**Université Toulouse 3,** 2009-2010
L3 Maths Fondamentales, algèbre **Corrigé de l'examen final**

Ceci est un corrigé abrégé.

**Exercice 1** 1. (a) Un calcul immédiat montre que

$$\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p+q \\ 0 & 1 \end{pmatrix} ,$$

donc $H$ est stable par multiplication et par passage à l'inverse. Comme il est évidemment non vide, c'est un sous-groupe.

(b) $H$ est engendré par la matrice

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} .$$

Donc $H$ est cyclique. Il n'est clairement pas distingué, par exemple

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \notin H .$$

2. (a) $A$ et $B$ sont à coefficients dans $\mathbb{Z}$ et de déterminant 1 donc il sont dans $SL(2,\mathbb{Z})$. Un calcul direct montre que $A^3 = -I$, si bien que $A^6 = I$ et $A$ est d'ordre 6. De même $B^2 = -I$ donc $B$ est d'ordre 4.
On note que $BA = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, or cette matrice engendre $H$. Donc $H \subset < A, B >$.

(b) Que pensez-vous des assertions suivantes ?
- C'est faux : $A$ et $B$ sont d'ordre fini, le groupe qu'ils engendrent contient $H$ et est donc infini.
- C'est faux aussi : $BA$ est dans le groupe engendré par $A$ et $B$ mais il n'est pas d'ordre fini, car le sous-groupe qu'il engendre, $H$, est d'ordre infini.

(c) Non, on vérifie immédiatement que $AB \neq BA$.

(d) On rappelle que le sous-groupe engendré par $A$ est constitué de $I, A, A^2, A^3 = -I, A^4 = -A, A^5 = -A^2$. De même, le sous-groupe engendré par $B$ est constitué de $I, B, -I, -B$. Or on vérifie immédiatement que $A, A^2, -A, -A^2$ sont distincts de $B, -B$.

**Exercice 2** 1. Soit $G$ un groupe cyclique, $G$ est isomorphe soit $\mathbb{Z}$, soit à $\mathbb{Z}/n\mathbb{Z}$ pour un certain $n > 0$. Dans le premier cas, les sous-groupes de $G$ correspondent aux $k\mathbb{Z}$ pour $k$ entier, ils sont donc cycliques. Dans le second cas ils sont isomorphes à $\mathbb{Z}/m\mathbb{Z}$, où $m$ est un entier strictement positif qui divise $n$. Dans tous les cas, les sous-groupes de $G$ sont cycliques.

2. Soit $\{a_1, \cdots, a_n\} \subset \mathbb{Q}$, avec $a_i = p_i/q_i$ pour tout $i \in \{1, \cdots, n\}$. Soit $q$ le ppcm des $q_i$. Alors tous les $a_i$ sont dans le sous-groupe de $\mathbb{Q}$ engendré par $1/q$, donc le sous-groupe $H$ engendré par les $a_i$ est inclus dans $< 1/q >$. On a vu que tout sous-groupe d'un groupe cyclique est cyclique, donc $H$ est cyclique. Donc $\mathbb{Q}$ est localement cyclique.

3. Tout sous-ensemble fini de $\mathbb{Q}$ engendre un sous-groupe cyclique, et ne peut donc pas engendrer $\mathbb{Q}$ tout entier. Donc $\mathbb{Q}$ n'est pas de type fini.

**Exercice 3** $255 = 3 \times 5 \times 17$. Soit $G$ un groupe d'ordre 255. Soit $n$ le nombre de 17-Sylow de $G$, les théorèmes de Sylow indiquent que $n$ est congru à 1 modulo 17 et qu'il divise 255. En examinant les nombres de la forme $17k+1$ on voit que le seul qui divise 255 est 1. Donc $n = 1$, $G$ contient un unique 17-Sylow, qui est donc distingué. Donc $G$ n'est pas simple.

