

Bonus : un peu de botanique des groupes

Ce poly (totalement facultatif, est-il besoin de le préciser) est à destination des élèves curieux et agiles (et à l'aise avec le cours fait en classe) qui veulent explorer un peu plus le monde merveilleux des groupes :

- soit en prenant de l'avance sur le programme de deuxième année, en se familiarisant, par exemple, avec la notion d'ordre d'un élément dans un groupe.
- soit en allant plus loin et en cherchant des exemples de groupes explicites vérifiant certaines propriétés : de façon générale, on appréhende mieux la notion de groupes en ayant des exemples explicites en tête, en ayant également bien en tête la façon dont les éléments interagissent entre eux, en comprenant bien également la notion de groupe engendré (au programme de deuxième année). Certains groupes classiques vus dans ce poly font d'ailleurs partie de la culture générale de tout mathématicien à partir de la licence et font souvent l'objet d'exercices d'oraux ou de sujets d'écrits.

Dans la suite, sauf indication contraire, G désigne un groupe dont la loi est notée multiplicativement.

I Un peu du programme de deuxième année

I.1 Groupe engendré par une partie

Proposition/Définition (Deuxième année). Soit A une partie de G . Il existe un unique plus petit sous-groupe de G qui contient A . On l'appelle le groupe engendré par A et on le note $\langle A \rangle$, $\langle A \rangle$ ou $\text{gr}(A)$.

DÉMONSTRATION. Il suffit de voir que

$$B = \bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subset H}} H$$

□

est un sous-groupe de G d'après ce qui précède car intersection de sous-groupes de G , et est contenu dans tous les sous-groupes de G contenant A . Il y a unicité car si C est un sous-groupe qui convient, alors $B \subset C$ car C est un sous-groupe de G contenant A , et $C \subset B$ pour la même raison donc $B = C$.

Remarques :

- Dans le cas où $A = \{x_1; \dots; x_n\}$ est un ensemble fini, on note ce groupe $\text{gr}(x_1, \dots, x_n)$ au lieu de $\text{gr}(\{x_1, \dots, x_n\})$.
- Dans le cas où A ne contient qu'un élément, le groupe engendré est très simple. Montrons que $\text{gr}(x) = \{x^n \mid n \in \mathbb{Z}\}$. D'après ce qui précède, $B = \{x^n \mid n \in \mathbb{Z}\}$ est inclus dans chaque sous-groupe de G contenant x . Pour conclure, il suffit donc de prouver que c'est un sous-groupe de G . $e = x^0 \in B$ donc B est non vide. Soit $(x_1, x_2) \in B^2$. Il existe $(n_1, n_2) \in \mathbb{Z}^2$ tel que $x_1 = x^{n_1}$ et $x_2 = x^{n_2}$ si bien que $x_1 x_2 = x^{n_1+n_2} \in B$: B est stable par produit. Enfin, il est stable par inverse puisque $x_1^{-1} = x^{-n_1} \in B$.
- Dans le cas où la loi est notée additivement, on a $\text{gr}(x) = \{nx \mid n \in \mathbb{Z}\}$. En particulier, lorsque $\alpha \in \mathbb{R}$, $\text{gr}(\alpha) = \alpha\mathbb{Z}$. On retrouve le fait que, si H est un sous-groupe de \mathbb{R} contenant α , alors $\alpha\mathbb{Z} \subset H$. Mais puisque ce n'est au programme qu'en deuxième

Même si, encore une fois, cela fait surtout appel au cours de deuxième année, donc ce n'est pas très grave si vous ne lisez pas ce poly cette année, voire si vous ne lisez pas ce poly du tout !

Plus petit au sens de l'inclusion, c'est-à-dire que si H est un sous-groupe qui contient A , alors $\text{gr}(A) \subset H$.

année, il faut savoir le redémontrer ! cf. paragraphes III.2 et III.3 du cours. Cependant, il est bon de connaître ce résultat car alors il devient un réflexe, et car l'idée de groupe engendré est assez intuitive et permet de mieux voir ce résultat.

- Cependant, lorsque A admet au moins deux éléments x_1 et x_2 , ce n'est plus aussi simple. La loi n'étant pas forcément commutative, $\text{gr}(A)$ contient (au moins) tous les éléments du type $x_1^{n_1} x_2^{n_2} x_1^{p_1} x_2^{p_2} \dots$. C'est pour cela qu'on ne cherche plus à expliciter tous les éléments de $\text{gr}(A)$ mais à le trouver explicitement.

I.2 Ordre d'un élément

Dans ce paragraphe, tous les groupes considérés sont finis.

Définition. Soit G un groupe fini. On appelle ordre de G le cardinal de G .

Exemple : Pour tout $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe d'ordre n .

Définition. Soit G un groupe fini. Soit $x \in G$. On appelle ordre de x le cardinal de $\text{gr}(x)$, le groupe engendré par x .

Le résultat suivant découle du théorème de Lagrange :

Corollaire. Soit G un groupe fini et soit $x \in G$. Alors l'ordre de x divise le cardinal de G .

Remarque : Le cardinal d'un groupe fini est parfois appelé son ordre (c'est-à-dire qu'un groupe d'ordre 4 est un groupe de cardinal 4). Ainsi, l'ordre d'un élément est l'ordre du groupe qu'il engendre et divise l'ordre de tout groupe auquel il appartient.

La proposition suivante donne une autre caractérisation de l'ordre d'un élément. C'est d'ailleurs comme cela qu'on le définit parfois :

Proposition. Soit G un groupe fini. Soit $x \in G$. L'ordre de x est le plus petit entier $n \geq 1$ tel que $x^n = e$. De plus, si on le note $\omega(x)$ alors, si $n \in \mathbb{Z} : x^n = e \iff \omega(x) | n$.

