Les problèmes de l'A.P.M.E.P.

Cette rubrique propose des problèmes choisis pour l'originalité de leur caractère : esthétique, subtil, ingénieux, voire récréatif, dont la solution nécessite initiatives, démarche inventive, recherche, effort intellectuel.

Elle accueille tous ceux qui aiment inventer, chercher de "beaux problèmes"...si possible trouver des solutions, et les invite à donner libre cours à leur imagination créatrice.

Priorité est naturellement réservée aux énoncés composés par des collègues et au dialogue ouvert entre eux par le jeu des réponses et des solutions. Les auteurs sont priés de joindre les solutions aux propositions d'énoncés. Enoncés, réponses et solutions sont à envoyer à l'adresse suivante (réponse à des problèmes différents sur feuilles séparées S.V.P., sans oublier votre nom sur chaque feuille) :

François LO JACOMO
21 rue Juliette Dodu,
75010 PARIS.

ÉNONCÉS

ÉNONCÉ N°234 (Jacques BOUTELOUP, Rouen)

On considère trois cercles (C_1), (C_2) et (C_3) de centres respectifs A, B et C, deux à deux extérieurs.

On désigne par (T_1), (T_2), (T_3) trois tangentes communes respectivement à (C_2, C_3), (C_3, C_1), (C_1, C_2) et l'on suppose que ces trois tangentes concourent en un point O.

On considère les tangentes communes (T'_1), (T'_2), (T'_3) respectivement symétriques de (T_1), (T_2), (T_3) par rapport à (BC), (CA), (AB).

Démontrer que les tangentes (T'_1), (T'_2), (T'_3) sont concourantes si et seulement si parmi les trois tangentes (T_1), (T_2), (T_3) 0 ou 2 sont des tangentes extérieures.

ÉNONCÉ N°235 (Marie-Laure CHAILLOUT, Sarcelles)

a, b, c étant trois réels, avec : $a > 0$, $c \neq 0$, montrer que toute application continue de $\mathbf{R} \to \mathbf{R}$ vérifiant :

$$\forall x \in \mathbf{R}, f \circ f(x) + cf(x) = ax + b$$

est affine.

ÉNONCÉ N°236 (Philippe JACQUEMIER, Revel)

Sur les côtés d'un triangle ABC, on construit trois triangles isocèles et semblables : ABC', BCA', CAB' ($AC' = BC'$, $BA' = CA'$, $CB' = AB'$; $\widehat{AC'B} = \widehat{BA'C} = \widehat{CB'A}$). Montrer que (AA'), (BB') et (CC') sont concourantes en K. Quel est le lieu de K lorsque C', A', B' se déplacent sur les médiatrices de $[AB]$, $[BC]$, $[CA]$ respectivement ?

SOLUTIONS

ÉNONCÉ N° 218 (Gérard LAVAU, Mesnil-Esnard)

Sous quelles conditions peut-on affirmer que : «Deux groupes finis G et G' sont isomorphes si et seulement si les ordres des éléments de G et G' sont les mêmes» ?

RÉPONSE

En dehors de la solution de M. Chamaraux, transmise par l'auteur, dans le cas très particulier où G et G' sont commutatifs, et d'une solution fausse, je n'ai reçu aucune réaction à cet énoncé. De fait, dans le cas général, deux groupes finis sont-ils isomorphes si les ordres de leurs éléments sont les mêmes ? Peut-être bien que oui, peut-être bien que non ! Je n'ai reçu ni démonstration, ni contre- exemple... et quand bien même ce résultat serait faux, rien ne prouve qu'on puisse trouver un contre-exemple «accessible» (qui n'ait pas des milliards d'éléments)! N'étant aucunement spécialiste des groupes finis, je redoute fort de dire des âneries à ce sujet... mais puisque j'ai proposé l'énoncé, il faut bien que je me mouille.

