

Groupes

I. Sous-groupe engendré par une partie

Dans tout le chapitre, $(G, \cdot)$ désigne un groupe de neutre e . On note x^k les puissances d'un élément x pour $k \in \mathbb{Z}$. En notation additive, on écrit plutôt kx et le neutre se note 0 . Les règles $x^{k+l} = x^k x^l$ et $(x^k)^l = x^{kl}$ sont vraies dans tout groupe. En revanche, l'égalité $(xy)^k = x^k y^k$ exige que x et y commutent.

1. Intersection de sous-groupes

La réunion de deux sous-groupes n'est pas un sous-groupe en général. Par exemple, $2\mathbb{Z} \cup 3\mathbb{Z}$ contient 2 et 3 mais pas 5 . L'intersection, en revanche, se comporte bien.

Proposition :

Soit $(H_i)_{i \in I}$ une famille non vide de sous-groupes de G . Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Démonstration :

Notons H cette intersection. D'abord, e appartient à chaque H_i , donc à H . Ensuite, soient $x, y \in H$. Pour tout i , on a $x, y \in H_i$, donc $xy^{-1} \in H_i$ car H_i est un sous-groupe. Par conséquent, $xy^{-1} \in H$, ce qui prouve que H est un sous-groupe.

2. Sous-groupe engendré

Définition :

Soit A une partie de G . Le **sous-groupe engendré** par A , noté $\langle A \rangle$, est l'intersection de tous les sous-groupes de G qui contiennent A . C'est le plus petit sous-groupe de G contenant A . On dit que A est une **partie génératrice** de G si $\langle A \rangle = G$.

Cette définition est abstraite. Heureusement, on dispose d'une description concrète des éléments de $\langle A \rangle$.

Théorème :

Si A est non vide, $\langle A \rangle$ est l'ensemble des produits finis $a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_r^{\varepsilon_r}$ avec $r \geq 1$, $a_j \in A$ et $\varepsilon_j \in \{-1, 1\}$. Si G est commutatif et noté additivement, et si $A = \{a_1, \dots, a_p\}$, alors

$$\langle A \rangle = \left\{ k_1 a_1 + \dots + k_p a_p, \right. \\ \left. (k_1, \dots, k_p) \in \mathbb{Z}^p \right\}.$$

En particulier, $\langle x \rangle = \left\{ x^k, \right. \\ \left. k \in \mathbb{Z} \right\}.$

Démonstration :

Notons P l'ensemble de ces produits. D'abord, P est un sous-groupe. En effet, il contient $a a^{-1} = e$ pour $a \in A$. De plus, le produit de deux éléments de P est encore dans P , et l'inverse de $a_1^{\varepsilon_1} \dots a_r^{\varepsilon_r}$ vaut $a_r^{-\varepsilon_r} \dots a_1^{-\varepsilon_1}$, qui est dans P . Comme P contient A , on a $\langle A \rangle \subset P$. Inversement, tout sous-groupe contenant A contient les inverses des éléments de A et leurs produits. Il contient donc P . Ainsi, $P \subset \langle A \rangle$. Dans le cas commutatif, on regroupe les facteurs égaux, ce qui donne la seconde forme.

Exemple :

Dans $(\mathbb{Z}, +)$, on a $\langle 4, 6 \rangle = \{4u + 6v, (u, v) \in \mathbb{Z}^2\}$. Tout élément est pair. Inversement, $2 = 6 - 4$ appartient à $\langle 4, 6 \rangle$, donc tous les multiples de 2 aussi. Finalement, $\langle 4, 6 \rangle = 2\mathbb{Z}$.

Méthode :

Pour déterminer $\langle A \rangle$, on devine un sous-groupe candidat H , puis on raisonne par double inclusion. D'une part, on vérifie que H est un sous-groupe qui contient A : alors $\langle A \rangle \subset H$. D'autre part, on montre que chaque générateur « naturel » de H s'écrit à l'aide des éléments de A : alors $H \subset \langle A \rangle$.

II. Sous-groupes de $\mathbb{Z}$ et groupe $\mathbb{Z}/n\mathbb{Z}$

1. Sous-groupes de $(\mathbb{Z}, +)$

Pour tout entier n , l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$. Le théorème suivant affirme qu'il n'y en a pas d'autre.

