Université Lyon 1
M1G. Théorie de Galois.

Le 29 mars 2017

PARTIEL

Durée : 1h30

Documents non admis.
Les résultats d'une question peuvent être utilisés pour les questions suivantes.

Problème 1

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

1. Donner une condition nécessaire et suffisante pour que $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$.
2. On suppose que $\sqrt{b} \notin \mathbb{Q}(\sqrt{a})$. Déterminer le groupe de Galois G de $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ sur $\mathbb{Q}$.
3. Donner ses éléments explicitement.
4. Déterminer tous les sous-groupes de G.
5. Déterminer tous les sous-corps de $\mathbb{Q}(\sqrt{a}, \sqrt{b})$.
6. Soit $n \in \mathbb{Z}$. Donner la condition nécessaire et suffisante pour que $\sqrt{n} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$.
7. Donner la condition nécessaire et suffisante pour que $\sqrt{n} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Solution.

1. $\mathbb{Q}(\sqrt{a}) = \mathbb{Q} \oplus \sqrt{a}\,\mathbb{Q}$. Donc $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ si et seulement s'il y a $q, r \in \mathbb{Q}$ avec $\sqrt{b} = q + \sqrt{a}\,r$. Donc

$$ar^2 = (\sqrt{b} - q)^2 = b + q^2 - 2q\sqrt{b}.$$

Si $q = 0$ on a $\sqrt{b} = r\sqrt{a}$ et $b = r^2 a$. Sinon $\sqrt{b} = (b + q^2 - ar^2)/2q$ et b est un carré dans $\mathbb{Q}$. Ainsi $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ si et seulement si b est un carré dans $\mathbb{Q}$ ou si $b^{-1}a$ est un carré dans $\mathbb{Q}$.

2. et 3. Puisque $b \notin \mathbb{Q}(\sqrt{a})$, le polynôme minimal de $\sqrt{b}$ sur $\mathbb{Q}(\sqrt{a})$ est $P_b(X) = X^2 - b$, puisqu'il est annulé par $\sqrt{b}$ et un diviseur propre de P_b serait de degré un, ce qui impliquerait $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$. Il est dans $\mathbb{Q}[X]$, et ses racines sont $\pm\sqrt{b}$.

Si a est un carré dans $\mathbb{Q}$, alors $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}$, et $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{b})$ contient les deux racines de P_b: C'est à la fois son corps de rupture et son corps de décomposition, et donc normal sur $\mathbb{Q}$ de degré $\deg P_b = 2$. $G = \mathbb{Z}/2\mathbb{Z}$, le groupe avec deux éléments. Ses éléments sont id et l'automorphisme induit sur $\mathbb{Q}$ par $\sqrt{b} \mapsto -\sqrt{b}$.

Si a n'est pas un carré dans $\mathbb{Q}$, alors $\sqrt{a} \notin \mathbb{Q}$ et le polynôme minimal de $\sqrt{a}$ sur $\mathbb{Q}$ est $X^2 - a$ pour les mêmes raisons. Alors $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ est le corps de décomposition de $P_a(X)P_b(X)$, et donc normal sur $\mathbb{Q}$. On a

$$[\mathbb{Q}(\sqrt{(a}, \sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})] \cdot [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2 \cdot 2 = 4,$$

et $|G| = 4$. Ses éléments sont id et les automorphismes induits sur $\mathbb{Q}$ par

$$\sigma_1 ! \sqrt{a} \mapsto -\sqrt{a},\ \sqrt{b} \mapsto \sqrt{b}, \quad \sigma_2 : \sqrt{a} \mapsto \sqrt{a},\ \sqrt{b} \mapsto -\sqrt{b}, \quad \sigma_3 : \sqrt{a} \mapsto -\sqrt{a},\ \sqrt{b} \mapsto -\sqrt{b}.$$

Ainsi $G = (\mathbb{Z}/2\mathbb{Z})^2$.

4. et 5. Si a est un caré dans $\mathbb{Q}$, les seuls sous-groupes de $G = \mathbb{Z}/2\mathbb{Z}$ sont $\{1\}$ et G, et les sous-corps invariants correspondants sont $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{b})$ et $\mathbb{Q}$.