Dans un sens, le résultat est évident: deux groupes ne sont isomorphes que si les ordres de leurs éléments sont les mêmes. Dans l'autre sens, l'énoncé semble poser deux questions distinctes :

1 - Peut-on prouver que deux groupes sont isomorphes autrement qu'en exhibant un isomorphisme effectif ?

2 - Quelle information pertinente la connaissance de l'ordre des éléments d'un groupe apporte-t-elle quant à la structure du groupe ?

Dans le cas de groupes commutatifs, pas de problème : tout groupe fini commutatif G est un produit de groupes cycliques $C_n = \mathbf{Z}/n\mathbf{Z}$. En effet, soit a un élément quelconque de G (autre que 1), d'ordre $n > 1$ ($a^n = 1$) ; a engendre un sous-groupe cyclique $H = \{1, a, a^2 \dots a^{n-1}\}$ de G, d'ordre n, et l'ensemble G/H des classes d'équivalence pour la relation : $u \sim v \Leftrightarrow u^{-1}v \in H$ a lui-même une structure de groupe commutatif fini d'ordre n fois plus petit que l'ordre de G, et l'on peut trouver un H (mais encore faut-il le prouver) tel que G soit isomorphe à G/H × H, ce qui permet de réitérer le procédé pour aboutir au résultat annoncé. Comme, par ailleurs, si n et m sont premiers entre eux, C_{nm} est isomorphe à $C_n \times C_m$, tout groupe commutatif fini G se décompose en produit de p-groupes cycliques, c'est-à-dire de groupes cycliques dont l'ordre est une puissance d'un nombre premier p, et il suffit de prouver que deux produits distincts ne sont pas isomorphes pour montrer que cette décomposition est unique et caractérise le groupe G, à l'ordre des facteurs près, bien évidemment.

Mais dans le cas d'un groupe non commutatif, d'une part l'ensemble des classes d'équivalence n'a une structure de groupe que si le sous-groupe H est distingué, donc si $\forall u \in G$, $\forall h \in H$, $u^{-1} hu \in H$, ce qui est rarement le cas du groupe cyclique engendré par un élément a ; mais en outre, il se peut qu'il n'existe aucun sous-groupe distingué H tel que G soit isomorphe à G/H × H : si deux groupes G et G' admettent des sous-groupes distingués H et H' isomorphes, avec en outre G/H isomorphe à G'/H', cela ne signifie nuellement que G est isomorphe à G'.

Maintenant, si je rajoute l'hypothèse que les ordres des éléments de G et G' sont les mêmes, peut-on alors, au moins dans le cas où G/H est isomorphe à un groupe particulier (par exemple, dans le cas où G/H n'a que deux éléments), prouver que G et G' sont isomorphes ? Même dans ce cas, a priori simple, je n'ai pas la réponse.

Revenons au cas des groupes commutatifs, pour citer la démonstration de M.CHAMARAUX, transmise par Gérard LAVAU :

G fini commutatif est isomorphe à $\prod G_p$ où p décrit un ensemble fini de nombres premiers, les G_p étant de la forme :

$$G_p = (\mathbf{Z}/p\mathbf{Z})^{n_1} \times (\mathbf{Z}/p^2\mathbf{Z})^{n_2} \times \dots \times (\mathbf{Z}/p^k\mathbf{Z})^{n_k}$$

La décomposition précédente est unique.

Posons $X_G(q)$ le nombre d'éléments de G d'ordre q. On peut remarquer que $X_G(p^i) = X_{G_p}(p^i)$, et que pour tout m entier, le nombre de solutions

dans G de l'équation $p^m x = 1$ est égal à : $\sum_{i=0}^{m} X_G(p^i)$.