Théorème :

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$. De plus, l'entier n est unique.

Démonstration :

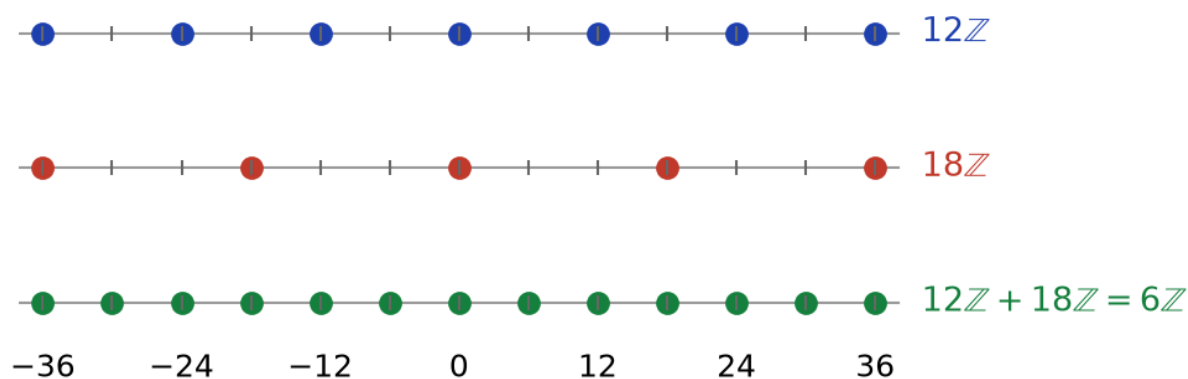
Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, H contient un entier non nul a , donc aussi $-a$. Ainsi, $H \cap \mathbb{N}^*$ est non vide et admet un plus petit élément n . Comme $n \in H$, tous ses multiples sont dans H : $n\mathbb{Z} \subset H$. Réciproquement, soit $h \in H$. La division euclidienne donne $h = qn + r$ avec $0 \leq r < n$. Or $r = h - qn$ appartient à H . Par minimalité de n , on obtient $r = 0$. Donc $h \in n\mathbb{Z}$. Enfin, n est le plus petit élément strictement positif de $n\mathbb{Z}$, d'où l'unicité.

Ce théorème fournit une définition « par les groupes » du pgcd et du ppcm. En effet, la somme $a\mathbb{Z} + b\mathbb{Z}$ et l'intersection $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$.

Propriété :

Pour $a, b \in \mathbb{N}^*$, on a $a\mathbb{Z} + b\mathbb{Z} = \langle a, b \rangle = d\mathbb{Z}$ où $d = a \wedge b$, et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ où $m = a \vee b$.

La figure ci-dessous illustre le cas $a = 12$ et $b = 18$. Les sommes d'un multiple de 12 et d'un multiple de 18 remplissent exactement les multiples de 6.



2. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n \geq 1$. La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. On note $\overline{k}$ la classe de k et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes.

Définition :

On pose $\overline{k} + \overline{l} = \overline{k+l}$. Cette addition est bien définie : si $k \equiv k'$ et $l \equiv l'$ modulo n , alors $k+l \equiv k'+l'$ modulo n . Muni de cette loi, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ est un groupe commutatif de cardinal n , de neutre $\overline{0}$.

L'application $k \rightarrow \overline{k}$ de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est un morphisme surjectif de noyau $n\mathbb{Z}$. Par ailleurs, on a $\overline{k}\overline{l} = \overline{kl}$. Ainsi, $\overline{1}$ engendre $\mathbb{Z}/n\mathbb{Z}$. Mais ce n'est pas le seul générateur.

