Département de mathématiques et de statistique
Université de Montréal
Théorie de Galois. Mat 3661. Examen Final
Le 26 avril 2017. 9h30-12h20
Professeure: Matilde N. Lalín

1. Aucun document ni autres instruments ne sont autorisés.
2. Une calculatrice simple est permise.
3. Les téléphones cellulaires doivent être éteints.
4. Lisez attentivement les questions avant de commencer à travailler.
5. **Justifiez tous vos raisonnements.**
6. Continuez sur le verso de la feuille si vous avez besoin de plus d'espace.
7. Répondez à toutes les questions dans les cahiers d'examen.
8. Évitez de déchirer les cahiers d'examen.
9. Le total des points de cet examen vaut 30. (Il y a 6 points additionnels.)

Quelques formules:

$$\begin{aligned}
D(x^3+px+q) &= -4p^3-27q^2\\
D(x^4+px^2+qx+r) &= 16p^4r-4p^3q^2-128p^2r^2+144pq^2r-27q^4+256r^3\\
\text{résolvente pour le degré 4 : } h(x) &= x^3-2px^2+(p^2-4r)x+q^2\\
D(x^n+px+q) &= (-1)^{n(n-1)/2}((1-n)^{n-1}p^n+n^nq^{n-1})
\end{aligned}$$

Dans cet examen, ≪ caractériser un groupe G ≫ veut dire ≪ donner le groupe abstrait auquel G est isomorphe ≫.

1. (6 points) Caractérisez le groupe de Galois de $x^3 - 2$

   (a) sur $\mathbb{Q}$,

   (b) sur $\mathbb{Q}(\sqrt{-3})$,

   (c) sur $\mathbb{F}_3$.

Solution: (a) Comme le polynôme est irréductible (Eisenstein $p = 2$) et le discriminant est -108 qui n'est pas de carré sur $\mathbb{Q}$ parce qu'il est < 0, le groupe de Galois est $\mathbb{S}_3$.

(b) Le corps de décomposition sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ qui a degré 3 sur $\mathbb{Q}(\sqrt{-3})$. Alors le groupe de Galois est $\mathbb{Z}/3\mathbb{Z}$.

(c) Sur $\mathbb{F}_3$, on a $x^3 - 2 = x^3 + 1 = (x + 1)^3$. Le groupe de Galois est donc le groupe trivial.

2. (6 points) Soit $f(x) \in \mathbb{Q}[x]$ un polynôme irréductible de degré 4. Soit $h(x)$ la résolvente cubique de $f(x)$. Caractérisez $\mathrm{Gal}(f(x))$ si

   (a) $h(x) = x^3 - 3x + 1$,

   (b) $h(x) = x^3 + 3x + 1$,

   (c) $h(x) = x^3 + 2x + 3$.

Solution: (a) Comme $h(1) = -1$ et $h(-1) = 2$, $h(x)$ est irréductible, parce qu'il n'a pas de racine. On a que $D(f(x)) = D(h(x)) = 81$, un carré en $\mathbb{Q}$, alors, $\mathrm{Gal}(f(x)) \cong \mathbb{A}_4$.

(b) Comme $h(1) = 5$ et $h(-1) = -3$, $h(x)$ est irréductible, parce qu'il n'a pas de racine. On a que $D(f(x)) = D(h(x)) = -135$, non-carré en $\mathbb{Q}$, alors, $\mathrm{Gal}(f(x)) \cong \mathbb{S}_4$.

(c) On a $h(x) = (x+1)(x^2 - x + 3)$ et $x^2 - x + 3$ est irréductible car sont discriminant est -11. Alors, $\mathrm{Gal}(f(x)) = D_8$ ou C_4. Mais $D(f(x)) = D(h(x)) = -275 < 0$. Alors $\mathrm{Gal}(f(x)) = D_8$.