Or, pour tout r, le nombre de solutions dans $\mathbf{Z}/p^r\mathbf{Z}$ de l'équation en question est égal à p^r si $r \leq m$ et à p^m si $r \geq m$. Le nombre de solutions dans G_p (et dans G) est donc égal à : $p^{n_1 \text{Min}(m,1) + n_2 \text{Min}(m,2) + \ldots + n_k \text{Min}(m,k)}$

On fait varier m de 1 à k (où k est la puissance maximale de p pour laquelle il existe des éléments d'ordre p^k) et l'on obtient un système de k équations à k inconnues :

$$n_1 \text{Min}(m,1) + n_2 \text{Min}(m,2) + \ldots + n_k \text{Min}(m,k) = \log_p \left[\sum_{i=0}^{m} X_G(p^i) \right]$$

permettant de trouver les n_i. (On peut en effet vérifier que le système obtenu est de Cramer).

Exemple : on donne

$X_G(1) = 1$

$X_G(2) = 3$ (soit 3 éléments d'ordre 2)

$X_G(3) = 8$ (soit 8 éléments d'ordre 3)

$X_G(6) = 24$ (etc.)

$X_G(9) = 18$

$X_G(18) = 54$

Pour $p = 2$, $m = 1 = k$ on obtient une équation. Elle donne : $n_1 = \log_2(4) = 2$

Pour $p = 3$, $1 \leq m \leq 2 = k$, on obtient

$n_1 + n_2 = \log_3(9) = 2$

$n_1 + 2n_2 = \log_3(27) = 3$

d'où $n_1 = 1 = n_2$.

Le groupe cherché est $(\mathbf{Z}/2\mathbf{Z})^2 \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}$. (Les valeurs $X_G(6)$ et $X_G(18)$ ne sont d'aucune utilité).

Notons qu'il est généralement possible de prouver qu'un groupe G est non commutatif à partir de l'ordre de ses éléments : un groupe ayant 24 éléments dont 6 d'ordre 4, 8 d'ordre 3 et 9 d'ordre 2, plus l'élément neutre 1 (d'ordre 1), est obligatoirement non commutatif, car dans un groupe commutatif, le produit d'un élément d'ordre 3 par un élément d'ordre 2 est obligatoirement un élément d'ordre 6.

Mais est-ce toujours possible ? Est-il possible, à partir de l'ordre de ses éléments de prouver qu'un groupe G est commutatif ?

Un groupe de 24 éléments dont 6 d'ordre 4, 8 d'ordre 3 et 9 d'ordre 2, cela peut être le groupe symétrique S_4 des permutations de $\{a, b, c, d\}$: 6 permutations circulaires σ caractérisées par $\sigma(a)$ (3 possibilités) et $\sigma^2(a)$ (2 possibilités), car $\sigma^3(a)$ s'en déduit ; et 8 permutations d'ordre 3 : si l'on détermine l'élément invariant (4 possibilités), il suffit de choisir dans quel sens on fait tourner les trois autres (2 possibilités). Les 9 éléments d'ordre 2 sont d'une part les $C_4^2 = 6$ transpositions, d'autre part les 3 permutations : $(a,b)\,(c,d)$; $(a,c)\,(b,d)$ et $(a,d)\,(b,c)$ qui, avec l'élément neutre, constituent le groupe de Klein $(\mathbf{Z}/2\mathbf{Z})^2$.

Mais cela peut être également le groupe des rotations laissant fixes un cube : autour des 3 axes de symétrie passant par les centres des faces, j'ai 6 rotations de $\pm\pi/2$ (d'ordre 4) et 3 de $\pm\pi$ (d'ordre 2) ; autour des 6 axes passant par les milieux des arêtes, j'ai 6 rotation de π (d'ordre 2) ; enfin, autour des 4 axes joignant deux sommets opposés, j'ai 8 rotations d'ordre 3. Effectivement, ce groupe est isomorphe au groupe symétrique S_4, et pour le prouver, on peut remarquer que dans un cube sont inscrits deux tétraèdres ABCD et son symétrique A'B'C'D' (cf. figure 1) ; certaines rotations du cube transforment l'un des tétraèdres en l'autre, mais je peux quand même leur associer une isométrie du tétraèdre, en les composant avec la symétrie par rapport au centre du cube. de sorte qu'à toute rotation du cube on peut associer une isométrie du tétraèdre, donc une permutation de ses quatre sommets A, B, C, D : comme la symétrie par rapport au centre du cube commute avec n'importe quelle rotation, cette application est un morphisme, et il suffit de prouver qu'elle est bijective pour démontrer que le groupe des rotations du cube est isomorphe à S_4. Mais ce dernier résultat peut-il être atteint autrement ?

