Partiel, 26 mars 2014, 14h30-16h30

Les règles du jeu :

1. Vous pouvez utiliser tout résultat du cours... sauf si la question est de démontrer un tel résultat.

2. Les documents, sauf les notes de cours de M. Tchoudjem sur sa page web, ainsi que la communication avec les autres étudiants ne sont pas autorisés.

3. Les questions à l'enseignant sont encouragées.

4. Il y a 5 exercices (24 points à gagner) qui attendent vos réponses. Bon travail...

Un peu de théorie

Exercice 1 (Rappels).

(a) (1 pt) *Soit L/K une extension galoisienne finie. Soit $\alpha \in L$. Montrer que α est un élément primitif si et seulement si le cardinal de son orbite sous l'action de* $\mathrm{Gal}(L/K)$ *est $[L : K]$.*

Réponse : D'abord on suppose α primitif, en d'autres termes $L = K(\alpha)$. Ceci équivaut à ce que L soit le corps de rupture du polynôme minimal P de α sur K. Par conséquent, $[L : K] = \deg(P)$. Comme L/K est galoisienne, $[L : K] = |\mathrm{Gal}(L/K)|$. Or, $P(X) = \prod_{\sigma\in\mathrm{Gal}(L/K)}(X - \sigma(\alpha))$, et est un polynôme séparable. Ainsi, l'ensemble $\{\sigma(\alpha)|\sigma \in \mathrm{Gal}(L/K)\}$ contient exactement $[L : K]$ éléments.

Supposons maintenant que l'orbite de α sous l'action de $\mathrm{Gal}(L/K)$ contient exactement $[L : K]$ éléments. Comme dans le paragraphe précédent, cette orbite est exactement l'ensemble des racines de P. Alors, P étant le polynôme minimal de α sur K, on déduit que $[K(\alpha) : K] = \deg(P)$. Or, comme P est séparable, son degré est aussi le nombre de ses racines, en l'occurrence $[L : K]$. Ainsi, $L = K(\alpha)$.

(b) (2 pts) *Soient $K \leq L$ deux corps. On suppose que L est le corps de décomposition d'un polynôme séparable $P \in K[X]$. Montrer que l'action de* $\mathrm{Gal}(L/K)$ *sur les racines de P est transitive si et seulement si P est irréductible sur K.*

Réponse : On admet que $\mathrm{Gal}(L/K)$ agit transitivement sur les racines de P. Si $P = QR$, où $Q, R \in K[X]$, alors pour tout $\sigma \in \mathrm{Gal}(L/K)$, σ fixe les polynômes Q, R. Il en découle que pour tout $\sigma \in \mathrm{Gal}(L/K)$ et α racine de Q (resp. racine de R), si $\sigma(\alpha)$ est racine de R (resp. racine de Q), alors elle est racine de Q (resp. racine de R), sauf si Q ou R est un polynôme constant. Or, l'action de $\mathrm{Gal}(L/K)$ est transitive et P n'a pas de racine multiple.

Dans le sense inverse, on suppose que P soit irréductible sur K. Soit α une racine de P. Ainsi, à un multiple constant et non nul près, P est le polynôme minimal de α sur K. Or, ce polynôme est exactement $\prod_{\sigma\in\mathrm{Gal}(L/K)}(X - \sigma(\alpha))$.

(c) (1 pt) *Soit K un corps. Montrer que si L est le corps décomposition d'un polynôme $P \in K[X]$, alors l'extension L/K est une extension normale.*

Réponse : Si les racines de P sont $\alpha_1, \ldots, \alpha_r$, alors $L = K(\alpha_1, \ldots, \alpha_r)$. Ceci entraîne que tout K-morphisme $\sigma : L \longrightarrow L'$ soit déterminé par $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_r)\}$. Or, cet ensemble est $\{\alpha_1, \ldots, \alpha_r\}$.

Exercice 2 (Éléments primitifs : théorie).
Soient K un corps infini et $L = K(\alpha, \beta)$ une extension algébrique. On suppose aussi que β est séparable sur K. L'objectif de cet exercice est de montrer que L/K contient un élément primitif.
On définit P et Q les polynômes minimaux de α et de β respectivement. Leurs degrés sont notés d_P et d_Q respectivement. On fixe une extension Ω de L où P et Q sont scindés. On note leurs ensembles de racines respectifs $\{\alpha_1, \ldots, \alpha_{d_P}\}$ et $\{\beta_1, \ldots, \beta_{d_Q}\}$, avec $\alpha_1 = \alpha$ et $\beta_1 = \beta$.

