École polytechnique 2022-2023
Théorie de Galois

Devoir maison à rendre le 28 avril 2023

Tous les résultats du cours, polycopié ou PC peuvent être utilisés à condition d'être clairement cités.

Exercice 1
Soit G un groupe d'ordre 8 non commutatif.

1. Quels sont les ordres possibles pour les éléments de G ? Montrer qu'il existe au moins un élément σ d'ordre 4.
2. Soit H le sous-groupe engendré par σ. Montrer que H est distingué dans G.
3. On suppose qu'il existe un élément τ d'ordre 2 qui n'est pas dans H. Montrer que $\sigma\tau = \tau\sigma^{-1}$.
4. Quels sont les ordres des éléments de G ? Quels sont les sous-groupes de G ?
5. On suppose maintenant qu'il n'y a pas d'élément d'ordre 2 dans $G \backslash H$. Montrer que pour tout $x \in G\backslash H$, $x^2 = \sigma^2$ et $\sigma x = x\sigma^{-1}$.
6. Quels sont les ordres des éléments de G ? Quels sont les sous-groupes de G ?

Solution

1. L'ordre d'un élément divise le cardinal du groupe, c'est-à-dire 8. De plus, il ne peut être égal à 8, sinon le groupe serait cyclique, donc commutatif. Il peut donc valoir $1, 2$ ou 4. S'il n'y aucun élément d'ordre 4, alors $x^2 = e$ pour tout $x \in G$. Cela implique que G est commutatif. En effet, on a $x = x^{-1}$, et $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ pour tous $x, y \in G$.
2. H est de cardinal 4, donc d'indice 2 dans G. Cela implique que H est distingué. En effet, si $g \in G$ n'est pas dans H, on a $G\backslash H = gH = Hg$, donc $gHg^{-1} = H$.
3. On voit que G est constitué des éléments $\sigma^k, \tau\sigma^k$, $0 \leq k \leq 3$. L'élément $\sigma\tau$ ne peut être égal à un σ^k, donc il existe j tel que $\sigma\tau = \tau\sigma^j$. Les éléments σ et σ^j sont conjugués, et ont donc le même ordre. Cela implique $\sigma\tau = \tau\sigma$ ou $\sigma\tau = \tau\sigma^{-1}$. Puisque le groupe est non commutatif, le premier cas est exclu.
4. On vérifie que
$$(\tau\sigma^k)(\tau\sigma^k) = \tau\tau\sigma^{-k}\sigma^k = e$$
Le groupe G a donc un élément d'ordre 1, cinq éléments d'ordre 2 et deux éléments d'ordre 4. Les sous-groupes non-triviaux sont d'ordre 2 ou d'ordre 4. Il y a cinq sous-groupes d'ordre 2 (engendré par chacun des éléments d'ordre 2). Soit K un sous-groupe d'ordre 4. En considérant le morphisme $G \to G/H \simeq \{-1, 1\}$, on voit que $H \cap K$ est de cardinal 2 ou 4 (suivant que la restriction du morphisme à K est surjective ou non). Dans tous les cas K contient σ^2. Puisque le groupe $< \sigma^2 >$ est distingué, un sous-groupe d'ordre 4 de G s'identifie à un sous-groupe d'ordre 2 de $G/ < \sigma^2 >$. Ce dernier groupe a cardinal 4, et ses éléments sont d'ordre 1 ou 2. Il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, et il y a donc 3 sous-groupes d'ordre 4 de G.
5. Dans ce cas, le groupe G est constitué de $\sigma^k, x\sigma^k$, $0 \leq k \leq 3$. L'élément x^2 ne peut être égal à $x\sigma^k$, donc $x^2 = \sigma^j$. Puisque x est d'ordre 4, x^2 est d'ordre 2, et $x^2 = \sigma^2$. Le même argument que précédemment montre que $\sigma x = x\sigma^{-1}$.

6. Tous les éléments dans $G \backslash H$ sont d'ordre 4. Le groupe G a donc un élément d'ordre 1, un élément d'ordre 2 et six éléments d'ordre 4. Il y a un sous-groupe d'ordre 2, engendré par σ^2. Puisque G ne contient qu'un seul élément d'ordre 2, un sous-groupe d'ordre 4 est cyclique, engendré par un élément d'ordre 4. Il y a donc trois sous-groupes d'ordre 4, engendré respectivement par σ, x et $x\sigma$.

Exercice 2

On considère le polynôme à coefficients rationnels $P = X^4 - 3X - 3$, et L son corps de décomposition (L est donc une extension finie de $\mathbb{Q}$).

1. Montrer que P est irréductible sur $\mathbb{Q}$, qu'il a deux racines réelles, et deux racines complexes conjuguées.
2. Soit $X^2 + aX + b$ l'unique polynôme réel irréductible de degré 2 divisant P. Montrer que $a^6 + 12a^2 - 9 = 0$.
3. Montrer que le degré de L est un multiple de 12.
4. Montrer que A_4 est l'unique sous-groupe de S_4 d'ordre 12.
5. Déterminer le degré de L sur $\mathbb{Q}$ et le groupe $\mathrm{Gal}(L/\mathbb{Q})$.

Solution

1. Le critère d'Eisenstein pour $p = 3$ montre que P est irréductible. Une étude de fonctions montre que P a exactement deux racines réelles.
2. On factorise P en $P = (X^2 + aX + b)(X^2 + a'X + b')$. On obtient les équations $a' = -a$, $b + b' = a^2$, $a(b' - b) = -3$ et $bb' = -3$. Les réels b, b', sont donc racines de $X^2 - a^2X - 3$, polynôme de discriminant $\Delta = a^4 + 12$. On a de plus
$$\Delta = (b - b')^2 = \frac{9}{a^2}$$
d'où $a^6 + 12a^2 - 9 = 0$.
3. Puisque P est de degré 4 et irréductible, le degré de L est un multiple de 4. De plus, L contient a^2, racine du polynôme $X^3 + 12X - 9$. On vérifie que ce polynôme est irréductible sur $\mathbb{Q}$. Si ce n'était pas le cas, il aurait une racine dans $\mathbb{Q}$. Celle =-ci serait entière, positive, diviserait 9 et serait multiple de 3. On vérifie que ce n'est pas le cas. Donc a^2 est de degré 3 sur $\mathbb{Q}$, et le degré de L est un multiple de 3.
4. Soit H une sous-groupe de S_4 d'ordre 12, distinct de A_4. La signature restreinte à H est donc surjective, et $H \cap A_4$ est d'ordre 6. Puisque A_4 ne contient pas d'élément d'ordre 6, il est isomorphe à S_3, et contient 3 élément d'ordre 2. Il contient donc K, le sous-groupe engendré par les double transpositions. On obtient une contradiction, car K est de cardinal 4, qui ne divise pas 6.
5. Le groupe de Galois de $L/\mathbb{Q}$ se plonge dans S_4, le groupe de permutations des racines de P. Il est de cardinal 12 ou 24. De plus, il contient la conjugaison complexe, qui échanges les deux racines complexes, et correspond donc à une transposition dans S_4. D'après ce qui précède, le groupe de Galois ne peut avoir cardinal 12, sinon il se plongerait dans A_4 ce qui n'est pas le cas. L est donc de degré 24, et $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_4$.