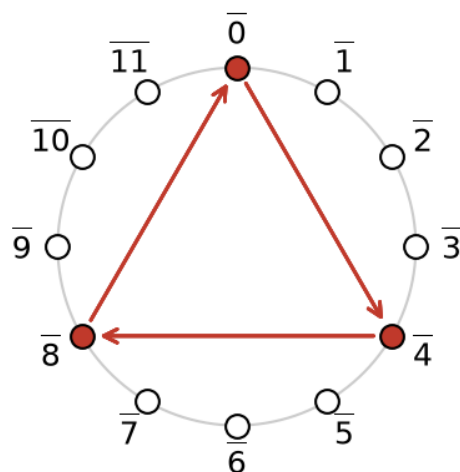
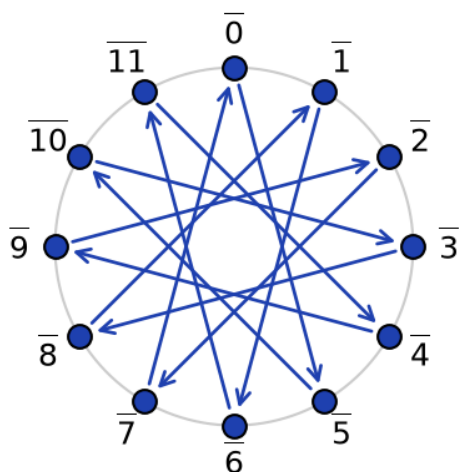
Théorème :

Soit $k \in \mathbb{Z}$. La classe $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

Démonstration :

Supposons que $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$. Alors $\overline{1}$ est un multiple de $\overline{k}$: il existe $u \in \mathbb{Z}$ tel que $u\overline{k} = \overline{1}$. Autrement dit, n divise $uk - 1$, donc il existe v tel que $uk + vn = 1$. Le théorème de Bézout donne $k \wedge n = 1$. Réciproquement, si $k \wedge n = 1$, on écrit $uk + vn = 1$. Alors $u\overline{k} = \overline{1}$. Par conséquent, $\overline{1}$ appartient à $\langle \overline{k} \rangle$, et donc tout $\overline{j} = j\overline{1}$ aussi.

La figure suivante représente $\mathbb{Z}/12\mathbb{Z}$ comme un cadran. En ajoutant $\overline{5}$ de proche en proche, on visite les douze classes, car $5 \wedge 12 = 1$. En revanche, les multiples de $\overline{4}$ ne forment qu'un triangle.



multiples de $\bar{5}$: on parcourt les 12 classes multiples de $\bar{4}$: on reste dans 3 classes

Méthode :

Pour lister les générateurs de $\mathbb{Z}/n\mathbb{Z}$, on décompose n en facteurs premiers. On garde ensuite les entiers $k \in \llbracket 1, n \rrbracket$ divisibles par aucun de ces facteurs. Pour $n = 12 = 2^2 \times 3$, on garde 1, 5, 7, 11. Pour exprimer $\bar{1}$ comme multiple d'un générateur $\bar{k}$, on utilise une relation de Bézout $uk + vn = 1$.

III. Ordre d'un élément d'un groupe

1. Définition et caractérisation

Définition :

Un élément $x \in G$ est dit **d'ordre fini** s'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$. Le plus petit tel entier s'appelle l'**ordre** de x . Sinon, on dit que x est d'ordre infini.

L'énoncé fondamental du chapitre relie l'ordre à la divisibilité. On le citera sans cesse.

Théorème :

Soit $x \in G$ d'ordre fini d . Alors, pour tout $k \in \mathbb{Z}$,

$$x^k = e \Leftrightarrow d \mid k.$$

De plus, $\langle x \rangle = \{e, x, x^2, \dots, x^{d-1}\}$ et ces d éléments sont distincts. Ainsi, l'ordre de x est égal au cardinal de $\langle x \rangle$.

Démonstration :

L'ensemble $K = \left\{ k \in \mathbb{Z}, x^k = e \right\}$ est un sous-groupe de $\mathbb{Z}$. En effet, $0 \in K$ et $x^{k-l} = x^k (x^l)^{-1}$. D'après la partie II, $K = d'\mathbb{Z}$ où d' est le plus petit élément strictement positif de K . Or ce plus petit élément est précisément d . D'où l'équivalence. Ensuite, soit $k \in \mathbb{Z}$ et $k = qd + r$ sa division euclidienne. Alors $x^k = (x^d)^q x^r = x^r$ avec $0 \leq r \leq d-1$. Enfin, si $x^r = x^s$ avec $0 \leq r, s \leq d-1$, alors $d \mid r-s$, donc $r = s$.

