Correction du CC1 du 27 octobre
“Algèbre 1 - HAX708X”

2023

Questions isolées

a. Soit A un anneau principal. Montrer que toute suite croissante d'idéaux de A est stationnaire. *(2 points)*

Soit $(J_k)_{k\in\mathbb{N}}$ une suite croissante d'idéaux de A, i.e.

$$(\star) \qquad J_k \subset J_{k+1}, \quad \forall k \in \mathbb{N}.$$

Alors $J = \bigcup_{k\in\mathbb{N}} J_k$ est un idéal de A (l'hypothèse $(\star)$ est cruciale ici). Comme A est principal, il existe $a \in A$ tel que $J = (a)$. Comme $a \in J$, il existe $k_o \in \mathbb{N}$ tel que $a \in J_{k_o}$. Cela implique que $J = (a) \subset J_{k_o} \subset J$ et donc $(a) = J_{k_o} = J$. On a ainsi montré que $J_k = J_{k_o}$ pour tout $k \geq k_o$.

b. Soit A un anneau commutatif et M un A-module. On suppose que M n'a pas de sous A-module autre que lui-même et $\{0\}$. Montrer que M est isomorphe à A/I, où I est un idéal maximal de A. *(2 points)*

Par hypothèse, on doit avoir $Am = M$ pour tout $m \in M - \{0\}$. Fixons $m_o \in M - \{0\}$ et notons $I = \{a \in M, a \cdot m_o = 0\}$. Alors $A/I \to M, \bar{a} = a + I \mapsto a \cdot m_o$ est un isomorphisme de A-modules.

Vérifions que I est maximal : pour cela il faut vérifier que $I + (a) = A$ pour tout $a \notin I$. Pour cela considérons l'élément $m_1 = a \cdot m_o \neq 0$ associé à $a \notin I$. Alors $A/I \supset A\bar{a} \simeq Am_1 = M$ et donc $A\bar{a} = A/I$: cette dernière identité signifie exactement que $I + (a) = A$.

c. On considère l'anneau de polynômes $\mathbb{Z}/5\mathbb{Z}[X]$, ainsi que le quotient $\mathbb{K} := \mathbb{Z}/5\mathbb{Z}[X]/(X^2 + X + 1)$. Montrer que $\mathbb{K}$ est un corps. Quel est son cardinal ? *(2 points)*

Comme $\mathbb{Z}/5\mathbb{Z}$ est un corps, le quotient $\mathbb{K} := \mathbb{Z}/5\mathbb{Z}[X]/(X^2 + X + 1)$ est un corps si et seulement si le polynôme $P(X) := X^2 + X + 1$ est irréductible dans $\mathbb{Z}/5\mathbb{Z}[X]$. Comme P est de degré 2, il est irréductible si et seulement si P n'a pas de racines dans $\mathbb{Z}/5\mathbb{Z}$. On calcule :

$$P(\bar{0}) = \bar{1}, \quad P(\bar{1}) = \bar{3}, \quad P(\bar{2}) = \bar{2}, \quad P(\bar{3}) = \bar{3} \quad P(\bar{4}) = \bar{1}.$$

Conclusion : $\mathbb{K}$ est un corps et de plus $\mathbb{K}$ est un $\mathbb{Z}/5\mathbb{Z}$-espace vectoriel de dimension égale à 2. Ainsi $\mathbb{K}$ est en bijection avec $(\mathbb{Z}/5\mathbb{Z})^2$. Cela montre que Cardinal$(\mathbb{K}) = 5^2$.

d. Soient $a, b \geq 1$: on note $a \wedge b$ leur pgcd. Montrer que le groupe $\hom_{\mathbb{Z}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$ est isomorphe à $\mathbb{Z}/a \wedge b\mathbb{Z}$. *(3 points)*

Un morphisme de groupe $\varphi \in \hom_{\mathbb{Z}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$ satisfait $\varphi(Cl_a(k)) = k \cdot \varphi(Cl_a(1)), \forall k \in \mathbb{Z}$. Ainsi φ est entièrement déterminé par $\varphi(Cl_a(1))$. Cela permet de voir que l'application $\varphi \mapsto \varphi(Cl_a(1))$ réalise un isomorphisme entre le groupe $\hom_{\mathbb{Z}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$ et le sous-groupe

$$H := \left\{\varphi(Cl_a(1)), \varphi \in \hom_{\mathbb{Z}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})\right\} \subset \mathbb{Z}/b\mathbb{Z}.$$

Comme $0 = \varphi(Cl_a(a)) = a \cdot \varphi(Cl_a(1))$, on remarque que $H \subset \{m \in \mathbb{Z}/b\mathbb{Z}, a \cdot m = 0\}$. Considérons maintenant $m \in \mathbb{Z}/b\mathbb{Z}$, tel que $a \cdot m = 0$. Alors le morphisme $k \in \mathbb{Z} \mapsto k \cdot m \in \mathbb{Z}/b\mathbb{Z}$ contient $a\mathbb{Z}$ dans son noyau, et donc il se factorise en un morphisme $\varphi_m : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ tel que $\varphi_m(Cl_a(k)) = k \cdot m$.

