

GROUPES, ANNEAUX et CORPS

1.0

1

Juillet 2017

ATIAMPO KODJO ARMAND@UVCI 2017

Légende



Référence Bibliographique

Table des matières

Objectifs		5
Introduction		7
I - GROUPES		9
A. Loi de cor	mposition interne	9
B. Exercice		10
C. Exercice		10
D. Notion de	groupe	10
E. Sous-grou	upes	12
F. Exercice		13
G. Exercice		13
H. Morphism	ne de groupes	13
I. Exercice		
II - ANNEAUX	ET CORPS	15
A. Introducti	ion aux Anneaux	
B. Exercice		
C. Exercice		
D. Sous-ann	neaux et morphisme d'anneaux	
E. Exercice		18
F. Corps		19
G. Exercice		19
H. Exercice		20
Conclusion		21

Bibliographie 27



À la fin de cette leçon, vous serez capable de :

- Identifier la structure de groupe
- Identifier les structures d'anneau et de corps
- **Identifier** les éléments et les opérations possibles dans les groupes les anneaux et les corps



Introduction

Il s'agit de formaliser les propriétés classiques des ensembles usuels (N, Z, Q, R, Q, R*,...) munis de leurs opérations naturelles (somme, produit). Nous donnons ici les définitions précises de ces notions.



GROUPES

Loi de composition interne	9
Exercice	10
Exercice	10
Notion de groupe	10
Sous-groupes	12
Exercice	13
Exercice	13
Morphisme de groupes	13
Exercice	14

Objectifs

À la fin de cette leçon, vous serez capable de :

- **Comprendre** la notion de groupe
- **Identifier** les éléments et les opérations possibles dans les groupes

A. Loi de composition interne

Cette section est un rappel des propriété élémentaire des lois de composition interne



Définition : Définition 1

Soit E un ensemble. On appelle **loi de composition interne** toute application **f de E** × E vers E.



Syntaxe

Nous noterons de telles applications non pas sous la forme f(x, y) mais à l'aide d'un symbole * sous la forme x * y.



Exemple

L'addition, la soustraction, la multiplication et la division dans les ensembles de nombres sont des lois de composition internes.



Exemple

Soit E un ensemble. On a sur P(E) l'ensemble des parties de E, L'intersection (\cap) et La réunion (\cup) sont des lois de composition interne.



Fondamental: Proposition

Soit E un ensemble muni d'une loi de composition interne notée T. On dit que T **est associative** si \forall (x, y, z) \in E3, x T (y T z) = (x T y) T z T **est commutative si** \forall (x, y) \in E2, x T y = y T x



Exemple

L'addition est une loi associative dans (R, +)



Attention

Soient E un ensemble et soit f, g et h des applications de E vers E alors al composée n"est pas associative

En effet, on a en général $(f \circ g) \circ h \neq f \circ (g \circ h)$

B. Exercice

Montez que l'intersection et la réunion sont des lois de composition internes pour l'ensemble des parties de E

C. Exercice

[Solution n°1 p 23]

Exercice

Parmi les propositions suivantes, lesquelles sont vérifiées

	La loi de composition interne T sur définie sur R par \forall x, y \in R (xTy)=xy+ (x2 -1)(y2 -1) est commutative

L'application T définie sur $R\setminus\{0 \times R \text{ par } (x, y)T(x',y') = (xx', xy' + y) \text{ est une}$				
loi de composition interne				

L'application T définie sur $R\setminus\{0\}$ ×R par $(x, y)T(x', y') = (xx', xy' + y)$ est une					
loi de composition interne commutative					

D. Notion de groupe

GROUPES



Définition

Soit G un ensemble muni d'une loi de composition interne notée *. On dit que le couple (G, *) est un groupe si

- 1. la loi * est associative
- 2. G possède un élément neutre : \exists e \in G, \forall x \in G, x * e = e * x = x
- 3. tout élément de G admet un inverse ou symétrique: \forall $\mathbf{x} \in \mathbf{G}$, \exists $\mathbf{y} \in \mathbf{G}$, $\mathbf{x} * \mathbf{y} = \mathbf{y} * \mathbf{x} = \mathbf{e}$.

Si de plus la loi * est commutative, on dit que le groupe (G, *) est **commutatif** ou encore **abélien.**



Exemple

(Z,+), (Q,+), (R,+) et (C,+) sont des groupes.



Exemple

 $(Q*, \times)$, $(R*, \times)$ et $(C*, \times)$ sont des groupes



Exemple

Soit E un ensemble. Alors (Bij(E), \circ) , l'ensemble des bijections sur E est un groupe.



Attention

Dire qu'un ensemble G est un groupe n'a pas de sens si on ne précise pas pour quelle loi. Un groupe est un couple, c'est un ensemble muni d'une loi.



Attention

Si le groupe n'est pas commutatif, on ne peut pas simplifier, certaines expressions : $xyx \neq x^2y$, $xyx^{-1}y^{-1} \neq e$



Fondamental: Proposition 2

Soit (G, *) un groupe d'élément neutre e. Alors

- L'élément neutre e est unique.
- Pour tout x dans G, son inverse est unique.
- L'inverse de *e* est *e*.
- L'inverse de xy est y-1x-1.
- Pour tous x, y et z dans G, $xy = xz \Rightarrow y = z$.



Attention

Faites attention à la notion d'inverse d'un élément qui est plus général que l'inverse d'un élément de R*.