**Exercice 4**

1. On va montrer que $A_0 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ contient trois sous-anneaux : $A_0$ lui-même,
$$A_1 = \{(a,a) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \mid a \in \mathbb{Z}/4\mathbb{Z}\} ,$$
$$A_2 = \{(a,b) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \mid b - a \in \{0,2\}\} .$$
On vérifie d'abord que ces trois sous-ensembles sont des sous-anneaux : ce sont des sous-groupes, il contiennent l'élément neutre $(1,1)$ de la multiplication, ils sont stables par multiplication.
Maintenant soit $A \subset \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ un sous-anneau. Alors $A$ contient $(0,0)$ et $(1,1)$. On voit par additions successives que $A$ contient $A_1$.
Supposons que $A$ contienne un élément de la forme $(a, a+1)$, alors, en soustrayant $(a,a) \in A_1$ et $(a+1, a+1)$, on voit que $A$ contient $(0,1)$ et $(-1,0)$, donc, en passant à l'opposé, $A$ contient $(1,0)$ et $(0,1)$. Donc $A = A_0$. Il en est de même si $A$ contient un élément de la forme $(a, a-1)$.
Supposons maintenant que $A$ contient un élément de la forme $(a, a+2)$, alors $A$ contient tous les éléments de cette forme (on le voit en ajoutant un élément de $A_1$). Donc $A_2 \subset A$, et il suit que $A = A_2$ ou bien $A = A_1$.
2. Soit $B = F \times F'$, il est clair que $B$ contient les idéaux non triviaux $\{0\} \times F'$ et $F \times \{0\}$ (ce sont bien des sous-groupes, et ils vérifient la propriété définissant un idéal). On va montrer que ce sont les seuls.
Soit $I \subset B$ un idéal non trivial, donc différent de $\{0\}$ et de $B$. Alors $I$ contient un élément non nul, soit $(a,b)$, avec $a \neq 0$ ou $b \neq 0$. Supposons $a$ et $b$ non nuls, alors $I$ contient $(a,b).(a^{-1}, b^{-1}) = (1,1)$, donc $I = B$, impossible. Donc soit $a$, soit $b$ est nul.
Si $a$ est nul, alors $I$ ne peut pas contenir d'élément de la forme $(a',0)$ avec $a' \neq 0$, sans quoi $I$ contiendrait $(a', b)$ donc $(1,1)$. Donc tous les éléments de $I$ sont de la forme $(0,b')$. De plus tous les éléments de cette forme sont dans $I$ car pour tout $b' \in F'$, $I$ contient $(0,b).(0, b'.b^{-1}) = (0,b')$. Donc $I = \{0\} \times F'$.
Le même argument montre que si $b$ est nul alors $I = F \times \{0\}$.
Comme chacun de ces idéaux est principal, $B$ est un anneau principal.

**Exercice 5** Soit $A$ un anneau intègre et $a, b, c \in A \setminus \{0\}$. Montrer que, chaque fois que les pgcd suivants existent, on a les égalités :

1. Soit $d = \text{pgcd}(a,b)$. Alors $d|a$ et $d|b$. Donc $cd|ca$ et $cd|cb$, et donc $cd|\text{pgcd}(ca, cb)$. De plus, par Bezout, il existe $u, v \in A$ tels que $d = au + bv$, si bien que $cd = cau + cbv$, donc $\text{pgcd}(ca,cb)|cd$. Donc $cd = \text{pgcd}(ca,cb)$.
2. Soit $x \in A$. Alors $x|\text{pgcd}(\text{pgcd}(a,b),c)$ ssi $x|\text{pgcd}(a,b)$ et $x|c$, donc ssi $x|a$ et $x|b$ et $x|c$. Par symétrie c'est vrai ssi $x|\text{pgcd}(a, \text{pgcd}(b,c))$. D'où le résultat.

Si $A$ est en plus factoriel, montrer que

3. Comme $\text{pgcd}(a,b) \sim 1$ et $\text{pgcd}(a,c) \sim 1$, $a$ n'a aucun facteur irréductible commun avec $b$ ou avec $c$, donc avec $bc$, donc $\text{pgcd}(a,bc) \sim 1$.
4. Comme $\text{pgcd}(a,b) \sim 1$, $a$ et $b$ n'ont pas de facteur commun. Comme $a|bc$, tous les facteur irréductibles de $a$ sont présents dans $bc$ avec une puissance au moins égale, donc ils sont tous présents dans $c$ avec une puissance au moins égale, donc $a|c$.

5. Comme $\text{pgcd}(b,c) = 1$, $b$ et $c$ n'ont pas de facteur commun. Comme $b|a$ tous les facteurs irréductibles de $b$ sont présents dans $a$ avec une puissance au moins égale, et de même pour $c$. Donc tous les facteurs irréductibles de $bc$ sont présents dans $a$ avec une puissance au moins égale, donc $bc|a$.

**Exercice 6**

1. Soit $n \in \mathbb{N}^*$. Comme $a \neq -1, 0, 1$, il a au moins un facteur premier $p$. Comme il est sans facteur premiers, $p|a$ mais $p^2$ ne divise pas $a$. On applique le critère d'Einsenstein, il donne immédiatement que $X^n - a$ est irréductible dans $\mathbb{Q}$.
2. Pour $X^4 - 8X^3 + 12X^2 - 6X + 2$ on applique le critère d'Einsenstein avec $p = 2$, pour $X^5 - 12X^3 + 36X - 12$ on l'applique avec $p = 3$ ($p = 4$ ne va pas car 4 n'est pas premier).