Contrôle du 9/12/2016

Exercice 1 :

Soit $i \in \mathbb{C}$ l'unité imaginaire complexe. Est-ce qu'il existe un polynôme $f(x) \in \mathbb{Q}[X]$ de degré 3, ayant pour racines $\sqrt{2}$, $\sqrt{2}+i$, $\sqrt{2}-i$?

Exercice 2 :

Question de cours : Soit K un corps de caractéristique nulle et L/K un corps de décomposition d'une famille de polynômes de $K[x]$. Démontrer que si $A(x) \in K[x]$ est un polynôme irréductible, et si A possède une racine dans L alors toutes les racines de A sont dans L.

Soit p un nombre premier. Soient $v = \sqrt[3]{p}$ et $u = \sqrt[3]{p} + \sqrt[3]{p^2}$.

1. Calculer le polynôme minimal $P(X)$ de u sur $\mathbb{Q}$;
2. Calculer les degrés $[\mathbb{Q}(u) : \mathbb{Q}]$ et $[\mathbb{Q}(v) : \mathbb{Q}]$;
3. Est-ce que $\mathbb{Q}(u) = \mathbb{Q}(v)$?
4. Calculer $(v-1)^{-1}$ dans la base $\{1, v, v^2, ...\}$ de $\mathbb{Q}(v)$ sur $\mathbb{Q}$.
5. Justifier que l'extension $\mathbb{Q}(u)$ ne peut pas être un corps de décomposition.
6. Soit Q le polynôme minimal de v sur $\mathbb{Q}$, et soient $L(P)$ et $L(Q)$ les corps de décompositions de P et Q respectivement sur $\mathbb{Q}$. Montrer que $L(P) = L(Q)$. (Utiliser la question de cours).
7. Calculer le corps de décomposition $L(P)$ du polynôme P.
8. Quel est le degré $[L(P) : \mathbb{Q}]$?
9. Montrer qu'un $\mathbb{Q}$-automorphisme $\sigma : L(P) \xrightarrow{\sim} L(P)$ stabilise u si et seulement si il stabilise v ;
10. Calculer le groupe des $\mathbb{Q}$-automorphismes de $L(P)$;
11. Trouver toutes les extensions intermédiaires $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(u)$.

Exercice 3 :

Soit p un nombre premier et soient k et k' deux corps finis de cardinaux p^n et p^m respectivement. Donner une condition nécessaire et suffisante pour qu'il existe un plongement $k \subseteq k'$?

Exercice 4 :

Soit k un corps fini de caractéristique p. Montrer que tout élément $a \in k$ admet une racine p-ème $a^{1/p}$ dans k. Plus généralement quelles sont les racines du polynôme $X^p - a$ dans k ?

SOLUTIONS :

Ex. 1 : Soit $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$ un polynôme ayant pour racines $\sqrt{2}, \sqrt{2}+i, \sqrt{2}-i$. Alors $f(x) = (x-\sqrt{2})(x-\sqrt{2}-i)(x-\sqrt{2}+i)$, et donc $a_0 = \sqrt{2}(\sqrt{2}-i)(\sqrt{2}+i) = 3\sqrt{2}$. Donc $f \notin \mathbb{Q}[x]$. (on peut aussi prendre $a_1 = -(\sqrt{2}+(\sqrt{2}+i)+\sqrt{2}-i) = -3\sqrt{2} \notin \mathbb{Q}$.

On paut également remarquer que le polynôme minimal de $\sqrt{2}$ est $P(x) = x^2 - 2$ et donc si $f \in \mathbb{Q}[x]$ alors P divise f, mais cela est absurde car par hypothèse $-\sqrt{2}$ n'est pas racine de f.

Ex. 2 :

Question de cours : Soit $\alpha \in L$ une racine de $A(x) \in K[x]$. Soit $\beta \in K^{\text{alg}}$ une autre racine de A. On a un isomorphisme K-linéaire $K[x]/(A(x)) \cong K(\alpha)$ qui envoie x dans α. De même, a un isomorphisme K-linéaire $K[x]/(A(x)) \cong K(\beta)$ qui envoie x dans β.

Il existe donc, par composition, un isomorphisme K-linéaire $\varphi : K(\alpha) \xrightarrow{\sim} K(\beta)$ qui envoie α dans β.

Par le théorème de prolongement des plongements on sait que l'isomorphisme $K(\alpha) \xrightarrow{\sim} K(\beta)$ se prolonge en un K-automorphisme de $\sigma : K^{\text{alg}} \xrightarrow{\sim} K^{\text{alg}}$. Cet isomorphisme envoie α dans β car $\sigma_{|K(\alpha)} = \varphi$.

