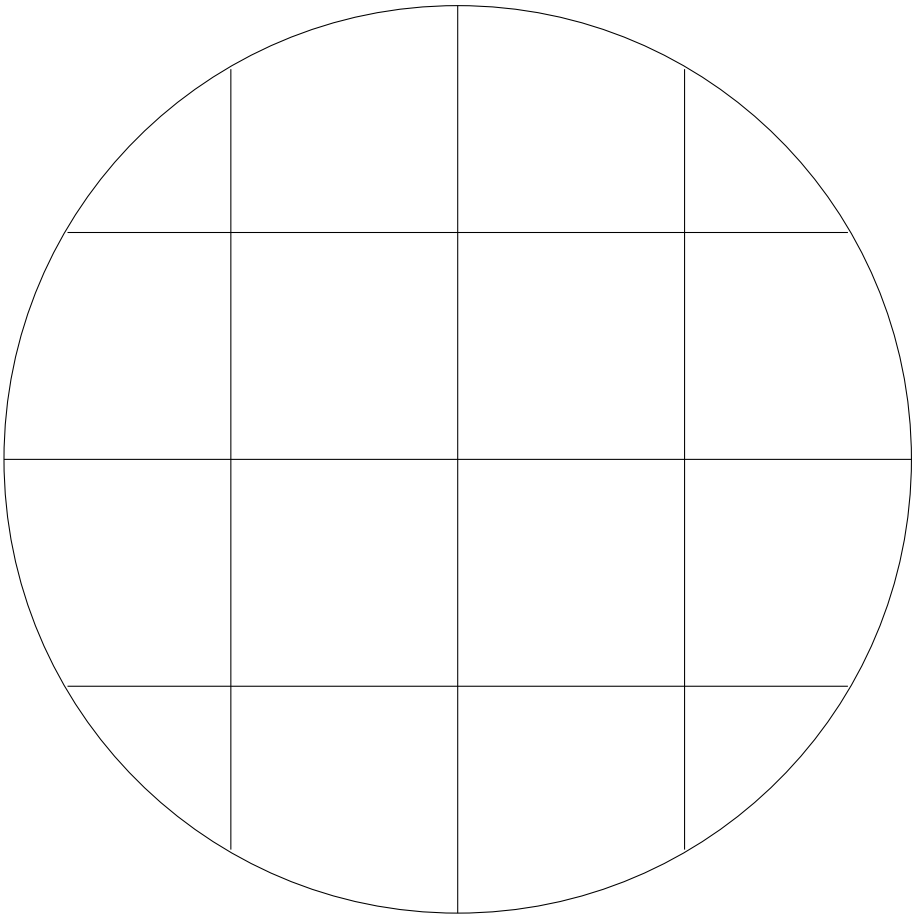
Ag8 : Groupes cycliques

I Isomorphisme entre $(\mathbf{U}_n, \times)$ et $(\mathbf{Z}/n\mathbf{Z}, +)$



II Sous-groupe engendré par un élément

II.1 Puissances d'un élément d'un groupe

Voir le **I.9.** du chapitre sur les structures (Ag1). Rappelons que, dans le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$, la « puissance n-ième » de l'élément x est, si $n \in \mathbf{N}_*$,

$$nx = \underbrace{x + \cdots + x}_{n \text{ fois}}$$

Et dans $(\mathbf{Z}/n\mathbf{Z}, \times)$? déjà, ce n'est pas un groupe. Bon, et dans $((\mathbf{Z}/n\mathbf{Z})^*, \times)$? la puissance est cette fois multiplicative, la terminologie est plus naturelle.

II.2 Elément d'ordre fini ; ordre d'un tel élément

Soit $(G, *)$ un groupe. Si $g \in G$, deux choses seulement peuvent se produire :
Cas 1 : La suite $e, g, g^2, g^3, \ldots$ est « infinie » ou, plus précisément, il n'y a pas deux éléments égaux dans cette suite.
Cas 2 : Cette suite est périodique.
On ne peut pas avoir de cas « bizarres » : suite de puissances seulement périodique à partir d'un certain rang, suite de puissances prenant une infinité de valeurs dont certaines plusieurs fois...Soyons plus précis :

Définition Soit $(G, *)$ un groupe, d'élément neutre e, soit $g \in G$. On dit que g est d'ordre fini lorsqu'il existe un entier naturel **non nul** n tel que $g^n = e$.

