Solutions structures algébriques
Semaine 14

EPFL, Semestre d'automne 2025

Exercice 1.
Soit $a, b \in \mathbb{Z}$. On rappel que pour un sous-groupe $H < \mathbb{Z}$ il existe un entier $n \in \mathbb{Z}$ tel que $H = n\mathbb{Z}$.

1. Montrez $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a, b)\mathbb{Z}$.
2. Montrez qu'il existe un isomorphisme
$$(\text{pgcd}(a, b)\mathbb{Z})/b\mathbb{Z} \cong a\mathbb{Z}/(\text{ppcm}(a, b)\mathbb{Z}).$$
3. Déduisez en que $\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = a \cdot b$.

Solution.
1. On remarque que $n\mathbb{Z} \subset d\mathbb{Z}$ ssi $d|n$.
   Ainsi Comme $a\mathbb{Z} \subset \text{pgcd}(a, b)\mathbb{Z}$ et $b\mathbb{Z} \subset \text{pgcd}(a, b)\mathbb{Z}$, on a que $a\mathbb{Z} + b\mathbb{Z} \subset \text{pgcd}(a, b)\mathbb{Z}$. Inversement, par Bézout il existe $x, y \in \mathbb{Z}$ tel que $\text{pgcd}(a, b) = ax + by$. Ainsi $\text{pgcd}(a, b)\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$ et on en déduit égalité par double inclusion.
   De manière duale, on a $\text{ppcm}(a, b)\mathbb{Z} \subset a\mathbb{Z}$ et $\text{ppcm}(a, b)\mathbb{Z} \subset b\mathbb{Z}$ donc $\text{ppcm}(a, b)\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$. S'il existait $n \in a\mathbb{Z} \cap b\mathbb{Z} \setminus ppcm(a, b)\mathbb{Z}$, on aurait par division euclidienne $r \in a\mathbb{Z} \cap b\mathbb{Z} \setminus ppcm(a, b)\mathbb{Z}$ tel que $0 < r < \text{ppcm}(a, b)$, mais ceci contredirait la minimalité du ppcm (observez que l'on démontre Bézout d'une manière analogue). Ainsi $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a, b)\mathbb{Z}$.
2. C'est une conséquence directe du deuxième théorème d'isomorphisme : on a
$$a\mathbb{Z} + b\mathbb{Z}/b\mathbb{Z} \cong a\mathbb{Z}/a\mathbb{Z} \cap b\mathbb{Z}$$
   et on conclut en utilisant la première partie.
3. Par l'exercice 5 de la série 9, les quotients de la partie 2 sont finis et de cardinalités
$$|\,\text{pgcd}(a, b)\mathbb{Z}/b\mathbb{Z}| = \frac{b}{\text{pgcd}(a, b)}, \quad |a\mathbb{Z}/\,\text{ppcm}(a, b)\mathbb{Z}| = \frac{\text{ppcm}(a, b)}{a}$$
   Ainsi on obtient par la partie 2 que $\frac{b}{\text{pgcd}(a,b)} = \frac{\text{ppcm}(a,b)}{a}$, c'est à dire que $\text{pgcd}(a, b)\,\text{ppcm}(a, b) = ab$.

Exercice 2.
Montrez que le groupe multiplicatif $\mathbb{Q}_{>0}$ n'est pas de type fini.

Solution.
Par l'absurde, on suppose que $\mathbb{Q}_{>0}$ est engendré par un nombre fini d'éléments, des nombres rationnels strictement positifs

$$\frac{a_1}{b_1}, \ldots, \frac{a_r}{b_r}, \quad a_i, b_i \in \mathbb{N}$$

Soit p un nombre premier qui ne divise aucun des b_i et aucun des a_i ; il existe un tel premier, puisque l'ensemble $\{b_i, a_j\}_{i,j}$ est fini et qu'il existe une infinité de nombres premiers. Il doit alors exister des entiers $n_i \neq 0 \in \mathbb{Z}$ tels que

$$p = \prod_i \left(\frac{a_i}{b_i}\right)^{n_i}.$$

En réarrangeant cette égalité de manière à ne plus avoir de fractions, on obtient

$$\left(\prod_{n_i>0} a_i^{n_i}\right)\left(\prod_{n_j<0} b_j^{-n_j}\right) = p\left(\prod_{n_i<0} a_i^{-n_i}\right)\left(\prod_{n_j>0} b_j^{n_j}\right).$$

Le côté droit de cette égalité est divisible par p, tandis que le côté gauche ne l'est pas par le choix de p. C'est une contradiction, ainsi $\mathbb{Q}_{>0}$ n'est pas de type fini.

Exercice 3.
Soit $n \geq 3$.

1. Montrez que S_n est engendré par les transpositions

$$(1\ 2), (2\ 3), \ldots, (n-1\ n).$$

Indication : il suffit de montrer que le sous-groupe engendré par ces transpostions contient toutes les transpositions de S_n.

