ALGÈBRE GÉNÉRALE

Contenus	Capacités & commentaires
a) Groupes et sous-groupes	
Groupe. Produit fini de groupes. Sous-groupe. Caractérisation d'un sous-groupe. Intersection de sous-groupes. Sous-groupe engendré par une partie. Sous-groupes du groupe $(\mathbb{Z}, +)$.	Exemples issus de l'algèbre et de la géométrie.
b) Morphismes de groupes	
Morphisme de groupes. Image et image réciproque d'un sous-groupe par un morphisme. Image et noyau d'un morphisme. Condition d'injectivité d'un morphisme. Isomorphisme de groupes. Réciproque d'un isomorphisme.	Exemples : signature et déterminant. Exemple : groupe spécial orthogonal d'un espace euclidien.
c) Groupes monogènes et cycliques	
Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$. Groupe monogène, groupe cyclique. Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.	Groupe des racines n-ièmes de l'unité.
d) Ordre d'un élément dans un groupe	
Élément d'ordre fini d'un groupe. Ordre d'un tel élément. Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour n dans $\mathbb{Z}$, on a $x^n = e \Leftrightarrow d \mid n$. L'ordre d'un élément d'un groupe fini divise le cardinal d'un groupe.	Si x est d'ordre fini, l'ordre de x est le cardinal du sous groupe de G engendré par x.

I — Rappels de MPSI en théorie des groupes

1) Propriétés générales d'une loi de composition interne

Définition : loi de composition interne *(1)*

Soit E un ensemble. Une loi de composition interne sur E est une **application** *de E^2 vers E.*
On utilise une notation infixe, du type $x * y$ si $(x, y) \in E^2$. En voici d'autres : $+ \times - \div \cdot \circ \otimes \oplus \perp \star \cup \cap$ ...

Définitions : vocabulaire d'une loi *(2)*

Soit E un ensemble muni d'une loi de composition interne $*$ et A une partie de E.
(1) : *On dit que A* **est stable par la loi** $*$ *lorsque pour tout $(x, y) \in A^2$, $x * y \in A$.*
L'application $\star$ devient donc une loi de composition interne pour A et on parle de loi induite sur A.
(2) : *On dit que $*$ est* **associative** *lorsque pour tout $(x, y, z) \in E^3$, $x * (y * z) = (x * y) * z$.*
(3) : *On dit que $*$ est* **commutative** *lorsque pour tout $(x, y) \in E^2$, $x * y = y * x$.*
(4) : *On dit que $*$ admet un* **élément neutre** *lorsqu'il existe $e \in E$ tel que pour tout $x \in E$, $x * e = e * x = x$.*
(5) : *Si E est aussi muni d'une loi de composition interne $\perp$, on dit que la loi $*$ est* **distributive à gauche** *(resp.* **à droite***) sur la loi $\perp$ lorsque pour tout $(x, y, z) \in E^3$, $x*(y\perp z) = (x*y)\perp(x*z)$ (resp. $(x\perp y)*z = (x*z)\perp(y*z)$).*
La loi $*$ est distributive sur la loi $\perp$ lorsqu'elle est distributive à gauche et à droite.

Propriétés *(3)*

Soit E un ensemble muni d'une loi de composition interne $*$ et A une partie **stable par** $*$ *de E.*
(1) (D) : *Si E admet un élément neutre, alors ce dernier est* **unique**.
(2) (D) : *Si $*$ est associative, alors la loi induite sur A aussi.*
(3) (Dm) : *Si $*$ est commutative, alors la loi induite sur A aussi.*
(4) (Dm) : *Si e est élément neutre pour $*$ et si $e \in A$, alors e est neutre pour la loi induite sur A.*
(5) (Dm) : *Si E est aussi muni d'une loi de composition interne $\perp$, si A est stable par $\perp$ et si $*$ est distributive sur $\perp$, alors les mêmes propriétés se retrouvent sur les lois induites.*

2) Éléments symétrisables

Définition *(4)*

Soit E un ensemble muni d'une loi de composition interne $*$ associative et qui admet un élément neutre e.
On dit que $a \in E$ est symétrisable lorsqu'il existe $a' \in E$ tel que $a * a' = a' * a = e$.
On dit alors que a' est le symétrique de a.
Notations :
(1) : *Si la loi de composition interne est notée multiplicativement, on notera a^{-1} le symétrique de a, s'il existe.*
(2) : *Si la loi de composition interne est notée additivement, on notera $(-a)$ le symétrique de a, s'il existe.*

Propriétés : *(5)*

Soit E un ensemble muni d'une loi de composition interne $*$ associative et qui admet un élément neutre e.
(1) (D) : *Si $x \in E$ admet un symétrique, alors ce dernier est* ***unique***.
(2) (D) : *Si a et b sont symétrisables, alors $a \star b$ l'est aussi et $(a * b)' = b' * a'$.*
(3) (D) : *Si a est symétrisable, alors a est régulier, i.e. si $a * x = a * y$, alors $x = y$ et si $x * a = y * a$, alors $x = y$.*
(4) (Dm) : *Si A est une partie stable de E pour la loi $*$, si $a \in A$ admet un symétrique a' pour la loi $*$, et si $a' \in A$, alors a' est le symétrique de a pour la loi induite sur A.*

3) Groupes

Définition (groupe) *(6)*

Un **groupe** *est un ensemble G :*
[H1] *muni d'une loi de composition $\cdot$ interne et associative,*
[H2] *possédant un élément neutre : $\exists e \in G, \forall x \in G, x \cdot e = e \cdot x = x$,*
[H3] *dans lequel tout élément admet un symétrique : $\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e$.*
Notation : $(G, \cdot)$.
[H4] **Si la loi est commutative,** *on dit que le groupe est abélien.* ***Notation :*** $(G, +)$.