Est-il nécessaire d'insister sur la nécessité du « non nul » ? **Exemple** : montrer que si G est fini, tout g de G est d'ordre fini. **Exemple** : On munit $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}$ de l'addition « naturelle » (groupe produit de $(\mathbf{Z}/2\mathbf{Z}, +)$ et $(\mathbf{Z}, +)$). Quels sont les éléments d'ordre fini ?

Définition Soit g d'ordre fini. On définit l'ordre de g :

$$o(g) = \min\left(\{k \in \mathbf{N}_* \ ; \ g^k = e\}\right)$$

II.3 Morphisme associé à un élément d'un groupe ; sous-groupe engendré par cet élément

Proposition-Définition Soit $(G, *)$ un groupe. L'application

$$\begin{array}{rccc} \phi_g : & \mathbf{Z} & \longrightarrow & G \\ & k & \longmapsto & g^k \end{array}$$

est un morphisme du groupe $(\mathbf{Z}, +)$ dans le groupe $(G, *)$.

Vérification pas bien compliquée. Mais ce morphisme sert à tout...ou presque. D'abord, il est intéressant de regarder le noyau et l'image de ce morphisme.

L'image de ϕ_g est, par définition,

$$\{g^k \ ; \ k \in \mathbf{Z}\}$$

Mais remarquons surtout que

Proposition $\mathrm{Im}(\phi_g) = \{g^k \ ; \ k \in \mathbf{Z}\}$ est le sous-groupe de $(G, *)$ engendré par g. On le note souvent $\langle g \rangle$.

Le noyau de ϕ_g est, comme on le sait, un sous-groupe de $(\mathbf{Z}, +)$. C'est donc un certain $n\mathbf{Z}$, $n \in \mathbf{N}$. Deux cas très différents sont envisageables :

Si $\mathrm{Ker}(\phi_g) = \{0\}$, alors ϕ_g est injectif, le sous-groupe engendré par g est isomorphe à $(\mathbf{Z}, +)$.
Si $\mathrm{Ker}(\phi_g) = n\mathbf{Z}$, $n \geq 1$, le sous-groupe engendré par g est fini, on peut le décrire comme

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$$

Il est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. On peut en effet définir un isomorphisme entre $\mathbf{Z}/n\mathbf{Z}$ et $\langle g \rangle$:

III Ordre d'un élément et ordre du groupe ; théorème de Fermat, théorème d'Euler

III.1 L'ordre d'un élément divise l'ordre du groupe

Théorème Dans un groupe fini $(G,*)$ d'ordre $n \geq 1$ ($|G| = 1$), tout $g \in G$ vérifie : $g^n = 1$. Autrement dit, l'ordre de tout élément de G divise l'ordre de G.

Démonstration *Le programme suggère de ne démontrer que dans le cas d'un groupe commutatif. Mais le résultat est vrai que le groupe soit commutatif ou non.*

Commençons par un exemple ; on va montrer que, dans le groupe $\left(\mathbf{Z}/7\mathbf{Z}^*, \times\right)$, on a $\overline{2}^6 = \overline{1}$. Pour cela, on calcule

$$\underbrace{\overline{2} \times \overline{1}} \times \underbrace{\overline{2} \times \overline{2}} \times \underbrace{\overline{2} \times \overline{3}} \times \underbrace{\overline{2} \times \overline{4}} \times \underbrace{\overline{2} \times \overline{5}} \times \underbrace{\overline{2} \times \overline{6}} \times =$$

Parenthèse hors-programme : le théorème de Lagrange Si H est un sous-groupe d'un groupe fini $(G,*)$, alors $\sharp(H)$ divise $\sharp(G)$.

Démonstration (hors-programme évidemment !) Voir exercice. On en déduit une preuve du résultat précédent dans le cas général (sans hypothèse de commutativité du groupe) : si $(G,*)$ est un groupe d'ordre n, si $g \in G$, le sous-groupe engendré par g, $\langle g \rangle$, est tel que $\sharp(\langle g \rangle)$ divise $\sharp(G)$. Or l'ordre de g est précisément $\sharp(\langle g \rangle)$.

III.2 Théorèmes d'Euler et de Fermat

Théorème d'Euler : Soit $n \geq 2$, soit $x \in (\mathbf{Z}/n\mathbf{Z})^*$. Alors $x^{\phi(n)} = \overline{1}$.

