Deuxième composition de mathématiques
École Nationale de la Météorologie - MP

NOTATIONS ET RAPPELS.
Pour (a,b) dans $\mathbf{Z}^* \times \mathbf{Z}^*$, on note $a \wedge b$ le pgcd de a et b et $a \vee b$ leur ppcm.
Soit n dans $\mathbf{N}^*$ et (a,b) dans $\mathbf{Z}^2$, on dit que a est congru à b modulo n, et on note $a \equiv b \pmod{n}$ si et seulement si n divise $b-a$. On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble quotient de $\mathbf{Z}$ par la relation $\equiv \pmod{n}$. $\mathbf{Z}/n\mathbf{Z}$ est un ensemble fini, à n éléments : $\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$.
On définit les deux lois de composition internes usuelles dans $\mathbf{Z}/n\mathbf{Z}$, notées $+$ et $\cdot$ par :

$$\forall (x,y) \in \mathbf{Z}^2\ ,\ \overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x} \cdot \overline{y} = \overline{xy}\ .$$

Il est facile de montrer (non demandé) que $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$ est un anneau commutatif.

- PREMIÈRE PARTIE -

.1) Lister les éléments inversibles (en précisant leur inverse) de $\mathbf{Z}/6\mathbf{Z}$ et ceux de $\mathbf{Z}/13\mathbf{Z}$.

.2) Montrer que le polynôme $X^2 - \overline{5}$ est irréductible sur $\mathbf{Z}/13\mathbf{Z}[X]$.

- DEUXIÈME PARTIE -

On note $\mathbf{K}_{169}$ l'ensemble $\mathbf{Z}/13\mathbf{Z} \times \mathbf{Z}/13\mathbf{Z}$ et on le munit des lois de composition suivantes :
$(x,y) \oplus (x',y') = (x+x', y+y')$
$(x,y) \bullet (x',y') = \big(x \cdot x' + \overline{5} \cdot y \cdot y', x \cdot y' + x' \cdot y\big)$
Pour α dans $\mathbf{K}_{169}$, on note $\alpha^2 = \alpha \bullet \alpha$.

.1) Montrer que $(\mathbf{K}_{169}, \oplus, \bullet)$ est un corps commutatif à 169 éléments.

.2) Soit $\mathbf{H}_{13}$ le sous-ensemble de $\mathbf{K}_{169}$ donné par $\mathbf{H}_{13} = \big\{\big(x, \overline{0}\big) \mid x \in \mathbf{Z}/13\mathbf{Z}\big\}$.
Montrer que $(H_{13}, \oplus, \bullet)$ est un sous-corps isomorphe à $(\mathbf{Z}/13\mathbf{Z}, +, \cdot)$.

.3) Désormais on identifie $\mathbf{H}_{13}$ et $\mathbf{Z}/13\mathbf{Z}$ en identifiant x et $\big(x, \overline{0}\big)$. Trouver les éléments α de $\mathbf{K}_{169}$ tels que $\alpha^2 = \overline{5}$ et factoriser $X^2 - \overline{5}$ dans $\mathbf{K}_{169}[X]$.

- TROISIÈME PARTIE -

Soit $(G, \cdot)$ un groupe commutatif fini et x dans G, on note $\mathrm{ord}_G(x)$ l'ordre de l'élément x de G.

.1) Soit a et b deux éléments de G d'ordres m et n respectivement. Montrer que si $m \wedge n = 1$, alors $\mathrm{ord}_G(a.b) = mn$.

.2) Montrer que, même si m et n ne sont pas premiers entre eux, il existe c dans G tel que $\mathrm{ord}_G(c) = m \vee n$.
On pourra remarquer que ce ppcm s'écrit $m'.n'$, avec m' divisant m, n' divisant n, et m' et n' premiers entre eux.

.3) Considérons le ppcm r des ordres des éléments de G ; c'est le plus petit des entiers n dans $\mathbf{N}^*$ tel que $\forall x \in G,\ x^n = 1$. Montrer qu'il existe c dans G, tel que $\mathrm{ord}_G(c) = r$.

.4) Soit $(F, +, \cdot)$ un corps commutatif et $(G, \cdot)$ un sous-groupe fini de $(F^*, \cdot)$. Montrer que G est cyclique.

.5) On note $\mathbf{K}_{169}^* = \mathbf{K}_{169} \setminus \{\big(\overline{0}, \overline{0}\big)\}$. Déterminer les 48 générateurs du groupe $(\mathbf{K}_{169}^*, \bullet)$.

Deuxième composition – Ecole Nationale de la Météorologie 1989

- PREMIÈRE PARTIE -

.1) Les éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$ sont les classes correpondant à des entiers premiers à n.

