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 $\mathbb{Z}/n\mathbb{Z}$. $\square$

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. $\square$

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
$$a = \begin{cases} \mathrm{Ent}(x) & \text{si } x - \mathrm{Ent}(x) \leq \mathrm{Ent}(x) - x + 1 \\ \mathrm{Ent}(x) + 1 & \text{sinon} \end{cases}$$
   et
$$b = \begin{cases} \mathrm{Ent}(y) & \text{si } y - \mathrm{Ent}(y) \leq \mathrm{Ent}(y) - y + 1 \\ \mathrm{Ent}(y) + 1 & \text{sinon} \end{cases}$$
   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 $f \in C^1(\mathbb{R}_+, \mathbb{R}_+^*)$ tel qu'il existe $a \in \mathbb{R}_-^*$ tel que $\frac{f'(x)}{f(x)} \underset{x\to+\infty}{\longrightarrow} a$.
Montrer que f et f' sont intégrables sur $[0, +\infty[$.

Démonstration. Comme $a < 0$ et $\frac{f'(x)}{f(x)} \underset{x\to+\infty}{\longrightarrow} a$, il existe $A \in \mathbb{R}_+^*$ tel que
$$\forall x \geq A, \frac{f'(x)}{f(x)} \leq \frac{a}{2}$$
Puis, par intégration,
$$\forall x \geq A, \ln(f(x)) - \ln(f(A)) \leq \frac{a(x - A)}{2}$$

Or exp est croissante, donc

$$\forall x \geq A, f(x) \overset{\star}{\leq} f(A)e^{\frac{a(x-A)}{2}}$$

De plus $a < 0$ donc $x \longmapsto e^{\frac{a(x-A)}{2}}$ est intégrable, d'où, par comparaison, f est intégrable sur $[A, +\infty[$ puis sur $\mathbb{R}_+$ par continuité.
Puis $f' \leq \frac{af}{2} \leq 0$ sur $[A, +\infty[$, ainsi

$$\forall x \geq A, \int_A^x |f'(t)|dt = -\int_A^x f(t)dt = f(A) - f(x)$$

Or, d'après $\star$, $f(x) \underset{x \to +\infty}{\longrightarrow} 0$, d'où f' est absolument intégrable sur $[A, +\infty[$ puis sur $\mathbb{R}_+$ par continuité. $\square$

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 $P_2 = Q_1 P_1$ et $P_1 = Q_2 P_2$.
Ainsi $P_2 = Q_1 Q_2 P_2$, puis, par intégrité de l'anneau $K[X]$, $1 = Q_1 Q_2$.
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.

$\square$

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 $\mathbb{Q}(\sqrt{2})$.

$\square$

Exercice. Montrer qu'il existe $f : [0, +\infty[\longrightarrow \mathbb{R}_+$ continue tel que f ne tende pas vers 0 en $+\infty$ et que $\int_0^\infty f(x)dx < +\infty$.

Démonstration. On considère les suites $(a_n)_{n\in\mathbb{N}^*}$ et $(b_n)_{n\in\mathbb{N}^*}$ définies par

$$\forall n \in \mathbb{N}, a_n = n - \frac{1}{n^2}, b_n = n + \frac{1}{n^2}$$

Puis la fonction affine par morceaux et continue $f; [0, +\infty[$ définie par :

1. $f = 0$ sur $[0, +\infty[\setminus \left(\bigcup_{n=1}^{+\infty}]a_n, b_n[\right)$.
2. $f = 1$ sur $\bigcup_{n=1}^{+\infty} \{n\} = \mathbb{N}$.
3. f affine sur les $[a_n, n]$ et les $[n, b_n]$.

Ainsi

$$\int_0^\infty f(x)dx = \sum_{n=1}^{+\infty} \int_{a_n}^{b_n} f(x)dx = \sum_{n=1}^{+\infty} \frac{1}{n^2} < +\infty$$

De plus f ne tend pas vers 0 vers $+\infty$ car $f(n) = 1 \underset{n\to+\infty}{\longrightarrow} 1$. $\square$

Khôlleur : Dorian Cacitti-Holland
Elève :

Question de cours. Enoncer le théorème d'intégration des relations de comparaison sur un intervalle de la forme $[a, b[\subset \mathbb{R}$.
Démontrer les cas suivants :

1. $\int_a^b g(x)dx$ convergente et $f \overset{b}{=} o(g)$.
2. $\int_a^b g(x)dx$ divergente et $f \overset{b}{=} O(g)$.

