Université Lyon 1
M1G. Théorie de Galois. Le 9 mars 2016

PARTIEL

Durée : 1h30

Problème 1

Soit K un corps et P un polynôme unitaire de $K[X]$. On note P' le polynôme dérivé de P.

1. Soit $Q \in K[X]$. Montrer que si Q^2 divise P, alors Q divise P'.
2. En déduire que si $\text{pgcd}(P, P') = 1$, alors P n'a pas de facteur carré dans sa décomposition en facteurs irréductibles dans $K[X]$.

Solution.

1. Si $P(X) = Q(X)^2 R(X)$ avec $R(X) \in K[X]$, alors

$$P'(X) = 2Q(X)Q'(X)R(X) + Q(X)^2 R'(X) = Q(X)\,[2Q'(X)R(X) + Q(X)R'(X)].$$

   Ainsi $Q(X)$ divise $P'(X)$ dans $K[X]$.

2. Par contraposition: Si $P(X)$ a un facteur carré $Q(X)^2$ dans sa décomposition en facteurs irréductibles dans $K[X]$ avec $\deg Q > 1$, alors $Q(X)$ divise $P(X)$ et $P'(X)$, et donc $\text{pgcd}(P, P')$. Donc $\text{pgcd}(P, P') \neq 1$.

Problème 2

On rappelle qu'un élément α est *constructible* (à la règle et au compas) si et seulement s'il est contenu dans une tour d'extensions de degré deux sur $\mathbb{Q}$. Soit P un polynôme irréductible sur $\mathbb{Q}$.

1. Montrer que si une racine α de P est constructible, alors toutes les racines de $\mathbb{Q}$ sont constructibles.
2. Montrer que si une racine de P est constructible, alors K admet une tour d'extensions de degré deux sur $\mathbb{Q}$, où K est le corps de décomposition de P sur $\mathbb{Q}$. En déduire que $[K : \mathbb{Q}]$ est une puissance de 2.

Solution.

1. Soit $L \leq \mathbb{C}$ une tour d'extensions de degré deux de $\mathbb{Q}$ contenant α. Alors pour toute autre racine α' de P il y a un $\mathbb{Q}$-homomorphisme σ de L dans $\mathbb{C}$ avec $\sigma(\alpha) = \alpha'$. Comme $\sigma(L)$ est aussi une tour d'extensions de degré deux sur $\mathbb{Q}$, toute autre racine de P est également constructible.
2. Soient L et L' deux tours d'extensions de degré deux sur $\mathbb{Q}$, disons $L = \mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_n)$ où $[\mathbb{Q}(\beta_1, \ldots, \beta_i) : \mathbb{Q}(\beta_1, \ldots, \beta_{i-1})] = 2$ pour tout $i \leq n$. Alors pour tout $i \leq n$ soit $\beta_i \in L'(\beta_0, \ldots, \beta_{i-1})$, soit

$$1 < [L'(\beta_0, \ldots, \beta_i) : L'(\beta_0, \ldots, \beta_{i-1}] \leq [\mathbb{Q}(\beta_1, \ldots, \beta_i) : \mathbb{Q}(\beta_1, \ldots, \beta_{i-1})] = 2.$$

   Donc dans le deuxième cas le degré de l'extension vaut deux. Ainsi $L'(\beta_0, \ldots, \beta_n)$ est une tour d'extensions de degré deux sur $\mathbb{Q}$. Par récurrence, K est contenu dans une tour $\bar{K}$ d'extensions de degré deux sur $\mathbb{Q}$.

   Soient $\alpha = \alpha_1, \ldots, \alpha_k$ les racines de P. Si on admet que $L = \mathbb{Q}(\alpha)$ est une tour d'extensions de degré deux sur $\mathbb{Q}$, alors la récurrence ci-dessus donne que $\mathbb{Q}(\alpha_1, \ldots, \alpha_k) = K$ est une tour d'extensions de degré deux sur $\mathbb{Q}$. Par multiplicativité du degré, $[K : \mathbb{Q}] = 2^\ell$, où ℓ est la hauteur de la tour.

   Sinon, on utilise la correspondance de Galois : Comme $\bar{K}$ est une tour d'extensions de degré deux sur $\mathbb{Q}$, son groupe de Galois $\text{Gal}(\bar{K}/\mathbb{Q})$ admet une séries de sous-groupes

$$\text{Gal}(\bar{K}/\mathbb{Q}) = G_0 > G_1 > G_2 > \cdots > G_n = \{1\}$$

   tel que $[G_i : G_{i+1}| = 2$ pour tout $i < n$. Soit

$$N = \text{Fix}(K) = \{\sigma \in G_0 : \sigma(a) = a \text{ pour tout } a \in K\}.$$

   Puisque K est un corps de décomposition, K est galoisien sur $\mathbb{Q}$. Donc N est distingué dans $\text{Gal}(\bar{K}/K)$. Ainsi $\text{Gal}(K/\mathbb{Q})$ admet une séries de sous-groupes

$$\text{Gal}(K/\mathbb{Q}) = G_0/N \geq G_1 N/N \geq \cdots \geq G_N/N = N/N$$

   de sous-groupes chacun d'indice au plus 2 dans son prdécesseur (et y est donc distingué). Ainsi

$$\mathbb{Q} = K^{G_0/N} \leq K^{G_1 N/N} \leq \cdots \leq K^{N/N} = K$$

   est une tour d'extensions de degré au plus deux. Ainsi K est une tour d'extensions de degré deux sur $\mathbb{Q}$.

