Table des matières

HISTOIRES DE GROUPES

Dominique Hoareau, domeh@wanadoo.fr

1 Division euclidienne dans $\mathbb{Z}$

1.1 Sous-groupes de $\mathbb{Z}$, congruence dans $\mathbb{Z}$

Propriété 1
Les sous-groupes de $(\mathbb{Z}, +)$ (monogène) sont aussi monogènes : les sous-groupes additifs de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{Z}$.

Les $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Réciproquement, soit H un sous-groupe de $\mathbb{Z}$, $H \neq \{0\}$. La partie $H \cap \mathbb{N}^*$ non vide de $\mathbb{N}$ a un plus petit élément qu´on appelle n. Clairement, $n\mathbb{Z} \subset H$. A présent, si $x \in H$, par division euclidienne, x s´écrit $x = nq + r$, avec $0 \leqslant r < n$. Ainsi $r = x - nq$ est dans H et dans $\mathbb{N}^*$, et $r = 0$ par statut de n. Finalement $x = nq \in n\mathbb{Z}$. D´où le résultat. On retiendra qu´un générateur d´un sous-groupe $H \neq \{0\}$ de $\mathbb{Z}$ est le plus petit entier naturel non nul qui se trouve dans H.

Pour a et b entiers relatifs, les sous-groupes $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ s´écrivent (de façon unique) $d\mathbb{Z}$ et $m\mathbb{Z}$ $(d, m \in \mathbb{N})$. L´entier d est appelé pgcd de a et b (notation : $d = a \wedge b$), m ppcm de a et b $(m = a \vee b)$. Lorsque $d = 1$, on dit que a et b sont premiers entre eux.

Soit $n \in \mathbb{N}$. On définit la relation de congruence modulo n en posant :

$$x \equiv y(n) \Leftrightarrow x - y \in n\mathbb{Z} .$$

L´ensemble des classes d´équivalence est notée $\mathbb{Z}/n\mathbb{Z}$ et la classe de x modulo $n\mathbb{Z}$ est $\bar{x} = x + n\mathbb{Z}$.

Lorsque $x \equiv 0(n)$, on dit que n divise x et on note : $n \mid x$.

Propriété 2 *: (lemme de Gauss)*
Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Puisque $a \wedge b = 1$, il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$. On a alors $c(au + bv) = c$, $acu + bcv = c$. Or bc s´écrit $bc = a\gamma$ avec $\gamma \in \mathbb{Z}$. Il vient $a(cu + \gamma v) = c$ donc $a \mid c$.

Exercice 1
1) Pour $d = a \wedge b$, montrer que $d \mid a$ et $d \mid b$, et que $[d' \mid a \ ; \ d' \mid b \Rightarrow d' \mid d]$.
2) Pour $m = a \vee b$, montrer que $a \mid m$ et $b \mid m$, et que $[a \mid m' \ ; \ b \mid m' \Rightarrow m \mid m']$.
3) Pour $m = a \vee b$, montrer qu´il existe a' et b' dans $\mathbb{Z}$, tels que $a' \mid a$, $b' \mid b$, $a' \wedge b' = 1$ et $m = a'b'$.
(On pourra décomposer a et b en produits de facteurs premiers :

$$a = \underbrace{p_1^{\alpha_1} ... p_k^{\alpha_k}}_{a'} p_{k+1}^{\alpha_{k+1}} ... p_j^{\alpha_j} \quad ; \quad b = p_1^{\beta_1} ... p_k^{\beta_k} \underbrace{p_{k+1}^{\beta_{k+1}} ... p_j^{\beta_j}}_{b'},$$

où $\alpha_i > \beta_i \geqslant 0$ si $1 \leqslant i \leqslant k$ et $0 \leqslant \alpha_i \leqslant \beta_i$ si $k + 1 \leqslant i \leqslant j$.)

Un entier p est dit premier si ses seuls diviseurs sont p, $-p$, 1 et -1. S´il ne divise pas un entier k, alors $k \wedge p = 1$.

Propriété 3

$$\mathbb{Z}\ /n\mathbb{Z}\ = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$$

Pour α et α' distincts entre 0 et $n-1$, on a $\alpha' - \alpha \notin n\mathbb{Z}$, donc $\bar{\alpha} \neq \bar{\alpha'}$. Par ailleurs, pour $m \in \mathbb{Z}$, on écrit $m = nq + r$ où $q \in \mathbb{Z}$ et $0 \leqslant r \leqslant n-1$. Ainsi : $m - r \in n\mathbb{Z}$ et $\bar{m} = \bar{r}$.

1.2 Le modèle $\mathbb{Z}$

Propriété 4 *Tout groupe $G =< a >$ monogène et infini est isomorphe à $\mathbb{Z}$.*

On considère le morphisme de groupes surjectif $f : n \mapsto a^n$ de $\mathbb{Z}$ sur G. Si f n´est pas injective, $\exists m, n \in \mathbb{Z} \quad m \neq n,\ a^m = a^l$, donc $a^{m-l} = 1$. On considère alors n, le plus petit entier naturel tel que $a^n = 1$. On a : $\{1, a, ..., a^{n-1}\} \subset G$ et on montre par division euclidienne l´autre inclusion $\{1, a, ..., a^{n-1}\} \supset G$. Absurde puisque G est supposé infini.

1.3 Ordre d´un élément

Soit G un groupe, $a \in G$ et $k \in \mathbb{Z}$. Si $a^k = 1$, on dit que k est un exposant de a .

On montre que l´ensemble $\mathcal{E}_a$ des exposants de a est un sous-groupe de $\mathbb{Z}$, donc $\mathcal{E}_a$ est un $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{N}$. Lorsque $\alpha \neq 0$, on dit que α est l´ ordre de a ou que a est d´ordre α. Sinon, on dit que a est d´ordre infini.

On envisage alors le morphisme surjectif $f : k \mapsto a^k$ de $\mathbb{Z}$ sur $< a >$ et la relation d´équivalence sur $\mathbb{Z}$ définie par :

$$k\mathcal{R}l \Leftrightarrow f(k) = f(l) \Leftrightarrow a^{k-l} = 1 \Leftrightarrow k - l \text{ est un exposant de } a \Leftrightarrow k - l \in \mathcal{E}_a = \alpha\mathbb{Z}\ .$$

On vérifie que $\bar{f} : \bar{k} \mapsto f(k)$ est correctement définie de $\mathbb{Z}\ /\alpha\mathbb{Z}$ dans $< a >$, surjective (comme f) et injective ("par construction"). Ainsi $< a >$ est infini comme $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ si a est d´ordre infini ($< a > \equiv \mathbb{Z}/0\mathbb{Z}$), et $\sharp(< a >) = \alpha$ si a est d´ordre $\alpha \neq 0$.

Propriété 5
Dans un groupe G, l´ordre d´un élément est égal à l´ordre du sous-groupe qu´il engendre.

On suppose G fini. L´ensemble $\mathcal{M}$ des entiers k tels que $\forall a \in G \quad a^k = 1$ est aussi un sous-groupe de $\mathbb{Z}$: en fait, $\mathcal{M} = \bigcap_{a \in G} \mathcal{E}_a$, donc $\mathcal{M}$ est $m\mathbb{Z}$ où m est le *ppcm* des ordres des éléments de G et aussi le plus petit entier naturel tel que $\forall a \in G \quad a^m = 1$. L´entier m est appelé exposant de G . Par exemple dans $\mathcal{S}_3$ (d´ordre 6), les permutations autres que 1 sont d´ordre 2 (transpositions) et d´ordre 3 (3-cycles), donc l´exposant de $\mathcal{S}_3$ est 6.

1.4 Groupe cyclique

Propriété 6 *Soit $G =< a >= \{1, a, ..., a^{n-1}\}$ un groupe cyclique d´ordre n. Alors*

0. L´ordre n de G est un exposant de chacun des éléments de G : $\forall g \in G \quad g^n = 1$.

1. *Tout sous-groupe $H \neq \{1\}$ de G est cyclique, engendré par la plus petite puissance de a qui se trouve dans H.*
2. *Pour $0 \leqslant k \leqslant n-1$, l´élément a^k est d´ordre $\alpha = \frac{n}{k \wedge n}$. Aussi, $< a^k >= G \Leftrightarrow k \wedge n = 1$.*
3. *Pour tout diviseur d de n, il existe un et un seul sous-groupe de G, d´ordre d.*

Question : Un groupe dont tous les sous-groupes sont cycliques, est-il nécessairement cyclique ?

Pour 1) :
On procède comme pour la caractérisation des sous-groupes de $\mathbb{Z}$. On écrit $H = \{1, a^{k_1}, ..., a^{k_j}\}$ où $0 < k_1 < ... < k_j < n$, et par division euclidienne de k_i par k_1, on montre que tout a^{k_i} est une puissance de a^{k_1}. On retiendra qu´un générateur de H est la plus petite puissance de a qui se trouve dans H.

Pour 2) :
On écrit $< a^k >= \{1, a^{k_1}, ..., a^{k_{\alpha-1}}\}$ (α éléments dans $< a^k >$) où $0 < k_1 < ... < k_{\alpha-1} < n$. On sait que a^k et a^{k_1} engendrent le même sous-groupe. Or, par statut de α (plus petit entier naturel tel que $(a^{k_1})^{\alpha} = 1$), 1 et les puissances $a^{k_1}, a^{2k_1}, ..., a^{(\alpha-1)k_1}$ de a^{k_1} (au nombre de α) sont distincts. D´où nécessairement :

$$< a^k >=< a^{k_1} >= \{1, a^{k_1}, a^{k_2} = a^{2k_1}, ..., a^{k_{\alpha-1}} = a^{(\alpha-1)k_1}\}.$$

L´entier $k_1 \times \alpha$ est un exposant de a, donc $n \mid k_1\alpha$. Or, $k_{\alpha-1} = (\alpha-1)k_1 < n$, donc $\alpha k_1 - k_1 < n$, $\alpha k_1 < n + k_1 < 2n$, d´où : $\boxed{n = k_1 \times \alpha}$. Par ailleurs, $a^k \in < a^{k_1} >$, donc k s´écrit $\boxed{k = k_1 \times \beta}$. Enfin, puisque $a^{k_1} \in < a^k >$, $a^{k_1} = a^{k\,s}$, $k_1 - ks$ est un exposant de a, donc s´écrit $k_1 - ks = nt$. Il vient : $k_1 - k_1\beta\ s = k_1\alpha t$, $\alpha t + \beta s = 1$, donc $\boxed{\alpha \wedge \beta = 1}$. Puisque par ailleurs $n = k_1\alpha$ et $k = k_1\beta$, on a $k_1 = k \wedge n$ et $\alpha = \frac{n}{k \wedge n}$.

Pour 3) :

Existence : Soit d un diviseur de n. On pose $\boxed{k = \dfrac{n}{d}}$ et $\boxed{x = a^k}$. L´ordre de x est d´après ce qui précède : $\frac{n}{k \wedge n} = \frac{n}{k} = d$.

Unicité : Soit H un sous-groupe d´ordre d de G (cyclique), soit alors $y = a^m$ dans G tel que $H =< y >$. Pour $g = a^{\alpha} \in < y >$, $g^d = a^{\alpha d} = 1$, donc il existe $l \in \mathbb{Z}$ tel que $\alpha d = l\,n$, $\alpha = \frac{l\,n}{d}$. Ainsi : $g = a^{\alpha} = a^{\frac{l\,n}{d}} = (a^{\frac{n}{d}})^l = (a^k)^l = x^l$ donc $g \in < x >$ et $< y > \subset < x >$. Puisque $\sharp(< y >) = \sharp(< x >)$, $< x >=< y >$.

Exercice 2 *Si G et $\{1\}$ sont les seuls sous-groupes d´un groupe G non trivial, alors G est monogène, fini et d´ordre premier.*

Soit $x \in G$, $x \neq 1$. On a $< x > \neq \{1\}$, donc $< x >= G$. Par ailleurs, $< x^2 >= \{1\}$ ou $< x^2 >=< x >$, donc $x^2 = 1$ ou $\exists m \in \mathbb{Z} \quad (x^2)^m = x$, i.e. $x^2 = 1$ ou $x^{2m-1} = 1$. Ainsi, G est cyclique de cardinal noté n. Soit enfin $d \mid n$ avec $1 < d < n$. Le sous-groupe $< x^{\frac{n}{d}} >$ est d´ordre $d \notin \{1, n\}$, donc $< x^{\frac{n}{d}} > \neq \{1\}$ et $< x^{\frac{n}{d}} > \neq G$. Impossible !

2 Théorème de Lagrange

2.1 Dans un groupe abélien fini

Soit G un groupe commutatif fini d´ordre n, et $g \in G$. On pose :

$$a = \prod_{x \in G} x.$$

La translation $t_g : x \mapsto gx$ est bijective et puisque G est commutatif, le produit dans G ne dépend pas de l´ordre des facteurs. Ainsi :

$$a = \prod_{x \in G} t_g(x) = \prod_{x \in G} gx$$

et toujours par commutativité de G, $a = g^n a$. En définitive :

$$\forall g \in G \qquad g^n = 1.$$

2.2 Relation modulo un sous-groupe

Soit G un groupe. Si H est un sous-groupe de G, on définit sur G la relation de congruence (à gauche) modulo H en posant : $g\mathcal{R}_H g' \Leftrightarrow g^{-1}g' \in H$. Pour $g \in G$, la classe de g est $\bar{g} = \{gh \ ; \ h \in H\}$, qu´on note aussi gH. L´espace des classes est noté G/H.

On suppose que G est fini. Pour $g \in G$, on vérifie que l´application $h \mapsto gh$ de H dans gH est une bijection, ce qui assure que toutes les classes ont le même cardinal $\circ(H)$.

Si on note $[G : H]$ le nombre de classes d´équivalence modulo $\mathcal{R}_H$ (indice de H dans G), on peut écrire :

$$\circ(G) = [G : H] \ \circ (H).$$

On vient d´établir *le théorème de Lagrange* :

Propriété 7 *Si G est un groupe fini et si H est un sous-groupe de G, alors l´ordre de H et son indice dans G divisent l´ordre de G.*

Exercice 3 *Montrer que si G est un groupe de cardinal impair, alors :*

$$\forall x \in G \quad \exists\, !\, y \in G \quad x = y^2.$$

Exercice 4 *On désigne par $\mathcal{S}_n$ le groupe des bijections de $\{1, ..., n\}$. On veut calculer son ordre β_n[1]. On définit sur $\mathcal{S}_n$ une relation d´équivalence en posant :*

$$\sigma\mathcal{R}\sigma' \textit{si, et seulement si, } \sigma(n) = \sigma'(n).$$

1) Montrer que $\mathcal{R}$ est la relation modulo le sous-groupe $H_n = \{\sigma \in \mathcal{S}_n \ ; \ \sigma(n) = n\}$ de $\mathcal{S}_n$.
2) Montrer que H_n est en bijection avec $\mathcal{S}_{n-1}$ et que G/H_n est en bijection avec $\{1, ..., n\}$.
3) En déduire par recurrence que $\beta_n = \circ(\mathcal{S}_n\ ) = n!$.

[1] Action naturelle de $\mathcal{S}_n$ sur $\{1, ..., n\}$

Question : Si G est un groupe fini d´ordre n et si m est un diviseur de n, G possède-t-il un sous-groupe d´ordre m ? La réponse est positive si G est cyclique.

Corollaire 1 *(l´ordre d´un groupe fini est un exposant de chacun de ses éléments)*

Si G est un groupe fini d´ordre n, alors : $\forall g \in G \quad g^n = 1$.

Soit $g \in G$. L´ordre de g est l´ordre du sous-groupe $< g >$, donc divise l´ordre de G, d´où le résultat.

Corollaire 2 *(Groupe d´ordre premier)*

Un groupe G d´ordre premier p est cyclique.

Soit $x \in G$, $x \neq 1$. On a $\circ(x) > 1$ et $\circ(x)$ est un diviseur de p, donc avec p premier, $\circ(x) = p$. Ainsi $G =< x >= \{1, x, .., x^{p-1}\}$.

Exercice 5 *Trouver les sous-groupes de $\mathcal{S}_3$.*

On étiquette les éléments de $\mathcal{S}_3$: Id, les transpositions (d´ordre 2) $\tau_1 = (2,3)$, $\tau_2 = (1,3)$, $\tau_3 = (1,2)$, et les 3-cycles $r = (1,2,3)$, $\rho = r^{-1} = (1,3,2)$. Si H est un sous-groupe propre de $\mathcal{S}_3$, son ordre est 2 ou 3, donc H est cyclique. Ainsi $H =< \tau_1 >$, ou $< \tau_2 >$, ou $< \tau_3 >$, ou $< r >=< \rho >$. Voici un exemple de groupe non cyclique (et même non commutatif) dont tous les sous-groupes propres sont cycliques.

Corollaire 3 *(Formule des indices)*

Soit S et T deux sous-groupes de G tels que : $S \subset T$. On a :

$$[G : S] = [G : T]\ [T : S].$$

On écrit : $[G : S] = \frac{\circ(G)}{\circ(S)} = \frac{[G:T]\ \circ(T)}{\circ(S)} = [G : T]\ [T : S]$.