Si a n'est pas un carré dans $\mathbb{Q}$, alors les sous-groupes de $G = (\mathbb{Z}/2\mathbb{Z})^2$ sont $\{1\}$, G, et les trois sous-groupes $\{[\mathrm{id}, \sigma_i\}$ pour $i = 1, 2, 3$, qui sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$. Les corps invariants respectifs sont

$$\mathbb{Q}(\sqrt{a}, \sqrt{b}), \quad \mathbb{Q}, \quad , \mathbb{Q}(\sqrt{b}), \quad \mathbb{Q}(\sqrt{a}), \quad \mathbb{Q}(\sqrt{ab})$$

de degré deux sur $\mathbb{Q}$.

6. On a $\sqrt{n} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$ si et seulement si $\mathbb{Q}(\sqrt{n})$ est un des sous-corps de degré 2 sur $\mathbb{Q}$ de $\mathbb{Q}(\sqrt{a}, \sqrt{b})$, qui sont $\mathbb{Q}(\sqrt{b})$, $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{ab})$. Comme dans 1. c'est le cas si et seulement si soit n est un carré dans $\mathbb{Q}$, ou si un de $n^{-1}a$, $n^{-1}b$ ou $n^{-1}ab$ est un carré dans $\mathbb{Q}$.

7. La condition est que un de n, $n/2$, $n/3$, $n/5$, $n/6$, $n/10$ ou $n/15$ est un carré dans $\mathbb{Q}$.

Problème 2

Soit $P(X) \in \mathbb{Q}[X]$ un polynôme irréductible de degré p où p est premier, et G son groupe de Galois.

1. Montrer que p divise l'ordre de G.

2. Montrer que G contient un élément d'ordre p.

3. On considère G comme un sous-groupe du groupe symétrique S_p. Montrer que G contient une permutation cyclique d'ordre p.

4. On suppose que $P(X)$ a exactement $p-2$ racines réelles. Montrer que G contient une transposition.

On admet le résultat suivant (assez simple) : Si un sous-groupe G de S_p contient un cycle d'ordre p et une transposition, alors $G = S_p$.

5. Soit $P(X) = X^5 - 10X + 2$. Montrer que $P(X)$ est irréductible sur $\mathbb{Q}$.

6. Montrer que le groupe de Galois de P est S_5. (*Indication: étudier les extréma locaux de $P(X)$.*)

Solution.

1. Soit K le corps de rupture de P sur $\mathbb{Q}$, et L son corps de décomposition, qui est la clôture normale de K. Alors $[K : \mathbb{Q}] = \deg P = p$ et
$$|G| = [L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}].$$
Ainsi $p \mid |G|$.

2. C'est le théorème de Cauchy.

3. Soit $\sigma \in G$ un élément d'ordre p. Alors σ est le produit de cycles disjoints $c_1,\ldots,c_k$ de longueurs $n_1,\ldots,n_k$, et l'ordre de σ est $\mathrm{ppcm}(n_1, \ldots, n_k)$. Si aucun de ces cycles n'est un p-cycle, alors $n_i < p$ pour tout $i \leq k$, et $\mathrm{ppcm}(n_1, \ldots, n_k)$ divise $(p-1)!$. Or, $p \nmid (p-1)!$, une contradiction. Donc σ est un p-cycle.

4. Les deux racines non-réelles de P doivcent être des racines complexes conjugués α et $\bar{\alpha}$, puisque P est un polynôme réel. Ainsi la conjugaison complexe induit le 2-cycle $(\alpha, \bar{\alpha}) \in G$, puisqu'il stabilise L par normalité, et fixe les racines réelles.

5. P est un polynôme unitaire sur $\mathbb{Z}$. On applique Eistenstein avec $p = 2$: on a que 2 divise tous les coefficients sauf le coefficient dominant, et 2^2 ne divise pas le terme constant. Donc P est irréductible sur $\mathbb{Z}$, et d'après le lemme de Gauss sur $\mathbb{Q}$.

6. On a $P'(X) = 5X^4 - 10$. Ainsi $P'(X) = 0$ si et seulement si $X^4 = 2$, si et seulement si $X = \pm\sqrt[4]{2}$, pour X réel. Puisque $\lim_{X\to-\infty} P(X) = -\infty$ et $\lim_{X\to\infty} P(X) = \infty$, il y a un maximum pour $X = -\sqrt[4]{2}$ et un minimum pour $X = \sqrt[4]{2}$; les valeurs sont
$$P(-\sqrt[4]{2}) = (-\sqrt[4]{2})(2-10) + 2 = 8\sqrt[4]{2} + 2 > 0 \quad \text{et} \quad P(\sqrt[4]{2}) = (\sqrt[4]{2})(2-10) + 2 = -8\sqrt[4]{2} + 2 < 0.$$
Il en découle que P a exactement 3 racines réelles. Les hypothèses de 1.–4. sont donc satisfaites, et G contient un 5-cycle et une transposition. D'après le résultat admis, $G = S_5$.

