Faculté des Sciences
Aix-Marseille Université

Licence de mathématiques, $3^{\text{ième}}$ année

☐ Aix-Montperrin
☐ Luminy
☒ Saint-Charles
☐ Saint-Jérôme
☐ Château-Gombert

Examen Structures Algébriques

9 mai 2017

Trois heures, ni calculatrices, ni documents Enseignants: H. Short, P. Mercat, K. Oeljeklaus

I. (Cours) barème 8 =1 + 1 + 1+(0.5+1)+ (1+0.5)+ 1 + 1

(1) Soit G un groupe, soit H un sous-groupe distingué de G et soit D un sous-groupe distingué de H. D est-il un sous-groupe distingué dans G ? Justifier la réponse.

(2) Rappeler ce qu'est une action fidèle d'un groupe sur un ensemble.

(3) Soit G un groupe agissant fidèlement sur un ensemble à n éléments. Montrer que G est de cardinal au plus $n!$.

(4) Rappeler ce qu'est un p-groupe. Que peut-on dire du centre d'un p-groupe ?

(5) Soit A, B des anneaux commutatifs, $f : A \to B$ un homomorphisme d'anneaux. Montrer que le noyau $\mathrm{Ker} f$ est un idéal de A. Si I est un idéal de A, montrer que le quotient A/I est un anneau commutatif.

(6) Soit A un anneau commutatif unitaire (c'est-à-dire contenant 1), dont les seuls idéaux sont $\{0\}$ et A. Montrer que A est un corps.

(7) Soit k un corps et $P(X) \in k[X]$ un polynôme. Montrer que le quotient $k[X]/\langle P(X)\rangle$ est sans diviseur de zéro si et seulement si $P(X)$ est irréductible (*il peut être utile de citer un théorème pour un des cas.*)

II. barème 6= 2 + (0.5 + 0.5) + (1+2)

a) Montrer qu'un groupe d'ordre 225 n'est pas simple.

b) Soit $\sigma \in S_{14}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 10 & 5 & 7 & 11 & 9 & 2 & 1 & 12 & 6 & 13 & 3 & 14 & 4 & 8 \end{pmatrix}.$$

Décomposer σ en produit de cycles disjoints. Calculer σ^{1789}.

c) Quel est le nombre d'éléments d'ordre 3 de S_6? Quel est le nombre de 3-sous-groupes de Sylow de S_6? Justifier vos réponses.

III. Groupe du Rubik's carré **barème 8= 1 + (1+0.5) + 1 +(0.5+1)+ 2+1**

On se propose d'étudier le groupe du Rubik's carré $3 \times 3 \times 1$.

3	ϵ_3	4
ϵ_2		ϵ_4
1	ϵ_1	2

Soit $G = \{-1, 1\}^4 \times S_4$ (ou S_4 est le groupe symétrique avec son opération usuelle). On muni G de la loi $*$:

$$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \sigma) * (\epsilon_1', \epsilon_2', \epsilon_3', \epsilon_4', \tau) = (\epsilon_1\epsilon_1', \epsilon_2\epsilon_2', \epsilon_3\epsilon_3', \epsilon_4\epsilon_4', \sigma\tau)$$

1. Montrer que $(G, *)$ est un groupe.

Soit

$$\varphi : \begin{array}{ccc} G & \to & \{-1, 1\} \\ (\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \sigma) & \mapsto & \epsilon_1\epsilon_2\epsilon_3\epsilon_4 \operatorname{sign}(\sigma), \end{array}$$

où $\operatorname{sign}(\sigma)$ est la signature de la permutation σ.

2. Montrer que φ est un morphisme de groupes surjectif.

Le groupe du Rubik's carré $3\times3\times1$ est le sous-groupe R du groupe G engendré par les éléments

$$b = (-1, 1, 1, 1, (1\,2)), \quad g = (1, -1, 1, 1, (1\,3)), \quad h = (1, 1, -1, 1, (3\,4)), \quad d = (1, 1, 1, -1, (2\,4)).$$

3. Montrer que R est un sous-groupe de $\operatorname{Ker}(\varphi)$.

Soit

$$\psi : \begin{array}{ccc} \operatorname{Ker}(\varphi) & \to & S_4 \\ (\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \sigma) & \mapsto & \sigma, \end{array}$$

4. Montrer que ψ est un morphisme vérifiant $\psi(R) = S_4$.

5. Montrer que les quatre éléments $b*g*b*g*b*g$, $b*d*b*d*b*d$, $g*h*g*h*g*h$, et $d*h*d*h*d*h$ engendrent le noyau de ψ.

6. En déduire l'égalité $R = \operatorname{Ker}(\varphi)$.

IV. Les entiers de Gauss **barème 7.5= (0.5+0.5)+(0.5+0.5)+(0.5 + 1)+1 + 2 + 1**

Soit $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, l'anneau des entiers de Gauss, avec les opérations induites de $\mathbb{C}$. On pose $N : \mathbb{Z}[i] \to \mathbb{Z}$, $N(a + ib) = a^2 + b^2$.

1. Monter que $N(xy) = N(x)N(y)$, $\forall x, y \in \mathbb{Z}[i]$. En déduire les éléments inversibles de $\mathbb{Z}[i]$.

2. Montrer que $x \in \mathbb{Z}[i]$ est irréductible si $N(x)$ est un entier premier. Donner un exemple pour montrer que la réciproque est fausse.

3. Soient $x, y \in \mathbb{Z}[i]$ tels que $y \neq 0$, et poser $\frac{x}{y} \in \mathbb{C}$.

a) Montrer qu'il existe $u, v \in \mathbb{Q}$ tels que $\frac{x}{y} = u + iv$ dans $\mathbb{C}$.

b) Prendre $u_0, v_0 \in \mathbb{Z}$ tels que $\max(|u - u_0|, |v - v_0|) \leq \frac{1}{2}$. Montrer qu'il existe $r \in \mathbb{Z}[i]$ tel que $x = y(u_0 + iv_0) + r$, et que $N(r) < N(y)$.

4. En déduire que $\mathbb{Z}[i]$ est un anneau principal (*on pourra regarder un élément minimisant la norme dans un idéal.*)

5. Soit p un nombre premier de $\mathbb{Z}$ avec $p > 3$.

Montrer que p est réductible dans $\mathbb{Z}[i]$ si et seulement si $\exists a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

6. En déduire que si $p \in \mathbb{Z}$ est tel que p est premier, $p > 3$, et $p = 3 \mod 4$, alors p est irréductible dans $\mathbb{Z}[i]$ (*on pourra regarder les carrés modulo 4, selon leur parité*).