

Examen corrigé AR4 -Première session- 26 Mai 2009

Question de cours sur 2

Redémontrez le résultat de cours suivant : si G est un groupe opérant sur un ensemble X , la relation binaire sur X "être dans une même orbite" (pour $x, y \in X$, $x\mathcal{R}y$ si $\exists g \in G$, tel que $x = gy$) est une relation d'équivalence sur X .

Réflexivité : soit $x \in X$, on note e le neutre du groupe G . D'après les axiomes d'une action, on a $x = ex$ donc $x\mathcal{R}x$.

Symétrie : soient x, y tels que $x\mathcal{R}y$, donc il existe $g \in G$ tel que $x = gy$. Donc $g^{-1}x = g^{-1}(gy) = ey = y$, donc $y\mathcal{R}x$.

Transitivité : soient x, y, z tels que $x\mathcal{R}y$ et $y\mathcal{R}z$, donc il existe g_1 et g_2 tels que $x = g_1y$ et $y = g_2z$. Donc $x = g_1(g_2z) = (g_1g_2)z$. Donc $x\mathcal{R}z$.

Exercice 1. sur 5

On note G le groupe multiplicatif $(\mathbb{Z}/100\mathbb{Z})^*$.

1. Calculez le cardinal du groupe G .

Son cardinal est donné par la fonction indicatrice d'Euler :

$$\varphi(100) = \varphi(2^2 * 5^2) = (2 - 1) * 2^{2-1} * (5 - 1) * 5^{2-1} = 40.$$

2. Calculez l'ordre de $\overline{41}$ dans G .

On calcule les puissances successives jusqu'à tomber sur 1 ; il n'est pas nécessaire de le faire pour les exposants qui ne divisent pas $\phi(100) = 40$.

$$\overline{41}^2 = \overline{81} \neq \overline{1}, \overline{41}^4 = \overline{61} \neq \overline{1}, \overline{41}^5 = \overline{1}.$$

donc l'ordre est 5.

3. Quel est l'inverse de $\overline{41}$ dans G ?

L'inverse est $\overline{41}^{-1} = \overline{41}^{(5-1)} = \overline{61}$.

4. Montrez que l'application $\mathbb{Z}/100\mathbb{Z} \rightarrow \mathbb{Z}/100\mathbb{Z}$, $x \mapsto 41x$, est un automorphisme de $\mathbb{Z}/100\mathbb{Z}$.

Notons f cette application. Soit $g : x \mapsto 61x$. On a pour tout $x \in \mathbb{Z}/100\mathbb{Z}$, $f \circ g(x) = x = g \circ f(x)$. Donc f est une bijection. De plus, $f(x + y) = 41(x + y) = 41x + 41y = f(x) + f(y)$, et donc f est un morphisme bijectif de $\mathbb{Z}/100\mathbb{Z}$ dans lui-même, donc un automorphisme.

Exercice 2. sur 5

Soient

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 8 & 9 & 7 & 5 & 4 & 2 & 3 & 1 \end{pmatrix}.$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 4 & 6 & 2 & 3 & 7 & 8 & 9 \end{pmatrix}.$$

Soit G le sous-groupe de $\mathcal{S}_9$ engendré par τ et σ .

1. Donnez la décomposition en produit de cycles à supports disjoint de τ et σ .

$$\tau = (1, 6, 4, 7, 2, 8, 3, 9), \sigma = (1, 5, 2)(3, 4, 6)$$

2. Donnez les ordres et les signatures de τ et σ .

L'ordre d'une permutation est le ppcm de la longueur des cycles le composant. Donc τ est d'ordre 8, σ d'ordre 3. Pour la signature, on calcule $\epsilon(\tau) = -1$ et $\epsilon(\sigma) = 1$.

3. Montrez que le cardinal de G est divisible par 24.

$\tau \in G$ est d'ordre 8 donc 8 divise le cardinal de G . De même σ est d'ordre 3 donc 3 divise le cardinal de G , donc ce cardinal est divisible par 3 et 8, donc par leur ppcm(3,8)=24.

4. Montrez que l'action de G sur l'ensemble $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ est transitive.

il suffit de montrer que l'orbite de 1 est tout. Par les itérés de τ , on peut envoyer 1 sur n'importe quel nombre différent de 5 ; $\sigma(1) = 5$ et donc l'orbite de 1 sous G est bien tout l'ensemble $\{1, 2, \dots, 9\}$.

5. En déduire que le cardinal de G est divisible par 72.

Le cardinal d'une orbite divise le cardinal du groupe, donc par la question 4, 9 divise le cardinal de G ; or il est divisible par 24 (question 3), donc par le ppcm(24,9)=72.

