Université Paris Diderot
L3 Math-Info, Algèbre et géométrie

Corrigé du contrôle de connaissance du mardi 20 octobre 2009

Questions de cours.

1) Supposons que G est un groupe abélien. On a, pour tous $x, y \in G$, que

$$I(xy) = (xy)^{-1} = y^{-1}x^{-1} = I(x)I(y).$$

Donc I est un morphisme de groupe. Réciproquement, si I est un morphisme de groupes, alors pour tous $x, y \in G$, on a $xy = I((xy)^{-1}) = I(y^{-1}x^{-1}) = I(y^{-1})I(x^{-1}) = yx$. Donc G est un groupe abélien.

2) (a) Soit h un élément quelconque. Par hypothèse l'ensemble $S := \{h^n : n \in \mathbb{N}^*\}$ est contenu dans H. Comme G est fini, on obtient que S est un ensemble fini. Il existe donc deux entiers $n > m$ dans $\mathbb{N}^*$ tel que $h^n = h^m$. On en déduit que $e = h^{n-m} \in S \subset H$. Pour montrer que H est un sous-groupe de G, il suffit de vérifier que, pour tout $x \in H$, on a $x^{-1} \in H$. Considérons l'application $M_x : H \to H$ qui envoie y en xy. C'est une application injective, donc surjective car H est un ensemble fini. Comme $e \in H$, il existe donc $y \in H$ tel que $xy = M_x(y) = e$. On obtient donc $x^{-1} = y \in H$.

(b) On peut prendre par exemple $G = \mathbb{Z}$ et $H = \mathbb{N}$.

3) (a) Tout endomorphisme de G est de la forme $x \to x^m$ ($m \in \{1, \cdots, p^n\}$). Il y a précisément p^n tels morphismes.

(b) D'abord, le morphisme φ est de la forme $x \mapsto x^m$ (où $m \in \{1, \cdots, p^n\}$). Le groupe G étant fini, φ est un isomorphisme si et seulement s'il est injectif, ou si le noyau de φ se réduit à $\{e\}$. Le noyau de φ est $\{x : x^m = e\}$. Si $p \mid m$, alors $e \neq a^{p^{n-1}} \in \operatorname{Ker}\varphi$. Si $p \nmid m$, alors pour tout $k \in \{1, \cdots, p^n - 1\}$, km n'est pas divisible par p^n. Donc $a^{km} \neq 0$ et $a^k \notin \operatorname{Ker}\varphi$. On en déduit donc $\operatorname{Ker}\varphi = \{e\}$ si et seulement si $p \nmid m$.

(c) Le cardinal de $\operatorname{Aut}(G)$ est le nombre des $m \in \{1, \cdots, p^n\}$ qui ne sont pas divisible par p, c'est-à-dire $p^{n-1}(p-1)$.

4) (a) $n!/2$ si $n > 1$; 0 si $n = 1$. (b) $(-1)^{n-1}$.

Exercice

1. On note $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Comme $\text{dét}\,(I) = 1$, on a $I \in \mathrm{SL}_2(\mathbb{Z})$. La loi de multiplication de matrices est associative. En outre, si A est une matrice dans $\mathrm{SL}_2(\mathbb{Z})$, alors $IA = AI = I$. Enfin, pour toute $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, la matrice $B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ vérifie $BA = AB = I$ puisque $ad - bc = \text{dét}\,(A) = 1$. Comme $\text{dét}\,(B) = 1$, la matrice A est inversible dans $\mathrm{SL}_2(\mathbb{Z})$. Donc $\mathrm{SL}_2(\mathbb{Z})$ est un groupe. Comme $ST \neq TS$, le groupe n'est pas abélien.

2. $$SA = \begin{bmatrix} -c & -d \\ a & b \end{bmatrix}, \qquad T^n A = \begin{bmatrix} a + nc & b + nd \\ c & d \end{bmatrix}$$

