Université Claude Bernard-Lyon 1 Semestre d'automne 2017-2018
Fondamentaux des mathématiques 1
CCP DS4 6 décembre 2017

L'objectif de ce problème est la résolution de l'équation $a^2 - 2b^2 = \pm 1$, avec $(a, b) \in \mathbb{Z}^2$
On pose $\mathbb{Z}[2] = \{a + b\sqrt{2} : (a, b) \in \mathbb{Z}^2\}$

Partie I

1. Montrer que :
   - $\sqrt{2} \notin \mathbb{Q}$
   - $1 \in \mathbb{Z}[2]$
   - Pour tout $x \in \mathbb{Z}[2]$ et $x' \in \mathbb{Z}[2]$: $x + x' \in \mathbb{Z}[2]$ et $xx' \in \mathbb{Z}[2]$
2.
   a. Etablir que pour tout $x \in \mathbb{Z}[2]$, il existe un unique $(a, b) \in \mathbb{Z}$ tel que $x = a + b\sqrt{2}$.
   On pose alors $\overline{x} = a - b\sqrt{2}$, et on l'appelle « conjugué de x ».
   b. Soit $\varphi : \mathbb{Z}[2] \to \mathbb{Z}[2]$ l'application définie par :
   $$\varphi(x) = \overline{x}$$
   Montrer que :
   - $\varphi(1) = 1$
   - Pour tout $x \in \mathbb{Z}[2]$ et $x' \in \mathbb{Z}[2]$, $\varphi(x + x') = \varphi(x) + \varphi(x')$ et $\varphi(xx') = \varphi(x)\varphi(x')$.
   - φ est bijective et déterminer φ^{-1}.
3. Pour $x \in \mathbb{Z}[2]$ on pose $N(x) = x\overline{x}$.
   a. Justifier que pour tout $x \in \mathbb{Z}[2]$, $N(x) \in \mathbb{Z}$, et montrer que pour tout $x \in \mathbb{Z}[2]$ et $x' \in \mathbb{Z}[2]$ $N(xx') = N(x)N(x')$.
   b. Montrer que $x \in \mathbb{Z}[2]$ admet un inverse dans $\mathbb{Z}[2]$ si et seulement si $N(x) = \pm 1$.

Partie II

On se propose dans cette partie de décrire l'ensemble $H = \{x \in \mathbb{Z}[2] : N(x) = \pm 1\}$, ce qui correspond à la résolution de l'équation initialement proposée.

1. Montrer que le produit de deux éléments de H est dans H.
2. Soit $x = a + b\sqrt{2} \in H$. Montrer que :
   a. $a \geq 0$ et $b \geq 0$ entraine que $x \geq 1$.
   b. $a \leq 0$ et $b \leq 0$ entraine que $x \leq -1$.
   c. $ab \leq 0$ entraine que $|x| \leq 1$. On pourra montrer que $|x^{-1}| \geq 1$.
3. On note $H^+ = \{x \in H : x > 1\}$.
   a. Alors montrer que si $x = a + b\sqrt{2} \in H^+$ alors $a > 0$ et $b > 0$.
   b. En déduire que $u = 1 + \sqrt{2}$ est le plus petit élément de H^+.
4. Soit $x \in H^+$
   a. Montrer qu'il existe un unique entier naturel n tel que $u^n \leq x < u^{n+1}$.
   b. En déduire que $x = u^n$. On pourra montrer que $\frac{u^{n+1}}{x} \in H^+$ et que $\frac{u^{n+1}}{x} \leq u$.
   c. Conclure que $H = \{\pm u^n : n \in \mathbb{Z}\}$. On fera une double inclusion. Pour montrer que $H \subset \{\pm u^n : n \in \mathbb{Z}\}$ on distinguera les cas $x > 1$; $x = 1$; $0 < x < 1$ et $x < 0$.

Correction

Partie I

1.

- On suppose qu'il existe $p, q \in \mathbb{N}$ tels que $\sqrt{2} = \frac{p}{q}$, on peut supposer de plus que p et q ne sont pas pairs tous les deux, sinon, on simplifie par 2.
  alors $2q^2 = p^2$, ce qui montre que p^2 est pair, donc p est pair car si p est impair son carré serait lui aussi impair. Il existe $k \in \mathbb{N}$ tel que $p = 2k$, ce que l'on remet dans l'égalité
  $$2q^2 = p^2 \Leftrightarrow 2q^2 = 4k^2 \Leftrightarrow q^2 = 2k^2$$
  Donc q^2 est pair, puis par le même raisonnement que précédemment q est pair, ce qui est impossible, finalement
  $$\sqrt{2} \notin \mathbb{Q}$$
- $1 = 1 + 0 \times \sqrt{2} \in \mathbb{Z}[2]$ car $(1,0) \in \mathbb{Z}^2$
  Soient $x = a + b\sqrt{2} \in \mathbb{Z}[2]$ et $x' = a' + b'\sqrt{2} \in \mathbb{Z}[2]$
- $x + x' = a + b\sqrt{2} + a' + b'\sqrt{2} = (a + a') + (b + b')\sqrt{2} \in \mathbb{Z}[2]$
  Car $a + a' \in \mathbb{Z}$ et $b + b' \in \mathbb{Z}$
- $xx' = \left(a + b\sqrt{2}\right)\left(a' + b'\sqrt{2}\right) = aa' + ab'\sqrt{2} + ba'\sqrt{2} + 2bb' = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in \mathbb{Z}[2]$
  Car $aa' + 2bb' \in \mathbb{Z}$ et $ab' + a'b \in \mathbb{Z}$.