3. (6 points) Soit $\zeta_{37} = e^{2\pi i/37}$ et soit $\alpha = \zeta_{37} + \zeta_{37}^{10} + \zeta_{37}^{26}$. Soit $H \leq \mathrm{Gal}(\mathbb{Q}(\zeta_{37})/\mathbb{Q})$ tel que $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_{37})^H$. Trouvez H et donnez $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Solution: Les automorphismes de $\mathbb{Q}(\zeta_{37})/\mathbb{Q}$ sont de la forme $\sigma_a : \zeta_{37} \to \zeta_{37}^a$ avec $\text{pgcd}(a, 37) = 1$. On cherche $\sigma_a(\alpha) = \alpha$, c'est-à-dire, $\zeta_{37} + \zeta_{37}^{10} + \zeta_{37}^{26} = \zeta_{37}^a + \zeta_{37}^{10a} + \zeta_{37}^{26a}$. If faut donc $a = 1, 10, 26$. Notons que $10 \cdot 10 \equiv 26 \pmod{37}$ et $10 \cdot 26 \equiv 1 \pmod{37}$, alors $a = 10$ fonctionne. Aussi $26 \cdot 10 \equiv 1 \pmod{37}$ et $26 \cdot 26 \equiv 10 \pmod{37}$, alors $a = 26$ fonctionne. On a donc

$$H = \{\sigma_1, \sigma_{10}, \sigma_{26}\} \cong \mathbb{Z}/3\mathbb{Z},$$

et

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\text{Gal}(\mathbb{Q}(\zeta_{37})/\mathbb{Q}) : H] = \frac{36}{3} = 12.$$

4. (6 points) (a) Décrivez explicitement les automorphismes et caractérisez le groupe de Galois de $f(x) = (x^2 - 2)(x^3 - 3) \in \mathbb{Q}[x]$.

   (b) Faites une liste de tous les sous-corps du corps de décomposition K qui contiennent $\mathbb{Q}(\zeta_3)$ et écrivez-les comme K^H avec $H \leq \text{Gal}(f(x))$. (La liste suffit, il ne faut pas justifier plus.)

   (c) Donnez (avec justification) une tour d'extensions

$$K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_n = K$$

   où K est le corps de décomposition de $f(x)$ sur $\mathbb{Q}$ et K_i/K_{i-1} est une extension cyclique pour $i = 1, \ldots, n$.

Solution: (a) $x^2 - 2$ et $x^3 - 3$ sont des polynômes irréductibles (Eisenstein $p = 2, 3$). Le corps de décomposition de $x^2 - 2$ est $K_1 = \mathbb{Q}(\sqrt{2})$ et ce de $x^3 - 3$ est $K_2 = \mathbb{Q}(\sqrt[3]{3}, \zeta_3)$, où $\zeta_3 = e^{2\pi i/3}$. On a $K = K_1 \cdot K_2 = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \zeta_3)$. Notons que $[K_2 : \mathbb{Q}] = 6$ parce que $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{R}$ et ζ_3 racine de $\Phi_3(x) = x^2 + x + 1$.

De plus, $K_1 \cap K_2 = \mathbb{Q}$. Sinon, on a que $\sqrt{2} \in K_2$. Comme $\zeta_3 \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, alors $[\mathbb{Q}(\zeta_3, \sqrt{2}) : \mathbb{Q}] = 4$. On a donc $4 \mid [K_2 : \mathbb{Q}] = 6$, contradiction. Par conséquent $\text{Gal}(K/\mathbb{Q}) \cong \text{Gal}(K_1/\mathbb{Q}) \times \text{Gal}(K_2/\mathbb{Q})$.

On a que $\text{Gal}(K_1/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, avec l'automorphisme non-trivial donné par $\tau : \sqrt{2} \to -\sqrt{2}$.

Comme $\text{Disc}(x^3 - 3) = -243 < 0$, $\text{Gal}(K_2/\mathbb{Q}) \cong \mathbb{S}_3$ est engendré par

$$\rho : \begin{array}{ccc} \sqrt[3]{3} & \to & \sqrt[3]{3}\zeta_3 \\ \zeta_3 & \to & \zeta_3 \end{array} \qquad \sigma : \begin{array}{ccc} \sqrt[3]{3} & \to & \sqrt[3]{3} \\ \zeta_3 & \to & \zeta_3^2 \end{array}$$

où ρ a ordre 3, σ a ordre 2, et $\sigma\rho = \rho^{-1}\sigma$.