DÉMONSTRATION. G étant fini, il existe $k \neq p$ dans \mathbb{N}^* tels que $x^k = x^p$. Sans perte de généralité, on peut supposer $k > p$. Par régularité (ou en multipliant p fois par x^{-1}), il vient $x^{k-p} = e$, d'où l'existence de ce plus petit entier. On note donc $\omega(x) = \min\{n \in \mathbb{N}^* | x^n = e\}$ (pour l'instant, $\omega(x)$ est défini comme le plus petit entier n tel que $x^n = e$, on ne sait pas encore que c'est l'ordre de x).

Soit $n \in \mathbb{Z}$. Effectuons la division euclidienne de n par $\omega(x)$: il existe $q \in \mathbb{N}$ et $0 \leq r < \omega(x)$ tels que $n = q\omega(x) + r$, si bien que $x^{q\omega(x)} \times x^r = e$. Or,

$$\begin{aligned} x^{q\omega(x)} &= (x^{\omega(x)})^q \\ &= e^q \\ &= e \end{aligned} \quad \square$$

et donc $x^n = x^r$. Si $r \neq 0$, alors $r \in \mathbb{N}^*$ et $r < n$ donc $x^n \neq e$. Si $r = 0$, alors $x^r = e$ donc $x^n = e$. Finalement, $x^n = e$ si et seulement si $r = 0$. Finalement, $x^n = e \iff \omega(x) | n$.

Pour conclure, il suffit donc de prouver que $\text{card}(\text{gr}(x)) = \omega(x)$. D'après ce qui précède, pour tout $n \in \mathbb{Z}$, $x^n = x^r$ où r est le reste de la division euclidienne de n par $\omega(x)$. Par conséquent, $\text{gr}(x) = \{x^n | n \in \mathbb{Z}\} = \{e; x; x^2; \dots; x^{\omega(x)-1}\}$. Il suffit pour conclure de prouver que ces éléments sont tous distincts. Or, si deux éléments sont égaux, disons x^n et x^p avec $n > p$, alors $x^{n-p} = e$ avec $0 < n-p < \omega(x)$ ce qui contredit la définition de $\omega(x)$, ce qui permet de conclure.

$\text{gr}(x)$ est inclus dans G qui est un ensemble fini donc est un ensemble fini : l'ordre de x est bien défini. On peut encore définir l'ordre d'un élément dans un groupe infini, mais celui-ci n'existe pas forcément car le groupe engendré peut être infini. Si ce groupe est fini, on dit que l'élément est d'ordre fini égal au cardinal du groupe engendré et alors la proposition ci-contre est encore vraie : cf. programme de deuxième année.

Corollaire. Soit G un groupe fini. Soit $x \in G$. Alors $\text{gr}(x) = \{e; x; x^2; \dots; x^{\omega(x)-1}\}$.

Remarque : En d'autres termes, lorsqu'on est dans un groupe fini, le groupe engendré par un élément x est obtenu en prenant les puissances successives de x , on finira par retomber sur e et on recommence (on parle de groupe cyclique, voir la suite). Ce groupe contient toutes les puissances de x , positives et négatives, car si $n \in \mathbb{Z}$, alors $x^n = x^r$ où r est le reste de la division euclidienne de n par r .

Exemples :

- Le seul élément d'ordre 1, c'est le neutre lui-même.
- Un élément est d'ordre 2 si et seulement s'il est différent du neutre et s'il est son propre inverse. En effet, x est d'ordre 2 si et seulement si $x^1 \neq e$ et $x^2 = e$.
- Dans \mathbb{U}_4 , i et $-i$ sont d'ordre 4 et -1 est d'ordre 2. Plus généralement (cf. exercice 72 du chapitre 7), $z \in \mathbb{U}_n$ est d'ordre exactement n si et seulement s'il existe $k \in \llbracket 0; n-1 \rrbracket$ premier avec n tel que $z = e^{2ik\pi/n}$. On dit alors que z est une racine primitive n -ième de l'unité.
- Lorsque le groupe est noté additivement, l'ordre du groupe est le plus petit entier $n \geq 1$ tel que $nx = 0$ (car le neutre est en général noté 0 dans un groupe additif). Par exemple, dans $\mathbb{Z}/2\mathbb{Z}$ et plus généralement dans $(\mathbb{Z}/2\mathbb{Z})^n$, tout élément non nul (i.e. différent du neutre) est d'ordre 2. Dans $\mathbb{Z}/4\mathbb{Z}$, $\bar{1}$ et $\bar{3}$ sont d'ordre 4 mais $\bar{2}$ est d'ordre 2.

