CONTRÔLE DES CONNAISSANCES DU COURS: *UN PEU DE CORPS*

CHRISTOPHE M. MARGERIN

Chaque exercice est indépendant, mais pas les questions au sein d'un même exercice. Les questions sont de difficultés très variables : certaines sont banales, beaucoup des applications directes du cours, d'autres encore réclament un peu de réflexion.

On pourra utiliser librement les résultats établis dans le cours : il suffira de *d'énoncer précisément* le résultat que vous voulez utiliser lors de sa première citation dans votre copie, et d'y renvoyer si besoin en lui attribuant une référence ; il est *inutile de les redémontrer.*

Il sera tenu grand compte de la *clarté* des arguments proposés et de la *qualité de rédaction* : Ne vous croyez pas obligé de traiter tous les exercices !

1. — Démontrez que tout corps dont le groupe des unités est cyclique est fini.

Que pensez-vous de la réciproque ?

2. — Soit K un corps *fini* : quelles valeurs peut prendre le produit $\prod_{k\in K^*} k$? (Justifiez votre réponse.)

3. — L'angle $\frac{1}{12}\pi$ est-il constructible *à la règle et au compas* ? (Justifiez votre réponse.)

4. — Donnez la liste des corps finis algébriquement clos. (Justifiez votre réponse.)

5. — Quel est le groupe de Galois de l'extension : $\mathbb{Q} \hookrightarrow \mathbb{R}$? (Justifiez votre réponse.)

6. — Soient L un corps, L_1 et L_2 deux sous-corps de L et K un sous-corps de L_1 et de L_2 ; on supposera que les extensions $L_1 \hookrightarrow L$ et $L_2 \hookrightarrow L$ sont algébriques.

6.1. Démontrez que l'extension $L_1 \cap L_2 \hookrightarrow L$ est algébrique dès que l'une des deux extensions $K \hookrightarrow L_i$, $i \in \{1, 2\}$, l'est.

6.2. L'hypothèse « il existe $i, i \in \{1, 2\}$, tel que l'extension : $K \hookrightarrow L_i$ est algébrique» est-elle nécessaire ?

6.3. On suppose désormais que l'extension $L_1 \cap L_2 \hookrightarrow L$ est algébrique (cf. les deux questions précédentes) ; démontrez que cette extension $L_1 \cap L_2 \hookrightarrow L$ est alors normale dès que les deux extensions $L_1 \hookrightarrow L$ et $L_2 \hookrightarrow L$ le sont.

7. — On dénote par x_1 et x_2 les deux racines réelles du polynôme $X^4 - X - 1$ de $\mathbb{Q}[X]$.

7.1. Démontrez que le nombre réel $(x_1 + x_2)^2$ est racine d'un polynôme cubique à coefficients rationnels, $P(X)$, $P(X) \in \mathbb{Q}_3[X]$.

7.2. Démontrez que ce polynôme $P(X)$ est irréductible dans $\mathbb{Q}[X]$.

7.3. En déduire qu'il existe de nombres réels algébriques de degré une puissance de 2 qui ne sont pas constructibles *à la règle et au compas.*

Date: 2021-07-15.

7.4. Ce résultat était-il prévisible ?

8. — Soit p un nombre premier, L le corps $\mathbb{F}_p(T)$, K le corps L^p, image de L par l'endomorphisme de Frobenius.

8.1. Evaluer le degré séparable de l'extension $K \hookrightarrow L$, $[L:K]_s$.

8.2. Caractériser les éléments de L qui sont séparables sur K.

9. — Soit n un entier naturel positif : $n \in \mathbb{N}^*$.

9.1. Donner un sous-corps de $\mathbb{C}$ isomorphe au corps de rupture du polynôme $X^n - 7$ de $\mathbb{Q}$.(Justifiez votre réponse.)