2.3 Congruence dans $\mathbb{Z}$

- Pour $n \in \mathbb{N}$, les classes d´équivalence de $\mathbb{Z}\ /n\mathbb{Z}$ sont notées $\bar{k}, k \in \mathbb{Z}$ et $\mathbb{Z}\ /n\mathbb{Z} = \{\bar{0}, ..., \overline{n-1}\}$.

Avec $(\mathbb{Z}\ , +)$ commutatif, on montre facilement que :

$$\bar{k} = \bar{k'} \quad et \quad \bar{l} = \bar{l'} \Rightarrow \overline{k+l} = \overline{k'+l'}.$$

On dit que la relation de congruence est compatible avec la loi additive de $\mathbb{Z}$. La l.c.i $(\bar{k}, \bar{l}) \mapsto \overline{k+l}$ est ainsi correctement définie, et donne à $\mathbb{Z}\ /n\mathbb{Z}$ une structure de groupe commutatif.

Si $G =< a >$ désigne un groupe monogène, on envisage le morphisme surjectif $f_a : n \mapsto a^n$ de $\mathbb{Z}$ sur G et la relation d´équivalence sur $\mathbb{Z}$:

$$x\mathcal{R}_a y \Leftrightarrow f_a(x) = f_a(y) \Leftrightarrow f_a(x)f_a(-y) = 1 \Leftrightarrow f_a(x-y) = 1 \Leftrightarrow x - y \in ker(f_a).$$

Or $ker(f_a)$ est un sous-groupe de $\mathbb{Z}$, donc l´ensemble des classes d´équivalence pour $\mathcal{R}_a$ est un $\mathbb{Z}\ /n\mathbb{Z}$. Deux cas se présentent :

– $n = 0$, f_a est alors injective et G est isomorphe à $\mathbb{Z}$.
– $n \neq 0$, on vérifie facilement que $\bar{f}_a : \bar{x} \mapsto f_a(x)$ est correctement définie de $\mathbb{Z}/n\mathbb{Z}$ dans G, surjective (comme f_a), injective et réalise un morphisme de $\mathbb{Z}/n\mathbb{Z}$ sur G.

On a montré :

Propriété 8 *Soit G un groupe monogène.*

1. *Si G est infini, G est isomorphe à $\mathbb{Z}$.*
2. *Si G est fini d´ordre n, alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Remarque : Si G est cyclique, on peut penser qu´il y a autant d´isomorphismes de $\mathbb{Z}/n\mathbb{Z}$ sur G, que de générateurs de G.

Exercice 6 *Si un groupe G possède exactement 3 sous-groupes, alors G est cyclique d´ordre p^2, avec p premier.*

Soit $x \in G$, $x \neq 1$. Le sous-groupe $< x >$ est différent de $\{1\}$ donc deux cas se présentent :

1. Si $< x >= G$, alors $< x >$ possède un seul sous-groupe propre non trivial. Puisque $\mathbb{Z}$ possède une infinité de sous-groupes propres, $< x >$ n´est pas isomorphe à $\mathbb{Z}$, est donc cyclique. Son ordre possède alors un unique diviseur propre et s´écrit nécessairement p^2, avec p premier.
2. Si $< x >\neq G$, $\{1\}$, $< x >$ et G sont les trois sous-groupes de G. Soit $y \in G \setminus < x >$. On a $< y >\neq \{1\}$ et $< x >\neq < y >$, donc $< y >= G$. On est alors ramené au cas précédent.

Question : Il n´y a qu´un seul modèle de groupe d´ordre n premier : $\mathbb{Z}/n\mathbb{Z}$. Mais peut-on affirmer que n est premier lorsqu´il n´y a qu´un modèle de groupe d´ordre n ?

• On vérifie que la congruence modulo n est également compatible avec la loi multiplicative de $\mathbb{Z}$, ce qui permet de définir une loi multiplicative sur $\mathbb{Z}/n\mathbb{Z}$. Muni de ces deux lois, $\mathbb{Z}/n\mathbb{Z}$ a alors une structure d´anneau.

• On rappelle que les inversibles de $\mathbb{Z}/n\mathbb{Z}$ (éléments ayant un symétrique pour la loi multiplicative) forment un groupe noté $\sqcup(\mathbb{Z}/n\mathbb{Z})$ et

$$\bar{k} \in \sqcup(\mathbb{Z}/n\mathbb{Z}) \Leftrightarrow k \wedge n = 1.$$

Propriété 9 *:(Lemme d´Euclide)*
Si p est premier et si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

2.4 Indicatrice d´Euler

Pour $n \geqslant 1$, on note $\varphi(n)$ le nombre des entiers $k \in \{1, ..., n\}$ premiers avec n. C´est aussi l´ordre du groupe multiplicatif $\sqcup(\mathbb{Z}/n\mathbb{Z})$, ou encore le nombre des $\bar{k}$ du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ tels que le sous-groupe $< \bar{k} >= \{j\bar{k} \ ; \ j \in \mathbb{Z}\}$ engendré par $\bar{k}$ soit égal à $\mathbb{Z}/n\mathbb{Z}$; C´est aussi le nombre des générateurs d´un groupe cyclique d´ordre n, ou enfin le nombre des éléments de $(\mathbb{Z}/n\mathbb{Z}, +)$ qui sont d´ordre exactement n.

Lorsque $n = p$ est premier, $\mathbb{Z}/p\mathbb{Z}$ est alors un corps et $\varphi(p) = p - 1$. Le théorème de Lagrange donne :

Propriété 10 *(Petit théorème de Fermat)*
Pour p premier et $k \neq 0(p)$, on a : $k^{p-1} = 1$.

Application 1 *Soit p premier. Dans l´anneau $\mathbb{Z}/p\mathbb{Z}[X]$, on a l´identité :*

$$X^p - X = \prod_{k=0}^{p-1} (X - k).$$

Conséquences :

1. $(p-1)! = -1(p)$.
2. $(X+1)^p = X^p + 1$ *dans l´anneau* $\mathbb{Z}/p\mathbb{Z}[X]$
3. *Pour* $0 < k < p$, $C_p^k = 0(p)$.

On constate que le polynôme $X^p - X$ unitaire de degré p admet les p éléments k du corps $\mathbb{Z}/p\mathbb{Z}$ comme racines, donc est le produit des $X - k$. Pour (1), on identifie le coefficient de X dans l´identité précédente. Pour (2), on écrit

$$X^p - X = \prod_{k \in \mathbb{Z}/p\mathbb{Z}} (X - k) = \prod_{k \in \mathbb{Z}/p\mathbb{Z}} (X - (k-1)) = \prod_{k \in \mathbb{Z}/p\mathbb{Z}} ((X+1) - k) = (X+1)^k - (X+1).$$

Enfin, la nullité des coefficients binomiaux C_p^k $(0 < k < p)$ s´obtient en développant (2).

2.4.1 Comment calculer $\varphi(n)$, pour tout $n \in \mathbb{N}^*$?

1) Pour p premier, $\varphi(p) = p - 1$.
2) Pour p premier et $\alpha \in \mathbb{N}$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
3) Si m et n sont deux entiers premiers entre eux, alors $\mathbb{Z}\,/mn\mathbb{Z}$ et $\mathbb{Z}\,/n\mathbb{Z} \times \mathbb{Z}\,/m\mathbb{Z}$ sont des groupes (et même des anneaux) isomorphes. Conséquence : $\varphi(mn) = \varphi(m)\,\varphi(n)$ dès que $m \wedge n = 1$. On dit que la fonction indicatrice d´Euler φ est multiplicative au sens de l´arithmétique.
4) Si n se décompose en facteurs premiers sous la forme $n = p_1^{\alpha_1} ... p_i^{\alpha_i}$, alors $\varphi(n) = n \prod_{k=1}^{i} (1 - \frac{1}{p_k})$.

Pour 3) : Puisque m et n sont premiers entre eux, on choisit $m', n' \in \mathbb{Z}$ tels que :

$$mm' + nn' = 1.$$

Pour p, p', q, q' dans $\mathbb{Z}$, $p = p'(n)$ et $q = q'(m)$ impliquent $p - p' \in n\mathbb{Z}$, $q - q' \in m\mathbb{Z}$, ce qui donne : $(p-p')mm' + (q-q')nn' \in mn\mathbb{Z}$ ou $pmm' + qnn' = p'mm' + q'nn'(mn)$. On définit donc correctement une application ϕ de $\mathbb{Z}\,/n\mathbb{Z} \times \mathbb{Z}\,/m\mathbb{Z}$ dans $\mathbb{Z}\,/mn\mathbb{Z}$ en posant : $\phi(\bar{p}, \bar{q}) = \overline{pmm' + qnn'}$. On vérifie facilement que $\phi\left((\bar{p}, \bar{q}) + (\bar{p'}, \bar{q'})\right) = \phi(\bar{p}, \bar{q}) + \phi\left(\bar{p'}, \bar{q'}\right)$, ce qui fait de ϕ un morphisme de groupe. A présent, si $\phi(\bar{p}, \bar{q}) = 0$, alors $pmm' + qnn' \in mn\mathbb{Z}$, donc $pmm' \in n\mathbb{Z}$ et comme $m \wedge n = m' \wedge n = 1$, on a $p \in n\mathbb{Z}$. De même, on vérifie que $q \in m\mathbb{Z}$, donc ϕ est injective. Puisque $\mathbb{Z}\,/n\mathbb{Z} \times \mathbb{Z}\,/m\mathbb{Z}$ et $\mathbb{Z}\,/nm\mathbb{Z}$ ont le même cardinal, finalement, on a bien :

$$\mathbb{Z}\,/n\mathbb{Z} \times \mathbb{Z}\,/m\mathbb{Z} \simeq \mathbb{Z}\,/nm\mathbb{Z}\,.$$

2.4.2 Une égalité classique : $n = \sum_{d|n} \varphi(d)$

Première preuve

Lemme : une réciproque partielle à Lagrange Soit $G =< a >$ un groupe cyclique d´ordre n. Pour tout diviseur d de n, il existe un et un seul sous-groupe de G, d´ordre d.

Fin de preuve : On définit sur G une relation d´équivalence de la façon suivante : pour x et y dans G, $x\mathcal{R}y$ si, et seulement si, il existe d diviseur de n tel que $o(x) = o(y) = d$. Avec la partie *existence* du lemme, il y a autant de classes d´équivalence que de diviseurs de n. Avec la partie *unicité*,

$$x\mathcal{R}y \Leftrightarrow < x >=< y >,$$

donc la classe de x est l´ensemble des générateurs de $< x >$, au nombre de $\varphi(d)$. Ainsi : $n = \sum_{d|n} \varphi(d)$.

Par récurrence
On raisonne par récurrence sur le nombre l d´entiers premiers de la décomposition de n. Si $l = 1$, n s´écrit $n = p^q$ avec p premier et $q \in \mathbb{N}^*$. Les diviseurs de n sont 1, p, ..., p^{q-1}, p^q, et

$$\sum_{d|n} \varphi(d) = 1 + (p-1) + (p^2 - p) + ... + (p^{q-1} - p^{q-2}) + (p^q - p^{q-1}) = p^q = n.$$

On suppose l´égalité vraie au rang l, et on envisage un entier $n = \prod_{1 \leqslant i \leqslant l+1} p_i^{\alpha_i} = \prod_{1 \leqslant i \leqslant l} p_i^{\alpha_i} \times p_{l+1}^{\alpha_{l+1}}$. Les diviseurs de n sont les diviseurs de $\prod_{1 \leqslant i \leqslant l} p_i^{\alpha_i}$ dont l´ensemble est noté $\mathcal{D}_l$ et les $d_l \times p_{l+1}^{\alpha}$ où $d_l \in \mathcal{D}_l$, $1 \leqslant \alpha \leqslant \alpha_{l+1}$, et $d_l \wedge p_{l+1}^{\alpha} = 1$. Par multiplicativité de la fonction indicatrice d´Euler et avec quelques factorisations judicieuses, on peut écrire : $\sum_{d|n} \varphi(d) = \sum_{d \in \mathcal{D}_l} \varphi(d) + \sum_{k=1}^{l+1} \left(\varphi(p_{l+1}^k) \sum_{d \in \mathcal{D}_l} \varphi(d) \right)$ puis

$$\sum_{d|n} \varphi(d) = \sum_{d \in \mathcal{D}_l} \varphi(d) \times \left(1 + \sum_{k=1}^{l+1} \varphi(p_{l+1}^k) \right) = \left(\prod_{1 \leqslant i \leqslant l} p_i^{\alpha_i} \right) \left(1 + (p_{l+1}^{\alpha_{l+1}} - 1) \right) = n.$$

2.5 Pour p premier, le groupe multiplicatif $\sqcup(\mathbb{Z}\ /p\mathbb{Z}\ ) = \mathbb{Z}/p\mathbb{Z}^*$ est cyclique.

2.5.1 Un lemme crucial : ordre d´un produit

Lemme 1 *Soit G un groupe fini, a et b deux éléments de G d´ordre α et β. On suppose que*
- *$ab = ba$.*
- *$\alpha \wedge \beta = 1$.*

Alors $\circ(ab) = \alpha\beta$.

On note γ l´ordre de ab.
a) $< a > \cap < b >= \{1\}$. (On pourra calculer x^α pour $x \in < a > \cap < b >$.)
b) $\gamma \mid \alpha\beta$.
c) $\alpha \mid \gamma$ et $\beta \mid \gamma$. (On remarquera que $(ab)^\gamma = 1$.)
d) $\gamma = \alpha\beta$.

Exercice 7 *Dans un groupe G commutatif et fini, l´ensemble des ordres est stable par ppcm. Ainsi, l´exposant m de G défini comme le ppcm des ordres des éléments de G, est aussi le plus grand des ordres des éléments de G.*

Soit x et y deux éléments de G d´ordre $\tilde{\alpha}$ et $\tilde{\beta}$. On prend α et β dans $\mathbb{Z}$ tels que $\alpha \mid \tilde{\alpha}$, $\beta \mid \tilde{\beta}$, $\alpha \wedge \beta = 1$ et $\tilde{\alpha} \vee \tilde{\beta} = \alpha\beta$. On pose $a = x^{\frac{\tilde{\alpha}}{\alpha}}$ et $b = y^{\frac{\tilde{\beta}}{\beta}}$ et ab est d´ordre $\tilde{\alpha} \vee \tilde{\beta}$.

2.5.2 Retour preuve

On veut exhiber un élément de $G = \mathbb{Z}/p\mathbb{Z}^*$ d´ordre $p-1$. Un candidat naturel est un élément $g \in G$ tel que :

$$\circ(g) = \max\{\circ(x)\,;\, x \in G\}.$$

On pose : $m = \max\{\circ(x)\,;\, x \in G\}$. La stratégie est la suivante : vérifier que tout x de G a un ordre l qui divise m. Ainsi, tous les éléments de G sont racines du polynôme $X^m - 1$ de $\mathbb{Z}/p\mathbb{Z}[X]$, ce qui impose $p - 1 \leqslant m$ et puisque par ailleurs m divise $p-1$, $m = p-1$.

Lemme 2
Soit G un groupe fini commutatif. Si x est un élément de G, alors l´ordre l de x divise l´exposant $m = \max\{\circ(x)\,;\, x \in G\}$ de G.

On décompose les entiers m et l en produits de facteurs premiers :

$$m = \underbrace{p_1^{\alpha_1}...p_k^{\alpha_k}}_{m'} p_{k+1}^{\alpha_{k+1}}...p_j^{\alpha_j} \quad ; \quad l = p_1^{\beta_1}...p_k^{\beta_k} \underbrace{p_{k+1}^{\beta_{k+1}}...p_j^{\beta_j}}_{l'},$$

où $\alpha_i > \beta_i \geqslant 0$ si $1 \leqslant i \leqslant k$ et $0 \leqslant \alpha_i \leqslant \beta_i$ si $k+1 \leqslant i \leqslant j$. Clairement : $m' \mid m$, $l' \mid l$, $m' \wedge l' = 1$, $m \vee l = m'l'$. Les éléments $g^{m/m'}$ et $x^{l/l'}$ ont pour ordre m' et l' ; Avec G commutatif et $m' \wedge l' = 1$, leur produit a pour ordre $m'\,l'$. Ceci impose $m'\,l' = m \vee l \leqslant m$, donc l divise m, ce qui termine la preuve.

3 Formule des indices, une preuve directe

S et T désignent deux sous-groupes de G tels que : $S \subset T$.

• Si $xS = x'S$, alors $x^{-1}x' \in S$, donc $x^{-1}x' \in T$ car $S \subset T$, ce qui assure que $xT = x'T$. On définit ainsi correctement une application ϕ de G/S vers G/T en posant $\phi(xS) = xT$.

• Soit r la relation d´équivalence associée à ϕ, définie sur G/S par :

$$xS\,r\,x'S \Leftrightarrow \phi(xS) = \phi(x'S).$$

On a : $xS\,r\,x'S \Leftrightarrow x\mathcal{R}_T x'$, donc le nombre de classes déquivalence pour r est égal à $[G : T]$.

