

Compléments sur les groupes

Je me souviens	2
1.1 Loi de composition interne	2
1.2 Structure de groupe	2
1.3 Morphisme de groupes	2
1.4 Les entiers	2
Cours	3
2 Sous-groupe engendré par une partie	3
3 Interlude : le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$	3
4 Groupes monogènes et groupes cycliques	4
5 Ordre d'un élément dans un groupe	5
6 Annexes	6
6.1 Annexe : pourquoi l'ordre d'un élément divise le cardinal du groupe	6
6.2 Annexe : théorème de Lagrange	6
Exercices	7
Exercices et résultats classiques à connaître	7
Le centre d'un groupe	7
Les sous-groupes de $(\mathbb{R}, +)$	7
Exercices	8
Petits problèmes d'entraînement	9

Je me souviens**1.1 Loi de composition interne**

1. Qu'est-ce qu'une loi de composition interne ?
2. Comment noter une loi de composition interne ?
3. Que signifient :
 - associatif ?
 - commutatif ?
 - élément neutre ?
 - symétrique ?
4. Soit E un ensemble, muni d'une loi de composition interne $*$. On suppose l'existence d'un élément neutre noté e . Soit a et b deux éléments de E qui admettent un symétrique. Est-ce que $(a*b)$ admet un symétrique ?
5. Pour un élément a et un entier n , qu'est-ce que a^n ?
6. Qu'est-ce qu'une **partie stable** de E pour $*$?

1.2 Structure de groupe

7. C'est quoi, un groupe ?
8. C'est quoi, un groupe abélien ?
9. Donner des exemples de groupes.
10. Comment définir le **groupe produit** de deux groupes ?
11. C'est quoi, un sous-groupe ?
12. Quels sont les deux sous-groupes triviaux de $(G, *)$?

1.3 Morphisme de groupes

13. Qu'est-ce qu'un morphisme de groupe ?
14. Donner des exemples de morphismes de groupes.

On considère $f : (G, *) \rightarrow (H, \cdot)$ un morphisme de groupe.

15. Quelle est l'image du neutre, du symétrique, par f ?
16. Que dire de l'image (directe) d'un sous-groupe par f ?
17. Que dire de l'image réciproque d'un sous-groupe par f ?
18. C'est quoi, le noyau de f ? Quel lien avec l'injectivité de f ?
19. C'est quoi, l'image de f ? Quel lien avec la surjectivité de f ?
20. Qu'est-ce qu'un **isomorphisme** de groupes.
21. Comment montrer qu'une application est un isomorphisme ?

1.4 Les entiers

22. Que désigne \mathbb{Z} ? $7\mathbb{Z}$?
23. Énoncer le théorème de la division euclidienne dans \mathbb{Z} .

2 Sous-groupe engendré par une partie

Proposition. Une intersection de sous-groupes est un sous-groupe : si $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, *)$, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition. Soit $(G, *)$ un groupe et A une partie de G . On appelle **sous-groupe engendré par A** le plus petit sous-groupe H de $(G, *)$ qui contient A .

Remarque. On note $\langle A \rangle$ le sous-groupe engendré par A , mais cette notation n'est pas dans le programme officiel.

Remarque. La définition signifie que H est le sous-groupe de $(G, *)$ engendré par A si et seulement si :

- H est un sous-groupe de $(G, *)$
- $A \subset H$
- Pour tout sous-groupe K de $(G, *)$, $A \subset K \implies H \subset K$

Proposition. Avec les notations précédentes :

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

Description du sous-groupe engendré par A . Soit G un groupe noté multiplicativement. $\langle A \rangle$ est l'ensemble des éléments de G qui s'écrivent sous la forme :

$$a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$$

où $n \in \mathbb{N}$, $a_1, \dots, a_n \in A$, $\varepsilon_1, \dots, \varepsilon_n = \pm 1$.

Remarque. Lorsque G est commutatif et noté additivement, le sous-groupe engendré par A est l'ensemble des éléments qui s'écrivent sous la forme :

$$k_1 a_1 + \dots + k_p a_p$$

où $p \in \mathbb{N}$, $a_1, \dots, a_p \in A$ sont distincts, et $k_1, \dots, k_p \in \mathbb{Z}$. Ce ne sont pas tout à fait des combinaisons linéaires, puisque les « scalaires » sont ici entiers.

Proposition. Les sous-groupes de \mathbb{Z} sont les $a\mathbb{Z} = \langle a \rangle$, où $a \in \mathbb{N}$.

