1}^{r}\deg(P_i) < n$.

4 Soit d un entier tel que $1 \leqslant d < n$ et soit $P \in E[T_1,\dots,T_n]$ un polynôme homogène de degré d. Démontrer qu'il existe $a \in E^n$ tel que $a \neq 0$ et $P(a) = 0$.

EXERCICE 5

Le but de l'exercice est de démontrer que le corps $\mathbf{C}$ des nombres complexes est algébriquement clos.

Si $P = a_n T^n + \cdots + a_0 \in \mathbf{C}[T]$ est un polynôme à coefficients complexes, on note $\overline{P}$ le polynôme conjugué défini par $\overline{P} = \overline{a_n}T^n + \cdots + \overline{a_0}$.

1 Démontrer que tout nombre complexe a une racine carrée dans $\mathbf{C}$. En déduire que toute équation du second degré à coefficients dans $\mathbf{C}$ a ses racines dans $\mathbf{C}$.

2 Soit $P \in \mathbf{R}[T]$ un polynôme de degré impair. Démontrer qu'il a une racine dans $\mathbf{R}$.

3 Soit P un polynôme irréductible de $\mathbf{R}[T]$. Démontrer qu'il existe une extension finie Ω de $\mathbf{C}$ dans laquelle P est scindé et séparable. On note $d = \deg(P)$ et $a_1,\dots,a_d$ les racines de P dans Ω.

4 Soit $c \in \mathbf{R}$. Démontrer que le polynôme de $\Omega[T]$ donné par

$$P_c = \prod_{1\leqslant j<k\leqslant d}(T-(a_j+a_k+ca_ja_k))$$

appartient à $\mathbf{R}[T]$. (Utiliser le théorème sur les polynômes symétriques élémentaires.)

5 On suppose que tout polynôme Q de $\mathbf{R}[T]$ tel que $v_2(\deg(Q)) < v_2(\deg(P))$ possède une racine dans $\mathbf{C}$. Démmontrer que pour tout $c \in \mathbf{R}$, le polynôme P_c a une racine dans $\mathbf{C}$. En choisissant convenablement plusieurs valeurs de c, montrer qu'il existe deux indices distincts j et k tels que $a_j + a_k$ et $a_j a_k$ appartiennent à $\mathbf{C}$. En déduire que a_j et a_k sont des éléments de $\mathbf{C}$.

6 Démontrer que tout polynôme non constant dans $\mathbf{C}[T]$ a une racine dans $\mathbf{C}$.

EXERCICE 6

Soit E un corps commutatif, soit F une extension finie de E et soit $a \in F$. On suppose que $[E(a) : E]$ est impair. Démontrer que $E(a^2) = E(a)$.

EXERCICE 7

Soit E un corps commutatif, soit p un nombre premier et soit $a \in E$. Soit F une extension de E dans laquelle le polynôme $T^p - a$ est scindé.

1 Quelles sont les racines du polynôme $T^p - a$ dans F ?

2 Soit $P \in E[T]$ un polynôme unitaire qui divise P et soit $n = \deg(P)$. On suppose que $1 \leqslant n < \deg(P)$ et on note b le terme constant de P. Démontrer que $(-1)^{np} b^p = a^n$.

3 En déduire que P est irréductible dans $E[T]$ si et seulement s'il n'a pas de racine dans E.

EXERCICE 8

Soit E un corps commutatif.

1 On suppose que E est de caractéristique 0. Démontrer que tout polynôme irréductible est séparable.

On suppose dans la suite de cet exercice que p est un nombre premier et que E est de caractéristique p.

2 Soit $a \in E$ un élément qui n'est pas la puissance p-ième d'un élément de E ; démontrer que le polynôme $T^p - a$ est irréductible dans $E[T]$ mais n'est pas séparable.

3 Soit $P \in E[T]$ un polynôme irréductible qui n'est pas séparable. Démontrer que $P' = 0$. En déduire qu'il existe un polynôme séparable $Q \in E[T]$ et un entier $n \geqslant 1$ tels que $P = Q(T^{p^n})$.

4 Prouver que tout polynôme irréductible de $E[T]$ est séparable si et seulement si tout élément de E est une puissance p-ième.

