Correction des exercices du 16/09/2024 (Intégration et structures algébriques)

Intégration :

Ex 1 : ***1.*** Soit $M > 0$ et $u : [1, +\infty[\to \mathbb{R}$ de classe $\mathcal{C}^1$ tel que : $\forall x \in [1, +\infty[,\ |u(x)| \leqslant M$.
Montrer que $\displaystyle\int_1^\infty \frac{u'(t)}{t} dt$ converge.

2. Montrer que $\displaystyle\int_1^\infty \frac{\sin t}{t} dt$ et $\displaystyle\int_1^\infty \sin(t^2) dt$ convergent.

3.Montrer que $\displaystyle\int_1^\infty \sin(t^3) dt$ converge.

Correction : ***1.*** La fonction $t \mapsto \dfrac{u'(t)}{t}$ est continue sur $[1, +\infty[$.
Soit $X \geq 1$. On a par intégration par parties :
$\displaystyle\int_1^X \frac{u'(t)}{t} dt = \left[\frac{u(t)}{t}\right]_1^X + \int_1^X \frac{u(t)}{t^2} dt = \frac{u(X)}{X} - u(1) + \int_1^X \frac{u(t)}{t^2} dt.$
On a $\displaystyle\lim_{X \to +\infty} \frac{u(X)}{X} = 0$, car $\left|\dfrac{u(X)}{X}\right| \leq \dfrac{M}{X}$.
La fonction $t \mapsto \dfrac{u(t)}{t^2}$ est intégrable sur $[1, +\infty[$, car : $\forall t \in [1, +\infty[,\ \left|\dfrac{u(t)}{t^2}\right| \leq \dfrac{M}{t^2}$.
Ainsi $\displaystyle\lim_{X \to +\infty} \int_1^X \frac{u(t)}{t^2} dt$ existe et donc $\displaystyle\lim_{X \to +\infty} \int_1^X \frac{u'(t)}{t} dt$ aussi.
Ainsi $\displaystyle\int_1^\infty \frac{u'(t)}{t} dt$ converge.

2. Pour $\displaystyle\int_1^\infty \frac{\sin t}{t} dt$, utiliser la question précédente avec $u(t) = -\cos(t)$ qui correspond à une fonction bornée et $\forall t \in [1, +\infty[,\ \dfrac{u'(t)}{t} = \dfrac{\sin(t)}{t}$.
Pour $\displaystyle\int_1^\infty \sin(t^2) dt = \int_1^\infty \frac{t\sin(t^2)}{t} dt$, utiliser la question précédente avec $u(t) = -\cos(t^2)/2$ qui correspond à une fonction bornée et on a bien $\dfrac{u'(t)}{t} = \dfrac{t\sin(t^2)}{t} = \sin(t^2)$).

3. On a qui par IPP : $\displaystyle\int_1^X \sin(t^3) dt = \int_1^X \frac{t^2\sin(t^3)}{t^2} dt = \left[\frac{-\cos(t^3)}{3t^2}\right]_1^X - \int_1^X \frac{2\cos(t^3)}{3t^3} dt$ et on conclut comme dans la première questions.

Structures algébriques :

Ex 2 :

1. Soit $a \in \mathbb{N}$. Montrer que le reste de la division euclidienne de a^2 par 8 est égal à $0, 1$ ou 4.
2. Soit $n \in \mathbb{N}$. Montrer que si $n \equiv 7[8]$, alors n ne peut pas être la somme de trois carrés d'entiers.

Correction :

1. Si a est impair, alors, $a = 1 + 2l$, avec l dans $\mathbb{N}$, puis $a^2 = 1 + 4l + 4l^2 = 1 + 4l(l + 1)$. Parmi les entiers l et $l + 1$, l'un d'eux est pair, donc $l(l + 1)$ et pair et donc $4l(l + 1)$ est un multiple de 8. Ainsi $a \equiv 1[8]$.
   Si a est pair, alors $a = 2l$, avec l dans $\mathbb{N}$. Si l est pair, alors a est de la forme $a = 2(2p) = 4p$,

sinon $a = 2(2p+1)$, avec p dans $\mathbb{N}$. Dans le premier cas $a^2 = 16p^2 \equiv 0[8]$ et dans le deuxième cas, $a^2 = 4 + 16p + 16p^2 \equiv 4[8]$.

$$\boxed{\text{Le reste de la division euclidienne de } a^2 \text{ par 8 est égal à } 0, 1 \text{ ou } 4}$$

