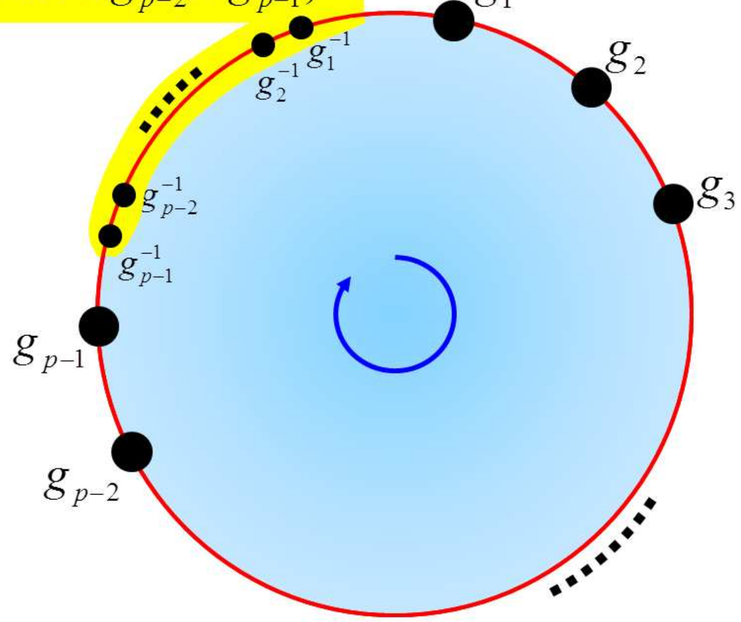
THEOREM OF THE DAY

Le théorème de Cauchy sur les groupes *Si l'ordre d'un groupe fini G est divisible par un nombre premier p alors G contient un élément d'ordre p.*

La table de multiplication à droite décrit un groupe d'ordre 10 : il y a dix éléments dont chacun s'affiche une fois dans chaque ligne et dans chaque colonne ; un des dix, l'élément e, (dit **neutre**) laisse inchangé tous les autres éléments pour la multiplication ; et la multiplication est **associative**, c'est à dire, par exemple, $(t \times r) \times w = j \times w = e$ s'accord avec $t \times (r \times w) = t^2 = e$. À noter, d'ailleurs, que t est un élément d'ordre 2 ($t^2 = e$) : le théorème de Cauchy affirme qu'un tel élément doit éxister parce que 2 divise 10. Il est moins facile de confirmer que l'équation $x^5 = e$ admet aussi une solution. Pourtant, il y en a cinq (y compris la solution triviale $x = e$) alors on peut tenter sa chance : c'est pile ou face ! Ou bien on reconnait le groupe diédral D_{10} et ainsi on connait déjà la bonne réponse.*

×	e	t	r	d	j	a	w	s	k	i
e	e	t	r	d	j	a	w	s	k	i
t	t	e	j	k	r	i	s	w	d	a
r	r	w	e	s	a	j	t	d	i	k
d	d	a	k	j	w	s	i	r	t	e
j	j	s	t	w	i	r	e	k	a	d
a	a	d	w	t	k	e	r	i	j	s
w	w	r	a	i	e	k	d	t	s	j
s	s	j	i	a	t	d	k	e	w	r
k	k	i	d	r	s	w	a	j	e	t
i	i	k	s	e	d	t	j	a	r	w

$$g_p = (g_1 \times g_2 \times \ldots \times g_{p-2} \times g_{p-1})^{-1}$$



$$g_1 \times g_2 \times \ldots \times g_{p-1} \times g_p = 1$$

*Aussi on peut reconstituer la table de multiplication classique de D_{10} en constatant que la liste des éléments du groupe est une anagramme du nom d'un scientifique célèbre.

Démonstration du théorème.
Notons 1 l'élément neutre d'un groupe fini quelconque G d'ordre n. Si p divise n alors le nombre de solutions de $x^p = 1$ doit être un multiple positif de p. Pour le voir, prenons l'ensemble X_p de tous les listes ordonnes de p éléments de G qui vérifient : $g_1 g_2 \cdots g_{p-1} g_p = 1$. Nous pouvons choisir n'importe quelles valeurs de $g_1, \ldots, g_{p-1}$, ensuite g_p est déterminé (voir le dessin ci-dessus à droite). Alors $|X_p| = n^{p-1}$. Or pour certaines listes de X_p tous les g_i sont identiques. Celles-ci correspondent aux solutions de $x^p = 1$. Supposons qu'il y a A telles listes. Chaque autre liste possède deux propriétés : (1) il s'agit d'un élément different d'X_p pour chaque décalage circulaire, parce que p est premier, de sorte qu'un p-gone ayant des sommets non identiques n'a pas de symétries, et (2) la valeur du produit reste égale à 1 pour tout décalage circulaire de ses éléments, parce que g_p peut être réécrit $g_{p-1}^{-1} \cdots g_2^{-1} g_1^{-1}$ et l'annulation de tous les éléments aura lieu quelque soit le point de départ de la multiplication (voir le dessin). Alors le nombre, notons B, de listes de X_p qui ne sont pas solutions à $x^p = 1$ est un multiple de p. Or $A + B = n^{p-1}$ et puisque B et n sont tous les deux divisibles par p, c'est le cas pour A aussi. Mais A n'est pas égale à zero, puisque 1 est une solution de $x^p = 1$, donc A est un multiple positif de p.

Tout élément d'ordre p engendre un sous-groupe d'ordre p, donc le théorème de Lagrange, affirmant que l'ordre d'un groupe doit être divisible par l'ordre de chacun de ses sous-groupes, trouve ici une réciprocité partielle, largement renforcé par les théorèmes célèbres de Sylow de 1872. Cauchy a démontré son théorème (affirmé indépendamment mais sans preuve par Évariste Galois) dans son œuvre fondamentale de 1845 'Mémoire sur les arrangements que l'on peut former avec des lettres données'. La démonstration décrite ci-dessus est due à James H. McKay, 1959.

merci à F.B., E.C.

Lien externe : bergeron.math.uqam.ca/cours-2/mat-2250-theorie-des-groupes-2. L'article originale de McKay math.uga.edu/~pete/McKay59.pdf.
À lire : *Éléments de théorie des groupes* par Josette Calais, PUF, 2014.