Comme L est un corps de décomposition, il est stable par σ, c'est à dire $\sigma(L) = L$. Donc $\beta = \sigma(\alpha) \in L$. L'assertion en découle.

1. On a (grâce au fait que $v^3 = p$)

$$u^3 = (v+v^2)^3 = (p + 3v^2v^2 + 3vv^4 + p^2) = p + p^2 + 3pv + 3pv^2 = p + p^2 + 3pu.$$

Donc u est zéro du polynôme $x^3 - 3px - (p+p^2)$. C'est un polynôme d'Eisenstein, donc irréductible. C'est donc le polynôme minimal $P(x)$ de u.

2. On a $[\mathbb{Q}(u) : \mathbb{Q}] = \deg(P) = 3$.

De même, le polynôme $Q(x) = x^3 - p$ est d'Eisenstein, donc irréductible. C'est donc le polynôme minimal de $v = \sqrt[3]{p}$, et on a $[\mathbb{Q}(v) : \mathbb{Q}] = \deg(Q) = 3$.

3. On a $\mathbb{Q}(u) = \mathbb{Q}(v)$. En effet, comme $u = v + v^2$, alors on a immédiatement $\mathbb{Q}(u) \subseteq \mathbb{Q}(v)$. L'inclusion dans l'autre sens peut se voir de plusieurs manière différentes. D'une part, elle suit d'un calcul sur les degrés : $[\mathbb{Q}(v) : \mathbb{Q}] = [\mathbb{Q}(v) : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}]$ on en déduit (question 2) que $[\mathbb{Q}(v) : \mathbb{Q}(u)] = 1$ et donc $\mathbb{Q}(v) = \mathbb{Q}(u)$. D'autre part on

peut exprimer explicitement v en fonction de u :

$$\begin{aligned} u = v + v^2 \quad &\to \quad u^2 = v^2 + v^4 + 2v^3 \\ &\to \quad u^2 = v^2 + pv + 2p \\ &\to \quad u^2 = (v^2 + v) - v + pv + 2p \\ &\to \quad u^2 = u + (p-1)v + 2p \\ &\to \quad v = \frac{u^2 - u - 2p}{(p-1)} \end{aligned}$$

Cela montre que $v \in \mathbb{Q}(u)$ et donc $\mathbb{Q}(v) \subseteq \mathbb{Q}(u)$.

Par curiosité, une autre expression de v en fonction de u est la suivante :

$$p - 1 = v^3 - 1 = (v-1)(1 + v + v^2) = (v-1)(1+u)$$

donc

$$v = \frac{p-1}{u+1} + 1 \quad \in \mathbb{Q}(u) \ .$$

4. Une base de $\mathbb{Q}(v)$ est $1, v, v^2$. L'inverse de $v-1$ est de la forme $a + bv + cv^2$, avec $a, b, c \in \mathbb{Q}$. La condition $(v-1)(a+bv+cv^2) = 1$ donne

$$1 = av + bv^2 + cv^3 - a - bv - cv^2 = (cp - a) + (a-b)v + (b-c)v^2$$

Comme $1, v, v^2$ est une base, on a $pc - a = 1$, $a - b = 0$ et $b - c = 0$. Donc $a = b = c = \frac{1}{p-1}$, et

$$\frac{1}{v-1} = \frac{1}{p-1}(1 + v + v^2).$$

Si on était malins, on aurait aussi pu voir directement que

$$\frac{1}{(v-1)} = \frac{1+v+v^2}{(v-1)(1+v+v^2)} = \frac{1+v+v^2}{v^3-1} = \frac{1+v+v^2}{p-1} \ .$$

5. Si le corps $M = \mathbb{Q}(u)$ était un corps de racines, alors il aurait la propriété évoquée dans la question de cours. Mais, par le point 3 on a $M = \mathbb{Q}(v)$ et donc si j est une racine 3-ème *primitive* de l'unité on aurait $v, jv, j^2v \in M$, car $\{v, jv, j^2v\}$ sont les trois racines de Q. Cela entrainerait $j = jv/v \in M$. Mais $M \subseteq \mathbb{R}$ (car $v \in \mathbb{R}$), et donc cela est absurde car il n'y a pas de racines 3-èmes primitives de l'unité dans $\mathbb{R}$.

Donc M ne peut pas être un corps de racines.

6. L'extension $L(Q) = \mathbb{Q}(v, jv, j^2v)$ contient $\mathbb{Q}(v)$. Mais $\mathbb{Q}(v) = \mathbb{Q}(u)$, donc $u \in L(Q)$. Par la propriété évoquée au point 5, les autres racines de P sont dans $L(Q)$ et donc $L(P) \subseteq L(Q)$.