(a) (1 pt) *Montrer qu'il existe $t \in K$ tel que $t \neq \frac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$ pour tous $1 \leq i, k \leq d_P$ et $1 \leq j \neq l \leq d_Q$. En déduire que $\alpha_i + t\beta_j \neq \alpha_k + t\beta_l$ pour tous $1 \leq i, k \leq d_P$ et $1 \leq j \neq l \leq d_Q$.*

Réponse : On considère les éléments de Ω de la forme $\alpha_i + t\beta_j$ ($1 \leq i \leq d_p$, $1 \leq j \leq d_q$, $t \in K$). Deux éléments $\alpha_i + t\beta_j$ et $\alpha_k + t\beta_l$ sont égaux si et seulement si $\alpha_i - \alpha_k = t(\beta_l - \beta_j)$. Si $j \neq l$, grâce à la séparabilité de P, cette égalité équivaut à $t = \frac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$. Bien évidemment, les $\frac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$ forment une partie finie de K. Par conséquent, $K \setminus \{\frac{\alpha_i - \alpha_k}{\beta_l - \beta_j} \mid 1 \leq i, k \leq d_p \ , \ 1 \leq j \neq l \leq d_q\} \neq \emptyset$, et pour tout t appartenant à ce sous-ensemble de K, $\alpha_i + t\beta_j \neq \alpha_k + t\beta_l$ quand $j \neq l$.

(b) (1 pt) *Montrer que le PGCD unitaire $h(X)$ des polynômes $Q(X)$ et $P(\alpha + t\beta - tX)$ dans $K(\alpha + t\beta)[X]$ est de degré au moins 1. (*Vous pouvez expliciter une racine commune*)*

Réponse : Simple calcul montre que β est racine de $Q(X)$ et de $P(\alpha + t\beta - tX)$. Ceci implique que le monôme $X - \beta$ divise $Q(X)$ et $P(\alpha + t\beta - tX)$. Par conséquent, le PGCD de ceux-ci est de degré au moins 1. Il reste à préciser le corps contenant les coefficients de ce PGCD. Or, $Q(X)$ et $P(\alpha + t\beta - tX)$ appartiennent à $K(\alpha + t\beta)[X]$. Ainsi, la détermination du PGCD, en utilisant la division euclidienne, montre que le PGCD appartient au même corps.

(c) (3 pts) *Montrer que h est linéaire. Quel est son terme constant ? (*Le polynôme Q n'a pas de racine multiple*).*

Réponse : Si h est de degré au moins 2, alors h partage une deuxième racine avec Q qui est nécessairement différente de β en raison de la séparabilité de Q. Cette deuxième racine sera de la forme β_j avec $2 \leq j \leq d_Q$. Alors, $P(\alpha + t\beta - t\beta_j) = 0$, ce qui implique qu'il existe α_i ($1 \leq i \leq d_P$) tel que $\alpha_i = \alpha + t(\beta - \beta_j)$. Équivalemment, $t = \frac{\alpha - \alpha_i}{\beta_j - \beta}$, ce qui contredit le choix de t.

(d) (1 pt) *Déduire du point précédent que $K(\alpha, \beta) = K(\alpha + t\beta)$.*

Réponse : Clairement, $K(\alpha + t\beta) \subset K(\alpha, \beta)$. Montrons l'autre inclusion. D'après le point précédent, $h(X) = X - \beta$. Or on sait d'après le point (b) que h appartient

à $K(\alpha + b\beta)[X]$. Par conséquent $\beta \in K(\alpha + t\beta)$. Comme $t \in K$, on en déduit que $t\beta \in K(\alpha + t\beta)$, et que par conséquent, $\alpha \in K(\alpha + t\beta)$.

Un peu de pratique

Exercice 3 (Éléments primitifs : pratique).
Soient P le polynôme $X^5 - 2$ sur $\mathbb{Q}$, L le corps de décomposition de P sur $\mathbb{Q}$.

(a) (0.5 pt) *Montrer que P irréductible sur $\mathbb{Q}$.*

Réponse : Le nombre 2 est premier et ne divise pas 1 qui est le coefficient de X^5. Le critère d'Eisenstein montre que $X^5 - 2$ est irréductible dans $\mathbb{Z}[X]$, et la même conclusion s'ensuit dans $\mathbb{Q}[X]$.

(b) (0.5 pt) *Montrer que $L/\mathbb{Q}$ est une extension galoisienne.*

Réponse : Par définition, L est le corps de décomposition de P sur $\mathbb{Q}$. Or, P est séparable puisqu'il est premier avec sa dérivée $5X^4$. Ainsi, d'après le théorème 3.9 des notes de cours, $L/\mathbb{Q}$ est une extension galoisienne.

