Université Côte d'Azur – Groupes et géométrie
Année 2020-2021

EPREUVE DU 15 JANVIER 2021

Les documents sont interdits,
TOUTES les réponses doivent être impérativement justifiées,
la qualité de la rédaction est prise en compte

Exercice 1

Parmi les assertions suivantes, démontrer celles qui sont vraies et donner un contre-exemple pour celles qui sont fausses (on indiquera d'abord si l'assertion est vraie ou fausse).

a) Soit G un groupe quelconque. Soient x, y dans G. Si xy est d'ordre fini p dans G, alors yx est d'ordre fini p dans G.

b) Si G est un groupe fini abélien et p est un nombre premier divisant $|\mathrm{G}|$, alors G contient un unique p-Sylow.

c) Soit p un nombre premier. Soit G un groupe fini vérifiant : pour tout $x \in \mathrm{G}$, il existe $m \in \mathbb{N}^*$ tel que $x^{p^m} = e_{\mathrm{G}}$. Alors G est un p-groupe.

Solution 1

a) C'est vrai. Remarquons que

$$(xy)^n = \underbrace{(xy)(xy)\dots(xy)}_{n \text{ termes}} = x\underbrace{(yx)(yx)\dots(yx)}_{(n-1) \text{ termes}}y = x(yx)^{n-1}y.$$

Ainsi

$$(xy)^n = e \iff x(yx)^{n-1}y = e \iff yx(yx)^{n-1}y = y \iff (yx)^n = e$$

ce qui montre que les ordres de xy et yx sont identiques.

b) C'est vrai. En effet on sait que G possède un p-Sylow S et que tout p-Sylow H est conjugué de S mais comme G est abélien ceci implique $\mathrm{H} = \mathrm{S}$.

c) C'est vrai. Sinon $|\mathrm{G}|$ aurait un diviseur premier $q \neq p$ et G contiendrait donc un q-Sylow non trivial H. Tout $x \neq e_{\mathrm{G}}$ dans H serait alors d'ordre q^s avec $s > 0$ ce qui n'est pas possible vu que l'hypothèse impose que l'ordre de x est de la forme p^r avec $r > 0$.

Exercice 2

Soient G_1, G_2, …, G_n des groupes cycliques d'ordres respectifs α_1, α_2, …, α_n. Posons $\mathrm{G} = \mathrm{G}_1 \times \mathrm{G}_2 \times \ldots \times \mathrm{G}_n$.

a) Pour tout i, soit x_i un élément de G_i d'ordre β_i. Montrer que $x = (x_1, x_2, \dots, x_n)$ est d'ordre $\mathrm{ppcm}(\beta_1, \beta_2, \dots, \beta_n)$ dans G.

b) Donner une condition nécessaire et suffisante portant sur les α_i pour que le groupe G soit cyclique.

Solution 2

a) Pour $1 \leqslant i \leqslant n$ notons e_i l'élément neutre de G_i de sorte que $e = (e_1, e_2, \dots, e_n)$ est l'élément neutre de G. Nous avons

$$x^p = e \iff \forall\, i \quad x_i^p = e_i \iff \forall\, i \quad \beta_i \text{ divise } p.$$

Le plus petit entier naturel non nul p tel que $x^p = e$ est donc le plus petit multiple commun aux β_i.

b) Montrons la condition nécessaire et suffisante : le groupe G est cyclique si et seulement si les α_i sont premiers entre eux deux à deux.

Condition nécessaire. Soit $x = (x_1, x_2, \ldots, x_n)$ engendrant G. Pour tout i, x_i engendre G_i donc est d'ordre α_i. D'après a) l'ordre de x est $\mathrm{ppcm}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Comme x engendre G son ordre est aussi $|\mathrm{G}| = \alpha_1\alpha_2 \ldots \alpha_n$. Ainsi $\mathrm{ppcm}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1\alpha_2 \ldots \alpha_n$ ce qui entraîne que les α_i sont premiers entre eux deux à deux.

Condition suffisante. Pour tout i, considérons $x_i \in \mathrm{G}_i$ d'ordre α_i (x_i existe puisque G_i est cyclique par hypothèse). D'après a) $x = (x_1, x_2, \ldots, x_n)$ est d'ordre $\mathrm{ppcm}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ dans G et ce dernier terme est égal à $\alpha_1\alpha_2 \ldots \alpha_n = |\mathrm{G}|$ puisque les α_i sont premiers entre eux deux à deux. Finalement $\mathrm{G} = \langle x \rangle$ est cyclique.

Exercice 3

Soient p et q deux nombres premiers distincts. Montrer qu'il n'existe pas de groupe simple d'ordre p^2q.

Solution 3

Soit G un groupe d'ordre p^2q. Soit n_p (resp. n_q) le nombre de p-Sylow (resp. q-Sylow) de G.

Nous allons distinguer le cas $q < p$ du cas $p < q$.

