Contôle (Algèbre 2)

Il sera tenu compte, dans l'appréciation des copies, de la précision des raisonnements ainsi que la clarté de la rédaction.

G H

LEEM

Corrigé

Montesquieu

✾ Les propositions mathématiques sont reçues comme vraies parce que personne n'a intérêt qu'elles soient fausses.

Questions de Cours

Cours

Exercice 1 (Question de cours)

Soit $f : G \to G'$ un morphisme de groupes.
On note e respectivement e' le neutre de G respectivement de G'. On rappel que $\ker f = \{x \in G \,/\, f(x) = e\}$ et $\text{Im}\, f = \{f(x) \,/\, x \in G\}$.

1. On a $f(e) = e'$ donc $e \in \ker f$. Soient $x, y \in \ker f$, on a

$$f(xy^{-1}) = f(x)(f(y))^{-1} = e'e'^{-1} = e'$$

Donc $xy^{-1} \in \ker f$. Ainsi $\ker f$ est un sous groupe de G.

2. On a $e' = f(e)$, donc $e' \in \text{Im}\, f$. Soient $a, b \in \text{Im}\, f$ alors ils existent $x, y \in G$ tels que $a = f(x)$ et $b = f(y)$. Or

$$ab^{-1} = f(x)(f(y))^{-1} = f(xy^{-1})$$

on a bien $ab^{-1} \in \text{Im}\, f$. Par conséquent $\text{Im}\, f$ est un sous groupe de G'.

Exercice 2

On considère les deux permutations de S_7 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 7 & 3 & 5 & 4 \end{pmatrix}, \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 1 & 7 & 5 & 6 \end{pmatrix}$$

1. Calcul de $\sigma\sigma'$: On a $(\sigma\sigma')(1) = \sigma(\sigma'(1)) = \sigma(4) = 7$, de même pour les autres éléments, on obtient

$$\sigma\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 6 & 2 & 4 & 3 & 5 \end{pmatrix}$$

2. Décomposition de σ et σ' en produit de cycles disjoints :

$$\sigma = (1\ 2)(3\ 6\ 5)(4\ 7) \quad \text{et} \quad \sigma' = (1\ 4)(5\ 7\ 6)$$

3. Les signatures de σ et σ' : On rappel que la signature d'un p-cycle est $(-1)^{p-1}$ et que ε (la signature) est un morphisme de groupes. En utilisant ces propriétés, on a
$\varepsilon(\sigma) = \varepsilon((1\ 2))\varepsilon((3\ 6\ 5))\varepsilon((4\ 7)) = (-1)\times 1\times(-1) = 1$.
$\varepsilon(\sigma') = \varepsilon((1\ 4))\varepsilon((5\ 7\ 6)) = -1$.

Exercice 3 On considère $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \ / \ a, b \in \mathbb{Z}\}$.

1. $\mathbb{Z}[i\sqrt{2}]$ est un sous anneau (unitaire) de $\mathbb{C}$: D'abord $0 = 0 + i.0.\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$. Soient $x = a + ib\sqrt{2}, y = c + id\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ où $a, b, c, d \in \mathbb{Z}$; on a

$$x - y = (a - c) + i(b - d)\sqrt{2}$$

Or $a - c, b - d \in \mathbb{Z}$ on a donc $x - y \in \mathbb{Z}[i\sqrt{2}]$. On a aussi

$$xy = (ac - 2bd) + i(ad + bc)\sqrt{2}$$

et les deux éléments $ac - 2bd$ et $ad + bc$ sont dans $\mathbb{Z}$, donc $xy \in \mathbb{Z}[i\sqrt{2}]$. Notons que $1 = 1 + 0.i.\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$. Donc $\mathbb{Z}[i\sqrt{2}]$ est un sous anneau unitaire de $\mathbb{C}$.

2. Si $z = a + ib\sqrt{2}$ où $a, b \in \mathbb{Z}$ alors clairement $\overline{z} = a - ib\sqrt{2} = a + i(-b)\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$.

3. Soit $z \in \mathbb{Z}[i\sqrt{2}]$. Si z est inversible dans $\mathbb{Z}[i\sqrt{2}]$ alors il existe $z' \in \mathbb{Z}[i\sqrt{2}]$ tel que $zz' = 1$. Par conséquent $\overline{z}\,\overline{z'} = \overline{zz'} = 1$, par suite $\overline{z}$ est un élément inversible dans $\mathbb{Z}[i\sqrt{2}]$ dont l'inverse est $\overline{z'}$ ($\in \mathbb{Z}[i\sqrt{2}]$).
Si $\overline{z}$ est inversible, en utilisant un un même raisonnement (que précédemment), alors $z = \overline{\overline{z}}$ est inversible.