(c) (0.5 pt) *Soit μ une racine primitive cinquième de 1. Montrer que $\mu \in L$ et que $[\mathbb{Q}(\mu) : \mathbb{Q}] = 4$.*

Réponse : Le nombre μ est racine de $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + 1)$. Comme il est différent de 1, il est racine de $X^4 + X^3 + X^2 + 1$. Ce dernier polynôme est le cinquième polynôme cyclotomique. Mais, même sans recours à ces connaissances "avancées", son irréductibilité sur $\mathbb{Q}$ est parmi les prérequis de ce cours.

(d) (1.5 pts) *Montrer que $L = \mathbb{Q}(\mu, 2^{1/5})$ et que $[L : \mathbb{Q}] = 20$. Quel est le polynôme minimal de $2^{1/5}$ sur $\mathbb{Q}(\mu)$?*

Réponse : Le corps L contient $\mathbb{Q}(\mu, 2^{\frac{1}{5}})$ puisque les racines de P sont de la forme $2^{\frac{1}{5}}\mu^i$ où $0 \leq i \leq 4$ et que L les contient tous. Quant à l'autre inclusion, il est clair que le corps $\mathbb{Q}(2^{\frac{1}{5}}, \mu)$ contient toutes les racines de P. Par conséquent, $L \leq \mathbb{Q}(2^{\frac{1}{5}}, \mu)$.

Le corps L contient $\mathbb{Q}(\mu)$ et $\mathbb{Q}(2^{\frac{1}{5}})$, deux extensions de $\mathbb{Q}$ de degrés 4 et 5 respectivement, selon les points (a) et (c) respectivement. Comme ces deux nombres sont premiers entre eux, la multiplicativité des degrés des extensions de corps implique que $[L : \mathbb{Q}] = 20$.

Il reste à déterminer le polynôme minimal de $2^{\frac{1}{5}}$ sur $\mathbb{Q}(\mu)$. C'est un diviseur de $X^5 - 2$ dans $\mathbb{Q}(\mu)[X]$. Or, L est le corps de rupture sur $\mathbb{Q}(\mu)$ du polynôme minimal sur $\mathbb{Q}(\mu)$ de $2^{\frac{1}{5}}$. Or, nos calculs montrent que $[L : \mathbb{Q}(\mu)] = 5$. Par conséquent, le polynôme minimal de $2^{\frac{1}{5}}$ sur $\mathbb{Q}(\mu)$ est $X^5 - 2$.

(e) (1 pt) *Montrer que* $\mathrm{Gal}(L/\mathbb{Q})$ *n'est pas commutatif.*

Réponse : L'extension de $\mathbb{Q}(2^{\frac{1}{5}})$ n'est pas normale puisqu'elle n'est pas stable sous l'action de $\mathrm{Gal}(L/\mathbb{Q})$. En effet, cette action permute transitivement les racines de P (le point (b) du premier exercice), mais celles-ci, sauf $2^{\frac{1}{5}}$, n'appartiennent pas à $\mathbb{R}$. Par conséquent, $\mathrm{Gal}(L/\mathbb{Q}(2^{\frac{1}{5}}))$ n'est pas un sous-groupe distingué de $\mathrm{Gal}(L/\mathbb{Q})$. Or, tout sous-groupe d'un groupe abélien est distingué.

(f) (1 pt) *Montrer que* $\mathrm{Gal}(L/\mathbb{Q}(\mu))$ *est distingué dans* $\mathrm{Gal}(L/\mathbb{Q})$.

Réponse : Le corps $\mathbb{Q}(\mu)$ est le corps de décomposition de $X^4+X^3+X^2+1$ sur $\mathbb{Q}$. C'est un polynôme irréductible sur $\mathbb{Q}$ comme on l'a rappelé dans le point (c), sa dérivée est non nulle. Il est donc séparable. Par conséquent, l'extension $\mathbb{Q}(\mu)/\mathbb{Q}$ est galoisienne.

(g) (3 pts) *Montrer que pour tout* $0 \leq i \leq 4$, *il existe un élément de* $\mathrm{Gal}(L/\mathbb{Q})$ *qui fixe* μ *et transforme* $2^{1/5}$ *en* $2^{1/5}\mu^i$. *Montrer que pour tout* $1 \leq i \leq 4$, *il existe un élément de* $\mathrm{Gal}(L/\mathbb{Q})$ *qui fixe* $2^{1/5}$, *et qui transforme* μ *en* μ^i. *Déterminer l'orbite de* $2^{1/5}+\mu$ *sous l'action du groupe de Galois* $\mathrm{Gal}(L/\mathbb{Q})$ *et en déduire que* $2^{1/5}+\mu$ *est un élément primitif de* $L/\mathbb{Q}$.

