Mathématiques spéciales

Feuille d'exercices n°6 (bis) - Révisions d'algèbre de Sup' : congruences, groupes, anneaux

1. Exercices basiques

a. Congruences

Exercice 1.

1. Déterminer, suivant les puissances de $n \in \mathbb{N}$, le reste de la division euclidienne de 2^n par 5.
2. Quel est le reste de la division par 5 de 1357^{2013} ?

Exercice 2.

Démontrer que la somme de trois cubes consécutifs est toujours divisible par 9.

Exercice 3.

1. Déterminer les entiers naturels n tels que $5^n \equiv -1$ [13].
2. Déterminer les entiers naturels n tels que 13 divise $5^{2n} + 5^n$.

Exercice 4.

Démontrer que 13 divise $3^{126} + 5^{126}$.

Exercice 5.

Démontrer que, pour tout entier naturel n, $3^{2n+1} + 2^{4n+2}$ est divisible par 7.

Exercice 6.

On considère la suite (u_n) d'entiers naturels définie par $u_0 = 14$ et $u_{n+1} = 5u_n - 6$.

1. Quelle conjecture peut-on émettre sur les deux derniers chiffres de (u_n) ?
2. Montrer que pour tout entier naturel n, $u_{n+2} \equiv u_n$ [4]. En déduire que pour tout entier naturel k, on a $u_{2k} \equiv 2$ [4] et $u_{2k+1} \equiv 0$ [4].
3. (a) Montrer que pour tout entier naturel n, on a $2u_n = 5^{n+2} + 3$.
   (b) En déduire que pour tout entier naturel n, on a $2u_n \equiv 28$ [100].
4. Valider la conjecture émise à la première question.

Exercice 7.

Soit a et b deux entiers tels que $a^2 + b^2$ soit divisible par 7. Démontrer que a et b sont divisibles par 7.

b. Groupes

Exercice 8.

Dans les questions suivantes, déterminer si la partie H est un sous-groupe du groupe G.

1. $G = (\mathbb{Z}, +)$; $H = \{\text{nombres pairs}\}$.
2. $G = (\mathbb{Z}, +)$; $H = \{\text{nombres impairs}\}$.
3. $G = (\mathbb{R}, +)$; $H = [-1, +\infty[$.
4. $G = (\mathbb{R}^*, \times)$; $H = \mathbb{Q}^*$.
5. $G = (\mathbb{R}^*, \times)$; $H = \{a + b\sqrt{2};\ a, b \in \mathbb{Q},\ (a, b) \neq (0, 0)\}$.
6. $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$; $H = \{f \in G;\ f(x) = x\}$ où E est un ensemble et $x \in E$.
7. $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$; $H = \{f \in G;\ f(x) = y\}$ où E est un ensemble et $x, y \in E$ avec $x \neq y$.

Exercice 9.

Dire si les parties suivantes de $GL_n(\mathbb{R})$ sont des sous-groupes de $GL_n(\mathbb{R})$.

1. $H_1 = \{A \in GL_n(\mathbb{R});\ A \text{ diagonale avec tous ses coefficients diagonaux non-nuls}\}$.
2. $H_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix};\ a > 0,\ b \in \mathbb{R} \right\}$ (ici, $n = 2$).
3. $H_3 = \left\{ \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix};\ a > 0,\ b \in \mathbb{R} \right\}$ (ici, $n = 2$).

Exercice 10.

Les applications $\phi : G \to H$ définies ci-dessous sont-elles des morphismes de groupes ?

1. $G = (GL_n(\mathbb{R}), \times)$, $H = (\mathbb{R}, +)$, $\phi(A) = \mathrm{tr}(A)$.
2. $G = (M_n(\mathbb{R}), +)$, $H = (\mathbb{R}, +)$, $\phi(A) = \mathrm{tr}(A)$.
3. $G = (\mathbb{R}^*, \times)$, $H = (\mathbb{R}^*, \times)$, $\phi(x) = |x|$.
4. $G = (\mathbb{R}^*, \times)$, $H = (\mathbb{R}^*, \times)$, $\phi(x) = 2x$.
5. $G = (\mathbb{R}, +)$, $H = (GL_2(\mathbb{R}), \times)$, $\phi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

Exercice 11.

Justifier que exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \cdot)$. Quel est son image ? Son noyau ?

Exercice 12.

Déterminer tous les morphismes de groupes que $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Exercice 13.

Les ensembles suivants munis des lois considérées sont-ils des groupes ?

