Groupes

* 1. Généralités
     1. Définition

Un groupe est un couple  constitué d’un ensemble *G* et d’une loi de composition interne  sur *G* de sorte que :

(1)  est associative

(2) Il y a dans *G* un élément neutre pour .

(3) Tout élément de *G* admet un symétrique pour la loi .

C’est-à-dire :



Remarque :

Si  est un groupe, il y a unicité du neutre (déjà vu en cas plus général).

Si de plus  est commutative, on dit que  est un groupe commutatif.

* + 1. Exemples

 n’est pas un groupe.

 est un groupe.

 n’est pas un groupe.

 n’est pas un groupe, mais  en est un.

* Créons un groupe à trois éléments 

Loi  définie par la table de Pythagore donnant  :



On pose *a* comme élément neutre, et on choisit 

* + 1. Règles de calcul
       1. En notation « bizarre »

Soit *G* un ensemble muni d’une loi  formant un groupe.

* Il y a dans *G* un et un seul élément neutre :

L’existence est déjà donnée par la définition d’un groupe.

Supposons que  sont deux neutres.

Alors  (première égalité :  est neutre ; deuxième : *e* est neutre)

On peut donc parler *du* neutre du groupe .

* Tout élément *x* de *G* admet un et un seul symétrique par  :

L’existence est toujours donnée par la définition d’un groupe.

Supposons que  sont deux symétriques de *x*.

Alors 

On note dans ce sous paragraphe  le symétrique de *x*.

* Pour tout  :



Donc *x* est symétrique de .

* Pour tous  :



Et 

Donc 

* Remarque :

On a, pour tout .

On peut donc le noter sans ambiguïté 

* « Résolution d’équations » :

Pour tous  :



Démonstration du (1) :

Si , alors .

Or, . Donc 

Si , alors 

La démonstration est la même pour (2)…

* Régularité

Pour tous , on a :



(Les autres implications sont vraies aussi mais évidentes)

Démonstration de (1) :

Si , alors 

Soit , donc  c'est-à-dire 

La démonstration est encore la même pour (2).

Conséquence : dans une table de Pythagore d’un groupe fini , on ne voit jamais deux fois le même élément dans une même rangée (ligne ou colonne) :

Si  et , alors , soit .

* Itéré d’un élément :

Soit . On note (dans ce sous paragraphe seulement) :

, 

Plus rigoureusement :

On définit, pour tout ,  par récurrence en posant :



Alors il est facile (mais pénible à écrire) d’établir que, pour tout ,  et 

* Itéré « un nombre négatif de fois » :

Soit , .

On pose 

Alors 

Les règles précédentes se généralisent à Z.

* + - 1. En notation « multiplicative » (réécriture)

Dans le groupe  avec les notations suivantes :

* Le neutre  appelé aussi élément unité
* Le symétrique de  est noté , appelé aussi inverse de *x*.
* L’itéré *n* fois est noté .
* Le symbole  est souvent omis :  est noté aussi .

Les règles précédentes donnent :



* + - 1. En notation « additive » (réservée aux groupes commutatifs)

Dans le groupe , avec les notations suivantes :

* Le neutre  est appelé l’élément nul de *G*
* Le symétrique de  est noté , appelé aussi opposé de *x*.
* L’itéré *n* fois est noté  ou .
* On suppose de plus que le groupe  est commutatif, c'est-à-dire :



Les règles donnent alors :





 ;  est noté aussi 



, noté aussi 



* + 1. Autres exemples de groupe

- Rappels :

Groupes de nombres :



- Groupes de permutation :

Soit *E* un ensemble non vide quelconque. On note  l’ensemble des permutations sur *E* (ensemble des bijections de *E* dans *E*). Alors  constitue une loi de composition interne sur , et  est un groupe, appelé groupe des permutations de *E*. Ce groupe est non commutatif dès que *E* a au moins trois éléments.

Démonstration :

* On peut composer deux bijections de *E* dans *E*, et on obtient une bijection de *E* dans *E*.
* La loi  est associative :



(Démontré dans un cas plus général et pas seulement pour les bijections)

* Neutre : 
* Tout  a un symétrique pour , à savoir .

Donc  est un groupe.