Les éléments inversibles de $\mathbf{Z}/6\mathbf{Z}$ sont donc $\overline{1}$ et $-\overline{1}$ et ils sont leurs propres inverses.

Tous les éléments non nuls de $\mathbf{Z}/13\mathbf{Z}$ sont inversibles.

Les éléments $\overline{1}$ et $-\overline{1}$ sont leurs propres inverses. Voici les autres éléments non nuls, regroupés par paires d'éléments inverses les uns des autres :

$$(\overline{2},-\overline{6}) \quad (\overline{3},-\overline{4}) \quad (\overline{4},-\overline{3}) \quad (\overline{5},-\overline{5}) \quad (\overline{6},-\overline{2})\ .$$

.2) Un polynôme de degré deux est irréductible si et seulement s'il n'a pas de racine. Or les carrés dans $\mathbf{Z}/13\mathbf{Z}$ sont obtenus en élevant $\overline{0}$, $\pm\overline{1}$, …, $\pm\overline{6}$ au carré, i.e. ce sont $\overline{0}$, $\overline{1}$, $\overline{4}$, $\overline{9}$, $\overline{3}$, $-\overline{1}$ et $-\overline{3}$ et donc $\overline{5}$ n'est pas un carré dans $\mathbf{Z}/13\mathbf{Z}$. Il en résulte que $X^2-\overline{5}$ est irréductible dans $\mathbf{Z}/13\mathbf{Z}[X]$.

- DEUXIÈME PARTIE -

.1) Soit A le sous-espace vectoriel du $\mathbf{Z}/13\mathbf{Z}$-espace vectoriel $\mathscr{M}_2(\mathbf{Z}/13\mathbf{Z})$ engendré par l'identité et par la matrice M définie par $M=\begin{pmatrix}\overline{0} & \overline{5}\\ \overline{1} & \overline{0}\end{pmatrix}$. Puisque $M^2=\overline{5}I_2$, A est en fait un sous-anneau de $\mathscr{M}_2(\mathbf{Z}/13\mathbf{Z})$.

De plus, si x et y sont dans $\mathbf{Z}/13\mathbf{Z}$, on a $(xI_2+yM)(xI_2-yM)=(x^2-\overline{5}y^2)I_2$. Si y est nul, alors $x^2-\overline{5}y^2$ n'est nul que si x l'est. Si y est non nul, on a $x^2-\overline{5}y^2=y^2((xy^{-1})^2-\overline{5})$ et cette quantité n'est pas nulle d'après I.2. Par conséquent, si (x,y) n'est pas $(\overline{0},\overline{0})$, $x^2-\overline{5}y^2$ est inversible dans $\mathbf{Z}/13\mathbf{Z}$. On note a son inverse et alors axI_2-ayM est l'inverse de xI_2+yM dans $\mathscr{M}_2(\mathbf{Z}/13\mathbf{Z})$, et est dans A. Il en résulte que A est un corps.

Soit maintenant f l'application de A dans $\mathbf{K}_{169}$ définie par $\begin{pmatrix}x & \overline{5}y\\ y & x\end{pmatrix}\mapsto(x,y)$. Par définition des lois $\oplus$ et $\bullet$, cette application est additive et multiplicative. Par transport de structure $(\mathbf{K}_{169},\oplus,\bullet)$ est un corps commutatif d'éléments neutres $f(0)$ et $f(I_2)$, i.e. $(\overline{0},\overline{0})$ et $(\overline{1},\overline{0})$.

Enfin le cardinal d'un produit cartésien étant le produit des cardinaux, $\mathbf{K}_{169}$ est de cardinal 13×13, i.e. 169 : $(\mathbf{K}_{169},\oplus,\bullet)$ est un corps commutatif à 169 éléments.

.2) On reprend l'application f précédente, de sorte que $\mathbf{H}_{13}$ est l'image des matrices scalaires par f. Comme f est un morphisme d'anneaux, on a $\mathbf{Z}/13\mathbf{Z}\cong\mathbf{Z}/13\mathbf{Z}I_2\cong\mathbf{H}_{13}$, où les isomorphismes sont des isomorphismes d'anneaux.

Comme $\mathbf{Z}/13\mathbf{Z}$ est un corps, ce sont en fait des isomorphismes de corps et donc

$(H_{13},\oplus,\bullet)$ est un sous-corps isomorphe à $(\mathbf{Z}/13\mathbf{Z},+,\cdot)$.

