Exercice 5.6, corrigé

Exercice 5.6. Notons $\alpha = \sqrt[8]{2}$ et $\xi = \mathrm{e}^{i\pi/4} = (1+i)/\sqrt{2}$. L'élément ξ est une racine primitive 8-ième de l'unité et appartient à K. On peut noter aussi que $\xi^2 = i$. De plus, les racines de $X^8 - 2$ sont les nombres $\xi^k\alpha$, avec $k \in \{0, \dots, 7\}$. De plus, on a $K = \mathbb{Q}(\alpha, \xi)$. Ainsi K est corps de décomposition de $X^8 - 2$ sur $\mathbb{Q}$. C'est donc une extension normale de $\mathbb{Q}$, également séparable puisqu'on est en caractéristique 0, donc galoisienne. On sait qu'alors K/k est galoisienne, pour toute extension intermédiaire $\mathbb{Q} \subset k \subset K$. Pour finir ces remarques préliminaires, on calcule $[K : \mathbb{Q}]$ en utilisant la décomposition $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$. Comme $X^8 - 2$ est irréductible sur $\mathbb{Q}$ par Eisenstein pour $p = 2$, on voit que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$. Comme $\mathbb{Q}(\alpha) \subset \mathbb{R}$, on voit que $X^2 + 1$ est irréductible sur $\mathbb{Q}(\alpha)$ puisqu'il n'y a pas de racine. Ceci montre que $[K : \mathbb{Q}(\alpha)] = 2$ et finalement $[K : \mathbb{Q}] = 16$. Pour chaque $i = 1, 2, 3$ on a $[k_i : \mathbb{Q}] = 2$, donc $[K : k_i] = 8$.

Posons $G_i = G(K/k_i)$. C'est un groupe d'ordre 8.

Étudions l'extension K/k_1. Comme α engendre K/k_1, un automorphisme $\sigma \in G_1$ est déterminé par la valeur $\sigma(\alpha)$ qui est de la forme $\xi^k\alpha$ pour un certain $k \in \{0, \dots, 7\}$. Il y a donc 8 possibilités pour σ. Comme G_1 est d'ordre 8, toutes ces possibilités définissent un (unique) automorphisme, en particulier il existe un automorphisme τ tel que $\tau(\alpha) = \xi\alpha$. Pour montrer que G_1 est cyclique, il suffit de montrer que τ l'engendre, et pour cela il suffit de montrer que les valeurs $\tau^k(\alpha)$ sont toutes distinctes. Ici il faut prendre garde au fait que la valeur $\tau(\xi)$, qui est uniquement déterminée, n'a pas de raison d'être ξ. (On a $\tau(i) = i$, ce qui ne suffit pas.) En particulier on ne peut pas écrire $\tau^k(\alpha) = \xi^k\alpha$, ce qui est d'ailleurs faux. En fait, utilisant le fait que $\xi^8 = 1$ on trouve $\tau(\xi) = \tau((1+i)/\alpha^4) = (1+i)/(\xi\alpha)^4 = -(1+i)/\alpha^4 = -\xi$. On calcule alors directement :

k	0	1	2	3	4	5	6	7
$\tau^k(\alpha)$	α	$\xi\alpha$	$\xi^6\alpha$	$\xi^7\alpha$	$\xi^4\alpha$	$\xi^5\alpha$	$\xi^2\alpha$	$\xi^3\alpha$

Ces valeurs sont toutes distinctes, donc les τ^k tous distincts, donc $G_1 = \langle\tau\rangle \simeq \mathbb{Z}/8\mathbb{Z}$.

Étudions maintenant K/k_2. Soit $\sigma \in G_2$. Alors il existe k tel que $\sigma(\alpha) = \xi^k\alpha$. Par ailleurs, du fait que $\sigma(\sqrt{2}) = \sqrt{2}$ il découle que $\xi^{4k}\alpha^4 = \sigma(\alpha^4) = \sigma(\sqrt{2}) = \sqrt{2} = \alpha^4$. Comme ξ est d'ordre 8, ceci impose que $k = 2\ell$ pour un $\ell \in \{0, \dots, 3\}$, donc $\sigma(\alpha) = \xi^{2\ell}\alpha = i^\ell\alpha$. Par ailleurs $\sigma(i) = \epsilon i$ pour un $\epsilon \in \{1, -1\}$. Comme α et i engendrent K/k_2, l'automorphisme σ est déterminé par le couple $(\sigma(\alpha), \sigma(i)) \in \{0, \dots, 3\} \times \{1, -1\}$. Ceci fait au plus 8 possibilités pour σ. Ici encore, comme G_2 est d'ordre 8, toutes ces possibilités définissent en effet un (unique) automorphisme. Parmi ces automorphismes on peut considérer les deux automorphismes particuliers λ, μ définis ainsi : $\lambda(\alpha) = i\alpha$ et $\lambda(i) = i$; $\mu(\alpha) = \alpha$ et $\mu(i) = -i$. On vérifie facilement que $\lambda^4 = \mu^2 = (\lambda\mu)^2 = \mathrm{id}$. Ce sont les relations qui définissent le groupe diédral à huit éléments D_4, donc $G_2 \simeq D_4$.