On a donc $\text{Gal}(K/\mathbb{Q}) = \langle(\tau, \sigma), (\tau, \rho)\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{S}_3$.

(b) On cherche les sous-groupes de $\mathrm{Gal}(K/\mathbb{Q})$ qui ne contiennent pas σ. On a $K = K^{\{1\}}$, $\mathbb{Q}(\zeta_3) = K^{H_1}$ avec $H_1 = \langle (1,\rho), (\tau, 1)\rangle$, $\mathbb{Q}(\zeta_3, \sqrt[3]{3}) = K_2 = K^{H_2}$ avec $H_2 = \langle (\tau, 1)\rangle$, $\mathbb{Q}(\sqrt{2}, \zeta_3) = K^{H_3}$ $H_3 = \langle (1,\rho)\rangle$.

(c)

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_3, \sqrt[3]{3}) \subset \mathbb{Q}(\zeta_3, \sqrt[3]{3}, \sqrt{2})$$

où l'extension $\mathbb{Q}(\zeta_3, \sqrt[3]{3})/\mathbb{Q}(\zeta_3)$ est cyclique par la théorie de Kummer et les autres sont cycliques parce qu'elles ont degré 2.

5. (6 points) Soit $f(x) \in \mathbb{Q}[x]$ irréductible. Montrez que si $f(x)$ a des racines réelles et complexes, son groupe de Galois n'est pas abélien. (Pistes: Considérez la conjugaison complexe.)

Solution: Soient $\alpha \in \mathbb{R}$, $\beta \in \mathbb{C} \setminus \mathbb{R}$ racines de $f(x)$. Comme $f(x)$ a des coefficients réels, $\bar{\beta}$ est aussi racine. Soit τ la conjugaison complexe et σ un automorphisme tel que $\sigma(\alpha) = \beta$. Alors, $\sigma \circ \tau(\alpha) = \sigma(\alpha) = \beta$ pendant que $\tau \circ \sigma(\alpha) = \tau(\beta) = \bar{\beta}$. Donc $\sigma \circ \tau \neq \tau \circ \sigma$.

6. (6 points) Caractérisez le groupe de Galois de $f(x) = x^5 + 6x^3 + 15x^2 + 3x + 30 \in \mathbb{Q}[x]$. Vous pouvez vous servir sans preuve du fait que $\mathrm{Disc}(f) = 3^4 \cdot 457 \cdot 73421$ (factorisation en des nombres premiers).

Solution: Par Eisenstein avec $p = 3$, le polynôme est irréductible et $\mathrm{Gal}(f)$ est un sous-groupe transitif de $\mathbb{S}_5$. On factorise modulo 2 et 5.

$$f(x) \equiv x^5 + x^2 + x \equiv x(x^4 + x + 1) \pmod 2$$
$$f(x) \equiv x^5 + x^3 + 3x \equiv x(x-1)(x+1)(x^2+2) \pmod 5$$

Notons que $x^4 + x + 1$ est irréductible sur $\mathbb{F}_2$ parce qu'il et copremier avec $x^4 - x = x^4 + x$ qui est le produit de tous les polynômes irréductibles de degré 1 et 2 sur $\mathbb{F}_2$.

$x^2 + 2$ est irréductible sur $\mathbb{F}_5$ parce qu'il n'a pas de racine, car $\left(\frac{-2}{5}\right) = -1$.

Alors, $\mathrm{Gal}(f)$ a un 4-cycle et un 2-cycle. En conséquent, $\mathrm{Gal}(f) \cong \mathbb{S}_5$.

Une autre forme : comme le polynôme est irréductible de degré 5, on peut conclure qu'il y a un 5-cycle parce que 5 est premier et divise $|\mathrm{Gal}(f)|$. En combinant cela avec la factorisation modulo 5, on a un 5-cycle et un 2-cycle ce qui donne $\mathrm{Gal}(f) \cong \mathbb{S}_5$.