Khôlleur : Dorian Cacitti-Holland
Elève :

Question de cours. Soit $n \in \mathbb{N}^*$, quels sont les générateurs de $\mathbb{Z}/n\mathbb{Z}$?

Réponse. Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\overline{k}$ avec k entier premier avec n.

Démonstration. Soit $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ générateur de $\mathbb{Z}/n\mathbb{Z}$.
En particulier il existe $u \in \mathbb{Z}$ tel que $\overline{1} = u\overline{k} = \overline{uk}$.
Donc $n \mid 1 - uk$, ie il existe $v \in \mathbb{Z}$ tel que $1 - uk = vn$, ie $1 = uk + vn$.
Ainsi, d'après le théorème de Bézout, k et n sont premiers entre eux.
Réciproquement soit $k \in \mathbb{Z}$ tel que k soit premier avec n.
Alors, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$, tel que $1 = un + kv$. Donc, pour $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$, on a

$$\overline{m} = 1 \times \overline{m} = un\overline{m} + kv\overline{m} = \overline{0} + \overline{k}\overline{um}$$

Donc $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$. □

Exercice. Déterminer tous les morphismes de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$.

Réponse. Le seul morphisme de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$ est le morphisme identiquement nul.

Démonstration. Soit f un morphisme de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$, alors $f(\mathbb{Q})$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $f(\mathbb{Q}) = n\mathbb{Z}$, avec $n \in \mathbb{N}$.
On suppose par l'absurde que $n \geq 1$.
Soit $x \in \mathbb{Q}$ tel que $f(x) = n$, alors $2f\left(\frac{x}{2}\right) = f(x) = n$, donc

$$\frac{n}{2} = f\left(\frac{x}{2}\right) \in f(\mathbb{Q}) = n\mathbb{Z}$$

ce qui est absurde.
Par conséquent $n = 0$ et f est le morphisme identiquement nul. □

Exercice. On considère $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$ et pour $z \in \mathbb{Z}[i]$, $N(z) := |z|^2$.

1. Montrer que $\mathbb{Z}[i]$ est un anneau commutatif unitaire.
2. Montrer que N est une application à valeurs dans $\mathbb{N}$ et multiplicative.
3. Déterminer les éléments inversibles de $\mathbb{Z}[i]$.
4. Montrer que N est un stathme sur $\mathbb{Z}[i]$, ie une application de $\mathbb{Z}[i]\backslash\{0\}$ dans $\mathbb{N}$ telle que pour tout $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]\backslash\{0\}$, il existe $q, r \in \mathbb{Z}[i]$ tel que $z = qw + r$ et $N(r) < N(w)$ ou $r = 0$.

Démonstration.

1. On considère $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{C}$ définie par $\forall P \in \mathbb{Z}[X], \varphi(P) = P(i)$.
   Ainsi φ est un morphisme d'anneaux et $\mathbb{Z}[i] = \varphi(\mathbb{Z}[X])$.
   Donc $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, en particulier un anneau commutatif et unitaire car $1 \in \mathbb{Z}[i]$.

2. Soit $z = a + ib \in \mathbb{Z}[i]$, alors $N(z) = |z|^2 = a^2 + b^2 \in \mathbb{N}$.
   De plus pour $z' \in \mathbb{Z}[i]$, par propriété du module sur $\mathbb{C}$, on a
   $$N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z')$$

3. Soit $z \in \mathbb{Z}[i]^\times$, alors il existe $z' \in \mathbb{Z}[i]$, tel que $1 = zz'$.
   Ainsi $1 = N(1) = N(z)N(z')$ car N est multiplicative.
   Or N est à valeurs dans $\mathbb{N}$, donc $1 = N(z)$.
   De plus il existe $a, b \in \mathbb{Z}$ tels que $z = a + ib$, donc $1 = a^2 + b^2$.
   Par conséquent $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$, ie $z \in \{1, -1, i, -i\}$.
   Réciproquement $1, -1, i, -i$ sont inversibles.
   Par conséquent $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

