Théorie de Galois L3, 2017-2018 Durée : 3h00 B. Calmès

Correction de l'examen de première session

Exercice 1. Soit F un corps de caractéristique 0 contenant μ_n, les racines n-ièmes de l'unité, i.e. toutes les racines du polynôme $X^n - 1$. Soient $a_1, \dots, a_k$ des éléments *distincts* non nuls de F. On considère E/F, une extension de décomposition du polynôme

$$P(X) = (X^n - a_1)(X^n - a_2) \dots (X^n - a_k).$$

(1) Montrer que les racines de P sont simples.

(2) Pour chaque $i \in \{1, \dots, k\}$, on choisit α_i une racine n-ième de a_i. Exprimer toutes les autres racines de $X^n - a_i$ en utilisant α_i et des éléments de F.

(3) Montrer qu'un élément σ du groupe de Galois $\mathrm{Gal}(E/F)$ est caractérisé par la donnée de $\big(\sigma(\alpha_i)\big)_{i=1,\dots,k}$.

(4) Montrer que $\mathrm{Gal}(E/F)$ est abélien. On pourra utiliser la question précédente pour comparer $\sigma\tau$ et $\tau\sigma$, lorsque $\sigma, \tau \in \mathrm{Gal}(E/F)$.

(5) L'extension E/F est-elle normale ?

(6) Montrer que l'ordre de tout élément de $\mathrm{Gal}(E/F)$ divise n. En déduire que le ppcm des ordres des éléments de $\mathrm{Gal}(E/F)$ divise n.

(7) Montrer que si $n = p$ est premier, et que $P(X) = X^p - a$ (un seul facteur), alors soit $X^p - a$ se décompose en produits de facteurs de degré 1 et $\mathrm{Gal}(E/F)$ est le groupe trivial, soit $\mathrm{Gal}(E/F)$ est cyclique d'ordre p.

(8) Trouver un exemple de polynôme P où le ppcm des ordres des éléments de $\mathrm{Gal}(E/F)$ est égal à n et un exemple où il est différent.

Solution. (1) Les racines sont différentes d'un facteur à l'autre, puisque leurs puissances n-ièmes sont différentes. Au sein d'un même facteur, il n'y a pas de racine double puisque la dérivée est nX^{n-1} et n'a que 0 pour racine.
(2) Les racines de $X^n - a_i$ sont les $\xi\alpha_i$ où $\xi \in \mu_n$.
(3) Un élément du groupe de Galois est caractérisé par son action sur toutes les racines (cf. cours). Mais ici, pour chaque i, la donnée de $\sigma(\alpha_i)$ suffit puisque les autres valeurs $\sigma(\xi\alpha_i) = \xi\sigma(\alpha_i)$ s'en déduisent.
(4) Vérifions que $\sigma\tau(\alpha_i) = \tau\sigma(\alpha_i)$ pour tout i. En effet, si $\sigma(\alpha_i) = \xi\alpha_i$ et $\tau(\alpha_i) = \zeta\alpha_i$, alors $\sigma\tau(\alpha_i) = \sigma(\zeta\alpha_i) = \zeta\xi\alpha_i$ et de même $\tau\sigma(\alpha_i) = \tau(\xi\alpha_i) = \xi\zeta\alpha_i$. Donc $\sigma\tau = \tau\sigma$.
(5) L'extension E/F est normale (et même finie) puisque c'est une éxtension de décomposition d'un polynôme.
(6) Soit $\sigma \in \mathrm{Gal}(E/F)$. Montrons que $\sigma^n = \mathrm{id}$ (et donc son ordre divise n). Il suffit de vérifier que $\sigma(\alpha_i) = \alpha_i$ pour tout i, par la question (3). Or $\sigma(\alpha_i) = \xi^k\alpha_i$ pour un