• On a : $\overline{xS} = \{x'S\ ;\ x' \in xT\} = \{xtS\ ;\ t \in H\}$. On vérifie que l´application $tS \mapsto xtS$ de T/S dans $\overline{xS}$ est bijective, ce qui assure que chaque classe $\overline{xS}$ possède $[T : S]$ éléments. On conclut alors aisément.

4 Conjugaison and co

Dans un groupe commutatif, a étant fixé dans G, pour tout $g \in G$, on a $ga = ag$ donc gag^{-1} vaut a. Dans un groupe non commutatif, gag^{-1} n´est plus nécessairement égal à a, et la diversité des résultats pour gag^{-1} quand g parcourt G, est un indicateur de la non commutativité de G. Par ailleurs, gag^{-1} même distinct de a reste proche de a. Ainsi par exemple, les exposants de a sont exactement les exposants de gag^{-1} (et $\circ(a) = \circ(gag^{-1})$).

4.1 Sous-groupe distingué

Deux éléments a et b sont conjugués ou "du même type" dans G si, et seulement si, il existe $g \in G$ tel que $b = gag^{-1}$. On définit ainsi une relation d´équivalence appelée conjugaison, qui permet de classer les éléments de G par affinité.

Exemples :
a) Dans $\mathbb{R}^3$ euclidien, si s est une symétrie orthogonale par rapport à un plan P et si f est une isométrie de $\mathbb{R}^3$, alors $f\,s\,f^{-1}$ est la symétrie orthogonale par rapport au plan $f(P)$.
b) Deux matrices conjuguées de $GL(n, \mathbb{R})$ représentent le même automorphisme linéaire de $\mathbb{R}^n$, mais dans des bases différentes.
c) Dans le groupe symétrique $\mathcal{S}_n$, si σ est un p-cycle, alors σ s´écrit :
$\sigma = (a_1, a_2, ..., a_p)$ et pour $\tau \in \mathcal{S}_n$, $\tau\,\sigma\,\tau^{-1}$ est le p-cycle $(\tau(a_1), ..., \tau(a_p))$.

La classe d´équivalence de $a \in G$ est appelée orbite de a et est notée $\mathcal{O}_a$.

Exercice 8 *On étiquette les éléments de $\mathcal{S}_3$: Id, $\tau_1 = (2,3)$, $\tau_2 = (1,3)$, $\tau_3 = (1,2)$, $r = (1,2,3)$ et $\rho = r^{-1} = (1,3,2)$. Montrer à la main que $\mathcal{S}_3$ a 3 classes de conjugaison : $\{Id\}$, $\{\tau_1, \tau_2, \tau_3\}$ et $\{r, \rho\}$.*

Exercice 9 *Dans $\mathcal{S}_3$, 2 éléments de même ordre sont conjugués. Est-ce vrai dans tout groupe ?*

Dans $\mathcal{S}_4$, considérer $(1,2)$ et $(1,2)(3,4)$, d´ordre 2 et de parité différente.

Exercice 10 *Quels sont les groupes commutatifs G dans lesquels les éléments de même ordre sont conjugués.*

Le groupe trivial $G = \{1\}$ convient. Soit $G \neq \{1\}$ commutatif vérifiant la propriété. Puisque toutes les orbites dans G abélien sont ponctuelles, deux éléments de même ordre sont identiques. Soit $a \in G$, $a \neq 1$ et $\alpha \geqslant 2$ son ordre. Dans le sous-groupe $< a >$, le nombre d´éléments d´ordre α est $\varphi(\alpha)$. Par nécessité, $\varphi(\alpha) = 1$. Ainsi, $\alpha \in \{1, 2\}$, et puisque $a \neq 1$, son ordre est nécessairement $\alpha = 2$. On a montré que G a 2 éléments, donc $G \equiv \mathbb{Z}/2\mathbb{Z}$. Réciproquement, $\mathbb{Z}/2\mathbb{Z}$ convient.

Un sous-groupe de G est dit distingué (ou normal ou invariant) dans G, et on note $H \lhd G$, s´il contient la classe de conjugaison de chacun de ses points, ie

$$\forall a \in H \quad \forall g \in G \quad gag^{-1} \in H.$$

G et $\{1\}$ sont toujours distingués dans G.

Exercice 11 *Dans le groupe des bijections de* $\mathbb{R}$ *sur* $\mathbb{R}$ *, le sous-groupe des bijections monotones est-il distingué ?*

On pose : $\phi(x) = \frac{1}{x}$ si $x \neq 0$, $\phi(0) = 0$, ce qui fait de ϕ une bijection de $\mathbb{R}$ sur $\mathbb{R}$, et on envisage l´application affine (croissante) $f : x \mapsto x + 1$ On a $\phi \circ f \circ \phi^{-1}(-1) = 0$, $\phi \circ f \circ \phi^{-1}(0) = 1$, $\phi \circ f \circ \phi^{-1}(1) = \frac{1}{2}$. La conclusion est aisée.

Question : Si G est commutatif, toutes les classes de conjugaison sont des singletons et tout sous-groupe est distingué dans G. Existe-t-il des groupes non commutatifs dont tous les sous-groupes sont distingués ?

Voici un résultat "générateur" d´exemples de sous-groupes distingués (facile à prouver) :

Propriété 11 *Si* G *et* G' *sont deux groupes et* f *un morphisme de* G *dans* G'*, alors* $ker(f)$ *est distingué dans* G*.*

Exemples :

- On considère le morphisme signature ε surjectif de $\mathcal{S}_n$ sur $\{-1, 1\}$ (qui envoie toute transposition sur -1). Son noyau, appelé groupe alterné de degré n et noté $\mathcal{A}_n$, est distingué. La relation d´équivalence sur $\mathcal{S}_n$: $\sigma \mathcal{R} \tau \Leftrightarrow \varepsilon(\sigma) = \varepsilon(\tau)$ est la relation de congruence modulo $ker(\varepsilon)$ et on définit à bon droit l´application $\overline{\varepsilon} : \mathcal{S}_n/\mathcal{A}_n \to \{-1, 1\}$, injective (par construction), surjective (comme ε). Par cette bijection, $\circ(\mathcal{A}_n) = \frac{n!}{2}$.
- Par le morphisme surjectif déterminant de $GL(n, \mathbb{C})$ (resp $O(n, \mathbb{R})$) sur $\mathbb{C}^*$ (resp $\mathbb{R}^*$), le groupe spécial linéaire $SL(n, \mathbb{C})$ ($SO(n, \mathbb{R})$) sont distingués.
- H étant distingué dans G, peut-on réaliser H comme noyau d´un morphisme de groupes de source G ?

Exercice 12 *Avec des notations évidentes, a-t-on* $H \lhd K \lhd G \Rightarrow H \lhd G$ *?*

On considère le groupe $GA(\mathbb{R})$ des bijections affines de $\mathbb{R}$: $f_{a,b} : x \mapsto ax + b$ avec $a \in \mathbb{R}^*$, $b \in \mathbb{R}$. Soit $T \equiv \mathbb{R}$ le sous-groupe des translations et $T_{\mathbb{Z}}$ le sous-groupe des $x \mapsto x + n$ ($n \in \mathbb{Z}$). Puisque T est commutatif, $T_{\mathbb{Z}} \lhd T$. Par ailleurs, T est le noyau du morphisme $f_{a,b} \mapsto a$ de $GA(\mathbb{R})$ sur $(\mathbb{R}^*, \times)$, donc T est distingué dans $GA(\mathbb{R})$. Enfin, l´égalité

$$f_{a,b} f_{1,n} {f_{a,b}}^{-1} = f_{a,b} f_{1,n} f_{\frac{1}{a}, \frac{-b}{a}} = f_{1,an}$$

valable pour $(a, b) \in \mathbb{R}^* \times \mathbb{R}$ et $n \in \mathbb{Z}$, montre que $T_{\mathbb{Z}} \not\lhd GA(\mathbb{R})$ puisqu´on peut choisir $a \in \mathbb{R}^*$ et $n \in \mathbb{Z}$ tels que $an \notin \mathbb{Z}$.

Exercice 13 *Si* G *est un groupe d´ordre pair* ($\circ(G) = 2n$)*, et si* H *est un sous-groupe de* G *d´ordre* n*, alors* H *est distingué dans* G*.*

Le nombre de classes de congruence modulo H est 2 selon le théorème de Lagrange. Soit $x \notin H$. H et xH constituent une partition de G. Pour $a \in H$,

1. Si $g \in H$, $gag^{-1} \in H$ puisque H, comme tout sous-groupe de G, est stable pour la lci.

2. Si $xax^{-1} \notin H$, xax^{-1} s´écrit xh, donc $ax^{-1} \in H$, $x^{-1} \in H$, $x \in H$ (stabilité de H pour le passage à l´inverse). Contradiction. On vient de vérifier que $\forall a \in H \quad xax^{-1} \in H$.
3. Si $g = xh$ avec $h \in H$, $gag^{-1} = x(hah^{-1})x^{-1}$, qui appartient bien à H d´après ce qui précède.

On peut montrer mieux :

Propriété 12 *Si H est un sous-groupe d´un groupe fini G, d´indice égal au plus petit diviseur premier de $\sharp(G)$, alors H est distingué dans G.*

Remarque : Peut-on omettre la précision "plus petit" ? Non ! Dans $\mathcal{S}_3$, considérer $\sigma = (1,2)$ et $\tau = (1,3)$. Le sous-groupe $< \sigma >$ est d´ordre 2 (d´indice 3) et $\tau \circ \sigma\tau^{-1} = (2,3) \notin < \sigma >$ montre que $< \sigma >$ n´est pas distingué dans $\mathcal{S}_3$.
Preuve : On va réaliser H comme noyau d´un "bon" morphisme de groupes. On note Q l´ensemble quotient $G/H = \{xH; x \in G\}$. Pour g fixé dans G et pour x et y dans G,

$$x \equiv y(H) \Leftrightarrow gx \equiv gy(H),$$

donc on définit correctement l´application injective $\phi_g : \bar{x} \mapsto \overline{gx}$ de Q dans Q. On envisage alors le morphisme de groupes (facile à vérifier) Φ[2] $: g \mapsto \phi_g$ de G dans le groupe $\mathcal{S}$ des permutations de Q. Pour $g \in G$,

$$g \in ker(\Phi) \Leftrightarrow \Phi(g) = Id \Rightarrow gH = H \Leftrightarrow g \in H,$$

donc $ker(\Phi) \subset H$. Par ailleurs,

$$\frac{\circ(G)}{\circ(ker(\Phi))} = \underbrace{\frac{\circ(G)}{\circ(H)}}_{p} \times \underbrace{\frac{\circ(H)}{\circ(ker(\Phi))}}_{\alpha \in \mathbb{N}^*}$$

et $\frac{\circ(G)}{\circ(ker(\Phi))} = \circ(Im(\Phi)) = \alpha p$ divise $\circ(\mathcal{S}) = p! = (p-1)! \times p$, donc $\alpha \mid (p-1)!$. Ainsi, si $\alpha \neq 1$, on choisit (et c´est possible) un diviseur premier de α qui est dans $\{1, ..., p-1\}$. Ce diviseur, qui est aussi un diviseur premier de $\circ(G) = \circ(ker(\Phi)) \times \alpha p$, est supérieur à p (plus petit diviseur premier de $\circ(G)$) : contradiction et $\alpha = 1$. On a donc $H = ker(\Phi)$.

Exercice 14 *Donner une condition nécessaire et suffisante pour qu´un sous-groupe $< \sigma >$ de G d´ordre 2 soit distingué dans G.*

(Réponse : $\sigma \in Z(G)$)

Exercice 15 *L´image directe (par un morphisme de groupes) d´un sous-groupe distingué est-elle distinguée ?*

Non : Considérer $\tau \in < (1,2) > \subset \mathcal{S}_3 \mapsto \tau \in \mathcal{S}_3$.

On dit qu´un groupe G est simple lorsque ses seuls sous-groupes distingués sont $\{1\}$ et G.

Exemple : Les groupes cycliques d´ordre premier sont simples, $\mathcal{S}_n$ $(n \geqslant 3)$ n´est pas simple.

[2] Action de G sur Q par translation

4.2 Centre d´un groupe

4.2.1 vu comme noyau

On peut vérifier que, pour tout $a \in G$, $\sigma_a : g \mapsto gag^{-1}$ est un automorphisme de G (dit automorphisme intérieur), et que $Int : a \mapsto \sigma_a$ est un morphisme de G dans le groupe $Aut(G)$ des automorphismes de G. Son noyau est $Z(G) = \{z \in G \setminus \forall g \in G \quad gz = zg\}$ et est appelé centre de G.

4.2.2 Centre du groupe linéaire et du groupe orthogonal

Soit $\mathbb{K}$ un corps commutatif et E un $\mathbb{K}$ -espace vectoriel. On note $\mathcal{L}(E)$ l´algèbre des endomorphismes de E et $GL(E)$ le groupe linéaire de E. Lorsque E est un espace euclidien ($\mathbb{R}$ -espace vectoriel de dimension finie muni d´un produit scalaire), on note $\mathcal{O}(E)$ le groupe orthogonal de E.

a) Caractérisation des homothéties

Lemme 3 (1) *Un endomorphisme f de E est une homothétie si, et seulement si,* (2) *pour tout $x \in E$, la famille $(x, f(x))$ est liée.*

L´implication (1) $\Rightarrow$ (2) est immédiate. On suppose à présent que pour tout $x \in E$, il existe un scalaire λ_x tel que $f(x) = \lambda_x x$. On choisit $x_0 \in E$, $x_0 \neq 0$, et on montre que $\lambda_x = \lambda_{x_0}$ pour tout $x \in E$. On distingue deux cas : $x \in \mathbb{K}\, x_0$ et (x, x_0) libre. Si $x = \mu x_0$ avec $\mu \in \mathbb{K}$, $f(x) = \mu\, \lambda_{x_0} x_0 = \lambda_{x_0}\, x$, ce qui conduit à $\lambda_x = \lambda_{x_0}$. Sinon, $\lambda_{x+x_0}(x + x_0) = f(x + x_0) = f(x) + f(x_0) = \lambda_x x + \lambda_{x_0} x_0$ et par liberté de (x, x_0), $\lambda_{x+x_0} = \lambda_x = \lambda_{x_0}$.

b) Théorèmes

Propriété 13 *On suppose E de dimension finie. Le centre de $GL(E)$ est le sous-groupe des homothéties de rapport non nul.*

Soit $f \in GL(E)$ telle que f commute avec tout élément de $GL(E)$. Si f n´est pas une homothétie, alors on peut trouver $x \in E$ tel que $(e_1 = x, e_2 = f(x))$ est libre. On complète (e_1, e_2) en une base $(e_1, e_2, e_3, ..., e_n)$. Soit $g \in \mathcal{L}(E)$ définie par $g(e_1) = g(x) = x = e_1$, $g(e_2) = x + f(x) = e_1 + e_2$, $g(e_i) = e_i$ pour $3 \leqslant i \leqslant n$. Si λ_1, ..., λ_n sont n réels vérifiant $\sum_{i=1}^{n} \lambda_i g(e_i) = 0$, alors

$$(\lambda_1 + \lambda_2)e_1 + \lambda_2 e_2 + ... + \lambda_n e_n = 0,$$

et puisque $(e_1, ..., e_n)$ est une base de E, $\lambda_1 + \lambda_2 = 0$, $\lambda_2 = 0$, ..., $\lambda_n = 0$. La famille $(g(e_i)$ est donc aussi libre donc g est un automorphisme linéaire de E. Ainsi, $x + f(x) = g(f(x)) = f(g(x)) = f(x)$ donc $x = 0$. Impossible puisque $(x, f(x))$ est libre.

Propriété 14 *On suppose E euclidien. Le centre de $\mathcal{O}(E)$ est $\{-Id, Id\}$.*

Clairement, $\{-Id, Id\} \subset Z(\mathcal{O}(E))$. Soit f une isométrie de E qui commute avec toutes les autres isométries. Pour D droite vectorielle de E, on note s_D la réflexion d´axe D. On a dans $\mathcal{O}(E)$:

$$s_{f(D)} = f \circ s_D \circ f^{-1} = s_D,$$

donc f laisse toute droite invariante : f est une homothétie. Son rapport est par nécessité 1 ou -1.

4.3 Equation des classes

On appelle centralisateur de a, le sous-groupe C_a de G formé des éléments g vérifiant $gag^{-1} = a$. C_a est formé des éléments qui commutent avec a. On vérifie facilement que

$$C_a = G \Leftrightarrow a \in Z(G) \Leftrightarrow \mathcal{O}_a = \{a\}.$$

L´application $\tau_a : g \mapsto gag^{-1}$ constitue un paramétrage de l´orbite $\mathcal{O}_a$, et pour mesurer le "surparamétrage", on définit sur G une relation déquivalence en posant

$$g\mathcal{R}_a g' \Leftrightarrow gag^{-1} = g'ag'^{-1}.$$

On vérifie que $\mathcal{R}_a$ est en fait la relation de congruence modulo C_a. Ainsi, par factorisation par le quotient, τ_a induit une bijection de G/C_a sur $\mathcal{O}_a$ et si G est fini :

$$\circ(G) = \circ(C_a)\, \sharp(\mathcal{O}_a).$$

Parmi les éléments de G, il y a les "solitaires", les éléments à classe de conjugaison ponctuelle. Ce sont les éléments du centre de G. Soit r le nombre d´orbites non réduites à un point et pour $1 \leqslant i \leqslant r$, a_i un représentant de chacune de ses classes. On a l´égalité

$$\circ(G) = \circ(Z(G)) + \sum_{i=1}^{r} [G : C(a_i)],$$

connue sous le nom équation des classes.