L'inclusion réciproque se voit exactement de la même manière : $\mathbb{Q}(v) = \mathbb{Q}(u) \subseteq L(P)$, donc les autres racines de Q sont dans $L(P)$, donc $L(Q) \subseteq L(P)$.

7. Par le point 6 on a $L(P) = L(Q)$. On voit que $L(Q) = \mathbb{Q}(v, jv, j^2v) = \mathbb{Q}(j, v)$. En effet l'inclusion $\subseteq$ résulte du fait que $jv, j^2v \in \mathbb{Q}(j, v)$ et l'inclusion $\supseteq$ résulte du fait que $j = jv/v \in \mathbb{Q}(v, jv, j^2v)$.

8. On a vu que $j \notin \mathbb{Q}(v)$. Le polynôme minimal de j sur $\mathbb{Q}$ est $\Phi_3(x) := X^2 + X + 1$ (polynôme cyclotomique). Φ_3 n'a donc pas de racines dans $\mathbb{Q}(v)$ et est alors irréductible dans $\mathbb{Q}(v)[x]$ car c'est un polynôme de degré 2. Donc $\mathbb{Q}(j)[x]/(\Phi_3(x)) \cong \mathbb{Q}(v)(j) = \mathbb{Q}(v, j)$. Donc $[\mathbb{Q}(v, j) : \mathbb{Q}(v)] = \deg(\Phi_3) = 2$. Par conséquence, grâce au point 7, on a $[L(Q) : \mathbb{Q}] = [\mathbb{Q}(v, j) : \mathbb{Q}(v)][\mathbb{Q}(v) : \mathbb{Q}] = 2 \cdot 3 = 6$.

9. L'automorphisme $\sigma : L \xrightarrow{\sim} L$ stabilise u si, et seulement si, il stabilise $\mathbb{Q}(u)$. De même il stabilise v si, et seulement si, il stabilise $\mathbb{Q}(v)$. Mais $\mathbb{Q}(u) = \mathbb{Q}(v)$, donc σ stabilise u si, et seulement si, il stabilise v.

On peut également observer que si σ stabilise v alors $\sigma(u) = \sigma(v + v^2) = \sigma(v) + \sigma(v)^2 = v + v^2 = u$, et réciproquement on peut utiliser les expressions de v en fonction de u qu'on a trouvé avant pour montrer que si σ stabilise u, alors

$$\sigma(v) = \sigma\Big(\frac{p-1}{u+1} + 1\Big) = \frac{p-1}{\sigma(u)+1} + 1 = \frac{p-1}{u+1} + 1 = v \ .$$

10. On a vu que $L(P) = \mathbb{Q}(j, v)$. L'extension $\mathbb{Q}(j)/\mathbb{Q}$ a degré 2 car le polynôme minimal de j est $X^2 + X + 1$ (polynôme cyclotomique). Donc $\mathbb{Q}(j)/\mathbb{Q}$ est un corps de rupture (car on a vu que toute extension de degré 2 est un corps de rupture). Maintenant, tout élément $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(j))$ envoyé j dans une autre racine de $x^2 + x + 1$ (i.e. dans j ou j^2), et σ est determiné une fois donné l'image de j (car j engendre l'extension $\mathbb{Q}(j)$). Le groupe $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(j))$ a donc deux éléments : l'identité et un automorphisme σ qui échange j et j^2.

Par le théorème vu en classe, ces deux automorphismes se prolongent à des $\mathbb{Q}$-automorphismes de $\mathbb{Q}^{\mathrm{alg}}$. Par ailleurs tout $\mathbb{Q}$-automorphisme de $\mathbb{Q}^{\mathrm{alg}}$ stabilise globalement les corps de rupture, donc nous avons un $\mathbb{Q}$-automorphisme $\widetilde{\sigma}$ de $L(P)$ dont la restriction à $\mathbb{Q}(j)$ est σ.