Exemples : $(\mathbb{R}, +)$, $(\mathbb{R}^{+*}, \times)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$, $(n\mathbb{Z}, +)$, $(\mathcal{M}_n(\mathbb{K}), +)$, $(\mathcal{P}(E), \Delta)$, $(GL(E), \circ)$, $(S_n, \circ)$...
Contre exemples : $(\mathbb{N}, +)$, $(\mathbb{Z}^*, \times)$, $(\mathcal{M}_n(\mathbb{R}), \times)$, $(\mathcal{P}(E), \cap)$, $(\mathcal{P}(E), \cup)$ NE sont PAS des groupes (car...)

Théorème - Définition : produit fini de groupes *(7)*

(1) (D) : *Soient $(G_1, *)$ et $(G_2, \perp)$ deux groupes. L'ensemble $G_1 \times G_2$ muni de la loi de composition interne $\circ$ définie par : $\forall (x_1, x_2, y_1, y_2) \in G_1 \times G_2 \times G_1 \times G_2$, $(x_1, x_2) \circ (y_1, y_2) = (x_1 * y_1, x_2 \perp y_2)$, est un groupe, appelé groupe produit des deux groupes.*
(2) (Dm) : *Par récurrence, si $G_1, G_2, \ldots, G_n$ sont des groupes, on peut munir le produit cartésien $G_1 \times \ldots \times G_n$ d'une structure de groupe produit.*

4) Itérés - puissances ou multiples - d'un élément a d'un groupe G.

Définition des puissances dans $(G, .)$ et multiples dans $(G, +)$ par récurrence. *(8)*

(1) : **Notation :** a^n *dans un groupe multiplicatif.*
(2) (Dm) : $a^{n+p} = a^n \times a^p$, $a^{np} = (a^n)^p = (a^p)^n$ *(pour tous entiers* relatifs *n et p).*
(3) (D) : **SI** $ab = ba$, **ALORS** $(ab)^n = a^n \times b^n$.
(4) : **Notation :** na *dans un groupe additif.*
(5) : $(n \pm p)a = na \pm pa$, $n(a \pm b) = na \pm nb$
(6) : $(np)a = n(pa) = p(na)$.

II — Approfondissement en théorie des groupes

1) Sous-groupes

Définition d'un sous-groupe *(9)*

Soit $(G, \cdot)$ un groupe et $H \subset G$. On dit que H est un sous groupe de G lorsque :
[H1] *H contient l'élément neutre du groupe $(G, \cdot)$.*
[H2] *H est une partie stable par la loi de composition,*
[H3] *H est stable par passage au symétrique.*

Théorème *(10)*

Si H est un sous groupe de G, alors $(H, \cdot)$ est un groupe.

Caractérisation d'un sous groupe *(11)*

Une partie H d'un groupe $(G, \cdot)$ est un sous groupe de G si et seulement si
[H1] *H est non vide*
[H2] *$\forall (x, y) \in H^2, x \cdot y^{-1} \in H$.*

Exemple : *(12)*

L'ensemble $\mathcal{O}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) | {}^tAA = I_n\}$ est un sous groupe de $(\mathrm{GL}_n(\mathbb{R}), \times)$.

Intersection de sous groupes *(13)*

(1) (D) : **L'intersection d'une famille de sous-groupes est un sous-groupe.**
(2) (D) : *L'union de deux sous groupes n'est pas un sous groupe sauf en cas d'inclusion de l'un dans l'autre.*

Théorème - Définition : sous-groupe engendré *(14)*

(1) : *Soit X une partie de G. On note $\langle X\rangle$ l'intersection de tous les sous-groupes de $(G,\cdot)$ contenant X.*
(2) (D) : *C'est le plus petit sous-groupe contenant X (on parle du* **sous-groupe engendré par** *X).*
(3) (Dm) : *$\langle X\rangle$ est constitué des "mots finis" construits sur $X \cup X^{-1}$.*

Exemples :

(1) (D) : $\langle a\rangle = a^{\mathbb{Z}}$ ou $\mathbb{Z}a$.

(2) (D) : Si H, K sont des sous-groupes d'un groupe additif alors $\langle H \cup K\rangle = H + K = \{h + k | h \in H \text{ et } k \in K\}$.

(3) (Dm) : En particulier dans un groupe additif, $\langle a, b\rangle = \{ua + vb,\ u, v \in \mathbb{Z}\}$.

Théorème - Définition : groupe monogène, groupe cyclique *(15)*

(1) : *On dit que X est une* **partie génératrice** *de G lorsque $G = \langle X\rangle$.*
(2) : *On dit que G est* **monogène** *lorsqu'il existe $a \in G$ tel que $G = \langle a\rangle$.*
Exemples : $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{U}_n$. Contre-exemple $\mathbb{Q}$.
(3) : *On dit que G est* **cyclique** *lorsque G est monogène et fini.*

Théorème : sous-groupes de $(\mathbb{Z},+)$ *(16)*

Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les ensembles $n\mathbb{Z}$, $n \in \mathbb{N}$.