4. Soit $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]\backslash\{0\}$.
   Alors $\frac{z}{w} \in \mathbb{C}$, donc il existe $x, y \in \mathbb{R}$ tels que $\frac{z}{w} = x + iy$.
   On considère
   $$a = \begin{cases} \text{Ent}(x) & \text{si } x - \text{Ent}(x) \leq \text{Ent}(x) - x + 1 \\ \text{Ent}(x) + 1 & \text{sinon} \end{cases}$$
   et
   $$b = \begin{cases} \text{Ent}(y) & \text{si } y - \text{Ent}(y) \leq \text{Ent}(y) - y + 1 \\ \text{Ent}(y) + 1 & \text{sinon} \end{cases}$$
   Ainsi, en notant $q = a + ib \in \mathbb{Z}[i]$, on obtient
   $$\left|\frac{z}{w} - q\right| \leq \frac{\sqrt{2}}{2}$$
   Par conséquent, en notant $r = z - wq \in \mathbb{Z}[i]$, on obtient
   $$z = wq + r$$
   et
   $$N(r) = N(z - wq) \leq \frac{1}{2}N(w) < N(w)$$

□

Exercice. Soit $n \in \mathbb{N}^*$ et K un corps fini de cardinal q.

1. Calculer le cardinal de $GL_n(K)$.
   Indication : Dénombrer les bases de K^n.
2. En déduire le cardinal de $SL_n(K)$.
3. On considère T l'ensemble des matrices carrés de taille n à coefficients dans K, triangulaires supérieures avec uniquement des 1 sur la diagonale, montrer que T est un sous-groupe de $GL_n(K)$ et calculer son cardinal.

Réponse.

1. $|GL_n(K)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1)$.

2. $|SL_n(K)| = \frac{|GL_n(K)|}{|K^*|} = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n}(q^i - 1)$.

3. $|T| = q^{\frac{n(n-1)}{2}}$

Démonstration.

1. On considère l'application $\varphi : GL_n(K) \longrightarrow (K^n)^n$ définie par, pour $M \in GL_n(K)$, $\varphi(M) = (C_1, ..., C_n)$ en notant $C_1, ..., C_n$ les vecteurs colonnes de la matrice M.
   Or, pour $M \in GL_n(K)$, ses vecteurs colonnes $C_1, ..., C_n$ forment une base de l'espace vectoriel $C_1, ..., C_n$.
   Ainsi, l'application φ est à valeurs dans l'ensemble des bases vectorielles de K^n.
   De plus, l'application φ est injective et surjective, donc bijective.
   Par conséquent $|GL_n(K)|$ est égal au nombre de bases vectorielles de K^n.
   Or, pour avoir une base de K^n, il faut et il suffit de choisir un vecteur non nul dans K^n ($q^n - 1$ choix possibles) puis de choisir un vecteur non colinéaire au premier ($q^n - q$ choix possibles), puis un vecteur n'appartenant pas au plan engendré par les deux premiers vecteurs ($q^n - q^2$ choix possibles), ainsi de suite, jusqu'à choisir le n-ième vecteur parmi les vecteurs de K^n n'appartenant pas au sous-espace engendré par les $n-1$ vecteurs précédemment choisis ($q^n - q^{n-1}$ choix possibles).
   On a donc $(q^n - 1)(q^n - q)...(q^n - q^{n-1}) = \prod_{j=0}^{n-1}(q^n - q^j)$ choix possibles pour une base de K^n.
   Par conséquent, d'après ce qui précède,

$$|GL_n(K)| = \prod_{j=0}^{n-1}(q^n - q^j) = \prod_{j=0}^{n-1} q^j(q^{n-j} - 1) = q^{\sum_{j=0}^{n-1} j} \prod_{i=1}^{n}(q^i - 1) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1)$$

2. En considérant le morphisme de groupes surjectif déterminant $det : GL_n(K) \longrightarrow K^*$, on a $SL_n(K) = \ker(\det)$
   Donc

$$|SL_n(K)| = \frac{|GL_n(K)|}{|K^*|} = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n}(q^i - 1)$$

3. L'ensemble T est en bijection avec $K^{\frac{n(n-1)}{2}}$.
   En effet pour choisir une matrice dans T il faut et il suffit de choisir $\frac{n(n-1)}{2}$ éléments dans K correspondants aux coefficients supérieurs de la matrice.
   Par conséquent

$$|T| = q^{\frac{n(n-1)}{2}}$$

□

Khôlleur : Dorian Cacitti-Holland
Elève :

Question de cours. Pour K un corps, de quelle forme sont les idéaux de $K[X]$?

Réponse. Les idéaux de l'anneau $K[X]$ sont exactement de la forme $\langle P\rangle$ avec $P \in K[X]$. Plus précisément, pour I idéal de $K[X]$, il existe un unique $P \in K[X]$ unitaire tel que $I = \langle P\rangle$.

