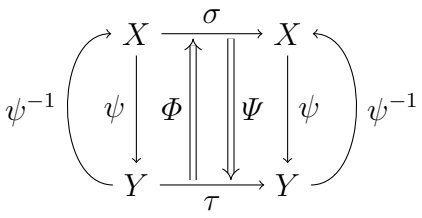
Structures algébriques

Lemme

S'il existe $\psi : X \xrightarrow{\cong} Y$, alors il existe $\Psi : \mathfrak{S}X \xrightarrow{\cong} \mathfrak{S}Y$.

Preuve

Soient $\psi : X \xrightarrow{\cong} Y$, $\sigma \in \mathfrak{S}X$ et $\tau \in \mathfrak{S}Y$.



Soit $\begin{aligned} \Psi : \mathfrak{S}X &\to \mathfrak{S}Y \\ \sigma &\mapsto \psi \circ \sigma \circ \psi^{-1} \end{aligned}$.
$\Psi(\sigma) \in \mathfrak{S}Y$ comme composition de bijections.

$$\begin{aligned} \Psi(\sigma_1 \circ \sigma_2) &= \psi \circ (\sigma_1 \circ \sigma_2)\psi^{-1} \\ &= \psi \circ \sigma_1 \circ \psi^{-1} \circ \psi \circ \sigma_2 \circ \psi^{-1} \\ &= \Psi(\sigma_1) \circ \Psi(\sigma_2) \end{aligned}$$

Donc, Ψ est un morphisme de groupes.
On pose $\begin{aligned} \Phi : \mathfrak{S}Y &\to \mathfrak{S}X \\ \tau &\mapsto \psi^{-1} \circ \tau \circ \psi \end{aligned}$.
$(\Psi \circ \Phi)(\tau) = \psi \circ \psi^{-1} \circ \tau \circ \psi \circ \psi^{-1} = \tau$.
Donc, $\Psi \circ \Phi = \mathrm{id}$. De même, $\Phi \circ \Psi = \mathrm{id}$.
Donc, Ψ est un isomorphisme.

Théorème : Théorème de Cayley

Tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique.

Preuve : Théorème de Cayley

Soient $g \in G$ et $\varphi_g : x \mapsto gx$.
φ_g est injective par régularité des éléments de G et bijective car les deux ensembles sont de même cardinal (fini).
Soit $n = |G|$.
On définit $\begin{aligned} f : (G, \times) &\to (\mathfrak{S}G, \circ) \\ g &\mapsto \varphi_g \end{aligned}$
$f(e) = \varphi_e = \mathrm{id}$

Soit $(x, y, z) \in G^3$.

$$\begin{aligned}(f(x \cdot y))(z) &= (x \cdot y) \cdot z \\ &= x \cdot (y \cdot z) \\ &= (f(x))(y \cdot z) \\ &= ((f(x)) \circ (f(y)))(z)\end{aligned}$$

On a donc bien un morphisme de groupes.
Soit $g \in \ker(f)$. $f(g) = \mathrm{id}$. Donc, pour tout $x \in G$, $g \cdot x = x$. Donc, $g = e$ par régularité des éléments de G.
Donc, $\ker(f) = \{e\}$. Donc, f est injective.
Donc, $f^{|\operatorname{im}(f)}$ est bijective. Donc, $\operatorname{im}(f) = f(G)$ est un sous-groupe de $\mathfrak{S}G$.
De plus, $G \cong [\![1, n]\!]$ car $|G| = n$.
Donc, d'après le lemme précédent, $(\mathfrak{S}G, \circ) \cong (\mathfrak{S}_n, \circ)$.
Donc, $\Psi\big(f^{|f(G)}(G)\big) = \big(\Psi \circ f^{|f(G)}\big)(G)$ est un sous-groupe de $\mathfrak{S}_n$.
De plus, $\Psi \circ f^{|f(G)}$ est un isomorphisme comme composition d'isomorphismes.
Donc, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Lemme

Si H et K sont deux sous-groupes de G d'ordres finis respectifs a et b tels que $a \wedge b = 1$, alors $H \cap K = \{e\}$.

Preuve

Soit H et K deux sous-groupes de G d'ordres finis a et b.
$H \cap K$ est un sous-groupe de H et de K. Donc, d'après le théorème de Lagrange, $|H \cap K| \mid a$ et $|H \cap K| \mid b$.
Donc, $|H \cap K| \mid 1$. Donc, $|H \cap K| = 1$.
Donc, $H \cap K = \{e\}$.

Propriété : Ordre d'un produit

Soient G un groupe abélien fini et x et y deux éléments de G d'ordres respectifs a et b.
Si $a \wedge b = 1$, alors xy est d'ordre ab.