Classique : Théorème : sous groupes de $(\mathbb{R},+)$ (HP) *(17)*

Soit H un sous-groupe de $(\mathbb{R},+)$. Alors :
[C1] *H est de la forme $x_0\mathbb{Z}$ pour $x_0 \in \mathbb{R}_+$*
OU
[C2] *H est dense dans $\mathbb{R}$ c'est à dire que pour tous les réels $x < y$, l'ensemble $H \cap]x, y[$ n'est pas vide.*

Coin de la culture : Théorème de Lagrange (HP) *(18)*

Soient G un groupe fini et H un sous-groupe de G. Alors le cardinal de H divise le cardinal de G

2) Morphismes

Définition *(19)*

Un **morphisme de groupes** *est une application de $(G,\star)$ dans $(H,\perp)$ compatible avec les lois des deux groupes, c'est à dire :*

$$\forall (x_1, x_2) \in G^2, f(x_1 \star x_2) = f(x_1) \perp f(x_2).$$

Un **endomorphisme de groupe** *est un morphisme d'un groupe sur lui-même.*
Un **isomorphisme de groupes** *est un morphisme* **bijectif** *entre deux groupes.*
Un **automorphisme de groupe** *est un endomorphisme bijectif.*

Exemples : *(20)*

(1) : *Fonction Id_G*
(2) : *$n \mapsto a^n$ ou $n \mapsto na$*
(3) : *signe et valeur absolue dans $\mathbb{R}^*$.*
(4) : *signature d'une permutation à support fini.*
(5) : *conjugaison dans un groupe multiplicatif.*
(6) : *Les fonctions $\ln : \mathbb{R}_+^* \to \mathbb{R}$ et $\exp : \mathbb{C} \to \mathbb{C}^*$.*
(7) : *$\varphi : (\mathbb{R}_+^*, \times) \times (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ telle que*
. $\varphi(r, \theta) = r\exp(i\theta)$.
(8) : *La fonction $\det : GL_n(\mathbb{K}) \to \mathbb{K}^*$.*

Propriétés des morphismes de groupes - Noyau et Image *(21)*

Soit f un morphisme de groupes de G dans H. Alors :
(1) (D) : *$f(e_G) = e_H$, $f(g^n) = f(g)^n$.*
(2) : *Le noyau de f est $Ker(f) = \{g \in G | f(g) = e_H\}$*
(3) : *Son image est $Im(f) = \{h \in H | \exists g \in G, f(g) = h\}$*
(4) (D) : *l'image directe d'un s.g. est un s.g.*
(5) (D) : *l'image réciproque d'un s.g. est un s.g.*
(6) (D) : *le noyau de f est un sous groupe.*
(7) (D) : *la composée de morphismes est un morphisme.*
(8) (D) : *la réciproque d'un isomorphisme est un isomorphisme*

Exemple *(22)*

L'ensemble $\mathcal{SO}_n(\mathbb{R}) = \mathcal{O}_n^+(\mathbb{R}) = \{A \in \mathcal{O}_n(\mathbb{R}) | \det(A) = 1\}$ est un groupe.

Théorème *(23)*

Soit f un morphisme de groupes. Alors f est injectif si et seulement si $\operatorname{Ker} f = \{e\}$.

Remarque *(24)*

L'ensemble des automorphismes de G noté $Aut(G)$ est un sous groupe de l'ensemble des permutations de G.

3) Le groupe $\mathbb{Z}/n\mathbb{Z}$

Théorème *(25)*

Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n est une relation d'équivalence compatible avec l'addition, la soustraction et la multiplication. Tout $x \in \mathbb{Z}$ est congru modulo n à un unique élément de $[\![0, n[\![$ noté $x \bmod n$.

Conséquence *(26)*

On note $\mathbb{Z}/n\mathbb{Z} = \{0 \bmod n, \dots, (n-1) \bmod n\}$ l'ensemble des classes d'équivalence de la relation de congruence modulo n et on définit dans $\mathbb{Z}/n\mathbb{Z}$ les opérations d'addition, de soustraction et de multiplication par :

$$(x \bmod n) + (y \bmod n) = (x+y) \bmod n,$$
$$(x \bmod n) - (y \bmod n) = (x-y) \bmod n,$$
$$(x \bmod n) \times (y \bmod n) = (x \times y) \bmod n.$$

Les résultats ne dépendent pas des représentants x, y choisis.

Proposition *(27)*

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe additif et l'application $x \to x \bmod n$ est un morphisme surjectif de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$. Son noyau est le sous-groupe $n\mathbb{Z}$.

Théorème - Propriété universelle *(28)*

Soit $f : (\mathbb{Z}, +) \to (G, .)$ un morphisme de groupes dont le noyau contient $n\mathbb{Z}$.
[C1] *Il existe une unique application $\dot{f} : \mathbb{Z}/n\mathbb{Z} \to G$ vérifiant : $\forall x \in \mathbb{Z}$, $\dot{f}(x \bmod n) = f(x)$.*
[C2] *De plus, $\dot{f}$ est un morphisme de groupes et* $\operatorname{Im} \dot{f} = \operatorname{Im} f$.
[C3] *Enfin, $\dot{f}$ est injectif si et seulement si* $\operatorname{Ker} f = n\mathbb{Z}$.

