Semaine 3 : Groupes, anneaux, corps, espaces vectoriels, algèbres, arithmétique

Questions de cours

Question de cours 1 : Formule du binôme de Newton

Enoncer et prouver la formule du binôme de Newton dans un anneau commutatif $\mathscr{A}$.

Question de cours 2 : Théorème de Bézout

Enoncer et prouver le théorème de Bézout en arithmétique.

Question de cours 3 : Sous-groupes de $(\mathbb{Z},+)$

Déterminer les sous-groupes de $(\mathbb{Z},+)$

Exercices

(*) Exercice 1 : Des groupes divers

Montrer que les ensembles suivants (pour les opérations associées) sont des groupes.

1. $SL_2(\mathbb{R}) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{M}_2(\mathbb{R}) \mid ad - bc = 1 \right\}$, muni de la multiplication matricielle.
2. $(\mathscr{P}(E), \Delta)$ où E est un ensemble dont on note $\mathscr{P}(E)$ l'ensemble des parties, et où Δ désigne la différence symétrique.
3. On pose, pour tout couple $(x,y) \in]-1,1[^2$, $x \star y = \dfrac{xy}{1+xy}$. Montrer que $(]-1,1[,\star)$ est un groupe.

(*) Exercice 2 : Un groupe d'ordre pair

Soit G un groupe d'ordre pair dont on note l'élément neutre e. Montrer qu'il existe un nombre impair d'éléments $x_i \in G$ tels que $x_i \neq e$ et $x_i^2 = e$.

(*) Exercice 3 : Le dernier chiffre

Trouver le dernier chiffre de $5467^{4291^{5523}}$.

(*) Exercice 4 : Les nombres premiers sont rares

Trouver 1000 entiers naturels consécutifs non premiers.

(*) Exercice 5 : Algèbre de matrices

Soit $A \in \mathcal{M}_n(\mathbb{R})$. On note $\mathscr{C}(A) = \left\{ B \in \mathcal{M}_n(\mathbb{R}) \;\middle|\; AB = BA \right\}$. Montrer que $\mathscr{C}(A)$ est une algèbre.

(*) Exercice 6 : Isomorphes ou non ?

Les groupes $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ et $(\mathbb{Z}/2\mathbb{Z})^3$ sont-ils isomorphes ?

(**) Exercice 1 : Le centre d'un groupe

Soit $(G,.)$ un groupe. On définit $Z(G) = \left\{ x \in G \;\middle|\; \forall y \in G, xy = yx \right\}$ le centre de G. Montrer que $Z(G)$ est un sous-groupe abélien de G. On suppose de plus que G admet un unique élément x_0 d'ordre 2. Montrer que $x_0 \in Z(G)$.

(**) Exercice 2 : Un peu de densité

Soit θ un réel tel que $\dfrac{\theta}{\pi}$ est irrationnel.

1. Montrer que $H := \left\{ e^{ik\theta} \;\middle|\; k \in \mathbb{Z} \right\}$ est un sous-groupe de $\mathbb{U}$.
2. Montrer que $\left\{ x \in \mathbb{R} \;\middle|\; e^{ix} \in H \right\}$ est un sous-groupe de $\mathbb{R}$ contenant 0 et 2π.
3. En déduire que $(\cos(n\theta))_{n\in\mathbb{N}}$ est dense dans $[-1,1]$.

(**) Exercice 3 : Une condition pour être un sous-groupe

A quelle condition la réunion de deux sous-groupes d'un groupe G est-elle un sous-groupe de G ?

(**) Exercice 4 : A un coup de peinture près

Les groupes $(\mathbb{Z}/8\mathbb{Z},+)$, $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},+)$ et $((\mathbb{Z}/2\mathbb{Z})^3,+)$ sont-ils isomorphes ?

(**) Exercice 5 : Théorème de Wilson

Montrer qu'un entier p est premier si et seulement si $(p-1)! \equiv -1\,[p]$.

(**) Exercice 6 : Les carrés de $\mathbb{Z}/p\mathbb{Z}$

Soit p un nombre premier impair.

1. Montrer que k est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $k^{\frac{p-1}{2}} = 1$
2. Si $x \in \mathbb{Z}/p\mathbb{Z}$, que peut valoir $x^{\frac{p-1}{2}}$?

(**) Exercice 7 : Anneau des rationnels à dénominateur impair

On note $\mathscr{A} = \left\{ \dfrac{p}{q} \;\middle|\; p \in \mathbb{Z}, q \in 2\mathbb{N}+1 \right\}$. Montrer que $(\mathscr{A}, +, \times)$ est un anneau, et déterminer ses éléments inversibles.

(**) Exercice 8 : Plus petit sous-corps de $\mathbb{R}$

Quel est le plus petit sous-corps (au sens de l'inclusion) de $(\mathbb{R}, +, \times)$?

(**) Exercice 9 : Une extension de $\mathbb{Q}$

On note $\mathbb{Q}[\sqrt{3}] = \left\{ a + b\sqrt{3} \;\middle|\; (a,b) \in \mathbb{Q}^2 \right\}$.

1. Montrer que $\mathbb{Q}[\sqrt{3}]$ est un sous-corps de $\mathbb{R}$.
2. Est-il isomorphe à $\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} \;\middle|\; (a,b) \in \mathbb{Q}^2 \right\}$?

