EPFL Automne 2016
Geometrie, MATH-120

Série 4-Corrigé

Exercice 1. Demontrer le theoreme suivant enonce pendant le cours :

Théorème. *Soit $(G, \star)$ un groupe et $A \subset G$ un sous-ensemble de G. Le sous-groupe engrendre par A est l'ensemble des element de G de la forme*

$$\langle A \rangle = \{g = a_1^{n_1} \star \cdots \star a_k^{n_k} \text{ avec } k \geqslant 1,\ a_1, \cdots, a_k \in A \text{ et } n_1, \cdots, n_k \in \mathbb{Z}\} -$$

Autrement dit c'est l'ensemble de tous les produits possibles de puissance d'elements de A.

Exercice 2. Soient G et H des groupes, $A, A' \subset G$, $B \subset H$ des sous-ensembles et $\phi : G \to H$ un morphisme.

1. Montrer que si $A' \subset A$ alors $\langle A' \rangle$ est un sous-groupe de $\langle A \rangle$.
2. On suppose que $\langle A \rangle = G$. Montrer que le morphisme ϕ est completement determine des lors qu'on connait les valeurs
$$\phi(a) \in H \text{ pour tout } a \in A.$$
3. On suppose que $\langle A \rangle = G$. Montrer que l'image de ϕ est engendree par l'image de A :
$$\operatorname{Im} \phi = \langle \phi(A) \rangle$$
4. On suppose que $H = \langle B \rangle$. Montrer que pour que ϕ soit surjectif il suffit que tout $b \in B$ appartienne a $\operatorname{Im} \phi$.
5. Montrer que le resultat analogue pour "injectif" n'est pas vrai : donner un ensemble ou $H = \langle B \rangle$ tel que pour tout $b \in B$, $\phi^{-1}(\{b\})$ comporte au plus 1 element mais tel que ϕ n'est pas injectif.

Démonstration. 1. Soit $g \in \langle A' \rangle$ un élément quelconque. Nous avons vu dans l'exercice précédent qu'il existe $a_1, \cdots, a_k \in A'$ et $n_1, \cdots, n_k \in \mathbb{Z}$ tels que $g = a_1^{n_1} \cdots a_k^{n_k}$. Or comme $A' \subset A$, chaque $a_i \in A, 1 \leqslant i \leqslant k$, et donc $g \in A$. Nous avons donc montré que $\langle A' \rangle$ est un sous-groupe de $\langle A \rangle$.

2. Soit $g \in G$ un élément quelconque. Comme $G = \langle A \rangle$, il existe $a_1, \cdots, a_k \in A$ et $n_1, \cdots, n_k \in \mathbb{Z}$, tels que $g = a_1^{n_1} \cdots a_k^{n_k}$. Nous avons alors

$$\phi(g) = \phi(a_1^{n_1} \cdots a_k^{n_k}) = \phi(a_1)^{n_1} \cdots \phi(a_k)^{n_k},$$

et connaissant les valeurs de $\phi(a_i) \in H$ pour $1 \leqslant i \leqslant k$, nous connaissons donc $\phi(g)$.

3. L'inclusion $\langle \phi(A) \rangle \subset \mathrm{Im}\ \phi$ est évidente du fait que $\mathrm{Im}\ \phi$ est un sous-groupe de H. Nous allons donc démontrer l'inclusion $\mathrm{Im}\ \phi \subset \langle A \rangle$. Soit donc $h \in \mathrm{Im}\ \phi$. Par définition il existe $g \in G$ tel que $h = \phi(g)$. Or comme $G = \langle A \rangle$, il existe $a_1, \cdots, a_k \in A$ et $n_1, \cdots, n_k \in \mathbb{Z}$ tels que $g = a_1^{n_1} \cdots a_k^{n_k}$. Nous concluons donc que

$$h = \phi(g) = \phi(a_1^{n_1} \cdots a_k^{n_k}) = \phi(a_1)^{n_1} \cdots \phi(a_k)^{n_k} \in \langle \phi(A) \rangle,$$

et donc $\mathrm{Im}\ \phi = \langle \phi(A) \rangle$.

