Lycée Bascan de Rambouillet
Introduction à l'exposé de Michel Broué *Des lois du mariage à Bourbaki* à la BNF,
conférences *Un texte, un mathématicien.*
15 mars 2010

Sur les structures en mathématiques

1 L'exposé en bref

Taquin (puzzle, modèle $1, \ldots, 15$, et la case vide numérotée 16, histoire américaine de Sam Loyd).
Permutations, inversions, signature, impossibilité du taquin impair.
Aspect groupe et définition groupe. Impact du groupe symétrique en combinatoire.

Topologie vue *via* les déformations continues des objets et les rétractions (objets homotopes). Exemple d'objets homotopes à la sphère ou au cylindre (au cercle). Le tore est-il homotope à la sphère ?
Lacets pointés, déformation continue des lacets, groupe fondamental. Le groupe de la sphère est trivial. Celui du tore ne l'est pas. Tores à g trous. Le genre est le seul invariant des surfaces compactes sans bord.

Corps $\mathbb{Q}[\sqrt{2}]$ ou $\mathbb{Q}[\sqrt[3]{5}]$ ou $\mathbb{Q}[\sqrt[p]{d}]$. Structure de corps. Expression conjuguée. Pythagore et construction des $\sqrt{d}$, ou des $\sqrt{c}$ lorsque c est constructible. Constructibilité des polygones réguliers. Non constructibilité de $\sqrt[3]{2}$. Un peu faux : un nombre c est constructible lorsque $\mathbb{Q}[c]$ se construit récursivement comme on construit $\mathbb{Q}[\sqrt{2}]$ à partir de $\mathbb{Q}$ ou $\mathbb{Q}[\sqrt[4]{2}]$ à partir de $\mathbb{Q}[\sqrt{2}]$ (extensions de degré deux).
Revenir au groupe de permutations des racines d'un polynôme (Galois). Exemples. Enoncé vague sur la résolution par radicaux.

$\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$, c'est tout (on perd successivement l'ordre compatible, la commutativité, l'associativité).

Géométrie des polyèdres. Description des 5, unicité. Groupes de rotations ou d'isométries (lien cristallographique, chimie minérale). Groupes du tétraèdre (permuter les sommets), du cube (permuter les quatre diagonales), de l'octaèdre (dual, permuter les médiatrices des faces), du dodécaèdre (permuter les cinq cubes circonscrits ou les cinq tétraèdres inscrits dont les sommets sont des sommets du dodécaèdre), de l'icosaèdre (dual, permuter les cinq cubes circonscrits ou les cinq tétraèdres inscrits dont les sommets sont des centres de faces de l'icosaèdre).

2 Permutations

Jeu de taquin : présentation, histoire (un peu arrangée) de Sam Loyd, de sa fortune et de son brevet (finalement retiré) du puzzle obtenu par action de la transposition (12).

Définition d'une permutation de $\{1, \ldots, n\}$. Présentation par le diagramme des images (en colonne).
Composition des permutations, associativité, inverse d'une permutation. Notation $\mathfrak{S}_n$ (groupe, déjà).
Inversions dans une permutation (croisements dans le diagramme). Nombre d'inversions. Signature.
Admis : $\varepsilon(st) = \varepsilon(s)\varepsilon(t)$ (groupe $\{\pm 1\}$, produit est préservé). Transpositions. La signature d'une transposition est -1, le voir sur le diagramme d'un exemple générique, par exemple (36) dans $\mathfrak{S}_7$.

Retour au taquin : voir la case vide comme une seizième case et une configuration intermédiaire comme une permutation de $\mathfrak{S}_{16}$. Une configuration finale est une configuration qui fixe 16. La configuration de Loyd est une transposition. On noirçit le jeu comme un damier : une solution du taquin dont la case vide est en bas à droite oblige la configuration finale à résulter d'un nombre pair de transformations élémentaires du jeu, qui sont des transpositions. Autrement dit, on n'atteint que des configurations finales dont la signature est 1 : la configuration de Loyd est impossible car elle est impaire.

Le groupe $\mathfrak{S}_n$ des permutations est un des objets centraux des mathématiques. Définition d'un groupe. Représentation des groupes abstraits comme des groupes de transformations dans des contextes variés. Par exemple, en géométrie (groupe des isométries qui stabilisent une figure). Théorie en soi. Répercussions dans de nombreux domaines des mathématiques et d'autres sciences.