- ◇ Si $p > q$, alors n_p divise q et $n_p \equiv 1 \bmod p$. Comme $q < p$ nécessairement $n_p = 1$; le groupe G possède alors un unique p-Sylow qui est distingué dans G et G n'est pas simple.
- ◇ Si $p < q$, alors n_q divise p^2 et $n_q \equiv 1 \bmod q$. Ainsi n_q appartient à $\{1, p, p^2\}$ et $n_q \equiv 1 \bmod q$. Puisque $q < p$, $n_q \neq p$, *i.e.* n_q appartient à $\{1, p^2\}$. Si $n_q = 1$, alors le groupe G n'est pas simple. Étudions la dernière possibilité : $n_q = p^2$. Si $n_q = p^2$, alors $p^2 \equiv 1 \bmod q$ et $p \equiv \pm 1 \bmod q$. Comme $p < q$ ceci entraîne que $p = q - 1$; étant donné que p et q sont premiers nous obtenons $p = 2$ et $q = 3$. Dans ce dernier cas, il y a quatre 3-Sylow d'ordre 3 qui contiennent huit éléments d'ordre 3. Ne reste de la place que pour un seul 2-Sylow qui devrait être distingué. Ce dernier cas n'est donc lui non plus pas possible.

Exercice 4

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

Solution 4

Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$. L'image de f est un sous-groupe de $\mathbb{Z}$, c'est-à-dire un certain $n\mathbb{Z}$, $n \in \mathbb{N}$.

- ◇ Si $n \geqslant 1$, on choisit un antécédent x de n. Nous obtenons alors $2f\left(\frac{x}{2}\right) = f\left(\frac{x}{2} + \frac{x}{2}\right) = f(x) = n$ et $\frac{n}{2} = f\left(\frac{x}{2}\right) \in n\mathbb{Z}$ ce qui est absurde.
- ◇ Si $n = 0$, alors f est le morphisme nul.

Ainsi un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ est nul.

Exercice 5

1. Soit G un groupe fini qui opère sur un ensemble fini non vide E. Supposons que G soit d'ordre p^m avec p premier et $m \in \mathbb{N}^*$. Posons
$$E^{\mathrm{G}} = \left\{x \in E \,|\, \forall\, g \in \mathrm{G},\, g \cdot x = x\right\}.$$
Montrer que $|E^{\mathrm{G}}| \equiv |E| \bmod p$.
2. Soit H un groupe fini d'ordre n. Soit p un diviseur premier de n. Montrer que H contient un élément d'ordre p (lemme de Cauchy). Indication : faire agir $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble E des $(x_1, x_2, \ldots, x_p)$ de H^p tels que $x_1x_2 \ldots x_p = e$.
3. Soit H un groupe fini d'ordre n. Soit $m \in \mathbb{N}^*$ tel que pour tout $x \in \mathrm{H}$ on ait $x^m = e$. Montrer que n divise une puissance de m.

Solution 5

1. Si x appartient à E, nous notons $\mathcal{O}(x)$ l'orbite de x sous l'action de G. Les éléments de E^{G} sont exactement les éléments x de E tels que $\mathcal{O}(x) = \{x\}$. Notons ω_1, ω_2, …, ω_r les orbites de E de cardinal strictement supérieur à 1. Si x_i est un élément de ω_i, alors $|\omega_i| = \left|\mathrm{G}/\mathrm{G}_{x_i}\right| = \frac{|\mathrm{G}|}{|\mathrm{G}_{x_i}|}$, c'est donc une puissance de p. Il résulte de l'équation aux classes que
$$|E| = |E^{\mathrm{G}}| + \sum_{i=1}^{r} |\omega_i| \equiv |E^{\mathrm{G}}| \mod p$$

2. Soit $(x_1, x_2, \ldots, x_p)$ un élément de E. Nous avons $x_1 x_2 \ldots x_p = e$. En multipliant à gauche par x_1^{-1} et à droite par x_1 nous obtenons $x_2 x_3 \ldots x_p x_1 = e$, *i.e.* $(x_2, x_3, \ldots, x_p, x_1)$ appartient à E. Notons c le cycle $(1\ 2\ \ldots\ p)$ de $\mathcal{S}_p$. Il s'agit d'un élément d'ordre p qui engendre un sous-groupe cyclique K isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Nous définissons une opération de K sur l'ensemble H^p par

$$c \cdot (x_1, x_2, \ldots, x_p) = (x_{c(1)}, x_{c(2)}, \ldots, x_{c(p)}) = (x_2, x_3, \ldots, x_p, x_1).$$

La remarque ci-dessus montre que E est stable par cette opération. Appliquons alors le résultat de la question précédente à l'opération induite sur E. Nous avons $|E| \equiv |E^{\mathrm{K}}| \mod p$. Le cardinal de E est n^{p-1} (en effet on peut choisir x_1, x_2, …, x_{p-1} quelconques, x_p est alors déterminé de manière unique). Comme p divise n, $|E^{\mathrm{K}}|$ est nul modulo p. Or les éléments de E^{K} sont justement les p-uplets $(x, x, \ldots, x)$ avec $x^p = e$. Notons que E^{K} contient le p-uplet $(e, e, \ldots, e)$; en particulier E^{K} est non vide et par suite E^{K} a un cardinal supérieur à p. Il y a donc au moins $(p-1)$ éléments d'ordre p dans H.