Pour une présentation limpide de ces concepts utilisant le langage des actions de groupes, cf [1].

4.4 Groupe quotient

Voici quelques résultats généraux ; Les preuves manquantes se trouvent par exemple dans [4].

a) Théorème d´isomorphisme

1. Les relations d´équivalence sur un groupe G compatibles avec la structure de groupe sont les relations modulo un sous groupe distingué de G.
2. Si H est un sous-groupe distingué de G, alors G/H muni de la l.c.i "$xH\,.\,yH = xyH$ " est un groupe d´élément neutre H. L´application $\Pi : x \mapsto \overline{x} = xH$ est un morphisme surjectif de G sur G/H, de noyau H.
3. Premier théorème d´isomorphisme : Si $f : G \to G'$ est un morphisme de groupes, alors $ker(f)$ est distingué dans G et le groupe quotient $G/ker(f)$ est isomorphe à $Im(f)$. En particulier, $\mathcal{S}_n/\mathcal{A}_n \equiv \mathbb{Z}\ /2\mathbb{Z}$.
4. On note $Aut(G)$ le groupe des automorphismes de G et $Int(G)$ le sous-groupe des automorphismes intérieurs de G. Montrer que $G/Z(G) \equiv Int(G)$. On pourra considérer le morphisme $Int : a \mapsto [\sigma_a : g \mapsto gag^{-1}]$ de G dans $Aut(g)$.

Remarque : Si G est un groupe d´ordre pair et si H est un sous-groupe de G d´indice 2, alors H est distingué dans G (déjà vu) et contient tous les carrés de G. En effet, on a $G/H \equiv \mathbb{Z}\ /2\mathbb{Z}$ et $\forall x \in G \quad \bar{x}^2 = \bar{x^2} = \bar{1}$ donc $x^2 \in H$. En particulier, si $\mathcal{A}_4$ d´ordre 12 possède un sous-groupe H d´ordre 6, alors H qui contient tous les carrés, contient tous les 3-cycles ($c^3 = 1 \Rightarrow c = (c^{-1})^2$) au nombre de $2 \times C_4^3 = 8$. Impossible !

b) Groupe dérivé
Dans un groupe G, un élément g est dit commutateur s´il existe x et y dans G tels que $g = xyx^{-1}y^{-1}$. Le groupe engendré par les commutateurs est appelé groupe dérivé de G et noté $D(G)$.

1. Pour f morphisme de G dans un autre groupe,

$$Im(f) \text{ est commutatif si, et seulement si, } D(G) \subset ker(f).$$

2. Un sous-groupe H de G qui contient $D(G)$ est distingué et vérifie : G/H est abélien.

   Preuve : Pour $g \in G$ et $h \in H$, $xhx^{-1} = xh(x^{-1}h^{-1}hx)x^{-1} = (xhx^{-1}h^{-1})(hxx^{-1}) = (xhx^{-1}h^{-1})\ h$, qui est bien dans H. On envisage alors la surjection canonique $p : x \mapsto \overline{x}$ de noyau $ker(p) = H$. Puisque $ker(p)$ contient $D(G)$, $Im(p) = G/H$ est commutatif.

3. $D(G)$ est le plus petit sous-groupe distingué de G (pour l´inclusion) dont le quotient est commutatif.

5 A propos de $\mathcal{A}_5$

5.1 Centre de $\mathcal{A}_5$

Propriété 15 *Pour $n \geqslant 4$, le centre de $\mathcal{A}_n$ est trivial.*

Soit $\sigma \in \mathcal{A}_n$, $\sigma \neq Id$, i tel que $\sigma(i) = j \neq i$, k tel que $k \neq i, j$, soit l tel que $l \neq i, j, k$ et enfin $\tau = (j, k)(k, l) \in \mathcal{A}_n$. Les égalités $\sigma\tau(i) = \sigma(i) = j$ et $\tau\sigma(i) = \tau(j) = k$ montrent que $\sigma \notin Z(\mathcal{A}_n)$.

5.2 Groupe dérivé de $\mathcal{A}_5$

On veut déterminer le groupe dérivé de $\mathcal{A}_5$.

Lemme 4 *Les 3-cycles sont conjugués dans $\mathcal{A}_5$ (dans $\mathcal{A}_n$ pour $n \geqslant 5$).*

Soit $\tau = (a, b, c)$ et $\tau' = (a', b', c')$ deux 3-cycles. Soit $\sigma \in \mathcal{S}_5$ telle que $a \mapsto a'$, $b \mapsto b'$ et $c \mapsto c'$. Si $\sigma \in \mathcal{A}_5$, c´est fini puisque $\sigma\tau\sigma^{-1} = \tau'$. Sinon, en écrivant $\{1, ..., 5\} = \{a, b, c, d, e\}$, on pose $\sigma' = (d, e)\sigma \in \mathcal{A}_5$ et on a $\sigma'\tau{\sigma'}^{-1} = \tau'$.

Lemme 5 *Pour $n \geqslant 3$, les 3-cycles engendrent $\mathcal{A}_n$.*

On sait que $\mathcal{A}_n$ est engendré par les produits de deux transpositions. Or, avec des notations évidentes, $(a, b)(b, c) = (b, a)(b, c) = (b, a)(c, b) = (a, b, c)$, et $(a, b)(c, d) = (a, c, b)(a, c, d)$, donc les 3-cycles sont dans $\mathcal{A}_n$ et engendrent $\mathcal{A}_n$.

Propriété 16
Pour $n \geqslant 5$, on a : $D(\mathcal{A}_n) = \mathcal{A}_n$.

Un 3-cycle σ et son carré (qui est aussi un 3-cycle) sont conjugués dans $\mathcal{A}_n$ donc $\sigma^2 = \tau^{-1}\sigma\tau$ avec $\tau \in \mathcal{A}_n$. Ainsi, le 3-cycle $\sigma = \sigma^{-1}\tau\sigma\tau$ est un commutateur. Puisque les 3-cycles engendrent $\mathcal{A}_n$, on a bien : $D(\mathcal{A}_n) = \mathcal{A}_n$.

5.3 Simplicité de $\mathcal{A}_5$

La taille des orbites (pour la relation de conjugaison), comme la grosseur du centre et du groupe dérivé, mesure le défaut de commutativité d´un groupe. Par exemple, si G est commutatif, les classes de conjugaison sont des singletons (au nombre de $\sharp(G)$). Dans un groupe "fortement non commutatif", les sous-groupes distingués sont à chercher parmi les gros sous-groupes de G, restriction qui laisse penser que les sous-groupes distingués y sont peu nombreux. Aussi, malgré l´exemple des groupes cycliques d´ordre premier, on peut s´attendre à trouver des groupes simples parmi les groupes fortement non commutatifs.

Propriété 17 *Le groupe $\mathcal{A}_5$ est simple.*

Première preuve : Vive Lagrange
On sait que $\mathcal{A}_5$ a $\frac{5!}{2} = 60$ éléments. Les 3-cycles et 5-cycles de $\mathcal{S}_5$ sont pairs puisque ce sont des carrés ($c^3 = 1 \Rightarrow c = (c^{-1})^2$ et $c^5 = 1 \Rightarrow c = (c^{-1})^2$). Dans $\mathcal{A}_5$, il y a :

- le neutre
- les produits de deux transpositions disjointes (d´ordre 2), au nombre de $\frac{C_5^2 C_3^2}{2} = 15$ (! : $(a,b)(c,d) = (c,d)(a,b)$)
- les 3-cycles au nombre de $C_5^3 \times 2 = 20$ (pour un même support, on a deux 3-cycles distincts)
- les 5-cycles au nombre de $4 \times 3 \times 2 \times 1 = 24$.

On a listé 60 éléments, on a donc toutes les permutations de $\mathcal{A}_5$.

Lemme 6 *Les produits de deux transpositions à supports disjoints sont conjugués dans $\mathcal{A}_5$.*

Soit $\tau = (a,b)(c,d)(e)$ et $\tau' = (a',b')(c',d')(e')$. Soit σ dans $\mathcal{S}_5$ envoyant $\square$ sur $\square'$, et $\sigma' = (c',d')\sigma$. On a $\sigma\tau\sigma^{-1} = \sigma'\tau\sigma'^{-1} = \tau'$ avec $\sigma \in \mathcal{A}_5$ ou $\sigma' \in \mathcal{A}_5$. D´où le résultat.

Lemme 7 *Si $\tau = (a,b,c,d,e)$ et $\tau' = (a',b',c',d',e')$ sont des 5-cycles, alors τ' est conjugué avec τ ou $\tau^2 = (a,c,e,b,d)$ dans $\mathcal{A}_5$.*

Soit $\sigma \in \mathcal{S}_5$ envoyant $\square$ sur $\square'$, et $\sigma' = (c',e')(b',c')(b',d')\sigma$. On vérifie que $\sigma\tau\sigma^{-1} = \sigma'\tau\sigma'^{-1} = \tau'$ avec σ ou σ' dans $\mathcal{A}_5$. D´où le résultat.

Retour preuve : Soit H un sous-groupe distingué de $\mathcal{A}_5$, distinct de $\{1\}$. Si H contient un 3-cycle (respectivement un élément d´ordre 2), il contient sa classe de conjugaison et donc tous les 3-cycles (respectivement tous les produits de deux transpositions disjointes). Si H contient un 5-cycle τ, il contient aussi τ^2, et contient donc n´importe quel 5-cycle τ'. Ainsi H contient le neutre et au moins deux permutations d´ordres différents. Sinon, $\sharp(H) = 1 + 24 = 25$, ou $\sharp(H) = 1 + 20 = 21$, ou $\sharp(H) = 1+15 = 16$. Impossible puisque 25, 21 et 16 ne divisent pas 60. Il suit : $\sharp(H) \geqslant 1+15+20 = 36$ et toujours avec Lagrange, nécessairement $\sharp(H) = 60$, $H = \mathcal{A}_5$.

Deuxième preuve : Vive le 3-cycle
Soit H un sous-groupe distingué de $\mathcal{A}_5$, distinct de $\{1\}$. Si H contient un 3-cycle, il contient tous les 3-cycles, donc $H = \mathcal{A}_5$. Si H contient un 5-cycle $\tau = (a,b,c,d,e)$, il contient le commutateur $(a,b,c)\tau(a,b,c)^{-1}\tau^{-1}$ qui est le 3-cycle (a,b,d). Le sous-groupe H contient alors tous les 3-cycles et $H = \mathcal{A}_5$. Enfin, si H contient un produit de 2 transpositions disjointes $\tau = (a,b)(c,d)$, il contient

le commutateur $\tau(a,b,e)\tau^{-1}(a,b,e)^{-1} = (a,b)(c,d)(a,b,e)(a,b)(c,d)(e,b,a) = (a,b,d)$ donc $H = \mathcal{A}_5$.
Remarque : Autre exemple de groupe ne possédant pas un sous-groupe d´ordre égal à un diviseur de l´ordre du groupe : $\mathcal{A}_5$ simple n´a pas de sous-groupe d´ordre 30.

5.4 Sous-groupes distingués de $\mathcal{S}_5$

Si $H \neq \{1\}$ est un sous-groupe distingué de $\mathcal{S}_5$, $H \cap \mathcal{A}_5$ est distingué dans $\mathcal{A}_5$ (importance de $\mathcal{A}_5 \lhd \mathcal{S}_5$), et puisque $\mathcal{A}_5$ est simple, $H \cap \mathcal{A}_5 = \mathcal{A}_5$ ou $\{1\}$. Si $H \cap \mathcal{A}_5$ est trivial, la restriction de la signature à H est injective, et même surjective puisque $H \neq \{1\}$, donc H a 2 éléments 1 et σ, où $\circ(\sigma) = 2$. Avec $H \lhd \mathcal{S}_5$, on a nécessairement $\tau \circ \sigma \circ \tau^{-1} = \sigma$ pour $\tau \in \mathcal{S}_5$, donc σ est dans le centre de $\mathcal{S}_5$: $\sigma = 1$. Contradiction ! Ainsi, $H \cap \mathcal{A}_5 = \mathcal{A}_5$, $\mathcal{A}_5 \subset H$. Premier cas : $H = \mathcal{S}_5$. Sinon, par Lagrange, $\circ(H) \leqslant \frac{n}{2}$, et par nécessité, $\circ(H) = \frac{n}{2}$ et $H = \mathcal{A}_5$.

Propriété 18 *Les seuls sous-groupes distingués de $\mathcal{S}_5$ sont $\{1\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$.*

On admet que

Propriété 19

- *Pour $n \geqslant 5$, $\mathcal{A}_n$ est simple.*
- *Les seuls sous-groupes distingués de $\mathcal{S}_n$ sont $\{1\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.*

Le groupe alterné $\mathcal{A}_n$ est un sous-groupe de $\mathcal{S}_n$ d´indice 2 (en fait, c´est le seul, cf propriete 29 page 33), et $\mathcal{S}_n$ possède des sous-groupes d´indice n (par exemple, $H_n = \{\sigma \in \mathcal{S}_n \ ; \ \sigma(n) = n\}$). Voici un résultat surprenant :

Application 2 *(Saut d´indice dans $\mathcal{S}_n$)*
Pour $n \geqslant 5$, si H est un sous-groupe de $\mathcal{S}_n$ d´indice $[\mathcal{S}_n : H] = N > 2$, alors $[\mathcal{S}_n : H] = N \geqslant n$

L´idée est de contruire une injection entre $\mathcal{S}_n$ (d´ordre $n!$) et le groupe des permutations de $Q = \mathcal{S}_n/H$ (de cardinal $N!$). On envisage le morphisme Φ[3] : $s \mapsto [\sigma H \mapsto s\sigma H]$ de $\mathcal{S}_n$ vers $\mathcal{S}_Q$. On choisit à bon droit 3 éléments distincts de Q : H, $\sigma_1 H$ et $\sigma_2 H$. Clairement, les 3 permutations Id, $\Phi(\sigma_1)$, $\Phi(\sigma_2)$ de $\mathcal{S}_Q$ sont distinctes donc $\sharp(Im(\Phi)) \geqslant 3$. Ainsi, $Ker(\Phi)$ est un sous-groupe distingué de $\mathcal{S}_n$ d´indice supérieur à 3, donc $Ker(\Phi) = \{1\}$ et Φ est injective. D´où $n! \leqslant N!$, $n \leqslant N$.

6 L´ensemble K des carrés non nuls du corps $\mathbb{Z}\ /p\mathbb{Z}$

Soit $p > 2$ un nombre premier. Certains résultats algébriques valables dans $\mathbb{R}$ ou $\mathbb{C}$ sont corrects dans le corps $\mathbb{Z}/p\mathbb{Z}$. On peut par exemple faire de l´algèbre linéaire et étudier les systèmes $AX = B$ où $A \in GL(n, \mathbb{Z}/p\mathbb{Z})$ et $B \in \mathbb{Z}/p\mathbb{Z}^n$. On peut aussi s´intéresser à des équations non linéaires, par exemple celles du second degré. Les formules usuelles avec discriminant, sont encore d´actualité et on est alors amené à considérer les éléments de $\mathbb{Z}/p\mathbb{Z}$ qui sont des carrés. On pose : $K = \{x^2 \ ; \ x \in \mathbb{Z}/p\mathbb{Z}^*\}$.

[3] Action de $\mathcal{S}_n$ sur Q

6.1 Morphisme de $\mathbb{Z}/p\mathbb{Z}^*$ sur $\{-1,1\}$

Si $\varphi : \mathbb{Z}/p\mathbb{Z}^* \to \{-1,1\}$ est un morphisme de groupes non trivial, φ est alors surjective et son noyau est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}^*$ d´indice 2. Or le groupe $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique et d´ordre pair, donc (cf page 5) $\mathbb{Z}/p\mathbb{Z}^*$ ne possède qu´un seul sous-groupe $\mathcal{K}$ d´ordre $\frac{p-1}{2}$. On écrit alors $\mathbb{Z}/p\mathbb{Z}^* = \mathcal{K} \cup x\mathcal{K}$ où x a été choisi en dehors de $\mathcal{K}$ et φ envoie nécessairement tout y de $\mathcal{K}$ sur 1 et tout $y \in x\mathcal{K}$ sur -1. On a montré qu´il existe au plus un morphisme non trivial de $\mathbb{Z}/p\mathbb{Z}^*$ sur $\{-1,1\}$.

