Exercices de théorie de Galois

Le niveau des exercices est indiqué comme suit :

- V piste verte : fait manipuler les définitions, présente un fait classique élémentaire
- B piste bleue : mobilise les concepts et résultats du cours pour établir un fait intéressant
- R piste rouge : nécessite un enchaînement d'arguments, un calcul long, une bonne idée
- N piste noire : nécessite les résultats importants du cours et de la créativité !

1 Anneaux et corps

Rappels sur les anneaux et les corps

V **Exercice 1**. (Sous-corps premier)
Montrer qu'il n'existe pas de morphisme entre deux corps de caractéristiques différentes.

V **Exercice 2**. (Sous-corps des puissances p-ièmes)
Soit K un corps de caractéristique $p > 0$. Montrer que $K_0 = \{x^p \in K \,|\, x \in K\}$ est un sous-corps de K.

B **Exercice 3**. (Un idéal premier non maximal)
Soit $\mathbb{Z}[X]$ l'anneau des polynômes à coefficients entiers. Montrer que 2 est premier dans $\mathbb{Z}[X]$. Montrer que l'idéal (2) n'est pas maximal.

B **Exercice 4**. (Points fixes d'un endomorphisme)
Soit A un anneau et $f : A \to A$ un endomorphisme de A.

1. Montrer que l'ensemble $A^f = \{x \in A \,|\, f(x) = x\}$ des points fixes de f est un sous-anneau de A. Si A est un corps, montrer que A^f est un corps.
2. On pose $A := \{a + b\sqrt{2} \in \mathbb{R} \,|\, a, b \in \mathbb{Z}\}$. Montrez que A est un sous-anneau de $\mathbb{R}$. Montrez que $f : A \to A$ défini par $f(a + b\sqrt{2}) = a - b\sqrt{2}$ est un automorphisme de A et calculez A^f.

R **Exercice 5**. (Groupe additif vs groupe multiplicatif d'un corps)
Soit K un corps. Montrer que $(K, +)$ et $(K^\times, \times)$ ne sont pas isomorphes. Montrer qu'en revanche, il peut arriver que $(K, +)$ soit isomorphe à un sous-groupe de $(K^\times, \times)$.

R **Exercice 6**. (Entiers quadratiques)
Posons $A := \{a + b\sqrt{2} \in \mathbb{R} \,|\, a, b \in \mathbb{Z}\}$.

1. Montrez que A est un sous-anneau de $\mathbb{R}$.
2. Montrez que A n'est pas isomorphe à $\mathbb{Z} \times \mathbb{Z}$
3. Montrez que l'idéal I de A engendré par $\sqrt{2}$ est maximal. Montrez que A/I est isomorphe à $\mathbb{F}_2$.
4. Montrez que, si $a, b \in \mathbb{Z}$ sont tels que $3|a^2 - 2b^2$, alors $3|a$ et $3|b$. En déduire que l'idéal J engendré par 3 est premier puis que le quotient A/J est un corps. Quelle est sa caractéristique ? Quel est son cardinal ?

R **Exercice 7**. (Entiers de Gauss)
Dans l'anneau $\mathbb{Z}[i]$, est-ce que i est un élément premier ? Et 2 ? Et 3 ?

Rappels sur l'algèbre des polynômes

B **Exercice 8**. (Idéaux maximaux de $K[X]$)
Soient K un corps et $P \in K[X]$ un polynôme irréductible. On souhaite montrer, par deux démonstrations différents, que l'idéal (P) est maximal.

1. Démontrez directement que si I est un idéal qui contient strictement (P), alors $I = K[X]$.
   (Indication : par exemple, pensez au théorème de Bézout.)
2. Démontrez que l'algèbre $K[X]/(P)$ est un corps.
   (Indication : montrez qu'une K-algèbre intègre de dimension finie est un corps.)

R **Exercice 9**. (Groupe multiplicatif d'un corps)

1. Soit $A = \mathbb{Z}$ et $K = \mathbb{Q}$ son corps de fractions. Démontrez les assertions suivantes :
   (a) on a un isomorphisme de groupes $A^\times \simeq \mathbb{Z}/2\mathbb{Z}$.
   (b) l'anneau A possède un ensemble $\mathcal{P}$ de représentants des éléments irréductibles à association près qui est dénombrable.
   (c) tout élément $x \in K^\times$ possède une écriture $x = up_1^{a_1} \cdots p_n^{a_n}$ avec $u \in A^\times$, $n \geqslant 0$, $p_i \in \mathcal{P}$ et $\alpha_i \in \mathbb{Z} \setminus \{0\}$, unique à l'ordre près des facteurs.
   (d) on a un isomorphisme de groupes $K^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^{(\mathbb{N})}$.
2. Montrez que pour $A = \mathbb{F}_3[X]$ et $K = \mathbb{F}_3(X)$, les quatre assertions de la question précédente sont encore vraies. Donnez deux corps non isomorphes K_1 et K_2 tels que $K_1^\times \simeq K_2^\times$.

