Université Paul Sabatier-Toulouse 3.
Master 1 de mathématiques fondamentales.
Algèbre. Corrigé de l'examen du 22 janvier 2008

I. Soient $\mathbb{F}_5$ un corps à 5 éléments et le polynôme
$$P(X) = X^5 - X + 1 \in \mathbb{F}_5[X].$$

(1) Montrer que $P(X)$ n'a pas de racine dans $\mathbb{F}_5$.

Il suffit de savoir que la puisssance 5*-ème est l'identité sur* $\mathbb{F}_5$.

(2) Soient $\mathbb{F}_5^{\mathrm{alg}}$ une clôture algébrique de $\mathbb{F}_5$ et $\alpha \in \mathbb{F}_5^{\mathrm{alg}}$ tel que $\alpha^2 = 2$.

(a) Montrer que $\mathbb{F}_5(\alpha)$ est une extension de degré 2 de $\mathbb{F}_5$.

En effet on vérifie que 2 *n'est pas un carré dans* $\mathbb{F}_5$.

(b) Montrer que $P(X)$ n'a pas de racine dans $\mathbb{F}_5(\alpha)$.

Il faut utiliser le fait que ($a, b \in \mathbb{F}_5$) $(a+b\alpha)^5 = a - b\alpha$, *cela se voit facilement car la puissance* 5*-ème est ici linéaire.*

(3) *En déduire* que $P(X)$ est irréductible sur $\mathbb{F}_5$.

Comme $P(X)$ *est ide degré* 5*, si* $P(X)$ *est réductible sur* $\mathbb{F}_5$*, il a soit une racine dans* $\mathbb{F}_5$*, soit il est divisible dans* $\mathbb{F}_5[X]$ *par un polynôme* $Q(X)$ *irréductible de degré* 2*. Une racine* β *dans* $\mathbb{F}_5^{\mathrm{alg}}$ *de* $Q(X)$ *vérifie* $\mathbb{F}_5(\beta) = \mathbb{F}_5(\alpha)$ *puisque* $\mathbb{F}_5^{\mathrm{alg}}$ *ne contient qu'un seul corps à* 5^2 *éléments. Donc ce diviseur* $Q(X)$ *n'existe pas.*

II. Soient $\mathbb{F}_5$ un corps à 5 éléments, $K = \mathbb{F}_5(T)$ un corps de fractions rationnelles à une indéterminée et le polynôme
$$Q(X) = X^5 - X + T \in K[X].$$

(1) Montrer que $Q(X)$ est irréductible sur K.

$Q(X)$*, vu comme un élément de* $\mathbb{F}_5[X][T]$*, estt un polynôme en* T *du premier degré et primitif, il est donc irréductible dans* $\mathbb{F}_5[X][T] = \mathbb{F}_5[T][X]$*, donc dans* $\mathbb{F}_5(T)[X]$*, d'après les propriétés des polynômes à coefficients dans les anneaux factoriels.*

(2) Soient K^{alg} une clôture algébrique de K et $\theta \in K^{\mathrm{alg}}$ une racine de $Q(X)$.

(a) Montrer que, si θ' est une autre racine de $Q(x)$ (dans K^{alg}), alors $\theta - \theta' \in \mathbb{F}_5$; en déduire que $K(\theta)/K$ est une extension galoisienne.

On a $0 = Q(\theta) - Q(\theta') = (\theta - \theta')^5 - (\theta - \theta')$, ce qui équivaut à dire que $\theta - \theta' \in \mathbb{F}_5$. On voit donc que $K(\theta)$ contient toutes les racines (dans K^{alg}) de $Q(X)$, c'est donc une extension normale de K. d'autre part $Q(X)$ est un polynôme séparable.

(b) Montrer que l'application

$$\mathrm{Gal}(K(\theta)/K) \to \mathbb{F}_5 \quad , \quad \sigma \mapsto \sigma(\theta) - \theta$$

est un isomorphisme de groupes.

Il n'y a aucune difficulté.

III. Soit le polynôme

$$P(X) = X^4 + 2X^2 - 2 \in \mathbb{Q}[X].$$

Soient les nombres complexes $\alpha = \sqrt{\sqrt{3} - 1}$ et $\beta = i\sqrt{\sqrt{3} + 1}$.