6.2 Un paramétrage de K

On considère l´application $f : x \mapsto x^2$ de $\mathbb{Z}/p\mathbb{Z}^*$ dans lui-même. On vérifie que f est un morphisme de groupes (pour la loi multiplicative), d´image K et de noyau $ker(f) = \{-1,1\}$ (avec $1 \neq -1$ puisque $p > 2$).

Propriété 20 *Dans $\mathbb{Z}/p\mathbb{Z}^*$, il y a autant de carrés que de non-carrés : K a $\frac{p-1}{2}$ éléments.*

Exercice 16 *Soit $p > 2$ premier, a et b dans $\mathbb{Z}/p\mathbb{Z}^*$. Alors il existe x et y dans $\mathbb{Z}/p\mathbb{Z}$ tels que $ax^2 + by^2 = 1$.*

Dans $\mathbb{Z}/p\mathbb{Z}$, il y a $1 + \frac{p-1}{2} = \frac{p+1}{2}$ carrés (on n´oublie pas 0 !), et par intégrité du corps $\mathbb{Z}/p\mathbb{Z}$, les ensembles $X = \{ax^2 \ ; \ x \in \mathbb{Z}/p\mathbb{Z}\}$ et $Y = \{1 - by^2 \ ; \ y \in \mathbb{Z}/p\mathbb{Z}\}$ ont aussi $\frac{p+1}{2}$ éléments, ce qui assure $X \cap Y \neq \oslash$.

6.3 Comment reconnaitre les carrés ?

Pour $x \in \mathbb{Z}/p\mathbb{Z}^*$, on pose $\phi(x) = x^{\frac{p-1}{2}}$. Par le petit théorème de Fermat ou théorème de Lagrange dans $(\mathbb{Z}/p\mathbb{Z}^*, \times)$, le morphisme de groupes ϕ "tue" les éléments de K. Y a-t-il d´autres éléments dans $ker(\phi)$? Le polynôme $X^{\frac{p-1}{2}} - 1$ à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}$ a au plus $\frac{p-1}{2}$ racines distinctes, d´où la caractérisation des carrés de K :

Propriété 21

- *Pour $x \in \mathbb{Z}/p\mathbb{Z}^*$, $x \in K$ si, et seulement si, $x^{\frac{p-1}{2}} = 1$.*
- *L´application $\left(\frac{\bullet}{p}\right) : x \mapsto x^{\frac{p-1}{2}}$, appelée symbole de Legendre, est le seul morphisme non trivial de $\mathbb{Z}/p\mathbb{Z}^*$ sur $\{-1,1\}$.*

En particulier,

Propriété 22 *-1 est un carré si, et seulement si, $p \equiv 1(4)$.*

Remarque : Une preuve élégante de ce résultat est donné dans RMS-mars-1986 : on envisage sur $\mathbb{Z}/p\mathbb{Z}^*$ la relation d´équivalence $x \Re y \Leftrightarrow y \in \{x, -x, x^{-1}, -x^{-1}\}$, on montre qu´il y a une seule classe à deux éléments (si -1 n´est pas un carré de $\mathbb{Z}/p\mathbb{Z}^*$) ou deux classes à deux éléments (si -1 est un carré), les autres classes au nombre de k ayant 4 éléments ; Cette partition de $\mathbb{Z}/p\mathbb{Z}^*$ donne alors : $p - 1 = 2 + 4k$ ou $p - 1 = 2 + 2 + 4k$...

6.4 Symbole de Zolotareff

Soit p un nombre premier impair. Pour n entier premier avec p, on note $\Pi_{n,p}$ la multiplication par n modulo p (endomorphisme du groupe additif $\mathbb{Z}/p\mathbb{Z}$). Puisque le corps $\mathbb{Z}/p\mathbb{Z}$ est intègre, le morphisme $\Pi_{n,p}$ est injectif, donc est une permutation de $\mathbb{Z}/p\mathbb{Z}$. Au passage, on a $(p-1)! = n2n...(p-1)n$ d´où : $(n^{p-1}-1)(p-1)! = 0(p)$ et on retrouve :

$$n^{p-1} = 1(p) \quad (\textit{petit théorème de Fermat}).$$

On définit le symbole de Zolotareff $(n \mid p)$ comme étant la signature de $\Pi_{n,p}$. On a, par exemple, $(-1 \mid p) = (-1)^{\frac{p-1}{2}}$ (décomposer $\Pi_{-1,p} = (1, p-1)(2, p-2)...(\frac{p-1}{2}, \frac{p+1}{2})$, d´où l´équivalence

$$(-1 \mid p) = 1 \Leftrightarrow p \equiv 1(4).$$

Par ailleurs, pour $(n, m) \in \mathbb{Z}^2$, $n \wedge p = 1$, $m \wedge p = 1$, on a : $nm \wedge p = 1$ et $\Pi_{nm,p} = \Pi_{n,p} \circ \Pi_{m,p}$ donc par le morphisme signature, le symbole de Zolotareff est multiplicatif.

Propriété 23 *(Lemme de Zolotareff)*
Soit $p > 2$ premier et n un entier premier à p. La signature $(n \mid p)$ de la multiplication $\Pi_{n,p}$ par n, est égale au symbole de Legendre $\left(\frac{n}{p}\right)$.

Soit x un générateur de $\mathbb{Z}/p\mathbb{Z}^*$. On écrit $n = x^k$ avec $k \in \mathbb{Z}$ et la multiplication par n est l´itérée $(\Pi_{x,p})^k$. Que vaut la signature $\varepsilon(\Pi_{x,p})$? Si on écrit $\mathbb{Z}/p\mathbb{Z} = \{0, x, x^2, ..., x^{p-1} = 1\}$, la multiplication par x est un $(p-1)$-cycle, donc est impaire. Ainsi $\varepsilon(\Pi_{n,p}) = (-1)^k$. Par ailleurs, le symbole de Legendre $\left(\frac{n}{p}\right)$ est : $n^{\frac{p-1}{2}} = \left(x^{\frac{p-1}{2}}\right)^k$. Or x n´est pas un carré modulo p (sinon, tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ seraient des carrés), donc $\left(\frac{n}{p}\right) = (-1)^k$. D´où le résultat.

7 Groupes d´ordre p^2

7.1 Détermination des groupes d´ordre 4

Les 2 modèles
Soit G un groupe d´ordre 4 non cyclique. L´ordre de tout élément distinct de 1 est un diviseur de 4, autre que 1 et 4 : c´est 2. On peut donc écrire $G = \{1, a, b, c\}$ où $a^2 = b^2 = c^2 = 1$. L´élément ab est clairement distinct de 1, a, b, ce qui impose $ab = c$. On fabrique ainsi sans problème la table de composition de G. Par ailleurs, on construit un isomorphisme ϕ de G sur le groupe additif $\mathbb{Z}\ /2\mathbb{Z}\ \times\ \mathbb{Z}\ /2\mathbb{Z}$ en posant $\phi(1) = (0,0)$, $\phi(a) = (1,0)$, $\phi(b) = (0,1)$, $\phi(c) = (1,1)$. G est appelé groupe de Klein et noté V_4 (Vierergruppe).

Une réalisation de V_4 : Dans le groupe $\mathcal{A}_4$ (groupe alterné de degré 4),
- les produits de 2 transpositions disjointes (qui sont d´ordre 2)

$$u = (1,2)\,(3,4), \quad v = (1,3)\,(2,4), \quad w = (1,4)\,(2,3)$$

- et Id

forment un sous-groupe dont aucun élément n´est d´ordre 4 : c´est V_4.
On peut noter que , pour a, b, c, d distincts dans $\{1, 2, 3, 4\}$ et pour σ dans $\mathcal{A}_4$ (resp $\mathcal{S}_4$),

$$\sigma\,(a,b)\,(c,d)\,\sigma^{-1} = \sigma\,(a,b)\,\sigma^{-1}\sigma\,(c,d)\,\sigma^{-1} = (\sigma(a),\sigma(b))\,(\sigma(c),\sigma(d)).$$

Ceci prouve que V_4 est distingué dans $\mathcal{A}_4$ (resp dans $\mathcal{S}_4$) et que $\mathcal{A}_4$ n´est pas simple.
Remarque : On illustre une nouvelle fois la non-transitivité de $\lhd$: Le sous-groupe $< u = (1,2)(3,4) >$ est distingué dans V_4, lui-même distingué dans $\mathcal{A}_4$, et pourtant $< (1,2)(3,4) >$ n´est pas distingué dans $\mathcal{A}_4$. En effet :

$$(1,3)\ (1,2)(3,4)\ (1,3) = (1,4)(2,3) \notin < (1,2)(3,4) > .$$

Exercice 17 *Puisque $\{u, v, w\}$ est une classe de conjugaison dans $\mathcal{S}_4$, on définit à bon droit l´application*

$$^4\Phi\ :\ \sigma \mapsto \begin{cases} \{u,v,w\} & \to \{u,v,w\} \\ z & \mapsto \sigma z \sigma^{-1} \end{cases},$$

qui est morphisme de groupes de $\mathcal{S}_4$ dans $\mathcal{S}_{\{u,v,w\}} \equiv \mathcal{S}_3$. On vérifie que chaque transposition de $\mathcal{S}_{\{u,v,w\}}$ est atteinte ; Par exemple, $< v, w >= \Phi(< 1, 2 >)$. Ainsi, Φ est surjective (puisque $\mathcal{S}_{\{u,v,w\}}$ est engendré par ses transpositions), ce qui donne : $\sharp(ker(\Phi)) = \frac{4!}{3!} = 4$. Or, $V_4 = \{Id, u, v, w\} \subset ker(\Phi)$, d´où :

$$ker(\Phi) = V_4 \qquad et \qquad \mathcal{S}_4/V_4 \equiv \mathcal{S}_3.$$

Interprétation (M. Alessandri) : "il y a 3 facons de grouper 4 objets distincts deux par deux. Une permutation de ces 4 objets induit une permutation des 3 facons de les grouper."

Une réalisation géométrique de V_4
Dans le plan affine euclidien, $ABCD$ désigne un rectangle non carré de centre O. On cherche l´ensemble $\mathcal{I}$ (en fait le groupe) des isométries affines conservant globalement $ABCD$. On admet que les éléments de $\mathcal{I}$ sont exactement les isométries conservant les 4 sommets A, B, C et D. Soit $f \in \mathcal{I}$. L´application affine f conserve le barycentre donc $f(O) = O$. Par conservation des longueurs, l´image de $[AB]$ est soit $[AB]$, soit $[CD]$.

- Si $f([AB]) = [AB]$, alors le milieu I de $[AB]$ est fixé. Ainsi la droite (OI) est fixée : $f = Id$ ou f est la réflexion s d´axe (OI).
- Si $f([AB]) = [CD]$, alors A est envoyé sur C ou D.
  - Si $A \mapsto C$, en notant s_O la symétrie centrale de centre O, $s_O \circ f$ fixe A et O, donc $s_O \circ f = Id$, ou $s_O \circ f$ est la réflexion d´axe (AC). Ce dernier cas est impossible : B serait envoyé sur D, les diagonales (AC) et (BD) seraient perpendiculaires, ce qui est exclu puisque $ABCD$ est supposé non carré. Ainsi $f = s_O$.
  - Si $A \mapsto D$, puisque $AD = Df(D)$, $f(D)$ est nécessairement A. Ainsi le milieu J de $[AD]$ est fixé. On a alors $f = Id$ ou f est la réfléxion d´axe (OJ).

On vérifie réciproquement que les involutions Id, s_O, $s_{(OI)}$ et $s_{(OJ)}$ sont dans $\mathcal{I}$ d´où :

$$\mathcal{I} = \{Id, s_O, s_{(OI)}, s_{(OJ)}\} \equiv V_4.$$

[4] Action de $\mathcal{S}_4$ sur $\{u, v, w\}$ par conjugaison

Sous-groupes du groupe quaternionique $\mathcal{H}_8$: On peut montrer que dans $GL(2,\mathbb{C})$, les matrices I_2, $-I_2$, $a = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & \text{-i} \end{pmatrix}$, $-a$, $b = \begin{pmatrix} 0 & 1 \\ \text{-1} & 0 \end{pmatrix}$, $-b$, $c = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$, et $-c$ forment un groupe noté $\mathcal{H}_8$ et appelé groupe quaternionique. Soit H un sous-groupe de $\mathcal{H}_8$. Si $H \neq \{1\}$ et $H \neq \mathcal{H}_8$, H a 2 ou 4 éléments.

- Si $H = \{I_2, \gamma\} \equiv \mathbb{Z}/2\mathbb{Z}$, alors $\gamma \neq I_2$ vérifie $\gamma^2 = I_2$. Or le seul élément de H d´ordre 2 est $-I_2$. Ainsi $H = \{I_2, -I_2\}$ et $\forall g \in \mathcal{H}_8 \quad \forall h \in H \quad ghg^{-1} = h \in H$.
- Si H est d´ordre 4 (nécessairement isomorphe à $\mathbb{Z}/4\mathbb{Z}$ puisque le seul élément d´ordre 2 dans $\mathcal{H}_8$ est $-I_2$), il est d´indice 2 dans $\mathcal{H}_8$, et donc distingué dans $\mathcal{H}_8$. Le sous-groupe $< a >$ est un exemple de sous-groupe de $\mathcal{H}_8$ d´ordre 4.

Bilan : Le groupe $\mathcal{H}_8$ est non commutatif et pourtant tous ses sous-groupes sont distingués. Cela laisse penser que $\mathcal{H}_8$ est un groupe des plus commutatifs parmi les groupes non commutatifs. Voici aussi un exemple de groupe non cyclique dont tous les sous-groupes propres sont cycliques.

Exercice 18 *Montrer que $D(\mathcal{H}_8) = \{I_2, -I_2\}$. Reconnaitre le quotient $\mathcal{H}_8/D(\mathcal{H}_8)$.*

$\mathcal{H}_8/\{I_2, -I_2\}$, qui est d´ordre 4, est commutatif (isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou V_4) donc $D(\mathcal{H}_8) \subset \{I_2, -I_2\}$. ainsi, $D(\mathcal{H}_8) = \{I_2\}$ ou $\{I_2, -I_2\}$. Or $D(\mathcal{H}_8) \neq \{I_2\}$ (sinon $\mathcal{H}_8$ serait commutatif), donc

$$D(\mathcal{H}_8) = \{I_2, -I_2\}.$$

Pour tout $g \in \mathcal{H}_8$, $g^2 = I_2$ ou $g^2 = -I_2$, donc tout élément de $\mathcal{H}_8/\{I_2, -I_2\}$ est involutif. Ainsi, $\mathcal{H}_8/\{I_2, -I_2\}$, qui est d´ordre 4, est isomorphe à V_4.

Remarque : Pour tout sous-groupe H de $\mathcal{H}_8$, $H \cap \{I_2, -I_2\} \neq \{I_2\}$. On dit que le sous-groupe $\{I_2, -I_2\}$ est dense dans $\mathcal{H}_8$. On note également que tout sous-groupe H contient $D(\mathcal{H}_8)$ et on retrouve ainsi que H est distingué dans $\mathcal{H}_8$.

Exercice 19 *Soit G un groupe fini et D un sous-groupe de G contenant tous les éléments de G d´ordre premier. Montrer que D est dense dans G.*

Soit H un sous-groupe de G non trivial. Soit $h \in H$, $h \neq 1$. On suppose $h \notin D$. On appelle δ l´ordre de h, qui n´est pas premier. On choisit alors un diviseur d premier de δ, et un $g \in < h >$ d´ordre d. L´élément g est dans H et dans D (par hypothèse).

7.2 Détermination des groupes d´ordre 9

Soit G un groupe d´ordre 9. Si G n´est pas cyclique, tout élément x de $G \setminus \{1\}$ est d´ordre 3. Soit $a \in G \setminus \{1\}$ et $b \in G \setminus \{1, a\}$. On a $a^2 = a^{-1} \neq b$ et $b^2 = b^{-1} \neq a$, donc le sous-groupe $< a, b >$ engendré par a et b contient les 9 éléments distincts $\{1, a, a^2, b, b^2, ab, ab^2, a^2b, a^2b^2\}$.
Ainsi $G =< a, b >$. L´élément ba, clairement distinct de 1, a, a^2, et b^2, appartient donc à $\{ab, a^2b, ab^2, a^2b^2\}$.

- Si $ba = a^2b^2$, alors $(ba)^2 = baba = a^2b^2ba = a^2b^3a = a^3 = 1$, donc $\circ(ba) = 2$. Impossible puisque 2 ne divise pas 9.
- Si $ba = ab^2$, alors $(ba)^2 = baba = ab^3a = a^2$. Il vient $(ba)^3 = b^2$, $(ba)^5 = a^2b^2$, $(ba)^6 = baa^2b^2 = 1$, ce qui est impossible puisque 6 ne divise pas 9.

– On montre de même que si $ba = a^2b$, alors $(ba)^6 = 1$, ce qui est impossible.

