Université de Bretagne Occidentale, Département de Mathématiques
MASTER 1, MATHEMATIQUES

Groupes et anneaux

Examen terminal, 7 janvier 2014, 13h30–16h30

CORRIGE ET BAREME

Question de cours. Théorème de la base d'Hilbert : Soit A un anneau noetherien. Alors, l'anneau de polynômes $A[X]$ est noetherien. **(2 pts)**
Démonstration. Par l'absurde : supposons I est un idéal de $A[X]$ qui n'est pas de type fini. Evidemment, $I \neq \{0\}$. On va construire, par récurrence, des éléments $P_1, P_2, P_3, \dots$ de I. Soit $P_1 \in I\backslash\{0\}$ un polynôme de plus bas degré. Comme I n'est pas de type fini, $(P_1) \subsetneq I$. Soit $P_2 \in I\backslash(P_1)$ un polynôme de plus bas degré. Alors, $(P_1, P_2) \subsetneq I$. On continue ainsi et on trouve finalement une suite des polynômes $P_1, P_2, P_3, \dots$ dans I telle que P_{n+1} soit un polynôme dans $I\backslash(P_1, \dots, P_n)$ de plus bas degré.

Soit d_i le degré du polynôme P_i et $a_i \in A$ le coefficient dominant du polynôme P_i, $i = 1, 2, 3, \dots$. Par construction, $d_{i+1} \geq d_i$ quel que soit $i \in \mathbb{N}$. Comme A est noetherien, la chaîne croissante d'idéaux de A

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots$$

est stationnaire à partir d'un certain rang n. En particulier, $a_{n+1} \in (a_1, \dots, a_n)$, c-à-d, il existe $b_i \in A$ tels que $a_{n+1} = \sum_{i=1}^n b_i a_i$. On a alors

$$P_{n+1} - \sum_{i=1}^{n} b_i X^{d_{n+1}-d_i} P_i \;\in\; I\backslash(P_1, \dots, P_n)$$

dont le degré est strictement inférieur à celui de P_{n+1}. Contradiction. **(4 pts)**

Exercice 1. a. Comme S et T sont des parties multiplicatives de A, on a $1 \in S$ et $1 \in T$. Du coup, $1 = 1 \times 1 \in ST$.

Soient $x, y \in ST$. On montre que $xy \in ST$. Comme $x, y \in ST$, on a $x = st$ et $y = uv$ avec $s, u \in S$ et $t, v \in T$. Du coup, $xy = stuv = (su)(tv) \in ST$ car $su \in S$ et $tv \in T$, les sous-ensembles S et T étant multiplicatifs. **(0,5 pt)**

b. Comme ι est un morphisme d'anneaux unitaires, on $\iota(1) = 1$. Du coup, $1 \in \iota(T)$.

Soient $x, y \in \iota(T)$. On montre que $xy \in \iota(T)$. Comme $x, y \in \iota(T)$, il existe $u, v \in T$ tels que $\iota(u) = x$ et $\iota(v) = y$. Du coup, $xy = \iota(u)\iota(v) = \iota(uv)$ car ι est un morphisme d'anneaux. Comme T est multiplicative, on a $uv \in T$ et donc $xy = \iota(uv) \in \iota(T)$. **(0,5 pt)**

c. Soit $\lambda\colon A \to (ST)^{-1}A$ le morphisme de localisation. En fait, $\lambda(a) = \frac{a}{1}$ pour tout $a \in A$. Comme $S \subseteq ST$, on a $\lambda(s) \in A^\times$ quel que soit $s \in S$. D'après la propriété universelle de la localisation par S, il existe un morphisme

$$\mu\colon S^{-1}A \longrightarrow (ST)^{-1}A$$

tel que $\mu \circ \iota = \lambda$. En fait, on a

$$\mu\left(\frac{a}{s}\right) = \frac{a}{s}$$

pour tout $\frac{a}{s} \in S^{-1}A$.