Si x est d'ordre infini, le même raisonnement montre que les x^k , $k \in \mathbb{Z}$, sont deux à deux distincts. Dans ce cas, $\langle x \rangle$ est infini.

Exemple :

Dans $GL_2(\mathbb{R})$, la matrice $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ vérifie $R^2 = -I_2$, $R^3 = -R$ et $R^4 = I_2$. Elle est donc d'ordre 4. En revanche, $2I_2$ est d'ordre infini, car $(2I_2)^k = 2^k I_2 \neq I_2$ pour $k \geq 1$.

2. Ordre d'une puissance

Proposition :

Soit x d'ordre fini d et $k \in \mathbb{Z}$. Alors x^k est d'ordre $\frac{d}{d \wedge k}$. En particulier, dans $\mathbb{Z}/n\mathbb{Z}$, la classe $\overline{k}$ est d'ordre $\frac{n}{n \wedge k}$.

Démonstration :

Posons $\delta = d \wedge k$, $d = \delta d'$ et $k = \delta k'$, avec $d' \wedge k' = 1$. Pour $m \in \mathbb{Z}$, on a $(x^k)^m = e$ si et seulement si $d \mid km$, c'est-à-dire $d' \mid k' m$. D'après le lemme de Gauss, cela équivaut à $d' \mid m$. Donc l'ordre de x^k est $d' = d / \delta$.

Méthode :

Pour calculer l'ordre d'un élément x , on cherche un entier N tel que $x^N = e$. L'ordre est alors un diviseur de N . Ensuite, on teste les diviseurs N/p pour chaque facteur premier p de N . Si aucun ne convient, l'ordre vaut N . Par exemple, si $x^{12} = e$, $x^6 \neq e$ et $x^4 \neq e$, alors x est d'ordre 12.

IV. Groupes monogènes et groupes cycliques

1. Définitions

Définition :

Un groupe G est **monogène** s'il existe $x \in G$ tel que $G = \langle x \rangle$. Un tel x est un générateur de G . Un groupe **cyclique** est un groupe monogène fini.

Par exemple, $(\mathbb{Z}, +)$ est monogène, engendré par 1 ou par -1 . De même, $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Un groupe monogène est toujours commutatif, car $x^k x^l = x^{k+l} = x^l x^k$.

2. Classification des groupes monogènes

Théorème :

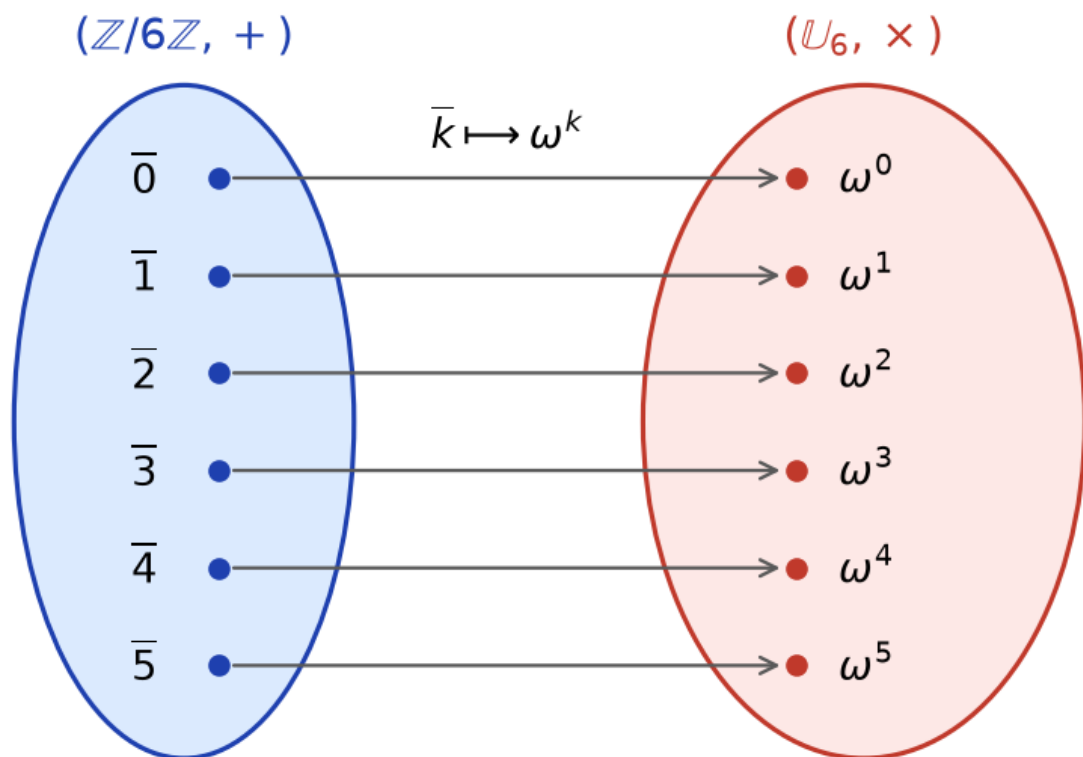
Soit $G = \langle x \rangle$ un groupe monogène.