Bilan : les générateurs a et b de G commutent donc G est abélien. On envisage alors l´application

$$\phi :< a > \times < b > \rightarrow G = \{1, a, a^2, b, b^2, ab, ab^2, a^2b, a^2b^2\}.$$

ϕ est un morphisme de groupe (G commutatif), surjectif ;
Puisque $< a > \times < b >$ et G ont même cardinal, ϕ réalise un isomorphisme de groupe entre $< a > \times < b >$ et G, ce qui peut s´écrire : $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq G$.

7.3 Cas général

Lemme 8 *(Centre d´un p-groupe)*
Soit p un entier premier, $k \in \mathbb{N}^*$ et G un groupe d´ordre p^k. On dit que G est un p-groupe. Alors le centre de G n´est pas trivial.

Avec l´équation aux classes, on a $p^k = \circ(Z(G)) + \sum_{x \in T} [G : C_x]$ où T désigne une transversales aux classes de conjugaison non ponctuelles. Or pour $x \in T$, $[G : C_x] > 1$ et $[G : C_x] \mid p^k$, donc $p \mid \circ(Z(G))$, donc $\circ(Z(G)) \geqslant p$.
Exemple : Le centre Z de $\mathcal{H}_8$ a 2 ou 4 éléments. Clairement $\{I_2, -I_2\} \subset Z$. Si $\circ(Z) = 4$, on choisit $x \in \mathcal{H}_8 \setminus Z$ et $Z \subsetneq Z \cup \{x\} \subset C_x$ donne $C_x = \mathcal{H}_8$ (avec Lagrange), donc x commute avec tous les éléments de $\mathcal{H}_8$. Absurde puisque $x \notin Z$. Ainsi $\circ(Z) = 2$ et $Z = \{I_2, -I_2\}$.

Exercice 20 *Un groupe G d´ordre p^k (p premier, $k \geqslant 2$) n´est pas simple.*

1. On suppose G abélien. Soit $x \in G$, $x \neq 1$. Si $< x > \neq G$, $< x >$ convient. Sinon, $< x^p >$ convient.
2. Si G n´est pas commutatif, on a $Z(G) \neq G$, $Z(G) \neq \{1\}$ et $Z(G)$ distingué dans G.

Lemme 9 *Si p est premier et si G est un groupe d´ordre p^2, alors G est commutatif.*

On raisonne par l´absurde ; Soit $x \in G \setminus Z(G)$. Le centralisateur C_x contient $Z(G)$ (donc au moins p éléments), et $x \notin Z(G)$, donc $\circ(C_x) \geqslant p + 1$, et puisque $\circ(C_x) \mid \circ(G)$, on a $\circ(C_x) = p^2$, $C_x = G$, $x \in Z(G)$. Contradiction.

Autre justification : On commence par un lemme (admis) :

Lemme 10 *Si $G/Z(G)$ est cyclique, alors G est commutatif.*

On raisonne encore par l´absurde ; Si G n´est pas commutatif, alors $Z(G)$ non trivial est d´ordre p. Le groupe $G/Z(G)$ est alors d´ordre p premier, donc cyclique, donc G est commutatif. Contradiction.

Propriété 24 *Soit p premier. Il y a 2 modèles de groupes d´ordre p^2 (tous deux commutatifs) : le groupe cyclique $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

On suppose G non cyclique. Soit $a \in G$, $a \neq 1$. On a $\circ(a) = p$. Soit à présent $b \in G$ tel que $b \notin < a >$. On remarque qu´on a aussi $\circ(b) = p$. On envisage alors l´application $\phi :< a > \times < b > \rightarrow G$ définie par $\phi((x, y)) = xy$. Avec G commutatif, on vérifie facilement que ϕ est un morphisme de groupe. Son image est un sous-groupe de G qui contient $\{1, a, .., a^{p-1}, b\}$, donc plus de $p+1$ éléments. Comme son cardinal vaut p ou p^2, c´est p^2. Ainsi ϕ est surjective et $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Si G est un groupe d´ordre p^2 et H un sous-groupe propre de G, alors l´ordre de H est p et H est cyclique. Voici donc un exemple de groupe *commutatif* non-cyclique dont tous les sous-groupes propres sont cycliques.

7.4 Réciproque de Lagrange dans les p-groupes

Propriété 25 *Soit p un nombre premier, $k \in \mathbb{N}^*$ et G un groupe d´ordre $n = p^k$. Alors, pour tout diviseur p^m $(0 \leqslant m \leqslant k)$ de $n = p^k$, il existe un sous-groupe de G d´ordre p^m.*

On procède par récurrence sur k. Si $k = 1$, p premier n´admet que les diviseurs 1 et p, et les sous-groupes triviaux de G conviennent. On suppose la propriété vraie pour tous les groupes d´ordre p^k. Soit G un groupe d´ordre p^{k+1} et $0 \leqslant m \leqslant k+1$. Si $m = 0$, c´est fini puisque $\{1\}$ est d´ordre $p^0 = 1$. On suppose $m > 0$. Puisque le centre de G n´est pas trivial, on choisit $z \in Z = Z(G)$, $z \neq 1$. Dans le sous-groupe cyclique $< z >$ dont l´ordre est nécessairement une puissance de p, on prend à bon droit h d´ordre p et on note $H =< h >$. Puisque $H \subset Z$, H est distingué dans G et le groupe quotient G/H (d´ordre p^k) possède un sous-groupe K d´ordre p^{m-1}. On pose : $L = \Pi^{-1}(K)$ où Π désigne la surjection $x \mapsto \overline{x} = xH$. L est un sous-groupe de G, et la restriction de Π à L est un isomorphisme de L sur son image $\Pi(L) = K$, donc $L/ker(\Pi_{|L}) = L/H \equiv K$, en particulier : $\circ(L) = \circ(H) \circ (K) = p^m$.

8 Théorème de Dixon

Soit G un groupe fini non commutatif. On tire successivement (avec remise) deux éléments de G, et on s´intéresse à la probabilité $P(G)$ pour que ces éléments commutent. (cf [2])

8.1 Dans $\mathcal{S}_3$

On étiquette les éléments de $\mathcal{S}_3$: Id, $\tau_1 = (2,3)$, $\tau_2 = (1,3)$, $\tau_3 = (1,2)$, $r = (1,2,3)$ et $\rho = r^{-1}$. La permutation Id est dans le centre de $\mathcal{S}_3$, τ_i commute avec Id et τ_i tandis que r et ρ commutent avec Id, r et ρ donc la probabilité cherchée est $P(\mathcal{S}_3) = \frac{6+3\times2+2\times3}{6^2} = \frac{1}{2}$.

8.2 Théorème

Propriété 26 *Soit G un groupe fini non commutatif. On tire successivement (avec remise) deux éléments de G. Alors la probabilité $P(G)$ pour que ces éléments commutent vérifie :*

$$P(G) \leqslant \frac{5}{8}.$$

Remarques préliminaires
Le centre $Z(G)$ étant un sous-groupe de G, par le théorème de Lagrange, il existe $m \in \mathbb{N}^*$ tel que : $\circ(G) = m \times \circ(Z(G))$. Puisque G est non commutatif, $Z(G) \neq G$ et $m \geqslant 2$.

Pour $x \in G$, Le centralisateur C_x de x est aussi un sous-groupe de G, donc il existe $k_x \in \mathbb{N}^*$ tel que $\circ(G) = k_x \times \circ(C_x)$. Par ailleurs, $Z(G)$ étant un sous-groupe de C_x, il existe $j_x \in \mathbb{N}^*$ tel que $\circ(C_x) = j_x \times \circ(Z(G))$. On peut écrire :

$$\forall x \in G \quad m = k_x\, j_x.$$

Pour $x \notin Z(G)$, $\exists y \in G \quad xy \neq yx$, donc $C_x \neq G$, donc $k_x \geqslant 2$. De plus $x \in C_x$, donc $C_x \neq Z(G)$, donc $j_x \geqslant 2$. En définitive, $m \geqslant 4$.

Preuve
Le nombre de tirages possibles est : $(\circ(G))^2$. Les couples favorables sont : $\bigcup_{x\in G} \{(x, y) \in G^2 \ ; \ y \in C_x\}$. La probabilité cherchée est donc : $P(G) = \frac{1}{(\circ(G))^2} \sum_{x\in G} \circ(C_x)$. On a : $P(G) = \frac{1}{(\circ(G))^2} \sum_{x\in Z(G)} + \sum_{x\notin Z(G)}$ c-à-d $P(G) = \frac{1}{(\circ(G))^2} \left\{ \circ(Z(G)) \circ (G) + \sum_{x\notin Z(G)} \circ(C_x) \right\}$. On peut remarquer que pour $x \notin Z(G)$, $k_x \geqslant 2$ donc : $\circ(C_x) \leqslant \frac{\circ(G)}{2}$ ✠. Ainsi $P(G) \leqslant \frac{1}{(\circ(G))^2} \left\{ \circ(Z(G)) \circ (G) + [\circ(G) - \circ(Z(G))] \times \frac{\circ(G)}{2} \right\}$,

$$P(G) \leqslant \frac{\circ(Z(G))}{\circ(G)} + \frac{1}{2} - \frac{1}{2}\frac{\circ(Z(G))}{\circ(G)} \leqslant \frac{1}{2}\frac{1}{m} + \frac{1}{2}.$$

On rappelle que $\frac{1}{m} \leqslant \frac{1}{4}$ ✠✠. Il vient :

$$P(G) \leqslant \frac{1}{8} + \frac{1}{2} = \frac{5}{8}.$$

8.3 Constante optimale

Si $P(G) = \frac{5}{8}$, alors il y a égalité dans l´inégalité ✠✠, donc $m = \frac{\circ(G)}{\circ(Z(G))} = 4$. Réciproquement, pour $x \notin Z(G)$, les assertions $k_x j_x = 4$, $k_x \geqslant 2$, et $j_x \geqslant 2$ imposent $j_x = k_x = 2$. Il y a alors égalité dans les inégalités ✠ et ✠✠, ce qui donne $P(G) = \frac{5}{8}$. En définitive,

$$P(G) = \frac{5}{8} \Leftrightarrow [G : Z(G)] = 4.$$

On exhibera dans la suite du texte des groupes finis G vérifiant $P(G) = \frac{5}{8}$.

9 Théorème de Cauchy

9.1 Deux lemmes

9.1.1 Groupe d´exposant 2

Lemme 11 *Soit G un groupe tel que : $\forall x \in G \quad x^2 = 1$.*
Alors :

1. *G est commutatif.*
2. *Si G est fini, $\circ(G) = n$ est une puissance de 2 ($n = 2^q$) et $G \simeq (\mathbb{Z}\ /2\mathbb{Z}\ )^q$.*

Pour u et v dans G, on écrit $uv\ uv = 1$, donc $uvu = v$, donc $uv = vu$.

Pour la deuxième assertion, on raisonne par récurrence sur l´ordre du groupe.
Initialisation : Si $G = \{1, x\}$, on a bien $2 = 2^1$ et $G \simeq \mathbb{Z}\ /2\mathbb{Z}$.
Hérédité : On suppose qu´un groupe dont l´ordre est inférieur ou égal à $n-1$ et dans lequel tout élément est involutif, a un cardinal qui est une puissance de 2.

Première justification : Soit $x_1, .., x_m \in G$ tels que $G =< x_1, .., x_m >$ et $x_m \notin < x_1, ..x_{m-1} >$. On écrit :

$$G = \left\langle \underbrace{< x_1, .., x_{m-1} >}_{H} \cup \{x_m\} \right\rangle .$$

On pose : $\mathcal{G} = \{hx_m^k\ ;\ h \in H, k \in \mathbb{Z}\ \} = \{hx_m^k\ ;\ h \in H, 0 \leqslant k < 2\} = H\ \ < x_m >$. La partie $\mathcal{G}$ de G est un sous-groupe de G (importance de G abélien), qui contient $H \cup \{x_m\}$, donc $\mathcal{G} = G$. A présent $(h, k) \in H \times \{0, 1\} \mapsto hx_m^k \in G$ est une application surjective, injective (facile à vérifier), donc $n = \circ(G) = 2\ \circ(H)$. Avec $\circ(H) \leqslant n-1$ et l´hypothèse de récurrence, n est bien une puissance de 2. On peut aussi considérer $(h, x) \in H \times < x_m > \mapsto hx \in G = H\ \ < x_m >$, qui est un morphisme de groupe (importance de G commutatif), surjectif, injectif (avec $H \cap < x_m >= \{1\}$), ce qui donne $G \simeq (\mathbb{Z}\ /2\mathbb{Z}\ )^q$.

Deuxième justification : Soit $x \in G$, $x \neq 1$. Grâce à la commutativité de G, pour $a, b, \alpha, \beta \in G$, on vérifie facilement que $\alpha < x >= a < x >$ et $\beta < x >= b < x >$ impliquent $\alpha\beta < x >= ab < x >$. On définit ainsi à bon droit une l.c.i sur $G/ < x >$ en posant $a < x >\ b < x >= ab < x >$. On montre sans problème que $G/ < x >$ muni de cette loi a une structre de groupe. Dans $G/ < x >$ (de cardinal $\frac{n}{2} < n$), tout élément est clairement involutif et par hypothèse de récurrence, $\frac{n}{2}$ est une puissance de 2. D´où le résultat.

Exercice 21 *Un groupe dans lequel tout élément distinct du neutre est d´ordre 3, est-il nécessairement commutatif ?*

Exercice 22
1) Soit G un groupe. On suppose que le groupe $Aut(G)$ des automorphismes de G est d´ordre $p > 2$ premier. Alors il existe $n \in \mathbb{N}^*$ tel que $G \equiv (\mathbb{Z}\ /2\mathbb{Z}\ )^n$.
2) En déduire qu´il n´existe pas de tel groupe G.

Le groupe $Aut(G)$ est cyclique donc le sous-groupe $Int(G) \equiv G/Z(G)$ des automorphismes intérieurs est lui-même cyclique, donc G est commutatif. A présent le passage à l´inverse $i : g \mapsto g^{-1}$ est un morphisme de G dans lui-même (importance de G commutatif), involutif, donc $i \in Aut(G)$. Puisque l´ordre de i ne peut être 2 ($2 \nmid p$), $i = Id_G$. Ainsi, tout élément de G est d´exposant 2 et $G \equiv (\mathbb{Z}\ /2\mathbb{Z}\ )^n$ avec $n \geqslant 1$. On termine en remarquant que $\mathbb{Z}\ /2\mathbb{Z}$ n´a qu´un seul automorphisme, donc on a nécessairement $n \neq 1$. On détermine maintenant l´ordre β_n de $Aut(\mathbb{Z}\ /2\mathbb{Z}\ )^n)$ et on vérifie que β_n n´est pas premier.

Lemme 12 *L´ordre β_n de $Aut((\mathbb{Z}/2\mathbb{Z})^n)$ est égal à $\beta_n = \prod_{i=0}^{n-1}(2^n - 2^i)$.*

Les automorphismes du groupe $((\mathbb{Z}/2\mathbb{Z})^n, +)$ sont exactement les automorphismes linéaires du $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel $(\mathbb{Z}/2\mathbb{Z})^n$, donc β_n est aussi le cardinal de l´ensemble des bases de $(\mathbb{Z}/2\mathbb{Z})^n$. En effet, en notant $(e_1, ..., e_n)$ la base canonique de $(\mathbb{Z}/2\mathbb{Z})^n$, on construit une bijection de $GL(n, \mathbb{Z}/2\mathbb{Z})$ sur l´ensemble des bases en envoyant toute matrice A de $GL(n, \mathbb{Z}/2\mathbb{Z})$ sur $(Ae_1, ..., Ae_n)$. A présent, pour choisir une base $(a_1, ..., a_n)$ de $(\mathbb{Z}/2\mathbb{Z})^n$, on choisit a_1 quelconque non nul, ce qui donne $2^n - 1$ choix pour a_1. Les vecteurs a_1, ..., a_i étant choisis, on prend a_{i+1} en dehors du sous-espace vectoriel $(a_1, ..., a_i)$, ce qui laisse $2^n - 2^i$ choix pour a_{i+1}. Ainsi :

$$\beta_n = \prod_{i=0}^{n-1}(2^n - 2^i).$$

9.1.2 Groupe diédral

Pour $n \geqslant 2$, on pose : $\omega = \exp\frac{2i\pi}{n}$ et pour $0 \leqslant k < n$, on note A_k le point d´affixe ω^k. On veut l´ensemble (en fait le groupe) D_n des isométries affines du plan euclidien conservant globalement le polygone régulier $A_0 A_1 .. A_{n-1}$. C´est aussi le groupe des isométries conservant l´ensemble $\{A_0, ..., A_{n-1}\}$ des n sommets. Soit $f \in D_n$. L´isométrie f conserve le barycentre donc $f(O) = O$. Pour l´image de A_0, on a à priori n possibilités (par exemple A_α) et par conservation des longueurs, l´image de A_1 est soit $A_{\alpha-1}$ ou $A_{\alpha+1}$ (les images des autres sommets étant alors parfaitement déterminées). Ceci donne donc l´information : $\sharp(D_n) \leqslant 2n$.

