Partiel, 31 mars 2015, 14h00-16h30

Exercice 1 (Révisions (6 pts)).

1. (0.5 pt) *Montrer que si $K \leq L \leq M$ sont des extensions algébriques des corps K, L, M et que M est une extension séparable de K, alors M est une extension séparable de L.*

   Réponse : D'après la définition d'une extension séparable, pour tout $\alpha \in M$, le polynôme minimal de α sur K est séparable. Or, le polynôme minimal de α sur L est un diviseur de celui sur K. Par conséquent, les racines de celui-ci sont distinctes si celles de celui-là le sont.

2. (1 pt) *Montrer que si $K \leq L \leq M$ sont des extensions algébriques des corps K, L, M et que M est une extension normale de K, alors M est une extension normale de L.*

   Répones : Par hypthèse, tout polynôme irréductible dans $K[X]$ qui a une racine dans M s'y scinde. Soient $\alpha \in M$ et P un polynôme irréductible dans $L[X]$ dont α est racine. Le polynôme P est donc le polynôme minimal de α à coefficient près. Alors, P divise le polynôme minimal de α sur K. Ce dernier se scinde dans M. Inévitablement, tous ses diviseurs s'y scindent aussi.

3. *Un corps K est dit parfait si toute extension algébrique de K est séparable.*

   (a) (0.5 pt) *Montrer que toute extension algébrique d'un corps parfait est parfait.*

   Réponse : Soient K un corps parfait et $L \geq K$ une extension algébrique de K. Toute extension algébrique L' de L est aussi une extension algébrique de K. Comme K est parfait, L'/K est une extension séparable. Le premier point de cet exercice montre que L'/L l'est aussi.

   (b) (1 pt) *Soit K un corps de caractéristique p non nulle. Si f est un polynôme irréductible dans $K[X]$, alors f est inséparable si et seulement si $f(X) \in K[X^p]$.* (Rappelons qu'un polynôme est dit inséparable s'il n'est pas séparable).

   Réponse : Le polynôme f est de la forme $\sum_{i=0}^{d} a_i X^i$ avec $d \in \mathbb{N}^*$ et $a_d \neq 0$. Comme f est irréductible dans $K[X]$, f est inséparable si et seulement si $f' = 0$. Or $f' = 0$ si et seulement si ia_i est divisible par p pour chaque $i \in \{0, \ldots, d\}$ si et seulement si p divise i ou a_i. Comme la deuxième possibilité équivaut à ce que $a_i = 0$ en caractéristique p, on conclut que les a_i non nuls sont les coefficients des termes en X de puissance divisible par p. En d'autres termes, P est de la forme $\sum_{i=0}^{d/p} b_i \, (X^p)^i$.

   (c) (2 pts) *Soit K un corps de caractéristique p. Montrer alors l'équivalence suivante : K est parfait si et seulement si l'endomorphisme de Frobenius $F : x \longmapsto x^p$ est surjectif.*

   Réponse : D'abord, on suppose K parfait. Soit $a \in K$. Le polynôme $X^p - a$ dans $K[X]$ détermine une extension algébrique de K qui est inséparable puisqu'il n'a qu'une seule racine par simple calcul, ou qu'il est inséparable par le point précédent de cette question. Or K est parfait et par conséquent, cette extension est aussi séparable. Ainsi, elle ne peut qu'être égale à K. Ceci implique que la racine de $X^p - a$

appartienne à K et que a ait une image inverse par rapport à l'endomorphisme Frobenius $x \mapsto x^p$ de K.

(d) (1 pt) *Montrer que les corps finis sont parfaits.*

Réponse : Soit K un corps fini de caractéristique p. Alors, l'endomorphisme Frobenius de K, $x \mapsto x^p$, est non nul puisque $1 \mapsto 1$. Comme c'est un morphisme de corps, il est alors injectif. Or, c'est une injection d'un ensemble fini vers lui-même. Ainsi, il est aussi surjectif.

Exercice 2 (Corps finis (5 pts)).
Soit K un corps fini de caractéristique p impaire. On dira que $x \in K$ est un carré s'il existe $y \in K$ tel que $y^2 = x$. On notera K^2 les carrés de K.

