Département de mathématiques et de statistique
Université de Montréal
Théorie de Galois. Mat 3661. Examen Intra
Le 22 février 2017. 9h30-11h20
Professeure: Matilde N. Lalín

1. Aucun document ni calculatrice ni autres instruments ne sont autorisés.
2. Les téléphones cellulaires doivent être éteints.
3. Lisez attentivement les questions avant de commencer à travailler.
4. **Justifiez tous vos raisonnements.**
5. Continuez sur le verso de la feuille si vous avez besoin de plus d'espace.
6. Répondez à toutes les questions dans les cahiers d'examen.
7. Évitez de déchirer les cahiers d'examen.

1. (6 points) Trouvez les corps de décomposition de $x^6 - 8$ sur $\mathbb{Q}$ et donnez son degré. Justifiez bien votre réponse.

Solution: Les racines de ce polynôme sont $\sqrt{2}\xi_6^k$ avec $k = 0, 1, \ldots, 5$. Alors, $K = \mathbb{Q}(\sqrt{2}, \xi_6)$. On écrit

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

On sait que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ($x^2 - 2$ irréductible par Einsestein). Aussi, on sait que le polynôme minimal de ξ_6 sur $\mathbb{Q}$ est $\Phi_6(x) = x^2 - x + 1$ (Preuve: on a vu que $\Phi_6(x) = \Phi_3(-x)$. Une autre forme: $x^6 - 1 = (x-1)(x^2+x+1)(x+1)(x^2-x+1)$ et comme $\Phi_1(x) = x-1$, $\Phi_2(x) = x+1$, $\Phi_3(x) = x^2+x+1$, on a que $\Phi_6(x) = x^2-x+1$). De plus, $\xi_6 \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. Alors, $[K : \mathbb{Q}(\sqrt{2})] = 2$ et $[K : \mathbb{Q}] = 4$.

Une autre faiçon de penser: on peut calculer que $\xi_6 = \frac{1 \pm \sqrt{3}i}{2}$. Alors, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}i)$ et $[K : \mathbb{Q}(\sqrt{2})] = 2$ parce que $\sqrt{3}i$ est racine de $x^2 + 3$ et $\sqrt{3}i \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$.

2. (6 points) (a) Trouvez le polynôme minimal de $\alpha = 2\cos\left(\frac{\pi}{10}\right)$ sur $\mathbb{Q}$. Vous pouvez vous servir du fait que

$$\cos(5\theta) = 16\cos(\theta)^5 - 20\cos(\theta)^3 + 5\cos(\theta).$$

(b) Trouvez $\mathbb{Q} \subseteq K \subset \mathbb{Q}(\alpha)$ tel que $[\mathbb{Q}(\alpha) : K] = 2$.

(c) Est-il possible de construire α avec un règle non-graduée et un compas ?

Solution: (a) Soit $\theta = \frac{\pi}{10}$ et $5\theta = \frac{\pi}{2}$. On a donc $\cos(5\theta) = 0$. Il faut donc considérer le polynôme

$$0 = 16x^5 - 20x^3 + 5x$$

En multipliant par 2 et en faisant le changement de variables $y = 2x$, on a

$$0 = (y^4 - 5y^2 + 5)y$$

Notons que $y^4 - 5y^2 + 5$ est irreductible par Eisenstein avec $p = 5$. Il est clair que $2\cos(\theta) \neq 1$. Alors, $m_{\alpha,\mathbb{Q}}(y) = y^4 - 5y^2 + 5$. Cela implique en particulier que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

(b) On a que $\alpha = \pm\sqrt{\frac{5 \pm \sqrt{5}}{2}}$ pour une choix particulière de signes, parce que $\beta = \frac{5 \pm \sqrt{5}}{2}$ sont les racines de $y^2 - 5y + 5$. Prenons donc $K = \mathbb{Q}(\sqrt{5})$ et il est clair que $\beta \in K$. On a $[K : \mathbb{Q}] = 2$ parce que $y^2 - 5$ est irréductible par Eisenstein $p = 5$. Alors, $[\mathbb{Q}(\alpha) : K] = 2$.

(c) On a trouvé que α peut être inclut dans une tour

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\alpha)$$

dont chaque degré est 2. Donc α est constructible. (On peut argumenter plus spécifiquement en disant que $\sqrt{5}$ est constructible, donc $\frac{5\pm\sqrt{5}}{2}$ est constructible, donc α est constructible.)

