L3 MF — Algèbre
2010-11
Correction abrégée de l'examen final, 5 janvier 2011

1. Action de $PSL(2,\mathbb{Z})$ sur le demi-plan. 1. Il est clair que le produit de deux matrices à coefficient entier est une matrice à coefficients entiers. Pour l'inverse il suffit d'utiliser la formule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{D}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

où D est le déterminant, qui est ici égal à 1 par définition de $SL(2,\mathbb{Z})$.

2. On note d'abord que pour toute matrice $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $SL(2,\mathbb{Z})$, le "produit" dont il est question ici est bien défini pour tout $z \in \mathcal{H}$, puisqu'alors $cz + d \neq 0$ (si c est non nulle, la partie imaginaire est non nulle, si $c = 0$ alors $d = 0$ puisque $u \in SL(2,\mathbb{R})$). De plus, le produit s'écrit

$$\frac{az+b}{cz+d} = \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2}.$$

La partie imaginaire du numérateur est $Im(adz + bc\overline{z}) = (ad - bc)Im(z) = Im(z)$, qui est donc positive si $z \in \mathcal{H}$. Donc le produit envoie $\mathcal{H}$ sur $\mathcal{H}$.

Enfin si $u, u' \in SL(2,\mathbb{R})$ alors un calcul immédiat montre que pour tout $z \in \mathcal{H}, u.(u'.z) = (uu').z$. On a donc bien défini une action.

3. La matrice $-I_2$ agit trivialement sur $\mathcal{H}$. De plus, si $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ agit trivialement alors, pour tout $z \in \mathcal{H}$, $z = \frac{az+b}{cz+d}$, si bien que $b = c = 0$ et soit $a = d = 1$, soit $a = d = -1$. Il existe donc exactement deux matrices qui agissent trivialement sur $\mathcal{H}$, I_2 et $-I_2$.

4. Il est évident que $\{-I_2, I_2\}$ est un sous-groupe, et qu'il est distingué dans $SL(2,\mathbb{R})$ puisque pour tout $u \in SL(2,\mathbb{R})$ on a $uI_2u^{-1} = I_2$ et $u(-I_2)u^{-1} = -I_2$.

On peut donc considérer le quotient $SL(2,\mathbb{R})/\{-I_2, I_2\}$. Comme I_2 et $-I_2$ agissent trivialement sur $\mathcal{H}$, $PSL(2,\mathbb{R})$ agit sur $\mathcal{H}$, et aucun élément autre que le neutre n'agit trivialement.

5. Soit $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et soit $z \in \mathcal{H}$ tel que $u.z = z$. Alors $az + b = z(cz + d)$ si bien que l'équation $cz^2 + (d - a)z - b = 0$ a une solution de partie imaginaire strictement positive. Comme on ne peut pas avoir $b = c = 0$ (sans quoi on aurait $u = \pm I_2$) on voit que $c \neq 0$ et donc l'équation est bien de degré 2. Son discriminant est donc négatif, donc $(d - a)^2 + 4bc < 0$, soit $(d + a)^2 - 4(ad - bc) < 0$, si bien que $tr(u)^2 < 4$, et donc $u \in \{-1, 0, 1\}$.

6. Si u a un point fixe dans $\mathcal{H}$ alors sa trace est -1, 0 ou 1. On considère les trois cas séparément, en se souvenant que le déterminant de u est 1.

Si $tr(u) = -1$, le polynôme caractéristique de u est X^2+X+1. Comme u annule son polynôme caractéristique, $(u^2 + u + I_2)(u - I_2) = 0$ si bien que $u^3 = I_2$ et donc $u^6 = I_2$.

Si $tr(u) = 0$, le polynôme caractéristique est $X^2 + 1 = 0$, donc $u^2 = -I_2$, donc $u^4 = I_2$.

Si $tr(u) = 1$, le polynôme caractéristique est $X^2 - X + 1 = 0$, donc $(u^2 - u + I^2)(u + I_2) = 0$ si bien que $u^3 + I_2 = 0$ et donc $u^6 = I_2$.

7. Soient $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $u' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ deux éléments de Γ_p. Alors $u^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ est encore un élément de Γ_p. De plus,

$$uu' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + bc' & cb' + dd' \end{pmatrix},$$

et tous les produits sont congrus à 0 modulo p sauf aa' et dd', qui sont congrus à 1. Donc $uu' \in \Gamma_p$, si bien que Γ_p est un sous-groupe de $SL(2,\mathbb{Z})$.

Soit $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \pm I_2$ un élément de Γ_p qui a un point fixe dans $\mathcal{H}$. Alors sa trace est -1, 0 ou 1. Mais $tr(u)$ est congrue à 2 modulo p. Donc nécessairement $p = 3$ et $tr(u) = -1$. Ainsi il existe $k, b', c' \in \mathbb{Z}$ tel que $a = 3k+1, b = -3k-2, b = 3b', c = 3c'$. Mais $\det(u) = 1$ si bien que $(3k+1)(-3k-2) - 9b'c' = 1$. En réduisant modulo 9 on a une contradiction.