On vient de vérifier que $H = \{m \in \mathbb{Z}/b\mathbb{Z}, a{\cdot}m = 0\}$. Un calcul classique montre que $\{m \in \mathbb{Z}/b\mathbb{Z}, a{\cdot}m = 0\}$ est le sous groupe engendré par $\frac{b}{a\wedge b}$ dans $\mathbb{Z}/b\mathbb{Z}$ et donc finalement $H = \{m \in \mathbb{Z}/b\mathbb{Z}, a{\cdot}m = 0\} \simeq \mathbb{Z}/a\wedge b\mathbb{Z}$.

e. Déterminer une base du $\mathbb{Z}$-module

$$M := \{(x, y, z) \in \mathbb{Z}^3,\ 6x + 15y - 10z \in 8\mathbb{Z}\}.$$

(3 points)

Notons $f : \mathbb{Z}^3 \to \mathbb{Z}$, le morphisme défini par $f(x, y, z) = 6x + 15y - 10z$. On voit que l'image de f est égale à $(6) + (15) + (10) = \mathbb{Z}$: un petit calcul permet de voir que $f(-14, 1, -7) = 1$. Alors

$$\mathbb{Z}^3 = \ker(f) \oplus \mathbb{Z}v_1$$

avec $v_1 = (-14, 1, -7)$. On obtient aussi que

$$M = \ker(f) \oplus \mathbb{Z}8v_1$$

La relation $6x + 15y - 10z = 0$ implique que $5\backslash x$, $2\backslash y$ et $3\backslash z$. En posant $x = 5x'$, $y = 2y'$ et $z = 3z'$, la relation $6x + 15y - 10z = 0$ devient $x' + y' = z'$. Ainsi $(x, y, z) \in \ker(f)$ si et seulement si il existe x', y' tels que

$$(x, y, z) = (5x', 2y', 3(x' + y')) = x' \underbrace{(5, 0, 3)}_{v_2} + y' \underbrace{(0, 2, 3)}_{v_3}$$

On vient de montrer que $\ker(f) = \mathbb{Z}v_2 \oplus \mathbb{Z}v_3$.

Conclusion : $\{8v_1, v_2, v_3\}$ est une base de M.

f. Calculer les facteurs invariants du groupe

$$G = \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/432\mathbb{Z} \times \mathbb{Z}/1000\mathbb{Z}.$$

(3 points)

On utilise les décompositions en facteurs premiers suivantes :

$$90 = 2 \cdot 3^2 \cdot 5, \quad 100 = 2^2 \cdot 5^2, \quad 432 = 2^4 \cdot 3^3, \quad 1000 = 2^3 \cdot 5^3.$$

On voit alors que

$$\begin{aligned} d_4 &= 2^4 \cdot 3^3 \cdot 5^3 \\ d_3 &= 2^3 \cdot 3^2 \cdot 5^2 \\ d_2 &= 2^2 \cdot 5 \\ d_1 &= 2 \end{aligned}$$

sont les facteurs invariants du groupe G, car d'une part $d_1\backslash d_2\backslash d_3\backslash d_4$, et d'autre part le lemme chinois nous permet de voir que G est isomorphe au groupe

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \mathbb{Z}/d_3\mathbb{Z} \times \mathbb{Z}/d_4\mathbb{Z}.$$

Exercice *(5 points)*

Soit A l'ensemble des nombres rationnels qui s'écrivent comme une fraction $\frac{a}{b}$ avec b premier avec 3.

(1) Montrer que A est un sous-anneau de $\mathbb{Q}$.

(2) Déterminer les éléments inversibles ainsi que les éléments irréductibles de A.

(3) Montrer que A est un anneau principal.

Pour le point (1), on vérifie que $1 \in A$ est que si $x, y \in A$ alors $x - y$ et xy appartiennent à A.

Une fraction non-nulle $\frac{a}{b}$ appartient à A ssi b premier avec 3. De plus elle est inversible dans A, ssi a est premier avec 3. Conclusion : les éléments inversibles de A sont les fractions $\frac{a}{b}$ avec a et b premiers avec 3.

D'après le calcul précédent on remarque que tout élément $x \in A - \{0\}$ se met sous la forme

$$x = 3^k u$$

avec $k \in \mathbb{N}$ et $u \in A^\times$. L'entier k est unique, on le note $k := \mathrm{val}_3(x)$.

On voit alors que $x \in A - \{0\}$ est irréductible si et seulement si $\mathrm{val}_3(x) = 1$.

Si $I \subset A$ est un idéal non nul, on pose

$$k(I) = \inf \left\{ \mathrm{val}_3(x), x \in I - \{0\} \right\}.$$

On montre alors assez facilement que I est l'idéal engendré par $3^{k(I)}$.

Conclusion : les idéaux de A sont de la forme A, $\{0\}$ ou (3^k), pour $k \geq 1$.