Montrons que $\mu(x)$ est inversible dans $(ST)^{-1}A$ pour tout $x \in \iota(T)$. En effet, si $x \in \iota(T)$, on a $x = \iota(t)$ pour un certain $t \in T$. Du coup, $\mu(x) = \mu(\iota(t)) = \lambda(t) = \frac{t}{1}$. Or, $\frac{t}{1}$ est inversible dans $(ST)^{-1}A$ car $t \in T \subseteq ST$. Par conséquent, il existe un morphisme

$$\nu\colon \iota(T)^{-1}(S^{-1}A) \longrightarrow (ST)^{-1}A$$

tel que $\nu \circ \delta = \mu$, où $\delta\colon S^{-1}A \to \iota(T)^{-1}(S^{-1}A)$ est la localisation de $S^{-1}A$ par la partie multiplicative $\iota(T)$. En fait, on a

$$\nu\left(\frac{\left(\frac{a}{s}\right)}{\left(\frac{t}{1}\right)}\right) = \frac{a}{st}.$$

Montrons que ν est un isomorphisme. Il est clair que ν est surjectif. Montrons donc son injectivité. Soit $(a/s)/(t/1)$ un élément du noyau de ν. Cela veut dire que $a/(st) = 0$ dans $(ST)^{-1}A$. Il existe donc $r \in ST$ tel que $ra = 0$. Comme $r \in ST$, on peut écrire $r = uv$ avec $u \in S$ et $v \in T$. Comme

$$\frac{v}{1} \cdot \frac{a}{s} = \frac{v}{1} \cdot \frac{ua}{us} = \frac{vua}{us} = \frac{ra}{us} = \frac{0}{us} = 0,$$

on a bien $(a/s)/(t/1) = 0$ dans $\iota(T)^{-1}(S^{-1}A)$. **(2,5 pt)**

d. D'après ce qui précède, les anneaux $\iota(T)^{-1}(S^{-1}A)$ et $(ST)^{-1}A$ sont isomorphes. En inversant les rôles de S et T, les anneaux $\kappa(S)^{-1}(T^{-1}A)$ et $(TS)^{-1}A$ sont isomorphes. Comme $TS = ST$ dans A, on en déduit que les anneaux $\iota(T)^{-1}(S^{-1}A)$ et $\kappa(S)^{-1}(T^{-1}A)$ sont isomorphes. **(0,5 pt)**

Exercice 2. a. $2014 = 2 \times 19 \times 53$. On a donc $p = 2$, $q = 19$ et $r = 53$. **(0,5 pt)**

b. D'après les Théorèmes de Sylow, $s_{19} \equiv 1 \pmod{19}$ et s_{19} divise 2×53. Or, $2 \not\equiv 1 \pmod{19}$ et $53 \equiv -4 \not\equiv 1 \pmod{19}$. Du coup, $2 \times 53 \equiv -8 \not\equiv 1 \pmod{19}$. Le seul diviseur de 2×53 qui est $\equiv 1 \pmod{19}$ est donc 1, i.e., $s_{19} = 1$. **(0,5 pt)**

c. D'après les Théorèmes de Sylow, $s_{53} \equiv 1 \pmod{53}$ et s_{53} divise 2×19. Or, $2 \not\equiv 1 \pmod{53}$, $19 \not\equiv 1 \pmod{53}$ et $2 \times 19 = 38 \not\equiv 1 \pmod{53}$. Le seul diviseur de 2×19 qui est $\equiv 1 \pmod{53}$ est donc 1, i.e., $s_{53} = 1$. **(0,5 pt)**

d. D'après le b, G contient un sous-groupe distingué H de cardinal 19. D'après le c, G contient un sous-groupe distingué K de cardinal 53. Du coup, HK est un sous-groupe de G de cardinal 19×53, i.e., d'indice 2 dans G.

Montrons que HK est le seul sous-groupe de G d'indice 2. Soit L un sous-groupe de G d'indice 2. Le groupe L est donc de cardinal 19×53. D'après les Théorèmes de Sylow, L contient un 19-sylow H' et un 53-sylow K'. Comme H' est aussi 19-sylow de G, on a $H' = H$. De même, $K' = K$. Du coup, $H \subseteq L$ et $K \subseteq L$, et donc aussi $HK \subseteq L$. Comme HK et L ont même cardinal, on a $HK = L$. Cela montre que HK est l'unique sous-groupe de G de d'indice 2. **(1 pt)**

e. Comme HK est un sous-groupe de G d'indice 2, il est distingué. Il s'ensuit que G est isomorphe à un produit semi-direct de HK et $\mathbb{Z}/2\mathbb{Z}$. Or, d'après le Théorème des groupes pq, le groupe HK est isomorphe à $\mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}$. Par conséquent,

G est isomorphe au produit semi-direct $(\mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}) \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$, où α est un morphisme de $\mathbb{Z}/2\mathbb{Z}$ dans le groupe

$$\mathrm{Aut}(\mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}) \cong \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/52\mathbb{Z}.$$