Montrons que, pour un ensemble *E* de plus de trois éléments,  n’est pas commutatif :

Soient *a*, *b*, *c* trois éléments de *E* distincts.

Soient  définies ainsi :



Alors *f* et *g* sont dans , puisque ce sont des applications de *E* dans *E* et inversibles d’inverse elles-mêmes (elles sont involutives).

Et on a alors  :



Exemples :

* On note  le groupe  lorsque . Ainsi,  est un groupe fini de cardinal .
* Table de Pythagore de  :

, où :



 définie par 

Tableau donnant  :



* Table de Pythagore de  :

, où :



 défini par  sinon.

 définie par 

 définie par .

Tableau donnant  :



* , où :

*A* est quelconque, et  est un groupe, avec :

 défini par :



* + 1. Classes d’équivalence modulo *n*.

Soit .

On définit sur Z la relation  par :

Pour tous 

Cette relation s’appelle la relation de congruence modulo *n*.

On note plutôt  ou encore 

Cette relation est une relation d’équivalence :

(1)  puisque 

(2) Pour tous , si  alors  donc  soit 

(3) Soient . Si  et , alors  s’écrit  où , et  s’écrit  où . Donc . Donc .

Donc  est réflexive (1), symétrique (2) et symétrique (3), c’est donc une relation d’équivalence.

Cette relation est compatible avec + :

Pour tout  :

Si , alors :

,  donc  soit , c'est-à-dire .

Pour tout , on appelle classe d’équivalence modulo *n*, et on note , l’ensemble des éléments de Z congrus à *x* modulo *n*. (Attention, la notation n’indique pas qu’on travaille modulo *n*). On a alors l’équivalence :

.

En effet :

Soient 

Si . Déjà,  (car  est réflexive), c’est à dire , donc .

Si . Soit . Alors . Donc  (car  est transitive). Donc . Donc . De même, . Donc .

D’où l’équivalence, pour tous .

On note  l’ensemble des classes d’équivalences modulo *n*.

Ainsi, .

Proposition, définition :

 est fini, et de cardinal *n*.

Pour tous , on pose .

Alors  définit une loi de composition interne sur , et  est un groupe commutatif.

Démonstration :

* Soit .

Alors il existe  tel que , c'est-à-dire tel que .

En effet :

En prenant , où , on a alors :

, donc , soit , c'est-à-dire , d’où l’existence.

Donc 

Donc  contient au plus *n* éléments, à savoir les . On doit donc maintenant montrer que tous ces éléments sont distincts.

Soient , supposons que , c'est-à-dire que .

Il existe donc  tel que .

Alors . On a :

. Donc 

Donc 

Donc . Or, . Donc 

Donc . Donc .

Donc 

Soit, par contraposée : .

Donc  contient au moins *n* éléments, à savoir les 

Donc  est fini, de cardinal *n*.

* Montrons déjà que la loi  est bien définie, c'est-à-dire que pour tous ,  ne dépend que de , et non pas de *x* et de *y*:

Si  est tel que , et  tel que , alors  et , soit  donc .

Déjà,  est évidemment une loi de composition interne sur 

 est associative : en effet, pour tous , on a :



Pour tout , on a :



Donc  admet un élément neutre pour , à savoir .

Soit , posons  (ainsi, ). On a alors :



Donc tout élément de  admet un symétrique pour .

Enfin,  est commutative : pour tous , on a :



Donc  est bien un groupe commutatif. (on notera plutôt + pour )

* 1. Sous-groupes (notation multiplicative)
     1. Définition

Soit  un groupe.

Soit *H* une partie de *G*.

On dit que *H* constitue un sous-groupe de  lorsque :

1. 
2. *H* est stable par  : 
3. *H* est stable par passage à l’inverse : 

Proposition :

Si *H* est un sous-groupe de , alors  constitue une loi de composition interne sur *H*, et  est un groupe.

* Déjà,  est bien une loi de composition interne sur *H* d’après (2)
* L’associativité n’est pas perdue par restriction.
* Neutre : c’est  qui est dans *H* d’après (1)
* Existence d’un inverse pour tout *x* de *H* d’après (3).
  + 1. Exemples

-  est un sous-groupe de ,  de  (et aussi de ), , ,  sont des sous-groupes de 

U est un sous-groupe de  ()

 est un sous-groupe de  ()

- Des sous-groupes de  sont : 

(Le dernier est une droite du plan complexe passant par *O*)

- Pour ,  est un sous-groupe de Z.

