Université Rennes 1, Année 2013-2014
Master 1 Math., Algèbre générale de base

Exercice 5.8 – solutions partielles

Exercice 5.8

Le corps $K = \mathbb{Q}(\sqrt[4]{2}, i)$ est une extension de $\mathbb{Q}$ de degré 8, galoisienne de groupe de Galois égal au groupe diédral à huit éléments $G = \mathbb{D}_4$, engendré par σ et τ satisfaisant les relations $\sigma^4 = \tau^2 = (\sigma\tau)^2 = 1$.

Éléments de G et leurs ordres. Dans G il y a :

- 1 élément d'ordre 1,
- 5 éléments d'ordre 2 : $\sigma^2, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$,
- 2 éléments d'ordre 4 : σ et σ^3.

On vérifie d'ailleurs que $1 + 5 + 2 = 8$ et qu'on les a donc tous.

Sous-groupes de G. Énumérons maintenant les sous-groupes. Il n'y a qu'un sous-groupe d'ordre 1 et un sous-groupe d'ordre 8. Les sous-groupes d'ordre 2 sont cycliques ; un tel sous-groupe possède un unique générateur qui est un élément d'ordre 2. Il y a donc 5 sous-groupes d'ordre 2, correspondant aux éléments ci-dessus. Enfin, les sous-groupes d'ordre 4 sont soit cycliques, soit isomorphes au groupe de Klein $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Les groupes cycliques sont engendrés par un élément d'ordre 4 ; il n'y en a qu'un puisque σ et σ^3 engendrent le même sous-groupe. Pour trouver les sous-groupes isomorphes au groupe de Klein on doit trouver les paires d'éléments d'ordre 2 qui commutent. Une petite remarque : parmi les éléments d'ordre 2, l'élément σ^2 est particulier car c'est le seul qui appartient au sous-groupe cyclique d'ordre 4 de G ; géométriquement, si on voit G comme le groupe des isométries du carré, c'est le seul déplacement (la symétrie centrale, ou rotation d'angle π) alors que $\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$ sont des antidéplacements (symétries de droite) et bien sûr, le composé (ou produit) de deux antidéplacements est un déplacement. Raisonnons par condition nécessaire. Un sous-groupe $H \subset G$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ contient trois éléments d'ordre 2, donc au moins 2 antidéplacements g, g' puisqu'il n'y a qu'un déplacement : σ^2. Alors $g^{-1}g'$ est un déplacement, c'est donc σ^2. Ceci montre que nécessairement H contient σ^2. On voit facilement que σ^2 commute avec chacun des 4 antidéplacements d'ordre 2. On trouve finalement 2 sous-groupes :

- le groupe $\langle \sigma^2, \tau \rangle$, qui est le même que $\langle \sigma^2, \sigma^2\tau \rangle$,
- le groupe $\langle \sigma^2, \sigma\tau \rangle$, qui est le même que $\langle \sigma^2, \sigma^3\tau \rangle$.

Sous-groupes distingués. On va appliquer la correspondance de Galois qui affirme que l'application $H \mapsto K^H$ est une bijection entre sous-groupes de G et extensions $L/\mathbb{Q}$ incluses dans K, et que par cette bijection se correspondent les sous-groupes distingués et les extensions $L/\mathbb{Q}$ qui sont galoisiennes. On aura donc besoin de savoir quels sont les sous-groupes distingués. Soit $g \in G$ et $c_g : G \to G$ la conjugaison par g, définie par $c_g(x) = gxg^{-1}$. Les sous-groupes distingués $H \subset G$ sont ceux qui sont stables par toutes les conjugaisons c_g, i.e. $c_g(H) \subset H$, ce qu'il suffit de vérifier pour $g = \sigma$ et $g = \tau$ puisque ceux-ci engendrent G.

On peut déjà observer que comme une conjugaison est un automorphisme, elle envoyer un sous-groupe cyclique d'ordre 4 de G sur un autre sous-groupe cyclique d'ordre 4 de G. Comme il n'y a qu'un tel sous-groupe : $\langle \sigma \rangle$, il est nécessairement envoyé sur lui-même par toutes les conjugaisons, donc distingué.

Le même argument montre que $c_g(\sigma^2) = \sigma^2$ puisque σ^2 est le seul élément d'ordre 2 dans le seul sous-groupe cyclique d'ordre 4 de G. En particulier le sous-groupe $\langle \sigma^2 \rangle$ est distingué.

Un simple calcul direct montre que les deux sous-groupes $\langle \sigma^2, \tau \rangle$ et $\langle \sigma^2, \sigma\tau \rangle$ sont stables par c_σ et c_τ, donc ils sont distingués.

Enfin, un calcul montre qu'aucun des 4 sous-groupes d'ordre 2 engendrés par $\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$ n'est distingué.

Une remarque finale : de toute manière, c'est un exercice facile (en tout cas classique) de montrer que dans un groupe fini, tout sous-groupe d'indice égal à 2 est distingué. Du point de vue de la théorie de Galois, ceci correspond au fait que toute extension de corps de degré 2 est galoisienne. Ceci explique pourquoi les sous-groupes d'ordre 4 sont distingués.

Corps de points fixes. Dans les deux tableaux ci-dessous, nous notons avec une étoile les sous-groupes distingués et les sous-extensions galoisiennes.

Le corps de points fixes de $H = \{1\}$ est K.
Le corps de points fixes de $H = G$ est $\mathbb{Q}$.
Les corps de points fixes des sous-groupes d'ordre 2 sont :

H	$\langle \sigma^2 \rangle^*$	$\langle \tau \rangle$	$\langle \sigma\tau \rangle$	$\langle \sigma^2\tau \rangle$	$\langle \sigma^3\tau \rangle$
K^H	$\mathbb{Q}(i, \sqrt{2})^*$	$\mathbb{Q}(\sqrt[4]{2})$	$\mathbb{Q}(\sqrt[4]{2}(1+i))$	$\mathbb{Q}(i\sqrt[4]{2})$	$\mathbb{Q}(\sqrt[4]{2}(1-i))$

Les corps de points fixes des sous-groupes d'ordre 4 sont :

H	$\langle \sigma \rangle^*$	$\langle \sigma^2, \tau \rangle^*$	$\langle \sigma^2, \sigma\tau \rangle^*$
K^H	$\mathbb{Q}(i)^*$	$\mathbb{Q}(\sqrt{2})^*$	$\mathbb{Q}(i\sqrt{2})^*$