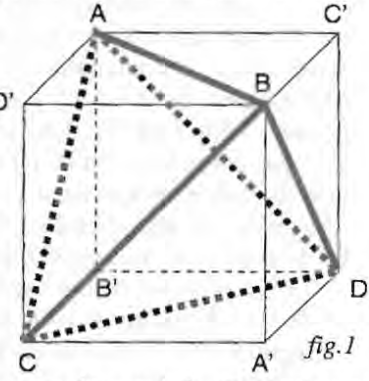

fig.1

Autre exemple : le groupe des rotations de l'icosaèdre possède 60 éléments. Les 20 faces triangulaires et les 10 axes qui relient leurs centres définissent 20 rotations d'ordre 3 ; les 30 arêtes et les 15 axes qui relient leurs milieux définissent 15 rotations d'ordre 2 ; les 12 sommets et les 6 axes qui les relients définissent 24 rotations d'ordre 5 plus, évidemment, l'identité.

Or le groupe alterné A_5 des permutations paires de 5 éléments contient lui aussi 60 éléments dont 24 d'ordre 5 (4 possibilités pour $\sigma(a)$, 3 pour $\sigma^2(a)(a)$ et 2 pour $\sigma^3(a)$), $2 \times C_5^3 = 20$ d'ordre 3 et 15 d'ordre 2 (5 possibilités pour fixer l'élément invariant et 3 pour permuter les quatre autres).

De fait, ce groupe alterné A_5 est isomorphe au groupe des rotations de l'icosaèdre : on peut le démontrer en prouvant qu'il existe 5 manières d'inscrire un icosaèdre dans un cube, chacune des 30 arêtes de l'icosaèdre appartenant à une face d'un et un seul des cinq cubes. Les rotations autour de l'axe BCE, par exemple (cf. fig.2) permutent les cubes contenant [BC], [CE] et [EB] en laissant fixes les deux autres, la rotation autour de l'axe médiateur de [AB] laisse fixe le cube contenant [AB] et transforme celui contenant [AC] en celui contenant [BC] et [A'E], donc [AE'], et celui] conte]nant [AF' en celui contenant [BE] et [A'D], donc [AD']. Enfin une rotation autour de l'axe (AA'), par exemple, permute les cinq cubes, d'où l'isomorphisme... mais peut-on le démontrer autrement ?

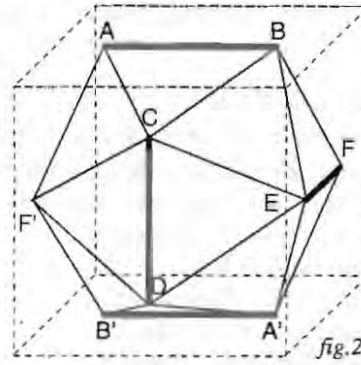

fig.2

Au vu de ces deux exemples, il semble que ce soit là la principale difficulté de notre problème, car si chaque fois qu'on veut prouver l'isomorphisme de deux groupes il faut recourir à une telle construction, on voit mal comment aborder le cas général. Or, les quelques textes que j'ai parcourus, sur les groupes finis, à l'occasion de ce problème ne m'ont pas permis de savoir si cette question *«comment prouver que deux groupes sont isomorphes»* avait été étudiée sous cette forme.

Mais il convient d'ajouter que la seconde question :*«quelle information pertinente la connaissance de l'ordre des éléments d'un groupe apporte-t-elle quant à la structure du groupe ?»* est tout à fait intéressante. Elle permet par exemple de prouver que le groupe A_5 ci-dessus, des permutations paires de cinq éléments, est non résoluble, ou plus précisément qu'il ne possède pas de sous-groupe distingué H tel que G/H soit cyclique, ce qui constitue l'élément décisif de la démonstration qu'une équation du cinquième degré n'est pas résoluble par radicaux.