Problème 3

Soit $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et soit $a \in \bar{\mathbb{Q}} \setminus \mathbb{Q}$.

1. Montrer qu'il existe un sous-corps $K \leq \bar{\mathbb{Q}}$ tel que $a \notin K$ et que tout sous-corps de $\bar{\mathbb{Q}}$ contenant strictement K contient a ; on dit que K est un sous-corps de $\mathbb{Q}$ maximal sans a. (*Indication : utiliser le lemme de Zorn.*)

On choisit un nombre premier p divisant $[K(a) : K]$. Soit $K \leq L \leq \bar{\mathbb{Q}}$ une extension finie non triviale de K. On note M la clôture normale de L dans $\bar{\mathbb{Q}}$ et $G := \mathrm{Gal}(M/K)$.

2. Montrer que p divise $[L : K]$.

3. Montrer que $[L : K]$ est une puissance de p. (*Indication : appliquer la théorie de Galois à l'extension* $K \leq M$.)

4. Montrer que $[K(a) : K] = p$ et que $K(a)$ est la seule sous-extension de $K \leq \bar{\mathbb{Q}}$ de degré p sur K.

Pour les parties 3. et 4. on pourra utiliser le théorème suivant (admis sans démonstration) :

Théorème de Sylow. Soit p un nombre premier et soit G un groupe fini de cardinal mp^r, où p ne divise pas m. Alors il existe un sous-groupe de G de cardinal p^r. Plus précisément, pour tout sous-groupe H de G de cardinal p^s, avec $0 \leq s \leq r$, et tout $s \leq t \leq r$, il existe un sous-groupe de G contenant H et de cardinal p^t.

Solution.

1. Les sous-corps de $\bar{\mathbb{Q}}$ qui ne conteinnent pas a sont partiellement ordonnés par inclusion, et une réunion d'une chaîne de sous-corps de $\bar{\mathbb{Q}}$ dont aucun ne contient a est toujours un sous-corps de $\bar{\mathbb{Q}}$ qui ne contient pas a. Donc c'est un ordre partiel inductif non-vide ($\mathbb{Q}$ en fait partie) ; d'après le lemme de Zorn il y a un élément maximal K, qui est un sous-corps de $\bar{\mathbb{Q}}$ maximal sans a.

2. Par maximalité de K on a $a \in L$, et donc $K(a) \leq L \leq M$. Ainsi

$$p \mid [L : K(a)] \cdot [K(a) : K] = [L : K].$$

3. On a $p \mid [M : L] \cdot [L : K] = [M : K] = |G|$. D'aprs le théorème de Sylow il y a un p-sous-groupe S de G tel que $p \nmid |G|/|S|$. Soit $N = M^S$ le corps invariant de S. Alors M est normal sur N et $\mathrm{Gal}(M/N) = S$. Ainsi

$$[N : K] = \frac{[M : K]}{[M : N]} = \frac{|\mathrm{Gal}(M/K)|}{|\mathrm{Gal}(M/N)|} = \frac{|G|}{|S|}.$$

Donc $p \nmid [N : K]$. D'après 2. appliqué à N, l'extension N/K est l'extension triviale. Ainsi $N = K$ et $G = S$. L'ordre du p-groupe S est une puissance de p (d'après le théorème de Cauchy aucun autre nombre premier peut diviser $|G|$).

4. On prend $L = K(a)$. Supposons $G \ncong \mathbb{Z}/p\mathbb{Z}$, donc $|G| = p^r$ avec $r > 1$. D'après le théorème de Sylow il y a un sous-groupe H de G de cardinal p^{r-1} ; soit N le corps fixe de H. Puisque $\{1\} < H < G$ on a $L > N > K$ d'après la correspondance de Galois. Ainsi N est une extension non-triviale de K, et doit contenir a. Alors $N \geq K(a) = L$, une contradiction. Donc $G = \mathbb{Z}/p\mathbb{Z}$, et $[K(a) : K] = p$.

Soit enfin $L \leq \bar{\mathbb{Q}}$ une extension de K de degré p. Alors $a \in L$ par maximalité de K, et $K \leq K(a) \leq L$. Puisque $[L : K] = [K(a) : L]$, on a $L = K(a)$.