3. (6 points) (a) Faites une liste des polynômes irréductibles sur $\mathbb{F}_2[x]$ de degré ≤ 2.

   (b) Soit $p(x) = x^4 + 17x + 3$. Est-ce que $p(x)$ est irréductible

   (1) sur $\mathbb{F}_2$? (2) sur $\mathbb{Q}$?

Solution: (a) Les polynômes irréductibles sur $\mathbb{F}_2[x]$ de degré ≤ 2 sont ceux qui divisent $x^{2^2} - x$,

$$x^4 + x = x(x+1)(x^2+x+1).$$

$x^2 + x + 1$ est irréductible parce qu'il n'a pas de racines. Les autres sont x, $x+1$ et 1. (b) (1) $p(x)$ n'a aucune racine sur $\mathbb{F}_2$, alors, s'il est réductible, il doit être produit des polynômes irréductibles de degré 2. Alors, la seule possibilité est

$$(x^2+x+1)^2 = x^4 + x^2 + 1,$$

qui est différent de $p(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Alors, $p(x) \in \mathbb{F}_2[x]$ irréductible.

(2) Comme $p(x)$ est irréductible sur $\mathbb{F}_2[x]$, et que ses coefficients son entiers, on trouve qu'il est irréductible sur $\mathbb{Z}[x]$ et par consequent, sur $\mathbb{Q}[x]$

4. (6 points) Pour chacun des polynômes suivants, déterminez le nombre de racines sur $\mathbb{F}_{81}$.

   (a) $x^{80} - 1$

   (b) $x^{81} - 1$

   (c) $x^9 - x^3 + 1$

Solution: Notons que $81 = 3^4$. (a) Les éléments de $\mathbb{F}_{81}$ sont les racines de $x^{81} - x$. Alors, toutes les racines de $x^{80} - 1$ sont dans $\mathbb{F}_{81}$. En plus, le polynome est séparable, donc, les racines sont toutes différentes et il y a 80 racines.

(b) Comme la caractéristique est 3, $x^{81} - 1 = (x-1)^{81}$. Ce polynôme a donc une racine, et elle appartient à $\mathbb{F}_{81}$.

(c) $x^9 - x^3 + 1 = (x^3 - x + 1)^3$. Le polynôme $x^3 - x + 1$ est irréductible sur $\mathbb{F}_3$ parce qu'il n'a pas de racines. Mais $[\mathbb{F}_{81} : \mathbb{F}_3] = 4$, alors il n'y a pas de racines sur $\mathbb{F}_{3^4}$, car $3 \nmid 4$.

5. (6 points) Factorisez $\Phi_7(x^4) \in \mathbb{Q}[x]$ en des polynômes irréductibles. Piste: Quelles sont les racines ?

Solution: Les racines de $\Phi_7(x)$ sont ξ_7^k avec $k = 1, 2, 3, 4, 5, 6$. On a que ξ_{28} est racine de $\Phi_7(x^4)$.

On a que $\deg \Phi_7(x) = \varphi(7) = 6$ et donc $\deg \Phi_7(x^4) = 24$

En plus, ξ_{28}^k est racine de $\Phi_7(x^4)$ ssi ξ_{28}^{4k} est racine 7-ième primitive. En écrivant $\xi_{28} = e^{2\pi i/28}$, on a

$$(e^{2\pi i/28})^{4k} = e^{2\pi ik/7}$$

qui est racine primitive ssi $0 \leq k \leq 27$ et $7 \not| k$. Cela donne que ξ_{28}^2 et ξ_{28}^4 sont aussi racines. Comme elles sont racines primitives d'ordre 14 et 7, on a

$$\Phi_{28}(x), \Phi_{14}(x), \Phi_7(x) | \Phi_7(x^4)$$

Les polynômes $\Phi_n(x)$ et $\Phi_m(x)$ sont toujours copremiers pour $n \neq m$, car une racine de l'unité ne peut pas être racine primitive d'ordre n et d'ordre m à la fois.

En vérifiant leur degrés, on trouve $\varphi(28) = 2 \cdot 6 = 12$, $\varphi(14) = 6$ et $\varphi(7) = 6$. Comme $12 + 6 + 6 = 24$, cela donne tous les facteurs et

$$\Phi_7(x^4) = \Phi_{28}(x)\Phi_{14}(x)\Phi_7(x).$$