1. (1 pt) *Montrer que le nombre de carrés dans K est $\frac{|K|+1}{2}$ où $|\ |$ note le nombre d'éléments dans l'ensemble en question.*

   Réponse : L'application $x \mapsto x^2$ est un morphisme du groupe multiplicatif $(K^\times, .)$ du corps K. Comme la caractéristique de K est différente de 2, le noyau de ce morphisme est $\{-1, 1\}$. Par conséquent son image, les carrés non nuls de K, est un ensemble de cardinal $\frac{|K|-1}{2}$. On y ajoute 0.

2. (0.5 pt) *Soit $\delta \in K \setminus K^2$. Montrer que l'extension $K(\sqrt{\delta})/K$ est galoisienne de degré 2.*

   Réponse : Le corps de $K(\sqrt{\delta})$ est le corps de décomposition du polynôme $X^2 - \delta$ dans $K[X]$. La caractéristique de K étant différente de 2, $X^2 - \delta$ a deux racines distinctes, donc séparable. La caractérisation des extensions galoisiennes montre que l'extension est galoisienne. Notons que ce qui précède n'est certainement pas la seule façon de vérifier que l'extension est galoisienne.

3. (1.5 pts) *Montrer, en considérant l'action des éléments de $\mathrm{Gal}(K(\sqrt{\delta})/K)$ sur $K(\sqrt{\delta})$, que l'application $x + y\sqrt{\delta} \longmapsto x^2 - y^2\delta$ $(x, y) \in K^2$ définit un homomorphisme du groupe multiplicatif de $K(\sqrt{\delta})$ dans le groupe multiplicatif de K.*

   Réponse : Pour tous $x, y \in K$, $x^2 - y^2\delta = (x + y\sqrt{\delta})(x - y\sqrt{\delta}) = \prod_{\sigma \in \mathrm{Gal}(K(\sqrt{\delta})/K))} \sigma(x + y\sqrt{\delta})$. Comme $(K(\sqrt{\delta})^\times, .)$ est un groupe commutatif et que δ n'est pas un carré dans K, $x + y\sqrt{\delta} \mapsto x^2 - y^2\delta$ est alors un endomorphisme de $(K(\sqrt{\delta})^\times, .)$. Son ensemble d'arrivée est contenu dans K puisque chacun de ses éléments est fixé par $\mathrm{Gal}(K(\sqrt{\delta})/K)$.

4. (1 pt) *Montrer que le morphisme du point précédent est surjectif.*

   Réponse : Soit $c \in K^\times$. Nous devons montrer que c a un antécédent par rapport au morphisme du point précédent. Nous avons vérifié qu'il existe $\frac{|K|+1}{2}$ carrés dans K. Par conséquent, il en existe autant de la forme $c + \delta y^2$. Par conséquent, les ensembles $\{x^2 | x \in K\}$ et $\{c - \delta y^2 | y \in K\}$ ont l'intersection non vide. Il en découle qu'il existe une paire $(x, y) \in K \times K$ telle que $x^2 - y^2\delta = c$.

5. (1 pt) *Montrer que pour chaque $c \in K^\times$, le nombre de solutions dans $K \times K$ de l'équation $x^2 - y^2\delta = c$ est $|K| + 1$.*

   Réponse : Comme $(1, \delta)$ est une base du K-espace vectoriel $K(\sqrt{\delta})$, le nombre de solutions dans $K \times K$ est le nombre d'éléments dans chaque fibre du morphisme $x + y\sqrt{\delta} \mapsto x^2 - y^2\delta$. Ce nombre est donné par le cardinal de l'image divisé par celui du noyau. Nous avons montré dans le point précédent que l'image contient exactement $|K| - 1$ éléments. Comme $|K(\sqrt{\delta})^\times| = |K|^2 - 1$, la conclusion s'ensuit.

Exercice 3 (Groupes de Galois (13 pts)).
On pose $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

1. (3 pts) *On commence avec une révision rapide. Montrer que* $K/\mathbb{Q}$ *est une extension galoisienne de degré* 4*, de groupe de Galois* $\mathrm{Gal}(K/\mathbb{Q})$ *isomorphe à* $(\mathbb{Z}/2\mathbb{Z}, +)\times(\mathbb{Z}/2\mathbb{Z}, +)$ *et engendré par les deux automorphismes*

$$\sigma \ : \ \left\{ \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{array} \right. \qquad\qquad \tau \ : \ \left\{ \begin{array}{ccc} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array} \right. \quad ,$$

dont on justifiera l'existence.
Réponse : L'auteur de ces lignes en a déjà assez dit.