Définition. La partie A de $(G, *)$ est dite **génératrice de G** lorsque le sous-groupe de $(G, *)$ engendré par A est G .

3 Interlude : le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Proposition. Pour $n \in \mathbb{N}$, la relation de **congruence modulo n** sur \mathbb{Z} est définie par :

$$\begin{aligned} a \equiv b [n] &\iff a - b \in n\mathbb{Z} \\ &\iff n \mid a - b \end{aligned}$$

C'est une relation d'équivalence.

Remarque. Si $n = 0$, il s'agit simplement de l'égalité. Si $n = 1$, tous les entiers sont en relation.

Proposition. Pour $n \geq 2$, il y a exactement n classes d'équivalences :

$$\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

Définition. On note $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$, appelé « \mathbb{Z} sur $n\mathbb{Z}$ ».

Remarque. On a bien $\text{Card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposition. Pour $n \geq 2$, il existe une unique loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$, encore notée $+$, pour laquelle l'application $\pi : k \mapsto \overline{k}$ soit un morphisme de groupes, i.e. :

$$\forall a, b \in \mathbb{Z}, \overline{a+b} = \overline{a} + \overline{b}$$

De plus, $\text{Ker } \pi = n\mathbb{Z}$.

Remarque. Ainsi, pour additionner deux classes d'équivalences, on additionne deux représentants de ces classes d'équivalences.

Proposition. Muni de cette loi, $(\mathbb{Z}/n\mathbb{Z}, +)$ est donc bien un groupe commutatif.

Exemple. Construire la table de la loi $+$ dans $\mathbb{Z}/4\mathbb{Z}$.

Corollaire. Pour $n \in \mathbb{N}^*$, $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ et $k \in \mathbb{Z}$,

$$k \cdot \bar{a} = \overline{ka}$$

Générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Soit n entier ≥ 2 . Sont équivalentes :

- (i) $\mathbb{Z}/n\mathbb{Z} = \langle \bar{a} \rangle$
- (ii) il existe $k \in \mathbb{N}$ tel que $\overline{ka} = 1$
- (iii) $a \wedge n = 1$

Remarque. Ainsi, $(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par chaque \bar{k} , où $k \in \{0, \dots, n-1\}$ est premier avec n .

Exemple. Donner la liste des éléments qui engendrent $(\mathbb{Z}/12\mathbb{Z}, +)$.

Comment définir un morphisme $\mathbb{Z}/n\mathbb{Z} \rightarrow G$.

Soit n entier ≥ 2 , et $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$.

$$k \mapsto \bar{k}$$

Si G est un groupe et $f : \mathbb{Z} \rightarrow G$ un morphisme de groupes, alors les propriétés suivantes sont équivalentes :

- (i) il existe un morphisme $g : \mathbb{Z}/n\mathbb{Z} \rightarrow G$ tel que $f = g \circ \pi$
- (ii) $n\mathbb{Z} \subset \text{Ker } f$

Remarque. Ainsi, pour définir un morphisme de groupe $\mathbb{Z}/n\mathbb{Z} \rightarrow G$, on définit un morphisme de groupe $\mathbb{Z} \rightarrow G$ dont le noyau contient $n\mathbb{Z}$, et on « passe au quotient ».

Proposition. Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et (\mathbb{U}_n, \times) sont isomorphes.

4 Groupes monogènes et groupes cycliques

Définition.

- Un groupe G est **monogène** s'il existe $x \in G$ tel que $G = \langle x \rangle$. On dit que x est un **générateur** de x .
- Lorsque G est un groupe fini et monogène, on dit que c'est un **groupe cyclique**.

Exemple.

- $(\mathbb{Z}, +)$ est monogène, engendré par 1 (et par -1).
- Tous les sous-groupes de \mathbb{Z} sont monogènes.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène. Ses générateurs sont les \bar{k} , où k est premier avec n .
- (\mathbb{U}_n, \times) est monogène. Ses générateurs sont les $e^{\frac{2ik\pi}{n}}$, où k est premier avec n .

Proposition. Soit $(G, *)$ un groupe et $x \in G$. Alors :

$$\langle x \rangle = \{x^k, k \in \mathbb{Z}\}$$

Ainsi $\langle x \rangle = \text{Im } \varphi_x$ où $\varphi_x : \mathbb{Z} \rightarrow G$.

$$k \mapsto x^k$$

Théorème.