Problème 3

Soient $p_1, \ldots, p_n$ dans $\mathbb{Q}$, et $K_i = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i})$ pour $i \leq n$. On pose $K_0 = \mathbb{Q}$ et $K = K_n$. Pour $I \subseteq \{1, \ldots, n\}$ soit $a_I = \prod_{i \in I} \sqrt{p_i}$ (en particulier $a_\emptyset = 1$).

1. Montrer que K est le corps de décomposition d'un polynôme (réductible) sur $\mathbb{Q}$. En déduire que K est une extension normale.

2. On suppose que $\sqrt{p_{i+1}} \notin K_i$ pour tout $i < n$.

   (a) Calculer $[K : \mathbb{Q}]$ et $|\mathrm{Gal}(K/\mathbb{Q})|$.

   (b) Montrer que $(a_I : I \subseteq \{1, \ldots, n\})$ est une $\mathbb{Q}$-base linéaire de K.

   (c) Pour $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ soit $\sigma_i = \sigma(\sqrt{p_i})/\sqrt{p_i}$ pour $i \in \{1, \ldots, n\}$. Montrer que $\sigma_i \in \{\pm 1\}$ et que $\sigma \mapsto (\sigma_1, \ldots, \sigma_n)$ est un isomorphisme de groupes entre $\mathrm{Gal}(K/\mathbb{Q})$ et le groupe multiplicatif $\{+1, -1\}^n$.

3. On suppose que $p_1, \ldots, p_n$ sont des nombres premiers distincts et on propose de montrer que $[K : \mathbb{Q}] = 2^n$.

   (a) Montrer que c'est vrai pour $n = 0$ et $n = 1$.

   (b) Supposons, pour une contradiction, que $i < n$ est minimal avec $\sqrt{p_{i+1}} \in K_i$. Montrer qu'il y a une combinaison $\mathbb{Q}$-linéaire s de $\{a_I : I \subseteq \{1, \ldots, i\}\}$ telle que $\sqrt{p_i} = s$. En considérant les images de s par $\mathrm{Gal}(K/\mathbb{Q})$ et l'indépendance linéaire de $\{a_I : I \subseteq \{1, \ldots, i\}\}$ sur $\mathbb{Q}$, montrer que $s = q a_I$ pour un certain $q \in \mathbb{Q}$ et $I \subseteq \{1, \ldots, i\}$. Conclure que c'est impossible.

4. Soient $p_1, \ldots, p_n$ comme dans la question 3., et $\alpha_1, \ldots, \alpha_n$ dans $\mathbb{Q}$ non nuls. Déterminer les images de $\alpha := \sum_i \alpha_i \sqrt{p_i}$ sous l'action de $\mathrm{Gal}(K/\mathbb{Q})$. En déduire que α est un élément primitif de K sur $\mathbb{Q}$.

5. (Bonus) Est-ce que $\sqrt{15} \in \mathbb{Q}(\sqrt{10}, \sqrt{42})$? Justifier la réponse.

Solution.

1. Soit $P(X) = \prod_{i=1}^n (X^2 - p_i)$. Alors les racines de P sont $\pm\sqrt{p_1}, \ldots, \pm\sqrt{p_n}$. Comme $\sqrt{p_i} \in K$ pour tout $i < n$, on a aussi $-\sqrt{p_i} \in K$. Ainsi K est le corps de décomposition de P. Puisque tout corps de décomposition est normal, K est une extension normale de $\mathbb{Q}$.

2. (a) On a $K_{i+1} = K_i(\sqrt{p_{i+1}})$ pour tout $i < n$, et $X^2 - p_{i+1}$ est le polynôme minimal de $\sqrt{p_{i+1}}$ sur K_i. Donc $[K_{i+1} : K_i] = \deg(X^2 - p_{i+1}) = 2$. Par multiplicativité du degré,
   $$|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = [K_n : K_{n-1}]\,[K_{n-1} : K_{n-2}] \cdots [K_2 : K_1]\,[K_1 : K_0] = 2^n.$$

   (b) Soit $B = (a_I : I \subseteq \{1, \ldots, n\})$ et $V = \langle B \rangle$ le sous-$\mathbb{Q}$-espace vectoriel de K engendré par B. Il est facile de voir que V est clos par multiplication, puisque $a_I \cdot a_J = (\prod_{i \in I \cap J} p_i)\, a_{I \triangle J}$, où $I \triangle J$ est la différence symétrique de I et J. Or, $K = \mathbb{Q}[\sqrt{p_1}][\sqrt{p_2}] \cdots [\sqrt{p_n}] \subseteq V$. Ainsi $K = V$. Comme $[K : \mathbb{Q}] = 2^n = |B|$ et B engendre K comme $\mathbb{Q}$-espace vectoriel, B est une $\mathbb{Q}$-base linéaire de K.