- Si $f(A_0) = A_0$, alors f laisse invariante la droite (OA_0) donc f est la reflexion s d´axe (OA_0) ou Id.
- Si A_0 est envoyé sur un A_i $(1 \leqslant i \leqslant n-1)$, en notant r la rotation $z \mapsto \omega z$ (de centre O et d´angle $\frac{2\pi}{n}$) et $k = n - i$, la rotation r^k vérifie $r^k \circ f(A_0) = A_0$. Ainsi, $r^k \circ f = Id = r^n$ ou $r^k \circ f = s = r^n s$. *Bilan* : $f = r^{n-k} = r^i$ ou $f = r^{n-k}s = r^i s$.

Le groupe $\{Id, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\}$ des isométries conservant $A_0 ... A_n$ est formé de n rotations et de n réflexions.

Lemme 13 *Soit $n \geqslant 2$. Deux groupes G et $\mathcal{G}$ vérifiant :*

1. $\circ(G) = \circ(\mathcal{G}) = 2n$
2. $G =< r, s >$ *et* $\mathcal{G} =< \rho, \sigma >$
3. $\circ(s) = \circ(\sigma) = 2$ *et* $\circ(r) = \circ(\rho) = n$
4. $\circ(rs) = \circ(\rho\sigma) = 2$

sont isomorphes. Un groupe vérifiant les quatre conditions ci-dessus est dit diédral d´ordre n et noté D_n.

Remarques

• $D_2 = V_4$ est commutatif. Pour $n \geqslant 3$, l´égalité $srsr = 1$ permet d´affirmer que D_n n´est pas commutatif (sinon $\circ(r) = n = 2$).

• On illustre une nouvelle fois la non-transitivité de $\lhd$. On considère pour cela le groupe D_4 des isométries du plan complexe qui conservent le carré de sommets 1, i, -1 et $-i$. On note s la symétrie

d´axe $y = 0$ et r la rotation de centre O qui envoie 1 sur i. On envisage alors les sous-groupes $H =< s >$ et $K =< s, -Id >$. Puisque K est commutatif (ses générateurs commutent), on a $H \lhd K$. Par ailleurs, l´égalité $rsr^{-1} = r^2 s = -s \in K \setminus H$ montre que $H \not\lhd D_4$ et $K \lhd D_4$.

Exercice 23 *Déterminer selon la parité de n, le centre Z et le groupe dérivé D de* D_n.

On commence par une *remarque préliminaire* : dans le groupe $D_n =< r, s >$, pour $0 \leqslant i \leqslant n$, $r^i s$ est une réflexion, donc $r^i s\ r^i s = 1$, donc $r^i s = sr^{-i}$. *Si n est impair*, soit $\phi \in Z$, $\phi \neq 1$. Si ϕ est une rotation, $\phi = r^i$ où $0 \leqslant i < n$. On a alors $\phi s = s\phi$, $r^i s = sr^i$, $r^i = r^{-i}$, $r^{2i} = 1$, $2i = n$, $2 \mid n$. Absurde ! Si ϕ est une réflexion, $\phi = r^i s$, et $r^i s\ s = s\ r^i s$ donne $r^i = r^{-i}$, $2i = n$ et de nouveau une contradiction avec n impair. En définitive, le centre Z de D_n est $\{1\}$ lorsque n est impair. Reste à envisager le cas $n = 2k$ *pair*. La rotation r^k commute avec toute rotation r^i, et avec toute réflexion $r^i s$. En effet, $r^k\ r^i s = r^i s\ r^k \Leftrightarrow r^{k+i} = r^{i-k} \Leftrightarrow r^{2k} = 1$, qui est bien vrai. Une rotation r^i $(0 < i < k)$ ne commute pas avec s : si $r^i s = sr^i$, $r^{2i} = 1$, ce qui n´est pas. Si $r^j \in Z$ avec $k < j < n$, $r^{-j} = r^{n-j} \in Z$ avec $0 < n - j < k$, ce qui est impossible d´après ce qui précède. Clairement, $s \notin Z$ puisque $rs = sr$ conduit à l´impossibilité $r^2 = 1$. La réflexion $r^i s$ $(0 < i < k)$ n´est pas non plus dans Z puisque $r^i s\ s = s\ r^i s$ conduit à $r^{2i} = 1$. De même, $r^j s \notin Z$ lorsque $k < j < n$. Qu´en est-il de $r^k s$? Si $r^k s\ r = r\ r^k s$, $r^{k-1} = r^{k+1}$, $r^2 = 1$, qui est faux. En résumé, le centre Z de D_{2k} est $\{1, r^k\} \equiv \mathbb{Z}/2\mathbb{Z}$.

Puisque $s^{-1}r^{-1}sr = sr^{-1}sr = sr^{-1}r^{-1}s = sr^{-2}s = r^2$, r^2 est un commutateur donc $< r^2 > \subset D$. Or $< r^2 >$ est d´ordre n si n est impair, $\frac{n}{2}$ si n est pair, donc $D_n/ < r^2 >$ est d´ordre 2 ou 4. Dans tous les cas, $D_n/ < r^2 >$ est abélien et $D \subset < r^2 >$. D´où $D =< r^2 >$.

Une parenthèse : Détermination des groupes d´ordre 8

Soit G un groupe d´ordre 8.

• Si G possède un élément d´ordre 8, alors $G \simeq \mathbb{Z}\ /8\mathbb{Z}$.

• Si tout élément distinct de 1 est d´ordre 2, alors G est commutatif et

$$G \simeq (\mathbb{Z}\ /2\mathbb{Z}\ )^3 .$$

• On suppose qu´aucune des conditions précédentes n´est réalisée. Pour $x \in G \setminus \{1\}$, $\circ(x) = 2$, ou 4. On peut choisir $a \neq 1$, $\circ(a) = 4$. Soit $b \notin < a >$. On a $G =< a > \sqcup\, b < a >= \underbrace{\{1, a, a^2, a^3, b, ab, a^2 b, a^3 b\}}_{8 \text{éléments distincts}}$

donc $G =< a, b >$. On remarque au passage que $b^2 \in < a >$, sinon $b^2 \in b < a >$ et $b \in < a >$ (ce qui est absurde). Une première piste pour la construction des groupes d´ordre 8 consiste à examiner successivement les cas :

$$b^2 = 1, \quad b^2 = a, \quad b^2 = a^2, \quad b^2 = a^3.$$

On utilise alors le fait que $< a >$ d´indice 2 dans G est distingué dans G. (cf [4])

Autre piste : l´élément ba vérifie clairement : $ba \in \{ab, a^2 b, a^3 b\}$.

Si $ba = a^2 b$, alors $ba^2 = a^2 ba = a^2 a^2 b = b$, ce qui est impossible.

Si les générateurs a et b de G commutent, par associativité de la loi, G est commutatif. On envisage alors à bon droit le sous-groupe $< a >< b >$ de G. Si $\circ(b) \geqslant 3$, alors $< a >< b >$ a plus de 8 éléments (ce qui

n´est pas), donc $\circ(b) = 2$. On considère $\phi : (\alpha, \beta) \in < a > \times < b > \mapsto \alpha\beta \in G$, qui est un morphisme de groupe (G commutatif), surjectif. Pour des raisons de cardinaux, $G \simeq < a > \times < b > \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On suppose $ba = a^3b$. Si on tente de remplir la table de G, on est vite coincé parce qu´on ne sait pas ce que fait b^2. Or $\circ(b) = 2$ ou 4.

1. Si $\circ(b) = 2$, alors $b^2 = 1$, $(ab)^2 = abab = aa^3bb = 1$, et on reconnaît le groupe diédral D_4.
2. Si $\circ(b) = 4$, on vérifie (facilement) que $b^2 \notin \{1, a, a^3\}$, donc $b^2 = a^2$, et on construit entièrement la table de G avec les relations $a^4 = 1$, $a^2 = b^2$, et $ba = a^3b$. G est appelé groupe quaternionique $\mathcal{H}_8$.

Pour une réalisation de $\mathcal{H}_8$, on peut considérer les matrices 2×2 complexes I_2, $-I_2$, $a = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & \text{-i} \end{pmatrix}$, $-a$, $b = \begin{pmatrix} 0 & 1 \\ \text{-1} & 0 \end{pmatrix}$, $-b$, $c = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$, $-c$ (cf page 23).

Remarque : Le 2-groupe D_4 (ou $\mathcal{H}_8$) n´est pas commutatif et son centre Z n´est pas trivial, donc $\circ(Z) = 2$, ou 4. Si $\circ(Z) = 4$, un élément $x \in G \setminus Z$ vérifie : $Z \subsetneq C_x$, donc $C_x = G$, $x \in Z$, ce qui est absurde. Ainsi, $\circ(Z) = 2$, donc

$$P(D_4) = P(\mathcal{H}_8) = \frac{5}{8}.$$

Exercice 24 *On reprend l´isomorphisme Φ de groupes de $\mathcal{S}_4$ dans $\mathcal{S}_{\{u,v,w\}} \equiv \mathcal{S}_3$, défini par :*

$$\Phi \ : \ \sigma \mapsto \begin{cases} \{u, v, w\} & \to \{u, v, w\} \\ z & \mapsto \sigma z \sigma^{-1} \end{cases} .$$

On considère le sous-groupe $U =< (v, w) >$ de $\mathcal{S}_{\{u,v,w\}}$ et on souhaite déterminer $\Phi^{-1}(U)$.
a) Montrer que $\Phi^{-1}(U)$ est le centralisateur C_u de u.
b) En déduire que $\Phi^{-1}(u)$ est d´ordre 8.
c) Vérifier que $V_4 \cup \{\tau = (1, 2); (3, 4)\} \subset \Phi^{-1}(u)$.
d) Montrer que $\Phi^{-1}(u) =< v, \tau > \equiv D_4$.

9.2 Cas d´un groupe abélien

Propriété 27 *Soit G un groupe commutatif d´ordre n et p un diviseur premier de n. Alors G possède un élément d´ordre p.*

Preuve (cf [3])

Lemme 14 *Soit H un sous-groupe de G, $x \in G$ d´ordre k. On pose $L =< H \cup \{x\} >$. Alors il existe un diviseur κ de k tel que : $\circ(L) = \kappa \times \circ(H)$.*

Soit $\mathcal{H} = \{m \in \mathbb{Z} \ ; \ x^m \in H\}$. On a $k \in \mathcal{H}$ puisque $x^k = 1$ donc $\mathcal{H}$ est non réduit à $\{0\}$. Par ailleurs, $\mathcal{H}$ est un sous-groupe de $\mathbb{Z}$. Il existe donc $\kappa \in \mathbb{N}$ tel que $\mathcal{H} = \kappa\mathbb{Z}$. On note au passage que κ divise k.

Le sous-groupe L contient tous les éléments de H et toutes les puissances de x, donc $\widetilde{L} = \{hx^m \ ; \ h \in$

$H, m \in \mathbb{Z}\ \} \subset L$. On vérifie par ailleurs que $\widetilde{L}$ est un sous-groupe de G, qui contient $H \cup \{x\}$, donc $L = \widetilde{L}$.
Pour $m \in \mathbb{Z}$, m s´écrit $m = \beta q + r$ où $0 \leqslant r < \beta$. Ainsi $u^m = \underbrace{(u^\beta)^q}_{\in H} u^r$, ce qui donne :

$$L = \{hx^m\ ;\ h \in H, 0 \leqslant m < \beta\}.$$

On envisage alors :

$$\psi\ :\ (h, m) \in H \times \{0, ..., \kappa\} \mapsto hx^m \in L.$$

L´application ψ est clairement surjective. Avec des notations évidentes,

$$hx^m = h'x^{m'} \Rightarrow x^{m'-m} \in H \Rightarrow \kappa \mid (m' - m) \Rightarrow m = m'$$

puisque $m, m' \in \{0, ..., \kappa\}$. On vient de prouver que ψ est injective, ce qui donne finalement : $\circ(L) = \kappa \times \circ(H)$.

Retour à la preuve : Soit $x_1, ..., x_n$ les éléments de G. On écrit :

$$G = \left\langle \underbrace{< x_1, ..., x_{n-1} >}_{H} \cup \{x_n\} \right\rangle.$$

D´après le lemme, n divise $\circ(H) \times \circ(x_n)$. Le raisonnement par descente est clair jusqu´à :

$$n \mid \prod_{x \in G} \circ(x).$$

Soit p un diviseur premier de n. Il existe $x \in G$ tel que $p \mid \circ(x)$. Dans le sous-groupe cyclique $< x >$, on choisit alors à bon droit (cf propriete 6 page 5) un élément d´ordre p.

Avec le théorème d´isomorphisme : On appelle x_1,...,x_n les éléments de G et l_1,...,l_n leur ordre. On envisage l´application $f : (y_1, ..., y_n) \mapsto y_1...y_n$ de $< x_1 > \times ... \times < x_n >$ dans (clairement sur) G. Puisque G est commutatif, f est un morphisme de groupes, donc

$$G \equiv < x_1 > \times ... \times < x_n > / ker(f).$$

Ainsi $\circ(G) = n \mid l_1...l_n$, $p \mid l_1...l_n$; Il existe alors un indice i tel que $p \mid l_i$, c-à-d un élément $x \in G$ tel que $p \mid \circ(x)$. Dans le sous-groupe cyclique $< x >$, on choisit alors à bon droit (cf propriete 6 page 5) un élément d´ordre p.

Remarque : Un diviseur premier p de $\circ(G) = n$ divise m^n où m désigne l´exposant de G. (cf page 11) L´entier premier p est donc aussi un diviseur de m.

Exercice 25 *Soit p, q premiers et G un groupe commutatif d´ordre pq. Alors G est cyclique.*

On choisit a, b dans G tels que $\circ(a) = p$, $\circ(b) = q$; Puisque $ab = ba$ et $p \wedge q = 1$, on a : $G =< ab >$.

9.3 Groupe d´ordre pair

9.3.1 Elément d´ordre 2

Propriété 28 *Soit G un groupe d´ordre $2n$. Alors G possède un élément d´ordre 2.*

Preuve : On définit sur G une relation d´équivalence de la façon suivante :

$$\forall (x,y) \in G \qquad x\mathcal{R}y \Leftrightarrow y \in \{x, x^{-1}\}.$$

Soit N_1 le nombre de classes réduites à un point et N_2 le nombre de classes à deux éléments. On a : $2n = N_1 + 2N_2$ donc N_1 est pair. Comme $\bar{1}$ est un singleton, $N_1 \neq 0$, donc $N_1 \geqslant 2$. Il existe donc $x \in G$, $x \neq 1$ tel que $x = x^{-1}$. cqfd

Remarque 1 (Retour de $\mathcal{R}$)
Soit p premier. Dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$, on retrouve la relation d´équivalence $\mathcal{R}$ pour obtenir la congruence de Wilson.

Les classes réduites à un singleton sont $\{-1\}$ et $\{p-1\}$ et dans le produit $(p-1)!$, on regroupe les facteurs par classe, ce qui donne :

$$(p-1)! \equiv -1(p)$$

Remarque 2 : (Soeur-jumelle de $\mathcal{R}$)
On suppose p premier.
Si m est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$, le petit théorème de Fermat donne :

$$m^{\frac{p-1}{2}} = 1.$$

Pour m non carré dans $(\mathbb{Z} \setminus p\mathbb{Z})^*$, on considère la relation d´équivalence : $x\mathcal{R}_m y \Leftrightarrow y \in \{x, mx^{-1}\}$. Les classes suivant $\mathcal{R}_m$ ont toutes deux éléments et en regroupant encore une fois les facteurs de $(p-1)!$ par classe, on obtient :

$$m^{\frac{p-1}{2}} = -1.$$

Application 3 *Tout groupe fini G vérifiant $P(G) = \frac{5}{8}$ a un ordre multiple de 8.*

Lemme : Tout carré de G est dans le centre $Z(G)$.

Soit $x \in G$. Si $x \in Z(G)$, alors $x^2 \in Z(G)$ car $Z(G)$ est un sous-groupe de G. Si $x \notin Z(G)$, on a $\frac{\circ(C_x)}{\circ(Z(G))} = 2$ (puisque $P(G) = \frac{5}{8}$), donc $C_x = Z(G) \sqcup xZ(G)$. on a alors : $x^2 \notin xZ(G)$ (Sinon $x \in Z(G)$).

Retour preuve
on a : $\circ(G) = m \times \circ(Z(G)) = 4 \times \circ(Z(G))$. Il suffit donc de vérifier que $Z(G)$ possède un élément d´ordre 2. Soit $x \notin Z(G)$. On a : $\circ(C_x) = 2 \times \circ(Z(G))$, donc C_x possède un élément u d´ordre 2. Si $u \in Z(G)$, tant mieux. Sinon, on choisit $y \notin C_x$, C_y possède un élément v d´ordre 2. Si $v \in Z(G)$, tant mieux. Dans le cas contraire, on montre que $z = (uv)^2$ est dans le centre $Z(G)$ et d´ordre 2.

- $z \neq 1$. Sinon, $uv = vu$, $C_u = C_v$, $C_x = C_y$, $y \in C_x$, contradiction.
- $z \in Z(G)$ (tout carré est dans le centre)

– $uz = \underbrace{u^2}_{\in Z(G)} vuv = vuu^2v = vuvu^2 = (vu)^2u = u(vu)^2$ donc $z = (vu)^2$.
– $z^2 = (uv)^2 (vu)^2 = uvuvvuvu = 1$.