Démonstration.
Condition nécessaire : Soit I idéal de $K[X]$.
Distinguons deux cas :

— Soit $I = \{0\}$, et dans ce cas $I = \langle 0\rangle$.
— Soit $I \neq \{0\}$.
On considère alors $D = \{\deg(P), P \in I\backslash\{0\}\}$ partie non vide de $\mathbb{N}$.
La partie D admet donc un élément minimal n_0 : il existe $P_0 \in I\backslash\{0\}$ tel que

$$\forall P \in I, \deg(P) \geq n_0 = \deg(P_0)$$

Soit $P \in I$. Effectuons la division euclidienne de P par P_0 : il existe $Q, R \in K[X]$ tels que $P = QP_0 + R$ et $\deg(R) < \deg(P_0)$.
Ainsi $R = P - QP_0 \in I$ puis par caractère minimal de $n_0 = \deg(P_0)$, on a $R = 0$ ie $P = QP_0 \in \langle P_0\rangle$.
Par conséquent $I \subset \langle P_0\rangle$.
Réciproquement $\langle P_0\rangle \subset I$, donc $I = \langle P_0\rangle$.

Condition suffisante : Soit $P \in K[X]$, alors $\langle P\rangle$ est un idéal de $K[X]$.
Unicité si unitaire : Soit $P_1, P_2 \in K[X]$ unitaires tel que $\langle P_1\rangle = \langle P_2\rangle$.
Alors $P_1 \mid P_2$ et $P_2 \mid P_1$, donc il existe $Q_1, Q_2 \in K[X]$ tels que $P_2 = Q_1P_1$ et $P_1 = Q_2P_2$.
Ainsi $P_2 = Q_1Q_2P_2$, puis, par intégrité de l'anneau $K[X]$, $1 = Q_1Q_2$.
Par conséquent $Q_1, Q_2 \in K^*$.
De plus P_1 et P_2 sont unitaires, donc $1 = \mathrm{cd}(P_2) = Q_1\mathrm{cd}(P_1) = Q_1$ puis $P_2 = P_1$. □

Exercice. Soit G un groupe admettant un nombre fini de sous-groupes.

1. Soit $x \in G$, montrer que x est d'ordre fini.
2. Montrer que G est fini.
Indication : Considérer E l'ensemble des sous-groupes de G et F l'ensemble des sous-groupes monogènes de G.

Démonstration.

1. On suppose par l'absurde que x est d'ordre infini.
Alors le sous-groupe $\langle x\rangle$ est isomorphe à $\mathbb{Z}$ admettant une infinité de sous-groupes ce qui est absurde par hypothèse.
Par conséquent x est d'ordre fini.
2. On considère E l'ensemble des sous-groupes de G et F l'ensemble des sous-groupes monogènes de G.
Alors $G = \bigcup_{H\in F} H$ car pour $x \in G$, $x \in \langle x\rangle$ avec $\langle x\rangle$ monogène.

Or, par hypothèse E est fini, donc F est fini comme sous-ensemble de E.
De plus, pour $H \in F$, d'après la question précédente, H est fini car engendré par un élément x d'ordre fini.
Par conséquent G est fini comme réunion fini d'ensembles finis.

□

Exercice. On considère $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$.

1. Montrer que $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $\mathbb{R}$.
2. Déterminer tous les automorphismes de $\mathbb{Q}(\sqrt{2})$.

Démonstration.

1. On considère le morphisme d'anneaux $\varphi : \mathbb{Q}(X) \longrightarrow \mathbb{R}$ défini par $\varphi(P) = P(\sqrt{2})$ pour $P \in \mathbb{Q}(X)$.
   Ainsi $\mathbb{Q}(\sqrt{2}) = \varphi(\mathbb{Q}(X))$ avec $\mathbb{Q}(X)$ un corps et φ un morphisme de corps entre les corps $\mathbb{Q}(X)$ et $\mathbb{R}$.
   Donc $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $\mathbb{R}$.
2. Soit $f \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$.
   Alors pour $n \in \mathbb{N}$, $f(n) = nf(1) = n$, puis $f(-n) + f(n) = f(0) = 0$, ainsi on a également $f(-n) = -f(n) = -n$.
   Et pour $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, on a $qf\left(\frac{p}{q}\right) = f(p) = p$, donc $f\left(\frac{p}{q}\right) = \frac{p}{q}$. Enfin, comme $f(\sqrt{2})^2 = f(2) = 2$, on a $f(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$.
   Par conséquent
   $$\forall a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}), f(a + b\sqrt{2}) = a + \varepsilon b\sqrt{2}$$
   avec $\varepsilon \in \{-1, 1\}$.
   Réciproquement ces deux applications définissent bien des automorphismes de $\mathbb{Q}(\sqrt{2})$.

