Université de Strasbourg
MPA Algèbre S1
P. Guillot, bureau 314, guillot@math.unistra.fr

6 – Groupes

Exercice 1. Décrire complètement les groupes $(\mathbb{Z}/3\mathbb{Z})^*$, $(\mathbb{Z}/5\mathbb{Z})^*$ et $(\mathbb{Z}/8\mathbb{Z})^*$. (C'est-à-dire, multiplier tous les éléments possibles.) Sont-ils tous les trois cycliques ?

Exercice 2. On définit deux matrices dans $GL_2(\mathbb{R})$:

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

1. Si $v = \begin{pmatrix} x \\ y \end{pmatrix}$ est un vecteur, calculer Rv et Sv. Interpréter géométriquement les applications $v \mapsto Rv$ et $v \mapsto Sv$, et expliquer l'emploi des lettres R et S.
2. Montrer que R est d'ordre 4, et S est d'ordre 2. En déduire R^{-1} et S^{-1}.
3. Montrer que $SR = R^{-1}S$.
4. Montrer que
$$G = \{R^i S^j \mid 0 \leq i < 4,\ 0 \leq j < 2\}$$
est un sous-groupe de $GL_2(\mathbb{R})$. Quel est son ordre ?
5. Sans écrire de matrice, calculer l'ordre de chaque élément de G. Est-ce que G est cyclique ?

Exercice 3. Soit G un groupe d'ordre 4. On suppose que G n'est pas cyclique. Décrire G le plus complètement possible.

En particulier, on va observer que G est abélien. Donc cet exercice montre que tout groupe d'ordre 4 est abélien.

Exercice 4. Décrire tous les sous-groupes du groupe G de l'exercice 2.

Il y en a 10, dont 7 sont cycliques.

Exercice 5. Dans cet exercice, G est un groupe, et on note $o(g)$ l'ordre de $g \in G$.

1. Montrer que $o(g^k)$ divise $o(g)$, pour tout $k \in \mathbb{Z}$.
2. Si $n = o(g)$ et $pgcd(k, n) = 1$, montrer que $o(g^k) = n$.
3. Soit $h \in G$ et $m = o(h)$. On suppose que $pgcd(n, m) = 1$. Montrer que, si $g^k = h^\ell$ pour des entiers k, ℓ, alors $g^k = h^\ell = 1$.
4. On suppose maintenant que $gh = hg$ (et toujours que $pgcd(n, m) = 1$). Montrer que $o(gh) = nm$.

Exercice 6.

1. Dresser la liste de tous les sous-groupes de $G = \mu_{12}$.
2. Pour chaque sous-groupe H, on définit le polynôme
$$P_H = \prod_{h \in H} (X - h) \in \mathbb{C}[X].$$
Donner une formule (très) simple pour P_H.
3. Vérifer que P_H divise $P_{H'}$ si et seulement si $H \subset H'$, si et seulement si $|H|$ divise $|H'|$.

4. Déduire de la question précédente l'expression développée de

$$\Psi_d = \prod_{o(g)=d} (X - g)\,.$$

Ici les g sont pris dans G, et d divise 12.

On appelle Ψ_d un « polynôme cyclotomique ». Nous allons voir que $\Psi_d \in \mathbb{Q}[X]$, et en fait on peut montrer (mais c'est plus difficile) que Ψ_d est un polynôme irréductible de $\mathbb{Q}[X]$.

Exercice 7. Soit $\phi\colon G \to H$ un homomorphisme. On définit

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1\}\,,$$

que l'on appelle le *noyau* de ϕ.

1. Montrer que $\ker(\phi)$ est un sous-groupe de G.
2. Montrer que ϕ est injective si et seulement si $\ker(\phi) = \{1\}$.

C'est très utile, d'un point de vue pratique, pour montrer qu'un homomorphisme est injectif.

Exercice 8.

1. Soit G un groupe, soit $g \in G$ un élément d'ordre d, et soit n un multiple de d. Montrer que $x \mapsto g^x$ définit un homomorphisme $\mathbb{Z}/n\mathbb{Z} \to G$.
   Procéder comme dans le cours. Il est utile d'écrire $\oplus$ pour l'addition sur $\mathbb{Z}/n\mathbb{Z}$, dans ce cas.
2. Décrire l'image, puis le noyau de cet homomorphisme.
3. Traduire en notation additive, puis dans le cas $G = \mathbb{Z}/d\mathbb{Z}$ et $g = \bar{1}$.
   On dit souvent que cet homomorphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ est « l'application naturelle ».

Exercice 9. Si G_1 et G_2 sont des groupes, leur produit $G_1 \times G_2$ est aussi un groupe, avec l'opération

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')\,.$$

L'élément neutre est $(1, 1)$. En notation additive, c'est

$$(g_1, g_2) + (g_1', g_2') = (g_1 + g_1', g_2 + g_2')\,,$$

avec l'élément neutre $(0, 0)$.

Montrer le *lemme chinois* : si $pgcd(n, m) = 1$, alors il existe un isomorphisme

$$\mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})\,.$$

Indication : on utilise l'exercice précédent pour construire un homomorphisme entre ces deux groupes.