Maintenant regardons le groupe $\mathrm{Aut}_{\mathbb{Q}(j)}(\mathbb{Q}(j,v))$. On sait que $[\mathbb{Q}(j,v):\mathbb{Q}]=6$, donc $[\mathbb{Q}(j,v):\mathbb{Q}(j)]=3$. Le polynôme minimal $A(x)$ de v sur $\mathbb{Q}(j)$ a donc degré 3, et comme A divise x^3-p on a $A(x)=x^3-p$. Maintenant, $\mathbb{Q}(j,\sqrt{2})$ contient les trois racines de x^3-p qui sont v, jv, j^2v. On sait que les $\mathbb{Q}(j)$-automorphismes de $\mathbb{Q}^{\mathrm{alg}}$ permutent transitivement les racines des polynômes irréductibles. Donc, plus précisément, il existent deux $\mathbb{Q}(j)$-automorphismes ϕ_1,ϕ_2 de $\mathbb{Q}^{\mathrm{alg}}$ tels que $\phi_1(v)=jv$ et $\phi_2(v)=j^2v$. Comme avant, ϕ_1 et ϕ_2 stabilisent globalement $L(P)$, mais cette fois leur restriction à $\mathbb{Q}(j)$ est l'identité. Un $\mathbb{Q}(j)$-automorphisme de $\mathbb{Q}(j,v)$ est déterminé par l'image de v, donc le groupe $\mathrm{Aut}_{\mathbb{Q}(j)}(\mathbb{Q}(j,v))$ compte exactement 3 éléments $\{\mathrm{Id},\phi_1,\phi_2\}$. Il est donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$ car il n'y a pas d'autres groupes d'ordre 3.

En composant les éléments de $\mathrm{Aut}_{\mathbb{Q}(j)}(\mathbb{Q}(j,v))$ avec $\widetilde{\sigma}$ on trouve les $\mathbb{Q}$- automorphismes $\{\widetilde{\sigma},\widetilde{\sigma}\circ\phi_1,\widetilde{\sigma}\circ\phi_2\}$. Chacun de ces $\mathbb{Q}$-automorphismes agit comme σ sut $\mathbb{Q}(j)$.

On a donc 6 automorphismes de $L(P)$:

$$\{\mathrm{Id},\phi_1,\phi_2,\widetilde{\sigma},\widetilde{\sigma}\circ\phi_1,\widetilde{\sigma}\circ\phi_2\}\ . \tag{1}$$

J'affirme qu'on n'a pas d'autres automorphismes. La raison est que $L(P)=\mathbb{Q}(j,v)$ est engendré par un seul élément (dit primitif), on peut prendre par exemple l'élément $w:=j+v$.

En effet, son polynôme minimal est compliqué à calculer, mais on sait que si $Irr(w,\mathbb{Q})\in\mathbb{Q}[x]$ est le polynôme minimal de w sur $\mathbb{Q}$, alors d'une part $\deg Irr(w,\mathbb{Q})=[\mathbb{Q}(w):\mathbb{Q}]$ divise le degré $[L(P):\mathbb{Q}]=6$ car $w\in L(P)$, et donc $Irr(w,\mathbb{Q})$ a au plus 6 racines. D'autre part les $\mathbb{Q}$-automorphismes de $L(P)$ permutent transitivement les racines de $Irr(w,\mathbb{Q})$, et on voit facilement que les 6 éléments

$$\{w,\phi_1(w),\phi_2(w),\widetilde{\sigma}(w),\widetilde{\sigma}\circ\phi_1(w),\widetilde{\sigma}\circ\phi_2(w)\}=\{v{+}j,\ jv{+}j,\ j^2v{+}j,\ v{+}j^2,\ jv{+}j^2,\ j^2v{+}j^2\}$$

sont tous différents (par exemple l'égalité $jv{+}j^2=j^2v{+}j$ équivaut à $j^2(v{-}1)=j(v{-}1)$, et comme $v\neq 1$ ça entraine $j=j^2$ ce qui est faux). Donc ces six élément sont *toutes* les racines de $Irr(w,\mathbb{Q})$ qui a donc degré *égal* à 6. Donc $\mathbb{Q}(w)=L(P)$.

Or, comme $L(P)=\mathbb{Q}(w)$, on sait que les automorphismes de $\mathrm{Aut}_{\mathbb{Q}}(L(P))$ sont déterminés par l'image de w, et il n'y a que 6 possibilités. Donc il n'y a que 6 $\mathbb{Q}$-automorphismes de $L(P)$ et $\mathrm{Aut}_{\mathbb{Q}}(L(P))$ est donné par les 6 éléments listé dans (1) ci plus haut.