2. On suppose qu'il existe a, b, c dans $\mathbb{N}$ tels que $n = a^2 + b^2 + c^2$. Ainsi $a^2 + b^2 + c^2 \equiv 7[8]$. Grâce à la question précédente, les congruences modulo 8 de a^2, b^2 et c^2 sont égales à $0, 1$ ou 4. Les différentes combinaisons des sommes de ces trois chiffres donnent : $0, 1, 2, 3, 4, 5, 6, 8, 9, 12$, mais aucun de ces nombres n'est congru à 7 modulo 8.

$$\boxed{\text{Si } n \equiv 7[8], \text{ alors } n \text{ ne peut pas être la somme de trois carrés d'entiers}}$$

Fin de la correction des exercices de TD

<u>Ex 3</u> : Soit G un groupe. On note $\widehat{G}$ l'ensemble des morphismes de groupes de G dans $(\mathbb{C}^*, \times)$.

1. Montrer que $\widehat{G}$ est un groupe.

2. Déterminer $\widehat{G}$ dans le cas où $G = \mathbb{Z}/n\mathbb{Z}$.

Correction :

1. Fait en TD

2. Soit $f \in \widehat{G}$. On pose $z = f(\overline{1})$. On a par morphisme de groupes :
$\forall k \in \mathbb{N}^*,\ f(\overline{k}) = f(\underbrace{\overline{1} + \ldots + \overline{1}}_{k \text{ fois}}) = \left(f(\overline{1})\right)^k = z^k$.
De plus, par morphisme de groupes, on a : $1 = f(\overline{0}) = f(\overline{n}) = z^n$ donc z est dans $\mathbb{U}_n$, donc il existe $p \in [\![0, n-1]\!]$ tel que $z = e^{\frac{2i\pi p}{n}}$.
Par morphisme de groupes : $\forall k \in \mathbb{Z},\ f(\overline{k}) = e^{\frac{2ik\pi p}{n}}$.

Réciproquement, pour $p \in [\![0, n-1]\!]$, soit $f : \overline{k} \mapsto e^{\frac{2ik\pi p}{n}}$. Montrons que f est bien définie.
Soient $k, l \in \mathbb{Z}$ tel que $\overline{k} = \overline{l}$. Il existe donc $q \in \mathbb{Z}$ tel que $k = l + nq$.
Ainsi : $e^{\frac{2ik\pi p}{n}} = e^{\frac{2il\pi p}{n} + 2i\pi pq} = e^{\frac{2il\pi p}{n}}$, donc $f(\overline{k}) = f(\overline{l})$.
On a enfin : $\forall k, l \in \mathbb{Z},\ f(\overline{k} + \overline{l}) = f(\overline{k+l}) = e^{\frac{2i(k+l)\pi p}{n}} = e^{\frac{2ik\pi p}{n}} e^{\frac{2il\pi p}{n}} = f(\overline{k})f(\overline{l})$. Ainsi f est bien un morphisme de groupe.

<u>Ex 4</u> : Soit G un groupe fini non réduit à un singleton. Montrer que $|G|$ est premier si et seulement si ses seuls sous-groupes sont $\{e\}$ et G.
Correction :
On suppose que $p = |G|$ est premier. Soit H un sous-groupe de G différent de $\{e\}$. Soit $h \in H \setminus \{e\}$. Alors l'ordre ℓ de h divise p. Mais $h \neq e$, donc son ordre vaut au moins 2, puis $\ell = p$, car p est premier. Ainsi $\langle h \rangle \subset G$ et $|\langle h \rangle| = p = |G|$, donc $\langle h \rangle = G$. Or on a : $\langle h \rangle \subset H$, donc $H = G$.

On suppose que les seuls sous-groupes sont $\{e\}$ et G. Soit $g \in G \setminus \{e\}$. Alors $\langle g \rangle$ est un sous-groupe de G différent de $\{e\}$, donc $\langle g \rangle = G$. Soit p l'ordre de G. Si on a $p = ab$, avec $1 < a < p$ et $1 < b < p$, alors montrons que g^a est d'ordre b.
On a $e = g^n = g^{ab} = (g^a)^b$, et comme g^a est d'ordre l, alors $l | b$.
Soit l l'ordre de g^a. On a alors $e = (g^a)^l = g^{al}$, donc $p | al$, car g est d'ordre p, puis $b | l$.
Ainsi $b = l$ et donc $\langle g^a \rangle$ est un sous-groupe de G différent de $\{e\}$ et G. Ceci est contradictoire, donc $p = |G|$ est premier.