Étudions enfin K/k_3. Il s'agit de montrer que $G_3 \simeq Q_8$, et pour cela bien sûr il faut connaître un peu le groupe des quaternions d'ordre 8. Quelques « rappels » : il y a 5 classes d'isomorphisme de groupes d'ordre 8, dont 3 abéliens : $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ et $(\mathbb{Z}/2\mathbb{Z})^3$, et 2 non abéliens : D_4 et Q_8. Parmi les non abéliens, on peut distinguer Q_8 comme le groupe possédant 1 seul élément d'ordre 2 (en effet D_4 en possède 5), ou alors comme le groupe possédant 6 éléments d'ordre 4 (en effet D_4 en possède seulement 2) qui ont tous le même carré, égal au seul élément d'ordre 2. Il existe bien d'autres caractérisations de Q_8, qui par ailleurs peut se décrire explicitement par $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ où -1 est central (il engendre le centre qui est $\simeq \mathbb{Z}/2\mathbb{Z}$) et $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $ik = -ki = -j$, $jk = -kj = i$. Revenons à notre extension. On note que $\sqrt{-2} = i\sqrt{2} = \xi^2\alpha^4$. L'extension K/k_3 est engendrée par α : en effet, la sous-k_3-extension de K engendrée par α contient $i\sqrt{2}$ et α, donc aussi $(i\sqrt{2})/\alpha^4 = i$, donc c'est K. Tout élément $\sigma \in G_3$ est déterminé par $\sigma(\alpha) = \xi^k\alpha$ avec $k \in \{0, \dots, 7\}$. Comme précédemment, puisque G_3 est d'ordre 8 on en déduit que toutes les possibilités se produisent. Continuons à décrire l'automorphisme σ qui vérifie $\sigma(\alpha) = \xi^k\alpha$ en calculant $\sigma(\xi)$. De $\sigma(\alpha) = \xi^k\alpha$ on tire $\sigma(\sqrt{2}) = \xi^{4k}\sqrt{2} = (-1)^k\sqrt{2}$. De $\sigma(i\sqrt{2}) = i\sqrt{2}$ on tire alors $\sigma(i) = i\sqrt{2}/(-1)^k\sqrt{2} = (-1)^k i$. On trouve ensuite :

$$\sigma(\xi) = \sigma((1+i)/\sqrt{2}) = \sigma((1+(-1)^k i)/((-1)^k\sqrt{2}) = (-1)^k\xi^{(-1)^k}.$$

Utilisant le fait que $(-1)^{k^2} = (-1)^k = \xi^{4k}$, on en déduit que

$$\sigma^2(\alpha) = \sigma(\xi^k\alpha) = \sigma(\xi^k)\sigma(\alpha) = ((-1)^k\xi^{(-1)^k})^k\xi^k\alpha = \xi^{(5+(-1)^k)k}\alpha.$$

Comme $\xi^8 = 1$, seules les valeurs de $(5+(-1)^k)k$ modulo 8 sont importantes. Or pour $k \in \mathbb{Z}/8\mathbb{Z}$, on voit que cette fonction vaut tout le temps 4 sauf en $k = 0$ et $k = 4$ où elle vaut 0. Nommons σ_k l'automorphisme tel que $\sigma_k(\alpha) = \xi^k\alpha$. Ce qui précède signifie que $(\sigma_4)^2 = \mathrm{id}$ et que pour $k \neq 0, 4$ on a $(\sigma_k)^2(\alpha) = -\alpha$, ou dit autrement :

$$(\sigma_k)^2 = \sigma_4.$$

On voit que G_3 possède un élément d'ordre 2 et six éléments d'ordre 4, qui ont tous un carré égal à l'élément d'ordre 2. Ceci caractérise le groupe Q_8.