- Si  est un groupe, alors  et *G* sont des sous-groupes de *G* (les autres sous-groupes sont appelés les sous-groupes propres de *G*)

-  est un sous-groupe (commutatif) de  qui n’est pas commutatif.

Soit , *A* une partie de  non vide.

Soit , c'est-à-dire que *H* est l’ensemble des permutations qui laissent stable *A* (remarque : si , comme  est bijective,  a le même cardinal que *A*, donc )

Alors *H* est un sous-groupe de  :

- 

- *H* est stable par  : si , , alors 

- *H* est stable par passage au symétrique : si , alors 

En effet :

Supposons que . Alors 

Soit . Donc .

Il existe donc *y* dans *A* tel que , avec 

Donc , donc 

D’où l’inclusion  (et même l’égalité puisque  est bijective)

- Des sous-groupes de  :

* L’ensemble des fonctions polynomiales
*  où *f* est un élément fixé de .
* 
*  où ,  où 
* Ensemble des fonctions *T*-périodiques (à *T* fixé)
* Ensemble des fonctions *k*-lipschitzienne (à *k* fixé)
* Ensemble des fonctions uniformément continues
* Ensemble des fonctions paires, impaires…

- Sous-groupes de  :

Pour  :



 engendre ,  aussi.

 et  engendrent .

 engendre .

On dit que  est un élément d’ordre 6,  et  d’ordre 3,  d’ordre 2.

* + 1. Les sous-groupes de .

Déjà, les , où , sont des sous-groupes de Z.

Y en a-t-il d’autres ?

Soit *G* un sous-groupe de Z autre que .

Il contient donc un élément non nul de Z, et son opposé (l’un d’eux étant alors dans ). Donc l’ensemble  est non vide et est une partie de N. il admet donc un plus petit élément, disons . Alors .

En effet :

Déjà, une récurrence rapide montre que , puis comme *G* est stable par passage à l’inverse, , donc 

L’autre inclusion maintenant :

Soit . La division euclidienne de *x* par *n* donne :

, où  et .

Donc .

Donc . Comme *n* est le plus petit élément de , on a nécessairement  (car )

Donc 

Ainsi, les sous-groupes de Z sont exactement les , où .

* + 1. Une caractérisation condensée des sous-groupes

Proposition :

Soit  un groupe, *H* une partie de *G*.

Alors *H* est un sous-groupe de 

Démonstration :

La première implication est évidente. Pour l’autre :

Supposons que 

Alors déjà …

En prenant , Alors, pour tout , .

Pour tout , , donc  c'est-à-dire 

* + 1. Intersections de sous-groupes

Théorème :

Soit  un groupe.

Alors toute intersection de sous-groupes de *G* est un sous-groupe de *G*.

Démonstration :

Soit  une famille de sous-groupes de *G* indexée par *I*. Notons 

Déjà, , puisque .

Soient . Alors, pour tout , ,  donc .

Donc .

Donc *H* est un sous-groupe de .

* + 1. Sous-groupe engendré par une partie

Soit  un groupe.

Soit *A* une partie de *G*.

On appelle sous-groupe engendré par *A* le plus petit sous-groupe de *G* contenant *A*.

Il y en a bien un, puisque déjà *G* contient *A*. Donc l’ensemble  des sous-groupes de *G* contenant *A* n’est pas vide.

Considérons alors . C’est un sous-groupe de *G*, il contient *A* et est contenu dans tout sous-groupe de *G* contenant *A*.

On note alors 

Cas particulier :

Un sous-groupe engendré par un singleton  est noté , et on parle du sous-groupe engendré par l’élément *a*.

Exemples :

- Dans  :





 (on dit que  est un générateur de )

 ( est une partie génératrice de )

- Dans  : 

- Dans  :

 ;  ;  ; 

* + 1. Groupe monogène

Définition :

Soit  un groupe.