Théorème chinois - version groupes *(29)*

Soient $n, p \in \mathbb{N}^*$ tels que $n \wedge p = 1$.
(1) (D) : *L'application $(x \bmod np) \mapsto (x \bmod n, x \bmod p)$ est bien définie et est un isomorphisme entre les groupes additifs $\mathbb{Z}/np\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.*
(2) (D) : *En particulier, pour tout $(a, b) \in \mathbb{Z}^2$, il existe $x \in \mathbb{Z}$ unique modulo np vérifiant $x \equiv a\ [n]$ et $x \equiv b\ [p]$. Et si $nu + pv = 1$ est une relation de* Bézout, *alors $x = nub + pva$ est une solution du système précédent.*

Théorème : générateurs de $\mathbb{Z}/n\mathbb{Z}$. *(30)*

Soit $x \in \mathbb{Z}$. La classe de congruence $x \bmod n$ engendre le groupe $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $x \wedge n = 1$.

Définition : Fonction indicatrice d'Euler *(31)*

on note $\varphi(n) = Card\ \{x \in [\![0, n[\![\text{ tel que } x \wedge n = 1\}$ le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$.

4) Ordre d'un élément. Théorème de Lagrange (du programme).

Définition : ordre d'un élément *(32)*

Si un élément a d'un groupe G engendre dans G un sous-groupe fini de cardinal d, on dit que a est d'ordre fini et, plus précisément, d'ordre d.
Si le sous-groupe engendré par a est infini, on dit que a est d'ordre infini.

Théorème : caractérisation de l'ordre d'un élément *(33)*

Si a est d'ordre fini, son ordre est le plus petit entier strictement positif m tel que $a^m = e$.

Exemples et remarques *(34)*

(1) : *dans $\mathbb{C}^*$, dans $\mathbb{Z}/n\mathbb{Z}$ et dans S_n.*
(2) : *$O(a) = 1 \iff a = e$. $O(a) = 1$ ou $2 \iff a^2 = e \iff a = a^{-1}$.*

Caractérisation de l'ordre *(35)*

a est d'ordre fini $n \iff (a^p = e \iff n \mid p) \iff (a^p = a^q \iff p \equiv q\ [n]) \iff Card\ \langle a \rangle = n$.
a est d'ordre infini $\iff (a^p = e \iff p = 0) \iff (a^p = a^q \iff p = q) \iff Card\ \langle a \rangle = \infty$.

Théorème de Lagrange *(36)*

Soient G un groupe fini et $a \in G$. Alors l'ordre de a divise le cardinal de G et en particulier, $a^{Card(G)} = e$.

5) Structure des groupes monogènes

Théorème : structure des groupes monogènes *(37)*

Soit G un groupe monogène.
[C1] *Si G est fini de cardinal n alors G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*
OU
[C2] *Si G est infini, G est isomorphe à $(\mathbb{Z}, +)$.*

Conséquences *(38)*

Soit G un groupe cyclique de cardinal n engendré par un élément a.
(1) : *Les générateurs de G sont les éléments de la forme a^k avec $k \wedge n = 1$. Leur nombre est égal à $\varphi(n)$.*
(2) : *Les sous-groupes de G sont monogènes et pour tout $d \mid n$, G admet exactement un sous-groupe de cardinal n/d, à savoir $\langle a^d \rangle$.*
(3) : *Tout groupe fini dont le cardinal n est un nombre premier est cyclique, isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et à $\mathbb{U}_n$.*

Proposition *(39)*

Pour tout $n \in \mathbb{N}^*$, le groupe multiplicatif $\mathbb{C}^*$ admet exactement un sous-groupe de cardinal n, à savoir $\mathbb{U}_n$.

Indicatrice d'Euler *(40)*

$$\sum_{d|n} \varphi(d) = n.$$

III — Étude élémentaire du groupe symétrique

Dans toute cette partie, n désigne un entier naturel au moins égal à 2.

1) Groupe symétrique d'ordre n

Définition-Théorème : *(41)*

(1) : *On appelle* **groupe symétrique d'ordre** n *l'ensemble des permutations de* $[\![\, 1\,,\, n\,]\!]$.
(2) (D) : *Il s'agit d'un groupe pour la loi de composition des applications (loi* $\circ$*), de cardinal* $n\,!$.
Notation : $\mathcal{S}_n$ *; pour deux permutations* σ *et* σ' *de* $\mathcal{S}_n$*, on note* $\sigma \circ \sigma'$ *ou simplement* $\sigma\sigma'$.
Enfin, une permutation $\sigma \in \mathcal{S}_n$ *peut s'écrire :* $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

Définition : Orbites *(42)*

Soit $\sigma \in \mathcal{S}_n$*. On note* $\mathcal{R}_\sigma$ *la relation d'équivalence sur les éléments de* $[\![\, 1\,,\, n\,]\!]$ *définie par :*
$\forall\, (x, y) \in [\![\, 1\,,\, n\,]\!]^2,\ x\mathcal{R}_\sigma y \Leftrightarrow \exists k \in \mathbb{Z},\ y = \sigma^k(x)$*. Les classes d'équivalence de* $\mathcal{R}_\sigma$ *sont appelées les orbites de* σ.