4. Clairement 1 et -1 sont inversibles dans $\mathbb{Z}[i\sqrt{2}]$. Soit maintenant $z = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ (où $a, b \in \mathbb{Z}$) un élément inversible de $\mathbb{Z}[i\sqrt{2}]$. D'après le résultat précédent $\overline{z}$ est aussi inversible. Par conséquent $a^2 + 2b^2 = z\overline{z}$ est inversible dans $\mathbb{Z}[i\sqrt{2}]$. Ils existent alors $\alpha, \beta \in \mathbb{Z}$ tels que $(a^2 + 2b^2)(\alpha + i\beta\sqrt{5}) = 1$, en regardons les parties réelles, on a $(a^2 + 2b^2)\alpha = 1$. Puisque $a^2 + 2b^2$ et α sont des entiers, il vient que $a^2 + 2b^2 = 1$. Comme a et b sont des entiers, $a = \pm 1$ et $b = 0$. Autrement dit $z = 1$ ou $z = -1$. On en déduit alors que $\mathbb{Z}[i\sqrt{2}] = \{-1, 1\}$.

Exercice 4 Soit G un groupe et H une partie finie non vide et stable pour la loi de G.

1. Si $h \in H$ alors $f(h) = ah \in H$ car $a, h \in H$ et H stable. L'application f_a est bien définie. Si $h, h' \in H$ tels que $f_a(h) = f_a(h')$ alors $ah = ah'$, on compose à gauche par l'inverse de a on obtient $h = h'$. L'application f_a est donc injective. Puisque H est finie, l'application $f_a : H \to H$ est alors bijective.

2. Puisque $a \in H$ et f_a surjective, il existe $b \in H$ tel que $f_a(b) = a$ autrement dit $ab = a$, donc $a^{-1}ab = a^{-1}a$ c'est-à-dire $b = e$. Ainsi $e = b \in H$.

3. Il suffit de montrer que H est stable par passage à l'inverse ; c'est-à-dire si $a \in H$ alors $a^{-1} \in H$. Soit $a \in H$ quelconque. En utilisant la surjectivité de l'application f_a et le fait que $e \in H$, il existe $a' \in H$ tel que $f_a(a') = e$ donc $a'a = e$. Ainsi $a^{-1} = a' \in H$.

PROBLÈME

Autour du théorème de Lagrange

Dans tout le problème G est un groupe fini de cardinal n et g un élément de G.

Première partie : Cas abélien

On suppose dans cette partie que G est commutatif et on considère l'application $f : G \to G$ définie pour tout $x \in G$ par $f(x) = gx$.

1. Si $f(x) = f(y)$ alors $gx = gy$ par suite $g^{-1}gx = g^{-1}gy$, ainsi $x = y$. L'application f est donc injective.
   Soit $z \in G$. On a $g^{-1}z \in G$ et $f(g^{-1}z) = gg^{-1}z = z$. Il en résulte alors que f est surjective.
   L'application f est à la fois injective et surjective donc elle est bijective.
2. De la surjectivité de f il découle $G = f(G) = \{f(x) \ / x \in G\} = \{gx \ / x \in G\}$
3. Du fait que les éléments gx avec $g \in G$ sont deux à deux distincts et $G = \{gx \ / x \in G\}$, l'élément $\prod_{x\in G} gx$ est le produit de tous les éléments de G, ainsi
   $$\prod_{x\in G} gx = \prod_{x\in G} x$$
   Puisque G est commutatif, $\prod_{x\in G} gx = g^{|G|}\prod_{x\in G} x = g^n \prod_{x\in G} x$. D'où
   $$g^n \prod_{x\in G} x = \prod_{x\in G} x$$
4. Posons $z = \prod_{x\in G} x$. D'après le résultat précédent on a $g^n z = z$ donc $g^n = e$.

Deuxième partie : Lagrange

Dans cette partie G est un groupe non nécessairement commutatif et H un sous groupe de G.
On définit sur G la relation binaire suivante : Pour tout $(x, y) \in G^2$, $x\mathscr{R}y \iff x^{-1}y \in H$.