La structure de groupe est une des premières structures abstraites de l'algèbre. Parler d'anneau (deux lois, $\mathbb{Z}$ par exemple mais aussi fonctions, ou l'anneau des nombres entiers modulo 6, non intègres), de corps (anneau avec inversion des éléments non nuls, par exemple $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ pour les élèves de TS).

3 Un peu de topologie

La topologie est l'étude d'objets de type géométriques (cercles, droites, couples de droites sécantes, sphères) à déformation continue près, ou parfois à rétraction près (ne pas définir mais illustrer). On imagine des objets en caoutchouc infiniment souple. Couper est interdit.
Par exemple, un cylindre et un cercle sont équivalents (on dira homotopes). Une sphère et une statue d'éléphant aussi. En revanche, un cercle et une sphère ne sont pas homotopes : tout lacet de la sphère se contracte sur un point, c'est faux sur le cercle. De même, le tore et la sphère ne sont pas homotopes car on peut trouver des lacets du tore qui ne sont pas homotopes à un point.
Question : le tore et le cercle sont-ils homotopes ? Le cercle et le huit ? Le tore à un trou et le tore à deux trous ?

On fixe un point sur la "variété" topologique et on considère les lacets issus de ce point, avec sens de parcours. On les compose en les concaténant. On dit que deux lacets sont homotopes lorsque on peut déformer continûment l'un sur l'autre. Les lacets à homotopie près forment un groupe (le groupe fondamental de la variété).
Le groupe fondamental du cercle est isomorphe à $\mathbb{Z}$ (visualiser). Celui du tore est plus compliqué (dessin) et on peut montrer qu'il n'est pas isomorphe à $\mathbb{Z}$ (mais au groupe libre à deux générateurs). Cela suffit à montrer que le tore et le cercle ne sont pas homotopes.
Par un raisonnement équivalent, le tore à deux trous n'est pas homotope au tore à un trou (groupe libre à quatre générateurs).

Ces exemples survolés illustrent comment la théorie des groupes peut s'appliquer à des domaines où le novice ne l'attend pas forcément.

4 Corps et géométrie de la Grèce antique

Expression conjuguée : $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \mathbb{Q}\sqrt{2}$ est un corps (un sous-corps de $\mathbb{R}$). Exemple sur l'inverse de $\frac{1}{3} + \frac{2}{5}\sqrt{2}$. Idem pour $\mathbb{Q}[\sqrt{d}]$ si d est un entier (pas intéressant si d est un carré).
On pousse un peu : $\mathbb{Q}[\sqrt[4]{2}] = \mathbb{Q} + \mathbb{Q}\sqrt[4]{2} + \mathbb{Q}(\sqrt[4]{2})^2 + \mathbb{Q}(\sqrt[4]{2})^3$ (définir $\sqrt[4]{2}$ pour les élèves de première) est aussi un corps. Décrire le calcul de l'inverse de $a+b\sqrt[4]{2}$ en passant par $\mathbb{Q}[\sqrt{2}][\sqrt[4]{2}]$, ou directement. Deux extension de degré deux.
On pousse encore : $\mathbb{Q}[\sqrt[3]{2}]$ est un corps. Décrire le calcul de l'inverse de $a+b\sqrt[3]{2}$ en multipliant numérateur et dénominateur par $(a+bj\sqrt[3]{2})(a+bj^2\sqrt[3]{2})$ où $j = \exp 2i\pi/3$. Les racines de X^3-2 (polynôme "minimal" qui annule $\sqrt[3]{2}$) sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$. Pour généraliser l'expression conjuguée comme méthode efficace pour inverser, on doit faire apparaître les racines de ce "polynôme minimal". Extension de degré trois.

La théorie des corps est une branche entière des mathématiques qui s'est beaucoup développée au dix-neuvième siècle (Ernst Kummer, Evariste Galois, *etc*).

Construction à la règle et au compas, seul procédé de construction géométrique admis par les géomètres de la Gèce antique. Exemple de construction de $\sqrt{2}$, $\sqrt{3}$, *etc* à l'aide du théorème de Pythagore. Construction de $\sqrt[4]{2}$, aussi.
En revanche, on ne peut pas construire $\sqrt[3]{2}$. La raison de cela est expliquée par un théorème (dix-neuvième siècle) dont voici un énoncé simplifié un peu faux : un nombre c est constructible à la règle et au compas

si, et seulement si $\mathbb{Q}[c]$ se construit récursivement comme on construit $\mathbb{Q}[\sqrt{2}]$ à partir de $\mathbb{Q}$ ou $\mathbb{Q}[\sqrt[4]{2}]$ à partir de $\mathbb{Q}$ en passant par $\mathbb{Q}[\sqrt{2}]$ (suite d'extensions de degré deux). L'extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}]$ est de degré trois : impossible de l'obtenir par une suite d'extensions de degré deux.