B **Exercice 10**. (Une divisibilité et une application)
Soient K un corps, A une K-algèbre et $a, b \in A$.

1. Démontrez que pour tout polynôme $P \in K[X]$ il existe $Q \in K[X, Y]$ tel que
$$P(a) - P(b) = (a - b)\, Q(a, b).$$
   (Indication : commencez par le cas $P = X^n$.)
2. Application : soit E un K-espace vectoriel et $f : E \to E$ un endomorphisme linéaire. On note $\chi \in K[X]$ le polynôme caractéristique de f et $\mu \in K[X]$ son polynôme minimal.
   (a) Rappelez la définition de μ.
   (b) Démontrez qu'il existe $Q \in K[X, Y]$ tel que $\mu(X) \cdot \mathrm{id}_E = (X\mathrm{id}_E - f)\, Q(X\mathrm{id}_E, f)$.
   (Indication : notez que $\mu(X) \cdot \mathrm{id}_E = \mu(X\mathrm{id}_E)$ et appliquez la question 1.)
   (c) Démontrez les divisibilités $\mu \mid \chi \mid \mu^n$.
   (Indication : prenez le déterminant.)
   (d) Déduisez-en que μ et χ ont les mêmes facteurs irréductibles.

Irréductiblité

Ⓑ **Exercice 11**. (Irréductibilité de $P \circ Q$)
Soient K un corps et $P \in K[X]$ un polynôme. Soient $a, b \in K$, $a \neq 0$.

1. Montrer que $Q = P(aX + b)$ est irréductible si et seulement si P est irréductible.
2. Donnez un exemple avec P irréductible mais $P(X^2)$ réductible.
3. Montrer que si $P(X^2)$ est irréductible alors P est irréductible.

Pour l'exercice suivant, on rappelle quelques notions sur les anneaux factoriels. Soit A un anneau factoriel de corps de fractions K.

- Deux éléments $x, y \in K$ sont *associés* s'il existe $u \in A^\times$ tel que $x = uy$.
- Pour $P \in A[X] \setminus \{0\}$, le *contenu* $\mathrm{c}(P)$ est le pgcd des coefficients, bien défini à association près.
- Le contenu est multiplicatif : $\mathrm{c}(P_1 P_2) = \mathrm{c}(P_1)\,\mathrm{c}(P_2)$.
- Le contenu s'étend au corps de fractions $\mathrm{Frac}(A[X]) \setminus \{0\}$ par $\mathrm{c}(P/Q) := \mathrm{c}(P)/\mathrm{c}(Q)$.
- On dit que P est *primitif* si $\mathrm{c}(P) = 1$.

Ⓡ **Exercice 12**. (Critère d'Eisenstein)
Soit A un anneau factoriel de corps de fractions K.

1. Soit $P \in K[X]$ non nul. Montrez qu'il existe une écriture $P = aP'$ avec $a \in K \setminus \{0\}$ et $P' \in A[X]$ primitif, et que cette écriture est unique à association près.
2. Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire de degré $n \geqslant 1$ avec $a_i \in A$. On suppose qu'il existe un élément premier $p \in A$ tel que $p \mid a_i$ pour $i = 0, \ldots, n-1$ et $p^2 \nmid a_0$. Montrez qu'alors P est irréductible dans $K[X]$.

Ⓑ **Exercice 13**. (Polynôme cyclotomique Φ_p)
Soit p un nombre premier. Démontrez que le polynôme $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ est irréductible dans $\mathbb{Q}[X]$. (Indication : on pourra s'intéresser à $\Phi_p(X+1)$.)

2 Extensions de corps

Éléments algébriques, extensions algébriques

Ⓥ **Exercice 14**. (Un classique)
Montrez que $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}] = 6$, avec $j := e^{2i\pi/3}$.

Ⓑ **Exercice 15**. (Degrés premiers entre eux)
Soit E/K une extension de corps. Soient $\alpha, \beta \in E$ des éléments algébriques sur K, de degrés m et n.

1. On suppose m et n premiers entre eux. Montrez que $[K(\alpha, \beta) : K] = mn$.
2. Le résultat subsiste-t-il sans l'hypothèse de primalité ?