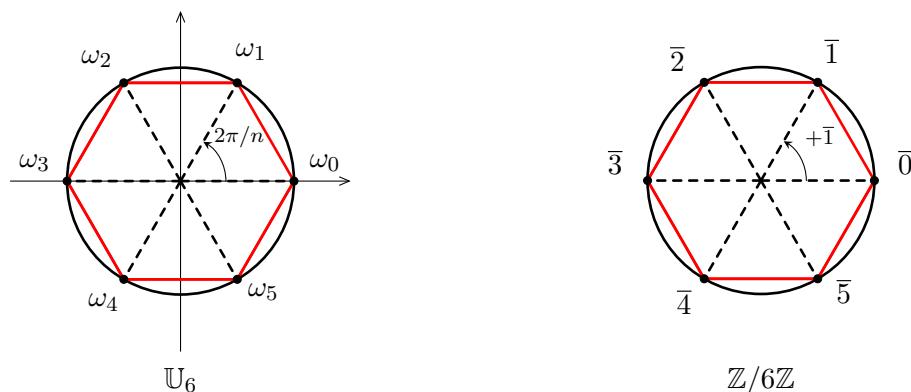
Remarque : On en déduit une nouvelle façon de prouver que certains groupes ne sont pas isomorphes : en regardant l'ordre de certains de leurs éléments. Montrons en effet que deux groupes isomorphes ont autant d'éléments l'un que l'autre du même ordre. Soient G_1 et G_2 deux groupes finis et soit $n \geq 1$. Montrons que si G_1 et G_2 sont isomorphes, alors ils ont autant d'éléments d'ordre n l'un que l'autre. Notons $A_1 = \{x \in G_1 \mid \omega(x) = n\}$ et $A_2 = \{x \in G_2 \mid \omega(x) = n\}$. Soit $f : G_1 \rightarrow G_2$ un isomorphisme. Soit $x \in A_1$. Alors $x^n = e_1$ donc $f(x^n) = f(e_1)$ mais f est un morphisme donc $f(x)^n = e_2$ si bien que $\omega(f(x))$ divise n . Si $\omega(f(x)) < n$ alors $f(x)^{\omega(f(x))} = e_2$ donc, toujours car c'est un morphisme, $f(x^{\omega(f(x))}) = e_2$. Par injectivité de f , $x^{\omega(f(x))} = e_1$ ce qui contredit la minimalité de n . Par conséquent, $f(A_1) \subset A_2$ et donc $\text{card}(A_1) \leq \text{card}(A_2)$. Par symétrie des rôles, on a l'autre inégalité donc $\text{card}(A_1) = \text{card}(A_2)$.

On en déduit par exemple que $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$ ne sont pas isomorphes car $\mathbb{Z}/4\mathbb{Z}$ a un élément d'ordre 4 mais tous les éléments de $(\mathbb{Z}/2\mathbb{Z})^2$ sont d'ordre 1 (le neutre) ou 2. De même, $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$ sont deux à deux non isomorphes (voir la fin du poly).

Ils sont non isomorphes alors qu'ils ont 4 éléments : avoir le même cardinal est une condition nécessaire non suffisante pour être isomorphes.

I.2.a Groupes cycliques et monogènes (deuxième année)

Nous avons représenté dans les chapitres 7 et 16 les ensembles \mathbb{U}_n et $\mathbb{Z}/n\mathbb{Z}$ de la même façon, à savoir des points sur un cercle :



Attention, pour $\mathbb{Z}/n\mathbb{Z}$, ce n'est qu'une façon de représenter ses éléments, cela ne signifie pas que les éléments de $\mathbb{Z}/n\mathbb{Z}$ soient des racines de l'unité ou même des complexes. Seulement,

cette représentation est assez pratique car elle permet de mieux visualiser la loi du groupe : par exemple, dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{1} + \bar{5} = \bar{0}$, ce qui se voit bien sur le dessin ci-dessus. Il semblerait que ces deux groupes soient les mêmes. Ce sont deux cas particulier d'un type de groupe plus général.

Définition. Soit G un groupe.

- G est dit monogène s'il est engendré par un élément donc s'il existe x tel que $G = \text{gr}(x)$.
- G est dit cyclique s'il est monogène et fini.

Remarques :

- En d'autres termes, un groupe est monogène lorsqu'il est de la forme $G = \{x^n \mid n \in \mathbb{Z}\}$. Par exemple, $\{2^n \mid n \in \mathbb{Z}\}$ est un groupe (et donc un sous-groupe de \mathbb{R}_+^* et de \mathbb{R}^*).
- Lorsque la loi est notée additivement, un groupe monogène est un groupe de la forme $G = \{nx \mid n \in \mathbb{Z}\}$. Par exemple, tout groupe de la forme $\alpha\mathbb{Z}$, pour $\alpha \in \mathbb{R}$, est monogène, et en particulier \mathbb{Z} est monogène.
- On a déjà vu que si x est un élément d'ordre fini $\omega(x)$, alors :

$$\text{gr}(x) = \{e; x; x^2; \dots; x^{\omega(x)-1}\}$$

En particulier, un groupe est cyclique lorsqu'il existe $x \in G$ et $n \in \mathbb{N}$ tel que $G = \{e; x; x^2; \dots; x^{n-1}\}$. L'ordre de x est alors égal à l'ordre du groupe.

Exemples :

- Si $n \geq 1$, notons $\omega = e^{2ik\pi/n}$. Alors $\mathbb{U}_n = \{1; \omega; \dots; \omega^{n-1}\}$ c'est-à-dire que \mathbb{U}_n est cyclique et engendré par ω .
- Rappelons que dans un groupe additif, la notation kx , pour $k \geq 1$, représente l'élément x itéré k fois, c'est-à-dire $\underbrace{x + x + \dots + x}_{k \text{ fois}}$. Par conséquent, si $n \geq 2$ et si on note $x = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$, alors $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; x; 2x; \dots; (n-1)x\} : \mathbb{Z}/n\mathbb{Z}$ est cyclique et engendré par x .

D'où les représentations en cercle ci-dessus !