EXERCICE 9

1 Soit G un groupe et soit F un corps commutatif. Soit Σ un ensemble d'homomorphismes de groupes de G dans $F^\times$. Démontrer que les éléments de Σ sont linéairement indépendants dans le F-espace vectoriel F^G. (Considérer une relation de dépendance linéaire $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$, où n est minimal.)

2 Soit E et F des corps commutatifs et soit Σ l'ensemble des homomorphismes de corps de E dans F. Démontrer que les éléments de Σ sont linéairement indépendants dans le F-espace vectoriel F^E.

EXERCICE 10

1 Soit E un corps commutatif et soit F une extension de degré 2 de E. Soit $x \in F - E$ tel que $x^2 \in E$. Soit $a \in E$; on suppose que a est un carré dans F. Démontrer que a est un carré dans E, ou ax^2 est un carré dans E.

2 Soit $p_1, \ldots, p_n$ des nombres premiers distincts. On considère les deux propriétés :

a_n Le corps $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ est de degré 2^n sur $\mathbf{Q}$;

b_n Un élément $x \in \mathbf{Q}$ est un carré dans $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ si et seulement s'il existe une partie I de $\{1, \ldots, n\}$ telle que $x \prod_{i \in I}$ soit un carré dans $\mathbf{Q}$.

Démontrer que la conjonction de (a_n) et (b_n) implique (a_{n+1}) et que la conjonction de (a_n) et (b_{n-1}) implique (b_n). En déduire que ces deux propriétés sont vraies pour tout entier n.

3 Démontrer que les racines carrées $\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots$ des nombres premiers sont linéairement indépendantes sur $\mathbf{Q}$.

EXERCICE 11

Soit E un corps commutatif et soit F une extension finie de E. On dit qu'un élément de F est séparable sur E si son polynôme minimal est séparable.

Soit Ω une extension algébriquement close de E.

1 On suppose que F est une extension galoisienne de E. Démontrer que tout élément de F est séparable sur E.

On suppose dans la suite de l'exercice qu'il existe une partie A de F formée d'éléments séparables sur A telle que $F = E(A)$.

2 Démontrer qu'il existe une extension F' de F qui est une extension galoisienne de E.

3 Démontrer que l'ensemble $\mathrm{Hom}_E(F, \Omega)$ est de cardinal $[F : E]$. Inversement, prouver que cette propriété entraîne que tout élément de F est séparable sur E.

4 Démontrer que l'ensemble des sous-corps K tels que $E \subset K \subset F$ est fini.

5 Démontrer qu'il existe un élément $a \in F$ tel que $F = K(a)$.

EXERCICE 12

Soit E le sous-corps de $\mathbf{C}$ engendré par i et $\sqrt{2}$.

1 Démontrer que $[E : \mathbf{Q}] = 4$.

2 Démontrer que E est une extension galoisienne de $\mathbf{Q}$.

3 Soit A l'ensemble $\{\pm i, \pm\sqrt{2}\}$. Démontrer que pour tout $a \in A$ et tout $\sigma \in \mathrm{Gal}(E/\mathbf{Q})$, on a $\sigma(a) \in A$. Démontrer que l'homomorphisme de $\mathrm{Gal}(E/\mathbf{Q})$ dans $\mathfrak{S}_A$ donné par $\sigma \mapsto \sigma|_A$ est injectif.

4 Quelle est l'image de cet homomorphisme ? En déduire que $\mathrm{Gal}(E/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

5 Déterminer un élément $a \in E$ tel que $E = \mathbf{Q}(a)$ et calculer son polynôme minimal.

EXERCICE 13

Soit E un corps commutatif, soit n un entier $\geqslant 1$ et soit $F = E(a)$ une extension de E engendrée par un élément d'ordre n.

1 Démontrer que la caractéristique de E ne divise pas n et que le polynôme $T^n - 1 \in E[T]$ est séparable.

2 Démontrer que F est une extension de décomposition du polynôme $T^n - 1 \in E[T]$.

3 Soit $\sigma \in \mathrm{Gal}(F/E)$. Démontrer qu'il existe un unique entier $d \in \{1, \ldots, n\}$ tel que $\sigma(a) = a^d$.

4 Construire un homomorphisme de groupes injectifs de $\mathrm{Gal}(F/E)$ dans $(\mathbf{Z}/n\mathbf{Z})^\times$. En déduire que $\mathrm{Gal}(F/E)$ est un groupe commutatif.