4. Afin de montrer que ϕ est surjectif, il suffit de montrer que $H = \langle B \rangle \subset \mathrm{Im}\ \phi$. Or si tout $b \in B$ appartient à $\mathrm{Im}\ \phi$, alors $\mathrm{Im}\ \phi$ est un sous-groupe de H contenant B. Par définition, $\langle B \rangle$ est le plus petit sous-groupe de H contenant B, et donc $H = \langle B \rangle \subset \mathrm{Im}\ \phi$.

5. Soit $\phi : \mathbb{Z} \to \mathbb{Z}$ le morphisme trivial donné par $\phi(n) = 0$ pour tout $n \in \mathbb{Z}$. Soit $B = \{1\}$, et donc $\mathbb{Z} = \langle B \rangle$. Nous avons alors que $|\phi^{-1}(\{1\})| = 0 \leqslant 1$, pour le seul élément de B mais ϕ n'est clairement pas injectif, vu que par exemple $\phi(0) = \phi(1) = 0$.

□

Exercice 3. On considere le groupe symetrique a n elements

$$\mathfrak{S}_n = \mathfrak{S}_{\{1,2,\cdots,n\}}.$$

Une permutation cyclique (ou un cycle) est une permutation que l'on ecrit sous la forme

$$(n_1, n_2 \cdots, n_l)$$

pour $l \geqslant 2$ et $n_i \in \{1, \cdots, n\}$ des entiers tous distincts ; la permutation en question envoie

$$n_1 \to n_2,\ n_2 \to n_3, \cdots, n_{l-1} \to n_l,\ n_l \to n_1$$

et laisse fixe tous les elements differents des n_i. On admettra que toute permutation $\sigma \in \mathfrak{S}_n$ peut s'ecrire comme composee de permutations cycliques.

L'entier $l \geqslant 2$ est la longueur du cycle. Une transposition est une permutation cyclique de longueur 2 : de la forme $(n_1 n_2)$ et qui echange donc n_1 et n_2 et laisse les autres elements fixes.

1. Montrer par recurrence (sur la longueur) que tout cycle peut s'ecrire comme compose de transpositions (pour fixer les idees considerer un cycle de la forme $(123\cdots l)$). Montrer que $\mathfrak{S}_n$ est engendre par les $\frac{n(n-1)}{2}$ transpositions transpositions,
$$(n_1 n_2),\ 1 \leqslant n_1 < n_2 \leqslant n.$$
2. Montrer que les differentes permutations sont conjuguees entre elles : pour tout $(n_1 n_2)$ et $(n_1' n_2')$ il existe $\sigma \in \mathfrak{S}_n$ telle que
$$\sigma \circ (n_1 n_2) \circ \sigma^{-1} = (n_1' n_2').$$
3. Soit
$$\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$$
un morphisme de groupes ($\{\pm 1\}$ est muni de la multiplication). Montrer que ε prend la meme valeur pour toute les transpositions.
4. En deduire qu'il y a au plus deux morphismes de groupes $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ (on verra plus tard dans le cours ou en algebre lineaire qu'il y en a exactement 2).

Démonstration. 1. Montrons par récurrence sur la longeur $\ell \geqslant 2$ que tout cycle peut s'écire comme un produit de transposition. Si $\ell = 2$, il n'y a rien à faire. Soit maintenant $(n_1 n_2 \cdots n_\ell)$ un cycle avec $\ell > 2$, on a alors
$$(n_1 n_2 \cdots n_\ell) = (n_1 \cdots n_{\ell-1})(n_{\ell-1} n_\ell)$$
et on applique l'hypothèse de récurrence.

2. Il suffit pour cela de remarquer que $\sigma \circ (n_1 n_2) \circ \sigma^{-1} = (\sigma(n_1)\sigma(n_2))$. On choisit alors $\sigma \in \mathfrak{S}_n$ tel que $\sigma(n_1) = n_1'$ et $\sigma(n_2) = n_2'$.

3. Soit $t_1, t_2 \in \mathfrak{S}_n$ deux transpositions et on montre que $\varepsilon(t_1) = \varepsilon(t_2)$. Par le point 2, il existe $\sigma \in \mathfrak{S}_n$ tel que $t_2 = \sigma \circ t_1 \circ \sigma^{-1}$, d' où, puisque ε est un homomorphisme de groupes et que $\{\pm 1\}$ est abélien
$$\varepsilon(t_2) = \varepsilon(\sigma \circ t_1 \circ \sigma^{-1}) = \varepsilon(\sigma)\varepsilon(t_1)\varepsilon(\sigma)^{-1} = \varepsilon(\sigma)\varepsilon(\sigma)^{-1}\varepsilon(t_1) = \varepsilon(t_1).$$
4. Puisque les transpositions engendrent le groupe $\mathfrak{S}_n$, le point 2 de l'exercice 2 nous dit qu'un morphisme de groupes $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est entièrement déterminé par ses valeurs sur les transpositions. Or le point précédent nous dit qu'un tel morphisme prend la même valeure sur toutes les transpositions. Finalement, puisque les seuls valeurs possibles sont ± 1, on en déduit qu'il y a au plus deux homomorphismes de groupes $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$.