Tout groupe monogène $\langle x \rangle$ est isomorphe :

- soit à $(\mathbb{Z}, +)$, lorsque $\text{Ker } \varphi_x = \{0\}$;
- soit à $(\mathbb{Z}/n\mathbb{Z}, +)$, lorsque $\text{Ker } \varphi_x = n\mathbb{Z}$.

Remarque. Dans le second cas, $n = \text{Min}\{k \in \mathbb{N}^*, x^k = e\}$.

5 Ordre d'un élément dans un groupe

Définition. Soit $(G, *)$ un groupe dont le neutre est noté e , et $x \in G$. Lorsque $\langle x \rangle$ est fini, on dit que x est d'ordre fini et on note :

$$\text{ord}(x) = \text{Min}\{n \in \mathbb{N}^*, x^n = e\}$$

l'ordre de x .

Remarque.

- $\text{ord}(x) = n \iff \text{Ker } \varphi_x = n\mathbb{Z}$
- Si $\langle x \rangle$ est infini, on convient parfois que x est d'ordre infini.

Exemple. Quel est l'ordre de $\bar{1}$ (resp. de $\bar{12}$) dans $\mathbb{Z}/42\mathbb{Z}$?

Proposition. Avec les notations précédentes, lorsque x est d'ordre fini n , on a :

$$x^k = e \iff n \mid k$$

Théorème.

Avec les notations précédentes,

$$\text{ord}(x) = \text{Card}(\langle x \rangle)$$

Corollaire. Si G est un groupe fini, alors tout $x \in G$ est d'ordre fini.

Théorème.

Soit G un groupe fini, et $x \in G$. Alors :

$$\text{ord}(x) \mid \text{Card}(G)$$

c'est-à-dire que $x^{\text{Card } G} = e$.

Corollaire. Tout groupe fini dont le cardinal est premier est cyclique, et engendré par chacun de ses éléments différent du neutre.

6 Annexes

6.1 Annexe : pourquoi l'ordre d'un élément divise le cardinal du groupe

Théorème.

Soit $(G, *)$ un groupe fini et $a \in G$. Alors l'ordre de a divise $\text{Card}(G)$.

Preuve lorsque G est abélien.

On note $n = \text{Card}(G)$ et on énumère les éléments de G : $G = \{g_1, \dots, g_n\}$. On considère $a \in G$ (c'est l'un des g_i) et d son ordre.

L'application $\sigma : x \mapsto a * x$ est une permutation de G , de réciproque $x \mapsto a^{-1} * x$, et donc :

$$\begin{aligned} g_1 * \dots * g_n &= \prod_{g \in G} g \\ &= \prod_{g \in G} \sigma(g) \\ &= (a * g_1) * \dots * (a * g_n) \\ &= a^n * (g_1 * \dots * g_n) \end{aligned}$$

en réordonnant les termes, puisque $*$ est commutative.

Ainsi, en multipliant par $(g_1 * \dots * g_n)^{-1}$, on en déduit :

$$e = a^n$$

et donc, $d \mid n$. □

Preuve dans le cas général, non exigible.

Soit $a \in G$ et d son ordre. On considère la relation :

$$x \mathcal{R} y \iff x^{-1}y \in \langle a \rangle$$

C'est une relation d'équivalence (réflexive, symétrique, transitive). Pour $x \in G$, la classe d'équivalence de x est :

$$\begin{aligned} \bar{x} &= \{y \in G, x^{-1}y \in \langle a \rangle\} \\ &= \{y \in G, \exists k \in \mathbb{Z}, y = xa^k\} \\ &= \{x, xa, xa^2, \dots, xa^{d-1}\} \end{aligned}$$

Cette classe contient exactement d éléments.

En effet, si $xa^k = xa^\ell$ où $0 \leq k \leq \ell \leq d-1$, alors $a^{\ell-k} = e$ donc $d \mid \ell - k$ et donc $\ell = k$ car $0 \leq \ell - k < d$.

L'ensemble G est donc partitionné en ses classes d'équivalences, que l'on note $\bar{x}_1, \dots, \bar{x}_p$:

$$G = \bigcup_{\substack{i=1 \\ \text{union} \\ \text{disjointe}}}^p \bar{x}_i$$

donc :

$$\text{Card}(G) = \sum_{i=1}^p \text{Card}(\bar{x}_i) = \sum_{i=1}^p d = pd$$

donc $d \mid \text{Card}(G)$. □

Remarque. Cette seconde démonstration, même si elle n'est pas exigible, est intéressante, parce qu'elle nous permet d'accéder à la démonstration du théorème de Lagrange.