Il n'y a que 2 groupes d'ordre 6 : S_3 et $\mathbb{Z}/6\mathbb{Z}\cong\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

J'affirme que le groupe $\mathrm{Aut}_{\mathbb{Q}}(L(P))$ n'est pas commutatif et doit donc être isomorphe à S_3. Montrons par exemple que $\widetilde{\sigma}\circ\phi_1\neq\phi_1\circ\widetilde{\sigma}$. Cela résulte du fait que $\phi_1(j^k\cdot v)=\phi_1(j)^k\cdot\phi_1(v)=j^k\cdot jv=j\cdot j^kv$. Donc ϕ_1 agit par multiplication par j sur les éléments de la forme j^kv. Or, on ne connait pas exactement $\widetilde{\sigma}$, mais on sait

qu'il doit permuter les racines de $x^3 - p$, donc il est de la forme $\widetilde{\sigma}(v) = j^k v$ pour un $k \in \{0, 1, 2\}$ convenable, et alors (grâce à ce qu'on a dit une ligne plus haut) l'action de ϕ_1 sur $\widetilde{\sigma}(v)$ est donné par la multiplication par j. On trouve

$$\phi_1 \circ \widetilde{\sigma}(v) = j \cdot \widetilde{\sigma}(v)\ , \qquad \widetilde{\sigma} \circ \phi_1(v) = \widetilde{\sigma}(jv) = \widetilde{\sigma}(j) \cdot \widetilde{\sigma}(v) = \sigma(j) \cdot \widetilde{\sigma}(v) = j^2 \cdot \widetilde{\sigma}(v)$$

Donc $\phi_1 \circ \widetilde{\sigma} \neq \widetilde{\sigma} \circ \phi_1$ et le groupe n'est pas commutatif.

11. On a $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Si $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(u)$ est une extension intermédiaire on doit avoir $[\mathbb{Q}(u) : F][F : \mathbb{Q}] = 3$. Donc $[F : \mathbb{Q}]$ est égal à 1 ou 3. Dans le premier cas $F = \mathbb{Q}$, dans le deuxième cas $F = \mathbb{Q}(u)$. Il n'y a donc que 2 extensions intermédiaires.

Ex. 3 : Soit p^n le cardinal de k et p^m le cardinal de k'. Pour que k soit contenu dans k' il faut et il suffit que $n|m$. En effet cette condition est nécessaire car si $k \subseteq k'$ alors on a un isomorphisme de k-espaces vectoriels $k' \cong k^s$ où $s := [k' : k]$ est le degré de l'extension. Donc le cardinal p^m de k' est celui de k à la puissance s : $p^m = (p^n)^s$ et $m = ns$.

Pour montrer que la condition $n|m$ est suffisante fixons une clôture algébrique $\mathbb{F}_p^{\text{alg}}$ de $\mathbb{F}_p$, et fixons deux plongements $k' \to \mathbb{F}_p^{\text{alg}}$ et $k \to \mathbb{F}_p^{\text{alg}}$. Comme le groupe multiplicatif de k est cyclique d'ordre $p^n - 1$, tout élément de k vérifie $x^{p^n} = x$. Comme le polynôme $x^{p^n} - x$ est de degré p^n ses racines s'identifient a l'ensemble sous-jacent à k (qui est donc un corps de décomposition). De même les éléments de k' s'identifient aux éléments de $\mathbb{F}_p^{\text{alg}}$ tels que $x^{p^m} = x$. Autrement dit, si $F : \mathbb{F}_p^{\text{alg}} \to \mathbb{F}_p^{\text{alg}}$ désigne l'application de Frobenius $F(a) = a^p$, alors k s'identifie à l'ensemble des points fixes par F^n et k' s'identifie à l'ensemble des points fixes par F^m.

Or, si $m = ns$ et si $x \in k$ alors $F^n(x) = x$, donc

$$F^m(x) = F^{ns}(x) = \overbrace{F^n \circ \cdots \circ F^n}^{s-\text{fois}}(x) = x$$

Donc $F^m(x) = x$ et $x \in k'$. Cela montre que $k \subseteq k'$ dans $\mathbb{F}_p^{\text{alg}}$.

Ex. 4 : Si k est un corps fini d'ordre p^n, alors tout élément $a \in k$ vérifie $a^{p^n} = a$. Donc l'élément $b := a^{p^{n-1}}$ vérifie $b^p = a$. Tout élément a donc une racine p-ème.

Le polynôme $X^p - a$ n'a qu'une seule racine b avec multiplicité p car $X^p - a = (X - b)^p$.

On aurait pu observer que l'application de Frobenius $x \mapsto x^p$ est un AUTOmorphisme de corps [1] en particulier elle est bijective et donc tout $a \in k$ a un unique antécédent, en d'autres termes l'équation $x^p = a$ a une, et une seule, solution.

1. On rappelle que c'est un homomorphisme d'anneau, donc son noyau est nul car k est un corps,

et comme il est injectif il est aussi surjectif car le corps est fini et on a égalité entre les cardinaux de k et de son image.