Département de mathématiques et de statistique
Université de Montréal
Théorie de Galois. Mat 3661. Examen Intra
Le 23 février 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 30 (il y a 3 points aditionels).

Question:	1	2	3	4	5	6	Total
Points:	5	6	5	5	5	7	33
Score:							

1. (5 points) (a) Faire une liste des polynômes irréductibles sur $\mathbb{F}_2[x]$ de degré ≤ 2.

(b) Soit $p(x) = x^4 + 15x^3 + 7$. 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 $x^{2^2} - x$,

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

(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 different de $p(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. 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 quíl est irréductible sur $\mathbb{Z}[x]$ et par consequent, sur $\mathbb{Q}[x]$

2. (6 points) Trouver les corps de décomposition K des polynômes suivants sur $\mathbb{Q}$ et donner leurs degrés. Justifier vos réponses.

   (a) $p(x) = x^6 - 8$.

   (b) $p(x) = x^6 - 32$.

Solution: (a) 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 $x^2 + 3$ (irréductible par Einsestein) et $\sqrt{3}i \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$.

(b) Dans ce cas-là, on trouve que les racines sont $\sqrt[6]{32}\xi_6^k$ avec $k = 0, 1, \ldots, 5$. Alors, $K = \mathbb{Q}(\sqrt[6]{32}, \xi_6)$. On note que $\sqrt[6]{2} = \frac{2}{\sqrt[6]{32}}$, alors, $K = \mathbb{Q}(\sqrt[6]{2}, \xi_6) = \mathbb{Q}(\sqrt[6]{2}, \sqrt{3}i)$. On continue comme dans le point (a). La seule difference est que $\sqrt[6]{2}$ est racine de $x^6 - 2$ (irréductible par Einsestein). Alors, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 2 \cdot 6 = 12$.

3. (5 points) Soit $p(x) = x^5 + x^4 + 1 \in \mathbb{F}_2[x]$.

(a) Trouver la factorisation de $p(x)$ en facteurs premiers.

(b) Décrire le corps de décomposition de $p(x)$ sur $\mathbb{F}_2[x]$ comme $\mathbb{F}_{2^d}$ (trouver le d).

Solution: (a) Comme $p(x)$ n'a pas de racines sur $\mathbb{F}_2$, le seule possibilité, s'il n'est pas irréductible, est qu'il soit produit d'un polynôme irréductible de degré 2 et un polynôme irréductible de degré 3. On a vu dans le problème 1, qu'il n'y a qu'un polynôme irréductible de degré 2. De plus, les coefficients independants des facteurs doivent être 1. Alors,

$$x^5+x^4+1 = (x^3+ax^2+bx+1)(x^2+x+1) = x^5+(a+1)x^4+(b+a+1)x^3+(1+b+a)x^2+(1+b)x+1.$$

On trouve $a = 0$ et $b = 1$. Alors,

$$x^5 + x^4 + 1 = (x^3 + x + 1)(x^2 + x + 1)$$

(b) Le corps de décomposition de x^3+x+1 est $\mathbb{F}_{2^3}$ (parce qu'il y a une seule extension de degré 3 et chaque racine d'un polynôme irréductible de degré 3 doit se trouver sur une extension de degré 3, alors, toutes les racines se trouvent sur la même extension). Le corps de décomposition de $x^2 + x + 1$ est $\mathbb{F}_{2^2}$ (Même idée). Alors, le corps de décomposition K de $p(x)$ est le corps composé de $\mathbb{F}_{2^3}$ et $\mathbb{F}_{2^2}$. On a, d'un coté,

$$[K : \mathbb{F}_2] \leq [F_{2^2} : \mathbb{F}_2][\mathbb{F}_{2^3} : \mathbb{F}_2] = 6$$

et dún autre coté,

$$[\mathbb{F}_{2^2} : \mathbb{F}_2], [\mathbb{F}_{2^3} : \mathbb{F}_2] | [K : \mathbb{F}_2] \Rightarrow 2, 3 | [K : \mathbb{F}_2]$$

alors, $[K : \mathbb{F}_2] = 6$ et $K = \mathbb{F}_{2^6}$.

4. (5 points) Soit $K = F(\alpha)$ pour α algébrique sur F, de degré impair. Montrer que $K = F(\alpha^2)$.

Solution: On a toujours que $F(\alpha^2) \subset F(\alpha)$, et α racine de $x^2 - \alpha^2 \in \mathbb{F}(\alpha^2)[x]$. Alors, $[F(\alpha) : F(\alpha^2)] \leq 2$. Noter aussi que $[F(\alpha^2) : F] | [F(\alpha) : F]$ qui est impair, alors, $[F(\alpha^2) : F]$ doit être impair. Par conséquent, $[F(\alpha) : F(\alpha^2)] = 1$ et $F(\alpha) = F(\alpha^2)$.

5. (5 points) Soient F, K, L des corps de caractéristique p avec $F \subset K \subset L$. Soit $\alpha \in L$ algébrique sur F. Montrer que si α est inséparable sur K, alors, α est inséparable sur F.

Solution: Soit $f(x) = m_{K,\alpha}(x)$ est $g(x) = m_{F,\alpha}(x)$ les polynômes minimals de α sur K et F. Alors, $g(x) \in \mathbb{F}[x] \subset K[x]$, et $f(x)|g(x)$ en $K[x]$. Alors, si $f(x)$ n'est pas séparable, il a des racines multiples, alors $g(x)$ a des racines multiples et il n'est pas séparable.

6. (7 points) (a) Soit $K \subset L$ une extension algébrique de corps de caractéristique p. Soit $p(x) = x^p - a \in K[x]$. Montrer que si $p(x)$ n'est pas irréductible sur $L[x]$, il se factorise comme $(x-\beta)^p$ sur $L[x]$ pour β tel que $\beta^p = a$. Piste: le polynôme $(x-\beta)^k$ est-il séparable? est-il irréductible?

(b) Soient F un corps de caractéristique p et β algébrique sur F. Montrer que β est séparable sur F si et seulement si $F(\beta) = F(\beta^p)$.

Solution: (a) On a que $p(x) = (x-\beta)^p$ sur une clôture algébrique de K. Si $p(x)$ n'est pas irréductible sur $L[x]$, $p(x)$ se factorise sur $L[x]$. Les facteurs irréductibles sont de la forme $(x-\beta)^k$ avec $k < p$. Noter que le polynôme $(x-\beta)^k$ n'est pas séparable si $k > 1$ mais $D_x((x-\beta)^k) = k(x-\beta)^{k-1} \neq 0$, alors, il ne peut pas être irréductible (parce que tous les irréductibles inséparables ont dérivée egale à zero). Seulement $x - \beta$ est irréductible et $p(x) = (x-\beta)^p$ sur $L[x]$.

(b) Si β est séparable sur F, $x^p - \beta^p$ n'est pas irréductible sur $F(\beta^p)$ (parce que sinon β serait inséparable par question 5). Ça veut dire que il se factorise lineairement, et que $\beta \in F(\beta^p)$, alors $F(\beta) = F(\beta^p)$. Si β est inséparable, soit $f(x) = m_{F,\beta}(x) = g(x^p)$. Alors, β^p est racine de $g(x)$, et $\deg g(x) = \frac{\deg f(x)}{p} < \deg f(x)$. Alors $[F(\beta^p) : F] \leq \deg g(x) < \deg f(x) = [F(\beta) : F]$ et $F(\beta^p) \neq F(\beta)$.