(1) Montrer que $P(X)$ est irréductible sur $\mathbb{Q}$, que ses quatre racines dans $\mathbb{C}$ sont $\pm\alpha$ et $\pm\beta$.

On voit que $P(X)$ est irréductible sur $\mathbb{Q}$ à l'aide du critère d'Eisenstein appliqué à l'anneau factoriel $\mathbb{Z}$ et à son irréductible 2.

(2) Montrer

(a) que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, i\sqrt{2})$ (on pourra par exemple remarquer que $\alpha\beta = i\sqrt{2}$),

C'est évident avec l'indication qui est donnée.

(b) que les extensions $\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}(\alpha)$ sont de degré 2,

On a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ puisque $P(X)$ est irréductible sur $\mathbb{Q}$, on a aussi $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, il ne reste plus qu'à remarquer que $\sqrt{3} \in \mathbb{Q}(\alpha)$ (ce qui est immédiat) pour obtenir $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 2$.

β est racine de $X^2 + \sqrt{3} + 1$ qui est un polynôme à coefficients dans $\mathbb{Q}(\alpha)[X]$, de plus β n'est pas réel et $\mathbb{Q}(\alpha)$ est un sous-corps de $\mathbb{R}$, donc β est de degré 2 sur $\mathbb{Q}(\alpha)$.

(c) que l'extension $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ est galoisienne de degré 8.

Avec ce qui précède le degré est clair. D'autre part $\mathbb{Q}(\alpha,\beta)$ *est engendré sur* $\mathbb{Q}$ *par toutes les racines de* $P(X)$*, c'est donc une extension normale de* $\mathbb{Q}$ *; ensuite* $\mathbb{Q}$ *est un corps parfait.*

(3) montrer

(a) $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}),\mathbb{C})$ a deux éléments, u_1 et u_2, caractérisés par

$$u_1(\sqrt{3}) = \sqrt{3} \quad \text{et} \quad u_2(\sqrt{3}) = -\sqrt{3},$$

Soit $s \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}),\mathbb{C})$*,* s *est caractérisé par* $s(\sqrt{3})$ *qui décrit les racines de* $(X^2-3)^s = X^2-3 = \mathrm{irr}(\sqrt{3},\mathbb{Q};X)$.

(b) que u_1 (resp. u_2) se prolonge en deux $\mathbb{Q}$-homomorphismes de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$, notés $u_{1,1}$ et $u_{1,2}$ (resp. $u_{2,1}$ et $u_{2,2}$) caractérisés par

$$u_{1,1}(\alpha) = \alpha \quad \text{et} \quad u_{1,2}(\alpha) = -\alpha,$$

$$u_{2,1}(\alpha) = \beta \quad \text{et} \quad u_{2,2}(\alpha) = -\beta,$$

que $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha),\mathbb{C}) = \{u_{i,j} \ / \ i,j = 1,2\}$.

Comme $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{3}) = 2]$ *(et que les extensions sont séparables), chaque élément de* $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}),\mathbb{C})$ *se prolonge en deux éléments de* $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha),\mathbb{C})$*. Si* $s \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}),\mathbb{C})$*, les deux prolongements* s_1 *et* s_2 *de* s *sont caractérisés par les valeurs qu'ils attribuent* α *:* $s_j(\alpha)$ *décrit les racines de* $(\mathrm{irr}(\alpha,\mathbb{Q}(\sqrt{3};X))^{s_j} = (X^2-(\sqrt{3}-1))^{s_j}$*. D'où les homomorphismes* $\mathbb{Q}(\alpha)\to\mathbb{C}$ *cherchés ; on les a tous car ils sont au nombre de* $4 = [\mathbb{Q}(\alpha):\mathbb{Q}$.

(c) que chaque $u_{a,b}$, $a,b = 1,2$, se prolonge en deux $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha, i\sqrt{2})$, notés $u_{a,b,c}$, $c = 1,2$, déterminés par

$$u_{a,b,1}(i\sqrt{2}) = i\sqrt{2} \quad \text{et} \quad u_{a,b,2}(i\sqrt{2}) = -i\sqrt{2},$$

que $G := \mathrm{Gal}(\mathbb{Q}(\alpha,\beta)/\mathbb{Q}) = \{u_{a,b,c} \ / \ a,b,c = 1,2\}$.

