Département de mathématiques et de statistique
Université de Montréal
Théorie de Galois. Mat 3661. Examen Final
Le 20 avril 2011
Professeure: Matilde N. Lalín

NOM:

CPER:

1. Aucune documentation permise.
2. Les téléphones cellulaires doivent être éteints. Les portables ne sont pas permis.
3. Ne pas oublier d'écrire vos nom et CPER sur cette feuille.
4. Lire attentivement les questions avant de commencer à travailler.
5. **Justifier tous vos raisonnements.**
6. Continuer sur le verso de la feuille si vous avez besoin de plus d'espace.
7. Répondre à toutes les questions.
8. Le total des points de cet examen vaut 50.

Quelques formules:

$$D(x^3 + px + q) = -4p^3 - 27q^2$$

$$D(x^4 + qx + r) = -27q^4 + 256r^3, \text{ résolvente: } h(x) = -4rx + q^2$$

Question:	1	2	3	4	5	Total
Points:	10	10	10	10	10	50
Score:						

1. (10 points) Caractériser le groupe de Galois de $x^3 - 10$
   (a) sur $\mathbb{Q}$.
   (b) sur $\mathbb{Q}(\sqrt{2})$.
   (c) sur $\mathbb{Q}(\sqrt{-3})$.

Solution: (a) Comme le polynôme est irréductible (Eisenstein $p = 2$) et le discriminant est -2700 qui n'est pas de carré sur $\mathbb{Q}$ parce qu'il est < 0, le groupe de Galois est $\mathbb{S}_3$.

(b) Par le point (a), le corps de décomposition sur $\mathbb{Q}$ qui est $\mathbb{Q}(\sqrt[3]{10}, \sqrt{-3})$ a degré 6 sur $\mathbb{Q}$. Notons que $\sqrt{-3} \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, alors $[\mathbb{Q}(\sqrt{-3}, \sqrt{2}) : \mathbb{Q}] = 4$. Comme $[\mathbb{Q}(\sqrt[3]{10}) : \mathbb{Q}] = 3$, on a $[\mathbb{Q}(\sqrt{-3}, \sqrt{2}, \sqrt[3]{10}) : \mathbb{Q}] = 12$ (car $(3, 4) = 1$) et ça veut dire que $[\mathbb{Q}(\sqrt{-3}, \sqrt{2}, \sqrt[3]{10}) : \mathbb{Q}(\sqrt{2})] = 6$ et le groupe de Galois est aussi $\mathbb{S}_3$.

(c) $-2700 = (10\sqrt{-3})^2$, carré sur $\mathbb{Q}(\sqrt{-3})$ alors le groupe de Galois est $\mathbb{Z}/3\mathbb{Z}$.

2. (10 points) Étant donné que $x^4 - 2$ et que $x^2 - 3$ sont irréductibles sur $\mathbb{Q}(i)$, caractériser le groupe de Galois de $f(x) = (x^4 - 2)(x^2 - 3)$ sur $\mathbb{Q}(i)$. Faire une liste (il ne faut pas justifier la liste) de toutes les sous-extensions du corps de décomposition de $f(x)$ sur $\mathbb{Q}(i)$ et donner leur degré.

Solution: Comme les racines de $g(x) = x^4 - 2$ sont $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$, le corps de décomposition de $g(x)$ sur $F = \mathbb{Q}(i)$ est $K_1 = F(\sqrt[4]{2})$ et son groupe de Galois est $\mathbb{Z}/4\mathbb{Z}$. De même, le corps de décomposition de $h(x) = x^2 - 3$ sur F est $K_2 = F(\sqrt{3})$ et son groupe de Galois est $\mathbb{Z}/2\mathbb{Z}$. On a que le corps de décomposition de $f(x)$ sur F est $K_1K_2 = F(\sqrt[4]{2}, \sqrt{3})$. Comme $\mathrm{Gal}(K_1/F)$ a une seule sous-extension de degré 2, elle doit être $F(\sqrt{2})$. Il est clair que $\sqrt{3} \notin F(\sqrt{2})$ alors $K_1 \cap K_2 = F$ et $[K_1K_2 : F] = 8$. On a que $\mathrm{Gal}(K_1K_2/F) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Les sous-extensions se correpondent aux sous-groupes du groupe de Galois. Alors, on a:

- degré 1: $\mathbb{Q}(i)(= K^{<(1,0),(0,1)>})$.
- degré 2: $\mathbb{Q}(i, \sqrt{2})(= K^{<(2,0),(0,1)>})$, $\mathbb{Q}(i, \sqrt{3})(= K^{<(1,0)>})$, $\mathbb{Q}(i, \sqrt{6})(= K^{<(1,1)>})$.
- degré 4: $\mathbb{Q}(i, \sqrt{2}, \sqrt{3})(= K^{<(2,0)>})$, $\mathbb{Q}(i, \sqrt[4]{2})(= K^{<(0,1)>})$, $\mathbb{Q}(i, \sqrt[4]{2}\sqrt{3})(= K^{<(2,1)>})$.
- degré 8: $\mathbb{Q}(i, \sqrt[4]{2}, \sqrt{3})(= K^{\{(0,0)\}})$.

3. (10 points) Soit $f(x) \in \mathbb{Q}[x]$ irréductible. Montrer que si $f(x)$ a des racines réelles et complexes, son groupe de Galois n'est pas abélien. (Pistes: Considérer 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 $\sigma \circ \tau \neq \tau \circ \sigma$.

4. (10 points) Soit $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$.

(a) Prouver que $f(x)$ est irréductible.

(b) Prouver que $f(x)$ a exactement 3 racines réelles.

(c) Prouver que si on pense à $\mathrm{Gal}_{\mathbb{Q}}(f(x)) \subset \mathbb{S}_5$, $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ contient une transposition et un 5-cycle. (Ça veut dire que $\mathrm{Gal}_{\mathbb{Q}}(f(x)) \simeq \mathbb{S}_5$).

Solution: (a) Par le critére d'Einsenstein avec $p = 2$, $f(x)$ est irréductible.

(b) $f(-2) = -22$, $f(0) = 2$, $f(1) = -1$, $f(2) = 18$. Alors, par le Théorème des valeurs intermédiaires, on trouve au moins 3 zeros sur $\mathbb{R}$. Comme la derivée est $f'(x) = 5x^4 - 4$ qui a seulement 2 racines réelles, on conclue qu'il n'y a pas de plus racines réelles. Une autre façon de concluire la même chose est en utilisant la régle de signes de Descartes.

(c) Comme le polynôme est irréductible, $5 | [K : \mathbb{Q}] = |\mathrm{Gal}_{\mathbb{Q}}(f(x))|$, alors il y a un 5-cycle sur $\mathrm{Gal}_{\mathbb{Q}}(f(x))$. Comme il y a un pair de racines complexes conjugées, la conjugaison est une transposition de $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ parce qu'elle permute les deux racines complexes et fixe les trois racines réelles . Puisque un 5-cycle et une transposition engendrent le groupe $\mathbb{S}_5$, on trouve que $\mathrm{Gal}_{\mathbb{Q}}(f(x)) \simeq \mathbb{S}_5$.

5. (10 points) Soit F un corps de caractéristique différente de 2 et 3. Soient $f(x), g(x) = x^2 - c$ des polynômes irréductibles sur F, de degré 3 et 2 respectivement, et D le discriminant de f. On suppose que

$$[F(\sqrt{D}) : F] = 2, \quad \text{et} \quad F(\sqrt{D}) \neq F(\sqrt{c}).$$

Montrer que le corps de décomposition de fg sur F est de degré 12.

Solution: Soient K_f, K_g les corps de décomposition de f, g. Comme $\sqrt{D} \notin F$, on a que $[K_f : F] = 6$. Comme g irréductible, $[K_g : F] = 2$. Voyons que $K_f \cap K_g = F$. Comme $K_f \cap K_g \subset K_g$ qui a degré 2 sur F, les seules possibilitées sont $K_f \cap K_g = F$ ou K_g. Si $K_f \cap K_g = K_g$, on a que $\sqrt{c} \in K_f$. Mais $\sqrt{c} \notin F(\sqrt{D})$ et $F(\sqrt{D}) \subset K_f$. Alors $[F(\sqrt{D}, \sqrt{c}) : F] = 4$ et $F(\sqrt{D}, \sqrt{c}) \subset K_f$ et ça veut dire que $4 | [K_f : F]$. Mais $[K_f : F] = 6$, contradiction. Alors $K_f \cap K_g = F$ et $[K_f K_g : F] = [K_f : F][K_g : F] = 12$.