École Polytechnique 2009-2010

Théorie de Galois

Feuille d'exercices 5

Exercice 1. (Rappels) Soit G un groupe. Pour X et Y des parties de G, on pose

$$XY = \{xy, x \in X, y \in Y\} \subset G.$$

Soit $H \subset G$ un sous-groupe de G. Si $g \in G$, on note $gH = \{g\}H$ le translaté de H à gauche par g et on désigne par $G/H \subset \mathcal{P}(G)$ l'ensemble des gH, $g \in G$. On a une définition analogue pour Hg. On rappelle que H est dit *distingué* (ou *normal*) dans G si $gH = Hg$ pour tout g dans G, on note $H \lhd G$.

(i) Montrer que $H \lhd G$ si, et seulement si, $\forall g, g' \in H$, $(gH)(g'H) = gg'H$.

(ii) En déduire que si $H \lhd G$, la loi de composition sur G/H définie par $(gH, g'H) \mapsto gg'H$ est une loi de groupe de neutre H. De plus, l'application $\pi : G \to G/H$, $g \mapsto gH$, est un morphisme de groupes, surjectif et de noyau H.

Ceci revient à dire qu'on a une suite exacte

$$1 \longrightarrow H \longrightarrow G \xrightarrow{\pi} G/H \longrightarrow 1.$$

(iii) Supposons $H \lhd G$. Montrer que l'application qui à un sous-groupe $X \subset G/H$ associe le sous-groupe $\pi^{-1}(X) \subset G$ est une bijection de l'ensemble des sous-groupes de G/H dans ceux de G contenant H. Si G est fini, vérifier que $|\pi^{-1}(X)| = |X||H|$.

(iv) Montrer qu'un sous-groupe H de G est distingué dans G si, et seulement si, il existe un morphisme $\varphi : G \to G'$ vers un autre groupe G' tel que $H = \mathrm{Ker}(\varphi)$.

Si $n \geq 1$, on note $\mathfrak{S}_n$ le groupe des bijections de $\{1, \ldots, n\}$ dans lui-même (pour la composition). Si $\sigma \in \mathfrak{S}_n$, on rappelle que le *support* de σ est l'ensemble des $i \in \{1, \ldots, n\}$ tels que $\sigma(i) \neq i$. Si $I = \{i_1, i_2, \ldots, i_k\} \subset \{1, \ldots, n\}$ et $|I| = k$, on note $(i_1, i_2, \cdots, i_k)$ le k-cycle $\sigma \in \mathfrak{S}_n$ fixant $\{1, \ldots, n\} \backslash I$ et tel que $\sigma(i_s) = i_{s+1}$ pour $1 \leq s < k$ et $\sigma(i_k) = i_1$.

Exercice 2. (i) Pour $\sigma \in \mathfrak{S}_n$, montrer que $\sigma(i_1, \cdots, i_k)\sigma^{-1} = (\sigma(i_1), \cdots, \sigma(i_k))$. En déduire que tous les k-cycles sont conjugués.

(ii) Vérifier que deux permutations à supports disjoints commutent. Remarquer que la réciproque est fausse : $(1,2)(3,4)$ et $(1,3)(2,4)$ commutent dans $\mathfrak{S}_4$.

(iii) Exprimer l'ordre d'une permutation σ en terme des longueurs des cycles intervenant dans sa décomposition en cycles.

(iv) Donner un exemple de cycle dont le carré n'est pas un cycle.

Exercice 3. On suppose dans cet exercice que $n \geq 2$.

(i) Montrer que les transpositions engendrent $\mathfrak{S}_n$.

(ii) Montrer qu'il existe exactement deux morphismes de groupes $\mathfrak{S}_n \to \mathbf{C}^*$: le morphisme constant et la signature ϵ.

(iii) Soit $\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n | \epsilon(\sigma) = 1\}$. Montrer que $\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$ et écrire une suite exacte faisant intervenir $\mathfrak{S}_n$ et $\mathfrak{A}_n$.

Exercice 4. Soient $n \geq 1$ et K un corps. Pour $k \geq 0$, on considère l'ensemble $\mathcal{T}_k$ des éléments de $GL_n(K)$ de la forme $I_n + N$ avec $N_{i,j} = 0$ pour $i > j - k$. Montrer que $\mathcal{T}_k$ est un sous-groupe de $GL_n(K)$ et écrire une suite exacte faisant intervenir $\mathcal{T}_k$ et $\mathcal{T}_{k+1}$.

