Université de Genève
Section de Mathématiques

Algèbre I
Session de printemps 2009
Série 7, corrigé partiel

Ex.6

Dans ce qui suit, on notera a et b deux éléments quelconques de $\mathbb{Z}[P^{-1}]$ *i.e.* deux éléments $a = \frac{r}{p_1^{i_1}\cdots p_k^{i_k}}$ et $b = \frac{s}{q_1^{j_1}\cdots q_l^{j_l}}$ avec $r, s \in \mathbb{Z}$ et, pour tout $m \in [\![1, k]\!]$ et $n \in [\![1, l]\!]$, $p_m, q_n \in P$ et $i_m, j_n \in \mathbb{N}$. Pour montrer que $\mathbb{Z}[P^{-1}]$ est un sous-anneau de $\mathbb{Q}$, il faut montrer que $\mathbb{Z}[P^{-1}]$ est :

- **stable par addition:** l'élément $a + b = \frac{rq_1^{j_1}\cdots q_l^{j_l} + sp_1^{i_1}\cdots p_k^{i_k}}{p_1^{i_1}\cdots p_k^{i_k} q_1^{j_1}\cdots q_l^{j_l}}$ est dans $\mathbb{Z}[P^{-1}]$ puisque le numérateur est dans $\mathbb{Z}$ et que le dénominateur est un produit d'éléments de P ;
- **stable par prise d'inverse:** l'élément $-a = \frac{-r}{p_1^{i_1}\cdots p_k^{i_k}}$ est également dans $\mathbb{Z}[P^{-1}]$;
- **unitaire:** l'ensemble $\mathbb{Z}[P^{-1}]$ contient bien $1 \in \mathbb{Z}$;
- **stable par multiplication:** l'élément $ab = \frac{rs}{p_1^{i_1}\cdots p_k^{i_k} q_1^{j_1}\cdots q_l^{j_l}}$ est enfin lui aussi dans $\mathbb{Z}[P^{-1}]$.

Réciproquement, supposons que A est un sous-anneau de $\mathbb{Q}$. Puisque A est unitaire, on a $1 \in A$. Or A est stable par addition, par récurrence, on a donc $\mathbb{N} \subset A$. Enfin, A est stable par prise d'inverse donc $\mathbb{Z} \subset A$.

Posons maintenant

$$P = \left\{ p \text{ premier} | \exists a, b \in \mathbb{Z}^* \text{ t.q. } \operatorname{pgcd}(a, p) = 1 \text{ et } \frac{a}{bp} \in A \right\}.$$

Soit $a/b \in A \setminus \{0\}$ avec $\operatorname{pgcd}(a, b) = 1$. Par définition de P, tout facteur premier de b est alors dans P et donc $a/b \in \mathbb{Z}[P^{-1}]$. Comme, de plus, $0 \in \mathbb{Z}[P^{-1}]$, on a donc $A \subset \mathbb{Z}[P^{-1}]$.

Montrons l'inclusion réciproque. Pour cela, il suffit de montrer que pour tout $p \in P$, $1/p \in A$, la stabilité par multiplication de A faisant alors le reste. Soit donc $p \in P$, alors il existe $a, b \in \mathbb{Z}^*$ avec $\operatorname{pgcd}(a, p) = 1$ tels que $\frac{a}{bp} \in A$. Mais alors $a/p = b.\frac{a}{bp} \in A$ puisque A contient $\mathbb{Z}$ et est stable par multiplication. Or, $\operatorname{pgcd}(a, p) = 1$ donc, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tq $au + pv = 1$. Mais alors $1/p = \frac{au+pv}{p} = u.\frac{a}{p} + v \in A$ puisque A contient toujours $\mathbb{Z}$ et est stable par addition.