.3) Soit α dans $\mathbf{K}_{169}$. Posons $\alpha=(x,y)$, avec x et y dans $\mathbf{Z}/13\mathbf{Z}$. Il vient $\alpha^2=(x^2+\overline{5}y^2,2xy)$ et donc $\alpha^2=\overline{5}$ si et seulement si $xy=\overline{0}$ et $x^2+\overline{5}y^2=\overline{5}$. Par intégrité de $\mathbf{Z}/13\mathbf{Z}$, ce système est équivalent à : soit $x=\overline{0}$ et $y^2=\overline{1}$, soit $y=\overline{0}$ et $x^2=\overline{5}$. Ce dernier cas est impossible et donc

les éléments α de $\mathbf{K}_{169}$ tels que $\alpha^2=\overline{5}$ sont $(\overline{0},\overline{1})$ et $(\overline{0},-\overline{1})$.

Il en résulte, dans $\mathbf{K}_{169}[X]$,

$$(X-(\overline{0},\overline{1}))(X+(\overline{0},\overline{1}))=X^2-(\overline{0},\overline{1})^2=X^2-\overline{5}$$

et donc la factorisation de $X^2-\overline{5}$ dans $\mathbf{K}_{169}[X]$ est $(X-(\overline{0},\overline{1}))(X+(\overline{0},\overline{1}))$.

- TROISIÈME PARTIE -

.1) Puisque G est commutatif, on a $(ab)^{mn} = a^{mn}b^{mn}$ et comme $\mathrm{ord}_G(a) \mid mn$ et $\mathrm{ord}_G(b) \mid mn$, il vient $(ab)^{mn} = 1_G 1_G = 1_G$, i.e. $\mathrm{ord}_G(ab) \mid mn$.

Soit $d = mn/\mathrm{ord}_G(ab)$ et p un diviseur premier de d. Alors p divise mn et donc, d'après le lemme de Gauss, il divise m ou n. Soit $k = \mathrm{ord}_G(ab) \times (d/p)$, c'est un entier et un multiple de $\mathrm{ord}_G(ab)$, donc $1_G = (ab)^k = a^k b^k$. Mais on a $k = (mn)/p$. Supposons alors $p \mid n$, il vient $m \mid k = m(n/p)$ de sorte qu'on a $a^k = 1_G$ et donc $b^k = 1_G$, d'où $n \mid k$. Comme $m \wedge n = 1$, il en résulte $n \mid (n/p)$ et ceci est une contradiction. Mutatis mutandis $p \mid m$ conduit à une même contradiction, et donc d ne peut avoir de diviseur premier, i.e. $d = 1$ et donc $\boxed{\text{si } m \wedge n = 1, \text{ alors } \mathrm{ord}_G(a.b) = mn.}$

.2) Soit d donné par $d = m \wedge n$ de sorte qu'on a, pour p premier $v_p(d) = \min(v_p(m), v_p(n))$ où v_p désigne la valuation p-adique. On pose

$$d_1 = \prod_{v_p(d)=v_p(m)} p^{v_p(d)}$$

où le produit s'étend aux nombres premiers p tels que $v_p(d) = v_p(m)$, i.e. tels que $v_p(m) \leq v_p(n)$. On pose

$$d_2 = \prod_{v_p(m)>v_p(n)} p^{v_p(d)}$$

où le produit s'étend aux nombres premiers p tels que $v_p(m) > v_p(n)$. On a donc $d = d_1 d_2$ puisque les ensembles d'indices précédents forment une partition de l'ensemble des nombres premiers et qu'on a $d = \prod_p p^{v_p(d)}$. De plus, toujours puisqu'on a affaire à une partition, $d_1 \wedge d_2 = 1$.

Par ailleurs posons $m' = m/d_1$ et $n' = n/d_2$. On a donc $m'n' = mn/(m \wedge n)$, soit $m'n' = m \vee n$.

Soit maintenant p un nombre premier. Si $p \mid m'$, alors $v_p(m) > v_p(d_1)$. Si on avait $v_p(m) \leq v_p(n)$, alors par définition de d_1, on aurait $v_p(d_1) = v_p(m)$. Il en résulte $v_p(d_1) = 0$ et donc $v_p(d) = v_p(d_2) = v_p(n)$, de sorte que p ne divise par n'. Par conséquent $m' \wedge n' = 1$.