On a $\mathrm{irr}(i\sqrt{2},\mathbb{Q}(\alpha);X) = X^2+2$*, et les prolongements des* $u_{a,b}$ *sont caractérisés par les valeurs qu'ils attribuent à* $i\sqrt{2}$*. On trouve ainsi* 8 *homomorphismes* $\mathbb{Q}(\alpha,\beta)\to\mathbb{C}$*, qui sont des* $\mathbb{Q}$*-automorphismes de* $\mathbb{Q}(\alpha,\beta)$*, puisque l'extension* $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ *est normale ; on trouve donc* G*.*

(4) Montrer que $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha + i\sqrt{2})$.

On vérifie que l'ensemble de $s(\alpha + i\sqrt{2})$*, où* s *décrit* G*, a* 8 *éléments (distincts), donc* $\mathbb{Q}(\alpha+i\sqrt{2})/\mathbb{Q}$ *est une sous-extension de* $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ *de même degré* 8*, d'où l'égalité cherchée.*

(5) Soient $\sigma = u_{2,2,2}$ et $\tau = u_{1,1,2}$, ce sont des éléments de $G = \mathrm{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$. Montrer

(a) que $\circ(\sigma) = 4$, $\circ(\tau) = 2$, $\tau\sigma = \sigma^3\tau$, que

$$G =< \sigma, \tau >= \left\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\right\},$$

Ce sont simplement des calculs, toutes ces formules se montrent en examinant les actions des automorphismes sur α *et* $i\sqrt{2}$ *; il ne faut pas oublier de vérifier que la présentation donnée de* G *dans l'énoncé possède bien* 8 *éléments (distincts).*

(b) que $\mathbb{Q}(\alpha, \beta)^{<\tau>} = \mathbb{Q}(\alpha)$, que $\mathbb{Q}(\alpha, \beta)^{<\sigma>} = \mathbb{Q}(i\sqrt{6})$ et que $\mathbb{Q}(\alpha, \beta)^{<\sigma\tau>} = \mathbb{Q}(\alpha - \beta)$.

$< \tau >$ *est d'ordre* 2 *donc* $\mathbb{Q}(\alpha, \beta)^{<\sigma\tau>}$ *est de degré* 4 *sur* $\mathbb{Q}$*, on vérifie que* $< \tau >$ *laisse* α *fixe, qui est de degré* 4 *sur* $\mathbb{Q}$*, d'où la formule cherchée. De même* $< \sigma >$ *est d'ordre* 4*, donc* $\mathbb{Q}(\alpha, \beta)^{<\sigma>}/\mathbb{Q}$ *est de degré* 2 *; on voit que* $i\sqrt{6}$ *est stable par* σ *et est de degré* 2 *sur* $\mathbb{Q}$*, etc.*

IV. Les questions (4) et (7) de ce problème sont facultatives, elles ne contribuent qu'à donner un supplément de points[1].

Soient p un nombre premier, $\mathbb{F}_p$ un corps à p éléments, $K = \mathbb{F}_p(T)$ un corps de fractions rationnelles et K^{alg} une clôture algébrique de K. Soit le polynôme

$$P(X) = X^{p^2} - TX^p - T \in K[X],$$

soient $\alpha \in K^{\mathrm{alg}}$ une racine de $P(X)$ et $\beta, \gamma \in K^{\mathrm{alg}}$ tel que

$$\beta^p = T \quad , \quad \gamma^{p(p-1)} = T.$$

(1) Montrer que $\gamma^{p-1} = \beta$ et que $\beta = \alpha^p/(\alpha + 1)$.

Évident.

(2) Montrer que $P(X)$ est irréductible sur K.

On utilise le critère d'Eisenstein pour l'anneau factoriel $\mathbb{F}_p[T]$ *et son irréductible* T.

[1]l'inséparabilité n'ayant pas été suffisamment traitée en travaux dirigés.

(3) Montrer que l'ensemble des racines de $P(X)$ dans K^{alg} est
$$\{\alpha + \lambda\gamma \;/\; \lambda \in \mathbb{F}_p\}\,.$$
Quel est le cardinal de cet ensemble ?

On cherche les racines de $P(X)$ sous la forme $\alpha + u$, il vient
$$P(\alpha+u) = P(\alpha) + u^{p^2} - Tu^p = (u^p - \beta u)^p,$$
donc $P(\alpha+u) = 0$ si et seulement si $u(u^{p-1} - \beta) = 0$, d'où le résultat attendu. Le nombre de racines distinctes de $P(X)$ (dans K^{alg}) est p.