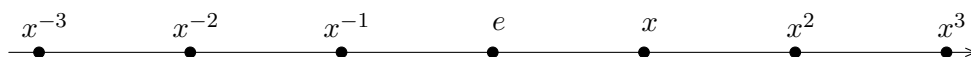
Celle-ci est intéressante également car elle permet de mieux visualiser la loi du groupe. En effet :

Proposition. Soit $n \geq 1$. Soit G un groupe cyclique d'ordre n engendré par x . Alors $x^n = e$, $x^{n+1} = x$, $x^{n+2} = x^2$ et, plus généralement, pour tout $k \in \mathbb{Z}$, si $k = nq + r$ est la division euclidienne de k par n , alors $x^k = x^r$.

DÉMONSTRATION. Déjà faite dans le paragraphe précédent.

En particulier, $x^k = e$ si et seulement si n divise k .

Remarque : Ainsi, on peut toujours représenter un groupe cyclique comme ci-dessus, car quand on itère n fois x , on arrive au neutre, et on recommence : x , x^2 etc. D'où le nom de groupe cyclique ! Pour un groupe monogène infini, avec les propriétés des puissances, la notation « en ligne » est plus adaptée :



Attention, les éléments de G ne sont pas forcément des réels, ce n'est qu'une notation, de façon analogue à la représentation en cercle des groupes cycliques. Ces représentations rendent intuitif le théorème suivant :

Théorème.

- Un groupe monogène infini est isomorphe à \mathbb{Z} .
- Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Remarque : En particulier, tout groupe monogène (fini ou non) est abélien. Attention, la réciproque fautive : voir ci-dessous.

DÉMONSTRATION. Supposons G monogène infini engendré par x si bien que $G = \{x^n \mid n \in \mathbb{Z}\}$. Montrons que $\varphi : n \mapsto x^n$ est un isomorphisme de \mathbb{Z} dans G .

- φ est surjective par hypothèse.
- Soit $n \in \ker(\varphi)$. Alors $x^n = e$. Si $n \neq 0$ alors $G = \{e; x; \dots; x^{n-1}\}$ (on le montre comme ci-dessus en effectuant la division euclidienne de $k \in \mathbb{Z}$ par n) ce qui est absurde. Ainsi, $n = 0$ donc $\ker(\varphi) = \{0\}$, φ est injective donc bijective.
- Enfin, φ est bien un morphisme car, pour tout $(n_1, n_2) \in \mathbb{Z}^2$,

$$\begin{aligned}\varphi(n_1 + n_2) &= x^{n_1 + n_2} \\ &= x^{n_1} * x^{n_2} \\ &= \varphi(n_1) * \varphi(n_2)\end{aligned}$$

Finalement, φ est bien un isomorphisme entre G et \mathbb{Z} .

Supposons à présent que G soit cyclique d'ordre n engendré par x si bien que $G = \{e; x; \dots; x^{n-1}\}$. Montrons que $\varphi : \bar{k} \mapsto x^k$ est un isomorphisme.

- Prouvons tout d'abord que φ est bien définie i.e. que l'image de \bar{k} ne dépend pas de l'élément de \bar{k} choisi (cf. chapitre 16). Si $\bar{k}_1 = \bar{k}_2$ alors k_1 et k_2 sont congrus l'un à l'autre modulo n donc ont même reste modulo n donc, si on note celui-ci r , $x^{k_1} = x^{k_2} = x^r$: φ est bien définie.
- Soit $\bar{k} \in \ker(\varphi)$, alors $x^k = e$ donc n divise k si bien que $\bar{k} = \bar{0}$. En d'autres termes, $\ker(\varphi) = \{\bar{0}\}$: φ est injective entre deux ensembles de même cardinal donc est bijective.
- Soit $(\bar{k}_1, \bar{k}_2) \in (\mathbb{Z}/n\mathbb{Z})^2$.

$$\begin{aligned}\varphi(\overline{k_1 + k_2}) &= \varphi(\overline{k_1 + k_2}) \\ &= x^{k_1 + k_2} \\ &= x^{k_1} * x^{k_2} \\ &= \varphi(\overline{k_1}) * \varphi(\overline{k_2})\end{aligned}$$

□

ce qui permet de conclure.

Corollaire. Soit G un groupe (pas forcément fini ou cyclique). Soit $x \in G$. Si x est d'ordre fini n , alors $\text{gr}(x)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.


DÉMONSTRATION. Découle de ce qui précède. En particulier, $\text{gr}(x) = \{e; x; x^2; \dots; x^{n-1}\}$.

Proposition. Soit G un groupe fini d'ordre n . Alors G est cyclique si et seulement si G admet un élément d'ordre n .

En particulier, \mathbb{U}_n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En fait, $\mathbb{Z}/n\mathbb{Z}$ est le groupe cyclique additif d'ordre n de référence, tandis que \mathbb{U}_n est le groupe cyclique multiplicatif d'ordre n de référence.

G admet alors un sous-groupe cyclique d'ordre n .

Et il est alors isomorphe à $\mathbb{Z}/n\mathbb{Z}$ d'après ce qui précède.

Remarque :  Attention, un produit de groupes cycliques ne l'est pas forcément ! Par exemple, $(\mathbb{Z}/2\mathbb{Z})^2$ n'est pas cyclique car tous ses éléments sont d'ordre 1 ou 2 (et donc il n'a aucun élément d'ordre 4) : un groupe commutatif n'est pas cyclique en général. Cependant, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ admet un élément d'ordre 6 (cf. paragraphe II.3 du cours) donc est cyclique et isomorphe à $\mathbb{Z}/6\mathbb{Z}$: c'est un cas particulier du lemme chinois (cf. cours de deuxième année).

DÉMONSTRATION. Si G est cyclique d'ordre n alors G est engendré par un élément d'ordre n (voir ci-dessus). En particulier, G admet un élément d'ordre n . Réciproquement, si G admet un élément d'ordre n noté x , alors, par définition de l'ordre d'un groupe, $\text{gr}(x)$ est un sous-groupe de G d'ordre n donc il est égal à n tout entier, si bien que $G = \text{gr}(x)$: G est cyclique.