certain k, puisque σ permute les racines de (tout polynôme à coeffciients dans F et en particulier) $X^n - a_i$. Donc $\sigma^n(\alpha_i) = (\xi^k)^n \alpha_i = \xi^{nk}\alpha_i = \alpha_i$ puisque $\xi \in \mu_n$.
(7) Dans le cas où $n = p$ est premier et où $P = X^p - a$, on a donc que l'ordre de tout élément dans le groupe de Galois divise p. Si tous les élément sont d'ordre 1, alors $\mathrm{Gal}(E/F) = \{1\}$ et $[E : F] = 1$. Donc $E = F$ et toutes les racines de P sont dans F. Il se décompose donc en produits polynômes de degré 1. Si au contraire il y a au moins un élément d'ordre p, alors $\#\mathrm{Gal}(E/F) \geq p$. Mais $E = F[\alpha]$ où α est une racine n-ième de a (les autres racines sont automatiquement dans $F[\alpha]$ puisque $\mu_n \subset F$), et $F[\alpha] \simeq F[X]/Q$ où Q est le polynôme minimal de α, qui divise donc $X^p - a$ et est donc de degré $\leq p$. D'où $[E : F] \leq p$. Mais $\#\mathrm{Gal}(E/F) = [E : F]$ donc les deux valent p et ce polynôme minimal est bien $X^p - a$ qui est ainsi irréductible. De plus $\mathrm{Gal}(E/F)$ est alors cyclique, engendré par exemple par l'élément d'ordre p choisi plus haut.
(8) Dans le cas où $n = p$ est premier, la question précédente nous dit que si on a un seul facteur et qu'il est irréductible, alors le ppcm des ordres est p puisque le groupe de Galois est $\mathbb{Z}/p\mathbb{Z}$ et on a donc égalité. Par exemple $X^2 - 2$ sur $\mathbb{Q}$ (qui contient $\mu_2 = \{\pm 1\}$). De même, si le polynôme n'est pas irréductible, alors il est scindé et le groupe de Galois est trivial, donc il n'y pas égalité ; par exemple $X^2 - 1$.

Exercice 2. On rappelle qu'un polynôme cyclotomique est irréductible sur $\mathbb{Q}$.

(1) Quel est le polynôme minimal sur $\mathbb{Q}$ du nombre complexe $\xi = e^{2i\pi/7}$?

(2) On rappelle qu'un nombre complexe z est *constructible* si et seulement s'il existe une tour d'extensions *quadratiques* $\mathbb{Q} = L_0 \subset L_1 \subset \cdots L_n = L$ avec $z \in L$. Montrer que ξ n'est pas constructible (en particulier le polygône régulier à 7 côtés n'est pas constructible à la règle et au compas).

(3) Décrire un isomorphisme entre $(\mathbb{Z}/7\mathbb{Z})^*$ et $\mathbb{Z}/2 \times \mathbb{Z}/3$ et en déduire que le groupe de Galois de $\mathbb{Q}[\xi]/\mathbb{Q}$ est isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/3$.

(4) Montrer qu'il contient exactement un élément d'ordre 2, qu'on notera τ, et deux éléments d'ordre 3, inverses l'un de l'autre ; on en choisit un qu'on note σ et l'autre σ^{-1}.

(5) Faire la liste de tous les sous-groupes du groupe de Galois et en déduire le nombre de sous-corps de $\mathbb{Q}[\xi]$.

(6) Notons $K = \mathbb{Q}[\xi]^\sigma$ et $L = \mathbb{Q}[\xi]^\tau$. Quels sont les degrés $[K : \mathbb{Q}]$ et $[L : \mathbb{Q}]$?

(7) Montrer que le polynôme minimal de ξ sur K est

$$X^3 - (\xi + \xi^2 + \xi^4)X^2 + (\xi^3 + \xi^5 + \xi^6)X - 1$$

(indication : penser à un exercice du DS).

(8) On note $u = \xi + \xi^2 + \xi^4$ et $v = \xi^3 + \xi^5 + \xi^6$. Montrer que ce sont les deux racines d'un polynôme de degré 2 sur $\mathbb{Q}$, puis les calculer (i.e. les exprimer avec des rationnels et des racines carrées de rationnels).

(9) En déduire que $K = \mathbb{Q}[\sqrt{-7}]$ (i.e. $\mathbb{Q}[i\sqrt{7}]$).

(10) Appliquer la même méthode pour trouver w (exprimé en fonction de ξ) tel que $L = \mathbb{Q}[w]$ et donner le polynôme minimal de w sur $\mathbb{Q}$. N.B. on ne demande pas d'exprimer w par racines cubiques, même si c'est possible par les formules de Cardan.

Solution. (1) C'est le polynôme cylotomique $\Phi_7(X) = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6$.
(2) L'extension qu'il engendre étant de degré 6, il ne peut être dans une tour d'extensions de degré 2.
(3) Ce groupe est canoniquement isomorphe à $(\mathbb{Z}/7\mathbb{Z})^\times$ d'après le cours, or ce dernier est de cardinal 6 et commutatif, donc isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/3$. On peut bien entendu donner un isomorphisme explicite : puisque ces deux groupes sont cycliques d'ordre 6 (théorème Chinois pour le deuxième, et on vérifie que $(\mathbb{Z}/7\mathbb{Z})^\times$ est engendré par 3, dont les puissances sont 3, $3^2 = 2$, $3^3 = 6 = -1$, $3^4 = -3 = 4$, $3^5 = -2$, $3^6 = 1$). Un isomorphisme $\mathbb{Z}/2 \times \mathbb{Z}/3 \to (\mathbb{Z}/7\mathbb{Z})^\times$ est alors obtenu en envoyant $(1,1)$ sur 3, et donc $k(1,1)$ sur 3^k. En calculant ces éléments l'un après l'autre, on voit alors que cet isomorphisme envoie un élément du premier tableau $(\mathbb{Z}/2 \times \mathbb{Z}/3)$ vers celui du deuxième en même position (dans $(\mathbb{Z}/7\mathbb{Z})^\times$)

