Exercice 8

5. On montre ici que si $p, -p$ ne peuvent pas s'écrire sous la forme $a^2 - db^2$ pour des $a, b \in \mathbb{Z}$ alors p est irréductible dans $\mathbb{Z}[\sqrt{d}]$.

Supposons qu'il existe $u = a + b\sqrt{d}$, $v = a' + b'\sqrt{d} \in \mathbb{Z}(\sqrt{d}$ tels que $u, v \notin \mathbb{Z}[\sqrt{d}]$

$$p = (a + b\sqrt{d})(a' + b'\sqrt{d}).$$

Il vient :

$$p = (aa' + dbb') + (ab' + ba')\sqrt{d}$$

et comme $p \in \mathbb{Z}$ il suit que l'on a $ab' + ba' = 0$. D'autre part

$$ab' + ba' = \begin{vmatrix} a & a' \\ -b & b' \end{vmatrix}$$

et il existe donc $t \in \mathbb{Q}$ tel que l'on ait :

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = t \begin{pmatrix} a \\ -b \end{pmatrix}.$$

On écrit $t = r/s$ avec r, s premiers entre eux. Comme $a', b' \in \mathbb{Z}$ il suit que l'on a $s|a$ et $s|b$. On pose $a'' = a/s, b'' = b/s$ et il suit que

$$p = rs\left((a'')^2 - (b'')^2 d\right).$$

Comme p est irréductible dans $\mathbb{Z}$ il suit que l'on est dans l'un des trois cas suivants :

(1) $rs = \pm 1$;

(2) $s\left((a'')^2 - (b'')^2 d\right) = \pm 1$;

(3) $r\left((a'')^2 - (b'')^2 d\right) = \pm 1$.

Supposons que l'on soit dans le cas 2. Alors $s = \pm 1$ et $\left((a'')^2 - (b'')^2 d\right) = \pm 1$il suit que :

$$N(u) = N(s(a'' - b''\sqrt{d})) = s^2\left((a'')^2 - (b'')^2 d\right) = \pm 1$$

et donc $u \in \mathbb{Z}[\sqrt{d}]^\times$ (par la question 4.), ce qui n'est pas possible vu les hypothèses. De même on voit que l'on ne peut pas être dans le cas 3 (on aurait alors $v \in \mathbb{Z}[\sqrt{d}]^\times$). On doit donc avoir $rs = \pm 1$, c'est-à-dire $t = \pm 1$ et il suit que l'on a

$$p = \pm(a^2 - db^2).$$

On a montré que si p n'est pas irréductible alors p ou $-p$ peut s'écrire sous la forme $a^2 - db^2$ pour des $a, b \in \mathbb{Z}$, ce qui est la contraposée de l'énoncé voulu.

Exercice 9

5. On définit une application :

$$\widetilde{\Phi} : \left\{ \begin{array}{ccc} \mathbb{R}[X] & \to & \mathbb{R} \times \mathbb{R} \\ f & \mapsto & (f(1), f(2)) \end{array} \right. .$$

On a montré en TD que c'est un morphisme surjectif de noyau $(X^2 - 3X + 2)$, d'où il suit par le « théorème d'isomorphisme » qu'elle se factorise en un isomorphisme

$$\Phi : \mathbb{R}[X]/(X^2 - 3X + 2) \to \mathbb{R} \times \mathbb{R}.$$

On va donner ici deux autres démonstrations du deuxième point (le calcul du noyau), qui reposent essentiellement sur les même propriétés de l'anneau $\mathbb{R}[X]$ mais dont la présentation est sensiblement différente. On notera $f = X^2 - 3X + 2$. On note que $f(1) = 0 = f(2)$.

(1) Pour la première démonstration on montre directement que si $h \in \mathbb{R}[X]$ vérifie $h(1) = 0 = h(2)$ alors f divise h. En effet soit $h = fq + r$ la division euclidienne de h par $X^2 - 3X + 2$. On a alors $r(1) = h(1) - f(1)q(1) = 0$ et de même $r(2) = 0$. Comme $\deg(r) < \deg(f) = 2$ il suit que r est un polynôme de degré au plus 1 ayant au moins deux racines, donc forcément $r = 0$ et donc $h = qf$ est divisible par f.

(2) Pour la deuxième preuve on utilise un raisonnement basé sur les idéaux. Le sous-ensemble I de $\mathbb{R}[X]$ défini par :

$$I = \{h \in \mathbb{R}[X] : h(1) = 0 = h(2)\}$$

est un idéal (en effet c'est le noyau de $\tilde{\Phi}$, mais ceci se vérifie aussi directement). Comme $\mathbb{R}[X]$ est principal il existe un polynôme $f_0 \in \mathbb{R}[X]$ tel que $I = (f_0)$. On a $f \in I$ et il existe donc $g \in \mathbb{R}[X]$ tel que $f = gf_0$. Si on avait $\deg(f_0) = 2$ il suivrait que $\deg(g) = 0$, autrement dit $g = c$ pour un $c \in \mathbb{R}$ et donc $(f_0) = (f)$, qui est ce que l'on veut démontrer.