Réponse : Nous avons vu dans le point (d) que X^5-2 est le polynôme minimal de $2^{\frac{1}{5}}$ sur $\mathbb{Q}(\mu)$. En utilisant l'un des points (a) ou (b) du premier exercice, on conclut que $\mathrm{Gal}(L/\mathbb{Q}(\mu))$ permute transitivement. Or, ce dernier est un sous-groupe de $\mathrm{Gal}(L/\mathbb{Q})$. Ainsi, pour tout $0 \leq i \leq 4$, il existe un élément de $\mathrm{Gal}(L/\mathbb{Q})$ qui fixe μ et transforme $2^{1/5}$ en $2^{1/5}\mu^i$.

Un raisonnement similaire à celui du point (d) montre que $X^4+X^3+X^2+X+1$ est le polynôme minimal de μ sur $\mathbb{Q}(2^{\frac{1}{5}})$. On reprend le raisonnement du paragraphe précédent dans le contexte de l'extension $L/\mathbb{Q}(2^{\frac{1}{5}})$ pour vérifier la seconde assertion.

Les diverses compositions des automorphismes obtenus dans les deux paragraphes précédents transforment $2^{\frac{1}{5}}+\mu$ en $2^{\frac{1}{5}}\mu^i+\mu^j$ où i et j décrivent $[\![0,4]\!]$ et $[\![1,4]\!]$ respectivement. La $\mathbb{Q}$-indépendance lineáire de $\{1,\mu,\ldots,\mu^4\}$ (c'est une base pour le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\mu)$) montre que $2^{\frac{1}{5}}\mu^i+\mu^j = 2^{\frac{1}{5}}\mu^k+\mu^l$ si et seulement si $i=k$ et $j=l$. Cette conclusion montre que l'orbite sous l'action de $\mathrm{Gal}(L/\mathbb{Q})$ contient 20 éléments. Vu que le groupe $\mathrm{Gal}(L/\mathbb{Q})$ a 20 éléments ce qui est aussi $[L:\mathbb{Q}]$, la conclusion finale découle du point (a) du premier exercice.

Exercice 4 (Corps finis).
Soient e, m *deux entiers strictement supérieurs à* 1. *On fixe un nombre premier* p *qui ne divise pas* e *et* q *une puissance non nulle de* p.

(a) (3 pts) *On note :*

$$\Phi_e \;=\; \prod_{x \text{ d'ordre } e \text{ dans } \mathbb{F}_{q^m}} (X-x)\,.$$

Montrer que $\Phi_e \in \mathbb{F}_q[X]$. *Montrer que le groupe de Galois de* Φ_e *sur* $\mathbb{F}_q$ *est cyclique engendré par l'automorphisme* $t \mapsto t^q$. *En utilisant la question b) de l'exercice* 1, *montrer que si* Φ_e *est irréductible sur* $\mathbb{F}_q$, *alors le groupe des inversibles de* $\mathbb{Z}/e\mathbb{Z}$ *est cyclique engendré par* $q \mod e$.

Réponse : Montrons d'abord que $\Phi_e \in \mathbb{F}_q[X]$. Comme les extension des corps finis sont toujours galoisiennes (le théorème 4.6 des notes de cours), il suffit de montrer que $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ fixe Φ_e. Or, pour tout $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, un élément x de $(\mathbb{F}_{q^m})^*$ est d'ordre e si et seulement si $\sigma(x)$ est d'ordre e. Par conséquent, $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ permute les racines de Φ_e, et ainsi, fixe Φ_e.

Ensuite, étudions $\mathrm{Gal}(\Phi_e/\mathbb{F}_q)$, ou encore $\mathrm{Gal}(L/\mathbb{F}_q)$ où L est le corps de décomposition sur $\mathbb{F}_q$ de Φ_e. L'automorphisme de Frobenius stabilise, et par conséquent, induit un $\mathbb{F}_q$-automorphisme de L. Le groupe multiplicatif L^* est cyclique. Soit t un générateur de L^*. Alors chaque élément de $\mathrm{Gal}(L/\mathbb{F}_q)$ est déterminé par son l'image de t. Or pour tout $i \in \mathbb{N}$, $\sigma^i(t) = t^{q^i}$, et il en existe exactement $[L : \mathbb{F}_q]$. Ainsi, $\mathrm{Gal}(L/\mathbb{F}_q)$ est cyclique engendré par σ.

