CIR_2 # TD de Maths - Corps

I. Quaternions

Dans l'anneau $\mathcal{M}_4(\mathbb{R})$ des matrices 4×4 à coefficients réels, on considère les matrices suivantes :

$$I=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\quad E=\begin{pmatrix}0&-1&0&0\\1&0&0&0\\0&0&0&1\\0&0&-1&0\end{pmatrix}\quad F=\begin{pmatrix}0&0&-1&0\\0&0&0&-1\\1&0&0&0\\0&1&0&0\end{pmatrix}\quad \text{et}\quad G=\begin{pmatrix}0&0&0&1\\0&0&-1&0\\0&1&0&0\\-1&0&0&0\end{pmatrix}$$

On notera que la famille $(I,E\ F,G)$ *est libre et donc que* $(aI+bE+cF+dG=0)\Leftrightarrow(a=b=c=d=0)$

Partie I

1. Vérifier que $E.F=G$, $E^2=-I$ et $F^2=-I$
   Calculer $F.E$ et $G.E$

Dans le reste de l'exercice, on ne fera plus aucun calcul de matrice, mais on utilisera les résultats du 1.

2. Démontrer que $E.G=-F$. Calculer de la même façon $F.G$, $G.F$ et G^2
3. Soit $H=\{I,E,F,G,-I,-E,-F,-G\}$. En utilisant 1. et 2. compléter la table de multiplication :
   (d'abord les produits de *I, E, F, G* puis compléter en tenant compte des signes)

↗	I	E	F	G	$-I$	$-E$	$-F$	$-G$
I								
E								
F								
G								
$-I$								
$-E$								
$-F$								
$-G$								

4. Démonter que *H* est un groupe pour la multiplication (un sous-groupe du groupe des matrices inversibles).
5. Déterminer le sous-groupe de *H* engendré par *E.*
6. Combien H a-t-il de sous-groupes d'ordre 4 ? d'ordre 2 ? Combien de sous-groupes en tout ?

Partie II

1. Calculer $(E+F)^2$, $(I+E)^2$, $(I+E)^3$.
2. Soit $K=\{aI+bE+cF+dG\ /\ (a,b,c,d)\in\mathbb{R}^4\}$:
   C'est l'ensemble des combinaisons linéaires des matrices I,E,F et G.
   Montrer que $(K,+,\times)$ est un sous-anneau de l'anneau $(\mathcal{M}_4(\mathbb{R}),+,\times)$.
3. Soit $Q=aI+bE+cF+dG$ un élément de *K*. On notera $Q^*=aI-bE-cF-dG$.
   Soit $V=bE+cF+dG$.
   Calculer V^2 puis $Q.Q^*=(aI+V)(aI-V)$.
   En déduire que si $Q\neq 0$, alors $Q.Q^*\neq 0$ et Q est inversible. Noter que son inverse est élément de *K*.
   $(K,+,\times)$ **est un corps non commutatif.**
4. Combien y a-t-il d'éléments Q de K tels que $Q^2=-I$? L'équation $X^2+1=0$ a donc plus que 2 racines ! ! !

II. Un corps à 4 éléments

Trouver un corps à 4 éléments.

III. Le groupe multiplicatif d'un corps fini. (On admet que tout corps fini est commutatif)

Soit $(\mathbb{K},+,\times)$ un corps à *q* éléments. Soit $G=\mathbb{K}-\{0\}$ le groupe multiplicatif de $\mathbb{K}$.
Pour tout naturel *d* non nul, on définit :

$E_d=\{x\in G / x^d=1\}$ (c'est l'ensemble des racines dans $\mathbb{K}$ du polynôme X^d-1)

et $F_d=\{x\in G \ / \ x \text{ est d'ordre } d\}$

1. Soit *d* tel que $F_d\neq\varnothing$ et $\alpha\in F_d$. On rappelle la notation $\langle\alpha\rangle=\{1,\alpha,\alpha^2,\cdots,\alpha^{d-1}\}$.
   a. Montrer que tout élément de $\langle\alpha\rangle$ appartient à E_d.
   En déduire, en étudiant les cardinaux des 2 ensembles, que $E_d=\langle\alpha\rangle$.
   b. Soient $i\in\{0,1,...,d-1\}$ et $\beta=\alpha^i$.
   Montrer que β est d'ordre *i* si et seulement si *i* est premier avec *d*.
   En déduire que le cardinal de F_d est égal à $\varphi(d)$ (indicatrice d'Euler).
2. Un exemple : Soit $(\mathbb{K},+,\times)$ un corps à 64 éléments. Soit $G=\mathbb{K}-\{0\}$ le groupe multiplicatif de $\mathbb{K}$.
   a. Soit α un élément de *G*. Quel peut être son ordre ?
   b. Pour chacune des valeurs *d* trouvées au a. , calculer $\varphi(d)$. Noter (cf 1.) que $Card(F_d)=0$ ou $\varphi(d)$
   En déduire le cardinal de chacun des F_d. Noter que *G* est cyclique.
   c. Soient α un élément d'ordre 9 et β un élément d'ordre 7.
   Montrer que $\alpha\beta$ ne peut être ni d'ordre 9 ni d'ordre 7 ni d'ordre 21. Conclusion ?
   Pour $i,i'\in\{0,1,...,8\}$ et $j,j'\in\{0,1,...,6\}$,
   à quelle condition a-t-on $\alpha^i\beta^j=1$? à quelle condition a-t-on $\alpha^i\beta^j=\alpha^{i'}\beta^{j'}$?

3. Retour au cas général
   a. Montrer que, si $F_d\neq\varnothing$, alors *d* divise $q-1$
   Montrer que l'ensemble des F_d, où *d* est un diviseur de $q-1$, est une partition de *G*.
   En déduire que $q-1=\sum_{d|q-1}\varphi(d)$ (la somme s'étend à tous les diviseurs de $q-1$)
   b. En déduire avec le 1. que, pour tout diviseur *d* de $q-1$, le cardinal de F_d est égal à $\varphi(d)$.

On a montré que le groupe multiplicatif de tout corps (commutatif) fini d'ordre *q* est cyclique et qu'il a exactement $\varphi(q-1)$ générateurs.

Evariste Galois (1811-1832)

Credit image: Bettmann Archive/Bettmann