Exercice 3. sur 3

Etant donnés deux nombres complexes $a, b \in \mathbb{C}$, on pose

$$M_{a,b} = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$$

1. Montrez que $M_{a,b} \in GL(2, \mathbb{C})$ si et seulement si $(a, b) \neq (0, 0)$.

Une matrice est inversible ssi son déterminant n'est pas nul. On calcule $\det(M_{a,b}) = |a|^2 + |b|^2$, cette somme de modules au carré est nulle ssi $a = b = 0$.

Soit G l'ensemble des matrices $M_{a,b}$, pour $(a, b) \neq (0, 0)$.

2. Montrez que G est un sous-groupe du groupe linéaire $GL(n, \mathbb{C})$.

Ici erreur de typo dans l'énoncé : il fallait lire $GL(2, \mathbb{C})$ et non pas $GL(n, \mathbb{C})$; il s'agit bien ici de matrices 2×2 . G n'est pas vide car il contient $I_2 = M_{1,0}$. Si $M_{a,b}, M_{c,d}$ sont dans G , on vérifie (il faut l'écrire en faisant le produit des matrices en question !!) que

$$M_{a,b}M_{c,d} = M_{ac-b\bar{d}, ad+b\bar{c}}.$$

matrice qui est inversible (produit de deux matrices inversibles) et donc encore dans G . D'autre part, si $M_{a,b} \in G$,

$$M_{a,b}^{-1} = \frac{1}{\det(M_{a,b})} {}^t(\text{com} M_{a,b}) = M_{\frac{\bar{a}}{|a|^2+|b|^2}, \frac{-b}{|a|^2+|b|^2}} \in G.$$

L'ensemble G est donc non vide, stable par produit et par inversion : c'est un sous-groupe de $GL(2, \mathbb{C})$.

Exercice 4. sur 5

Soit G un groupe à 18 éléments. On considère X l'ensemble des sous-parties de G à 9 éléments. On fait agir G par translation à gauche sur X , càd

$$g \cdot \{x_1, \dots, x_9\} = \{gx_1, \dots, gx_9\}.$$

1. Montrez que $|X|$ n'est pas divisible par 3.

Le nombre de parties à p éléments dans un ensemble à n éléments est le coefficient binomial $\binom{n}{p} = \frac{n!}{p!(n-p)!}$. Ici on a donc

$$|X| = \binom{18}{9} = \frac{18 * 17 * 16 * 15 * 14 * 13 * 12 * 11 * 10}{9 * 8 * 7 * 6 * 5 * 4 * 3 * 2} = 17 * 13 * 11 * 5 * 2^2,$$

(après simplifications), qui n'est pas divisible par 3, car pas de 3 dans sa décomposition en facteur premier. On peut aussi calculer ce produit à la main, $|X| = 48620$, mais ça n'était pas demandé.

2. En déduire que soit il existe un point fixe, soit il existe une orbite de cardinal 2 (possibilités non exclusives).

Le cardinal d'une orbite divisant le cardinal du groupe, ici 18, les orbites ont leur cardinals dans la liste suivante : 1, 2, 3, 6, 9, 18. Raisonnons par l'absurde, supposons qu'il n'y ait aucune orbite de cardinal 1 ou 2. D'après l'équation aux classes, le cardinal de X est la somme des cardinaux des orbites; or ceux-ci sont 3, 6, 9 ou 18 par hypothèse, donc divisibles par 3; ainsi $|X|$ est somme de nombres divisibles par 3, donc divisible par 3, ce qui contredit 1).

3. Montrez qu'il n'y a pas de point fixe pour cette action (on pourra par exemple montrer que si $x \in X$ est point fixe, il contiendrait plus de dix éléments et obtenir une contradiction).

Soit $x = \{x_1, \dots, x_9\}$ un éventuel point fixe pour cette action. Soit $g \in G$ quelconque, par hypothèse $gx = x$, c'est à dire $\{gx_1, \dots, gx_9\} = \{x_1, \dots, x_9\}$, en particulier $gx_1 \in \{x_1, \dots, x_9\} = x$. Or la translation à droite par x_1 est une bijection de G dans G , mais on vient de voir que son image est incluse dans x , qui est de cardinal 9. Absurde.

4. En conclure que G admet (au moins) un sous-groupe de cardinal 9, et que ce dernier est distingué.

D'après les questions 2 et 3, il existe une orbite $\mathcal{O}(x)$ de cardinal 2. Soit H son stabilisateur, on sait que $|\mathcal{O}(x)| \cdot |H| = |G|$, et donc H est de cardinal 9. Il reste à montrer que H est distingué : en effet, on a vu en cours qu'un sous-groupe d'indice 2 est toujours distingué; une autre façon de le montrer et de voir que G agit sur l'orbite $\mathcal{O}(x)$ (car c'est un sous-ensemble stable), et que cette action définit ainsi un morphisme de G dans le groupe symétrique de $\mathcal{O}(x)$. Comme c'est un ensemble à seulement 2 éléments, le stabilisateur de x est également le noyau du morphisme; un noyau est toujours distingué, d'où le résultat.