Définition : Cycles *(43)*

On appelle **cycle** *de* $\mathcal{S}_n$ *toute permutation de* $\mathcal{S}_n$ *telle qu'il existe une et une seule orbite non réduite à un élément. Le cardinal de l'orbite non réduite à un élément d'un cycle de* $\mathcal{S}_n$ *s'appelle la longueur ou l'***ordre** *du cycle. C'est un élément de* $[\![\, 2\,,\, n\,]\!]$*. Un cycle de longueur* n *de* $\mathcal{S}_n$ *s'appelle une* **permutation circulaire**.

Cycles et orbites - Propriétés : *(44)*

Soit $\sigma \in \mathcal{S}_n$ *un cycle de longueur* p *et* $a \in [\![\, 1\,,\, n\,]\!]$ *dont l'orbite est de longueur* p*. Alors :*
(1) (D) : *L'orbite de* a *est l'ensemble* $\{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{p-1}(a)\}$ *et*
(2) (D) : p *est le plus petit entier naturel* k *non nul tel que* $\sigma^k(a) = a$.
Notation : *On peut donc noter un cycle sous la forme* $\big(a\ \sigma(a)\ \ldots\ \sigma^{p-1}(a)\big)$.
(3) : *Déterminer les orbites d'une permutation permet de décomposer cette permutation en produit de cycles qui commutent.*
(4) (D) : *Un* p*-cycle à la puissance* p *est l'identité.*

2) Transpositions et signature

Décomposition en produit de transpositions *(45)*

(1) : *On appelle* **transposition** *de* $\mathcal{S}_n$ *tout cycle de longueur 2.*
(2) (D) : *Toute permutation de* $\mathcal{S}_n$ *se décompose en produit de transpositions.*
(3) (D) : *Un* p*-cycle est produit de* $p-1$ *transpositions :* $(a_1\ a_2\ \ldots\ a_p) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{p-1}\ a_p)$.

Signature : *(46)*

(1) : *On appelle* **inversion** *de* $\sigma \in \mathcal{S}_n$ *tout couple* $(i, j) \in [\![\, 1\,,\, n\,]\!]^2$ *tel que* $i < j$ *et* $\sigma(i) > \sigma(j)$.
Notation : *On note* $I(\sigma)$ *le nombre d'inversions de* σ.
(2) : *On appelle* **signature** *de* $\sigma \in \mathcal{S}_n$ *le nombre* $(-1)^{I(\sigma)}$. ***Notation :*** $\varepsilon(\sigma)$.
(3) : *Si* $\varepsilon(\sigma) = 1$*, on dit que* σ *est une permutation* **paire** *et sinon, on dit que* σ *est une permutation* **impaire**.
(4) (Dm) : *Une transposition est une permutation impaire.*
(5) (D) : *Pour toute permutation* σ *de* $\mathcal{S}_n$*,* $\varepsilon(\sigma) = \displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}$.

Propriétés : *(47)*

(1) (D) : *La fonction* $\varepsilon : \sigma \mapsto \varepsilon(\sigma)$ *est un morphisme de groupes surjectif de* $(\mathcal{S}_n, \circ)$ *sur* $(\{-1, 1\}, \times)$.
(2) (D) : *Un* p*-cycle a pour signature* $(-1)^{p-1}$.
(3) (D) : *Le noyau de* ε *est appelé* **groupe alterné d'ordre** n*, sous-groupe de* $\mathcal{S}_n$ *d'ordre* $\frac{n\,!}{2}$. ***Notation :*** $\mathcal{A}_n$.
(4) : *Le groupe* $\mathcal{A}_n$ *est constitué des produits de cardinaux pairs de transpositions.*

IV — Travaux dirigés

Exercice 1 : Essai de tables

Les tables d'opérations suivantes sont-elles définissent-elles des structures de groupes ? Justifier.

(1) :

	a	b	c
a	a	a	a
b	a	b	b
c	a	b	c

(2) :

	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

(3) :

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	d	c	b	a
d	c	d	a	b

Exercice 2 : Tables d'un groupe

Construire la table du seul groupe à 3 éléments (a, b, c).
Combien existe-t-il de groupes à 4 éléments (a, b, c, d) ? En donner les tables.

Exercice 3 : Groupes à 4 éléments

On a vu qu'il existe seulement deux tables de groupes à 4 éléments. Vérifier que ces tables sont celles des groupes U_4 et $U_2 \times U_2$ muni de sa structure de groupe produit.

Exercice 4 : Groupes à 6 éléments

On connait au moins trois groupes à 6 éléments : $U_6, \mathcal{S}_3$ et $U_2 \times U_3$.
(1) : *Dresser leurs tables et vérifier que celles de U_6 et de $U_2 \times U_3$ sont les mêmes.*
(2) : *Sont-ils commutatifs ?*
Pour les plus motivés : *en existe-t-il d'autres ?*

Exercice 5 : Loi Δ

Soit E un ensemble et $G = \mathcal{P}(E)$.
Jusitifier que $(G, \cup)$ et $(G, \cap)$ ne sont pas des groupes.
Pour deux parties A et B de E, on pose $A \Delta B = (A \cup B) \setminus (A \cap B)$ (appelée différence symétrique de A et de B).
Montrer que (G, Δ) est un groupe commutatif.