2. Montrez que S_n est engendré par $(1\ 2)$ et $(2\ 3\ \ldots\ n)$.
3. Soit $H \leq S_n$ un sous-groupe engendré par 2 transpositions distinctes. Montrez que soit $H \cong S_3$, soit $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution. 1. Puisque S_n est généré par ses transpositions, il suffit de vérifier que chaque transposition de la forme $(i\ j)$ pour $1 \leq i < j \leq n$, est dans le sous-groupe généré par les transpositions,

$$(1\ 2), (2\ 3), \ldots, (n-1\ n).$$

Soit $H = \langle (1\ 2), ..., (n-1\ n) \rangle$ le sous groupe engendré par ces transpositions. Supposons que $(1\ i) \in H$ pour un certain$i < n$ soit engendré par ces transpositions. Alors par conjugaison on obtient que

$(1\ i+1) = (i\ i+1)(1\ i)(i\ i+1) \in H$. On obtient donc par récurrence que $(1\ i) \in H$ pour tout $i \in \{2, ..., n\}$. Soit $i \neq j \in \{1, ..., n\}$, on obtient alors

$$(i\ j) = (1\ j)(1\ i)(1\ j) \in H$$

et donc $S_n = \langle (i\ j) \rangle_{i \neq j} \subset H$ comme on voulait le montrer.

2. On procède de manière similaire. Soit $\sigma = (2\ 3\ ...\ n)$. Alors on observe que

$$\sigma^{i-2}(1\ 2)\sigma^{2-i} = (1\ i)$$

et donc par le même argument que dans la partie 1, S_n est engendré par $\{(1\ 2), \sigma\}$.

3. Distinguons deux cas.
   - **Les deux transpositions ont des supports disjoints.** Alors les deux transpositions commutent entre elles et sont d'ordre 2 ; donc H est 2-torsion et $|H| = 4$. Ainsi $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par l'exercice 2 de la série 13.
   - **Les supports des deux transpositions ne sont pas disjoints.** Sans perte de généralité, ces transpositions sont $(1\ 2)$ et $(2\ 3)$. Donc H s'identifie au sous-groupe de S_3 généré par $(1\ 2)$ et $(2\ 3)$, qui est égal à S_3 par le premier point. Donc $H \cong S_3$.

Exercice 4.
Soit $n \geq 3$. Montrez que A_n est engendré par des 3-cycles.

Solution.
Une permutation est un élément de A_n si et seulement si elle est le produit d'un nombre pair de transpositions. On note que $(i\ j)(i\ k) = (i\ j\ k)$ et $(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l)$ pour i, j, k, l distincts. Ainsi les trois cycles génèrent tous les produits d'un nombre pair de transpositions.

Exercice 5 (Troisième théorème d'isomorphisme)**.**
Soit $M \lhd G, N \lhd G$ et $M < N$.

1. Montrez que $M \lhd N$ et $N/M \lhd G/M$.
2. Montrez que

$$(G/M)/(N/M) \cong G/N$$

Solution. 1. Montrons que $M \lhd N$ et $N/M \lhd G/M$. Comme $M \lhd G$, pour tout $g \in G$,

$$gMg^{-1} = M.$$

En particulier, pour tout $n \in N$, comme $n \in G$, on a :

$$nMn^{-1} = M.$$

Cela montre que M est stable par conjugaison dans N, donc $M \lhd N$.

Pour $N/M \lhd G/M$: soit $gM \in G/M$ et $nM \in N/M$. Montrons que la conjugaison de nM par gM reste dans N/M. En effet,

$$(gM)(nM)(gM)^{-1} = gng^{-1}M.$$

Or, puisque $N \lhd G$, on a $gng^{-1} \in N$. Donc $gng^{-1}M \in N/M$.

2. Montrons que $(G/M)/(N/M) \cong G/N$. On peut multiplier librement les classes à gauche en utilisant la normalité prouvée au point 1.
   Définissons l'application suivante :

$$\varphi : G/N \to (G/M)/(N/M), \quad \varphi(gN) = (gM)(N/M).$$

   — φ est bien définie.
   Supposons que $gN = hN$, c'est-à-dire $\exists n \in N$, $hg^{-1} = n$. Donc $hM = ngM = nMgM$, donc gM et hM sont dans la même classe modulo N/M. Ainsi, φ est bien définie.
   — Injectivité :
   Supposons que $\varphi(gN) = \varphi(hN)$. Par définition :

$$(gM)(N/M) = (hM)(N/M).$$

   Cela signifie qu'il existe $n \in N$ tel que $gM = nMhM$ donc $g^{-1}h \in N$ et $gN = hN$.
   — Surjectivité : soit $(gM)(N/M) \in (G/M)/(N/M)$. Par définition de φ, l'élément $gN \in G/N$ s'envoie sur cette classe.
   — Morphisme de groupe. On a bien $\varphi(N) = M$ dans N/M, qui est l'élément neutre. Il est clair également que $\varphi(gNg'N) = \varphi(gg'N) = gg'M = gMg'M = \varphi(gN)\varphi(g'N)$ dans N/M.