IL suffit donc de montrer que $\deg(f_0) = 2$, ce que l'on va faire dans ce paragraphe. En fait il est suffisant de montrer $\deg(f_0) \geq 2$: comme $(f_0) = I$ contient f qui est de degré 2 on a de toute façon $\deg(f_0) \leq 2$. Supposons donc que $\deg(f_0) \leq 1$. Tout d'abord $f_0 = 0$ n'est pas possible puisque $I \neq (0)$ (il contient f). Mais comme f_0 a au moins deux racines (il est dans I, donc s'annule en 1 et en 2) il n'est pas possible non plus qu'il soit de degré 0 ou 1. On a donc forcément $\deg(f_0) = 2$, ce qui finit la démonstration.

Exercice 14

Si A est un anneau on notera $A[X]_{\leq d}$ l'espace vectoriel des polynômes à coefficients dans A de degré au plus d.

3. On remarque que le pgcd des coefficients de $X^3 - 2X$ est 1, et donc on ne peut pas avoir $n|(X^3 - 2X)$ dans $\mathbb{Z}[X]$ pour un $n \in \mathbb{Z}$ tel que $|n| > 1$. On va voir qu'un polynôme de degré 3 s'écrivant sous la forme PQ pour des $P \in I$ et $Q \in J$ est forcément divisible par 2 ou 3. Ceci implique en particulier que $X^3 - 2X$ ne peut pas s'écrire sous cette forme.

Pour la preuve du fait ci-dessus on va utiliser les deux lemmes suivants :

(1) On a $J \cap \mathbb{Z}[X]_{\leq 1} = 3\mathbb{Z}[X]_{\leq 1}$;

(2) On a $I \cap \mathbb{Z}[X]_{\leq 2} = 2X\mathbb{Z}[X]_{\leq 1}$

En admettant ceci il suit que P est de degré 1, 2 ou 3. S'il est de degré 1 ou 2 alors (à cause de 2) il est divisible par $2X$ et donc par 2, ce qui n'est pas possible puisqu'alors $X^3 - 2X$ le serait aussi. S'il est de degré 3 alors Q est de degré 0 et donc (à cause de 1) divisible par 3, ce qui n'est pas non plus possible.

On va maintenant démontrer 2 et 1. Pour le second on va donner deux preuves.

Pour la première preuve de 1 on suppose que

$$h = (a_d X^d + \cdots + a_0)(X^2 + 1) + 3(b_e X^e + \cdots + b_0) \in \mathbb{Z}[X]_{\leq 1} \in J \cap \mathbb{Z}[X]_{\leq 1}.$$

On voit immédiatement que $e = d + 2$. Supposons que $d = 0$. Alors

$$h = (a_0 + 3b_2)X^2 + 3b_1 X + (3b_0 + a_0)$$

et il vient $a_0 + 3b_2 = 0$, donc $3|a_0$ et en écrivant $a_0 = 3a_0'$ il vient $h = 3(b_1 X + (a_0' + b_0))$ et donc $3|h$. Si $d \geq 1$ on va montrer, de manière similaire mais par récurrence sur $i \geq 0$, que $a_{d-2i} = 0 = a_{d-2i-1}$ pour $i = 0, \ldots, \lfloor d/2 \rfloor$. On a :

$$h = (a_d + 3b_{d+2})X^{d+2} + (a_{d-1} + 3b_{d+1})X^{d+1} + \sum_{i=0}^{\lfloor d/2 \rfloor} (a_{d-2i-2} + a_{d-2i} + 3b_{d-2i})X^{d-2i}.$$

Comme $d+1, d+2 \geq 2$ on voit que $a_d + 3b_{d+2} = 0 = a_{d-1} + 3b_{d+1}$ et donc $3|a_d, a_{d-1}$, ce qui établit le cas $i = 0$. Si $\lfloor d/2 \rfloor \geq i \geq 1$ et $d|a_{d-2i+2}$ alors on a $d - 2i + 1 \geq 2$ et il suit que le coefficient de degré $d - 2i + 2$ de h est nul, donc d'après l'expression ci-dessus

$$a_{d-2i} + a_{d-2i+2} + 3b_{d-2i} = 0$$

puis que $3|a_{d-2i}$ puisque par l'hypothèse de récurrence $3|a_{d-2(i-1)}$. De même on obtient que $3|a_{d-2i-1}$.

La seconde preuve est plus conceptuelle. Vu que $J = (3, X^2 + 1)$ on a un isomorphisme $\Pi : \mathbb{Z}[X]/J \to (\mathbb{Z}/3\mathbb{Z})[X]/(X^2 + 1)$. Comme $\mathbb{Z}/3\mathbb{Z}$ est un corps on voit que $(\mathbb{Z}/3\mathbb{Z})[X]_{\leq 1} \cap (X^2 + 1) = \{0\}$. Et comme $(X^2 + 1)$ est l'image de J par Π on obtient ce qu'on voulait.

Pour prouver 2 on peut faire la même preuve que la première ci-dessus (elle sera un peu simplifiée puisque les deux générateurs sont des monômes) et aussi adapter la seconde. Les deux sont laissées à la lectrice.