6.2 Annexe : théorème de Lagrange

Théorème de Lagrange, hors programme.

Si G est un groupe fini de cardinal n , alors pour tout H sous-groupe de G , $\text{Card } H \mid \text{Card } G$.

Preuve du théorème de Lagrange.

Soit H un sous-groupe de G et d son cardinal. On considère la relation :

$$x \mathcal{R} y \iff x^{-1}y \in H$$

C'est une relation d'équivalence (réflexive, symétrique, transitive). Pour $x \in G$, la classe d'équivalence de x est :

$$\begin{aligned} \bar{x} &= \{y \in G, x^{-1}y \in H\} \\ &= \{y \in G, \exists h \in H, y = xh\} \\ &= xH \end{aligned}$$

Cette classe contient exactement d éléments, comme H .

L'ensemble G est donc partitionné en ses classes d'équivalences, que l'on note $\bar{x}_1, \dots, \bar{x}_p$:

$$G = \bigcup_{\substack{i=1 \\ \text{union} \\ \text{disjointe}}}^p \bar{x}_i$$

donc :

$$\text{Card}(G) = \sum_{i=1}^p \text{Card}(\bar{x}_i) = \sum_{i=1}^p d = pd$$

donc $d \mid \text{Card}(G)$. □

Exercices et résultats classiques à connaître**Le centre d'un groupe****110.1**

Soit (G, \star) un groupe. On définit son **centre** comme l'ensemble des éléments de G qui commutent avec tous les éléments de G :

$$C = \{g \in G, \forall h \in G, g \star h = h \star g\}$$

Montrer que C est un sous-groupe de (G, \star) .

Les sous-groupes de $(\mathbb{R}, +)$ **110.2**

Montrer que, si G est un sous-groupe de $(\mathbb{R}, +)$, alors il est soit de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}$, soit dense dans \mathbb{R} . Dans le cas où $G \neq \{0\}$, on s'intéressera à $\alpha = \inf(G \cap \mathbb{R}_+^*)$ et on discutera selon que $\alpha > 0$ ou $\alpha = 0$.

Exercices

110.3

Soit E un ensemble non vide muni d'une loi $*$ possédant un neutre e . Montrer que a admet un inverse si et seulement si l'application

$$\begin{array}{ccc} f : E & \rightarrow & E \\ x & \mapsto & a * x \end{array}$$

est bijective.

110.4

Soit $n \in \mathbb{N}^*$. On considère $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$ l'ensemble des racines n -èmes de l'unité. Montrer que (\mathbb{U}_n, \times) est un groupe.

110.5

Soit E un ensemble non vide, $a \in E$. On considère :

$$H = \{f \in \mathfrak{S}(E), f(a) = a\}$$

l'ensemble des permutations de E fixant a . Montrer que (H, \circ) est un groupe.

110.6

Montrer que :

$$\mathrm{SL}_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}), \det(M) = 1\}$$

est un groupe pour la multiplication.

110.7

Montrer que :

$$H = \{x + y\sqrt{3}, x, y \in \mathbb{Z}, x^2 - 3y^2 = 1\}$$

est un sous-groupe de (\mathbb{R}^*, \times) .

110.8

Déterminer le sous-groupe de $(\mathbb{Z}, +)$ engendré par $\{-27, 12, 18\}$.

110.9

Montrer que le sous-groupe de (\mathbb{C}^*, \times) engendré par $\{i = e^{i\frac{\pi}{2}}, j = e^{i\frac{2\pi}{3}}\}$ est \mathbb{U}_{12} , l'ensemble des racines 12-ièmes de l'unité.

110.10

Déterminer tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

110.11

Soit G et G' deux groupes notés additivement, et $f : G \rightarrow G'$ un morphisme de groupes.

- (a) Montrer que, pour tout $x \in G$ et tout $n \in \mathbb{N}$, $f(nx) = nf(x)$.
- (b) Est-ce encore vrai lorsque $n \in \mathbb{Z}$?
- (c) Comment s'écrivent ces résultats lorsque les groupes sont notés multiplicativement ?

110.12

Soit $(G, *)$ un groupe commutatif. On considère g_1, g_2 deux éléments d'ordre d_1, d_2 respectivement. On suppose que $d_1 \wedge d_2 = 1$. Montrer que $g_1 * g_2$ est d'ordre fini, et calculer cet ordre.