- Si G est infini, l'application $k \rightarrow x^k$ est un isomorphisme de $(\mathbb{Z}, +)$ sur G .
- Si G est fini de cardinal n , l'application $\bar{k} \rightarrow x^k$ est un isomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ sur G .

Démonstration :

L'application $\varphi : k \rightarrow x^k$ est un morphisme de $\mathbb{Z}$ dans G , surjectif par définition de $\langle x \rangle$. Son noyau est $\left\{ \begin{matrix} k, \\ x^k = e \end{matrix} \right\}$. Si G est infini, x est d'ordre infini, donc ce noyau vaut $\{0\}$ et φ est injectif. Si G est fini de cardinal n , alors x est d'ordre n d'après la partie III. Le noyau vaut donc $n\mathbb{Z}$. Posons alors $\psi(\bar{k}) = x^k$. Cette définition ne dépend pas du représentant : si $k \equiv l$ modulo n , alors $x^k - l = e$. Ensuite, ψ est un morphisme surjectif. Enfin, $\psi(\bar{k}) = e$ impose $n \mid k$, soit $\bar{k} = \bar{0}$. Donc ψ est injectif.

La figure ci-dessous montre cet isomorphisme pour le groupe des racines sixièmes de l'unité. L'addition des classes modulo 6 correspond au produit des racines.



$\omega = e^{2i\pi/6}$: l'addition des classes devient le produit des racines

Remarque :

Un isomorphisme envoie un générateur sur un générateur. Ainsi, un groupe cyclique d'ordre n possède exactement autant de générateurs que $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire autant d'entiers de $\llbracket 1, n \rrbracket$ premiers avec n . Ce nombre sera noté $\varphi(n)$ dans le chapitre d'arithmétique.

Méthode :

Pour montrer qu'un groupe fini G de cardinal n est cyclique, il suffit d'exhiber un élément d'ordre n . En effet, $\langle x \rangle$ a alors n éléments et coïncide avec G . Pour l'identifier à $\mathbb{Z}/n\mathbb{Z}$, on utilise l'isomorphisme $\bar{k} \rightarrow x^k$ du théorème.