2.

a. L'existence vient de la définition de $\mathbb{Z}[2]$, il faut montrer l'unicité du couple $(a, b) \in \mathbb{Z}$. On suppose qu'il a deux couples $(a, b) \in \mathbb{Z}^2$ et $(a', b') \in \mathbb{Z}^2$ tels que
$$x = a + b\sqrt{2} = a' + b'\sqrt{2} \Rightarrow a - a' = (b' - b)\sqrt{2}$$
Si $b \neq b'$ alors
$$a + b\sqrt{2} = a' + b'\sqrt{2} \Rightarrow \frac{a - a'}{b' - b} = \sqrt{2}$$
Comme $\frac{a-a'}{b'-b} \in \mathbb{Q}$, c'est impossible.
Si $b = b'$ alors
$$a + b\sqrt{2} = a' + b'\sqrt{2} \Rightarrow a = a'$$
Ces deux couples sont donc égaux.

b.
$$\varphi(1) = \varphi\left(1 + 0 \times \sqrt{2}\right) = 1 - 0 \times \sqrt{2} = 1$$
Soient $x = a + b\sqrt{2} \in \mathbb{Z}[2]$ et $x' = a' + b'\sqrt{2} \in \mathbb{Z}[2]$
$$\varphi(x + x') = \varphi\left((a + a') + (b + b')\sqrt{2}\right) = (a + a') - (b + b')\sqrt{2}$$
$$= \left(a - b\sqrt{2}\right) + \left(a' - b'\sqrt{2}\right) = \varphi(x) + \varphi(x')$$
$$\varphi(xx') = \varphi\left((aa' + 2bb') + (ab' + a'b)\sqrt{2}\right) = (aa' + 2bb') - (ab' + a'b)\sqrt{2}$$
Et
$$\varphi(x)\varphi(x') = \left(a - b\sqrt{2}\right)\left(a' - b'\sqrt{2}\right) = (aa' + 2bb') - (ab' + a'b)\sqrt{2} = \varphi(xx')$$
On remarque que pour tout $x \in \mathbb{Z}[2]$.
$$\varphi \circ \varphi(x) = \varphi(\overline{x}) = \overline{\overline{x}} = x$$
Ce qui montre que $\varphi \circ \varphi = Id_{\mathbb{Z}[2]}$, et donc que φ est bijective avec $\varphi^{-1} = \varphi$.

3.

a. Soient $x = a + b\sqrt{2} \in \mathbb{Z}[2]$ et $x' = a' + b'\sqrt{2} \in \mathbb{Z}[2]$

$N(xx') = xx'\overline{xx'} = xx'\varphi(xx') = xx'\varphi(x)\varphi(x') = x\varphi(x)x'\varphi(x') = x\overline{x}x'\overline{x'} = N(x)N(x')$

b. Soit $x \in \mathbb{Z}[2]$.

Si x est inversible dans $\mathbb{Z}[2]$ alors $xx^{-1} = 1$ donc $N(xx^{-1}) = N(1) = 1$, par conséquent $N(x)N(x^{-1}) = 1$, comme $N(x)$ et $N(x^{-1})$ sont des entiers on en déduit que $N(x)$ et $N(x^{-1})$ valent -1 ou 1

Réciproque

Si $N(x) = \pm 1$

Si $N(x) = 1$ alors $x\overline{x} = 1$ donc x est inversible d'inverse $\overline{x} \in \mathbb{Z}[2]$.

Si $N(x) = -1$ alors $x\overline{x} = -1$ donc x est inversible d'inverse $-\overline{x} \in \mathbb{Z}[2]$.

Partie II

1. Soit $x \in H$ et $x' \in H$, $xx' \in \mathbb{Z}[2]$ d'après I.1 $N(xx') = N(x)N(x') = \pm 1 \times \pm 1 = \pm 1$ donc $xx' \in H$.
2.
   a. Comme $(0,0) \notin H$, $(a,b) \neq (0,0)$.

   Si $a > 0$ et $b \geq 0$ donc $a \geq 1$ et $x = a + b\sqrt{2} \geq 1$.

   Si $a \geq 0$ et $b > 0$ donc $b \geq 1$ et $x = a + b\sqrt{2} \geq 1$

   Si $a > 0$ et $b > 0$ même raisonnement.

   En fait tout vient que a et b ne peuvent être nul en même temps.

   b. Comme $(0,0) \notin H$, $(a,b) \neq (0,0)$.