Théorème de Fermat : Soit p un nombre premier, soit $x \in \mathbf{Z}/p\mathbf{Z} \setminus \{\overline{0}\}$. Alors $x^{p-1} = \overline{1}$

Théorème d'Euler : Soit $n \geq 2$, soit k un entier tel que $n \wedge k = 1$. Alors $k^{\phi(n)} \equiv 1\ [n]$.

Théorème de Fermat : Soit p un nombre premier, soit k un entier tel que $p \not| k$. Alors $k^{p-1} \equiv 1\ [p]$

Corollaire : Soit p un nombre premier, k un entier. Alors $k^p \equiv \quad [p]$

IV Groupes cycliques ; exemples

Définition Un groupe $(G, *)$ est dit cyclique lorsqu'il vérifie les deux conditions suivantes :
(i) G est fini.
(ii) Il existe un élément g de G tel que $G = \langle g \rangle$

Exemples $(\mathbf{Z}/n\mathbf{Z}, +)$, $(\mathbf{U}_n, \times)$.

V Isomorphisme entre les groupes cycliques de même ordre

Théorème vague Deux groupes cycliques d'ordre n sont isomorphes.

Il n'y a donc qu'une et une seule « structure » de groupe cycliques d'ordre n. Deux groupes cycliques d'ordre n peuvent contenir des objets très différents (un nombre complexe et une classe de congruence, ce n'est pas la même chose), mais ils ont la même structure, i.e. la même « forme ».

Théorème précis Soit $(G, *)$ un groupe cyclique d'ordre n, g un générateur de G. L'application

$$\psi : \overline{k} \longmapsto g^k$$

définit un isomorphisme de $(\mathbf{Z}/n\mathbf{Z}, +)$ sur $(G, *)$.

Utilisation Tout énoncé commençant par « soit $(G, *)$ un groupe cyclique… » peut se traiter en supposant que $(G, *)$ est $(\mathbf{U}_n, \times)$. Il est bien plus intéressant, en général, de se placer dans $(\mathbf{U}_n, \times)$ plutôt que dans $(\mathbf{Z}/n\mathbf{Z}, +)$. D'abord, on travaille sur des nombres complexes, avec un aspect géométrique clair. Ensuite et surtout, tous les $\mathbf{U}_n$ étant des sous-groupes du même groupe $(\mathbf{U}, \times)$ (qui lui n'est pas cyclique, ni monogène), cela donne des propriétés intéressantes. Par exemple, $\mathbf{U}_3$ est un sous-groupe de $(\mathbf{U}_{12}, \times)$. En revanche, $\mathbf{Z}/3\mathbf{Z}$ n'est pas une partie de$\mathbf{Z}/12\mathbf{Z}$.

VI Générateurs d'un groupe cyclique

VI.1 Introduction

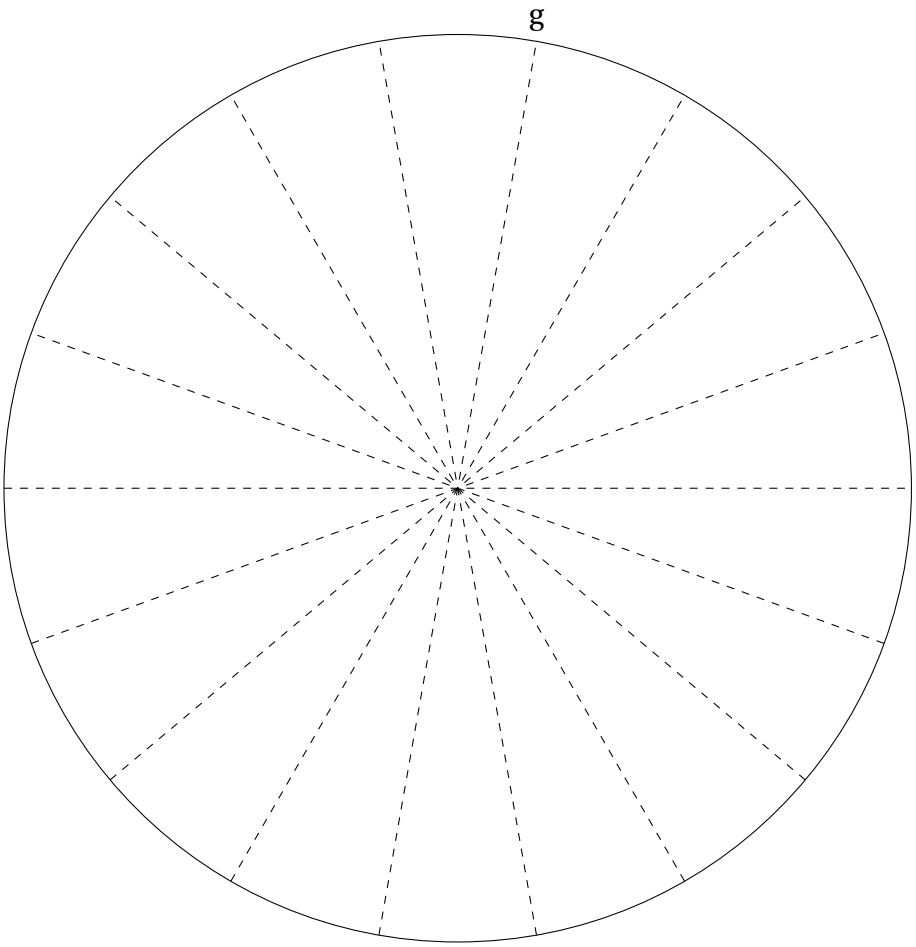
On va ici aborder une question plus générale : comment déterminer l'ordre d'un élément d'un groupe? Il ne sera pas ici question d'astuce : si $g \in G$, on essaye d'aboutir à quelque chose comme

