Correction des exercices du 23/09/2024 (Structures algébriques)

Ex 1 : On pose $u = 2 + \sqrt{3}$ et $v = 2 - \sqrt{3}$. Pour $n \in \mathbb{N}$, on note $M_n = 2^n - 1$ et $s_n = u^{2^n} + v^{2^n}$.

1. Montrer que si M_n est premier, alors n est premier.
2. Montrer que : $\forall n \in \mathbb{N},\ s_{n+1} = s_n^2 - 2$. Qu'en déduire sur la suite (s_n) ?
3. Soit q un nombre premier. On munit l'ensemble $B = (\mathbb{Z}/q\mathbb{Z})^2$ des deux lois de composition interne définies par :

$$(x, y) + (x', y') = (x + x', y + y') \quad \text{et} \quad (x, y).(x', y') = (xx' + 3yy', xy' + x'y).$$

   (a) Montrer que les deux lois précédentes munissent B d'une structure d'anneau commutatif fini.

   (b) On note $A = \mathbb{Z} + \sqrt{3}\mathbb{Z}$. Montrer que l'application $\pi : \left\{ \begin{array}{ccc} A & \to & B \\ a + \sqrt{3}b & \mapsto & (\overline{a}, \overline{b}) \end{array} \right.$ est bien défini et est un morphisme surjectifs d'anneaux.

4. On suppose n premier. Montrer que si M_n divise s_{n-2}, alors M_n est premier.
   Indication : on pourra raisonner par l'absurde en considérant le plus petit facteur premier q de M_n et déterminer l'ordre de $(\overline{2}, \overline{1})$ dans le groupe des éléments inversibles de l'anneau B.

Correction :

1. Supposons n composé, on écrit $n = ab$ avec $a \geq 2$, $b \geq 2$. La factorisation $X^{ab} - 1 = (X^a)^b - 1 = (X^a - 1)\displaystyle\sum_{k=0}^{b-1} X^{ka}$ évaluée en $X = 2$ permet d'affirmer que $2^a - 1$ divise M_n.
   On a :$1 = 2^1 - 1 < 2^a - 1 < 2^n - 1 = M_n$, donc M_n n'est pas premier, ce qui termine la preuve par contraposée.
2. Soit $n \in \mathbb{N}$, on a $s_n^2 = (u^{2^n})^2 + 2u^{2^n}v^{2^n} + (v^{2^n})^2 = s_{n+1} + 2(uv)^{2^n} = s_{n+1} + 2$ car $uv = 1$.
   Par récurrence on montre que s_n est un entier et $s_n \geq 4$.
   Ainsi $s_{n+1} = (s_n - \sqrt{2})(s_n + \sqrt{2}) \geq s_n + \sqrt{2} > s_n$, donc la suite (s_n) est strictement croissante.
   On montre par récurrence que : $\forall n \in \mathbb{N},\ s_n \geq n$, ce qui permet de dire que $\lim s_n = +\infty$.
3. (a) L'ensemble $(B, +)$ est un groupe additif fini d'après le cours. La multiplication est bien une loi de composition interne commutative dont $(1, 0)$ est le neutre par vérification immédiate.
   On vérifie ensuite que

$$\begin{aligned}((x, y).(x', y')).(u, v) &= (xx' + 3yy', xy' + x'y).(u, v) \\ &= (xx'u + 3yy'u + 3(xy' + x'y)v, xx'v + 3yy'v + xy'u + x'yu)\end{aligned}$$

   et

$$\begin{aligned}(x, y).((x', y').(u, v)) &= (x, y).(x'u + 3y'v, x'v + y'u) \\ &= (x(x'u + 3y'v) + 3y(x'v + y'u), xx'v + xy'u + y(x'u + 3y'v))\end{aligned}$$

   ce qui prouve l'associativité de la multiplication.
   Pour la distributivité, on vérifie bien que

$$((x, y) + (x', y')).(u, v) = (x.y).(u, v) + (x', y').(u, v)$$

   ce qui termine la preuve.
   B est fini, car $|B| = |\mathbb{Z}/q\mathbb{Z}| \times |\mathbb{Z}/q\mathbb{Z}| = q^2$.