Exercice 15

1. On a $0, 1 \in \mathbb{D}$ (en fait $\mathbb{Z} \subset \mathbb{D}$), et si $a = n/10^k$, $b = m/10^l$ sont des éléments de $\mathbb{D}$ alors on a

$$a + b = \frac{10^l n + 10^k m}{10^{k+l}} \in \mathbb{D} \text{ et } ab = \frac{mn}{10^{k+l}} \in \mathbb{D}.$$

Il suit que $\mathbb{D}$ est bien un sous-anneau de $\mathbb{Q}$.

2. Soit $a = n/10^k \in \mathbb{D}$. Comme $\mathbb{Q}$ est un corps a est inversible dans $\mathbb{Q}$, d'inverse $1/a = 10^k/n$, et a est inversible dans $\mathbb{D}$ si et seulement si $1/a \in \mathbb{D}$. Pour que ce soit le cas il faut et il suffit que l'on puisse écrire $|n| = 10^l/m$ pour des entiers $l \geq 0$ et $m \geq 1$, autrement dit les seuls facteurs premiers de n sont ceux de 10, c'est-à-dire 2 et 5. Il suit que les éléments inversibles de $\mathbb{D}$ sont ceux du sous-ensemble donné par :

$$\{\pm 2^k 5^l : k, l \in \mathbb{Z}\}.$$

3. On va plutôt démontrer l'énoncé suivant, qui est plus précis que ce qui est demandé :

Pour tout $d \in \mathbb{D}$ il existe un unique triplet $(d', v, w)ij\mathbb{Z}^3$ tel que $2, 5 \not| d'$ et $d = 2^v 5^w d'$.

Soit $d = n/10^k$ un élément de $\mathbb{D}$. Soient 2^{k_2} et 5^{k_5} les plus grande puissances respectives de 2 et 5 divisant n et $d' = n/2^l 5^k$, $v = k_2 - k$ et $w = k_5 - k$. Alors $d = 2^v 5^w d'$, $2 \not| d'$ (sinon 2^{k_2+1} diviserait n) et de même $5 \not| d'$, ce qui démontre l'existence d'un tel (d', v, w).

Pour démontrer l'unicité on suppose que $2^{v_1} 5^{w_1} d_1 = 2^{v_2} 5^{w_2} d_2$ avec $d_i, v_i \in \mathbb{Z}$ et $2, 5 \not| d_i$ et on va montrer que $v_1 = v_2$, $w_1 = w_2$ et $d_1 = d_2$. Supposons $v_1 \geq v_2$ (l'autre cas se traite exactement de la même manière). Il vient $5^{w_2} d_2 = 2^{v_1 - v_2} 5^{w_1}$. Il suit que $v_1 = v_2$, puisque sinon on airait $v_1 - v_2 \geq 1$ et donc $2|5^{w_2} d_2$, et comme 2 est premier à 5 il suivrait encore que $2|d_2$, ce qui n'est pas le cas par hypothèse. On démontre de même que $w_1 = w_2$. Finalement, on a $2^{v_1} 5^{w_1} d_1 = 2^{v_1} 5^{w_1} d_2$ et il suit que $d_1 = d_2$ puisque $2^{v_1} 5^{w_1} \neq 0$.

4. Soit $d \in \mathbb{D}$, on l'écrit sous la forme $d = 2^v 5^w d'$ comme ci-dessus et on pose

$$N(d) = |d'|.$$

On va montrer que N est un stathme sur $\mathbb{D}$. Il est facile (et laissé au lecteur) de vérifier que l'on a $N(ab) = N(a)N(b)$ pour touts $a, b \in \mathbb{D}$ et comme N est à valeurs entières positives il suit que $N(ab) \geq N(a)$. On va montrer que l'on peut faire des divisions euclidiennes : soient $a, b \in \mathbb{D}$ et a', b' des entiers premiers à $2, 5$ tels que $a = 2^{v(a)} 5^{v(a)} a'$ et $b = 2^{v(b)} 5^{w(b)} b'$. Soit $a' = b'q + r$ la division euclidienne de a' par b'. On peut alors écrire

$$a = b \cdot (q 2^{v(a)-v(b)} 5^{w(a)-w(b)}) + (r 2^{v(a)} 5^{w(a)}) \tag{0.1}$$

et on voit que $N(r 2^{v(a)} 5^{w(a)}) = |r| < |b'| = N(b)$ de sorte que (0.1) est bien une division euclidienne.

5. Si $a = 2^{v(a)}5^{w(a)}a'$, $b = 2^{v(b)}5^{w(b)}b'$ alors les idéaux $(a, b), (a', b')$ endendrés respectivement par a, b et par a', b' dans $\mathbb{D}$ coïncident. On a donc :

$$\left(\frac{46}{10}, \frac{12}{100}\right) = (5^{-1} \cdot 23, 5^{-2} \cdot 3) = (23, 3)$$

et comme $1 = 8 \cdot 3 - 23 \in (23, 3)$ il suit que $\left(\frac{46}{10}, \frac{12}{100}\right) = (1)$ est l'anneau tout entier.