$$(g^k = e) \iff (n|k)$$

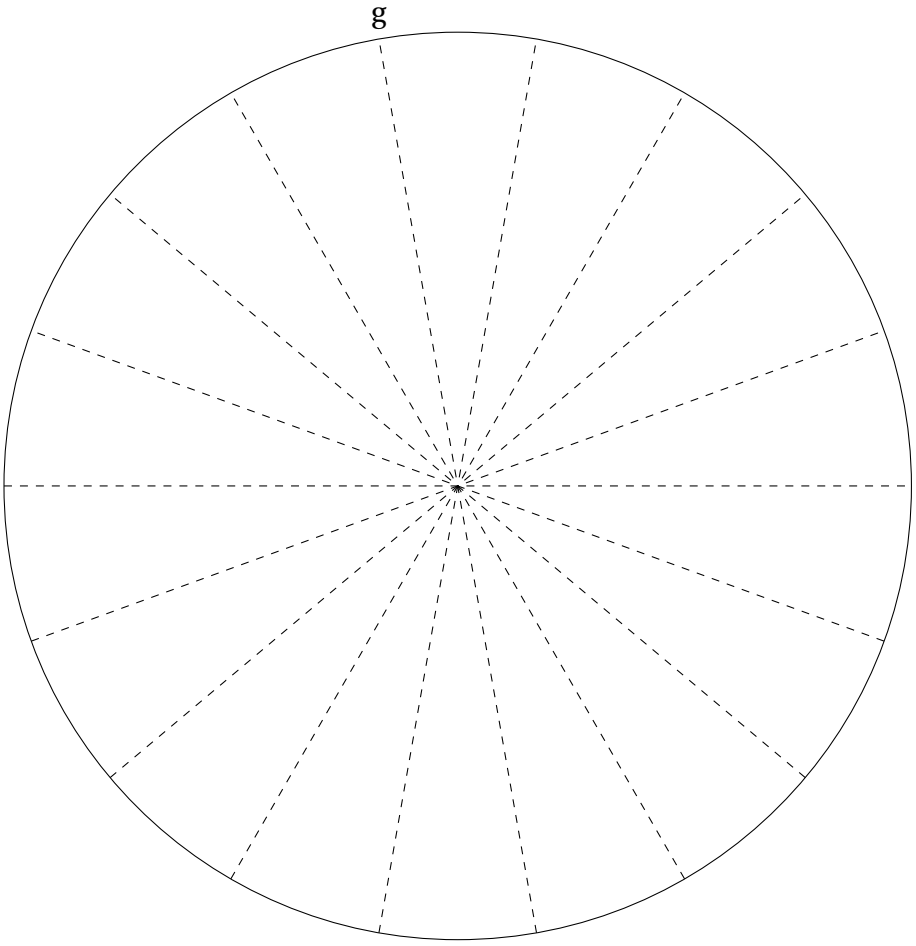
et on conclut alors que l'ordre de g est n.