$$\begin{array}{ccc} (0,0) & (0,1) & (0,2) \\ (1,0) & (1,1) & (1,2) \end{array} \qquad \begin{array}{ccc} 1 & 4 & 2 \\ 6 & 3 & 5 \end{array}$$

On aurait bien entendu également pû faire correspondre $(1,1)$ avec l'autre élémen d'ordre 6, qui est 5 (l'inverse de 3). (4) Il y a exactement un élément d'ordre 2 dans $\mathbb{Z}/2 \times \mathbb{Z}/3$, l'élément $(1,0)$. Il correspond à l'élément d'ordre 2 qui est la classe de -1 dans $(\mathbb{Z}/7\mathbb{Z})^\times$. Il envoie donc ξ sur $\xi^{-1} = \xi^6$. Il y a exactement deux éléments d'ordre 2 dans $\mathbb{Z}/3 \times \mathbb{Z}/3$, les éléments $(0,1)$ et $(0,-1)$, évidemment inverses l'un de l'autre. Ils correspondent aux éléments 2 et 4 dans $(\mathbb{Z}/7\mathbb{Z})^\times$ et envoient donc ξ respectivement sur ξ^2 et ξ^4. Décidons pour la suite que σ est celui qui envoie ξ sur ξ^2.
(5) Les sous-groupes de $\mathbb{Z}/2 \times \mathbb{Z}/3$ sont le groupe trivial, le groupe tout entier, $\mathbb{Z}/2$ et $\mathbb{Z}/3$. Il y a donc quatre sous-groupes dans le groupe de Galois (en comptant le trivial et le groupe tout entier). Il y a donc quatre sous-corps de $\mathbb{Q}[\xi]$ (un tel sous-corps contient forcément $\mathbb{Q}$), et donc deux qui sont strictement entre $\mathbb{Q}$ et $\mathbb{Q}[\xi]$.
(6) Par la correspondance de Galois, puisque σ engendre un groupe d'ordre 3, on a $[\mathbb{Q}[\xi] : K] = 3$ et donc $[K : \mathbb{Q}] = 2$ puisque $[\mathbb{Q}[\xi] : K][K : \mathbb{Q}] = [\mathbb{Q}[\xi] : \mathbb{Q}] = 6$. De même $[L : \mathbb{Q}] = 3$.
(7) Par l'exercice du DS, le polynôme minimal de ξ sur K est constitué du produit des $(X - y)$ où y parcourt l'orbite de ξ par σ. Or $\sigma(\xi) = \xi^2$. Donc l'orbite de ξ est $\{\xi, \xi^2, \xi^4\}$ et le polynôme minimal est $(X - \xi)(X - \xi^2)(X - \xi^4)$ qui est égal à celui recherché en utilisant $\xi^7 = 1$.
(8) En utilisant les relations $\xi^7 = 1$ et $\sum_0^7 \xi^i = 0$, on voit que $u + v = -1$ et $uv = 2$. Le polynôme recherché est donc $X^2 + X + 2$, dont les racines sont $u = (-1 + i\sqrt{7})/2$ et $v = (-1 - i\sqrt{7})/2$ (u est de partie imaginaire positive).

(9) On a donc $K = \mathbb{Q}[u] = \mathbb{Q}[i\sqrt{7}]$, puisque u est dans K, et hors de $\mathbb{Q}$, donc $\mathbb{Q}[u] = K$ pour des raisons de degré.
(10) Par la même méthode, on voit que le polynôme minimal de ξ sur L est $(X - \xi)(X - \xi^{-1}) = X^2 - (\xi + \xi^{-1})X + 1$. Posons $w = \xi + \xi^{-1}$. En calculant w^2 et w^3, on voit immédiatement que $w^3 + w^2 - 2w - 1 = 0$. Ce polynôme est bien le polynôme minimal de w, sinon on aurait $[\mathbb{Q}[w] : \mathbb{Q}] < 3$ donc $6 = [\mathbb{Q}[\xi] : \mathbb{Q}] = [\mathbb{Q}[\xi] : \mathbb{Q}[w]][\mathbb{Q}[w] : \mathbb{Q}] < 2 \cdot 3 = 6$. On a donc $[\mathbb{Q}[w] : \mathbb{Q}] = 3$ donc $L = \mathbb{Q}[w]$.