3. Sous-groupes d'un groupe cyclique

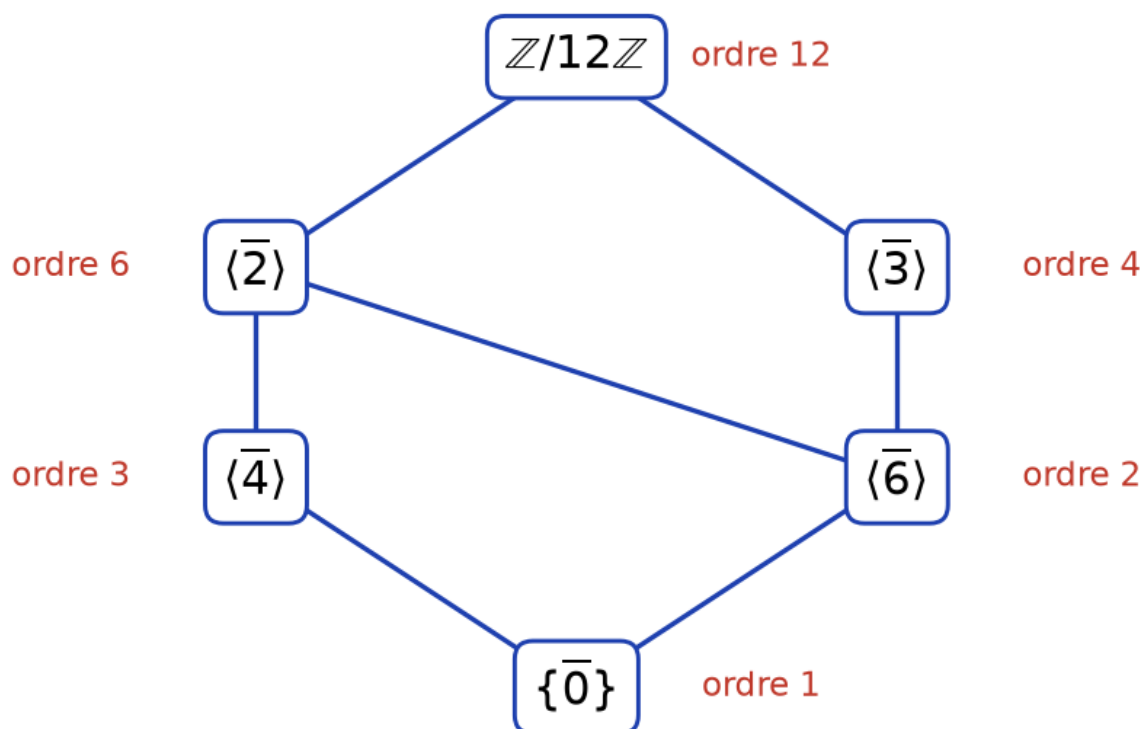
Proposition :

Soit $G = \langle x \rangle$ cyclique d'ordre n . Tout sous-groupe de G est cyclique. De plus, pour chaque diviseur d de n , il existe un unique sous-groupe d'ordre d : c'est $\langle x^{n/d} \rangle$.

Démonstration :

Soit H un sous-groupe de G . L'ensemble $K = \left\{ \begin{matrix} k \\ , \mathbb{Z}, \\ , x^k \in H \end{matrix} \right\}$ est un sous-groupe de $\mathbb{Z}$ contenant n . Donc $K = a\mathbb{Z}$ avec $a \geq 1$ et $a \mid n$. Par suite,
 $H = \left\{ x^k, \begin{matrix} k \in a\mathbb{Z} \end{matrix} \right\} = \langle x^a \rangle$. D'après la partie III, x^a est d'ordre n/a . Ainsi, H est d'ordre d si et seulement si $a = n/d$.

Le diagramme suivant représente les six sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, un par diviseur de 12. Un trait relie deux sous-groupes quand le plus petit est inclus dans le plus grand.



V. Groupe des racines n-ièmes de l'unité

Soit $n \geq 1$. On note $\mathbb{U}_n = \left\{ z \in \mathbb{C}, z^n = 1 \right\}$. C'est un sous-groupe du groupe $(\mathbb{U}, \times)$ des complexes de module 1.

Théorème :