VI.2 Pour s'amuser un peu

Dans $(\mathbf{U}_{18}, \times)$, écrire sur le dessin les puissances successives de g, en déduire l'ordre de g.


g

Même question :



VI.3 Recherche de l'ordre d'un élément d'un groupe cyclique

Soit $(G,*)$ un groupe cyclique d'ordre $n \geq 1$. Soit g un générateur de G. Soit $h \in G$; il existe k tel que $h = g^k$ (k n'est pas unique, mais il est unique modulo n). Déterminons l'ordre de h :
$h^j = e \Longleftrightarrow$

VI.4 Générateurs d'un groupe cyclique

Le paragraphe précédent permet de déterminer les générateurs de $(G, *)$ et leur nombre.

VI.5 Exemples

Ecrire la liste des générateurs de $(\mathbf{Z}/18\mathbf{Z}, +)$, la liste des générateurs de $(\mathbf{U}_{36}, \times)$.

VII L'exercice d'oral sur les groupes cycliques

Il serait exagéré de dire qu'il n'y a qu'un exercice d'oral sur les groupes cycliques. Mais il y en a un qui se pose souvent, et dont la résolution est très instructive. On peut trouver l'énoncé sous sa forme la plus simple :
Enoncé : Montrer que tout sous-groupe d'un groupe cyclique est cyclique.
Ou, plus précis :
Enoncé : Soit $(G,*)$ un groupe cyclique d'ordre $n \geq 2$. Montrer que, pour tout diviseur d de n, il y a un unique sous-groupe H d'ordre d de G.
On retiendra que l'idée est de regarder les sous-groupes d'un groupe cyclique.

VII.1 Une méthode savante

1. Soit m et n deux entiers naturels non nuls. Donner une condition nécessaire et suffisante de divisibilité entre m et n équivalente à $n\mathbf{Z} \subset m\mathbf{Z}$.

   $m|n$

   ---

2. Soit $(G,*)$ un groupe cyclique d'ordre $n \geq 2$, g un générateur de G. On note ϕ_g le morphisme « habituel » de $(\mathbf{Z},+)$ sur $(G,*)$. Soit H un sous-groupe de G. Montrer que $\phi_g^{-1}(H)$ est un sous-groupe de $(\mathbf{Z},+)$. Le comparer (pour la relation d'inclusion) avec le noyau de ϕ_g.

   L'image réciproque par un morphisme de groupe d'un sous-groupe est un sous-groupe. Notant e l'élément neutre de G, $e \in H$, donc $\mathrm{Ker}(\phi_g) \subset \phi^{-1}(H)$.

   ---

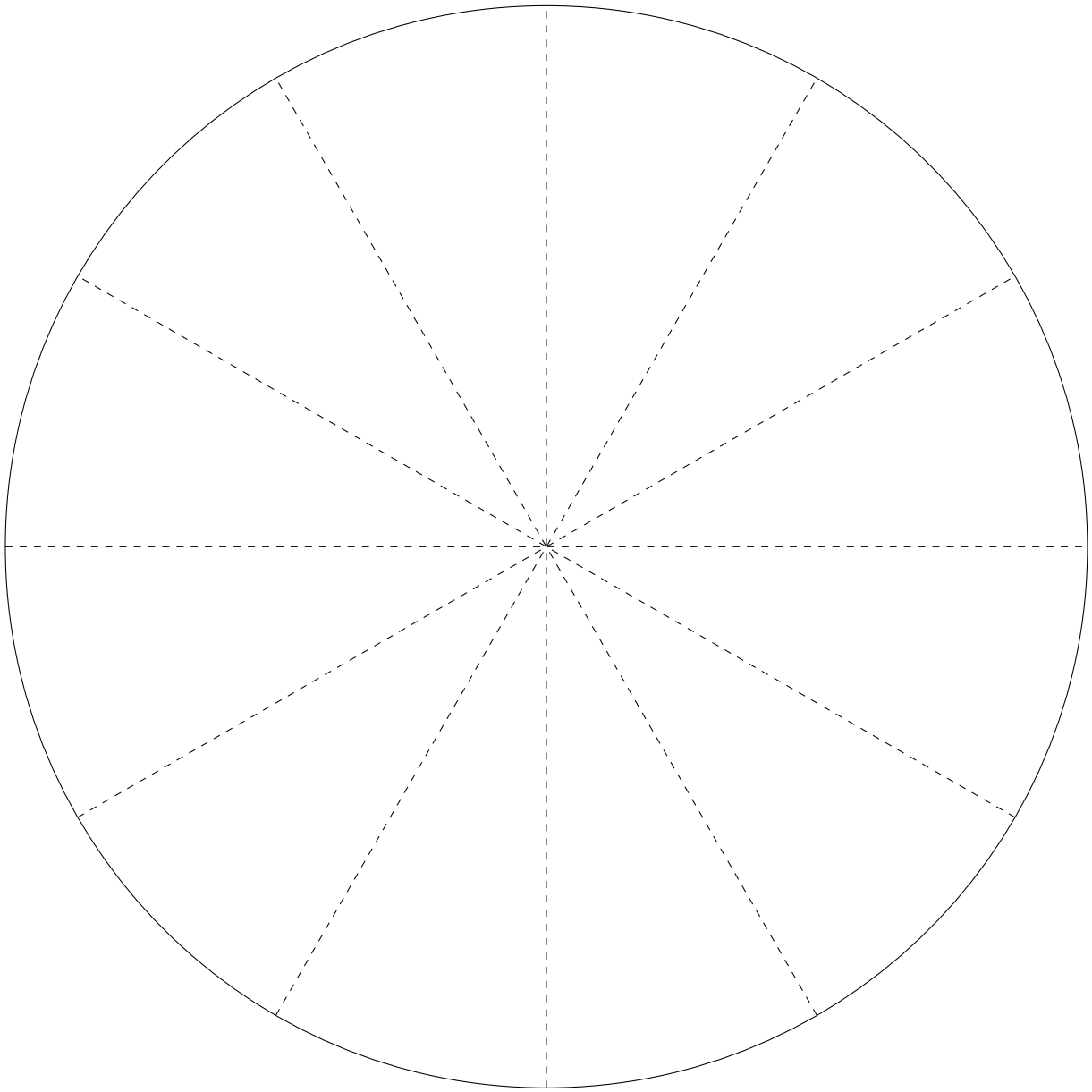
3. A partir des considérations précédentes, résoudre les deux exercices énoncés plus haut.