On a même montré que tout élément x d'ordre n engendre G c'est-à-dire que $G = \{e; x; x^2; \dots; x^{n-1}\}$.

II Botanique des groupes

II.1 Groupes d'ordre un nombre premier

Proposition. Soit G un groupe d'ordre p premier. Alors tous les éléments de G à part le neutre sont d'ordre p . En particulier, G est cyclique et donc est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

DÉMONSTRATION. Soit $x \neq e$ un élément de G . Puisque $x \neq e$, alors l'ordre de x est différent de 1. Or, l'ordre de x divise le cardinal du groupe donc divise p qui est premier donc est égal à p . Il en découle que G est cyclique engendré par x .

Exemples : À isomorphisme près, il n'y a qu'un groupe d'ordre 3, $\mathbb{Z}/3\mathbb{Z}$ (ou le groupe {chou; banane; carotte} qui lui est donc isomorphe), qu'un seul groupe d'ordre 5, $\mathbb{Z}/5\mathbb{Z}$, et qu'un seul groupe d'ordre 7, $\mathbb{Z}/7\mathbb{Z}$.

En d'autres termes, il n'y a qu'un seul groupe d'ordre p à isomorphisme près : $\mathbb{Z}/p\mathbb{Z}$.

II.2 Groupes d'ordre 4

On veut dans ce paragraphe donner tous les groupes à 4 éléments (à isomorphisme près, c'est-à-dire qu'on veut donner tous les modèles de groupes à 4 éléments). On a déjà vu deux modèles de groupes différents : $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$ qui ne sont pas isomorphes car l'un contient un élément d'ordre 4 et l'autre n'en a aucun (ou car l'un est cyclique et l'autre non). Prouvons qu'il n'y en a pas d'autre.

Soit G un groupe à 4 éléments. On sait que l'ordre d'un élément divise l'ordre du groupe et que le seul élément d'ordre 1 est le neutre. Par conséquent, soit G contient un élément d'ordre 4, et alors il est cyclique et isomorphe à $\mathbb{Z}/4\mathbb{Z}$, soit tous les éléments du groupe distincts du neutre sont d'ordre 2, ce qu'on suppose à présent.

Soient a et b deux éléments de G distincts et distincts du neutre e . Montrons que $G = \{e; a; b; ab\}$. e, a et b sont distincts par hypothèse. De plus, $ab \neq a$ car, si $ab = a$, alors $b = e$ car tout élément d'un groupe est régulier (ou en multipliant par a^{-1} à gauche) ce qui est exclu. De même, $ab \neq b$. Enfin, $a^2 = e$ car a est d'ordre 2 donc $ab \neq e$ car, si $ab = e$ alors $ab = a^2$ donc $a = b$ ce qui est exclu. Il en découle que e, a, b et ab sont distincts et G a 4 éléments donc $G = \{e; a; b; ab\}$.

Donnons la table de G .

*	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$(\mathbb{Z}/2\mathbb{Z})^2$ est souvent noté V_4 et appelé Vierergruppe ou groupe de Klein : c'est le plus petit groupe non cyclique.

- La première ligne et la première colonne viennent du fait que e est le neutre.
- Tout élément hormis e est d'ordre 2 : d'où la diagonale.
- Puisque $a^2 = e$, $a(ab) = (aa)b = eb = b$ (la loi est associative). D'où la deuxième ligne.
- ba est distinct de a, b et e de même que ci-dessus donc $ba = ab$. Dès lors, $b(ab) = (ba)b = (ab)b = a(bb) = ae = a$. D'où la troisième ligne.
- De même, en utilisant le fait que $ba = ab$ et que $a^2 = b^2 = e$, on trouve la dernière ligne.

Puisque $ab = ba$, le groupe est abélien. C'est un résultat classique (cf. exercice 19) : un groupe dont tous les éléments sont d'ordre 1 ou 2 est abélien.

Il existe donc **au plus** deux groupes à 4 éléments. Pourquoi « au plus » ? Car, attention, on a fait sans le dire un raisonnement par analyse synthèse : on a supposé l'existence d'un groupe d'ordre 4 dont tous les éléments sauf le neutre sont d'ordre 2 et on en a déduit sa table. Il reste à faire la synthèse. Deux options ici :

- Vérifier qu'on a bien un groupe : loi associative, neutre, inverse. C'est un peu long mais ça se fait (et parfois on n'a pas le choix, voir l'exemple du groupe des quaternions dans la suite).
- Soit reconnaître une table qu'on connaît déjà : la synthèse (c'est-à-dire l'existence) est donc automatique. Et ici, on reconnaît la table de $(\mathbb{Z}/2\mathbb{Z})^2$. La table donne donc une structure de groupe (car c'est la table d'un ensemble dont on sait déjà qu'il est un groupe) et deux groupes ayant cette table sont isomorphes : G est donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Plus précisément, on montre facilement que la fonction $f : G \rightarrow (\mathbb{Z}/2\mathbb{Z})^2$ définie par $f(e) = (\bar{0}, \bar{0})$, $f(a) = (\bar{1}, \bar{0})$, $f(b) = (\bar{0}, \bar{1})$ et $f(ab) = (\bar{1}, \bar{1})$ est un isomorphisme.

En conclusion, il existe deux groupes à 4 éléments à isomorphisme près : $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$.