Réponse. Soit $f, g : [a, b[\longrightarrow \mathbb{R}$ continues par morceaux avec g positive au voisinage de b. Soit $R \in \left\{ \underset{b}{=} O, \underset{b}{=} o, \underset{b}{\sim} \right\}$. On suppose $f \ R \ g$. Alors :

1. Si $\int_a^b g(x)dx$ est convergente alors $\int_x^b f(t)dt \ R \ \int_x^b g(t)dt$.
2. Si $\int_a^b g(x)dx$ est divergente alors $\int_a^x f(t)dt \ R \ \int_a^x g(t)dt$.

Démonstration. Démontrons deux des six propriétés :

1. On suppose que $\int_a^b g(x)dx$ est convergente et $f \underset{b}{=} o(g)$.
   Soit $\varepsilon \in \mathbb{R}_+^*$, alors il existe $c \in [a, b[$ tel que
   $$\forall x \in [c, b[, |f(x)| \leq \varepsilon |g(x)| = \varepsilon g(x)$$
   Soit $x \in [c, b[$, comme $\int_x^b g$ est convergente, on a $|f|$ intégrable sur $[x, b[$ et
   $$\int_x^b |f(t)|dt \leq \varepsilon \int_x^b f(t)dt$$
   ce qui montre que $\int_x^b f(t)dt \underset{x \to b}{=} o\left(\int_x^b g(t)dt\right)$.
2. On suppose que $\int_a^b g(x)dx$ est divergente et $f \underset{b}{=} O(g)$.
   Alors il existe $M \in \mathbb{R}_+^*$ et $c \in [a, b[$ tel que
   $$\forall x \in [c, b[, |f(x)| \leq M g(x)$$
   Donc
   $$\forall x \in [c, b[, \left| \int_c^x f(t)dt \right| \int_c^x |f(t)|dt \leq M \int_c^x g(t)dt$$
   Or $\int_a^b g(t)dt$ est divergente, donc il existe $d \in [c, b[$ tel que $\left| \int_a^c f(t)dt \right| \leq \int_a^d g(t)dt$.
   Ainsi, par relation de Chasles et inégalité triangulaire,
   $$\forall x \in [d, b[, \left| \int_a^x f(t)dt \right| \leq (M+1) \int_a^x g(t)dt$$
   ce qui montre que $\int_a^x f(t)dt \underset{x \to b}{=} 0\left(\int_a^x g(t)dt\right)$

$\square$

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 $f \in C(\mathbb{R}_+, \mathbb{R}_+)$ tel que $\frac{f(x+1)}{f(x)} \underset{x \to +\infty}{\longrightarrow} l \in [0, 1[$. Déterminer la nature de l'intégrale $\int_0^{+\infty} f(x)dx$.

Réponse. L'intégrale est convergente.

Démonstration. Comme $l \in]0, 1[$, il existe $q \in]l, 1[$.
De plus $\frac{f(x+1)}{f(x)} \underset{x \to +\infty}{\longrightarrow} l$, donc il existe $A \in \mathbb{R}_+^*$ tel que

$$\forall x \geq A, \frac{f(x+1)}{f(x)} \leq q$$

ie

$$\forall x \geq A, f(x+1) \leq qf(x)$$

On en déduit donc par récurrence sur $n \in \mathbb{N}$,

$$\forall x \in A, f(x+n) \leq q^n f(x)$$

Ainsi, pour tout $n \in \mathbb{N}$,

$$\int_A^{A+n} f(x)dx = \sum_{k=0}^{n-1} \int_{A+k}^{A+k+1} f(x)dx = \sum_{k=0}^{n-1} \int_A^{A+1} f(x+k)dx \leq \sum_{k=0}^{n-1} q^k \int_A^{A+1} f(x)dx$$

Or $0 < q < 1$, donc en faisnant tendre n vers $+\infty$ on obtient $\int_A^{+\infty} f(x)dx < +\infty$, puis on en déduit $\int_0^{+\infty} f(x)dx < +\infty$. $\square$