Construction des polygones réguliers : par un raisonnement analogue, on peut savoir quand un polygone régulier est constructible à la règle et au compas. Le pentagone l'est ($\cos 2\pi/5$ est solution d'une équation de degré deux à coefficients entiers). Le 17-gone aussi. Le 11-gone ou le 13-gone ne le sont pas.

Retour aux groupes de permutations. Question de la résolubilité des équations algébriques par radicaux. Cas des degrés 2, 3 (Cardan) et 4 (on se ramène à Cardan). Degré supérieurs : pas de formule générale pour exprimer les racines en fonction des coefficients à l'aide de radicaux. Théorème de Galois (difficile). Evocation de la raison : prenons par exemple l'équation $x^5 - 2 = 0$. Les cinq racines complexes du polynôme $X^5 - 2$ sont les $\sqrt[5]{2}\zeta^k$ où $\zeta = \exp 2i\pi/5$ et $k \in \{0, \ldots, 4\}$ (dessin). Effet de la conjugaison complexe : ne modifie pas le polynôme mais permute les racines comme le produit de deux transpositions (12)(34). Les racines du polynôme sont permutées par les transformations du plus petit corps qui les contient qui préservent la somme et le produit (les automorphismes du corps, la conjugaison complexe en est un). Le théorème de Galois est relié aux propriétés des groupes de permutations des racines par les automorphismes de corps.

5 $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$, c'est tout

Le corps des nombres complexes permet de ramener toute la géométrie du plan euclidien à du calcul sur des nombres (même si la méthode n'est pas toujours la plus simple).
Qu'en est-il des géométries dans les espaces de dimension plus grande ? Peut-on ramener la géométrie en n'importe quelle dimension à du calcul sur des nombres (dans un corps) ?
En dimension trois, possible. Corps des quaternions, $\mathbb{H}$ (comme Hamilton). On a perdu la commutativité.
Et après ? impossible en dimensions 4, 5, 6. Possible en dimension 7. Octaves de Cayley, $\mathbb{O}$. On a perdu l'associativité (et on y perd aussi tous les réflexes de calcul !).
Ensuite, plus jamais possible. Ce théorème, à y bien regarder, est un théorème de géométrie ou de topologie.

6 Les polyèdres de Platon

Tétraèdre régulier. Description. Quelles rotations le préservent ? Quelles symétries le préservent ?
Question utile par exemple en cristallographie ou en chimie minérale (agencement de molécules ou de cristaux).
Considérer les rotations d'ordre 3 ou 2 qui préservent le tétraèdre. Elles permutent les sommets. On peut montrer que les rotations qui stabilisent le tétraèdre correspondent aux permutations paires des sommets (groupes isomorphes). Si on permet les symétries et toutes les compositions de rotations et de symétries, on obtient le groupe des isométries du tétraèdre, qui correspondent à toutes les permutations des sommets. Dans le jargon, le groupe des isométries du tétraèdre est isomorphe au groupe $\mathfrak{S}_4$.

Le cube. Rotations qui préservent le cube. Exemple des rotations d'ordre 4, 3 ou 2. Elles agissent sur les quatre diagonales. On peut montrer que ce groupe de rotations est isomorphe au groupe $\mathfrak{S}_4$ (action sur les diagonales).

Y a-il d'autres polyèdres réguliers (écarter la discussion sur "régulier") ?

L'octaèdre, dual du cube. Même groupe de rotations (action sur les quatre droites joignant deux faces opposées).

Le dodécaèdre. Description. Il contient cinq tétraèdres inscrits dont les sommets sont des sommets du dodécaèdre et que le groupe des rotations permute. Avec cette action sur les tétraèdres, on montre que le groupe des rotations du dodécaèdre est isomorphe au groupe $\mathfrak{A}_5$ des permutations paires de 5 éléments.

Le dual du dodécaèdre : l'icosaèdre. Description. Même groupe de rotations. L'action se fait cette fois sur cinq tétraèdres inscrits dont les sommets sont des centres de faces de l'icosaèdre.

D'autres encore ? Non, polyèdres de Platon, résultat connu des géomètres de l'antiquité grecque.