□

Exercice. Soit $n \in \mathbb{N}$ avec $n \geq 2$, et on considère, pour $r \in \mathbb{R}_+^*$, $N(r)$ le nombre de points de $\mathbb{Z}^n$ de norme inférieure ou égale à r.

1. Pour $n = 2$, montrer que $N(r) \underset{r\to+\infty}{\sim} \pi r^2$ l'aire du disque de rayon r.
   Indication : Considérer les hypercubes $C_x = \left\{t \in \mathbb{R}^n, \forall i \in [\![1, n]\!], |t_i - x_i| \leq \frac{1}{2}\right\}$ pour $x \in \mathbb{Z}^n$.
2. Dans le cas général, en considérant b_n le volume de la boule unité dans $\mathbb{R}^n$, montrer que $N(r) \underset{r\to+\infty}{\sim} b_n r^n$.

Démonstration.

1. Soit $x \in \mathbb{Z}^n$, on considère l'hypercube de côté 1 centrée en x
   $$C_x = \left\{t \in \mathbb{R}^n, \forall i \in [\![1, n]\!], |t_i - x_i| \leq \frac{1}{2}\right\}$$

Ces hypercubes sont de volume 1, donc, pour $r \in \mathbb{R}_+^*$, le volume de leur réunion est $\mathcal{V}\left(\bigcup_{x\in\overline{B}(0,r)} C_x\right) = N(r)$.
Dans le cas $n = 2$, on a

$$\forall x \in \mathbb{Z}^n, \forall t \in C_x, \|t - x\| \leq \frac{\sqrt{2}}{2}$$

Donc, pour $r \in \mathbb{R}_+^*$,

$$\forall x \in \overline{B}(0,r), \forall t \in C_x, \|t\| \leq \|x\| + \frac{\sqrt{2}}{2} \leq r + \frac{\sqrt{2}}{2}$$

Ainsi $\bigcup_{x\in\overline{B}(0,r)} C_x \subset \overline{B}\left(0, r + \frac{\sqrt{2}}{2}\right)$, d'où, d'après l'égalité précédente, $N(r) \leq \pi\left(r + \frac{\sqrt{2}}{2}\right)^2$.
De même, pour r assez grand, $\overline{B}\left(0, r - \frac{\sqrt{2}}{2}\right) \subset \bigcup_{x\in\overline{B}(0,r)} C_x$, donc

$$\pi\left(r - \frac{\sqrt{2}}{2}\right)^2 \leq N(r) \leq \pi\left(r + \frac{\sqrt{2}}{2}\right)^2$$

ce qui montre bien que $N(r) \underset{r\to+\infty}{\sim} \pi r^2$.

2. Par homogénéité le volume de $\overline{B}(0,r)$, pour $r \in \mathbb{R}_+^*$, est $V(r) = b_n r^n$.
De même la distance maximale d'un point d'un de nos hypercubes à son centre est $\frac{\sqrt{n}}{2}$, donc l'inégalité précédente s'écrit

$$b_n\left(r - \frac{\sqrt{n}}{2}\right)^n \leq N(r) \leq b_n\left(r + \frac{\sqrt{n}}{2}\right)^n$$

ce qui montre bien que $N(r) \underset{r\to+\infty}{\sim} b_n r^n$.

□

Khôlleur : Dorian Cacitti-Holland
Elève :

Question de cours. Parmi les ensembles suivants $\mathbb{Q}, \mathbb{R}$ et $\mathbb{R}\backslash\mathbb{Q}$, lesquels sont dénombrables ? Le démontrer.

Réponse. L'ensemble $\mathbb{Q}$ est dénombrable alors que les ensembles $\mathbb{R}$ et $\mathbb{R}\backslash\mathbb{Q}$ ne le sont pas.

