Corrigé des exercices 12, 13, 14 (planche 2)

Exercice 12

Si A est un corps, $x = 0$ convient. Sinon, soit $x_0 \in A$ tel que

$$N(x_0) = \min\{N(x) > 0/\ x \notin A^*\}.$$

Notons $\pi : A \to A_{/(x)}$ la projection canonique. Soit un élément $\pi(y)$ de $A_{/(x)}$. Alors $y \in A$ s'écrit sous la forme $y = qx_0 + r$, avec $r = 0$ ou $N(r) < N(x_0)$. Ceci force $r = 0$ ou $r \in A^*$. De plus on a bien $y \in r + (x)$, donc $\pi(y) = \pi(r)$.
Montrons que tout élément non nul $\pi(y)$ de $A_{/(x)}$ est inversible : il existe $r \in A^* \cup \{0\}$ tel que $\pi(y) = \pi(r)$. En particulier, $r \neq 0$, donc r est inversible et $\pi(y)\pi(r^{-1}) = 1$.

Exercice 13

1. Il est immédiat que N est multiplicative, et que

$$N(u + v\alpha) = (u + v/2)^2 + (v\sqrt{19}/2)^2 = u^2 + uv + 5v^2.$$

   Si $x = u + v\alpha$ est une unité de A, alors il existe $y \in A$ tel que $xy = 1$ et donc en passant à la norme, $N(x)$ est un inversible (positif) de $\mathbb{Z}$. Ainsi $N(x) = 1$, ce qui force $v = 0$ et $u = \pm 1$.

   Réciproquement, si $N(x) = 1$, on a $x = \pm 1$ qui est une unité de A. Finalement : x est une unité de A ssi $N(x) = 1$, ssi $x = \pm 1$.

2. Considérons l'application $\mathbb{Z}[X] \ni P \overset{f}{\mapsto} P(\alpha)$: elle est à valeurs dans A (car $\alpha^2 = \alpha - 5$, et par récurrence toutes les puissances de α sont dans A), et c'est un morphisme d'anneau. Son noyau $\{P \in \mathbb{Z}[X]/\ P(\alpha) = 0\}$ est l'idéal $(X^2 - X + 5)$ (faire la division euclidienne par $X^2 - X + 5$). D'après le théorème de factorisation (pour des anneaux), f passe au quotient en un isomorphisme de $\mathbb{Z}[X]_{/(X^2-X+5)}$ dans A.

   Si B est un anneau et $g : A \to B$ un morphisme d'anneaux, alors $b = g(\alpha)$ convient car $b^2 - b + 5 = g(\alpha^2 - \alpha + 5) = 0$. Réciproquement, si b vérifie $b^2 - b + 5 = 0$, posons $g(u + v\alpha) = u + vb$: g est bien définie car tout élément de A s'écrit de façon unique sous la forme $u + v\alpha$, et on vérifie facilement que g est un morphisme d'anneaux.

   L'équation $x^2 - x + 5 = 0$ n'ayant pas de solutions dans $\mathbb{Z}_{/2\mathbb{Z}}$ et $\mathbb{Z}_{/3\mathbb{Z}}$, il n'existe pas de morphisme de A dans $\mathbb{Z}_{/2\mathbb{Z}}$ ni dans $\mathbb{Z}_{/3\mathbb{Z}}$.

3. Supposons par l'absurde que A est euclidien. D'après l'exercice 12, il existe $x \in A$ non inversible tel que $A_{/(x)}$ soit un corps et il existe une surjection de $A^* \cup \{0\} \to A_{/(x)}$. Or $A^* \cup \{0\} = \{-1; 0; 1\}$, donc $A_{/(x)}$ est un corps à 2 ou 3 éléments. Cela donne un morphisme surjectif de A sur $\mathbb{F}_2$ ou $\mathbb{F}_3$, ce qui contredit la question précédente. Ainsi A n'est pas euclidien.

Exercice 14

1. Soit $a, b \in A$ et $z = a/b = u + v\alpha$ avec $u, v \in \mathbb{Q}$. On cherche $q = k + l\alpha$ $(k, l \in \mathbb{Z})$ tel que $N(z-q) < 1$ ou $N(2z-q) < 1$. On a $N(z-q) = (u-k)^2 + (u-k)(v-l) + 5(v-l)^2$.

   Premier cas : $\mathrm{dist}(v, \mathbb{Z}) \leq 1/3$. Alors comme $\mathrm{dist}(u, \mathbb{Z}) \leq 1/2$, on obtient en prenant k (resp. l) l'entier le plus proche de u (resp. de v) :

   $$N(z-q) \leq \frac{1}{4} + \frac{1}{6} + 5\frac{1}{9} < 1.$$

   Deuxième cas : $\mathrm{dist}(v, \mathbb{Z}) > 1/3$. Alors $2z = 2u + 2v\alpha$, et $\mathrm{dist}(2v, \mathbb{Z}) \leq 1/3$ puisque

   $$[v] + \frac{1}{3} < v < [v] + \frac{2}{3} \Longrightarrow 2[v] + \frac{2}{3} < 2v < 2[v] + 1 + \frac{1}{3}.$$

   On est donc ramené au cas précédent, en prenant k (resp. l) l'entier le plus proche de $2u$ (resp. de $2v$).

2. L'anneau $A_{/(2)}$ est isomorphe à $Z_{/2\mathbb{Z}}[X]_{/(X^2-X+5)}$. Or $X^2 - X + 5$ est de degré 2, sans racine dans $Z_{/2\mathbb{Z}}$, il est donc irréductible, donc premier dans l'anneau factoriel $Z_{/2\mathbb{Z}}[X]$. Puisque $Z_{/2\mathbb{Z}}$ est un corps, $Z_{/2\mathbb{Z}}[X]$ est principal et donc l'idéal $(X^2 - X + 5)$ est maximal. Ainsi $Z_{/2\mathbb{Z}}[X]_{/(X^2-X+5)}$ est un corps, donc $A_{/(2)}$ est un corps et (2) est maximal.

3. Soit b qui minimise $\{N(x) > 0 / x \in I\}$: montrons que $I = (b)$. Soit $a \in I$.

   Premier cas : il existe $q, r \in A$ tels que soit $r = 0$, soit $N(r) < N(b)$, et $a = bq + r$. Comme $a \in I$ et $b \in I$, on a $r \in I$ ce qui par définition de b force $r = 0$: d'où $a = bq \in (b)$.

   Deuxième cas : il existe $q, r \in A$ tels que soit $r = 0$, soit $N(r) < N(b)$, et $2a = bq + r$. De nouveau $r = 0$, c'est-à-dire $2a = bq$. Comme l'idéal (2) est maximal donc premier, 2 est premier dans A et (lemme de Gauss) nécessairement 2 divise b ou q.

   Si 2 divise q, alors $2a = bq = 2bqq'$ *ie* $a = bq' \in (b)$.

   Sinon, $b = 2b'$ et donc $a = b'q$, où $N(b') < N(b)$. Montrons que c'est impossible : il suffit en fait de montrer que $b' \in I$. Puisqu'on a supposé que 2 ne divise pas q *ie* $q \notin (2)$, on a $(q, 2) = A$ car (2) est maximal. Ainsi il existe $x, y \in A$ tels que $1 = qx + 2y$, et

   $$b' = xqb' + 2yb' = xa + yb \in I :$$

   contradiction.

   Finalement $a \in (b)$.