Département de mathématiques et de statistique
Université de Montréal
Théorie de Galois. Mat 3661. Examen Intra
Le 25 février 2019. 13h30-15h20
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.

Quelques formules trigonométriques.

$$\cos(2\theta) = 2\cos(\theta)^2 - 1 \tag{1}$$
$$\cos(3\theta) = 4\cos(\theta)^3 - 3\cos(\theta) \tag{2}$$
$$\cos(5\theta) = 16\cos(\theta)^5 - 20\cos(\theta)^3 + 5\cos(\theta) \tag{3}$$

1. (6 points) Soit K/F une extension de corps et soit $\gamma \in K$ tel que $\deg m_{\gamma,F}(x) = 9$. Soit $h(x) \in F[x]$ tel que $\deg h(x) = 2$. Prouvez que $\deg m_{h(\gamma),F}(x) = 9$.

Solution: On a $F(h(\gamma)) \subseteq F(\gamma)$ et $[F(\gamma) : F] = 9$. Comme $\deg h(x) = 2$, on a que $[F(\gamma) : F(h(\gamma))] = 1$ ou 2 (parce que γ est racine de $h(x) - h(\gamma) \in F(h(\gamma))[x]$ qui est un polynôme de degré 2) et $[F(\gamma) : F(h(\gamma))] \mid [F(\gamma) : F] = 9$. Par conséquent $[F(\gamma) : F(h(\gamma))] = 1$ et $[F(h(\gamma)) : F] = 9$. Cela implique que $\deg m_{h(\gamma),F}(x) = 9$.

2. (6 points) Trouvez les corps de décomposition de $(x^4 - 3)(x^2 + x + 1)$ sur $\mathbb{Q}$ et donnez son degré. Justifiez bien votre réponse.

Solution: Les racines de ce polynôme sont $\sqrt[4]{3}i^k$ avec $k = 0, 1, 2, 3$ et ξ_3^j avec $\xi_3 = \frac{-1+\sqrt{3}i}{2}$. Alors, $K = \mathbb{Q}(\sqrt[4]{3}, i)$ contient les racines de $x^4 - 3$ mais aussi celles du polynôme cyclotomique $\Phi_3(x) = x^2 + x + 1$. On écrit

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}]$$

On sait que $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$ ($x^4 - 3$ irréductible par Eisenstein avec $p = 3$). Aussi, on sait que le polynôme minimal de i sur $\mathbb{Q}$ est $\Phi_4(x) = x^2 + 1$. De plus, $i \notin \mathbb{Q}(\sqrt[4]{3}) \subset \mathbb{R}$. Alors, $[K : \mathbb{Q}(\sqrt[4]{3})] = 2$ et $[K : \mathbb{Q}] = 8$.

3. (6 points) (a) Trouvez le polynôme minimal de $\alpha = 4\cos\left(\frac{\pi}{9}\right)^2$ sur $\mathbb{Q}$.

   Vous pouvez vous servir des formules de la première page.

   (b) Est-il possible de construire α avec une règle non-graduée et un compas ? Justifiez bien.

Solution: (a) Soit $\beta = \cos\left(\frac{2\pi}{9}\right)$. Par l'équation (1),

$$\beta = \frac{\alpha}{2} - 1$$

et par l'équation (2),

$$-\frac{1}{2} = \cos\left(\frac{2\pi}{3}\right) = 4\beta^3 - 3\beta = 4\left(\frac{\alpha}{2} - 1\right)^3 - 3\left(\frac{\alpha}{2} - 1\right) = \frac{\alpha^3}{2} - 3\alpha^2 + \frac{9}{2}\alpha - 1$$

En multipliant par 2, α est racine de

$$x^3 - 6x^2 + 9x - 1.$$

Le polynôme est irréductible sur $\mathbb{Q}$ parce que si on fait $x = y+1$ on obtient y^3-3y^2+3 qui est irréductible par le critère d'Eisenstein avec $p = 3$.

Autre forme: par le critère de la racine, le polynôme est irréductible parce que les seules racines possibles sont ± 1 et $1^3 - 6 \cdot 1^2 + 9 \cdot 1 - 1 = 3 \neq 0$, et $(-1)^3 - 6 \cdot (-1)^2 + 9 \cdot (-1) - 1 = -17 \neq 0$

On a donc

$$m_{\alpha,\mathbb{Q}}(x) = x^3 - 6x^2 + 9x - 1.$$

(b) α n'est pas constructible parce qu'il a degré 3 sur $\mathbb{Q}$ et 3 ne divise pas les puissances de 2.

4. (6 points) Dans cette question, on fixe une clôture algébrique $\overline{\mathbb{F}_2}$ de $\mathbb{F}_2$ et on travaille toujours à l'intérieur de cette clôture.

   (a) Combien y a-t-il d'éléments $\alpha \in \mathbb{F}_{2^{12}}$ tels que $\mathbb{F}_{2^{12}} = \mathbb{F}_2(\alpha)$?

   Piste : $\mathbb{F}_{2^{12}} = \mathbb{F}_2(\alpha)$ ssi α n'est pas un élément d'une subextension propre.