   On peut écrire $\phi^{-1}(H) = m\mathbf{Z}$ avec $n = mq$. Donc $H = \langle g^m \rangle$, de cardinal q. Inversement, si H' est un sous-groupe de cardinal q, $\phi^{-1}(H')$ ne peut être que $m\mathbf{Z}$.

VII.2 Une approche plus simple

Un isomorphisme entre deux groupes transforme sous-groupe en sous-groupe, groupe cyclique en groupe cyclique, générateur en générateur...Si cela ne vous paraît pas évident, démontrez-le.
On peut donc traiter l'exercice pour le groupe $(\mathbf{U}_n, \times)$, c'est suffisant. Or, dans ce cadre, l'aspect géométrique rend les choses plus claires.

En effet, si on prend par exemple $n = 12$, les groupes $\mathbf{U}_k$, $k = 1, 2, 3, 4, 6, 12$ sont des sous-groupes de $\mathbf{U}_{12}$.



Soit H un sous-groupe de $(\mathbf{U}_n, \times)$ ($n \geq 2$). On suppose $H \neq \{1\}$. On pose $\omega = \exp\left(\dfrac{2i\pi}{n}\right)$.

1. On définit
$$k_0 = \min\Big(\{k \in [\![1, n-1]\!] \; ; \; \omega^k \in H\}\Big)$$
Montrer que H est le sous-groupe de $\mathbf{U}_n$ engendré par ω^{k_0}. Calculer son ordre en fonction de n et de k_0. Conclure pour les deux énoncés.

2. On s'y prend autrement. On note $d = |H|$. On sait que, pour tout $h \in H$, $h^d = 1$. Montrer que $H = \mathbf{U}_d$. C'est fini.

On peut être surpris de la dernière méthode, où l'on ne fait rien. C'est parce qu'on profite, en étant sur $\mathbf{C}$*, de résultats habituels et néanmoins essentiels, comme le fait que 1 a exactement* d *racines* d*-ièmes.*

Exercice (Oral Mines 2022) Si G et H sont deux groupes cycliques d'ordres respectifs n et m, donner une condition nécessaire et suffisante pour que $G \times H$ soit cyclique.

VIII Groupes monogènes ; isomorphisme entre les groupes monogènes infinis

Définition Un groupe $(G, *)$ est dit monogène lorsqu'il vérifie les deux conditions suivantes :

(i) Il existe $g \in G$ tel que $G = \langle g \rangle$.

(ii) G est infini.

L'application $k \mapsto g^k$ est alors un isomorphisme de $(\mathbf{Z}, +)$ sur $(G, *)$.

Proposition Tous les groupes monogènes sont isomorphes.

Question : Les sous-groupes d'un groupe monogène sont-ils monogènes ?

Table des matières