Correction du CC du 23 octobre 2024
"Algèbre 1 - HAX708X"

Questions isolées

a. Soit $j = e^{\frac{2i\pi}{3}}$. Déterminez les éléments inversibles de l'anneau $\mathbb{Z}[j]$.

$\mathbb{Z}[j]$ est l'image du morphisme $\phi : P \in \mathbb{Z}[X] \mapsto P(j)$. Comme $\ker(\phi)$ est engendré par $X^2 + X + 1$, les éléments de $\mathbb{Z}[j]$ sont de la forme $z = a + bj$ avec $a, b \in \mathbb{Z}$. Un élément $z \in \mathbb{Z}[j]$ est inversible si et seulement si $N(z) = z\bar{z} = 1$. On a $N(a + bj) = a^2 + b^2 - ab$. Comme $|ab| \leq \max\{a^2, b^2\}$, la relation $a^2 + b^2 = ab + 1$ implique que $\inf\{a^2, b^2\} = 0$ ou 1. Finalement, on voit que les éléments inversibles de l'anneau $\mathbb{Z}[j]$ sont ± 1, $\pm j$, $\pm(1 + j)$.

b. Soit I le noyau de l'homomorphisme d'anneaux de $\mathbb{C}[X, Y]$ dans $\mathbb{C}$ donné par $P(X, Y) \mapsto P(1, 2)$. Montrer que I n'est pas un idéal principal.

Tout polynôme $P \in \mathbb{C}[X, Y]$ s'exprime de manière unique sous la forme

$$P = \sum_{k,l \in \mathbb{N}} a_{k,\ell}(X - 1)^k (Y - 2)^\ell.$$

Comme $a_{0,0} = P(1, 2)$, on voit que l'idéal I est engendré par $\{X - 1, Y - 2\}$. L'idéal I n'est pas principal car les polynômes $X - 1$ et $Y - 2$ sont irréductibles : il n'existe pas de polynôme non-constant qui divise à la fois $X - 1$ et $Y - 2$.

c. À isomorphisme près, combien y a-t-il de groupes abéliens de cardinal 600 ? En donner la liste.

On a $600 = 3 \cdot 5^2 \cdot 2^3$. On cherche les groupes $G = \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_q\mathbb{Z}$ associés à une suite d'entiers $a_1 \geq 2, \ldots a_q \geq 2$ tels que

$$a_1 \backslash a_2 \backslash \cdots \backslash a_q \qquad \text{et} \qquad a_1 a_2 \cdots a_q = 600.$$

Voici les 6 possibilités :

(1) $q = 1$: Alors $a_1 = 600$.
(2) $q = 2$: Alors $(a_1, a_2) \in \{(10, 60), (5, 120), (2, 300)\}$
(3) $q = 3$: Alors $(a_1, a_2, a_3) \in \{(2, 10, 30), (2, 2, 150)\}$.

d. Déterminer une base du $\mathbb{Z}$-module $M := \{(x, y, z) \in \mathbb{Z}^3,\ 10x + 15y - 8z \in 4\mathbb{Z}\}$.

On pose $\varphi(x, y, z) = 10x + 15y - 8z$. On voit que l'image de φ est égal à $10\mathbb{Z} + 15\mathbb{Z} + 8\mathbb{Z} = \mathbb{Z}$ car $pgcd(10, 15, 8) = 1$. Posons $u = (0, -1, -2)$. Comme $\varphi(u) = 1$, on a

$$\mathbb{Z}^3 = \ker(\varphi) \oplus \mathbb{Z}u \qquad \text{et} \qquad M = \ker(\varphi) \oplus \mathbb{Z}4u.$$

Soit $(x, y, z) \in \ker(\varphi)$. La relation $(\star)$ $10x + 15y - 8z = 0$ impose que $2 \backslash 15y$ et donc $y = 2y'$ avec $y' \in \mathbb{Z}$. La relation $(\star)$ devient $10x + 30y' - 8z = 0$ soit $5x + 15y' - 4z = 0$. Cette relation implique de la même façon que $5 \backslash 4z$ et donc $z = 5z'$ avec $z' \in \mathbb{Z}$. Finalement on obtient $x + 3y' - 4z' = 0$. On a montré que

$$\ker(\varphi) = \{(-3y' + 4z', 2y', 5z');\ y', z' \in \mathbb{Z}\}.$$

Conclusion : $\{(-3, 2, 0), (4, 0, 5)\}$ est une base de $\ker(\varphi)$, et $\{(-3, 2, 0), (4, 0, 5), 4u\}$ est une base de M.

