L3 Algèbre. Exercices Feuille 5.

1) a) Montrer que 2 est un générateur du groupe multiplicatif $\mathbb{F}_{19}^*$.
Quels sont les autres générateurs ?
b) Montrer que l'application

$$\begin{aligned} f &: \mathbb{Z}/18\mathbb{Z} \to \mathbb{F}_{19}^* \\ &: k \mapsto 2^k \end{aligned}$$

est un isomorphisme de groupes.
c) Utiliser f^{-1} noté L_2 pour résoudre l'équation $11.x^4 = 1\ mod(19)$.

2)a) Montrer que 24 est une racine carrée de 2 dans $\mathbb{F}_{41}$.
b) Déterminer toutes les racines de $X^2 - 3X + 12$ dans $\mathbb{F}_{41}$.

3) a) Quel est le degré de l'extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(i, \sqrt[4]{2})$
b) L'élément $\alpha = \sqrt[4]{2} + i\sqrt[4]{2}$ est-il un élément primitif de cette extension?
c) Soit $\beta = \sqrt[4]{2} + 2i\sqrt[4]{2}$. Montrer que

$$\begin{aligned} \beta^2 + 3\sqrt{2} &= 4i\sqrt{2} \\ \beta^4 + 6\sqrt{2}\beta^2 &= -50 \end{aligned}$$

En déduire que $\sqrt{2} \in \mathbb{Q}(\beta)$, $i\sqrt{2} \in \mathbb{Q}(\beta), i \in \mathbb{Q}(\beta), \sqrt[4]{2} \in \mathbb{Q}(\beta)$.
L'élément β est-il un élément primitif de cette extension?

4)a) Soit $P(X) = X^4 - 12X^2 + 25$ calculer $P(X + 1)$.
Montrer que P est irréductible sur $\mathbb{Q}$.
Trouver toutes les racines dans $\mathbb{C}$ du polynôme $X^4 - 12X^2 + 25$.
b) Soient

$$\alpha = \sqrt{6 + \sqrt{11}} \text{ et } \beta = \sqrt{6 - \sqrt{11}}$$

Déterminer le polynôme minimal de α sur $\mathbb{Q}$.
c) Soit $N \hookrightarrow \mathbb{C}$ le corps de décomposition de P est-ce que $N = \mathbb{Q}(\alpha)$?
d) Déterminer le groupe $Aut_{\mathbb{Q}}N$.

L3 Algèbre. Exercices. Feuille 5. Corrigé.

1) a) Pour montrer que 2 est un générateur du groupe multiplicatif $\mathbb{F}_{19}^*$ on calcule les 2^k, $k = 0, ..., 17$ (modulo 19) et on constate qu'on a une et une seule fois les 18 élements de $\mathbb{F}_{19}^*$.
Les autres générateurs seront du type 2^k pour les k premiers avec 18.
b) L'application f est un morphisme du groupe $(\mathbb{Z}/18\mathbb{Z}, +)$ dans le groupe multiplicatif $\mathbb{F}_{19}^*$ et elle est bijective.
c) Les solutions de cette équation définissent des éléments qui sont dans $\mathbb{F}_{19}^*$. On transforme donc l'équation $11.x^4 = 1\ mod(19)$ par L_2, ce qui donne dans$\mathbb{Z}/18\mathbb{Z}$ l'équation

$$L_2(11) + 4L_2(x) = L_2(1) = 0$$

ou $12 + 4y = 0$ en posant $y = L_2(x)$.

L'équation $12+4y=0\ (mod 18)$ donne $y=3\ (mod 18)$ ou $y=12\ (mod 18)$. On revient ensuite à x au moyen de f ce qui donne

$x=8\ (mod 19)$ ou $x=11\ (mod 19)$

2)a) On a $24^2=576=14.41+2$ d'où $24^2=2$ dans $\mathbb{F}_{41}$.

b)Le discriminant de de $X^2-3X+12$ est $\Delta=9-4.12=-39=9=24^2$ dans $\mathbb{F}_{41}$. Donc on a

$$x=2^{-1}(3\pm 24)=-20((3\pm 24)$$

ce qui donne $x=34$ ou $x=10$ dans $\mathbb{F}_{41}$.