   Si $a < 0$ et $b \leq 0$ donc $a \leq -1$ et $x = a + b\sqrt{2} \leq -1$.

   Si $a \leq 0$ et $b < 0$ donc $b \leq -1$ et $x = a + b\sqrt{2} \leq -1$

   Si $a < 0$ et $b < 0$ même raisonnement.

   En fait tout vient que a et b ne peuvent être nul en même temps.

   c. a et b n'ont pas le même signe.

   Si $x^{-1} = \overline{x} = a - b\sqrt{2} \geq 1$ ou ≤ -1 d'après les questions précédentes.

   Si $x^{-1} = \overline{x} = -a + b\sqrt{2} \geq 1$ ou ≤ -1 d'après les questions précédentes.

   Ce qui montre que $|x^{-1}| \geq 1$, par conséquent $|x| = \frac{1}{|x^{-1}|} \leq 1$.
3.
   a. Soit $x = a + b\sqrt{2} \in H^+$, on a $x > 1$ et grâce à la question 1. on en déduit que $a \geq 0$ et $b \geq 0$. En effet si a et b sont négatifs c'est impossible à cause de 1.b., s'ils sont de signes opposés c'est impossible à cause de 1.c.

   Est-ce que a et b peuvent être nul ? Si $a = 0$ l'équation $a^2 - 2b^2 = 1$ n'a pas de solution, si $b = 0$ alors l'équation $a^2 - 2b^2 = 1$ devient $a^2 = 1$, ce qui implique que $x = 1$, là encore c'est impossible puisque $x > 1$. Par suite $a > 0$ et $b > 0$.

   b. $u = 1 + \sqrt{2} \in H^+$. Car $u > 1$ et $N(u) = 1^2 - 2 \times (1^2) = -1$. De plus pour tout $x \in H^+$, $x = a + b\sqrt{2}$ avec $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ donc $x \geq u$

   Ainsi u est le plus petit élément de H^+.
4.
   a. On pose $n = E\left(\frac{\ln(x)}{\ln(u)}\right) = \left\lfloor \frac{\ln(x)}{\ln(u)} \right\rfloor$, la partie entière de $\frac{\ln(x)}{\ln(u)}$.

$$n \leq \frac{\ln(x)}{\ln(u)} < n+1 \Leftrightarrow n\ln(u) < \ln(x) \leq (n+1)\ln(u) \Leftrightarrow \ln(u^n) \leq \ln(x) < \ln(u^{n+1}) \Leftrightarrow u^n \leq x < u^{n+1}$$

b. Comme $u \in \mathbb{Z}[2]$, d'après I.1. $u^2 \in \mathbb{Z}[2]$, par une récurrence immédiate $u^n \in \mathbb{Z}[2]$
Comme $u \in H$, d'après I.3.a. $N(u^2) = N(u)N(u) = 1$ et par une récurrence immédiate, pour tout $p \in \mathbb{N}$, $N(u^{2p}) = 1$ et $N(u^{2p+1}) = -1$. Finalement pour tout $n \in \mathbb{N}$, $u^{n+1} \in H$.
Si $x \in H$ alors $\frac{1}{x} = x^{-1} \in H$, d'après I.3.b.
On en déduit que $\frac{u^{n+1}}{x} \in H$ d'après II.1. et puisque $\frac{u^{n+1}}{x} > 1$, $\frac{u^{n+1}}{x} \in H^+$

$$\frac{u^{n+1}}{x} = u\frac{u^n}{x} \leq u\frac{x}{x} = u$$

D'après II.4.a.
De plus u est le plus petit élément de H^+ ce qui entraine que

$$\frac{u^{n+1}}{x} = u$$

En simplifiant par u, on en déduit que $x = u^n$.

c. Puisque $u \in H$, $\forall n \in \mathbb{Z}$, $u^n \in H$. De plus $-1 \in H$ donc $\forall n \in \mathbb{Z}, -u^n \in H$, ainsi

$$\{\pm u^n, n \in \mathbb{Z}\} \subset H$$

Inversement
Soit $x \in H$, donc $x \neq 0$
Si $x > 1$ alors $x \in H^+$ donc il existe $n \in \mathbb{N}$ tel que $x = u^n$
Si $x = 1$ alors $x = u^0$.
Si $0 < x < 1$ alors $\frac{1}{x} = x^{-1} \in H^+$ et donc il existe $n \in \mathbb{N}$ tel que $\frac{1}{x} = u^n$, ce qui équivaut à $x = u^{-n}$
Si $x < 0$ alors $y = -x = (-1)x \in H$ car -1 et x sont dans H, puisque $y > 0$, d'après les trois premiers cas, il existe $n \in \mathbb{Z}$ tel que $y = u^n$ et donc $x = -u^n$ et dans tous les cas $x \in \{\pm u^n, n \in \mathbb{Z}\}$ ce qui montre que $H \subset \{\pm u^n, n \in \mathbb{Z}\}$ et finalement

$$\{\pm u^n, n \in \mathbb{Z}\} = H$$