1. G est l'ensemble des fonctions de $\mathbb{R} \to \mathbb{R}$ définies par $x \mapsto ax + b$, avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, muni de la composition ;
2. G est l'ensemble des fonctions croissantes de $\mathbb{R}$ dans $\mathbb{R}$, muni de l'addition ;
3. $G = \{f_1, f_2, f_3, f_4\}$, où

$$f_1(x) = x,\ f_2(x) = -x,\ f_3(x) = \frac{1}{x},\ f_4(x) = -\frac{1}{x},$$

   muni de la composition.

Exercice 14.

Montrer que $H = \{x + y\sqrt{3};\ x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$ est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Exercice 15.

Traduire en termes de morphismes de groupes les propriétés bien connues suivantes (dont le domaine de validité a volontairement été omis) :

1. $\ln(xy) = \ln(x) + \ln(y)$;
2. $|zz'| = |z||z'|$;
3. $\sqrt{xy} = \sqrt{x}\sqrt{y}$;
4. $e^{x+y} = e^x e^y$;
5. $\det(MM') = \det(M)\det(M')$.

Exercice 16.

Montrer que les lois suivantes munissent l'ensemble G indiqué d'une structure de groupe, et préciser s'il est abélien :

1. $x \star y = \frac{x+y}{1+xy}$ sur $G =]-1, 1[$;
2. $(x, y) \star (x', y') = (x + x', ye^{x'} + y'e^{-x})$ sur $G = \mathbb{R}^2$;

Exercice 17.

Soit $(G, \cdot)$ un groupe. Démontrer que les parties suivantes sont des sous-groupes de G :

1. $C(G) = \{x \in G;\ \forall y \in G, xy = yx\}$ ($C(G)$ s'appelle le centre de G) ;
2. $aHa^{-1} = \{aha^{-1};\ h \in H\}$ où $a \in G$ et H est un sous-groupe de G.

3. On suppose de plus que G est abélien. On dit que x est un élément de torsion de G s'il existe $n \in \mathbb{N}$ tel que $x^n = e$. Démontrer que l'ensemble des éléments de torsion de G est un sous-groupe de G.

Exercice 18.

Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

Exercice 19.

Soit G un groupe et H, K deux sous-groupes de G. Démontrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Exercice 20.

Déterminer tous les morphismes de $(\mathbb{Z}, +)$ dans lui-même. Lesquels sont injectifs ? surjectifs ?

c. Anneaux, sous-anneaux

Exercice 21.

Un élément x d'un anneau A est dit nilpotent s'il existe un entier $n \geq 1$ tel que $x^n = 0$. On suppose que A est commutatif, et on fixe x, y deux éléments nilpotents.

1. Montrer que xy est nilpotent.
2. Montrer que $x + y$ est nilpotent.
3. Montrer que $1_A - x$ est inversible.
4. Dans cette question, on ne suppose plus que A est commutatif. Soit $u, v \in A$ tels que uv est nilpotent. Montrer que vu est nilpotent.

Exercice 22.

On dit qu'un anneau A est un anneau de Boole si, pour tout $x \in A$, $x^2 = x$. On fixe A un tel anneau.

1. Démontrer que, pour tout $x \in A$, $x = -x$.
2. Montrer que A est commutatif.

Exercice 23.

Soit $(G, +)$ un groupe commutatif. On note $\mathrm{End}(G)$ l'ensemble des endomorphismes de G sur lequel on définit la loi $+$ par $f + g : G \to G,\ x \mapsto f(x) + g(x)$. Démontrer que $(\mathrm{End}(G), +, \circ)$ est un anneau.

Exercice 24.

Soit $A = \left\{\frac{m}{n};\ m \in \mathbb{Z},\ n \in 2\mathbb{N}+1\right\}$ (c'est-à-dire que A est l'ensemble des rationnels à dénominateur impair). Démontrer que $(A, +, \times)$ est un anneau. Quels sont ses éléments inversibles ?

Exercice 25.

Pour $d \in \mathbb{N}$, on note $A_d = \{(x, y) \in \mathbb{Z}^2;\ y - x \in d\mathbb{Z}\}$.

1. Démontrer que, pour tout $d \in \mathbb{N}$, A_d est un sous-anneau de $\mathbb{Z}^2$.
2. Réciproquement, soit A un sous-anneau de $\mathbb{Z}^2$. Démontrer que $H = \{x \in \mathbb{Z};\ (x, 0) \in A\}$ est un sous-groupe de $\mathbb{Z}$.
3. En déduire qu'il existe $d \in \mathbb{N}$ tel que $A = A_d$.