On définit $\theta = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ *et* $L = K(\theta)$*. Clairement* $\theta^2 \in K$*.*

2. (1 pt) *Montrer que* $\frac{\sigma(\theta^2)}{\theta^2} = (\sqrt{2}-1)^2$ *et* $\frac{\tau(\theta^2)}{\theta^2} = \left(\frac{3-\sqrt{3}}{\sqrt{6}}\right)^2$.
Réponse : On calcule :

$$\frac{\sigma(\theta^2)}{\theta^2} \ = \ \frac{\sigma((2+\sqrt{2})(3+\sqrt{3}))}{(2+\sqrt{2})(3+\sqrt{3})} \ = \ \frac{2-\sqrt{2}}{2+\sqrt{2}} \ = \ \frac{\sqrt{2}-1}{\sqrt{2}+1} \ = \ (\sqrt{2}-1)^2 \ ;$$

$$\frac{\tau(\theta^2)}{\theta^2} \ = \ \frac{3-\sqrt{3}}{3+\sqrt{3}} \ = \ \left(\frac{3-\sqrt{3}}{\sqrt{6}}\right)^2 \ .$$

3. (1 pt) *Déduire du point précédent que* $\theta \notin K$*. (*Vous pouvez utiliser le raisonnement par l'absurde ce qui légitimera l'écriture $\sigma(\theta)$ et permettra de calculer $\sigma^2(\theta)$.*)*
Réponse : Supposons $\theta \in K$. Alors, $\frac{\sigma(\theta^2)}{\theta^2} = \left(\frac{\sigma(\theta)}{\theta}\right)^2 = (\sqrt{2}-1)^2$. Ceci équivaut à $\sigma(\theta) = \pm\theta(\sqrt{2}-1)$. Comme σ est d'ordre 2, on en déduit que

$$\theta = \sigma^2(\theta) = \pm\sigma(\theta)(-\sqrt{2}-1) = \pm(\pm\theta(\sqrt{2}-1)(-\sqrt{2}-1)) = \theta(\sqrt{2}-1)(-\sqrt{2}-1) \ .$$

Notons qu'il n'y a pas d'ambiguité en ce qui concerne les $\pm$ parce que chaque fois c'est le même signe qu'on obtient. Ce calcul a pour conclusion $\theta = -\theta$, absurde en caractéristique différente de 2.

4. (1 pt) *Si* $\mu : L \longrightarrow \mathbb{C}$*, montrer que* $\mu(L)$ *prolonge un élément de* $\mathrm{Gal}(K/\mathbb{Q})$*. Déduire de ceci et des calculs du point 2 que* $L/\mathbb{Q}$ *est une extension normale, et par conséquent galoisienne.*
Réponse : Comme μ est un morphisme de corps qui fixe $\mathbb{Q}$ point par point, $\mu(\sqrt{2})$ (resp. $\mu(\sqrt{3})$) est racine de X^2-2 (resp. X^2-3). Par conséquent, $\mu(\sqrt{2}) = \pm\sqrt{2}$ (resp. $\mu(\sqrt{3}) = \pm\sqrt{3}$). Notons au passage que ceci montre que la restriction de μ à L induit un automorphisme de K.
Alors, de manière similaire au point précédent de l'exercice,

$$\frac{\mu(\theta^2)}{\theta^2} \ = \ \left(\frac{\mu(\theta)}{\theta}\right)^2 \ = \ \left\{ \begin{array}{c} \sqrt{2}-1 \\ \frac{3-\sqrt{3}}{\sqrt{6}} \end{array} \right. .$$

On en déduit que $\mu(\theta)$ est soit $\pm\theta(\sqrt{2}-1)$ soit $\pm\theta\frac{3-\sqrt{3}}{\sqrt{6}}$. Dans chaque cas, $\mu(\theta) \in L$. Il en découle que $L/\mathbb{Q}$ est une extension normale. Comme en caractéristique 0, toute

extension est séparable, on conclut que $L/\mathbb{Q}$ est une extension galoisienne. On peut donc parler de son groupe de Galois.

On notera $G = \mathrm{Gal}(L/\mathbb{Q})$.