Démonstration.
L'ensemble $\mathbb{Q}$ est dénombrable : Soit $x \in \mathbb{Q}$, alors il existe un unique couple $(p_x, q_x) \in \mathbb{Z}\times\mathbb{N}^*$ tel que $x = \frac{p_x}{q_x}$ et p_x et q_x soient premiers entre eux.
On peut donc considérer l'application $\begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{Z}\times\mathbb{N}^* \\ x & \longmapsto & (p_x, q_x) \end{array}$.
Cette application est injective car : pour $x, y \in \mathbb{Q}$ tels que $p_x = p_y$ et $q_x = q_y$, alors on a $x = \frac{p_x}{q_x} = \frac{p_y}{q_y} = y$.
Ainsi l'ensemble $\mathbb{Q}$ s'injecte dans $\mathbb{Z}\times\mathbb{N}^*$ qui s'injecte dans $\mathbb{Z}\times\mathbb{Z}$ dénombrable comme produit cartésien de deux ensembles dénombrables.
L'ensemble $\mathbb{R}$ n'est pas dénombrable : On suppose par l'absurde que $\mathbb{R}$ est dénombrable.
Alors l'intervalle $[0,1[\subset \mathbb{R}$ est dénombrable, on peut donc écrire $[0,1[= (x_n)_{n\in\mathbb{N}}$.
On construit ensuite $x \in [0,1[$ de la manière suivante :

- Si d_n la n-ième décimale de x_n est différente de 9 alors la n-ième décimale de x est $d_n + 1$
- Si d_n la n-ième décimale de x_n est 9 alors la n-ième décimale de x est 0

Par conséquent x appartient bien à $[0,1[$ mais n'appartient pas $(x_n)_{n\in\mathbb{N}}$ ce qui est absurde.
L'ensemble $\mathbb{R}\backslash\mathbb{Q}$ n'est pas dénombrable : Si on suppose par l'absurde que $\mathbb{R}\backslash\mathbb{Q}$ est dénombrable alors $\mathbb{R} = \mathbb{R}\backslash\mathbb{Q} \cup \mathbb{Q}$ serait dénombrable ce qui n'est pas. □

Exercice. Soit G un groupe abélien fini (dont la loi est notée multiplicativement).

1. Soit $x, y \in G$ d'ordres respectifs a, b premiers entre eux, montrer que xy est d'ordre ab.
2. Soit $x, y \in G$ d'ordres respectifs a, b, montrer que xy est d'ordre $\text{ppcm}(a, b)$.
3. Montrer qu'il existe $z \in G$ tel que l'ordre de z soit le plus petit commun multiple des ordres des éléments de G.
4. En déduire que pour K un corps et G un sous-groupe fini de $K^\times$, G est cyclique.

Démonstration.

1. On a par caractère abélien $(xy)^{ab} = x^a y^b = 1$, donc

$$o(xy) \mid ab$$

De plus, pour $n \in \mathbb{N}$ tel que $(xy)^n = 1$, on a $y^{an} = (xy)^{an} = 1$ et $x^{bn} = (xy)^{bn} = 1$.
Donc $b \mid an$ et $a \mid bn$, d'où, comme a et b sont premiers entre eux, $b \mid n$ et $a \mid n$ puis $ab \mid n$.
En particulier pour $n = o(ab)$,

$$ab \mid o(xy)$$

Par conséquent $ab = o(xy)$.

2. On considère
$$k = \prod_{p\in\mathcal{P},\nu_p(a)>\nu_p(b)} p^{\nu_p(a)}, l = \prod_{p\in\mathcal{P},\nu_p(a)\leq\nu_p(b)} p^{\nu_p(b)}$$
Alors $kl = ppcm(a,b)$ et k, l sont premiers entre eux.
Donc $x' := x^{\frac{a}{k}}$ et $y' := y^{\frac{b}{l}}$ sont d'ordres respectifs k et l, d'où, d'après ce qui précède, $z := x'y'$ est d'ordre $kl = ppcm(a,b)$.

3. L'ensemble des ordres des éléments de G est fini d'après le théorème de Lagrange et non vide, donc admet un élément maximal : il existe $z \in G$ tel que
$$\forall g \in G, o(g) \leq o(z) =: a$$
Soit $x \in G$ d'ordre b.
Considérons k et l définies à la question précédente.
Alors $z^{\frac{a}{k}}$ est d'ordre k et $x^{\frac{b}{l}}$ d'ordre l.
Donc, d'après la question 1, $z^{\frac{a}{k}}x^{\frac{b}{l}}$ est d'ordre $kl = ppcm(a,b)$.
Or, d'après la condition sur a, on a $ppcm(a,b) \leq a$ ie $ppcm(a,b) = a$ puis $b \mid a$.
Par conséquent, ceci étant vrai pour tout élément $x \in G$, a est multiple commun de tous les ordres des éléments de G.
De plus a est le plus petit parmi ces éléments-ci, donc z est d'ordre a le plus petit multiple commune des ordres des éléments de G.