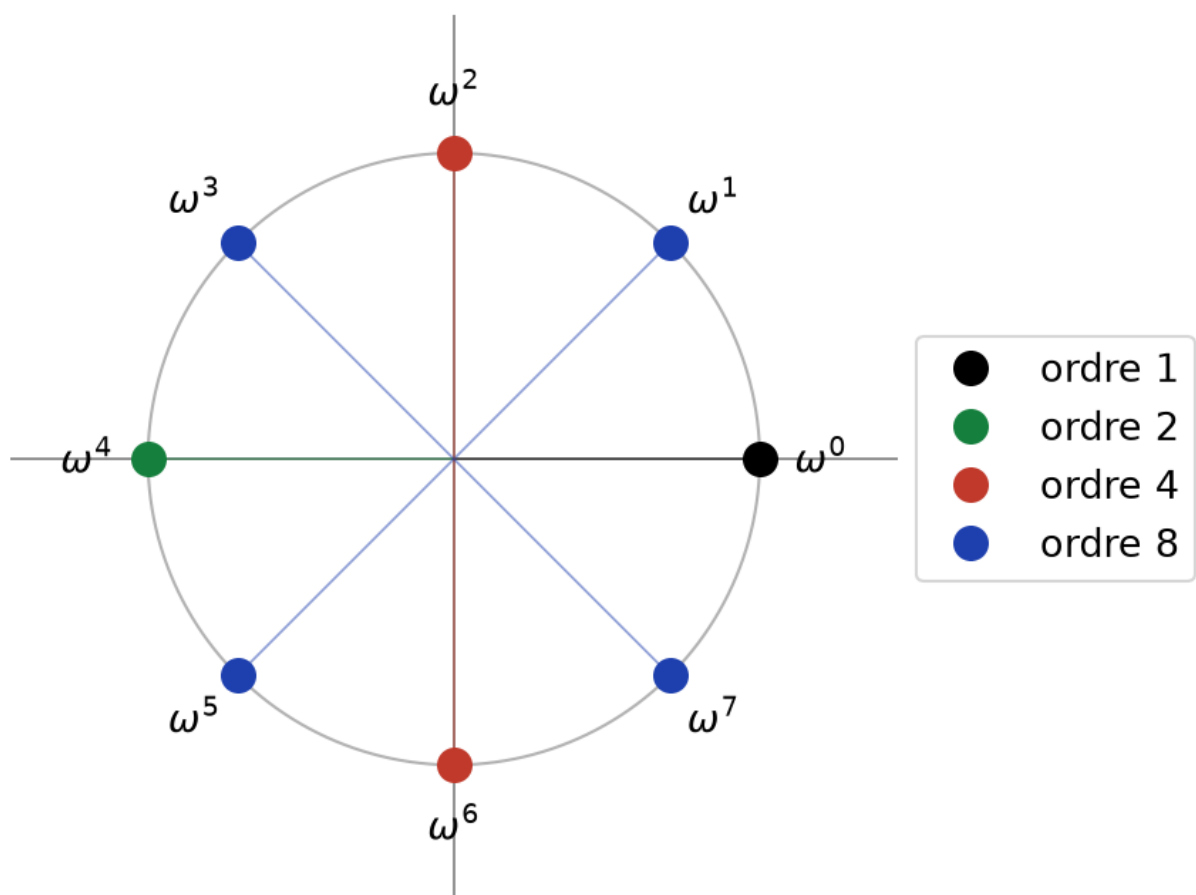
Posons $\omega = e^{2i\pi/n}$. Alors $\mathbb{U}_n = \left\{ \omega^k, 0 \leq k \leq n-1 \right\}$ est cyclique d'ordre n , engendré par ω . L'élément ω^k est d'ordre $\frac{n}{k \wedge n}$. Les générateurs de $\mathbb{U}_n$, appelés racines primitives n -ièmes de l'unité, sont les ω^k avec $k \wedge n = 1$.

Démonstration :

Le cours de sup donne $\mathbb{U}_n = \{\omega^k, 0 \leq k \leq n-1\}$, avec n éléments distincts. Ainsi, ω est d'ordre n et engendre $\mathbb{U}_n$. Les autres points découlent de la proposition sur l'ordre d'une puissance et de la classification.

Exemple :

Dans $\mathbb{U}_8$, les racines primitives sont $\omega, \omega^3, \omega^5, \omega^7$. Ensuite, $\omega^2 = i$ et $\omega^6 = -i$ sont d'ordre 4, tandis que $\omega^4 = -1$ est d'ordre 2. La figure ci-dessous colore chaque racine huitième selon son ordre.



Attention :

Le groupe $(\mathbb{U}, \times)$ tout entier n'est pas monogène. En effet, un groupe monogène est l'image de $\mathbb{Z}$, donc il est fini ou dénombrable. Or $\mathbb{U}$ est en bijection avec $[0, 2\pi[$, qui n'est pas dénombrable.

VI. Théorème de Lagrange dans le cas commutatif

Dans $\mathbb{Z}/12\mathbb{Z}$ ou dans $\mathbb{U}_8$, on constate que l'ordre de chaque élément divise le cardinal du groupe. Ce phénomène est général.

Théorème :

Soit G un groupe **commutatif** fini de cardinal n . Pour tout $x \in G$, on a $x^n = e$. Par conséquent, l'ordre de tout élément de G divise n .