110.13

Démontrer que la matrice :

$$\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

est d'ordre fini dans $\mathrm{GL}_2(\mathbb{R})$.

110.14

Dans \mathfrak{S}_{10} , déterminer l'ordre de :

$$(14378)(257)$$

110.15

Voici la liste des éléments de \mathfrak{S}_3 :

$$\{\mathrm{Id}, (12), (13), (23), (123), (132)\}$$

Indiquer pour chaque élément son ordre.

Petits problèmes d'entraînement

110.16

Soit (G, \star) un groupe, et \mathfrak{S} l'ensemble des permutations de G . On rappelle que (\mathfrak{S}, \circ) est un groupe. Pour $g \in G$, on définit :

$$\begin{aligned} \phi_g : G &\rightarrow G \\ h &\mapsto g \star h \star g^{-1} \end{aligned}$$

- (a) Montrer que $\phi : g \mapsto \phi_g$ est un morphisme de (G, \star) dans (\mathfrak{S}, \circ) .
- (b) Caractériser les éléments du noyau de ϕ .

110.17

- (a) Soit $(G, *)$ un groupe. Pour tout $g \in G$, on note :

$$\begin{aligned} \phi_g : G &\rightarrow G \\ x &\mapsto g * x \end{aligned}$$

Montrer que $g \mapsto \phi_g$ est un morphisme de groupes de $(G, *)$ dans (\mathfrak{S}_G, \circ) , et qu'il est injectif.

- (b) En déduire que tout groupe fini ayant n éléments se plonge dans \mathfrak{S}_n , c'est-à-dire est isomorphe à un sous-groupe de \mathfrak{S}_n .
- (c) Dans le cas où $n = 4$, identifier dans \mathfrak{S}_4 un sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$ et un autre isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

110.18

On note $\text{GL}_2(\mathbb{Z})$ l'ensemble des matrices carrées d'ordre 2 à coefficients dans \mathbb{Z} dont le déterminant vaut 1 ou -1 .

- (a) Soit M une matrice carrée d'ordre 2 à coefficients entiers. Montrer que si M est inversible et que M^{-1} est à coefficients entiers, alors $\det(M) = \pm 1$.
- (b) Montrer que $(\text{GL}_2(\mathbb{Z}), \times)$ est un groupe.
- (c) On considère $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Calculer l'ordre de A , de B et de AB . Que peut-on en conclure ?

110.19

- (a) Soit H et K deux sous-groupes d'un même groupe G . On suppose $\text{Card}(H) = \alpha$ et $\text{Card}(K) = \beta$ avec $\alpha \wedge \beta = 1$. Montrer que $H \cap K = \{e\}$.
- (b) Soit H et K deux sous-groupes de G de même cardinal p premier. Montrer que $H = K$ ou $H \cap K = \{e\}$.

110.20

Soit G un groupe abélien noté multiplicativement, H et K deux sous-groupes de G .

- (a) Montrer que $HK = \{hk, h \in H, k \in K\}$ est un sous-groupe de G .
- (b) Montrer que $HK = \langle H \cup K \rangle$.
- (c) Montrer que, si $H \cap K = \{e\}$, alors HK est isomorphe au produit cartésien $H \times K$.
- (d) On suppose que G est de cardinal p^2 , où p est premier. Montrer que tout sous-groupe de G est de cardinal 1, p ou p^2 .

110.21

Soit G un groupe non réduit à $\{e\}$. Montrer que G n'admet aucun sous-groupe propre si et seulement si il est cyclique de cardinal p premier.

110.22

Pour $n \in \mathbb{N}^*$, \mathfrak{S}_n désigne le groupe symétrique, c'est-à-dire l'ensemble des permutations de $\llbracket 1, n \rrbracket$.

- (a) Montrer que, pour tout $\sigma \in \mathfrak{S}_n$ et tout $a_1, \dots, a_k \in \llbracket 1, n \rrbracket$ distincts :

$$\sigma \circ (a_1 \ a_2 \ \dots \ a_k) \circ \sigma^{-1} = (a_{\sigma(1)} \ a_{\sigma(2)} \ \dots \ a_{\sigma(k)})$$

On rappelle que la notation $(a_1 \ a_2 \ \dots \ a_k)$ désigne la permutation γ telle que $\gamma(a_i) = a_{i+1}$ avec $\gamma(a_k) = a_1$, les autres éléments étant laissés invariants.

