Examen Théorie de Galois 2022

Toutes les réponses aux questions posées doivent être justifiées par des démonstrations.

(1) Soit K un corps qu'on suppose infini pour que l'exercice ne soit pas trivial. Montrer que les groupes $(K,+)$ et $(K^\times,\times)$ ne sont pas isomorphes.

(2) Soit E un sous-corps de $\mathbb{C}$ tel que $E/\mathbb{Q}$ est une extension de degré 2. Montrer qu'il existe $n\in\mathbb{Q}$ tel que $E=\mathbb{Q}(\sqrt{n})$ ($\sqrt{n}$ désigne une racine carrée de n dans $\mathbb{C}$).

(3) (a) Montrer que $\mathbb{Q}(\sqrt{1+\sqrt{3}})/\mathbb{Q}$ est de degré 4.

(b) Donner un exemple d'un nombre rationnel r tel que $\mathbb{Q}(\sqrt{r+\sqrt{3}})/\mathbb{Q}$ est de degré 2 (et vérifier qu'il marche).

(4) Soit E/K une extension algébrique. Soit A un sous-anneau de E qui contient K. Montrer que A est un corps.

(5) Donner un exemple d'extension <u>normale</u> $E/\mathbb{Q}$ de degré 36.

(6) Soit K un corps algébriquement clos. Soit n le nombre de racines 12-èmes de l'unité dans K. Donner n, en séparant selon la caractéristique de K (démontrer).

(7) Soient K un corps fini et E/K une extension de degré 3. Donner une condition nécessaire et suffisante sur le cardinal de K modulo 3 pour que E s'écrive sous la forme $K(\sqrt[3]{x})$ avec $x\in K$ (entendu que $\sqrt[3]{x}$ désigne un élément a de E tel que $a^3=x$).

(8) Rappelons que le groupe de Galois $Gal(E/K)$ est défini pour toute extension E/K, galoisienne ou pas, et désigne le groupe des K-automorphismes de corps de E.

Soit E/K une extension finie. Soient U/K et V/K des extensions de K dans E (c'est-à-dire des sous-corps de E qui contiennent K), qu'on suppose normales. On note UV le sous-corps de E engendré par U et V.

(a) Si B est une base de U en tant que K-espace vectoriel, montrer que B est une famille génératrice de UV en tant que V-espace vectoriel.

(b) Montrer que $Gal(UV/K)$ est isomorphe à un sous-groupe de $Gal(U/K)\times Gal(V/K)$.

Corrigé

(1) L'idée est de chercher les éléments d'ordre 2. Les équivalences suivantes sont évidentes :
- $(K,+)$ contient un élément d'ordre 2
- il existe $x \in K^*$ tel que $2x = 0$
- la caractéristique de K est 2 (en simplifiant avec x)
- $X^2 - 1 = (X-1)(X+1)$ a une seule racine et c'est 1
- $(K,\times)$ ne contient aucun élément d'ordre 2.

Donc K contient un élément d'ordre 2 si et seulement si $K^\times$ n'en contient pas. Ainsi, les groupes ne sont jamais isomorphes.

(2) Soit $x \in E\backslash\mathbb{Q}$. Alors le polynôme minimal P de x est de degré 2. Si $P(X) = X^2 + aX + b$ (avec $a, b \in \mathbb{Q}$), alors dans $\mathbb{C}$ on a $x = \frac{-a\pm\sqrt{\Delta}}{2}$, où $\Delta = a^2 - 4b$ et $\sqrt{\Delta}$ est une racine carrée de Δ dans $\mathbb{C}$. Notez que $\Delta = a^2 - 4b$ est un rationnel. On a $x = \frac{-a\pm\sqrt{\Delta}}{2}$, donc $x \in \mathbb{Q}(\sqrt{\Delta})$ et donc $\mathbb{Q}(x) \subset \mathbb{Q}(\sqrt{\Delta})$. On a $\sqrt{\Delta} = \pm(2x + a)$ et donc et $\sqrt{\Delta} \in \mathbb{Q}(x)$, d'où $\mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(x)$. Enfin, $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{\Delta})$ par double inclusion.