2. Exercices d'entraînement

a. Congruences

Exercice 26.

1. Soit $n \geq 1$. Montrer que $(n+1) | \binom{2n}{n}$.
2. Soit $p \geq 2$ premier. Montrer que $p | \binom{p}{k}$ pour $k \in \{1, \ldots, p-1\}$.
3. En déduire une preuve du petit théorème de Fermat : si $n \geq 1$ et p est premier, $n^p \equiv n\ [p]$.
4. (Plus difficile). Déduire de 2. que, pour tout $N \in \mathbb{N}^*$, pour tout $j \in \mathbb{N}^*$, pour tous $(x_1, \ldots, x_N) \in \mathbb{Z}^N$, on a
$$\left(\sum_{i=1}^{N} x_i\right)^{p^j} \equiv \sum_{i=1}^{N} x_i^{p^j}\ [p].$$

Exercice 27.

On note $\mathcal{A} = \{A, B, C, \ldots, Z\}$ l'alphabet, $\mathcal{E} = \{0, 1, 2, \ldots, 25\}$ l'ensemble des 26 premiers entiers naturels, et g la bijection naturelle de $\mathcal{A}$ sur $\mathcal{E}$ consistant à numéroter les lettres :
$$g(A) = 0,\ g(B) = 1,\ g(C) = 2, \ldots, g(Z) = 25.$$

1. Pour tout entier x de $\mathcal{E}$, on note $f(x)$ le reste de la division euclidienne de $35x$ par 26.
   (a) Montrer que l'on définit ainsi une bijection de $\mathcal{E}$ sur $\mathcal{E}$.
   (b) On convient de coder un mot quelconque de la façon suivante : on remplace chaque lettre α du mot par la lettre β dont le numéro $g(\beta)$ est tel que $g(\beta) = f(x)$, où $x = g(\alpha)$. Comment se code le mot OUI ? Montrer que cette méthode de codage est sans ambigüité (deux mots sont distincts ont des codages différents). Quel est le mot dont la codage est NWN ?

(c) On veut généraliser en remplaçant $35x$ par $ax+b$, avec a et b entiers naturels et $a \neq 0$. Quelle(s) hypothèse(s) doit-on faire sur a et b pour que la même méthode s'applique ?

2. Pour tout couple d'entiers (x, y) de $\mathcal{E} \times \mathcal{E}$, on note $f(x, y)$ et $h(x, y)$ les uniques entiers de $\mathcal{E}$ tels que

$$f(x, y) \equiv 5x + 17y \ [26] \text{ et } h(x, y) \equiv 4x + 15y \ [26].$$

(a) Justifier que l'application $f \times h$ est une bijection de $\mathcal{E} \times \mathcal{E}$ sur $\mathcal{E} \times \mathcal{E}$.

(b) On convient de coder tout mot contenant un nombre *pair* de lettres de la façon suivante : en partant de la gauche vers la droite, on remplace chaque couple de lettres successives (α, β) par le couple (γ, δ) dont les numéros $s = g(\gamma)$, $t = g(\delta)$ sont donnés par

$$s = f(x, y) \text{ et } t = h(x, y), \text{ où } x = g(\alpha) \text{ et } y = g(\beta) \text{ sont les numéros de } \alpha \text{ et } \beta.$$

Comment se code le mot ENFANT ? Le codage d'une lettre dépend-il de la place de cette lettre dans le mot ? Démontrer que le principe de codage est sans ambigüité, et que tout mot d'un nombre pair de lettres est le codage d'un et d'un seul mot. Quel est le mot dont le codage est XMEO ?

(c) On voudrait généraliser cette méthode de codage à un alphabet comprenant m lettres, en considérant les fonctions

$$f(x, y) \equiv ax + by \ [m] \text{ et } h(x, y) \equiv cx + dy \ [m],$$

avec a, b, c, d des entiers naturels. Donner une condition sur a, b, c, d et m assurant que la méthode de codage fonctionne encore.

Exercice 28.

Résoudre, dans $\mathbb{Z}^2$, les équations diophantiennes suivantes :

1. $xy = 2x + 3y$.
2. $x^2 - y^2 - x + 3y = 30$.
3. $x^2 - 5y^2 = 3$.

b. Groupes

Exercice 29.

On note $GL_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$, à coefficients dans $\mathbb{Z}$, qui sont inversibles et dont l'inverse est à coefficients dans $\mathbb{Z}$.