4. Soit K un corps et G un sous-groupe fini de $K^\times$.
On note n le cardinal de G et a son exposant.
Comme pour tout $x \in G$, $x^a = 1$, on a
$$G \subset \{x \in K, x^a - 1 = 0\}$$
Or l'ensemble des racines de $X^a - 1$ est fini et de carinal au plus a, donc $n \leq a$.
De plus, d'après la question précédente, il existe $z \in G$ d'ordre a, donc, d'après le théorème de Lagrange, $a \leq n$.
Par conséquent $a = n$ et z est un générateur de G ce qui montre que G est cyclique.

□

Exercice. On dit qu'un anneau A est principal si pour tout idéal I de A, il existe $a \in A$ tel que $I = \langle a \rangle$.
Citer deux anneaux principaux.
Montrer que l'anneau $\mathbb{Z}[X]$ n'est pas principal.
Indication : Considérer l'idéal $\langle 2, X \rangle$.

Réponse. Les anneaux $\mathbb{Z}$ et $K[X]$ sont principaux.

Démonstration. On suppose par l'absurde que $\mathbb{Z}[X]$ est principal et on considère l'idéal $I = \langle 2, X \rangle$.
Alors il existe $P \in \mathbb{Z}[X]$ tel que
$$\langle 2, X \rangle = I = \langle P \rangle$$
En particulier $2 \in I$, donc il existe $Q \in \mathbb{Z}[X]$ tels que $2 = QP$.
On en déduit que $P \in \{1, -1, 2, -2\}$.

De plus $X \in I$, donc il existe $R \in \mathbb{Z}[X]$ tel que $X = RP$.
Par conséquent en identifiant le coefficient devant le terme en X, on en déduit que P ne peut pas être égal à 2 ou -2 car R est à coefficients dans $\mathbb{Z}$.
Donc $P \in \{1, -1\}$ puis $\langle 2, X\rangle = I = \mathbb{Z}[X]$.
En particulier $1 \in \mathbb{Z}[X]$, donc il existe $U, V \in \mathbb{Z}[X]$ tels que $1 = 2U + XV$.
Par conséquent, en évaluant en 0, on obtient $1 = 2U(0)$ avec $U(0) \in \mathbb{Z}$ ce qui est absurde car 2 ne divise pas 1 dans $\mathbb{Z}$.
On en déduit donc que $\mathbb{Z}[X]$ n'est pas principal. □

Exercice. Soit $n \in \mathbb{N}^*$. Déterminer a_n le nombre de manières de recouvrir un damier de dimension $2 \times n$ avec des pièces de dimension 1×2. Indication : aboutir à une relation de récurrence.

Réponse. On a $a_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right)$.

Démonstration. Déterminons une relation de récurrence entre les a_n.

1. Pour commencer on a $a_1 = 1, a_2 = 2$ et $a_3 = 3$.
2. Puis pour calculer a_{n-1} on partitionne l'ensemble des dispositions dans un damier de taille $2 \times n + 1$ selon que la case $(1, n + 1)$ est recouverte par un domino vertical ou horizontal.
   Dans le premier cas il reste à recouvrir un damier de taille $2 \times n$ soit a_n possibilités.
   Dans le second cas il reste à recouvrir un damier de taille $2 \times n - 1$ soit a_{n-1} possibilités.
   Par conséquent on obtient la relation de récurrence

   $$a_{n+1} = a_n + a_{n-1}$$

   On réconnait la suite de Fibonnaci décalé d'un rang.
   L'équation caractéristique de la suite $(a_n)_{n\in\mathbb{N}}$ est $x^2 - x - 1 = 0$ de solutions réelles distinctes $\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$.
   Donc il existe $u, v \in \mathbb{R}$ tels que $a_n = u \left(\frac{1+\sqrt{5}}{2} \right)^n + v \left(\frac{1-\sqrt{5}}{2} \right)^n$.
   Puis avec les cas a_1 et a_2 on obtient les valeurs de u et v pour conclure que

   $$a_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right)$$

□