3. Soit H le sous-groupe de G engendré par S et T. Considérons l'action du groupe H sur G par multiplication à gauche. Il suffit de montrer que cette action est transitive. Soit A un élément dans $\mathrm{SL}_2(\mathbb{Z})$. On montrera que $I \in \mathrm{orb}(A)$. Soit $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ un élément dans $\mathrm{orb}(A)$ tel que $|c|$ soit le minimum. Montrons que $c = 0$. Si $c \neq 0$, alors il existe $n \in \mathbb{Z}$ tel que $|a + nc| < |c|$. On a alors $ST^nB = \begin{bmatrix} -c & -d \\ a+nc & b+nd \end{bmatrix} \in \mathrm{orb}(A)$, une contradiction. Comme $\mathrm{dét}\,(A) = ad = 1$, on obtient que $d = \pm 1$. Quitte à remplacer B par $T^{\pm b}B$, on peut supposer que $b = 0$, c'est-à-dire $B = \pm I$. Si $B = I$, alors I est déjà dans $\mathrm{orb}(A)$; sinon on a $S^2B = I \in \mathrm{orb}(A)$.
4. On a $I \cdot z = z$. En outre, si $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ et $B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ sont dans $\mathrm{SL}_2(\mathbb{Z})$, alors
$$\begin{aligned} A \cdot (B \cdot z) = A \cdot \frac{a'z + b'}{c'z + d'} &= \frac{a\frac{a'z+b'}{c'z+d'} + b}{c\frac{a'z+b'}{c'z+d'} + d} = \frac{a(a'z+b') + b(c'z+d')}{c(a'z+b') + d(c'z+d')} \\ &= \frac{(aa' + bc')z + (ab' + bd')}{(ca' + dc')z + (cb' + dd')} = (AB) \cdot z. \end{aligned}$$
5. $S \cdot z = -1/z$, $T \cdot z = z + 1$.
6. Il suffit de montrer que, si $z \in \mathbb{H}$, alors il en sont de dême de $S \cdot z$ et $T \cdot z$. Mais cela repose sur les relations $\mathrm{Im}(S \cdot z) = \mathrm{Im}(z)/|z|^2$ et $\mathrm{Im}(T \cdot z) = \mathrm{Im}(z)$.
7. $\mathrm{Stab}(i) = \{\pm I, \pm S\}$. Comme $TST^{-1} \notin \{\pm I, \pm S\}$, ce groupe n'est pas un sous-groupe distingué de $\mathrm{SL}_2(\mathbb{Z})$.
8. (b) On a $A \cdot z = \frac{az+b}{cz+d} = \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{ac|z|^2+bd+(adz+bc\overline{z})}{|cz+d|^2}$. Donc $\mathrm{Im}(A \cdot z) = \frac{(ad-bc)}{|cz+d|^2}\mathrm{Im}(z) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$ puisque $ad - bc = \mathrm{dét}\,(A) = 1$. Supposons que $z = x + iy$ $(x, y \in \mathbb{R})$. On a $|cz + d|^2 = (cx + d)^2 + (cy)^2$. Pour tout $R > 0$, l'ensemble $\{(c, d) \in \mathbb{Z}^2 \mid |cz + d|^2 \leqslant R^2\}$ est fini. Cela montre que la fonction $f_z(A)$ atteint son maximum.
(c) Soit $A \in \mathrm{SL}_2(\mathbb{Z})$ tel que $f_z(A)$ atteint son maximum. Quitte à remplacer A par certain T^nA (on a $f_z(A) = f_z(T^nA)$), on peut supposer que $\mathrm{Re}(Az) \in]-\frac{1}{2}, \frac{1}{2}]$. On a $|Az| \geqslant 1$, sinon $\mathrm{Im}(SAz) = \mathrm{Im}(Az)/|Az|^2 > \mathrm{Im}(Az)$, une contradiction. Si $|Az| > 1$, alors on a $Az \in \Gamma$. Sinon Az est de la forme $e^{i\theta}$ avec $\pi/3 \leqslant \theta < 2\pi/3$. Lorsque $\theta \in [\pi/3, \pi/2]$, on a $Az \in \Gamma$. Si $\theta \in]\pi/2, 2\pi/3[$, on a $SAz = e^{i(\pi-\theta)} \in \Gamma$. Par conséquent, $\Gamma \cap \mathrm{orb}(z) \neq \emptyset$. Pour montre l'unicité du point commun de $\mathrm{orb}(z)$ et Γ, il suffit de montrer que, si w_1 et w_2 sont deux points de Γ et $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ est tel que $Aw_1 = w_2$, alors on a $w_1 = w_2$. Ce dernier est vérifié lorsque $c = 0$ car dans ce cas-là on a $A = \pm I$. Dans la suite, on suppose que $c \neq 0$. Par la symétrie, on peut supposer que $\mathrm{Im}(w_1) \leqslant \mathrm{Im}(w_2)$. On a alors $|w_1| = 1$ car sinon $|cw_1 + d|^2 = c^2|w_1|^2 + 2cd\,\mathrm{Re}(w_1) + d^2 > c^2 - |cd| + d^2 \geqslant 1$ qui contradit $\mathrm{Im}(w_1) \leqslant \mathrm{Im}(w_2) = \mathrm{Im}(w_1)/|cw_1 + d|^2$. Si $d = 0$, alors $A = \pm S$. Dans ce cas-là $Aw_1 \notin \Gamma$, une contradiction. Donc $d \neq 0$. Par conséquent, on a $w_1 = e^{i\pi/3}$ et $d = -c = \pm 1$ (sinon on a encore $|cw_1 + d|^2 > 1$). On peut supposer $d = -c = -1$ (car $-Aw_1 = Aw_1$) et donc $a + b = -1$. On en déduit $Aw_1 = a + e^{i\pi/3}$. Donc $a = 0$ et $w_1 = w_2$.