Exercice 1

Soit A un anneau commutatif intègre et soit M un A-module. Soit M_{tor} l'ensemble des éléments de torsion de M, c'est-à-dire l'ensemble des $m \in M$ tels qu'il existe $a \in A - \{0\}$ tel que $am = 0$.

(1) Montrer que M_{tor} est un sous-module de M.
(2) Montrer que le module quotient M/M_{tor} est sans torsion *(i.e. 0 est le seul élément de torsion).*

Cet exercice a été traité en cours.

Exercice 2

Soit $p \geq 2$ un nombre premier. On note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ le corps à p élément et $\pi_p : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme associé à la projection canonique $\mathbb{Z} \to \mathbb{F}_p$. Soit $\Phi_p := \sum_{k=0}^{p-1} X^k \in \mathbb{Z}[X]$.

(1) Montrer que pour tout $1 < k < p$, le coefficient binomial C_k^p est divisible par p.
On a $p! = C_k^p\,(p-1)!\,k!$, donc p divise le produit $C_k^p\,(p-1)!\,k!$. Si $1 < k < p$, p ne divise pas $(p-1)!\,k!$, et donc $p \backslash C_k^p$.

(2) Montrer que pour tout $P, Q \in \mathbb{F}_p[X]$, on a $(P-Q)^p = P^p - Q^p$.
La formule du binôme donne

$$(P-Q)^p = \sum_{k=0}^{p} C_k^p (-1)^k P^{p-k} Q^k = P^p + (-1)^p Q^p$$

car $C_k^p = 0$ dans $\mathbb{F}_p$, pour $k \neq 0, p$. Maintenant on voit que $(-1)^p = -1$ dans $\mathbb{F}_p$ pour tout nombre premier $p \geq 2$.

(3) Montrer que $\pi_p(\Phi_p) = (X-1)^{p-1}$. *On calculera* $(X-1)\Phi_p$.
Comme $(X-1)\Phi_p = X^p - 1$, on a $\pi_p\Big((X-1)\Phi_p\Big) = X^p - 1 = (X-1)^p$ dans $\mathbb{F}_p[X]$ d'après la question précédente. La relation $(X-1)\pi_p(\Phi_p) = (X-1)^p$ permet de conclure que $\pi_p(\Phi_p) = (X-1)^{p-1}$.

(4) Montrer que Φ_p est irréductible dans $\mathbb{Z}[X]$.
Supposons que Φ_p n'est pas irréductible dans $\mathbb{Z}[X]$. Comme Φ_p est primitif et unitaire, il existe deux polynômes unitaires $A, B \in \mathbb{Z}[X]$ de degré ≥ 1 tels que $\Phi_p = AB$. Les images $\mathbf{A} := \Phi_p(A)$ et $\mathbf{B} := \Phi_p(B)$ sont des polynômes unitaires de $\mathbb{F}_p[X]$ qui satisfont la relation $\mathbf{AB} = (X-1)^{p-1}$. Comme $X-1$ est irréductible dans $\mathbb{F}_p[X]$, il existe $\alpha, \beta \geq 1$ tels que $\alpha + \beta = p-1$ et

$$\mathbf{A} = (X-1)^\alpha \quad \text{et} \quad \mathbf{B} = (X-1)^\beta.$$

Relevons ces identités dans $\mathbb{Z}[X]$: il existe $P, Q \in \mathbb{Z}[X]$ tels que

$$A(X) = (X-1)^\alpha + pP(X) \quad \text{et} \quad B(X) = (X-1)^\beta + pQ(X).$$

Finalement,

$$\Phi_p(X) = A(X)B(X) = \Big((X-1)^\alpha + pP(X)\Big)\Big((X-1)^\beta + pQ(X)\Big)$$

En évaluant la relation précédente en $X = 1$, on obtient

$$p = \Phi_p(1) = A(1)B(1) = p^2 P(1)Q(1).$$

Sachant que $P(1)Q(1) \in \mathbb{Z}$, on constate que la relation précédente est fausse. On a ainsi montré que Φ_p est irréductible dans $\mathbb{Z}[X]$.