On suppose maintenant Φ_e irréductible. Alors, $\mathrm{Gal}(L/\mathbb{F}_q)$ agit transitivement sur les racines de Φ_e. Posons $m = \deg(\Phi_e)$ pour simplifier la notation. Alors, si x est une racine de Φ_e, les autres racines seront de la forme x^{q^i} avec $i \in [\![0, m-1]\!]$ en raison de l'action de l'automorphisme de Frobenius. Ceci entraîne que $x^{q^m} = x$, et que donc, e divise $q^m - 1$. Or m est la plus petite puissance de q telle que e divise $q^m - 1$ vu que $\mathbb{F}_q(a) = \mathbb{F}_{q^m}$. En fait, nous venons de faire la preuve de la proposition 4.10 des notes de cours dans le cas particulier où le polynôme irréductible P de cette proposition est précisément Φ_e.

Or, les racines de Φ_e sont les générateurs du seul sous-groupe cyclique d'ordre e de $\mathbb{F}_{q^m}$. Il en existe donc $\phi(e)$. L'hypothèse d'irréductibilité de Φ_e entraîne en utilisant le théorème 4.11 des notes de cours que $m = \phi(e)$. Comme, d'après la conclusion du paragraphe précédent, m est l'ordre de q dans le groupe multiplicatif des inversibles de $\mathbb{Z}/m\mathbb{Z}$, on conclut alors que ce dernier groupe est cyclique.

(b) (1 pt) *Montrer que Φ_{12} est réductible sur tout corps fini de caractéristique $\neq 2, 3$.*

Réponse : Il suffit de vérifier que $(\mathbb{Z}/12\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. En effet, $\{1, 5, 7, 11\}$ sont les inversibles mod 12 et ils sont tous d'ordre au plus 2.

Exercice 5 (Éléments transcendants).
On définit $K = \mathbb{C}(t^4)$ et $L = \mathbb{C}(t)$, où t est transcendant sur $\mathbb{C}$. On pose $P(X) = X^4 - t^4$.

(a) (1 pt) *Montrer que L est le corps de décomposition de P sur K. En déduire que L/K est une extension galoisienne de degré ≤ 4.*

Réponse : Le polynôme P se factorise comme $P(X) = (X + \sqrt{-1}t)(X - \sqrt{-1}t)(X + t)(X - t)$. Il en découle que P se scinde dans L. Or $L = \mathbb{C}(t)$, ainsi L est le corps de décomposition de P sur K.

Le polynôme P est séparable puisque ses racines sont simples, ainsi L/K est une extension galoisienne. Comme P est séparable, L/K est galoisienne.

Finalement, comme $L = \mathbb{C}(t) = K(t)$, le degré $[L : K]$ est celui du polynôme minimal de t sur K. Or celui-ci est un diviseur de P puisque $P(t) = 0$. L'assertion sur $[L : K]$ en découle.

(b) (2 pts) *Déterminer $\mathrm{Gal}(L/K)$ et en déduire l'irréductibilité du polynôme P sur K (*trouver d'abord l'ordre de l'automorphisme $t \longmapsto \sqrt{-1}\, t$*).*

Réponse : Commençons par noter que $t^2 \notin K$. En effet sinon, il existerait deux polynômes P, Q premiers entre eux dans $\mathbb{C}[X]$ tels que $t^2 = \frac{P(t^4)}{Q(t^4)}$. Or, ceci entraîne la relation polynômiale $P(t^4) - t^2 Q(t^4) = 0$, ce qui contredit que t est transcendant sur $\mathbb{C}$. Un raisonnement similaire montre que $t \notin K(t^2)$. Nous avons donc deux extensions successives de degré 2, avec les polynômes minimaux $X^2 - T^2$ de t sur

$K(t^2)$, et $X^2 - T^4$ de t^2 sur $K(t^4)$. Comme L/K est galoisienne, ceci montre que $\mathrm{Gal}(L/K)$ a quatre éléments.

Le paragraphe précédent entraîne l'existence d'un morphisme de $K(t^2)/K$ qui transforme t^2 en $-t^2$. Ceci se prolonge à un automorphisme σ de L/K. La comparaison des racines carrées de t^2 et $-t^2$ montre que $\sigma(t) = \pm\sqrt{-1}t$. Les deux choix donnent les deux générateurs du groupe cyclique d'ordre 4 auquel est isomorphe $\mathrm{Gal}(L/K)$.

Finalement, l'action déjà décrite de $\mathrm{Gal}(L/K)$ sur les racines de P est transitive. Il s'ensuit en utilisant le point (b) de l'exercice 1 que P est irréductible sur K.