□

Exercice 4. Soit G un groupe fini de cardinal $|G| = p$ un nombre premier et H un groupe quelconque. Montrer que tout morphisme de groupe $\phi : G \to H$ est soit constant soit injectif.

Exercice 5. Montrer que tout sous-groupe d'un groupe commutatif est distingue.

Exercice 6. On considere l'application exponentielle (reelle)

$$\exp : x \in \mathbb{R} \mapsto \exp(x) = e^x.$$

1. Montrer que exp un isomorphisme du groupe additif $(\mathbb{R}, +)$ vers le groupe multiplicatif $(\mathbb{R}_{>0}, \times)$. Quel est l'isomorphisme inverse ?
2. Soit $\phi : (\mathbb{R}, +) \mapsto (\mathbb{R}_{>0}, \times)$ un morphisme de groupes. On suppose de plus que l'application $x \mapsto \phi(x)$ est continue et on pose $a = \phi(1)$. Soit $\lambda = \log a$, on va demontrer que $\phi(x) = \exp(\lambda x)$
   — Montrer que pour tout $n \in \mathbb{Z}$, on a $\phi(n) = \exp(\lambda n)$.
   — Montrer que pour tout $x \in \mathbb{R}$ et $n \in \mathbb{Z}$, $n \neq 0$, on a $\phi\left(\frac{x}{n}\right) = \phi(x)^{1/n}$. En deduire que pour tout $q \in \mathbb{Q}$, on a $\phi(q) = \exp(\lambda q)$
   — Conclure (utiliser le fait que tout nombre reel est la limite d'une suite de nombres rationnels).

Démonstration. 1. Le fait que exp : $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ soit un homomorphisme de groupes résulte de l'indentité bien connue

$$\exp(a + b) = e^{a+b} = e^a e^b = \exp(a)\exp(b).$$

Pour la bijectivité, nous pouvons utiliser des arguments analytiques. En effet, puisque e^x est continue et que $\lim_{x\to-\infty} e^x = 0$, $\lim_{x\to+\infty} e^x = +\infty$, la fonction e^x est surjective. Enfin puisque $(e^x)' = e^x > 0\ \forall x \in \mathbb{R}$, on en déduit qu'elle est aussi injective. L'homomorphisme réciproque est donné par le logarithme naturel log.

2. Soit $\phi : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ un morphisme que l'on suppose continu. On pose $a = \phi(1)$ et $\lambda = \log(a)$, donc $\phi(1) = \exp(\lambda)$.

i) Pour tout $n \in \mathbb{Z}$, nous avons

$$\phi(n) = \phi(1 + ... + 1) = \phi(1)^n = \exp(\lambda n).$$

ii) Pour $x \in \mathbb{R}$ et $n \in \mathbb{Z}$, on remarque que $\phi(\frac{x}{n})^n = \phi(n\frac{x}{n}) = \phi(x)$, donc $\phi(\frac{x}{n}) = \phi(x)^{1/n}$. Il s'en suit que pour tout nombre rationels $q = a/b \in \mathbb{Q}$,

$$\phi(q) = \phi(\frac{a}{b}) = \phi(a)^{1/b} = \exp(a\lambda)^{1/b} = \exp(\frac{a}{b}\lambda) = \exp(q\lambda).$$

iii) Si $x \in \mathbb{R}$, on choisit une suite de nombre rationels $(q_n)_{n\geqslant 1}$ telle que $\lim_{n\to\infty} q_n = x$. La continuité de ϕ nous permet d'avoir

$$\phi(x) = \phi(\lim_{n\to\infty} q_n) = \lim_{n\to\infty} \phi(q_n) = \lim_{n\to\infty} \exp(q_n\lambda) = \exp(x\lambda).$$

$\square$