II.3 Groupes d'ordre 6

Donnons là aussi tous les groupes d'ordre 6 à isomorphisme près. Soit G un groupe à 6 éléments

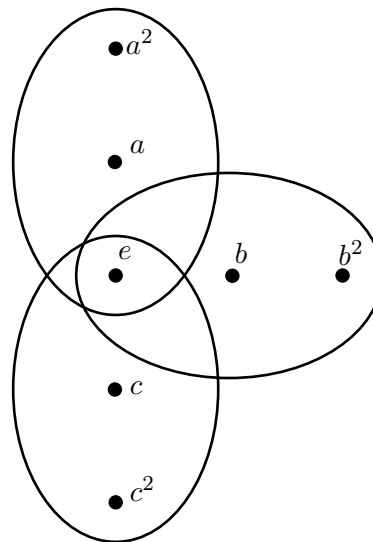
Puisque l'ordre d'un élément divise l'ordre du groupe, les éléments du groupe (à part le neutre) sont d'ordre 2, 3 ou 6. Montrons qu'il existe un élément d'ordre 2 et un élément d'ordre 3. Plusieurs cas de figure se présentent : soit tous les éléments (sauf le neutre) sont d'ordre 2, soit ils sont tous d'ordre 3, soit il y a au moins un élément d'ordre 6, soit il n'y a aucun élément d'ordre 6 mais au moins un élément d'ordre 2 et un élément d'ordre 3.

Là aussi, on fait sans le dire un raisonnement par analyse synthèse sans le dire.

- Supposons que tous les éléments de G sauf e soient d'ordre 2. Soient a et b deux éléments de G distincts et distincts de e . Alors, en utilisant le fait que G est commutatif (cf. exercice 19), on montre aisément que $H = \{e; a; b; ab\}$ est un sous-groupe de G car stable par produit (car le groupe est commutatif) et par inverse puisque tout élément est son propre inverse. Or, un groupe à 6 éléments ne peut pas admettre un sous-groupe à 4 éléments d'après le théorème de Lagrange. En conclusion, il n'est pas possible que tous les éléments de G à part le neutre soient d'ordre 2.
- Supposons que tous les éléments sauf le neutre soient d'ordre 3. Soit $a \in G$ distinct de e . Puisque a est d'ordre 3, son groupe engendré contient trois éléments et est égal à $\text{gr}(a) = \{e; a; a^2\}$. Soit $b \in G \setminus \text{gr}(a)$. De même, $\text{gr}(b) = \{e; b; b^2\}$. Or, on sait (cf. paragraphe III.4 du cours) que l'intersection de deux groupes distincts à 3 éléments est réduite à $\{e\}$: en effet, l'intersection de ces deux groupes est un groupe donc est un sous-groupe de $\text{gr}(a)$ et $\text{gr}(b)$. D'après le théorème de Lagrange, le cardinal de l'intersection vaut 1 ou 3, mais ce cas est exclu car sinon les deux ensembles seraient confondus, ce qui n'est pas car $b \notin \text{gr}(a)$.

On peut s'en tirer sans théorème de Lagrange : $b \notin \text{gr}(a)$ par hypothèse et si $b^2 \in \text{gr}(a)$ alors $b^2 = e$ ou $b^2 = a$ ou $b^2 = a^2$ mais aucun cas n'est possible. $b^2 \neq e$ car b est d'ordre 3. Si $b^2 = a$ alors $b^4 = a^2$. Or, $b^4 = b$ car $b^3 = e$ donc $b = a^2 \in \text{gr}(a)$ ce qui est contraire à l'hypothèse. On exclut le cas $b^2 = a^2$ de la même façon.

Il en découle que e, a, a^2, b, b^2 sont 5 éléments distincts : il ne reste qu'un élément c dans G privé de $\text{gr}(a)$ et de $\text{gr}(b)$. Cependant, c étant aussi d'ordre 3, $\text{gr}(c) = \{e; c; c^2\}$ et on montre comme précédemment que c^2 n'appartient ni à $\text{gr}(a)$ ni à $\text{gr}(b)$ et il est distinct de e et de c ce qui fait un septième élément distinct des autres : absurde puisque G n'a que 6 éléments.



On a une configuration en « bataille navale ».

En conclusion, il n'est pas possible que tous les éléments de G sauf le neutre soient d'ordre 3.

- Si G admet un élément a d'ordre 6, alors a^2 est d'ordre 3 (puisque a^2 et a^4 sont distincts de e) et a^3 est d'ordre 2 donc G contient bien un élément d'ordre 2 et un élément d'ordre 3.
- Dans le dernier cas, il n'y a rien à prouver.

En conclusion, dans tous les cas, G contient un élément d'ordre 2 qu'on notera a et un élément d'ordre 3 qu'on notera b . Montrons que $G = \{e; a; b; b^2; ab; ab^2\}$.

- a et b sont distincts et distincts de e puisque a est d'ordre 2 et b d'ordre 3.
- b^2 est distinct de e car b est d'ordre 3. Si $b^2 = b$ alors (tout élément est régulier), $b = e$ ce qui est exclu. Enfin, $b^3 = e$ donc $b^4 = b \neq e$: b^2 n'est pas d'ordre 2 donc $b^2 \neq a$.
- a est d'ordre 2 donc est son propre inverse donc b n'est pas l'inverse de a : on en déduit que $ab \neq e$. Tout élément est régulier et $b \neq e$ donc $ab \neq a$. De même, $ab \neq b$ et $ab \neq b^2$.
- $b^2 \neq a$ donc b^2 n'est pas l'inverse de a donc $ab^2 \neq e$. Ensuite, en utilisant la régularité, on exclut les autres cas, par exemple $ab^2 \neq a$ car $b^2 \neq e$ etc.