9.2. Donner un corps de décomposition de ce polynôme. (Justifiez votre réponse.)

9.3. Quel est le nombre minimal de générateurs de ce corps sur $\mathbb{Q}$ (comme corps). (Justifiez votre réponse.)

10. — Soient K un corps et G un sous-groupe infini du groupe des automorphismes du corps K, que nous noterons $\mathrm{Aut}(K)$. On rappelle que par K^G on représente les points fixes de K sous l'action de G.

10.1. Démontrer que le degré de l'extension $K^G \subseteq K$ est alors infini.

10.2. Démontrer par un exemple que l'extension $K^G \hookrightarrow K$ n'est pas nécessairement algébrique.

10.3. Démontrer que l'extension $K^G \hookrightarrow K$ est galoisienne dès qu'elle est algébrique.

11. — On représente par K l'extension de décomposition du polynôme de $\mathbb{Q}[X]$: $X^5 - 6X + 3$ incluse dans $\mathbb{C}$.

11.1. Démontrez que le groupe de Galois de cette extension, $\mathrm{Gal}(K/\mathbb{Q})$, est un sous-groupe de $\mathfrak{S}_5$ qui contient (au moins) une transposition.

11.2. Démontrez que le cardinal de ce groupe de Galois, $\mathrm{Card}(\mathrm{Gal}(K/\mathbb{Q}))$, est un multiple de 5 ; en déduire l'existence d'un cycle de longueur 5 dans ce groupe.

11.3. Déduire des résultats précédents le groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$.

11.4. Soit L un corps ; on supposera la caractéristique de L différente de 2. Démontrez que le groupe de Galois (d'une extension de décomposition) d'un polynôme unitaire séparable de degré n de $L[X]$, $P(X)$, est un sous-groupe du groupe alterné $\mathfrak{A}_n$ si et seulement si le discriminant du polynôme $P(X)$ est un carré dans L.

11.5. Quelles sont les sous-extensions galoisiennes de l'extension $\mathbb{Q} \hookrightarrow K$? Que vient faire l'entier 21451 dans cette discussion ?

12. — Dans ce problème, K, L et M représentent des corps ; on dira qu'un corps K a la propriété $\mathcal{P}$ si tout polynôme irréductible de $K[X]$ est séparable.

12.1. Soit F un corps de caractéristique positive, $p > 0$ et f un élément de $F \setminus F^p$, où F^p représente l'image du corps F par le morphisme de Frobenius. Démontrer que le polynôme $X^p - f$ est inséparable et qu'il est irréductible dans $F[X]$.

12.2. Démontrer que, pour un corps K, la propriété $\mathcal{P}$ est équivalente à la proposition suivante : si la caractéristique de K est positive et égale à p, alors $K = K^p$, où K^p représente l'image de K par l' endomorphisme de Frobenius.

12.3. Démontrer que tout corps fini a la propriété $\mathcal{P}$.

12.4. Démontrer qu'un corps K a la propriété $\mathcal{P}$ si et seulement si toute extension algébrique de K est séparable.

12.5. Considérons la double extension $K \hookrightarrow L \hookrightarrow M$ du corps K ; démontrez que l'extension $K \hookrightarrow M$ est séparable si et seulement si les deux extensions qui la composent, $K \hookrightarrow L$ et $L \hookrightarrow M$, sont elles-mêmes séparables.

12.6. Démontrez que pour toute extension finie de corps $K \hookrightarrow L$, les propositions «K a la propriété $\mathcal{P}$» et «L a la propriété $\mathcal{P}$» sont équivalentes.

12.7. Soit l'extension de corps $K \hookrightarrow L$; démontrez que le sous-ensemble des éléments de L qui sont séparables sur K forment un sous-corps de L ; on le notera $L^{s;K}$.

12.8. Démontrez qu'un corps K a la propriété $\mathcal{P}$ si et seulement si tous les éléments de sa clôture algébrique $\bar{K}$ sont séparables sur K, c'est à dire si et seulement si $\bar{K}^{s;K} = \bar{K}$.

12.9. Quels sont les éléments séparables de l'extension $\bar{K}^{s;K} \hookrightarrow \bar{K}$?