(3) Déjà vu : on pose $x = \sqrt{1+\sqrt{3}}$; alors $x^2-1 = \sqrt{3}$, donc $(x^2-1)^2 = 3$; alors x est racine du polynôme unitaire $P(X) = X^4 - 2X^2 - 2$, qui se trouve être irréductible par le critère d'Eisenstein appliqué au nombre premier 2. Donc P est le polynôme minimal de x et comme $\mathbb{Q}(x)/\mathbb{Q}$ est de degré $\deg(P)$ par des résultats de cours concernant les extensions monogènes, on a $[\mathbb{Q}(x) : \mathbb{Q}] = 4$.

(Vu que $\sqrt{3} \in \mathbb{Q}(\sqrt{r+\sqrt{3}})$,) on cherche r tel que $\mathbb{Q}(\sqrt{r+\sqrt{3}}) = \mathbb{Q}(\sqrt{3})$. On cherche r tel qu'il existe $a, b \in \mathbb{Q}$ tels que $r+\sqrt{3} = (a+b\sqrt{3})^2$. (À partir des égalités $a^2+3b^2 = r$ et $2ab = 1$,) on balance $a = 1$ et $b = 1/2$, ce qui donne $r = \frac{7}{4}$. Ensuite on explique pourquoi $\mathbb{Q}(\sqrt{\frac{7}{4}+\sqrt{3}}) = \mathbb{Q}(\sqrt{3})$ (double inclusion, car $\sqrt{\frac{7}{4}+\sqrt{3}} = \pm(1+\frac{1}{2}\sqrt{3})$).

(4) Soit $x \in A$, différent de 0. Soit $P(X) = \sum_{i=0}^n a_i X^i$ le polynôme minimal de x sur K ($a_n = 1$). Alors le coefficient constant a_0 de P n'est pas nul sans quoi P aurait une racine 0 dans K et ne serait pas irréductible. Donc $xy = -a_0$, où $y = \sum_{i=1}^n a_i x^{i-1}$ est un élément de A, puisque somme de produits d'éléments de A (rappel : $K \subset A$). Comme $-a_0 \neq 0$, il a un inverse u dans K (donc dans A), et uy est alors un inverse dans A de x.

(5) Posons $E = \mathbb{Q}(\varepsilon)$, avec $\varepsilon := e^{\frac{2i\pi}{37}}$. Le polynôme minimal de ε est, selon le cours, le polynôme cyclotomique Φ_{37}, et son degré est $\phi(37) = 36$, car 37 est premier. Donc $[E : \mathbb{Q}] = 36$. Aussi, toute racine de Φ_{37} est une racine 37-ème de l'unité, donc une puissance de ε, et appartient donc à E. Puisque Φ_{37} est scindé sur E (et que E est un corps de rupture pour Φ_{37}), E est le corps de décomposition de Φ_{37}. Alors $E/\mathbb{Q}$ est normale d'après le cours.

(6) Il s'agit de chercher le nombre de racines distinctes du polynôme $P(X) = X^{12} - 1$ dans K. On a $P' = 12X^{11}$. Si la caractéristique de K est différente de 2 ou 3, alors la seule racine de P' est 0, qui n'est pas racine de P. Comme K est algébriquement clos, P a 12 racines dans K comptées avec leurs multiplicités, mais ici les racines sont simples parce qu'elles ne sont pas racines de P'. Donc $n = 12$.

Si la caractéristique de K est 2, on a $X^{12} - 1 = (X^3 - 1)^4$ et donc les racines des P sont les racines de $X^3 - 1$. Ce dernier polynôme a trois racines distinctes dans K parce que sa dérivée formelle $3X^2$ n'a que 0 comme racine, donc $n = 3$.

Si la caractéristique de K est 3, alors $X^{12} - 1 = (X^4 - 1)^3$, et, par le même procédé, $n = 4$.