(b) Tout d'abord, π est bien définie car si $x = a + b\sqrt{3} \in A$, l'irationnalité de $\sqrt{3}$ entraîne l'unicité du couple (a, b) d'entiers de cette décomposition. En effet, si $a + b\sqrt{3} = a' + b'\sqrt{3}$, alors $(b' - b)\sqrt{3} = a - a'$, ce qui est absurde si $b \neq b'$, donc $b = b'$, puis $a = a'$.

L'application π est clairement un morphisme de groupes additifs, il suffit ensuite de remarquer que dans A, $(a + b\sqrt{3})(a' + b'\sqrt{3}) = aa' + 3bb' + \sqrt{3}(ab' + a'b)$ pour en déduire que $\pi(xy) = \pi(x)\pi(y)$.

Enfin, on a $\pi(1) = (1, 0)$, ce qui prouve que π est un morphisme d'anneaux. Le caractère surjectif de B provient directement du fait de la définition de B, l'élément $a + b\sqrt{3}$ est un antécédent du couple $(\overline{a}, \overline{b})$ (on choisit des représentants des classes d'équivalences dans $[\![0, q-1]\!]$).

4. Soit q le plus petit facteur premier de M_n que l'on suppose différent de M_n. On a donc $M_n \geq q^2$. Prouvons que $(\overline{2}, \overline{1})$ est exactement d'ordre 2^n dans B, on notera $0_B = (\overline{0}, \overline{0})$ et $1_B = (\overline{1}, \overline{0})$ les neutres respectifs de B pour l'addition et la multiplication. Le groupe des inversibles de l'anneau B est fini, donc $(\overline{2}, \overline{1})$ est d'ordre fini. Dans l'anneau B, $\pi(u) = (\overline{2}, \overline{1})$, et $\pi(s_{n-2}) = (\overline{s_{n-2}}, \overline{0}) = 0_B$, donc $\pi(u)^{2^{n-2}} + \pi(v)^{2^{n-2}} = 0_B$, or $\pi(u)\pi(v)\pi(1) = 1_B$ d'où $\pi(v) = \pi(u)^{-1}$, ce qui donne encore $\pi(u)^{2^{n-2}} = -\pi(u)^{-2^{n-2}}$, ce qui donne enfin $\pi(u)^{2^{n-1}} = -1_B$. En conclusion, $\pi(u)^{2^n} = 1_B$, donc l'ordre de $\pi(u)$ divise 2^n, et puisque $\pi(u)^{2^{n-1}} \neq 1_B$ (q est impair), l'ordre de $\pi(u)$ est exactement 2^n, ce qui prouve que le groupe des inversibles de B est de cardinal au moins 2^n et au plus $q^2 - 1$. On obtient donc l'inégalité $2^n \leq q^2 - 1 \leq M_n - 1 = 2^n - 2$, ce qui est absurde par définition de M_n.
Ainsi M_n n'a pas de facteurs premiers strictement inférieur, donc il est premier.

<u>Ex 2</u> : CV de $\sum \left(\frac{1}{n}\right)^{1+\frac{1}{n}}$.

Correction : On a : $\left(\frac{1}{n}\right)^{1+\frac{1}{n}} = \frac{1}{n} \times \left(\frac{1}{n}\right)^{\frac{1}{n}} = \frac{1}{n} \times e^{\frac{1}{n}\ln\left(\frac{1}{n}\right)} = \frac{1}{n} \times e^{-\frac{\ln(n)}{n}}$. Or : $\lim\limits_{n \to +\infty} \frac{\ln(n)}{n} = 0$, par croissance comparée et donc : $\lim\limits_{n \to +\infty} e^{-\frac{\ln(n)}{n}} = 1$, puis $e^{-\frac{\ln(n)}{n}} \underset{n \to +\infty}{\sim} 1$, puis $\left(\frac{1}{n}\right)^{1+\frac{1}{n}} \underset{n \to +\infty}{\sim} \frac{1}{n}$ et par comparaison de séries à termes négatifs, $\sum \left(\frac{1}{n}\right)^{1+\frac{1}{n}}$ diverge.