   (c) Pour $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ l'image $\sigma(\sqrt{p_i})$ est une racine du polynôme minimal de $\sqrt{p_i}$ sur $\mathbb{Q}$. Donc $\sigma(\sqrt{p_i} = \pm\sqrt{p_i}$ et $\sigma_i = \sigma(\sqrt{p_i})/\sqrt{p_i} = \pm 1$. Si $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, alors
   $$(\tau \circ \sigma)(\sqrt{p_i}) = \tau(\sigma(\sqrt{p_i})) = \tau(\sigma_i \sqrt{p_i}) = \sigma_i \tau(\sqrt{p_i}) = \sigma_i \tau_i \sqrt{p_i}$$
   et $(\tau \circ \sigma)_i = \tau_i \cdot \sigma_i$. Donc $\sigma \mapsto (\sigma_1, \ldots, \sigma_n)$ est un homomorphisme de groupes. Son noyau est trivial, car si $\sigma_i = 1$ pour $i = 1, \ldots, n$, alors σ fixe tous les $\sqrt{p_i}$ et donc K. Ainsi l'homomorphisme est injectif ; comme $|\mathrm{Gal}(K/\mathbb{Q})| = 2^n = |\{+1, -1\}^n|$, il est aussi surjectif, et donc un isomorphisme.

3. (a) Pour $n = 0$ on a $[K_0 : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}] = 1 = 2^0$. Pour $n = 1$, comme p_1 est premier, on a $\sqrt{p_1} \notin \mathbb{Q}$ et $[K_1 : \mathbb{Q}] = 2 = 2^1$.

   (b) Soit $B = (a_I : I \subseteq \{1, \ldots, i\})$. D'après 2.($b$) c'est une $\mathbb{Q}$-base de K_i. Donc si $\sqrt{p_{i+1}} \in K_i$, il est égal à a une $\mathbb{Q}$-combinaison linéaire de B, disons $\sqrt{p_{i+1}} = \sum_{I \subseteq \{1,\ldots,i\}} q_I a_I$ avec $q_I \in \mathbb{Q}$. Supposons que $q_{I_0}, q_{I_1} \neq 0$ pour des $I_0 \neq I_1$. On peut supposer qu'il y a $j \in I_0 \setminus I_1$. D'après 2.(c) il y a $\sigma \in \mathrm{Gal}(K_i/\mathbb{Q})$ avec $\sigma_\ell = 1$ pour $\ell \neq j$ et $\sigma_j = -1$. Alors $\sigma(a_I) = a_I$ si $j \notin I$ et $\sigma(a_I) = -a_I$ si $j \in I$. De plus,
   $$\pm \sum_{I \subseteq \{1,\ldots,i\}} q_I a_I = \pm\sqrt{p_{i+1}} = \sigma(\sqrt{p_{i+1}}) = \sigma\Big(\sum_{I \subseteq \{1,\ldots,i\}} q_I a_I\Big) = \sum_{I \subseteq \{1,\ldots,i\}} q_I \sigma(a_I) = \sum_{j \notin I} q_I a_I - \sum_{j \in I} q_I a_I.$$
   On en déduit soit $\sum_{j \in I} q_I a_I = 0$, soit $\sum_{j \notin I} q_i a_I = 0$, ce qui contredit l'indépendance linéaire de B. Donc $q_I = 0$ pour tout I sauf un, et $\sqrt{p_{i+1}} = q_{I_0} a_{I_0}$ pour un $I_0 \subseteq \{1, \ldots, i\}$ et $q_{I_0} \in \mathbb{Q}$. Donc $p_{i+1} = q_{I_0}^2 \prod_{i \in I_0} p_i$, ce qui est impossible d'après le lemme de Gauss.

4. On a $\sigma(a) = \sigma(\sum_{i=1}^n a_i \sqrt{p_i}) = \sum_{i=1}^n \sigma_i a_i \sqrt{p_i}$. Ces éléments sont tous différents. Ainsi a a 2^n images sous l'action de $\mathrm{Gal}(K/\mathbb{Q})$ d'après 2. et 3., et a est bien un élément primitif.

5. On prend $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ et $p_4 = 7$, et $\sigma \in \mathrm{Gal}(K_4/\mathbb{Q})$ avec $\sigma_2 = \sigma_5 = \sigma_7 = -1$ et $\sigma_3 = 1$. Alors $\mathbb{Q}(\sqrt{10}, \sqrt{42}) \leq I(\langle\sigma\rangle)$, mais $\sigma(\sqrt{15}) = -\sqrt{15}$. Donc $\sqrt{15} \notin \mathbb{Q}(\sqrt{10}, \sqrt{42})$.