3) a) Le degré de l'extension $\mathbb{Q}\hookrightarrow\mathbb{Q}(i,\sqrt[4]{2})$ est 8 car on l'écrit

$$\mathbb{Q}\hookrightarrow\mathbb{Q}(\sqrt[4]{2})\hookrightarrow\mathbb{Q}(\sqrt[4]{2})(i)$$

la première est de degré 4 (le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}$) est X^2-4 irréductible sur $\mathbb{Q}$), la seconde de degré 2 (le polynôme minimal de i sur $\mathbb{Q}(\sqrt[4]{2})$ est X^2+1 (irréductible sur $\mathbb{Q}(\sqrt[4]{2})$) et on utilise le th. de multiplicativité des degrés.

b) On a $\alpha^2=2i\sqrt{2}$ d'où $\alpha^4=-8$, donc α est de degré inférieur à 4 sur $\mathbb{Q}$ et ne peut être élément primitif de $\mathbb{Q}\hookrightarrow\mathbb{Q}(i,\sqrt[4]{2})$ qui est de degré 8.

c) On vérifie facilement que

$$\begin{aligned}\beta^2+3\sqrt{2} &= 4i\sqrt{2}\\ \beta^4+6\sqrt{2}\beta^2 &= -50\end{aligned}$$

donc $\sqrt{2}\in\mathbb{Q}(\beta)$ par la deuxième équation, ensuite $i\sqrt{2}\in\mathbb{Q}(\beta)$ par la première, d'où $i=\frac{i\sqrt{2}}{\sqrt{2}}\in\mathbb{Q}(\beta)$ et $\sqrt[4]{2}=\beta/(1+2i)\in\mathbb{Q}(\beta)$.

Comme $i\in\mathbb{Q}(\beta)$ et $\sqrt[4]{2}=\in\mathbb{Q}(\beta)$ on a $\mathbb{Q}(i,\sqrt[4]{2})\subset\mathbb{Q}(\beta)$ et comme $\beta\in\mathbb{Q}(i,\sqrt[4]{2})$ on a on a $\mathbb{Q}(i,\sqrt[4]{2})\supset\mathbb{Q}(\beta)$ donc β est un élément primitif de cette extension.

4)a) On a $P(X+1)=X^4+4X^3-6X^2-20X+14$, le pollynôme $P(X+1)$ est irréductible sur $\mathbb{Q}$ par le critère D'Eisenstein (avec p=2), donc P aussi.

Les racines dans $\mathbb{C}$ du polynôme $(X^2)^2-12(X^2)+25$

$$\pm\sqrt{6+\sqrt{11}}\text{ et }\pm\sqrt{6-\sqrt{11}}$$

b)Le polynôme minimal de α sur $\mathbb{Q}$ est P

c) On a $\beta=5/\alpha$ donc $N\subset Q(\alpha)$ et comme $\alpha\in N$ on a $N=\mathbb{Q}(\alpha)$

d) Si $f\in Aut_{\mathbb{Q}}N$ est déterminé par l'image de α, on a les cas suivants:

$f_1(\alpha)=\alpha$ donc $f_1(\beta)=f_1(5/\alpha)=5/f_1(\alpha)=5/\alpha=\beta$

$f_2(\alpha)=-\alpha$ donc $f_2(\beta)=f_2(5/\alpha)=5/f_2(\alpha)=5/-\alpha=-\beta$

$f_3(\alpha)=\beta$ donc $f_3(\beta)=f_3(5/\alpha)=5/f_3(\alpha)=5/\beta=\alpha$

$f_4(\alpha)=-\beta$ donc $f_4(\beta)=f_4(5/\alpha)=5/f_4(\alpha)=5/-\beta=-\alpha$

On voit donc que $Aut_{\mathbb{Q}}N$ a quatre éléments et qu'il est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.