Soit enfin a^{d_1} et b^{d_2} : ce sont des éléments d'ordres respectifs m/d_1 et n/d_2 et comme ces deux nombres sont premiers entre eux, la question précédente montre que c donné par $c = a^{d_1} b^{d_2}$ est d'ordre $m'n'$, i.e. $\boxed{c \text{ est d'ordre } m \vee n.}$

.3) Soit n le maximum des ordres des éléments de G et a un élément d'ordre n. Soit maintenant b un autre élément de G, d'après la question précédent il existe un élément c de G d'ordre $n \vee \mathrm{ord}_G(b)$. Par maximalité de n, on a $n \geq n \vee \mathrm{ord}_G(b)$ et donc $\mathrm{ord}_G(b) \mid n$. Il en résulte que n est un multiple de tous les ordres d'éléments de G et est lui-même l'ordre d'un élément de G, donc n est le ppcm des ordres des éléments de G, i.e. $n = r$. Comme a est d'ordre n, on a montré $\boxed{\text{qu'il existe } c \text{ dans } G \text{ tel que } \mathrm{ord}_G(c) = r.}$

.4) Soit n le cardinal de G et r son exposant. Puisque $X^r - 1$ admet au plus r racines dans F^* et qu'on a $G \subset F^*$, on a $n \leq r$. De plus si c est un élément d'ordre r dans G, $\langle c \rangle \cong \mathbf{Z}/r\mathbf{Z}$ et donc $\langle c \rangle$ est de cardinal r. Comme c'est un sous-groupe de G, il en résulte $r \leq n$. On en conclut $n = r$, $G = \langle c \rangle$ et donc $\boxed{G \text{ est cyclique.}}$

.5) Déterminer un élément d'ordre 168 revient à trouver des éléments d'ordres 8, 3 et 7 et à prendre leur produit.

Comme $(\mathbf{Z}/13\mathbf{Z})^\times$ est cyclique d'ordre 12, on va trouver un élément d'ordre 3 et un autre d'ordre 4 dans $\mathbf{H}_{13}$. On vérifie directement que $\overline{2}$ est d'ordre 12 puisque ses puissances successives sont :

$$\overline{1}\,,\ \overline{2}\,,\ \overline{4}\,,\ -\overline{5}\,,\ \overline{3}\,,\ \overline{6}\,,\ -\overline{1}$$

et les suivantes s'obtiennent pas changement de signe. Par conséquent $\overline{2}^4$ est d'ordre 3 et $\overline{2}^3$ ou encore $\overline{2}^9$ sont d'ordre 4.

Puisque $\overline{2}^4 = \overline{3}$, on a $\langle\overline{3}\rangle \cong \mathbf{Z}/3\mathbf{Z}$ et les racines de $X^3 - \overline{1}$ dans le corps $\mathbf{K}_{169}$ sont donc les éléments de ce sous-groupe. Et les seuls qui sont d'ordre exactement 3 sont donc $\overline{3}$ et $\overline{3}^2$, i.e. $-\overline{4}$.

Puisque $\overline{2}^9 = \overline{5}$, $\overline{5}$ est d'ordre 4 et donc une racine carrée de $\overline{5}$ est d'ordre 8. Soit $\alpha = (\overline{0}, \overline{1})$, on a donc $\langle\alpha\rangle \cong \mathbf{Z}/8\mathbf{Z}$ et les racines de $X^8 - 1$ sont donc les éléments de ce sous-groupe. Les éléments qui sont exactement d'ordre 8 sont les α^k avec k premier à 8, i.e. k impair : α, α^3, α^5 et α^7. Comme $\alpha^2 = \overline{5}$, ces nombres sont α, $\overline{5}\alpha$, $-\alpha$ et $-\overline{5}\alpha$, i.e. $(\overline{0}, y)$ pour y dans $\{\pm\overline{1}, \pm\overline{5}\}$.

Enfin pour trouver un élément d'ordre 7, il faut chercher à la main. On pose $\beta = (\overline{4}, \overline{4})$ et on calcule les puissances successives de β :

$$1\,,\ \beta\,,\ (\overline{5},\overline{6})\,,\ (-\overline{3},\overline{5})\,,\ (-\overline{3},-\overline{5})\,,\ (\overline{5},-\overline{6})\,,\ (\overline{4},-\overline{4})\,,\ 1$$

et donc β est d'ordre 7, et les éléments d'ordre 7 sont exactement les éléments de la forme β^k avec $1 \leq k \leq 6$.

On en déduit que les 48 générateurs du groupe $(\mathbf{K}_{169}^*, \bullet)$ sont les éléments $u\alpha\beta^k$ avec u parmi $\pm\overline{2}$, $\pm\overline{3}$, $\pm\overline{4}$, $\pm\overline{6}$ et k entier entre 1 et 6.

Remarque : d'après la question précédente, $\mathbf{K}_{169}^*$ est cyclique d'ordre 168 et on a, d'après le théorème des restes chinois

$$(\mathbf{Z}/168\mathbf{Z})^\times \cong (\mathbf{Z}/8\mathbf{Z})^\times \times (\mathbf{Z}/3\mathbf{Z})^\times \times (\mathbf{Z}/7\mathbf{Z})^\times$$

i.e.

$$(\mathbf{Z}/168\mathbf{Z})^\times \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$$

et donc $\mathbf{Z}/168\mathbf{Z}$ admet effectivement 48 générateurs.