3. Il suffit de montrer que tous les facteurs premiers de n sont des facteurs premiers de m. Soit p un premier divisant n. Le lemme de Cauchy assure l'existence d'un élément $x \in \mathrm{H}$ d'ordre p. Or par hypothèse $x^m = e$ donc p divise m.

Exercice 6

On rappelle qu'un morphisme $(\rho, V) \to (\pi, W)$ entre deux représentations de G est un morphisme $\mathbb{C}$-linéaire $\varphi\colon V \to W$ tel que $\varphi \circ \rho(g) = \pi(g) \circ \varphi$ pour tout $g \in \mathrm{G}$. On parle aussi de G-morphisme, ou encore d'application linéaire G-équivariante.

Le but de cet exercice est de montrer que le centre du groupe $\mathrm{GL}(n, \mathbb{C})$ est le groupe des homothéties. Soit ρ l'action naturelle de $\mathrm{GL}(n, \mathbb{C})$ sur $\mathbb{C}^n$.

a) Montrer que la représentation ρ est irréductible.

b) Montrer que tout élément du centre de $\mathrm{GL}(n, \mathbb{C})$ est un morphisme de la représentation ρ.

c) Conclure en utilisant le Lemme de Schur.

Solution 6

Puisque ρ est l'action naturelle de $\mathrm{GL}(n, \mathbb{C})$ sur $\mathbb{C}^n$, ρ est l'identité de $\mathrm{GL}(n, \mathbb{C})$ dans $\mathrm{GL}(n, \mathbb{C})$.

a) Si un sous-espace vectoriel V de $\mathbb{C}^n$ est stable par tous les éléments de $\mathrm{GL}(n, \mathbb{C})$, alors il est évident que $V = \{0\}$ ou $V = \mathbb{C}^n$, c'est-à-dire que ρ est irréductible.

b) Soit h un élément du centre de $\mathrm{GL}(n, \mathbb{C})$. Donc pour tout $M \in \mathrm{GL}(n, \mathbb{C})$ on a $\rho(M) \circ h = Mh = hM = h \circ \rho(M)$, donc h est bien un morphisme de la représentation ρ.

c) Comme ρ est irréductible, d'après le Lemme de Schur, on a $h = \lambda \mathrm{id}$ avec $\lambda \in \mathbb{C}^*$, c'est-à-dire que h est une homothétie.

Exercice 7

On rappelle qu'un morphisme $(\rho, V) \to (\pi, W)$ entre deux représentations de G est un morphisme $\mathbb{C}$-linéaire $\varphi\colon V \to W$ tel que $\varphi \circ \rho(g) = \pi(g) \circ \varphi$ pour tout $g \in \mathrm{G}$. On parle aussi de G-morphisme, ou encore d'application linéaire G-équivariante.

Soit G un groupe abélien.

a) Si $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ est une représentation de G, montrer que tout élément g de G définit un G-morphisme $V \to V$.

b) En déduire que toute représentation irréductible de G est de dimension 1.

c) Donner toutes les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$.

Solution 7

Comme souvent on note $g \cdot x$ pour $\rho(g)(x)$.

a) Pour tous g, h, $x \in \mathrm{G}$, nous avons

$$g \cdot (h \cdot x) = (gh) \cdot x = (hg) \cdot x = h \cdot (g \cdot x)$$

c'est-à-dire l'application $\rho(g)\colon x \mapsto g \cdot x$ est un G-morphisme pour tout $g \in \mathrm{G}$.

b) On suppose que V est une représentation irréductible de G. Si $g \in \mathrm{G}$, alors d'après la question précédente et le Lemme de Schur, $\rho(g) = \lambda \mathrm{id}$. De plus, comme $\rho(g) \in \mathrm{GL}(V)$, on a $\lambda \neq 0$. Donc tout sous-espace vectoriel de V est stable par G, et est donc une sous-représentation de G. Comme V est irréductible, on a nécessairement $\dim(V) = 1$.

c) D'après la question précédente, une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes $\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}(1, \mathbb{C}) = \mathbb{C}^*$. Comme tout élément k de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre divisant n, l'élément $\rho(k)$ sera aussi d'ordre divisant n, c'est-à-dire $\rho(k)^n = 1$. Réciproquement, pour toute racine $n$ème de l'unité ω, l'application

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*, \qquad k \mapsto \omega^k$$

est une représentation de $\mathbb{Z}/n\mathbb{Z}$, donc on les obtient toutes ainsi. On voit ainsi que l'espace des représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure de groupe qui le rend isomorphe à $\mathbb{Z}/n\mathbb{Z}$.