Programme primes 2018: Le groupe A_5

Matthew Meyer et Andres Briones

17 juin 2018

Buts de cet exposé

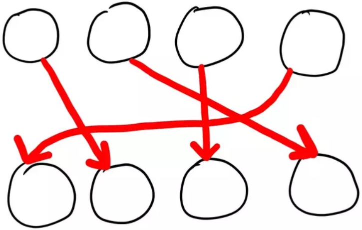
Les buts de cet exposé sont :

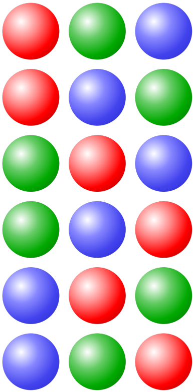
- Présenter le groupe alterné A_5 et montrer quelques-unes de ces propriétés, dont notamment le fait que A_5 est un groupe simple.
- Montrer en quoi le groupe A_5 est intéressant dans l'étude des équations polynomiales de degré 5.

Les permutations

Définition

Une permutation est une bijection d'un ensemble fini vers lui-même. Le groupe des permutations à n éléments est noté S_n.





Les transpositions

Définition

Une transposition est une permutation qui échange deux éléments et fixe tous les autres. On note $(a_1 \ a_2)$ la transposition qui échange a_1 et a_2.

Proposition

Chaque permutation peut être écrite comme produit de transpositions.

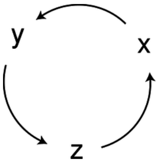
Exemples

- $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (13)(12)$
- $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (12)(13)(24)$

Les permutations cycliques

Définition

Une permutation cyclique ou *k-cycle* est une permutation qui permute k éléments de manière cyclique et fixe les autres.



Notation

Un k-cycle est noté $(a_1 \ a_2 \ \ldots \ a_k)$ où a_i est envoyé sur a_{i+1} et $a_k = a_1$.

Parité d'une permutation

Définition

La parité d'une permutation est égale à la parité du nombre de transpositions qu'il faut composer afin d'obtenir cette permutation.

Proposition

La composition de deux permutations paires est paire.

Exemples

- L'identité est une permutation paire.
- Tout 3-cycle est pair.

Le groupe A_n

Définition

$A_n \subset S_n$ est le groupe de toutes les permutations paires.

Exemples

- $A_2 = \{id\}$
- A_3 est constitué de l'identité, d'un 3-cycle, et l'inverse de ce 3-cycle.

La conjugaison

Définition

Soit G un groupe et $g, h \in G$. Le terme ghg^{-1} est le conjugué de h par g.

Définition

Deux éléments $a, a' \in G$ sont dits conjugués dans G si il existe $g \in G$ tel que $a' = gag^{-1}$.

Le sous-groupe normal

Définition

Un sous-groupe H de G est dit normal dans G si pour tout $h \in H$ et pour tout $g \in G$, le conjugué de h par g est dans H (i.e. $ghg^{-1} \in H$).

Exemples

- Tout sous-groupe d'un groupe abélien est normal.
- Le sous-groupe trivial est normal.

Les 3-cycles sont conjugués dans A_5

Proposition

Les 3-cycles sont deux-à-deux conjugués dans A_5.

Conséquence

Soit H un sous-groupe normal de A_5. Si H contient un 3-cycle, alors il contient tous les 3-cycles.

Groupe généré par un ensemble

Définition

Un groupe G est dit *généré* par un sous-ensemble S de G si tout élément de G peut s'écrire comme produit d'un nombre fini d'éléments de S et de leurs inverses.

Exemples

- Les nombres pairs sont générés par $\{2\}$.
- $\mathbb{Q}^\times$ est généré par $\mathbb{Z} \setminus \{0\}$.

A_5 est généré par les 3-cycles

Proposition

Le groupe A_5 est généré par l'ensemble des 3-cycles.

Preuve que $\langle\{abc\}\rangle \subset A_5$

Tout 3-cycle est pair donc leur produit sera une permutation paire.

A_5 est généré par les 3-cycles (suite)

Preuve que $A_5 \subset \langle \{abc\} \rangle$

- Soit une permutation paire $\sigma \neq id$ qui fixe m éléments.
- On va prouver qu'il existe un 3-cycle $\alpha \in A_5$ tel que $\sigma\alpha$ fixe $m+1$ éléments.
- Soit σ contient un k-cycle avec $k \geq 3$,
- Soit σ est le produit de 2 transpositions.

Le groupe simple

Définition

Un groupe simple est un groupe dont les seuls sous-groupes normaux sont lui-même et le groupe trivial.

Exemples

- $\mathbb{Z}/p\mathbb{Z}$ pour un premier p.

A_5 est simple

Proposition

Le groupe A_5 est simple.

Preuve

- Soit $H \neq \{1\}$ un sous-groupe normal de A_5.
- Si H contient un 3-cycle, alors $H = A_5$.
- Soit $\sigma \in H$. On a 2 autres cas.
- Dans les deux cas, on peut choisir $\tau \in A_5$ tel que $\tau\sigma\tau^{-1}\,\sigma^{-1}$ est un 3-cycle.

Groupes résolubles

Définition

Un groupe G est dit résoluble lorsqu'il existe une suite finie G_0, G_1, ... , G_k de sous-groupes normaux de G telle que :

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{k-1} \lhd G_k = G$$

où G_{i+1}/G_i est abélien pour $i = 0, 1, \ldots, k-1$.

Groupes résolubles (suite)

Quelques propriétés

- Un groupe simple est résoluble si et seulement s'il est abélien.
- Tout sous-groupe d'un groupe résoluble est résoluble.

On en déduit que S_5 n'est pas résoluble.

Corps de décomposition d'un polynôme

Définition

Soit F un corps et $f(x) \in F[x]$ un polynôme. Le plus petit corps $E \supseteq F$ tel que $f(x)$ est scindé sur E est dit le corps de décomposition de $f(x)$.

Le groupe de Galois

Définition

Le groupe de galois $\mathrm{Gal}(E/F)$ est le groupe des automorphismes de E qui fixent tous les éléments de F.

Résolubilité par radicaux

Définition

Un polynôme est dit résoluble par radicaux si l'on peut appliquer un nombre fini de fois à ses coefficients l'addition, la multiplication et l'extraction de racines n-ièmes afin d'obtenir les racines du polynôme.

Exemple : Les équations quadratiques et la formule de Viète.

Toute équation de la forme

$$ax^2 + bx + c = 0$$

est résoluble par radicaux.

Le théorème de Galois

Théorème (Galois)

Un polynôme $p(x)$ est résoluble par radicaux si et seulement son groupe de Galois est résoluble.

Conséquences

Vu que S_5 n'est pas résoluble, un polynôme ayant comme groupe de Galois S_5 n'est pas résoluble par radicaux.

Exemples

- $x^5 - 3x - 1 = 0$
- $x^5 - 4x + 2 = 0$
- $x^5 - 10x + 2 = 0$

Remerciements

Théorème

Vu que nous avons eu une superbe expérience avec PRIMES, nous remercions nos tuteurs Solenn et Donald, l'UNIGE et le MIT.