Exercice 5. (i) Soit X l'ensemble des partitions en deux parties égales de l'ensemble $\{1, 2, 3, 4\}$, c'est à dire des paires $P, Q \in \mathcal{P}(\{1, 2, 3, 4\})$ telles que $|P| = |Q| = 2$ et $P \cap Q = \emptyset$. Vérifier que $|X| = 3$ et que $\mathfrak{S}_4$ agit sur X par $\sigma.\{P, Q\} = \{\sigma(P), \sigma(Q)\}$.

(ii) Soit $K \subset \mathfrak{S}_4$ le sous-groupe engendré par les trois doubles transpositions dans $\mathfrak{S}_4$ (*groupe de Klein*). Montrer que $K \simeq (\mathbf{Z}/2\mathbf{Z})^2$ et que K est distingué dans $\mathfrak{S}_4$.

(iii) Soit $\varphi : \mathfrak{S}_4 \longrightarrow \mathfrak{S}(X) \simeq \mathfrak{S}_3$ le morphisme de groupes associé à l'action du (i). Montrer que φ est surjectif, que $\mathrm{Ker}(\varphi) = K$, et en déduire l'existence d'une suite exacte

$$1 \longrightarrow K \longrightarrow \mathfrak{S}_4 \longrightarrow \mathfrak{S}_3 \longrightarrow 1.$$

(iv) Retrouver géométriquement cette suite exacte en réalisant $\mathfrak{S}_4$ comme groupe d'isométries d'un tétraèdre régulier (regarder l'action sur les trois *paires d'arêtes opposées*).

Exercice 6. Soit G un groupe et H un sous-groupe d'indice 2 (i. e. tel que $|G/H| = 2$). Montrer que H est distingué dans G. En utilisant l'exercice 3, en déduire que $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$.

Exercice 7. (*Sous-groupes finis du groupe multiplicatif d'un corps*) (i) Soient G un groupe et x, y deux éléments d'ordre fini de G. On suppose que $xy = yx$ et que les ordres respectifs n et m de x et y sont premiers entre eux. Montrer que xy est d'ordre fini nm.

On fixe dorénavant un corps k et $G \subset k^*$ un sous-groupe fini (multiplicatif).

(ii) Si $n = |G|$, montrer que $X^n - 1$ est scindé dans $k[X]$, ses racines étant exactement les éléments de G. En déduire que pour tout d divisant n, $X^d - 1$ est scindé à racines distinctes dans G.

(iii) Conclure que G est un groupe cyclique d'ordre n. (On pourra commencer par montrer que si p^r divise n, avec p premier, alors G admet un élément d'ordre p^r, puis on construira un élément d'ordre n dans G)

(iv) En déduire que $(\mathbf{Z}/p\mathbf{Z})^*$ est un groupe cyclique (*Théorème de Gauss*).

Exercice 8. (plus difficile) Un sous-groupe $G \subset \mathfrak{S}_n$ est dit *transitif* si pour tout i, j dans $\{1, \ldots, n\}$ il existe $g \in G$ tel que $g(i) = j$.

(i) Lister les sous-groupes transitifs de $\mathfrak{S}_n$ pour $n \leq 3$, et ceux non-transitifs de $\mathfrak{S}_4$. Montrer que si $G \subset \mathfrak{S}_n$ est transitif, alors n divise $|G|$.

On va montrer qu'un sous-groupe transitif $G \subset \mathfrak{S}_4$ est conjugué à un, et un seul, des 5 sous-groupes : $C = \langle(1, 2, 3, 4)\rangle$, le groupe de Klein K, $D = \langle C, (1, 3)\rangle$, $\mathcal{A}_4$ et $\mathfrak{S}_4$.

(ii) Vérifier que ces groupes conviennent et que $|D| = 8$. Décrire le commutant de chaque élément d'ordre 2 de $\mathfrak{S}_4$, et réaliser D de la sorte. Conclure si $|G|$ divise 8 (on pourra utiliser que le centre d'un p-groupe est non trivial).

(iii) Conclure (on pourra utiliser le résultat de l'exercice 6).