5. (3 pts) *Déduire du point précédent que* σ *(resp.* τ*) s'étend à un automorphisme de* $L/\mathbb{Q}$ *qu'on notera* $\bar{\sigma}$ *(resp.* $\bar{\tau}$*). Montrer ensuite que* $\bar{\sigma}$ *et* $\bar{\tau}$ *sont d'ordre* 4 *et qu'ils ne commutent pas.* (Vous pouvez vous inspirer des calculs du point 2, et aussi calculer $\bar{\sigma}\bar{\tau}(\theta)$ et $\bar{\tau}\bar{\sigma}(\theta)$.).
Réponse : Le polynôme $X^2 - \theta^2$ se scinde dans L. D'après le théorème d'unicité du corps de décomposition (le théorème 1.9 des notes de cours), σ et τ s'étendent à des morphismes de L, qui est par ailleurs stable sous l'action de ces morphismes comme le montre le point précédent. Il s'agit donc des automorphismes de L.
Les calculs des deux points précédents s'appliquent à $\bar{\sigma}$ et $\bar{\tau}$ et montrent que $\bar{\sigma}^2(\theta) = -\theta$, $\bar{\tau}^2(\theta) = -\theta$. Comme $\bar{\sigma}(\sqrt{2}) = -\sqrt{2}$ (resp. $\bar{\tau}(\sqrt{3}) = -\sqrt{3}$) et $\bar{\sigma}(\sqrt{3}) = \sqrt{3}$ (resp. $\bar{\tau}(\sqrt{2}) = \sqrt{2}$), on déduit que $\bar{\sigma}^4$ et $\bar{\tau}^4$ sont l'identité.
On calcule ensuite

$$\bar{\sigma}\bar{\tau}(\theta) \;=\; \bar{\sigma}\left(\pm\frac{3-\sqrt{3}}{\sqrt{6}}\;\theta\right) \;=\; \pm\frac{3-\sqrt{3}}{-\sqrt{6}}(\pm(\sqrt{2}-1))\theta \;\;;$$

$$\bar{\tau}\bar{\sigma}(\theta) \;=\; \bar{\tau}(\pm(\sqrt{2}-1)\theta) \;=\; \pm\frac{3-\sqrt{3}}{\sqrt{6}}(\pm(\sqrt{2}-1))\theta \;\;.$$

Le signe de $\sqrt{6}$ au dénominateur montre que les deux produits ne sont pas égaux. Notons que les $\pm$ ne causent pas d'ambiguité.

6. (2 pts) *Montrer en les explicitant en fonction de* $\bar{\sigma}$ *et* $\bar{\tau}$ *que* G *a six éléments d'ordre* 4 *et* 1 *d'ordre* 2. (Il suffira de déterminer l'ordre de $\bar{\sigma}\bar{\tau}$.)
Réponse : Nous avons déjà déterminé dans le point précédent que $\bar{\sigma}$, $\bar{\sigma}^{-1}$, $\bar{\tau}$, $\bar{\tau}^{-1}$ sont distincts et d'ordre 4. Ensuite on calcule

$$(\bar{\sigma}\bar{\tau})^2(\theta) \;=\; \bar{\sigma}\bar{\tau}\left(\pm\frac{3-\sqrt{3}}{-\sqrt{6}}(\pm(\sqrt{2}-1))\theta\right) \;=\; \bar{\sigma}\left(\frac{3+\sqrt{3}}{\sqrt{6}}(\pm(\sqrt{2}-1))\;\frac{3-\sqrt{3}}{\sqrt{6}}\;\theta\right) \;=$$

$$=\; \frac{3+\sqrt{3}}{-\sqrt{6}}\;(-\sqrt{2}-1)\;\frac{3-\sqrt{3}}{-\sqrt{6}}\;(\sqrt{2}-1)\;\theta \;=\; -\theta \;\;.$$

On déduit de ce calcul, en prenant en compte que $(\bar{\sigma}\bar{\tau})^2$ fixe $\sqrt{2}$ et $\sqrt{3}$, que $\bar{\sigma}\bar{\tau}$ et son inverse sont d'ordre 4. Clairement, ils sont différents des quatre autres éléments d'ordre 4 que nous avons déjà déterminés. En ce qui concerne les éléments d'ordre 2, σ^2 en est un. Par ailleurs, comme $L/\mathbb{Q}$ est une extension galoisienne et que $[L:\mathbb{Q}] = [L:K][K:\mathbb{Q}] = 2\,.\,4 = 8$, le groupe G a 8 éléments. Ainsi, nous avons fait le comptage exact des divers éléments de G.

7. (2 pts) *Montrer que* G *est isomorphe au groupe* $\mathbf{Q}_8$ *(de présentation* $\langle\, a, b \mid a^2 = b^2 = (ab)^2 \rangle$ *). Montrer que si* $\mathbb{Q} \leq M \leq L$*, alors* $M/\mathbb{Q}$ *est galoisienne.*
Réponse : En utilisant des connaissances antérieures, il suffit de faire correspondre $\bar{\sigma}$ à a et $\bar{\tau}$ à b.