Les 6 éléments sont distincts, ce qui donne le résultat voulu. Donnons à présent la table de G . Ce qui suit est immédiat car e est le neutre, a d'ordre 2 et b d'ordre 3 :

*	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b		b^2	e		
b^2	b^2		e	b		
ab	ab		ab^2	a		
ab^2	ab^2		a	ab		

On cherche ba . Par régularité, on ne peut pas avoir $ba = b$, $ba = b^2$ ou $ba = e$ car $a^2 = e$. De plus, on ne peut pas avoir $ba = a$. Finalement, $ba = ab$ ou $ba = ab^2$. Faisons deux cas de figure.

- Premier cas : $ba = ab$. Alors a et b commutent et puisque tous les éléments du groupe s'écrivent à l'aide de a et de b , G est commutatif. Mais il suffit de regarder chaque cas de figure et d'utiliser l'associativité de la loi. $ba = ab$ donc (par associativité de la loi) :

$$\begin{aligned} b(ab) &= (ba)b \\ &= (ab)b \\ &= a(bb) \\ &= ab^2 \end{aligned}$$

et puisque $b(ab^2) = (bab)b$ (associativité), il vient $b(ab^2) = ab^2b = a$. Les autres lignes s'obtiennent de façon analogue (toujours par associativité en utilisant le fait que $ab = ba$).

*	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab	b^2	e	ab^2	a
b^2	b^2	ab^2	e	b	a	ab
ab	ab	b	ab^2	a	b^2	e
ab^2	ab^2	b^2	a	ab	e	b

- Deuxième cas : $ba = ab^2$. De même, en utilisant l'associativité de la loi, on finit par remplir le tableau. Par exemple,

$$\begin{aligned} b(ab) &= (ba)b \\ &= (ab^2)b \\ &= a(b^2b) \\ &= ab^3 \\ &= a \end{aligned}$$

*	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

Il en découle qu'il y a au plus deux groupes à 6 éléments : un abélien et un non abélien. Les deux mêmes options que ci-dessus se représentent :

- Vérifier qu'on a bien un groupe.
- Soit reconnaître une table qu'on connaît déjà.

Or, il se trouve qu'on connaît déjà deux groupes à 6 éléments, l'un abélien et l'autre non : $\mathbb{Z}/6\mathbb{Z}$ et S_3 (qui sont donc non isomorphes). Par conséquent, les deux tables ci-dessus sont bien des tables de groupes, celle du groupe abélien étant celle du groupe $\mathbb{Z}/6\mathbb{Z}$ et celle du groupe non abélien étant celle de S_3 . Si on veut s'en convaincre encore plus, dans le cas où $ab = ba$, on écrit :

+	e	ab	b^2	a	b	ab^2
e	e	ab	b^2	a	b	ab^2
ab	ab	b^2	a	b	ab^2	e
b^2	b^2	a	b	ab^2	e	ab
a	a	b	ab^2	e	ab	b^2
b	b	ab^2	e	ab	b^2	a
ab^2	ab^2	e	ab	b^2	a	b

On reconnaît la table de $\mathbb{Z}/6\mathbb{Z}$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

On reconnaît également la table de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (cf. paragraphe II.3 du cours). Il en découle que tous ces groupes sont isomorphes, et plus généralement qu'un groupe à 6 éléments abélien est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ (et donc est cyclique).

Enfin, dans le cas où $ba = ab^2$, c'est forcément la table de S_3 car S_3 est un groupe non abélien à 6 éléments. Nous verrons sa table au chapitre 32 quand nous verrons plus en détail le groupe symétrique. En particulier, puisque tout groupe d'ordre 1, 2, 3, 4, 5 est abélien (voir ci-dessus), S_3 est le plus petit groupe non abélien.

Plus généralement, si a et b sont premiers entre eux, $\mathbb{Z}/ab\mathbb{Z}$ est isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, cf. programme de deuxième année

II.4 Le groupe des quaternions

Nous n'allons pas donner tous les groupes d'ordre 8 (il y en a 5 à isomorphisme près, cf. exercice 41) mais utiliser les mêmes méthodes que dans les paragraphes précédents pour donner la table d'un groupe particulier.

Soit G un groupe d'ordre 8 et supposons qu'il existe un élément $i \in G$ d'ordre 4 et que tout élément $x \in G \setminus \text{gr}(i)$ soit d'ordre 4. Donnons la table de G .

Notons 1 le neutre. Dès lors, $\text{gr}(i) = \{1; i; i^2; i^3\}$. Posons également $\varepsilon = i^2$ si bien que $i^3 = \varepsilon i$ et donc $\text{gr}(i) = \{1; i; \varepsilon; \varepsilon i\}$ et que $\varepsilon^2 = 1$. Soit $j \in G \setminus \text{gr}(i)$ et posons $k = ij$. Montrons que $G = \{1; i; \varepsilon; \varepsilon i; j; \varepsilon j; k; \varepsilon k\}$.

cf. paragraphe VI.3 du cours : il y a une analogie entre i et le complexe i , et alors $\varepsilon = -1$. Nous gardons la notation ε pour qu'il n'y ait pas de confusion, mais nous pouvons garder en tête l'identification « $\varepsilon = -1$ » tout en étant très prudent avec elle.

