EPFL
Geometrie, MATH-120

Automne 2015

Solutions série 2

Exercice 1. Soit $(G, \star)$ un groupe.

- (Unicite de l'element neutre) Montrer que si $e'_G \in G$ est tel que pour au moins un element $g \in G$ on a $g \star e'_G = g$ alors $e'_G = e_G$.
- (Unicite de l'inverse) Montrer que si h verifie $g \star h = e_G$ alors $h = g^{-1}$.
- Que vaut $(g^{-1})^{-1}$?
- Calculer $(g \star h)^{-1}$ en fonction de g^{-1} et h^{-1}.

Solution 1.

- Soit $g \in G$ tel que $g = g \star e'_G$. En multipliant l'équation à la gauche avec g^{-1} on obtient
$$g^{-1} \star g = g^{-1} \star (g \star e'_G).$$
Par l'associativité du group G et la définition de g^{-1} on a donc
$$e_G = (g^{-1} \star g) \star e'_G,$$
qui nous donne finalement
$$e_G = e_G \star e'_G = e'_G$$
par définition de l'élément neutre.
- Comme avant on multiplie les deux côtés de l'équation à la gauche avec g^{-1} et on obtient
$$h = e_G \star h = (g^{-1} \star g) \star h = g^{-1} \star (g \star h) = g^{-1} \star e_G = g^{-1}.$$
- Comme on a $g \star g^{-1} = g^{-1} \star g = e_G$, on sait que g est un inverse pour g^{-1}. Comme l'inverse est unique par l'exercise d'avant on a donc $(g^{-1})^{-1} = g$.
- On a
$$(g \star h) \star (h^{-1} \star g^{-1}) = g \star (h \star h^{-1}) \star g^{-1} = g \star g^{-1} = e_G$$
et de la même manière aussi $(h^{-1} \star g^{-1}) \star (g \star h) = e_G$. De nouveau, comme l'inverse est unique on obtient $(g \star h)^{-1} = h^{-1} \star g^{-1}$.

Exercice 4. Soit $\mathfrak{S}_n$ le groupe des permutations de l'ensemble
$$E_n = \{1, 2, \cdots, n\}.$$

On note Id l'identite de E_n. Pour decrire les elements de $\mathfrak{S}_n$ on utilise la notation suivante : $(1,2)$ designe la permutation

$$(1,2): \ 1 \mapsto 2, \ 2 \mapsto 1, \ 3 \mapsto 3$$

$(1,2,3)$ designe la permutation

$$(1,2,3): \ 1 \mapsto 2, \ 2 \mapsto 3, \ 3 \mapsto 1.$$

et on defini de meme $(1,3)$, $(2,1,3)$, $(1,n,2,5)$ ... Bien entendu pour que la notation soit bien definie il faut que tous les entiers apparaissant dans les parentheses soient distincts. Une telle permutation s'appelle un cycle ; soit $(m_1,\cdots,m_k)$ un cycle (les $m_1,\cdots,m_k$ sont distincts) ; l'entier $k \geqslant 2$ est la longueur du cycle et le sous-ensemble $\{m_1,\cdots,m_k\} \subset E_n$ s'appelle le support du cycle. On peut montrer que toute permutation s'ecrit comme produit de cycles a supports disjoints et que cette decomposition est essentiellement unique.

— On considere le cas $n = 3$. Montrer que

$$\mathcal{S}_3 = \{\mathrm{Id}_3, \ (1,2), \ (1,3), \ (2,3), \ (1,2,3), \ (1,3,2)\}$$

— Ecrire la table de multiplication de ce groupe.
— Ce groupe est-t-il commutatif ?
— Montrer que pour $n \geqslant 4$, le groupe $\mathfrak{S}_n$ n'est pas commutatif (trouver deux permutations qui ne commutent pas).

Solution 4. — On sait qu'il existe $3! = 6$ permutations de l'ensemble E_3 et comme $\{\mathrm{Id}_3, \ (1,2), \ (1,3), \ (2,3), \ (1,2,3), \ (1,3,2)\}$ sont 6 permutations différentes on sait que la liste est complète.

TABLE 1 – table de multiplication de $\mathcal{S}_3$

$\star$	Id_3	(1,2)	(1,3)	(2,3)	(1,2,3)	(1,3,2)
Id_3	Id_3	(1,2)	(1,3)	(2,3)	(1,2,3)	(1,3,2)
(1,2)	(1,2)	Id_3	(1,3,2)	(1,2,3)	(2,3)	(1,3)
(1,3)	(1,3)	(1,2,3)	Id_3	(1,3,2)	(1,2)	(2,3)
(2,3)	(2,3)	(1,3,2)	(1,2,3)	Id_3	(1,3)	(1,2)
(1,2,3)	(1,2,3)	(1,3)	(2,3)	(1,2)	(1,3,2)	Id_3
(1,3,2)	(1,3,2)	(2,3)	(1,2)	(1,3)	Id_3	(1,2,3)

— On voit que $\mathcal{S}_3$ n'est pas commutatif comme la table de multiplication n'est symetrique. Par exemple on a $(1,3)\star(1,2) = (1,2,3) \neq (1,3,2) = (1,2)\star(1,3)$.

— soit $n \geqslant 4$, il suffit de considerer les permutations precedentes dans $\mathfrak{S}_n$ (vuent comme permutations qui fixent tous les $k \in \{4, \cdots, n\}$)

Exercice 6. On considere le groupe additif des entiers relatifs $(\mathbb{Z}, +)$.

1. Montrer que pour $N \in \mathbb{Z}$,
$$N\mathbb{Z} = \{Nn,\ n \in \mathbb{Z}\}$$
l'ensemble des multiples de N est un sous-groupe de $\mathbb{Z}$ (que vaut ce sous-groupe pour $N = 0$?).
2. On va montrer la reciproque : tout sous-groupe de $\mathbb{Z}$ est de la forme $N\mathbb{Z}$. Soit $H \subset \mathbb{Z}$ un sous-groupe ; on considere $0 < N \in H$ le plus petit entier strictement positif contenu dans H . Que ce passe-t-il si N n'existe pas ?
3. On suppose que N existe. Soit $m \in H$, montrer que $r \geqslant 0$ le reste de la division euclidienne de m par N appartient a H.
4. En deduire que $r = 0$ et conclure.

Solution 6.

1. Soient $m, n \in N\mathbb{Z}$ alors $m = Nm',\ n = Nn'$ et
$$m - n = N(m' - n') \in \mathbb{N}\mathbb{Z}$$
donc $(N\mathbb{Z}, +)$ est un sous-groupe. Si $N = 0$, $N\mathbb{Z} = \{0\}$ est le groupe trivial.
2. Supposons que $H \neq 0$ alors il existe $n \in H - \{0\}$. Quitte a remplacer n par $-N$ on peut supposer $n > 0$. Soit $N > 0$ et appartenant a H et de plus minimal pour ces proprietes, alors H contient tous les multiples de N et donc $H \supset N\mathbb{Z}$. montrons l'inclusion inverse.
3. Soit $m \in H$ et realisons la division euclidienne de m par N : il existe $k \in \mathbb{Z}$ et $r \in \{0, \cdots, N-1\}$ tel que
$$m = kN + r.$$
comme kN et m sont dans H, $r = m - kN$ est egalement dans H (car H est un sous-groupe).
4. L'entier r est positif ou nul et strictement plus petit que N : par minimalite de N, r ne peut etre que nul et donc $m = kN \in N\mathbb{Z}$.