Exercice 6 : Translations surjectives

Soit G un ensemble non vide muni d'une opération interne $\cdot$ associative telle que :

$$\forall\, (a, b) \in G^2,\ \exists\, (x, y) \in G^2 \text{ tel que } a = x \cdot b = b \cdot y.$$

Montrer que $(G, \cdot)$ est un groupe.

Exercice 7 : Loi associative régulière

Soit E un ensemble fini muni d'une opération interne $*$ associative pour laquelle tout élément est régulier à droite et à gauche. Montrer que E est un groupe.

Exercice 8 : Partie finie stable par produit

Soit G un groupe multiplicatif et H une partie finie de G non vide, stable par multiplication. Montrer que H est un sous-groupe de G.

Exercice 9 : Groupe sans sous-groupe non trivial

Soit G un groupe ayant au moins deux éléments et n'ayant pas de sous-groupe non trivial. Montrer que G est monogène, fini, et que $\operatorname{Card} G$ *est un nombre premier.*

Exercice 10 : Centre d'un groupe et commutant

Soit G un groupe multiplicatif. On note $Z(G) = \{a \in G \text{ tel que } \forall\, b \in G, \text{ on a } ab = ba\}$ (centre de G), et pour $a \in G$: $C(a) = \{b \in G \text{ tel que } ab = ba\}$ (commutant de a).
Montrer que $Z(G)$ et $C(a)$ sont des sous-groupes de G.

Exercice 11 : Transport de structure

Soit G un groupe multiplicatif, E un ensemble, et $\varphi : G \to E$ une bijection. On définit une opération $*$ sur E par :

$$\forall\, x, y \in E,\ x * y = \varphi(\varphi^{-1}(x)\varphi^{-1}(y)).$$

Montrer que $*$ est une loi de groupe et que les groupes G et E sont isomorphes.

Exercice 12 : Transport de structure

Pour $x, y \in \mathbb{R}$, on pose $x * y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$.
(1) : *Vérifier que $\sqrt{1+(x*y)^2} = \sqrt{1+x^2}\sqrt{1+y^2} + xy$.*
(2) : *Montrer que $(\mathbb{R}, *)$ est un groupe.*
(3) : *Montrer que l'application* sh *est un isomorphisme entre $(\mathbb{R}, +)$ et $(\mathbb{R}, *)$.*

Exercice 13 : Transport de structure

Pour $x, y \in \mathbb{R}$, on pose $x * y = \sqrt[3]{x^3 + y^3}$. Montrer que $(\mathbb{R}, *)$ est un groupe isomorphe à $(\mathbb{R}, +)$.

Exercice 14 : Autour de $\mathcal{P}(E)$

Soit E un ensemble et $G = \mathcal{P}(E)$ muni de la loi Δ.
(1) : *Pour $a \in E$, on note* $\varphi_a : \begin{cases} (G, \Delta) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ X & \longmapsto & \dot{0} \text{ si } a \notin X \\ X & \longmapsto & \dot{1} \text{ si } a \in X. \end{cases}$
Montrer que φ_a est un morphisme de groupes.
(2) : *On prend $E = [\![1, n]\!]$ et on note* $\varphi : \begin{cases} (G, \Delta) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^n \\ X & \longmapsto & (\varphi_1(X), \ldots, \varphi_n(X)). \end{cases}$
Montrer que φ est un isomorphisme de groupes. En déduire le cardinal de G.

Exercice 15 : Structure de solutions

Soit f un morphisme de groupes entre G_1 et G_2. Soit $a \in G_2$. On suppose que l'équation $f(x) = a$ admet au moins une solution.
(1) : *Montrer que dans ce cas, l'ensemble des solutions S est $\{x_0 \cdot u,\ u \in \operatorname{Ker} f\} = \{v \cdot x_0,\ v \in \operatorname{Ker} f\}$ où x_0 est une solution particulière.*
(2) : *En déduire que le cardinal de S est celui de* $\operatorname{Ker} f$.
(3) : *Retrouver que f est injective si et seulement si* $\operatorname{Ker} f = \{e_{G_1}\}$.
(4) : *Application : si $a \wedge b = d \neq 0$, montrer que l'équation $ax + by = c$ a des solutions (x, y) dans $\mathbb{Z}^2$ si et seulement si $d \mid c$ et que dans ce cas, les solutions diffèrent entre elles d'un multiple de $(b/d, -a/d)$.*

Exercice 16 : "Formule du rang" pour les morphismes de groupes

Soit $f : G \to G'$ un morphisme de groupes où G est un groupe fini.
Montrer que $\operatorname{Card}(\operatorname{Ker} f) \times \operatorname{Card}(\operatorname{Im} f) = \operatorname{Card}(G)$.