Pour le plaisir, voici un autre clin d´oeil aux carrés dans un groupe :

Propriété 29 *Pour $n \geqslant 3$, $\mathcal{A}_n$ est le seul sous-groupe de $\mathcal{S}_n$ d´indice 2.*

Soit H un sous-groupe de $\mathcal{S}_n$ d´indice 2.

1. H contient tous les carrés de $\mathcal{S}_n$. (cf remarque page 16)
2. On sait (cf lemme 5 page 17) que $\mathcal{A}_n$ est engendré par les 3-cycles. Or, si c est un 3-cycle, $c^3 = 1$ donc $c = \left(c^{-1}\right)^2$, ce qui montre que $\mathcal{A}_n$ est aussi engendré par les carrés de $\mathcal{S}_n$. On conclut en remarquant que le sous groupe H d´indice 2 dans $\mathcal{S}_n$ contient tous les carrés de $\mathcal{S}_n$ donc contient $\mathcal{A}_n$ et pour des raisons de cardinaux, $H = \mathcal{A}_n$.

9.3.2 Groupe d´ordre $2p$

Propriété 30 *Soit G un groupe d´ordre $2p$ avec p premier. Alors G possède un élément d´ordre p.*

Preuve : Pour $a \in G$, $a \neq 1$, l´ordre de a est $2, p$ ou $2p$. Si $\exists a \in G \quad \circ(a) = 2p$, alors $G \simeq \mathbb{Z}/2p\mathbb{Z}$, et puisque 2 et p sont premiers entre eux, $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. L´élément $(\bar{2}, \bar{0})$, par exemple, est d´ordre p dans $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ donc G possède aussi un élément d´ordre p. Si pour tout $a \in G$, $\circ(a) = 2$, alors $\circ(G)$ est une puissance de 2. Contradiction. Autre argument possible : on prend $a \neq 1$, $b \neq 1$, $b \neq a$. On a $< a, b >= \{1, a, b, ab\}$ donc 4 divise $2p$, 2 divise p, ce qui est absurde.

Détermination des groupes d´ordre $6 = 2 \times 3$
On suppose G non cyclique. Soit $r \in G$, $r \neq 1$, $\circ(r) = 3$. On rappelle que le sous groupe $< r >$ d´indice 2 dans G est distingué. Soit $s \in G$, $\circ(s) = 2$. On montre que $\circ(sr) = 2$. On a $srs = srs^{-1}$ donc $srs \in \{1, r, r^2\}$. Si $srs = 1$, alors $r = 1$! Si $srs = r$, alors $sr = rs$ et l´application

$$\phi : (\rho, \sigma) \in < r > \times < s > \mapsto \rho\sigma \in G$$

est un morphisme de groupe. Son image contient $\{1, \rho, \rho^2, s\}$ donc son image dont le cardinal divise 6, est nécessairement G. Ainsi ϕ est surjectif, donc $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, donc G est cyclique (puisque $2 \wedge 3 = 1$). Contradiction. Bilan : $srs = r^2$, $srsr = r^3 = 1$. Enfin G contient les 6 éléments distincts $1, s, r, r^2, sr$ et rs, donc $G =< r, s >$. En définitive, $G = D_3$.

Remarque 1 On note au passage que D_3 est le plus petit groupe non commutatif.

Remarque 2 : *Aucun sous − groupe d'ordre* 6 *dans* $\mathcal{A}_4$.
Dans le groupe alterné d´ordre 4, il y a :

1. Id
2. Les produits de deux transpositions à supports disjoints qui sont d´ordre 2 et au nombre de 3. On rappelle que ces éléments forment avec Id un sous-groupe de $\mathcal{A}_4$ isomorphe à V_4.

3. Les 3-cycles

$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

$$r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

ainsi que les 3-cycles inverses, tous étant d´ordre 3.

On a listé 12 permutations de $\mathcal{A}_4$, on les a donc toutes.

Si $\mathcal{A}_4$ possède un sous-groupe H d´ordre 6, on a $H \simeq D_3$ puisque H ne possède aucun élément d´ordre 6. On choisit alors un 3-cycle r et un élément s de V_4 tels que : $\circ(rs) = 2$ et $H =< r, s >$. La permutation $\sigma = rs$ appartient donc au sous-groupe V_4, ce qui impose $r = \sigma\ s \in V_4$. Absurde puisque $\circ(r) = 3$.

Exercice 26
1) Montrer que V_4 est le seul sous-groupe de $\mathcal{A}_4$ d´ordre 4.
2) Justifier $\mathcal{S}_4/V_4 \equiv \mathcal{S}_3$.

Soit H un sous-groupe de $\mathcal{A}_4$ d´ordre 4. Tout élément de H est d´ordre 1,2 ou 4, et puisque $\mathcal{A}_4$ ne possède aucun élément d´ordre 4, tout élément de H est involutif. Par nécessité, $H = V_4$.

Par la formule des indices, $\mathcal{S}_4/V_4$ a 6 éléments, donc est isomorphe à $\mathbb{Z}\ /6\mathbb{Z}$ ou $\mathcal{S}_3$. On pose $x = (1,2)$ et $y = (2,3)$. Le commutateur $xyx^{-1}y^{-1} = (1,2,3)(1,2,3) = (1,3,2)$ est un 3-cycle donc $xy(yx)^{-1} \notin V_4$, $\overline{xy} \neq \overline{yx}$. Ainsi, $\mathcal{S}_4/V_4$ n´est pas commutatif, d´où : $\mathcal{S}_4/V_4 \equiv \mathcal{S}_3$.

Exercice 27 *Le groupe $Aut(\mathcal{S}_3)$ des automorphismes de $\mathcal{S}_3$ est isomorphe à $\mathcal{S}_3$.*

Soit $\mathcal{T} = \{(1,2);(1,3);(2,3)\}$ l´ensemble des transpositions de $\mathcal{S}_3$. Puisque les automorphismes de groupes conservent la période (ou l´ordre) des éléments du groupe et puisque $\mathcal{T}$ est exactement les permutations d´ordre 2 de $\mathcal{S}_3$, on envisage à bon droit le morphisme

$$\Phi^5 : \phi \in Aut(\mathcal{S}_3) \mapsto [\tau \in \mathcal{T} \mapsto \phi(\tau)]$$

de $Aut(\mathcal{S}_3)$ dans le groupe (isomorphe à $\mathcal{S}_3$) des permutations de $\mathcal{T}$. Si $\phi \in ker(\Phi)$, alors la restriction de ϕ à $\mathcal{T}$ est l´identité, et puisque $\mathcal{T}$ engendre $\mathcal{S}_3$, ϕ est l´identité. Ainsi Φ est injective, donc $Aut(\mathcal{S}_3)$ est isomorphe au sous-groupe $\Phi(Aut(\mathcal{S}_3))$ de $\mathcal{S}_3$. A présent, le sous-groupe $Int(\mathcal{S}_3) < Aut(\mathcal{S}_3)$ des automorphismes intérieurs de $\mathcal{S}_3$ est isomorphe à $\mathcal{S}_3/Z(\mathcal{S}_3) \equiv \mathcal{S}_3$ puisque le centre $Z(\mathcal{S}_3)$ est trivial. Il vient $\sharp(Aut(\mathcal{S}_3)) \geqslant \sharp(Int(\mathcal{S}_3)) = 6$. Avec ce qui précède, $Aut(\mathcal{S}_3) = Int(\mathcal{S}_3) \equiv \Phi(Aut(\mathcal{S}_3)) = \mathcal{S}_3$.

Détermination des groupes d´ordre $2p$.
On choisit dans G un élément r d´ordre p, et un élément s d´ordre 2. On a $s \notin < r >$ car 2 ne divise pas p. Avec $< r >$ d´indice 2 dans G, on peut écrire : $G/ < r >= \{< r >, s < r >\}$, $G = \{1, r, .., r^{p-1}\} \cup \{s, sr, .., sr^{p-1}\}$, $G =< r, s >$.

– Si G est cyclique, $G \simeq \mathbb{Z}\ /2p\mathbb{Z} \simeq \mathbb{Z}\ /2\mathbb{Z} \times \mathbb{Z}\ /p\mathbb{Z}$.

[5] Action naturelle de $Aut(\mathcal{S}_3)$ sur $\mathcal{T} = \{(1,2);(1,3);(2,3)\}$

– On suppose G non cyclique. Pour $\sigma \notin < r >$, σ s´écrit $\sigma = sr^k$ $(0 \leqslant k \leqslant p-1)$. Si $\sigma^2 \neq 1$, alors $\sigma^2 = (sr^k s)\, r^k = (sr^k s^{-1})\, r^k$ et avec $< r >$ distingué, on a $\sigma^2 = r^i$ avec $1 \leqslant i \leqslant n-1$. Avec $p = 2q+1$, on écrit : $\sigma^{2q} = \sigma^{p-1} = r^{iq}$ donc $\sigma r^{iq} = 1$, $\sigma \in < r >$. Contradiction. Bilan : $\forall \sigma \notin < r > \quad \sigma^2 = 1$. En particulier, $(sr)^2 = 1$ et on reconnaît le groupe diédral d´ordre p.

Remarque : Le groupe D_p est un groupe non cyclique dont tous les sous-groupes propres sont cycliques.

9.3.3 Sous-groupe d´indice 2 et unicité

Propriété 31 *Soit G un groupe fini et H un sous-groupe distingué de G d´ordre m. On suppose que : $\circ(H) \wedge [G:H] = m \wedge [G:H] = 1$. Alors H est l´unique sous-groupe (distingué) de G d´ordre m.*

Peut-on se passer de l´hypothèse "H distingué" ? Non, dans $\mathcal{S}_3$ de cardinal 2×3, considérer les sous-groupes $< (1,2) >$ et $< (2,3) >$ qui sont d´ordre 2.

Remarque : On retrouve le fait que V_4 distingué dans $\mathcal{A}_4$ est l´unique sous-groupe de $\mathcal{A}_4$ d´ordre 4.

Preuve : On note Π le morphisme surjectif $x \mapsto \overline{x}$ de G sur G/H. Si K désigne un sous-groupe de G d´ordre m, on envisage la restriction de Π à K, qu´on continue à noter Π. Puisque $\Pi(K)$ est un sous-groupe de G/H, $\circ(\Pi(K))$ divise $[G:H]$. Par ailleurs, puisque $K/ker(\Pi) \equiv \Pi(K)$, $\circ(\Pi(K))$ divise $\circ(K) = m$. Or $m \wedge [G:H] = 1$, donc $\circ(\Pi(K)) = 1$, $\Pi(K) = \{H\}$, $K \subset H$, et finalement $K = H$.

Application : Si m est un entier naturel impair, alors le sous-groupe $< r >$ des rotations de $D_{2m} =< r, s >$ est l´unique sous-groupe de D_{2m} d´indice 2.

9.4 Cas général

Propriété 32 *Soit G un groupe fini d´ordre n et p un diviseur premier de n.*
Alors G possède un élément d´ordre p.

Preuve (cf [4])
On raisonne par récurrence sur l´ordre n de G. Si $n = 2$, c´est évident. On suppose la propriété vraie pour tout groupe d´ordre $m < n$. Soit p un diviseur premier de n. Si G est commutatif, c´est acquis. On suppose donc désormais : $Z(G) \neq G$.

• Si $\exists x \in G \setminus Z(G) \quad p \mid \circ(C_x)$, on applique à bon droit l´hypothèse de récurrence à C_x ($x \notin Z(G) \Rightarrow C_x \subsetneq G$) : il existe dans C_x (et donc dans G) un élément d´ordre p.

• Si pour tout $x \in G \setminus Z(G)$ p ne divise pas $\circ(C_x)$, p (premier) qui divise $n = \circ(C_x) \times [G:C_x]$, divise $[G:C_x]$ et d´après l´équation aux classes, p divise $\circ(Z(G))$. D´après l´hypothèse de récurrence, $Z(G)$ donc G possède alors un élément d´ordre p.

On peut montrer mieux :

Propriété 33 *Soit G un groupe fini de cardinal n et p un nombre premier. Si $p^m \mid n$ avec $m \in \mathbb{N}$, alors G contient un sous-groupe d´ordre p^m.*

Application 4 *Soit G un groupe fini et $p > 0$ un nombre premier. Les deux propriétés suivantes sont équivalentes :*

1. *$\sharp(G)$ est une puissance de p ou G est un p-groupe.*
2. *Tout élément de G a pour ordre une puissance de p.*

$1 \Rightarrow 2$ est une conséquence immédiate du théorème de Lagrange. On suppose maintenant que l´ordre de tout élément de G est une puissance de p. Soit q un diviseur premier de $\sharp(G)$. Avec Cauchy, G possède un élément d´ordre q, donc q sécrit p^α, et puisque q est premier, $q = p$. D´où le résultat.

Application 5 *Il n´y a qu´un seul sous-groupe d´ordre 15, à savoir $\mathbb{Z}/15\mathbb{Z}$.*

Avec Cauchy, on choisit un élément a d´ordre 3, et un élément b d´ordre 5. Puisque 3 est le plus petit diviseur premier de l´ordre de G, le sous-groupe $< a >$ est distingué dans G (cf page 14). Ainsi, $b^{-1}ab = a$, ou $b^{-1}ab = a^2$.

1. Si $b^{-1}ab = a$, alors $ab = ba$ et puisque $a \wedge b = 1$, ab est d´ordre $3 \times 5 = 15$: G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.
2. Si $b^{-1}ab = a^2$, alors $b^{-1}ab\ b^{-1}ab = a$, $b^{-1}a^2b = a$. Par ailleurs, $b^{-1}ab = a^2$ donne $ba^2b^{-1} = a$. Ainsi, $b^{-1}a^2b = ba^2b^{-1}$, $b^4a^2b = ba^2b^4$, $b^3a^2b = a^2b^4$, $b^3a^2 = a^2b^3$. Or a^2 comme a, est d´ordre 3 et b^3 comme b est d´ordre 5. Il vient : $\circ(a^2b^3) = 15$, G commutatif, $b^{-1}ab = a$, $a = a^2$. Impossible.

Application 6 *(avec le concours de Michiel Vieumelen)*
Soit $p > 2$ un nombre premier et G un groupe d´ordre $p + 1$. On note $Aut(G)$ le groupe des automorphismes de G. Le nombre p divise l´ordre de $Aut(G)$ si, et seulement si, $\exists n > 1 \quad G \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

Si p premier divise l´ordre de $Aut(G)$, d´après Cauchy, le groupe $Aut(G)$ possède un élément φ d´ordre p. Sur $X = G \setminus \{1\}$, on considère alors la relation d´équivalence [6] :

$$x \mathcal{T} y \Leftrightarrow \exists 0 \leqslant k \leqslant p-1 \quad \varphi^k(x) = y.$$

Pour $x \in X$, on pose $\Gamma_x = \{\psi \in \Gamma \ ; \ \psi(x) = x\}$. On vérifie que Γ_x est un sous-groupe de Γ, donc $\Gamma_x = \{Id\}$, ou $\Gamma_x = \Gamma$. Si pour tout $x \in X$, $\Gamma_x = \Gamma$, alors $\forall x \in X \quad \forall \psi \in \Gamma \quad \psi(x) = x$, donc $\varphi = Id$. Contradiction. Ainsi, $\exists a \in X \quad \Gamma_a = \{Id\}$. Les p éléments $a, \varphi(a), .., \varphi^{p-1}(a)$ sont alors distincts dans X. G étant d´ordre pair, X possède un élément $b = \varphi^l(a)$ d´ordre 2. Pour x quelconque dans X, x s´écrit : $x = \varphi^k(a) = \varphi^{k-l}(b)$. On a alors $x^2 = \varphi^{k-l}(b^2) = 1$, ce qui assure que tout élément de G est involutif et prouve que $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$. On pourra reprendre la preuve ci-dessus en utilisant le langage éclairant des actions de groupes.

Pour la réciproque, $Aut((\mathbb{Z}/2\mathbb{Z})^n) = Gl_n(\mathbb{Z}/2\mathbb{Z})$ a $(2^n - 1)(2^n - 2)...(2^n - 2^{n-1})$ éléments (cf page 28), donc on a bien $p = 2^n - 1 \mid \circ(Aut((\mathbb{Z}/2\mathbb{Z})^n))$.

[6] Action naturelle de $< \varphi >$ sur X

Références

[1] Thèmes de géométrie, chapitre 1, M. Alessandri, Dunod
[2] RMS-mai-juin-1996, Examens oraux
RMS 112, volume 2, I. Gozard, M. Serris, Vuibert
[3] Problèmes corrigés de mathématiques supérieures,
M. Quercia, F. Ranty, Ellipses
[4] Groupes, A. Bouvier, D. Richard, Hermann
[5] Exercices d´algèbre et dánalyse, Tome 2, P. Meunier, Puf
[6] Algèbre, Tome 1, D. Guin, Belin et Editions espaces 34