Ⓑ **Exercice 16**. (Extensions quadratiques de $\mathbb{Q}$)
Soit $K/\mathbb{Q}$ une extension de degré 2, avec $K \subset \mathbb{C}$. Montrez qu'il existe $n \in \mathbb{N}^*$ tel que $K = \mathbb{Q}(\sqrt{n})$ ou $K = \mathbb{Q}(i\sqrt{n})$. (Indication : commencer par fixer un $x \in K \setminus \mathbb{Q}$. Montrer que son polynôme minimal est de degré 2 puis que la racine carrée de son discriminant se trouve dans $K \setminus \mathbb{Q}$, et conclure.)

Ⓑ **Exercice 17**. (Extension biquadratique)
Montrez que $\mathbb{Q}(\sqrt{5},\sqrt{7})$ est une extension monogène de $\mathbb{Q}$, c'est-à-dire de la forme $\mathbb{Q}(x)$.

Ⓑ **Exercice 18**. (Degré de sommes de nombres algébriques)
Dans chaque cas, trouver le degré sur $\mathbb{Q}$ de α, de β et de $\alpha+\beta$.

1. $\alpha=\sqrt{2}$ et $\beta=\sqrt[3]{5}$.
2. $\alpha=\sqrt[3]{2+\sqrt{3}}$ et $\beta=\sqrt[3]{2-\sqrt{3}}$. (Indication : on pourra calculer $(\alpha+\beta)^3$.)

Clôture algébrique

Ⓥ **Exercice 19**. (Algébriquement clos implique infini)
Montrer qu'un corps algébriquement clos n'est jamais fini.

Ⓥ **Exercice 20**. (Extension contenant une clôture algébrique)
Soit E/K une extension telle que E contient une clôture algébrique $\bar{K}$ de K. Monter que, si H est une extension algébrique de K dans E, alors $H\subset\bar{K}$.

Ⓑ **Exercice 21**. (Racines n-ièmes de l'unité dans $\bar{K}$)
Soit K un corps de caractéristique $p\geqslant 0$ et $\bar{K}$ une clôture algébrique. Pour tout entier $n\geqslant 1$ on note $\mu_n(\bar{K})$ l'ensemble des racines n-ièmes de l'unité dans $\bar{K}$.

1. On suppose que $p=0$ ou $p>0$, $p\nmid n$. Montrez que $\operatorname{card}\mu_n(\bar{K})=n$.
2. On suppose que $p>0$ et on note $n=p^s m$ avec $s\geqslant 0$ et $p\nmid m$. Montrez que $\operatorname{card}\mu_n(\bar{K})=m$.

Corps de rupture, corps de décomposition

Ⓑ **Exercice 22**. (Un cas de permanence d'irréductibilité)
Soit E/K une extension finie de degré m et $P\in K[X]$ un polynôme de degré n irréductible sur K.

1. On suppose m et n premiers entre eux. Montrez que P reste irréductible sur E. (Indication : considérez un facteur irréductible Q de P, et son corps de rupture E'.)
2. Le résultat subsiste-t-il sans l'hypothèse de primalité ?

Ⓡ **Exercice 23**. (Extensions finies de $\mathbb{R}$)
Montrer qu'il n'existe pas d'extension de $\mathbb{R}$ de degré 4.

Ⓝ **Exercice 24**. (Irréductibilité de X^p-t)
Soit K un corps. On considère le polynôme $P=X^p-t$ où p est un nombre premier et $t\in K$ n'est pas une puissance p-ième dans K. On souhaite montrer que le polynôme $P=X^p-t$ est irréductible.

1. Montrez qu'un corps de décomposition de P est de la forme $K'=K(\zeta,a)$ où $a^p=t$ et $\zeta^p=1$. Précisez le degré $[K':K]$ (on distinguera selon la caractéristique de K).

Supposons que $P=QR$ avec $Q,R\in K[X]$ unitaires de degrés $i,j\in\{1,\dots,p-1\}$.

2. Montrez que i et j sont premiers entre eux.
3. On suppose que la caractéristique de K est différente de p. Écrivez la factorisation de P dans K' et déduisez-en la forme des coefficients constants $q=Q(0)$ et $r=R(0)$. En utilisant une relation de Bézout $ui+vj=1$, montrez que $q^u r^v$ est une racine de P dans K. Concluez.
4. On suppose que la caractéristique de K est p. En regardant le coefficient de X^{i-1} dans Q, montrez que $a\in K$. Concluez.