On dit que *G* est monogène lorsqu’il admet un générateur, c'est-à-dire lorsqu’il existe  tel que , c'est-à-dire : 

Remarque :



En effet :

- Soit *H* un sous-groupe de *G* contenant *a*. Alors, comme *H* est stable par  et passage à l’inverse, une récurrence évidente montre qu’alors *H* contient .

- L’ensemble  est effectivement un sous-groupe de *G* contenant *a*:

Il contient .

Il est stable par , puisque pour tous , *x* s’écrit , *y* s’écrit  (où ) et 

Il est stable par passage à l’inverse puisque pour tout , *x* s’écrit  où , et .

C’est donc un sous-groupe de *G*, et enfin il contient *a* puisque .

Donc  est un sous-groupe de *G* qui contient *a*, et c’est le plus petit.

Remarque :

Plus généralement,  est l’ensemble des produits de puissances d’éléments de *A*.

Définition :

Un groupe *G* est dit cyclique lorsqu’il est monogène et fini.

Exemples :

-  est monogène infini :  (Attention, notation additive)

Tous les sous-groupes de Z sont monogènes (infinis) : 

-  est cyclique, engendré par  (qui n’est généralement pas le seul)

-  est aussi cyclique :  où .

* 1. Morphismes de groupes

(Morphisme est une apocope de homomorphisme)

* + 1. Définition (en notation « bizarre »)

Soient  et  deux groupes.

Un morphisme de  vers  est une application  telle que :



Exemples :

 est un morphisme de  vers 

 de  vers  (ou vers  aussi)

 de  vers 

 de  vers 

* L’ensemble  des suites réelles convergentes est un sous-groupe de  et l’application  est un morphisme de  vers .
  + 1. Propriétés (notation multiplicative)

Proposition :

Soit  un morphisme d’un groupe  vers un groupe .

Alors :



Démonstration :

* C’est la définition.
* .

L’élément  de *H* vérifie donc . Donc 

* Soit . Alors 

De même, 

Donc 

* Soit . Montrons par récurrence que  :

Pour , 

Soit , supposons que .

Alors 

On passe aux *n* négatifs avec le point précédent.

* + 1. Noyau et image d’un morphisme

Définition, proposition :

Soit  un morphisme d’un groupe  vers un groupe .

L’image de , notée , c’est , c'est-à-dire 

Alors  est un sous-groupe de *H*.

Démonstration :

-  contient  car 

-  est stable par  :

Soient . Alors *u* s’écrit  où , *v* s’écrit  où .

Donc 

-  est stable par passage à l’inverse :

Soit . Alors *u* s’écrit  où .

Et : 

Définition :

Soit  un morphisme d’un groupe  vers un groupe .

Le noyau de , noté  est par définition :



Proposition :

 est un sous-groupe de *G*.

Démonstration :

-  car .

- Pour tous , on a  donc .

- Pour tout ,  donc .

Théorème :

Soit  un morphisme d’un groupe  vers un groupe . Alors :

1. Pour tous , 
2.  est injective 

Démonstration :

1. On a les équivalences :



1. Supposons  injective :

Soit . Alors .

Donc, comme  est injective, . Donc 

De plus,  est un sous-groupe de *G*, donc , donc .

D’où l’égalité.

Réciproquement, supposons que  :

Soient alors . Supposons que .

Alors . Donc . Donc .

Donc  est injective.

Exemple :

L’application  est un morphisme de  vers  de noyau  et d’image 

* + 1. Composition

Proposition :

La composée, quand elle est définie, de deux morphismes de groupes est un morphisme de groupes.

Démonstration :

Soient  trois groupes.

Soient  et  deux morphismes.

Alors  est bien définie, et va de  dans .

Soient . On a :



* + 1. Isomorphisme

Proposition, définition :

Soit  un morphisme bijectif de  vers . Alors  est un morphisme (bijectif) de  vers . On dit que  est un isomorphisme.

Lorsqu’il existe un isomorphisme entre deux groupes, on dit que ces deux groupes sont isomorphes.

Démonstration :

Soit  un morphisme bijectif de  vers .

Soient .

Soient  tels que . (C'est-à-dire ).

Alors 

Donc  est un morphisme de  vers .