- (b) En déduire qu'il n'y a que deux morphismes de groupes de (\mathfrak{S}_n, \circ) dans (\mathbb{C}^*, \times) : le morphisme constant égal à 1, et la signature.

110.23

Soit $(G, *)$ un groupe et $\varphi : G \rightarrow E$ une application bijective. On définit sur E une loi en posant :

$$x \top y = \varphi(\varphi^{-1}(x) * \varphi^{-1}(y))$$

Montrer que (E, \top) est un groupe.

110.24

Montrer que :

$$H = \{z \in \mathbb{C}, \exists n \in \mathbb{N}, z^n = 1\}$$

est un sous-groupe de (\mathbb{C}^*, \times) .

110.25

On s'intéresse à l'équation :

$$(E); x^2 - 2y^2 = 1$$

d'inconnue $(x, y) \in \mathbb{Z}^2$. On considère l'ensemble :

$$G = \{(x, y) \in \mathbb{N}^* \times \mathbb{Z}, x^2 - 2y^2 = 1\}$$

Pour $(x, y), (x', y') \in G$ on pose :

$$(x, y) \star (x', y') = (xx' + 2yy', xy' + x'y) \text{ et } \varphi(x, y) = \ln(x + \sqrt{2}y)$$

(a) Montrer que (G, \star) est un groupe, dont on précisera le neutre e .

(b) On pose $a = (3, 2) \in G$. Montrer que :

$$\forall (x, y) \in G, 0 \leq \varphi(x, y) < \varphi(a) \implies (x, y) = e$$

(c) Vérifier que, pour tout $(x, y), (x', y') \in G$:

$$\varphi((x, y) \star (x', y')) = \varphi(x, y) + \varphi(x', y')$$

(d) En déduire que les éléments de G sont les a^n , pour $n \in \mathbb{Z}$.

110.26

Soit H une partie finie non vide d'un groupe $(G, *)$. On suppose que H est stable pour la loi $*$. Montrer que H est un sous-groupe de G .

110.27

Soit H, K deux sous-groupes d'un groupe G noté multiplicativement. On considère :

$$HK = \{xy, x \in H \text{ et } y \in K\} \text{ et } KH = \{yx, x \in H \text{ et } y \in K\}$$

(a) Montrer que HK est un sous-groupe de G si et seulement si $KH \subset HK$.

(b) Montrer que, dans ce cas, $HK = KH$.

110.28

Lorsque $(G, *)$ est un groupe, on appelle **caractère** de $(G, *)$ tout morphisme de groupes de $(G, *)$ dans (\mathbb{C}^*, \times) . L'ensemble des caractères est noté \widehat{G} .

(a) Soit $n \in \mathbb{N}^*$. Déterminer tous les caractères de $(\mathbb{Z}/n\mathbb{Z}, +)$.

On pourra commencer par montrer que l'image d'un caractère est incluse dans \mathbb{U}_n .

(b) Soit (G, \star) un groupe fini, et f_1, \dots, f_n des éléments distincts dans \widehat{G} . Montrer que la famille (f_1, \dots, f_n) est libre dans le \mathbb{C} -espace vectoriel $\mathcal{F}(G, \mathbb{C}) = \mathbb{C}^G$.

On pourra procéder par récurrence.

(c) En déduire que $\text{Card}(\widehat{G}) \leq \text{Card}(G)$, et montrer que cette inégalité peut-être stricte.

110.29

Soit G un groupe fini, noté multiplicativement.

(a) Pour $x \in G$, on appelle **normalisateur de x** l'ensemble :

$$N(x) = \{g \in G, gxg^{-1} = x\}$$

Montrer que $N(x)$ est un sous-groupe de G .

- (d) On suppose dans cette question que G est de cardinal p^α , où p est premier et $\alpha \in \mathbb{N}^*$. Montrer que le centre $C(G)$ n'est pas réduit à $\{1\}$.

- (b) Montrer que l'on définit une relation d'équivalence en posant, pour $x, y \in G$:

$$x \mathcal{R} y \iff \exists g \in G, y = gxg^{-1}$$

- (c) On note $\text{Cl}(x)$ la classe d'équivalence d'un élément x pour la relation \mathcal{R} . Montrer que :

$$\text{Card}(G) = \text{Card}(\text{Cl}(x)) \times \text{Card}(N(x))$$