8. Montrer que Γ_p est distingué et d'indice fini dans $SL(2,\mathbb{Z})$.

2. Exercice. Soit $a \in A$ non nul, on considére la suite des (a^n). C'est une suite décroissante d'idéaux, elle est donc stationnaire. Il existe donc $n \in \mathbb{N}$ tel que $a^{n+1} \ni (a^n)$. Ceci implique que $a^n = ua^{n+1}$, pour un certain $u \in A$. Alors $a^n(1-ua) = 0$ et, comme A est intègre, $1 = ua$ et donc a est inversible d'inverse u.

3. Exercice. On applique le critère d'Einsenstein avec $p = 5$. p divise tous les coefficients sauf le coefficient dominant, et p^2 ne divise pas 35, donc le polynôme est irréductible dans $\mathbb{Z}[X]$.

4. Polynômes premiers de $\mathbb{Z}[X]$. 1. Montrons d'abord que $B \cap J$ est un idéal de B. C'est un sous-groupe de B puisque l'intersection de deux sous-groupes est un sous-groupe. De plus si $a \in B \cap J$ et $b \in B$ alors $ab \in J$ car J est un idéal, et $ab \in B$ car B est un sous-anneau, donc $ab \in B \cap J$.

Soit $a, b \in B$ tels que $ab \in B \cap J$. Alors $ab \in J$ et comme J est premier, $a \in J$ ou $b \in J$. Si par exemple $a \in J$ alors $a \in B \cap J$, ce qui montre bien que $B \cap J$ est un idéal.

2. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[X]$ (on identifie $\mathbb{Z}$ aux polynômes de degré 0) donc d'après la question précédente $\mathbb{Z} \cap J$ est un sous-anneau premier de $\mathbb{Z}$. Mais ce ne peut être $\mathbb{Z}$ tout entier, sans quoi J contiendrait 1, et alors on aurait $J = \mathbb{Z}[X]$, ce qui est exclu. Donc $\mathbb{Z} \cap J$ est soit (0), soit (p) pour un p premier.

3*. Soit P_1 un élément de J non nul de degré minimal. Alors $P_1 = nP_0$, où P_0 est de contenu 1. Comme J est premier, $n \in J$ ou $P_0 \in J$, mais la première alternative est exclue car $\mathbb{Z} \cap J = (0)$. Donc $P_0 \in J$.

Soit maintenant P un autre polynôme de degré non nul de J. On pose la division euclidienne de P par P_0 dans $\mathbb{Q}[X]$, on obtient que

$$P = \frac{1}{q} P_0 Q_0 + \frac{1}{q'} R_0 \ ,$$

où $q, q' \in \mathbb{N}$ et ne divisent pas les contenus respectivement de $Q_0, R_0 \in \mathbb{Z}[X]$, et Q_0 est de degré inférieur au degré de P_0.

Il suit que

$$qq'P = q'P_0Q_0 + qR_0 \ ,$$

donc $qR_0 \in J$, donc $qR_0 = 0$ par minimalité du degré de P_0.

Ainsi $qP = P_0Q_0$. En prenant le contenu des deux membres on obtient que $q = 1$. Donc $P = P_0Q_0$ ce qui montre bien que $P \in (P_0)$.

4*. Montrons d'abord que $r_p^{-1}(r_p(J)) = J$. Soit $P \in r_p^{-1}(r_p(J)) = J$, alors par définition il existe $Q \in J$ tel que $r_p(P) = r_p(Q)$, et alors $P - Q \in (p)$ (ici (p) est l'idéal engendré par p dans $\mathbb{Z}[X]$). Donc $r_p^{-1}(r_p(J)) \subset J + (p)$. Mais $p \in J$ donc $J + (p) = J$. L'inclusion inverse est claire puisque $r_p(p) = 0 \in r_p(J)$.

Montrons que $r_p(J)$ est premier. Soit $A, B \in (\mathbb{Z}/p\mathbb{Z})[X]$ dont le produit est dans $r_p(J)$, soient a, b des antécédents de A, B dans $\mathbb{Z}[P]$. Alors $r_p(ab) = AB \in J$ donc $ab \in r_p^{-1}(r_p(J)) = J$, donc $a \in J$ ou $b \in J$, et donc A ou B est dans $r_p(J)$. Donc $r_p(J)$ est premier.

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $(\mathbb{Z}/p\mathbb{Z})[X]$ est principal et $r_p(J) = (G)$, où $G \in (\mathbb{Z}/p\mathbb{Z})[X]$ est irréductible. Soit $g \in \mathbb{Z}[X]$ un antécédent de G par r_p. Alors tout élément de (p, g) a pour image par r_p un multiple de G et est donc dans $r_p^{-1}(r_p(J))$, si bien que $(p, g) \subset J$. Réciproquement, si $q \in J$ alors $r_p(q) \in (G)$ donc $q \in (g, p)$.