Exercice 3. Soit F un corps et E une extension finie de F. On dit qu'une extension L de E est une *clôture normale* de E si L/F est normale finie, et si elle est minimale : il n'existe aucun sous-corps strict $K \subset L$ contenant (l'image de) E tel que K/F soit normale.

(1) Montrer que si $\omega : F \hookrightarrow \Omega$ est une clôture algébrique de F, alors on peut factoriser ω à travers E. Dans la suite, on identifiera F et E à leurs images dans Ω et on considèrera donc que $F \subset E \subset \Omega$.
(2) Rappeler pourquoi on peut écrire $E = F[a_1, \ldots, a_n]$ pour certains $(a_i)_{i=1,\ldots,n}$ dans E.
(3) Pour chaque $i \in \{1, \ldots, n\}$, notons $P_i \in F[X]$ le polynôme minimal de a_i et notons L' l'extension de décomposition de $Q = \prod_{i=1}^n P_i$ contenue dans Ω. Montrer que c'est une clôture normale de E.
(4) Réciproquement, montrer qu'un sous-corps L de Ω contenant E et qui est une clôture normale de E doit contenir L'.
(5) En déduire que $L' = L$ et qu'il existe donc une unique clôture normale de E contenue dans Ω.
(6) Application : rappeler pourquoi $\mathbb{Q}[\sqrt[3]{2}]$ n'est pas normale sur $\mathbb{Q}$ et déterminer sa clôture normale incluse dans dans $\mathbb{C}$.
(7) Rappeler pourquoi une extension normale finie en caractéristique zéro n'a qu'un nombre fini de sous-extensions.
(8) En déduire que toute extension finie en caractéristique zéro n'a qu'un nombre fini de sous-extensions.

Solution. (1) C'est une proposition du cours (5.8 du résumé 1).
(2) Cela a été prouvé et utilisé de nombreuses fois dans le cours. On raisonne par récurrence sur le degré (fini) $[E : F]$. Soit $E = F$ et c'est terminé (avec $n = 0$, aucun élément), soit $E \neq F$ et on prend un élément $a \in E \setminus F$. Alors a est algébrique sur F (puisque E est finie donc algébrique) et $[F[a] : F] > 1$ sinon $F[a] = F$ et $a \in F$. Donc $[E : F[a]] < [E : F]$ et par l'hypothèse de récurrence, il existe des $a_1, \ldots, a_k$ tels que $E = (F[a])[a_1, \ldots, a_k]$. Donc $E = F[a_1, \ldots, a_k, a]$.
(3) Appelons L/E l'extension de décomposition de Q (considéré dans $E[X]$). Alors L/F est également une extension de décomposition de Q (considéré dans $F[X]$), puisque Q se décompose dans L en produit de facteurs de degré 1 et une telle extension de F doit contenir tous les a_i, donc contient E. L'extension L/F est donc normale puisqu'une extension de décomposition d'un polynôme est normale par le

cours. De plus, elle est minimale puisque toute sous-extension normale K/F de L contenant E doit, par normalité, contenir pour chaque i toutes les racines de P_i puisqu'elle contient $a_i \in E$. Elle est donc égale à L.
(4) Réciproquement, une extension normale L de F contenant E doit contenir toutes les racines de chaque P_i (donc de Q) par normalité puisqu'elle contient chaque a_i, donc elle doit contenir L'.
(5) On a alors $L' = L$ par minimalité. Toute clôture normale de E dans Ω est donc égale à ce L', d'où l'unicité.
(6) La clôture normale de $\mathbb{Q}[\sqrt[3]{2}]$ incluse dans $\mathbb{C}$ est donc égale à $\mathbb{Q}[\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, j]$.
(7) Si une extension L/F est normale finie en caractéristique zéro, alors la correspondance de Galois s'applique et fournit une bijection entre ses sous-extensions de L/F et les sous-groupes du groupe de Galois $\mathrm{Gal}(L/F)$, qui sont en nombre fini puisque $\mathrm{Gal}(E/F)$ est lui-même fini. On a donc un nombre fini de sous-extensions.
(8) On la plonge dans sa clôture normale qui n'a elle-même qu'un nombre fini de sous-extensions.