En effet, soit H un sous-groupe distingué d'un groupe G. A tout élément $u \in G$, je peux associer sa classe $\dot{u} \in G/H$, par le morphisme de $G \to G/H$.

L'image par ce morphisme de u^k sera $\dot{u}^k$, si bien que : $u^k = 1 \Rightarrow \dot{u}^k = 1$. En d'autres termes, l'ordre de $\dot{u}$ divise l'ordre de u, ce qui peut se traduire de deux manières, compte tenu que chaque classe de G/H contient le même nombre d'éléments de G :

1 - si n divise l'ordre de $\dot{u}$, n divise l'ordre de u ; en d'autres termes, la proportion $Y_n(G)$ d'éléments de G dont l'ordre est divisible par n est $\geq Y_n(G/H)$.

2 - Si l'ordre de u divise n, l'ordre de $\dot{u}$ divise n, donc la proportion $Z_n(G)$ d'éléments de G dont l'ordre divise n est $\leq Z_n(G/H)$. Dans le cas particulier où $G = H_1 \times H_2$, l'ordre de $u = (u_1, u_2)$ est le PPCM (ordre de u_1, ordre de u_2), si bien que : (ordre de u divise n) $\Leftrightarrow$ (ordre de u_1 divise n) **et** (ordre de u_2 divise n). Donc $Z_n(G) = Z_n(H_1) . Z_n(H_2)$ pour tout n.

Dans le cas du groupe alterné A_4, on a $Y_2(A_4) = 1/4$ et $Y_3(A_4) = 2/3$, car sur 12 éléments, 3 sont d'ordre 2 et 8 d'ordre 3 ; $\forall n \geq 4$, $Y_n(A_4) = 0$. Ce groupe peut admettre un sous-groupe distingué H tel que le groupe quotient soit le groupe cyclique C_3, car $Y_2(A_4) \geq Y_2(C_3) = 0$, $Y_3(A_4) \geq Y_3(C_3) = 2/3$ et $\forall n \geq 4$, $Y_n(A_4) \geq Y_n(C_3) = 0$.

Mais dans le cas du groupe alterné A_5, qui vérifie : $Y_2(A_5) = 1/4$, $Y_3(A_5) = 1/3$ et $Y_5(A_5) = 2/5$, et pour tout n autre que 0, 1, 2, 3 ou 5, $Y_n(A_5) = 0$, ceci ne serait éventuellement possible que s'il existait un cyclique C_m vérifiant : $Y_2(C_m) \leq 1/4$, $Y_3(C_m) \leq 1/3$ et $Y_5(C_m) \leq 2/5$, avec $Y_n(C_m) = 0$ pour tout autre $n \in \mathbf{N}$ (autre que 0 ou 1). Or, si m est multiple de 2, $Y_2(C_m) \geq 1/2$; si m est multiple de 3, $Y_3(C_m) \geq 2/3$ et si m est multiple de 5, $Y_5(C_m) \geq 4/5$. Si m n'est multiple d'aucun de ces trois entiers, il est multiple d'un autre nombre premier p pour lequel $Y_p(C_m) \geq (p-1)/p$. D'où l'impossibilité.

Peut-on généraliser cette méthode aux autres groupes alternés A_q pour $q > 5$? Il suffirait de prouver que pour chacun d'eux, et pour tout nombre premier p, il existe au moins une proportion $1/p$ d'éléments, outre l'élément neutre, dont l'ordre n'est pas multiple de p : c'est vraisemblable, mais je n'ai pas la démonstration. Par ailleurs, peut-on par ce biais attaquer des problèmes plus compliqués ? C'est possible...

J'ignore jusqu'à quel point ce genre de technique a déjà été exploité et est encore exploitable, et j'en appelle aux spécialistes des groupes finis...