(**) Exercice 10 : Un anneau d'entiers

On pose $\mathbb{Z}[\sqrt{2}] = \left\{ a + b\sqrt{2} \mid (a,b) \in \mathbb{Z}^2 \right\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.
2. On note, pour $(a,b) \in \mathbb{Z}^2$, $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que pour tout $(x,y) \in \mathbb{Z}[\sqrt{2}]^2$, $N(xy) = N(x)N(y)$
3. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont de la forme $a + b\sqrt{2}$, où $a^2 - 2b^2 = \pm 1$

(**) Exercice 11 : Produit dans un corps fini

Soit K un corps fini. Calculer $\prod_{x \in K^*} x$

(**) Exercice 12 : Suite d'anneaux

Soit $\mathscr{A}$ un anneau principal.

1. On suppose que toute suite décroissante (pour l'inclusion) d'idéaux de $\mathscr{A}$ est stationnaire. Montrer que $\mathscr{A}$ est un corps.
2. Montrer que toute suite croissante (pour l'inclusion) d'idéaux de $\mathscr{A}$ est stationnaire.

(**) Exercice 13 : Des factorielles !

Soit $n \in \mathbb{N}^*$. Montrer que $n! + 1$ et $(n+1)! + 1$ sont premiers entre eux.

(**) Exercice 14 : Un reste

Quel est le reste dans la division euclidienne de $(2222)^{3333}$ par $(3333)^{2222}$?

(**) Exercice 15 : Des combinaisons

Montrer que si $(k, n) \in \mathbb{N}^2$, alors :

$$k \wedge n = 1 \implies n \Big| \binom{n}{k}$$

(**) Exercice 16 : Des divisions

Montrer que, pour tout $n \in \mathbb{N}$:

1. 9 divise $2^{2^n} + 15n - 1$
2. 17 divise $3 \times 5^{2n-1} + 2^{3n-2}$
3. 9 divise $n^3 + (n+1)^3 + (n+2)^3$
4. n^2 divise $(n+1)^n - 1$

(**) Exercice 17 : Une division par 30

Montrer que pour tout $(m, n) \in \mathbb{Z}^2$, 30 divise $mn(m^4 - n^4)$.

(**) Exercice 18 : Les nombres de Fermat

On pose, pour $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$. Montrer que si $n \neq p$, F_n et F_p sont premiers entre eux.

(***) Exercice 1 : Sous-groupes additifs de $\mathbb{R}$

Soit G un sous-groupe de $(\mathbb{R}, +)$. Montrer que G est de la forme $\alpha\mathbb{Z}$ ou dense. (On pourra considérer $\alpha = \inf G \cap \mathbb{R}_+^*$)
En déduire une caractérisation des fonctions continues sur $\mathbb{R}$ admettant 1 et $\sqrt{2}$ comme périodes.

(***) Exercice 2 : Des sous-groupes distincts

Soit $(G, .)$ un groupe fini d'ordre $2n$ ($n \in \mathbb{N}^*$), d'élément neutre e. On suppose qu'il existe deux sous-groupes distincts H et H' de $(G, .)$, d'ordre n, tels que $H \cap H' = \{e\}$. Montrer que $n = 2$ et dresser la table de $(G, .)$.

(***) Exercice 3 : L'indicatrice d'Euler

On définit l'indicatrice d'Euler sur $\mathbb{N}^*$, notée φ, de la façon suivante. Si $n \in \mathbb{N}^*$, $\varphi(n)$ est égal au nombre d'entiers de $[\![1, n]\!]$ premiers avec n. Soit $n \in \mathbb{N}^*$. Montrer que :

$$\varphi(n) = \sum_{d|n} \varphi(d)$$

(***) Exercice 4 : Racine d'un idéal

Soient $(\mathscr{A}, +, \times)$ un anneau commutatif et $\mathscr{I}$ un idéal de $\mathscr{A}$. On appelle racine de $\mathscr{I}$ l'ensemble :

$$\sqrt{\mathscr{I}} = \left\{x \in \mathscr{A} \mid \exists n \in \mathbb{N}^*, x^n \in \mathscr{I}\right\}$$

1. Montrer que $\sqrt{\mathscr{I}}$ est un idéal de $\mathscr{A}$.
2. Montrer que $\sqrt{\sqrt{\mathscr{I}}} = \sqrt{\mathscr{I}}$.
3. Soient $\mathscr{I}$ et $\mathscr{J}$ deux idéaux de $\mathscr{A}$. Montrer que :
   (a) $\sqrt{\mathscr{I}} \cap \sqrt{\mathscr{J}} = \sqrt{\mathscr{I} \cap \mathscr{J}}$
   (b) $\sqrt{\mathscr{I}} + \sqrt{\mathscr{J}} \subset \sqrt{\mathscr{I} + \mathscr{J}}$
   (c) $\sqrt{\mathscr{I} + \mathscr{J}} = \sqrt{\sqrt{\mathscr{I}} + \sqrt{\mathscr{J}}}$

(***) Exercice 5 : Le carré d'un entier

1. Soit $(a, b) \in (\mathbb{N}^*)^2$. On suppose que a et b sont premiers entre eux et que ab est le carré d'un entier. Montrer que a et b sont des carrés d'entiers.
2. Montrer que le produit de trois entiers naturels non nuls consécutifs n'est jamais le carré d'un entier.

(***) Exercice 6 : Un peu de probabilités

1. Soit N un entier positif à 100 chiffres. Déterminer la probabilité que N^3 se termine par 11.
2. Déterminer tous les entiers positifs à 100 chiffres dont le cube se termine par 11.
3. Montrer que le résultat persiste pour un entier à p chiffres, où $p \geqslant 3$.