Exemples :

 et  sont isomorphes, où  est la loi définie par :



C'est-à-dire 

(Ainsi, , où , qui réalise bien une bijection de  dans R)

 est un morphisme surjectif de  vers  mais non injectif. Son noyau est  :

Déjà, c’est un morphisme, puisque pour tous , on a :

.

*f* est surjective puisque tout élément  s’écrit  où .

Mais *f* n’est pas injective : pour tout , on a les équivalences :



Donc le noyau de *f* est , donc *f* n’est pas injective.

 où *k* est tel que  par contre est bijectif.

Démonstration :

Déjà, il faut montrer que la définition de  est cohérente, c'est-à-dire que  ne dépend que de  et non pas de *k*.

Si deux éléments  sont tels que , on a alors :

. Donc . Donc  (on est en notation additive)

Donc .

C’est un morphisme :

Pour tous  s’écrivant  et  où  :

.

 est surjective, puisque tout élément  s’écrit  où .

 est aussi injective :

Soit . Alors *u* s’écrit  où .

Alors . Donc . Donc . Donc .

Comme  est un sous-groupe de , on a aussi l’autre inclusion et donc l’égalité. Donc  est injective.

Donc  est bijective. Donc  et  sont isomorphes.

Remarque :

La relation « être isomorphe à » est une relation d’équivalence sur l’ensemble des groupes :

- Elle est réflexive (l’identité est un isomorphisme d’un groupe *G* vers *G*)

- Elle est symétrique (si *G* est isomorphe à *H*, alors *H* est isomorphe à *G*)

- Elle est transitive (la composée de deux isomorphismes est un isomorphisme)

* + 1. Vocabulaire (rappels)

- Un morphisme de *G* vers *H* est aussi appelé homomorphisme de *G* vers *H*.

- Un isomorphisme de *G* vers *H* est un morphisme bijectif de *G* vers *H*.

- Un endomorphisme de *G* est un morphisme de *G* vers *G*.

- Un automorphisme de *G* est un morphisme bijectif de *G* vers lui-même.

isomorphisme de *G* vers lui-même.

endomorphisme bijectif de *G*.

* 1. Ordre d’un élément d’un groupe

Soit  un groupe.

Théorème, définition :

Soient . Alors les trois affirmations suivantes sont équivalentes :

1.  est fini et de cardinal *n*.
2. Il existe  tel que , et *n* est le plus petit des ces entiers.
3. L’ensemble  n’est pas réduit à , c’est même .

Lorsque l’une des ces affirmations (et donc les trois) est vraie, on dit que *a* est un élément d’ordre fini de *G*, égal à *n*.

Démonstration :

Considérons . Alors  est un morphisme de  vers .

En effet, .

On a :



 est un sous groupe de  donc du type  où .

* Si ,  donc  est injective. Donc  réalise une bijection de Z sur . Donc  est infini.
* Si , . En effet :

Une première inclusion,  est déjà évidente.

Soit maintenant .

Alors *b* s’écrit  où . La division euclidienne de *k* par *m* () donne :

 avec .

Donc , d’où l’autre inclusion, et l’égalité.

De plus,  : il n’existe pas  distincts dans  tels que  car si par exemple , et si on avait , on aurait  ce qui ne se peut pas car  donc .

Avec cela, il est maintenant facile de montrer que  et  :

Supposons (1).

Alors, en gardant les notations précédentes, .

Donc *n* est bien le plus petit des  tels que , car  et  (puisque  et on a montré que les  sont distincts)

Et d’autre part l’ensemble des  tels que  est bien  (c’est )

Donc  et .

Supposons maintenant (3) : On est alors dans la situation  (car )

Donc le sous-groupe engendré par *a* est de cardinal *n*.

De même, .

Exemples :

Dans  :

 est d’ordre 3 :  de cardinal 3

Autre justification :  et 

 est d’ordre 2,  et  sont d’ordre 6,  est d’ordre 1.

Dans , 0 est d’ordre 1, tout les autres sont d’ordre infini.

Dans  :

Notation (dans ) : la permutation  est notée généralement .

Prenons par exemple . Alors  est d’ordre fini, car  et  est de cardinal fini (Donc au pire  est d’ordre ce cardinal, à savoir 15)