Exercice 4 (Séparable/Inséparable (10 pts)).
Soit t un élément transcendant sur $\mathbb{F}_5$. On définit $K = \mathbb{F}_5(t)$.

1. (2 pts) *Montrer que le polynôme $P = X^3 + tX + t$ est irréductible dans $K[X]$. Montrer que P est séparable.*

   Réponse : Comme t est transcendant sur $\mathbb{F}_5$, il est irréductible dans l'anneau $\mathbb{F}_5[t]$. Alors, le critère d'Eisenstein montre que P est irréductible dans $\mathbb{F}_5[t][X]$. Or, $\mathbb{F}_5[t]$ est un anneau factoriel dont le corps de fractions est $\mathbb{F}_5(t)$. Par conséquent, P est irréductible dans $\mathbb{F}_5(t)[X]$ aussi.

   Comme nous avons vérifié que P est irréductible dans $K[X]$, il suffit de vérifier que $P' \neq 0$. Or, $P'(X) = 3X^2 + t$ est non nul, et on conclut que P est séparable.

2. (3 pts) *Montrer que le corps de décomposition L de P sur K est de degré 6 en utilisant son discriminant.* (Voir ci-dessous pour la formule générale du discriminant pour les polynômes de degré 3).

   Réponse : Remarquons d'abord que comme P est séparable, l'extension L/K est galoisienne. Le discriminant de P est $-4t^3 - 27t^2 = t^2(t+2)$. On vérifie que $t+2$ n'est pas un carré dans $\mathbb{F}_5(t)$ de la même manière qu'on vérifie la même conclusion pour un polynôme du premier degré à coefficients dans $\mathbb{F}_5$. Il s'ensuit que le groupe de $\mathrm{Gal}(L/K)$ n'est pas contenu dans le groupe alterné sur un ensemble à trois éléments. Comme P est irréductible, l'ordre de $\mathrm{Gal}(L/K)$ est nécessairement divisible par 3. Alors, $\mathrm{Gal}(L/K)$ est S_3, et en particulier son ordre est 6. Comme L/K est galoisienne, on conclut que $[L : K] = 6$.

3. (2 pts) *On définit $Q = P(X^{5^2})$. Montrer que Q est irréductible dans $K[X]$. Déterminer le nombre de racines de Q et leurs multiplicités.*

   Réponse : L'irréductibilité de Q équivaut à celle de P. Pour un élément α de L, $Q(\alpha) = 0$ si et seulement si $P(\alpha^{5^2}) = 0$. Or en caractéristique 5, l'application $x \mapsto x^{5^i}$ est injective pour tout $i \in \mathbb{N}^*$. Par conséquent, Q a exactement 3 racines, chacune de multiplicité 25.

4. (3 pts) *Soit M le corps de décomposition de Q sur K. Déterminer $[M : K]$ et $[M : K]_s$.*

   Réponse : L'extension M est de la forme $K(\alpha_1^{1/25}, \alpha_2^{1/25}, \alpha_3^{1/25})$ où $\alpha_1, \alpha_2, \alpha_3$ sont les racines de P. Alors, Q se décompose comme $\prod_{i=1}^3 (X^{25} - \alpha_i)$ dans $K(\alpha_1, \alpha_2, \alpha_3)[X]$, soit encore $Q = \prod_{i=1}^3 (X - \alpha_i^{1/25})^{25} = (X^3 + t^{1/25}X + t^{1/25})^{25}$. En particulier, $X^3 + t^{1/25}X + t^{1/25} \in M[X]$, ce qui implique que $t^{1/25} \in M$.

   Le paragraphe précédent montre que M est le corps de décomposition de $X^3 + t^{1/25}X + t^{1/25}$ sur $K(t^{1/25})$. Par conséquent, $[M : K(t^{1/25})] \leq 6$. Ceci est en fait une égalité puisque nous avons déjà vérifié que $[L, : K] = 6$, où $L = K(\alpha_1, \alpha_2, \alpha_3)$. Il en découle que $[M : K] = 6 \,.\, 25$ et que $[M : K]_s = 25$.

Formule du discriminant pour $X^3+pX+q \in K[X]$ séparable avec K de caractéristique différente de 2 et 3 : $-4p^3 - 27q^2$.