(7) Supposons que E/K est une extension de degré 3 et telle que $E = K(a)$ avec $a^3 = x \in K$. Alors le polynôme minimal de a est de degré 3, et par ailleurs a annule $X^3 - x$. Donc le polynôme

minimal de a est $X^3 - x$. Donc ce polynôme est irréductible. Il n'a donc pas de racine dans K. Or, si 3 ne divise pas $|K^\times|$, alors le groupe $K^\times$ n'a pas d'élément d'ordre 3. Donc le morphisme de groupes $f : K^\times \to K^\times$ défini par $t \mapsto t^3$ est injectif, donc bijectif. Alors x est dans l'image de f et P a une racine dans K. Réciproquement, si 3 divise $|K^\times|$, alors le groupe $K^\times$ a un élément d'ordre 3 (par Cauchy, ou parce qu'il est cyclique) et donc son noyau n'est pas réduit à 1 et il n'est pas injectif et il n'est alors pas surjectif et il existe $x \in K^\times$ un élément qui n'est pas dans l'image de f. Alors le polynôme $X^3 - x$ est irréductible parce qu'un polynôme de degré 3 à coefficients dans K est réductible si et seulement s'il a une racine dans K. Si E' est un corps de rupture de $X^3 - x$, alors E' est une extension de degré 3 de K et qui peut s'écrire $E' = K(\sqrt[3]{x})$. Mais toutes les extension de degré 3 de K sont K-isomorphes (ce sont les corps de décomposition du même polynôme sur K, le fameux $X^{|K|^3} - X$). Donc E et E' sont K-isomorphes et il est facile de voir que E est alors, aussi, du type $K(\sqrt[3]{x})$.

(8) (a) Je vais utiliser des expressions du type "K-CL" pour "combinaison linéaire à coefficients dans K".

Soit X l'espace vectoriel engendré par B sur V, autrement dit l'ensemble des les V-CL d'éléments de B. Il est immédiat que X est stable par somme. Quand on fait le produit de deux éléments de X, on trouve une V-CL de produits $x_i x_j$ avec $x_i, x_j \in B$. Or, $x_i x_j \in U$ et donc $x_i x_j$ est une K-CL d'éléments de B, donc aussi une V-CL d'éléments de B. Finalement, $\sum \lambda_i (x_i x_j) = \sum \lambda_i (\sum \mu_k x_k)$ avec les λ et les μ dans V et les $x_k \in B$. Donc X est stable par produit aussi ? X contient 1 (parce que X contient V). Donc X est un sous-anneau de E. Par (4), X est alors un corps. Il contient clairement V. X contient également U parce que

- X contient les V-CL d'éléments de B,
- U est l'ensemble des K-CL d'éléments de B,
- $K \subset V$.

Aussi, UV contient X parce que UV contient V et B donc toutes les V-CL des éléments de B. Par double inclusion, $UV = X$.

(b) Soit σ un élément de $Gal(UV/K)$. σ est un K morphisme de UV dans UV, donc, comme U/K et V/K sont normales, on a $\sigma(U) = U$ et $\sigma(V) = V$ par le théorème de l'extension normale du cours. Donc σ induit des K automorphismes σ_U et σ_V de U et respectivement V. L'application $\sigma \mapsto (\sigma_U, \sigma_V)$ est une application de $Gal(UV/K)$ dans $Gal(U/K) \times Gal(V/K)$. On vérifie que c'est une morphisme de groupes (il faut vérifier la composition). Montrons qu'il est injectif. Soit σ un élément de $Gal(UV/K)$ dont l'image est l'identité, c'est-à-dire que σ_U et σ_V sont l'identité. Soit $x \in X$. Alors $x = \sum \lambda_i x_i$ avec $\lambda_i \in V$ et $x_i \in B \subset U$. On a $\sigma(x) = \sum \sigma(\lambda_i)\sigma(x_i) = \sum \sigma_V(\lambda_i)\sigma_U(x_i) = \sum \lambda_i x_i = x$. Donc σ est l'identité.