Preuve : Ordre d'un produit

Soit $(x, y) \in G^2$.
$(xy)^{ab} = x^{ab}y^{ab} = (x^a)^b\big(y^b\big)^a = e$.
Donc, $\operatorname{ord}(xy) \mid ab$.
Pour tout $n \in \mathbb{N}$, $(xy)^n = e = x^n y^n \Leftrightarrow x^n = y^{-n} \in \langle x \rangle \cap \langle y \rangle$.
Or, $\operatorname{ord}(\langle x \rangle) \wedge \operatorname{ord}(\langle y \rangle) = 1$. Donc, d'après le lemme précédent, $\langle x \rangle \cap \langle y \rangle = \{e\}$.
D'où, $x^n = y^{-n} = e$. Donc, $a \mid n$ et $b \mid n$. Or, $a \wedge b = 1$. Donc, $ab \mid n$.
D'où la minimalité de ab.
Donc, $\operatorname{ord}(xy) = ab$

Lemme

Soit G un groupe fini.
S'il existe un élément x d'ordre a danse G, alors in existe dans G un élément z d'ordre d avec $d \mid a$.

Preuve

Soit x un élément de G d'ordre a. Soit d un diviseur de a.
On pose $z = x^{\frac{a}{d}}$.
$z^d = x^a = e$. Donc, $\text{ord}(z) \leqslant d$.
Soit $m \in [\![1, d-1]\!]$. $z^m = x^{\frac{a}{d}m} \neq e$ car $\dfrac{a}{d}m \leqslant a$ et $\text{ord}(x) = a$.
Donc, $\text{ord}(z) = d$.

Lemme : Lemme de Cauchy

Soit G un groupe fini.
Si un nombre premier p divise l'ordre de G, alors il existe dans G un élément d'ordre p.

Preuve : Lemme de Cauchy

Soit G un groupe fini.
Soit p un nombre premier tel que $p \mid |G|$.
Soit $E = \{(x_1, \cdots, x_p) \in G^p \mid x_1 \cdots x_p = e\}$.
On définit sur E la relation $\sim$: $(x_1, \cdots, x_p) \sim (y_1, \cdots, y_p)$ si et seulement si $(y_1, \cdots, y_p)$ est obtenu de $(x_1, \cdots, x_p)$ par permutation circulaire.

Montrons que $\sim$ est une relation d'équivalence.
Réflexivité : $(x_1, \cdots, x_p) \sim (x_1, \cdots, x_p)$.
Symétrie : Soit $((x_1, \cdots, x_p), (x_1, \cdots, x_p)) \in E^2$ tel que $(x_1, \cdots, x_p) \sim (y_1, \cdots, y_p)$.
Ainsi, il existe $T \in \mathbb{Z}$ tel que pour tout $k \in [\![1, p]\!]$, $x_k = y_{k+T}$ (indices considérés modulo k).
Ainsi, pour tout $k \in [\![1, p]\!]$, $y_k = x_{k-T}$.
Donc, $(y_1, \cdots, y_p) \sim (x_1, \cdots, x_p)$.
Transitivité : Soit $((x_1, \cdots, x_p), (y_1, \cdots, y_p), (z_1, \cdots, z_p)) \in E^3$ tel que $(x_1, \cdots, x_p) \sim (y_1, \cdots, y_p)$ et $(y_1, \cdots, y_p) \sim (z_1, \cdots, z_p)$.
Ainsi, il existe $(T_1, T_2) \in \mathbb{Z}^2$ tel que pour tout $k \in [\![1, p]\!]$, $x_k = y_{k+T_1}$ et $y_k = z_{k+T_2}$ (indices considérés modulo k).
Ainsi, pour tout $k \in [\![1, p]\!]$, $x_k = z_{k+T_1+T_2}$.
Donc, $(x_1, \cdots, x_p) \sim (z_1, \cdots, z_p)$.
Donc, $\sim$ est une relation d'équivalence.

Soit $(x_1, \cdots, x_p) \in E$.
On prolonge les x_i en une suite $(u_n)_{n \in \mathbb{Z}}$ avec $u_n = x_{n \bmod p}$.
(u_n) est de période p. Donc la période minimale de (u_n) divise p. C'est donc 1 ou p.
Ainsi, les classes d'équivalence de $\sim$ sont soit de cardinal 1 (période minimale égale à 1), soit de cardinal p (période minimale égale à p).

Pour $x_1, \cdots, x_{p-1}$ fixés, on a une unique valeur possible pour $x_p = (x_1 \cdots x_{p-1})^{-1}$.
Donc, $|E| = |G|^{p-1}$. Donc, $p \mid |E|$.
Ainsi, le nombre de classes de cardinal 1 est divisible par p. Cela correspond à l'ensemble de $x \in G$ tel que $x^p = e$. Donc, ces x sont d'ordre 1 ou p et le seul élément d'ordre 1 est e.
Donc, le nombre d'éléments d'ordre p est congru à $p - 1$ modulo p.
Donc, il existe $x \in G$ tel que $\text{ord}(x) = p$.