- i étant d'ordre 4, 1, i, i^2 et i^3 sont distincts.
- j n'appartient pas à $\text{gr}(i)$ donc j est distinct de ces 4 éléments par hypothèse.
- Si $\varepsilon j \in \text{gr}(i)$ alors, en multipliant à gauche par $\varepsilon \in \text{gr}(i)$, $j \in \text{gr}(i)$ car celui-ci est stable par produit, ce qui est absurde. De plus, $\varepsilon j \neq j$ par régularité et car $\varepsilon \neq 1$. Ainsi, εj est distinct des 5 éléments précédents.
- Puisque $k = ij$, si $k \in \text{gr}(i)$ alors, en multipliant à gauche par $i^3 \in \text{gr}(i)$, $j \in \text{gr}(i)$ de la même façon ce qui est absurde. Ainsi, k est distinct de 1, i, ε et εi . Par régularité, k est distinct de j et de εj puisque i est distinct de i et de ε .
- Idem. Ces 8 éléments sont donc distincts et G a 8 éléments, d'où le résultat.

Donnons à présent la table de G . La sous-table de $\text{gr}(i)$ est immédiate puisque $\varepsilon = i^2$ et $i^4 = 1$. En particulier, $\text{gr}(i)$ est abélien (il est même isomorphe à $\mathbb{Z}/4\mathbb{Z}$).

De plus, par hypothèse, tous les éléments de $G \setminus \text{gr}(i)$ sont d'ordre 4. Il en découle que ε est le seul élément d'ordre 2 de G . Or, j et k sont d'ordre 4 donc j^2 et k^2 sont d'ordre 2, si bien que $j^2 = k^2 = \varepsilon$.

Il en découle que ε commute avec i, j et k . En effet, $\varepsilon = j^2$ donc (la loi est associative) :

$$\begin{aligned}\varepsilon j &= j^2 \times j \\ &= j^3 \\ &= j \times j^2 \\ &= j\varepsilon\end{aligned}$$

et de même pour les autres. De plus, $ij = k$ donc $ik = i(ij) = (ii)j = \varepsilon j$ et de même on trouve $i \times \varepsilon k = j$ (la loi est associative et ε commute avec tout le monde). On en déduit le début de la table de G :

En rouge la table de $\text{gr}(i)$, sous-groupe de G isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

+	1	i	ε	εi	j	εj	k	εk
1	1	i	ε	εi	j	εj	k	εk
i	i	ε	εi	1	k	εk	εj	j
ε	ε	εi	1	i	εj	j	εk	k
εi	εi	1	i	ε	εk	k	j	εj
j	j		εj		ε	1		
εj	εj		j		1	ε		
k	k		εk		εi	i	ε	1
εk	εk		ε		i	εi	1	ε

Pour conclure, il suffit de donner la valeur de ji : on pourra ensuite conclure avec l'associativité de la loi, le fait que $i^2 = j^2 = k^2 = \varepsilon$ et le fait que $\varepsilon^2 = 1$. Or, $ji \neq \varepsilon = i^2$ puisque $j \neq i$ et car tout élément de G est régulier (si $ji = i^2$ alors $j = i$ ce qui est exclu). De même,

$ji \neq 1$ car $j \neq \varepsilon i$ si bien que ji est d'ordre 4 (tous les éléments de G sont d'ordre 4 sauf ε qui est d'ordre 2 et 1 qui est d'ordre 1). Il en découle que $(ji)^2$ est d'ordre 2 donc $(ji)^2 = \varepsilon$. Par associativité de la loi, $(ji)^2 = (ji)(ji) = j(ij)i = \varepsilon$ et donc, en multipliant par j à gauche, par i à droite, il vient : $j^2(ij)i^2 = j\varepsilon i$. Dès lors, comme ε commute avec tout le monde, $\varepsilon \times ij \times \varepsilon = \varepsilon ji$ donc $ji = \varepsilon ij$. En d'autres termes, on peut inverser l'ordre entre i et j à condition de multiplier par ε (et en particulier $ji = \varepsilon k$). On en déduit facilement le reste de la table :

+	1	i	ε	εi	j	εj	k	εk
1	1	i	ε	εi	j	εj	k	εk
i	i	ε	εi	1	k	εk	εj	j
ε	ε	εi	1	i	εj	j	εk	k
εi	εi	1	i	ε	εk	k	j	εj
j	j	εk	εj	k	ε	1	i	εi
εj	εj	k	j	εk	1	ε	εi	i
k	k	j	εk	εj	εi	i	ε	1
εk	εk	εj	ε	j	i	εi	1	ε

On peut écrire, dans l'ordre : i, j, k . Le produit de deux éléments consécutifs (de la gauche vers la droite) donne l'élément suivant (par exemple, $ki = j$), et si on va de la droite vers la gauche, il faut multiplier par ε (par exemple, $ji = \varepsilon k$).

Comme précédemment, on vient de terminer la phase analyse : si un groupe G vérifie ces conditions, il est unique. Pour la synthèse, ici, le problème est que cette table ne correspond à aucun groupe à 8 éléments connu : ce n'est pas la table de $\mathbb{Z}/8\mathbb{Z}$ car il n'y a aucun élément d'ordre 8, ni celle de $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ car celui-ci contient deux éléments d'ordre 2 (exo), ni celle de $(\mathbb{Z}/2\mathbb{Z})^3$ car celui-ci n'a que des éléments d'ordre 1 ou 2. Il faut donc vérifier les conditions à la main : il y a bien un neutre, tout élément admet bien un inverse, et il faudrait vérifier l'associativité, ce qui serait fastidieux mais pas difficile. On peut heureusement s'en passer grâce aux matrices : cf. exercice 21 du chapitre 21.

Ce (modèle de) groupe est noté \mathbb{H}_8 et est appelé groupe des quaternions : cf. paragraphe VI.3 du cours.