Démonstration :

Soit $x \in G$. L'application $\tau : y \rightarrow xy$ est une bijection de G sur G , de réciproque $y \rightarrow x^{-1}y$. Notons $P = \prod_{y \in G} y$, produit bien défini car G est commutatif. Comme τ permute les éléments de G , on a

$$P = \prod_{y \in G} (xy) = x^n \prod_{y \in G} y = x^n P.$$

En simplifiant par P , on obtient $x^n = e$. Enfin, d'après la partie III, l'ordre de x divise n .

Remarque :

Le résultat reste vrai dans un groupe fini quelconque. Cependant, sa démonstration générale n'est pas

exigible en MP. Pour un groupe non commutatif, on admettra donc le résultat s'il est rappelé par l'énoncé.

Corollaire :

Tout groupe commutatif de cardinal premier p est cyclique, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$. De plus, chacun de ses éléments distincts de e l'engendre.

Démonstration :

Soit $x \neq e$. Son ordre divise p et ne vaut pas 1. Il vaut donc p . Ainsi, $\langle x \rangle$ a p éléments et égale G .

Méthode :

Pour trouver l'ordre d'un élément d'un groupe commutatif fini de cardinal n , on ne teste que les diviseurs de n . Par exemple, dans un groupe commutatif de cardinal 35, les ordres possibles sont 1, 5, 7 et 35. Ainsi, un élément x tel que $x^5 \neq e$ et $x^7 \neq e$ engendre le groupe.

Ce qu'il faut retenir

- Une intersection de sous-groupes est un sous-groupe, et $\langle A \rangle$ est le plus petit sous-groupe contenant A .
- Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, et $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.
- La classe $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

- Si x est d'ordre d , alors $x^k = e \Leftrightarrow d \mid k$, et d est le cardinal de $\langle x \rangle$.
- L'ordre de x^k vaut $d / (d \wedge k)$.
- Un groupe monogène infini est isomorphe à $\mathbb{Z}$; un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- Un groupe cyclique d'ordre n possède un unique sous-groupe d'ordre d pour chaque diviseur d de n .
- $\mathbb{U}_n$ est cyclique, engendré par $e^{2i\pi/n}$, et ses générateurs sont les racines primitives.
- Dans un groupe commutatif fini de cardinal n , on a $x^n = e$: c'est le théorème de Lagrange.

Questions fréquentes sur groupes

Quelle différence entre groupe monogène et groupe cyclique ?

Un groupe est monogène s'il est engendré par un seul élément. Un groupe cyclique est un groupe monogène fini. Ainsi, $(\mathbb{Z}, +)$ est monogène mais pas cyclique, tandis que $(\mathbb{Z}/n\mathbb{Z}, +)$ et les racines n -ièmes de l'unité sont cycliques.

Comment trouver rapidement les générateurs de $\mathbb{Z}/n\mathbb{Z}$?

La classe de k engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k et n sont premiers entre eux. On liste donc les entiers de 1 à n premiers avec n . Par exemple, les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont les classes de 1, 5, 7 et 11.

Comment calculer l'ordre d'une puissance d'un élément ?

Si x est d'ordre n , alors x^k est d'ordre n divisé par $\text{pgcd}(n, k)$. Par exemple, dans un groupe où x est d'ordre 20, l'élément x^6 est d'ordre 10. La preuve repose sur l'équivalence entre $x^m = e$ et n divise m .

Le théorème de Lagrange est-il vrai dans un groupe non commutatif ?

Oui : dans tout groupe fini, l'ordre d'un élément divise le cardinal du groupe. Le programme de MP n'exige cependant la démonstration que dans le cas commutatif. Celle-ci utilise le produit de tous les éléments du groupe, qui est invariant par translation.

Pour aller plus loin en maths spé

- Les énoncés : [exercices de maths spé sur groupes](#)
- Chapitre suivant : [Anneaux, idéaux, \$\mathbb{Z}/n\mathbb{Z}\$ et algèbres](#)
- Le même thème en L2 : [groupes, cours de maths en L2](#)
- Tester vos connaissances : [QCM de maths spé par chapitre](#)
- Le sommaire : [tous les chapitres de maths spé](#) et les [chapitres de maths sup](#)