1. Démontrer que si M est à coefficients dans $\mathbb{Z}$, alors $M \in GL_n(\mathbb{Z})$ si et seulement si $\det(M) = \pm 1$.
2. En déduire que $GL_n(\mathbb{Z})$ est un sous-groupe de $GL_n(\mathbb{R})$.

Exercice 30.

Soit $(G, \cdot)$ un groupe. Pour $a \in G$, on note $\tau_a : G \to G$ défini par $\tau_a(x) = axa^{-1}$.

1. Démontrer que τ_a est un endomorphisme de G.
2. Vérifier que, pour tous $a, b \in G$, $\tau_a \circ \tau_b = \tau_{ab}$.
3. Montrer que τ_a est bijective et déterminer son inverse.
4. En déduire que $\Theta = \{\tau_a;\ a \in G\}$ muni du produit de composition est un groupe.

Exercice 31.

Soit G un groupe fini d'élément neutre e. On suppose que le cardinal de G est pair. Démontrer qu'il existe $x \in G$ avec $x \neq e$ tel que $x = x^{-1}$.

Exercice 32.

Soit G un ensemble fini muni d'une loi de composition interne $\star$ associative. On dit qu'un élément a de G est régulier si les deux conditions suivantes sont réalisées :

— l'égalité $a \star x = a \star y$ entraine $x = y$;

— l'égalité $x \star a = y \star a$ entraine $x = y$.

On suppose que tous les éléments de G sont réguliers, et on fixe $a \in G$.

1. Démontrer qu'il existe $e \in G$ tel que $a \star e = a$.
2. Démontrer que, pour tout $x \in G$, on a $e \star x = x$.
3. Démontrer que, pour tout $x \in G$, on a $x \star e = x$.
4. Démontrer que $(G, \star)$ est un groupe.
5. Le résultat subsiste-t-il si G n'est pas fini ?

Exercice 33.

Soit $(G, \cdot)$ un groupe fini et A, B deux sous-groupes de G. On note $AB = \{ab;\ a \in A,\ b \in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.

Exercice 34.

Démontrer que les groupes multiplicatifs $(\mathbb{R}^*, \cdot)$ et $(\mathbb{C}^*, \cdot)$ ne sont pas isomorphes.

Exercice 35.

Un groupe $(G, \cdot)$ est dit divisible si, pour tout $g \in G$ et tout $n \in \mathbb{N}^*$, il existe $u \in G$ tel que $u^n = g$.

1. Le groupe $(\mathbb{Q}, +)$ est-il divisible ?
2. Montrer que $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \cdot)$ ne sont pas isomorphes.

Exercice 36. *Théorème de Lagrange*

Soit $(G, \cdot)$ un groupe fini et H un sous-groupe de G.

1. Montrer que pour tout $a \in G$, H et $aH = \{ah;\ h \in H\}$ ont le même nombre d'éléments.
2. Soient $a, b \in G$. Démontrer que $aH = bH$ ou $aH \cap bH = \varnothing$.
3. En déduire que le cardinal de H divise le cardinal de G.

c. Anneaux, sous-anneaux

Exercice 37.

Soit $\mathbb{D}$ l'ensemble des nombres décimaux,

$$\mathbb{D} = \left\{ \frac{n}{10^k};\ n \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$

Démontrer que $(\mathbb{D}, +, \times)$ est un anneau. Quels sont ses éléments inversibles ?

Exercice 38.

On considère $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.
2. On note $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que, pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy) = N(x)N(y)$.
3. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a+b\sqrt{2}$ avec $a^2-2b^2 = \pm 1$.

Exercice 39.

Soit A un anneau. On appelle caractéristique de A l'ordre de 1_A dans le groupe additif $(A, +)$. Dans la suite, on supposera que A est de caractéristique finie n.

1. Démontrer que, pour tout $x \in A$, $nx = 0$.
2. Démontrer que si A est intègre, n est un nombre premier.
3. Démontrer que si A est intègre et commutatif, alors $x \mapsto x^n$ est un morphisme d'anneaux.

3. Exercices d'approfondissement

a. Groupes

Exercice 40.

Soit H un sous-groupe strict d'un groupe $(G, \cdot)$. Déterminer le sous-groupe engendré par le complémentaire de H.

Exercice 41.

Soit f un morphisme non constant d'un groupe fini $(G, \cdot)$ dans $(\mathbb{C}^*, \cdot)$. Calculer $\sum_{x \in G} f(x)$.

b. Anneaux, sous-anneaux

Exercice 42.

Soit A un anneau intègre commutatif fini. Démontrer que A est un corps.