Il existe 4 de tels morphismes : le morphisme trivial, le morphisme qui envoie 1 sur $(9,0)$, le morphisme qui envoie 1 sur $(0,26)$, et le morphisme qui envoie 1 sur $(9,26)$. Dans le premier cas G est isomorphe à $\mathbb{Z}/2014\mathbb{Z}$, dans le deuxième cas G est isomorphe à $D_{19} \times \mathbb{Z}/53\mathbb{Z}$, dans le troisième cas G est isomorphe à $D_{53} \times \mathbb{Z}/19\mathbb{Z}$, et dans le dernier cas G est isomorphe à D_{1007}. **(1,5 pt)**

f. Rappelons que le groupe diédral D_n contient exactement n éléments d'ordre 2 lorsque n est impair. Il contient donc aussi exactement n 2-sylows. Du coup, si G est isomorphe à $\mathbb{Z}/2014\mathbb{Z}$, il contient exactement 1 2-sylow. Si G est isomorphe à $D_{19} \times \mathbb{Z}/53\mathbb{Z}$, il en contient exactement 19. Si G est isomorphe à $D_{53} \times \mathbb{Z}/19\mathbb{Z}$, il en contient exactement 53. Si G est isomorphe à D_{1007}, il en contient exactement 1007. **(1 pt)**

Exercice 3. a. Définir f sur la base standard de $\mathbb{Z}^3$ par $f(1,0,0) = (1,0,0)$, $f(0,1,0) = (0,1,0)$ et $f(0,0,1) = (0,0,1)$. Comme la famille $(1,0,0),(0,1,0),(0,0,1)$ est génératrice de G, le morphisme f est surjectif. **(0,5 pt)**

b. Un groupe abélien H est de type fini si et seulement s'il existe un morphisme surjectif $g\colon \mathbb{Z}^n \to H$, pour un certain entier naturel n. D'après le a, il existe un morphisme surjectif $f\colon \mathbb{Z}^3 \to G$, le groupe abélien G est donc de type fini. **(0,5 pt)**

c. D'après le cours, tout sous-groupe de $\mathbb{Z}^3$ est de type fini. **(0,5 pt)**

d. Comme K est le sous-groupe $12\mathbb{Z}\times 18\mathbb{Z}\times\{0\}$ de $\mathbb{Z}^3$, la famille $(12,0,0),(0,18,0)$ est génératrice de K. **(0,5 pt)**

e. Définir g sur la base standard par $g(1,0) = (12,0,0)$ et $g(0,1) = (0,18,0)$. Comme la famille $(12,0,0),(0,18,0)$ est génératrice de K, le morphisme g est surjectif. **(0,5 pt)**

f. La matrice de g dans les bases standard est

$$M = \begin{pmatrix} 12 & 0 \\ 0 & 18 \\ 0 & 0 \end{pmatrix}. \quad \textbf{(0,5 pt)}$$

g. On effectue l'algorithme de Smith sur M :

$$\begin{pmatrix} 12 & 0 \\ 0 & 18 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 12 & 18 \\ 0 & 18 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 12 & 6 \\ 0 & 18 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & 6 \\ -36 & 18 \\ 0 & 0 \end{pmatrix} \to$$
$$\begin{pmatrix} 6 & 6 \\ -18 & 18 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 6 & 0 \\ -18 & 36 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 6 & 0 \\ 0 & 36 \\ 0 & 0 \end{pmatrix} \quad \textbf{(1 pt)}$$

h. Soit M' la matrice diagonale $\mathrm{diag}(6,36)$ ci-dessus, obtenue donc à partir de M en effectuant l'algorithme de Smith. Par construction, il existe des matrices $U \in \mathrm{GL}_3(\mathbb{Z})$ et $V \in \mathrm{GL}_2(\mathbb{Z})$ telles que $UMV = M'$. Soit $\mathcal{C}'$ la base de $\mathbb{Z}^3$ constituée des colonnes de la matrice U^{-1}. Soit $\mathcal{B}'$ la base de $\mathbb{Z}^2$ constituée des colonnes de la matrice V. Alors M' est la matrice de g dans les bases $\mathcal{B}'$ et $\mathcal{C}'$. **(0,5 pt)**

i. Par construction, G est isomorphe au conoyau de g. D'après le h, le conoyau de g est isomorphe à $\mathbb{Z}^3/(6\mathbb{Z} \times 36\mathbb{Z} \times \{0\})$. Ce dernier groupe est isomorphe à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}$. **(0,5 pt)**