   (b) Trouvez un polynôme irréductible $g(x) \in \mathbb{F}_4[x]$ tel que $\mathbb{F}_{16} = \mathbb{F}_4[x]/(g(x))$.

   Vous pouvez répresenter les éléments de $\mathbb{F}_4$ comme $\{0, 1, \beta, \beta + 1\}$ avec β racine de $x^2 + x + 1 \in \mathbb{F}_2[x]$.

Solution: (a) Rappelons que $\mathbb{F}_{2^d} \subseteq \mathbb{F}_{2^{12}}$ ssi $d \mid 12$. Les possibilités sont $d = 1, 2, 3, 4, 6, 12$. Il faut donc s'assurer que $\alpha \notin \mathbb{F}_{2^4} \cup \mathbb{F}_{2^6}$ (parce que les autres subextensions sont contenues dans ces deux). Notons que $\mathbb{F}_{2^4} \cap \mathbb{F}_{2^6} = \mathbb{F}_{2^2}$. Alors, il faut exclure

$$|\mathbb{F}_{2^4} \cup \mathbb{F}_{2^6}| = |\mathbb{F}_{2^4}| + |\mathbb{F}_{2^6}| - |\mathbb{F}_{2^2}| = 16 + 64 - 4 = 76 \text{ possibilités.}$$

On a donc $2^{12} - 76 = 4020$ possibilités pour α.

(b) Il suffit de trouver un polynôme irréductible de degré 2 sur $\mathbb{F}_4$. Soit $P(x) = x^2 + ax + b$ un tel polynôme. On veut que $0, 1, \beta, \beta + 1$ no soient pas des racines. On a

$$P(0) = b,\ P(1) = 1 + a + b,\ P(\beta) = \beta^2 + a\beta + b = (a + 1)\beta + (b + 1),$$

$$P(\beta + 1) = \beta^2 + 1 + a\beta + a + b = (a + 1)\beta + a + b.$$

On peut prendre, par exemple $a = \beta$ et $b = 1$.

En fait, il y a 6 solutions possibles: $x^2 + \beta x + 1$, $x^2 + x + \beta$, $x^2 + (\beta + 1)x + 1$, $x^2 + x + \beta + 1$, $x^2 + \beta x + \beta$, $x^2 + (\beta + 1)x + (\beta + 1)$.

5. (6 points) Soit p premier. Considérons $\Phi_p(x) = x^{p-1} + \cdots + x + 1$. Nous avons prouvé en classe que $\Phi_p(x)$ est irréductible sur $\mathbb{Q}$ (vous pouvez vous servir de ce fait sans le reprouver).

(a) Prouvez que $\Phi_p(x)$ est irréductible sur $\mathbb{Q}(\sqrt[p]{3})$.

Piste: Pensez au corps de décomposition de $x^p - 3$ sur $\mathbb{Q}$.

(b) Donnez la factorisation de $\Phi_p(x)$ sur $\mathbb{F}_p$.

Considérons $\Phi_{24}(x) = x^8 - x^4 + 1$.

(c) Donnez la factorisation de $\Phi_{24}(x)$ sur $\mathbb{F}_2$. Quels sont $\deg_s \Phi_{24}(x)$ et $\deg_i \Phi_{24}(x)$ sur $\mathbb{F}_2$?

(d) Donnez le plus petit $k \in \mathbb{Z}_{>0}$ tel que $\Phi_{24}(x)$ se décompose en des facteurs linéaires sur $\mathbb{F}_{2^k}$.

Solution: (a) Le corps de décomposition de $x^p - 3$ est $\mathbb{Q}(\sqrt[p]{3}, \xi_p)$, ou $\xi_p = e^{2\pi i/p}$. On a que $[\mathbb{Q}(\sqrt[p]{3}) : \mathbb{Q}] = p$ parce que $x^p - 3$ est irréductible sur $\mathbb{Q}$ par Eisenstein avec premier 3 et $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$ parce que $\Phi_p(x)$ est irréductible sur $\mathbb{Q}$. On a alors que $[\mathbb{Q}(\sqrt[p]{3}, \xi_p) : \mathbb{Q}] = p(p-1)$ parce qu'il est divisible par p et par $p-1$. Alors $[\mathbb{Q}(\sqrt[p]{3}, \xi_p) : \mathbb{Q}(\sqrt[p]{3})] = p - 1$ et $\Phi_p(x)$ doit être irréductible sur $\mathbb{Q}(\sqrt[p]{3})$.

(b) $\Phi_p(x) = \frac{x^p-1}{x-1} = \frac{(x-1)^p}{x-1} = (x-1)^{p-1}$.

(c) On a $x^8 - x^4 + 1 = x^8 + x^4 + 1 = (x^2 + x + 1)^4$. On peut écrire $\Phi_{24}(x) = \Phi_{24sep}(x^4)$, où $\Phi_{24sep}(x) = x^2 + x + 1$. Cela donne $\deg_s \Phi_{24}(x) = 2$ et $\deg_i \Phi_{24}(x) = 4$.

(d) La plus petite extension où $x^2 + x + 1$ se factorise doit avoir degré 2 sur $\mathbb{F}_2$, alors, elle est $\mathbb{F}_{2^2}$ et $k = 2$.