EXERCICE 14

Soit $E \subset F$ une extension galoisienne et soit G son groupe de Galois. Soit H un sous-groupe de G et soit $K = F^H$. Démontrer qu'il existe une plus petite extension galoisienne L de E telle que $K \subset L \subset F$. Déterminer le sous-groupe de G qui lui est associé par la correspondance de Galois.

EXERCICE 15

Soit K un corps commutatif et soit $F = K(T_1, \ldots, T_n)$ le corps des fractions rationnelles en n indéterminées $T_1, \ldots, T_n$. Soit E le sous-corps de F engendré par les polynômes symétriques $S_1, \ldots, S_n$.

1 Démontrer que l'extension $E \subset F$ est galoisienne et que $\mathrm{Gal}(F/E)$ est isomorphe à $\mathfrak{S}_n$.

2 Soit $a = T_1 + 2T_2 + \cdots + nT_n$. Démontrer que $F = E(a)$.

EXERCICE 16

Soit $E \subset F$ une extension finie galoisienne, soit G son groupe de Galois.

1 Soit $a \in F$ et soit $G_a = \{\sigma \in G ; \sigma(a) = a\}$. Démontrer que l'extension $E(a)$ est associée au sous-groupe G_a de G par la correspondance de Galois.

2 Démontrer que $E(a) = F$ si et seulement si $G_a = \{\mathrm{id}\}$.

3 Soit b un élément de F tel que $G_a \subset G_b$. Démontrer qu'il existe un polynôme $P \in E[T]$ tel que $P(a) = b$.

EXERCICE 17

Soit K un corps commutatif; soit Ω une extension de K et soit E, F deux extensions de K contenues dans Ω. On note EF le sous-corps de Ω engendré par $E \cup F$.

On suppose que l'extension $K \subset E$ est galoisienne.

1 Démontrer que l'extension $F \subset EF$ est galoisienne, de même que l'extension $E \cap F \subset E$.

2 Démontrer que l'on définit un homomorphisme de groupes $\varphi\colon \mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/K)$ en posant $\varphi(\sigma) = \sigma|_E$ pour tout $\sigma \in \mathrm{Gal}(EF/F)$.

3 Démontrer que cet homomorphisme est injectif et que son image est $\mathrm{Gal}(E/E \cap F)$.

4 En déduire que $[EF : F] = [E : E \cap F]$, et que $[EF : K] = [E : K]\,[F : K]$ si et seulement si $K = E \cap F$.

Dans la suite de cet exercice, on suppose aussi que l'extension $K \subset F$ est galoisienne.

5 Démontrer que les extensions $K \subset EF$ et $K \subset E \cap F$ sont galoisiennes.

6 Démontrer que l'on définit un homomorphisme de groupes

$$\varphi\colon \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$$

en posant $\varphi(\sigma) = (\sigma|_E, \sigma|_F)$ pour tout $\sigma \in \mathrm{Gal}(EF/K)$.

7 Prouver que cet homomorphisme est injectif et que son image est le sous groupe de $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ formé des couples (σ, τ) tels que $\sigma|_{E\cap F} = \tau|_{E\cap F}$.

8 Si $K = E \cap F$, en déduire que $\mathrm{Gal}(EF/K)$ est isomorphe à $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$.

EXERCICE 18

Soit K un corps commutatif, soit L une extension finie de K et soit E et F des extensions de K contenues dans L. On suppose que $[E:K]$ et $[F:K]$ sont premiers entre eux. Démontrer que $[EF:K] = [E:K]\,[F:K]$.

EXERCICE 19

Soit E un corps commutatif, soit $P \in E[T]$ un polynôme séparable (unitaire) et soit F une extension de décomposition de P. Soit A l'ensemble des racines de P dans F.

1 Démontrer que A est stable par $\mathrm{Gal}(F/E)$.

2 Démontrer que l'application $\sigma \mapsto \sigma|_A$ définit un homomorphisme injectif du groupe $\mathrm{Gal}(F/E)$ dans le groupe $\mathfrak{S}_A$ des permutations de A.

3 Démontrer que P est irréductible si et seulement si $\mathrm{Gal}(F/E)$ agit transitivement sur A.

4 Plus généralement, construire une bijection entre l'ensemble des facteurs irréductibles (unitaires) de P et l'ensemble des orbites de $\mathrm{Gal}(F/E)$ dans A.