5. Soit $x \in G$. On a $x^{-1}x = e \in H$ donc $x\mathscr{R}x$. D'où la réflexivité.
   Soit $x, y \in G$ tels que $x\mathscr{R}y$, c'est-à-dire $x^{-1}y \in H$. On a $y^{-1}x = (x^{-1}y)^{-1}$, or $x^{-1}y \in H$ et H sous groupe de G, on a donc $(x^{-1}y)^{-1} \in H$ autrement dit $y^{-1}x \in H$. Par conséquent $y\mathscr{R}x$. La relation $\mathscr{R}$ est symétrique.
   Soient $x, y, z \in G$ tels que $x\mathscr{R}y$ et $y\mathscr{R}z$ c'est-à-dire $xy^{-1} \in H$ et $yz^{-1} \in H$. Clairement
   $$xy^{-1} = \underbrace{(xy^{-1})}_{\in H}\underbrace{(yz^{-1})}_{\in H} \in H$$
   car H sous groupe de G. Ainsi $x\mathscr{R}z$. D'où la transitivité de $\mathscr{R}$.
6. Soit $x \in G$.
   $$\begin{aligned}\overline{x} &= \{y \in G \ / x\mathscr{R}y\} = \{y \in G \ / x^{-1}y \in H\}\\ &= \{y \in G \ / \exists h \in H \text{ tel que } x^{-1}y = h\}\\ &= \{y \in G \ / \exists h \in H \text{ tel que } y = xh\}\\ &= xH\end{aligned}$$
7. Notons d'abord que $|H| = |xH|$ (l'application $h \mapsto xh$ réalise une bijection de H dans xH). La famille $(\overline{x_i})_{1\le i\le r}$ forme une partition de G, donc
   $$|G| = |x_1| + \ldots + |x_r| = |x_1H| + \ldots + |x_rH| = |H| + \ldots + |H| = r|H|$$
8. Découle de l'égalité $|G| = r|H|$.

www.algebre.aqalmoun.com Mohamed Aqalmoun

Troisième partie : Cas non commutatif

Dans cette partie $H = \{g^k \ / k \in \mathbb{Z}\}$.

9. On a $e = g^0 \in H$. Soient $x, y \in H$. Ils existent $k, l \in \mathbb{Z}$ tels que $x = g^k$ et $y = g^l$. On a $xy^{-1} = g^k g^{-l} = g^{k-l}$, or $k - l \in \mathbb{Z}$ on a donc $xy^{-1} \in H$.

10. On considère l'ensemble suivant $A = \{k \in \mathbb{N}^* \ / g^k = e\}$. Il s'agit de démontrer que A admet un plus petit élément. Or A est une partie de $\mathbb{N}$, il suffit alors de démontrer qu'il est non vide. Puisque H est fini, ils existent au moins deux entiers distincts k et k' tels que $g^k = g^{k'}$. On a $k < k'$ ou $k' < k$. Dans le cas $k > k'$, on a $g^{k-k'} = e$ et $k - k' \in \mathbb{N}^*$, dans l'autre cas on a $g^{k'-k} = e$ et $k' - k \in \mathbb{N}^*$. Autrement dit, l'un des deux entiers $k - k'$ ou $k' - k$ appartient à A. Ainsi A est non vide.

11. Clairement $\{e, g, \ldots, g^{p-1}\} \subseteq H$. Réciproquement, soit $x \in H$. Il existe $k \in \mathbb{Z}$ tel que $x = g^k$. En effectuant la division euclidienne de k par p il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $k = pq + r$ et $0 \leq r \leq p - 1$, mais alors $x = g^k = g^{pq} g^r = (g^p)^q g^r = g^r$ car $g^p = e$. Donc $x = g^r \in \{e, g, \ldots, g^{p-1}\}$ car $0 \leq r \leq p - 1$.

12. On a $|H| = p$ car les éléments $e, g, \ldots, g^{p-1}$ sont deux à deux distincts ; en effet, si $g^r = g^{r'}$ avec $r \neq r'$ sont des éléments de $\{0, 1, \ldots, p-1\}$. Sans perte de généralité on peut supposer que $r < r'$. Dans ce cas $g^{r'-r} = e$ mais par un encadrement simple on a $0 < r' - r < p$, ce qui contredit la minimalité de p. On en déduit que $p = |H|$.
D'après le résultat de la question 8, $p = |H|$ divise $|G| = n$.

13. D'après le résultat de la question précédente, il existe $d \in \mathbb{N}$ tel que $n = pd$, donc

$$g^n = g^{pd} = (g^p)^d = e^d = e$$

D'où le résultat.

www.algebre.aqalmoun.com
Mohamed Aqalmoun