Exercice 17 : Images directes et réciproques

Soit G un groupe additif et $f : G \to G'$ un morphisme de groupes.
(1) : *Montrer que pour tout sous-groupe H de G on a : $f^{-1}(f(H)) = H + \operatorname{Ker} f$.*
(2) : *Montrer que pour tout sous-groupe H' de G' on a : $f(f^{-1}(H')) = H' \cap \operatorname{Im} f$.*

Exercice 18 : Groupe des automorphismes

Soit G un groupe multiplicatif. On note $\boldsymbol{Aut}(G)$ l'ensemble des isomorphismes $\varphi : G \to G$.
(1) : *Montrer que $\boldsymbol{Aut}(G)$ est un groupe pour la loi $\circ$.*
(2) : *Déterminer $\boldsymbol{Aut}(\mathbb{Z})$.*
(3) : *Pour $a \in G$ on note $\varphi_a : \begin{cases} G & \longrightarrow & G \\ x & \longmapsto & axa^{-1}. \end{cases}$ Montrer que $\varphi_a \in \boldsymbol{Aut}(G)$, et que l'application $a \mapsto \varphi_a$ est un morphisme de groupes.*

Exercice 19 : Ordre d'un élément

(1) : *Soient G et G' deux groupes et f un morphisme de G dans G'. Pour $a \in G$, comparer l'ordre de a et celui de $f(a)$.*
(2) : *Soient $(a, b) \in G^2$. Comparer les ordres de a et de bab^{-1}.*
(3) : *Soient $(a, b) \in G^2$. Comparer les ordres de ab et de ba.*

Exercice 20 : Ordre de ab

Soient a, b deux éléments d'un groupe multiplicatif G tels que : a est d'ordre α, b est d'ordre β, $\alpha \wedge \beta = 1$, $ab = ba$. Déterminer l'ordre de ab.

Exercice 21 : Décomposition d'un élément d'ordre fini

Soit G un groupe multiplicatif et $a \in G$ d'ordre np avec $n \wedge p = 1$. Montrer qu'il existe $b, c \in G$ uniques tels que b est d'ordre n, c est d'ordre p, $a = bc = cb$.

Exercice 22 : Sous-groupes d'un groupe cyclique

Soit $n \in \mathbb{N}^*$ et $G = \mathbb{Z}/n\mathbb{Z}$. Soit $k \in \mathbb{Z}$ et $d = k \wedge n$.
(1) : *Déterminer l'ordre de $\dot{k}$ dans G.*
(2) : *Montrer que $\dot{k}$ et $\dot{d}$ engendrent le même sous-groupe de G.*
(3) : *Quels sont tous les sous-groupes de G ?*

Exercice 23 : Morphismes entre deux groupes cycliques

Soit G un groupe cyclique engendré par a d'ordre n, G' un deuxième groupe, et $a' \in G'$.
Montrer qu'il existe un morphisme $\varphi : G \to G'$ tel que $\varphi(a) = a'$ si et seulement si a' est d'ordre fini divisant n.
Application : déterminer tous les morphismes $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$, $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Exercice 24 : Morphismes de $\mathbb{Q}$ additif

Déterminer tous les morphismes de …
(1) : $(\mathbb{Q}, +)$ *dans* $(\mathbb{Q}, +)$. (ce sont les $x \mapsto ax$**,** $a \in \mathbb{Q}$**.**)
(2) : $(\mathbb{Q}, +)$ *dans* $(\mathbb{Z}, +)$. (il n'y a que $x \mapsto 0$**.)**
(3) : $(\mathbb{Q}, +)$ *dans* $(\mathbb{Q}^*, \times)$.(il n'y a que $x \mapsto 1$**.**)

Exercice 25 : Sous groupes finis de $\mathbb{C}^*$

Déterminer tous les sous-groupes finis de $(\mathbb{C}^*, \times)$.

Exercice 26 : Groupe diédral

Soit $n \in \mathbb{N}$, $n3$. On note $\omega = e^{2i\pi/n}$ et :

$$f_k : \begin{cases} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \omega^k z \end{cases} (1) \ : g_k : \begin{cases} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \omega^k \overline{z} \end{cases} (2) \ : (0 \leqslant k < n)$$

(3) : *Montrer que $G = \{f_0, \ldots, f_{n-1}, g_0, \ldots, g_{n-1}\}$ est un groupe pour la composition des applications.*
(4) : *Soit $a > 0$ et A_k le point du plan d'affixe $a\omega^k$. Montrer que G représente le groupe des isométries du polygone $A_0 \ldots A_{n-1}$.*
(5) : *G est-il cyclique ?*
(6) : *Montrer que G est engendré par les applications f_1 et g_0 et que l'on a : $f_1 \circ g_0 = g_0 \circ f_1^{-1}$.*
(7) : *Soit H un groupe quelconque engendré par deux éléments ρ et σ tels que ρ est d'ordre n, σ est d'ordre 2, $\rho\sigma = \sigma\rho^{-1}$. Montrer que G et H sont isomorphes.*

Exercice 27 : Groupe d'ordre pair

Soit G un groupe fini de cardinal pair. Montrer qu'il existe un élément d'ordre 2.

Exercice 28 : Groupe d'ordre impair

Soit G un groupe fini de cardinal impair. Montrer que : $\forall\, x \in G,\ \exists!\, y \in G$ tel que $x = y^2$.

Exercice 29 : Groupe d'exposant 2

Soit G un groupe fini tel que : $\forall\, x \in G,\ x^2 = e$.
(1) : *Montrer que G est commutatif (considérer $(xy)(xy)$).*
(2) : *Soit H un sous-groupe de G et $x \in G \setminus H$. On note K le sous groupe engendré par $H \cup \{x\}$. Montrer que* $\operatorname{Card} K = 2 \operatorname{Card} H$.
(3) : *En déduire que* $\operatorname{Card} G$ *est une puissance de 2.*

Exercice 30 : Groupes d'ordre 6

Déterminer tous les groupes finis de cardinal 6 (on admettra que dans un tel groupe, il existe un élément a d'ordre 2, et un élément b d'ordre 3).