EXERCICE 20

Soit E l'extension de $\mathbf{Q}$ engendrée par $a = \sqrt{2+\sqrt{3}}$.

1 Calculer le polynôme minimal P de a ? Quelles sont ses racines ?

2 En déduire que E est une extension de décomposition du polynôme P.

3 Prouver que $\mathrm{Gal}(E/\mathbf{Q})$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$ et en déterminer un générateur.

EXERCICE 21

Soit $P \in \mathbf{Q}[T]$ un polynôme irréductible dont le degré est un nombre premier p. Soit A l'ensemble des racines de P dans $\mathbf{C}$; on suppose que $\mathrm{Card}(A \cap \mathbf{R}) = p-2$. Soit E le sous-corps de $\mathbf{C}$ engendré par A.

1 Démontrer que l'extension E de $\mathbf{Q}$ est galoisienne.

2 Démontrer que $\mathrm{Gal}(E/\mathbf{Q})$ agit transitivement sur A.

3 Soit G l'image de l'homomorphisme injectif de $\mathrm{Gal}(E/\mathbf{Q})$ dans $\mathfrak{S}_A$ donné par $\sigma \mapsto \sigma|_A$.

4 Démontrer que G contient une transposition.

5 Démontrer que G contient un élément d'ordre p.

6 Démontrer que $G = \mathfrak{S}_A$.

7 Soit $Q_1 = (T^2+1)\prod_{a=1}^{p-2}(T-a)$ et soit $Q_2 \in \mathbf{Z}[T]$ un polynôme unitaire de degré p. On suppose que l'image de Q_2 dans $(\mathbf{Z}/2\mathbf{Z})[T]$ est irréductible. Démontrer que pour tout entier n assez grand, le polynôme $P = Q_2 + 2^n Q_1$ vérifie les conditions de l'exercice.

EXERCICE 22

Soit E le sous-corps de $\mathbf{C}$ engendré par les racines du polynôme $P = T^3 - 2$.

1 Démontrer que P est le polynôme minimal de $\sqrt[3]{2}$.

2 Démontrer que $E \neq \mathbf{Q}(\sqrt[3]{2})$.

3 En déduire que $[E:\mathbf{Q}] = 6$ et que $\mathrm{Gal}(E/\mathbf{Q}) \simeq \mathfrak{S}_3$.

EXERCICE 23

Soit E un corps commutatif et soit F une extension finie de E.

1 On suppose que F est une extension galoisienne de E. Soit $a \in F$. Expliciter à l'aide du groupe $\mathrm{Gal}(F/E)$ le polynôme minimal de a. En déduire qu'il est scindé dans F.

2 On suppose que pour tout $a \in F$, le polynôme minimal de a sur E est séparable et scindé dans F. Démontrer que l'extension F de E est galoisienne.

EXERCICE 24

Soit E un corps commutatif. Soit $P \in E[T]$ un polynôme unitaire, soit $n = \deg(P)$; on note $P = T^n + c_1 T^{n-1} + \cdots + c_n$. Soit A le quotient de l'anneau des polynômes $E[T_1,\ldots,T_n]$ par l'idéal engendré par les polynômes $S_p - (-1)^p c_p$, où $S_1,\ldots,S_n$ sont les polynômes symétriques élémentaires.

1 Soit $a_1,\ldots,a_n$ les images de $T_1,\ldots,T_n$ dans A. Démontrer que l'on a l'égalité $P = \prod_{p=1}^{n}(T-a_p)$ dans $A[T]$.

2 Démontrer que A est un E-espace vectoriel de dimension $n!$.

3 Soit M un idéal maximal de A. Démontrer que A/M est une extension de décomposition de P sur E.

4 Démontrer qu'il existe une action du groupe symétrique $\mathfrak{S}_n$ dans A (par automorphismes de E-algèbres) tel que $\sigma(a_i) = a_{\sigma(i)}$.

5 On suppose que P est séparable. Identifier le groupe de Galois de A/M sur E au stabilisateur de M dans $\mathfrak{S}_n$.

6 On suppose toujours que P est séparable. Démontrer que l'ensemble des idéaux maximaux de A est fini. Si on les note $M_1,\ldots,M_r$, démontrer que A est isomorphe au produit des corps $A/M_1,\ldots,A/M_r$.