(4) Montrer que l'extension $K(\beta)/K$ est de degré p et est purement inséparable, que l'extension $K(\gamma)/K(\beta)$ est de degré $p-1$ et est séparable.

On voit, avec par exemple le critère d'Einsenstein appliqué à l'anneau factoriel $\mathbb{F}_p[T]$ et son irréductible T, que $\operatorname{irr}(\beta, K, X) = X^p - T$, ce polynôme n'a qu'une seule racine (dans K^{alg}), ce qui monte que le nombre de K-homomorphismes de $K(\beta)$ dans K^{alg} est 1.

Le polynôme minimal de γ sur $K(\beta)$ divise $X^{p-1} - \beta$, il est donc de degré $< p$, par suite de degré premier à p, donc l'extension $K(\gamma)/K(\beta)$ est séparable.

(5) Montrer que l'extension $K(\alpha^p)/K$ est de degré p et séparable, que l'extension $K(\alpha)/K(\alpha^p)$ est de degré p et purement inséparable.

On a $\operatorname{irr}(\alpha^p, K, X) = X^p - TX - T$ et ce polynôme est séparable.

On sait que l'extension $K(\alpha)/K$ est de degré p^2, que l'extension $K(\alpha^p)/K$ est de degré p, donc $K(\alpha)/K(\alpha^p)$ est de degré p, par suite $\operatorname{irr}(\alpha, K(\alpha^p), X) = X^p - \alpha^p$ et ce polynôme n'a qu'une seule racine (dans K^{alg}).

(6) Montrer que $K(\alpha,\gamma)$ est une extension normale de K de degré $p^2(p-1)$, de degré de séparabilité $p(p-1)$.

On a le diagramme
$$\begin{tikzcd} K \arrow[r, "p"] & K(\beta) \arrow[rr, "p"] \arrow[dr] & & K(\alpha) \arrow[r] & K(\alpha,\gamma) \\ & & K(\gamma) \arrow[ur] & & \end{tikzcd}$$

L'extension $K(\gamma)/K(\beta)$ est galoisienne, on a $K(\gamma) \cap K(\alpha) = K$ puisque ces deux corps ont des degrés premiers entre eux, d'après un théorème du cours il suit en particulier que $[K(\alpha,\gamma) : K(\alpha)] = [K(\gamma) : K(\beta)] = p-1$; ceci montre que $[K(\alpha,\gamma) : K] = p^2(p-1)$. D'autre part dans le diagramme précédent, *la seule extension qui possède de l'inséparabilité est $K(\beta)/K$, qui est ttalement inséparable. Donc le egré d'inséparabilité de $K(\alpha,\gamma)/K$ est p. Enfin $[K(\alpha,\gamma)/K$ est normale car $K(\alpha,\gamma)/K$ est un corps de décomposition de $P(X)$ sur K.*

(7) Soit $G = \mathrm{Gal}(K(\alpha,\gamma)/K)$, montrer que

$$(K(\alpha,\gamma))^G = K(\beta).$$

Compte tenu du calcul précédent du degré de séparabilité on sait que $K(\alpha,\gamma)/K(\alpha,\gamma)^G$ est de degré $p(p-1)$, donc $K(\alpha,\gamma)^G/K$ est de degré p ; on vérifie que $K(\alpha,\gamma)^G$ contient β, l'égalité cherchée vient alors de l'égalité des degrés de $K(\alpha,\gamma)^G$ et $K(\beta)$ sur K.

(8) On munit $\mathbb{F}_p \times \mathbb{F}_p^\times$ de l'opération définie par

$$(\lambda,\mu)\cdot(\lambda',\mu') = (\lambda+\mu\lambda', \mu\mu'),$$

on sait, ou on admet, que pour cette loi $\mathbb{F}_p \times \mathbb{F}_p^\times$ est un groupe (c'est un produit semi-direct standard). Montrer qu'il existe une application

$$G \to \mathbb{F}_p \times \mathbb{F}_p^\times \ , \ \sigma \mapsto \big(\gamma^{-1}(\sigma(\alpha)-\alpha), \gamma^{-1}\sigma(\gamma)\big)$$

et que cette application est un isomorphisme de groupes.

Un élément s de G est complètement déterminé par $s(\alpha)$ et $s(\gamma)$.