Exercice 31 : Groupe d'homographies

Soit $E = \mathbb{R} \setminus \{0, 1\}$, et $f : \begin{cases} E & \longrightarrow & E \\ x & \longmapsto & \dfrac{1}{x}, \end{cases}$ (1) : $g : \begin{cases} E & \longrightarrow & E \\ x & \longmapsto & 1 - x. \end{cases}$
Vérifier que f et g sont des bijections et déterminer le groupe engendré par f et g pour la loi $\circ$ (il contient exactement six éléments).

Exercice 32 : Groupes de similitudes

Pour $\alpha \in \mathbb{C}^*$ et $\beta \in \mathbb{C}$, on note $f_{\alpha,\beta} : \begin{cases} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \alpha z + \beta \end{cases}$
(1) : *Montrer que l'ensemble des fonctions $f_{\alpha,\beta}$ est un groupe pour la loi $\circ$. Est-il commutatif ?*
(2) : *A quelle condition sur α, β, $f_{\alpha,\beta}$ est-elle d'ordre fini ?*

Exercice 33 : Thm de Lagrange

Soit G un groupe fini et H un sous-groupe de G. On définit une relation sur G par :

$$\forall\, x, y \in G,\ x \sim y \Leftrightarrow \exists\, h \in H \text{ tel que } x = hy.$$

(1) : *Montrer que $\sim$ est une relation d'équivalence. Quelle est la classe de e ?*
(2) : *Soit $a \in G$. Montrer que à est équipotent à H.*
(3) : *En déduire que* $\operatorname{Card} H$ *divise* $\operatorname{Card} G$ *(Théorème de Lagrange).*

Exercice 34 : Sous-groupes de type fini de $\mathbb{Q}$

(1) : *Soit H un sous-groupe additif de $\mathbb{Q}$ engendré par un nombre fini d'éléments. Montrer que H est monogène.*
(2) : *Trouver un sous-groupe non trivial de $\mathbb{Q}$ qui n'est pas engendré par une famille finie.*

Exercice 35 : $(\mathbb{Q}, +)$ et $(\mathbb{Q}^{+*}, \times)$ ne sont pas isomorphes

Montrer que les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}^{+*}, \times)$ ne sont pas isomorphes.

Exercice 36 : Centre d'un p-groupe

Soit G un groupe fini de cardinal p^k où p est un nombre premier et $k \in \mathbb{N}^*$. On note Z le centre de G.
(1) : *En considérant l'action de G sur lui-même par automorphismes intérieurs montrer que* $\operatorname{Card}(Z) \equiv 0\ [p]$.
(2) : *En déduire que tout groupe d'ordre p^2, p premier, est commutatif et est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$ soit à $(\mathbb{Z}/p\mathbb{Z})^2$.*

Exercice 37 : Groupe fini ?

Soit G un groupe ayant un nombre fini de sous-groupes. Montrer que G est fini.

V — Sujets d'oraux de concours autres que CCP

Exercice 38 : Centrale

Montrer que

$$\left\{x + y\sqrt{3} \mid x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\right\}$$

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

Exercice 39 : Polytechnique

1. *Montrer que tout sous-groupe additif de* $\mathbb{R}$ *qui n'est pas monogène est dense dans* $\mathbb{R}$.
2. *Soit* $x \in \mathbb{R} \setminus \mathbb{Q}$. *Montrer qu'il existe une infinité de* $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ *tels que*

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$$

3. *Montrer la divergence de la suite de terme général*

$$u_n = \frac{1}{n \sin n}$$

Exercice 40 : Centrale

Quel est le plus petit entier n *tel qu'il existe un groupe non commutatif de cardinal* n *?*

Exercice 41 : Centrale

Soit n *un entier naturel non nul,* $(e_1, \ldots, e_n)$ *la base canonique de* $E = \mathbb{R}^n$.
Soit $\mathcal{S}_n$ *l'ensemble des permutations de* $\{1, 2, \ldots, n\}$. *Soit* $t_i = (1, i)$.
Pour $s \in \mathcal{S}_n$, *on définit* $u_s(e_i) = e_{s(i)}$.

1. *Montrer que* $(t_2, t_3, \ldots, t_n)$ *engendre* $\mathcal{S}_n$.
2. *Interpréter géométriquement* u_s *lorsque* s *est une transposition.*
3. *Soit* $s = (1\ 2\ \ldots\ n-1\ n)$. *On suppose que* s *est la composée de* p *transpositions. Montrer que* $p \geqslant n - 1$.
4. *Quel est le cardinal minimal d'une famille de transpositions génératrice de* $\mathcal{S}_n$ *?*

Exercice 42 : Mines

On note V *l'ensemble des matrices à coefficients entiers du type*

$$\begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}$$

et G *l'ensemble des* $M \in V$ *inversibles dans* $\mathcal{M}_4(\mathbb{R})$ *et dont l'inverse est dans* V.

1. *Quelle est la structure de* G *?*
2. *Soit* $M \in V$. *Montrer que* $M \in G$ *si, et seulement si,* $\det M = \pm 1$.
3. *Donner un groupe standard isomorphe à* G *muni du produit.*