- En effet si on considère (R,+) alors l'inverse d'un élément x est -x. On l'appelle encore opposé.
- De même si on considère l'ensemble Bij(E, F) l'ensemble des bijections de E vers F muni de la loi interne o ou loi composée, l'inverse d'une bijection f est f-1 qui est alors appelé bijection réciproque.



Exemple

On munit $A = R \times R$ d'une loi T définie par (x,y)T(x',y') = (x+x', y+y'). nous allons montrer que (A,+) est un groupe commutatif :

E. Sous-groupes



Définition

Soit (G, *) un groupe d'élément neutre e et soit $H \subset G$.

Soit (G, *) un groupe et $H \subset G$. On dit que H est un **sous-groupe de G** si (H, *) est un groupe, c'est-à-dire si la restriction de la loi * au sous-ensemble H confère à H une structure de groupe.

L'ensemble H est un sous-groupe de G si

∀ x ∈ H, ∀ y ∈ H, x * y ∈ H;
 e ∈ H;

- \forall x ∈ H, x-1 ∈ H.



Exemple

- L'ensemble des nombres pairs est un sous-groupe de (Z,+).
- Le groupe tout entier G et {e} sont des sous-groupes de (G, *).
- Soient H et K deux sous-groupes du groupe G. En général H \cup K n'est pas un sous-groupe.

sous-groupe engendré

Soit (G, *) un groupe et $A \subset G$. On appelle **sous-groupe engendré par A** le plus petit sous-groupe (pour l'inclusion) de G contenant A. On le note < A >.



Exemple

- Dans (Z,+), le sous-groupe < 2 > engendré par 2 est le sous-groupe des nombres pairs.

 $< 2 > = \{2k \mid k \in Z\}$

Si < A >= G, on dit que l'ensemble A engendre le groupe G.



Exemple

Les nombres 2 et 3 engendrent (Z,+): < 2,3 >= Z. Ce résultat nous dit que tous les nombres entiers relatifs peuvent tous s'écrire à partir d'une combinaison des chiffres 2 et 3. Cela peut sembler bien curieux. les plus audacieux pourront tenter de le démontrer



Fondamental : Proposition

Soit (G, *) un groupe fini et H un sous-groupe de G. Alors le cardinal de H divise

GROUPES

le cardinal de G.



Syntaxe

Soit (G, *) un groupe de cardinal fini. Soit H un sous groupe de G et $x \in G$. On appelle **ordre de H** le cardinal de H. On appelle **ordre de H** le cardinal du sousgroupe H H sousgroupe H H is cardinal du sousgroupe H H sousgroupe H H is cardinal du sousgroupe H so H so H so H is cardinal du sousgroupe H so H



Fondamental

- Soit x un élément d'un groupe (G, *). **L'ordre de x** est le plus petit entier positif d non nul tel que xd = e.
- Le sous-groupe engendré par x est alors l'ensemble $\{x, x^2, x^3, \dots, x^{d-1}, x^d\}$.

F. Exercice

Soient H et K deux sous groupes d'un groupe G montrez que $\mathsf{H} \cap \mathsf{K}$ est un sous groupe.

G. Exercice

Soit E l'ensemble des parties d'un ensemble à deux éléments : $E = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$

On définit sur E la loi * suivante :

Réunion : A * B = A U B

- a) Écrire la table de composition de la loi.
- b) L'ensemble possède-t-il un élément neutre pour la loi?
- c) La loi est-elle associative ?
- d) La loi est-elle commutative ?
- e) L'ensemble muni de la loi est-il un groupe ?

H. Morphisme de groupes

Un morphisme, du grec morphos, la forme, est une application qui préserve la structure.



Définition

Soient (G, *) et (F, \times) des groupes et $f: G \rightarrow F$ une application. On dit que f est un **morphisme** ou **homomorphisme** de groupes si f préserve la structure de groupe, c'est-à-dire si

```
\begin{split} \forall x \in G, \ \forall y \in G, \ f(x*y) = f(x) \times f(y) \ ; \\ f\left(e_G\right) = e_F \ ; \\ \forall x \in G, \ f\left(x^{-1}\right) = f(x)^{-1}. \end{split}
```



Conseil

Pour montrer que f est un morphisme de groupes, il suffit en fait de vérifier la première condition. Elle implique en effet les deux autres conditions.



Définition

L'ensemble des morphismes de (G, *) dans (F, \times) se note Hom(G, F).

Si $f \in Hom(G, G)$, on dit que f est un **endomorphisme**.

Si $f \in Hom(G, F)$ est une bijection, on dit que f est un **isomorphisme** de groupes.

La composée de deux morphismes de groupes est un morphisme de groupes



Définition

Soit $f \in Hom(G, F)$. On appelle noyau de f l'ensemble

$$Ker(f) = f^{-1}\left(\{e_F^{}\}\right) = \{x \in G \mid f(x) = e_F^{}\}.$$



Fondamental: Proposition

Soit $f \in Hom (G, F)$. Alors

- Ker(f) est un sous-groupe de (G, *);
- Im(f) est un sous-groupe de (F, ×);

I. Exercice

Soient (G, *) et (F, \times) deux groupes et $f \in Hom (G, F)$. Montrez que Ker(f) est un sous groupe de G



ANNEAUX ET CORPS

Introduction aux Anneaux	15
Exercice	17
Exercice	17
Sous-anneaux et morphisme d'anneaux	17
Exercice	18
Corps	19
Exercice	19
Exercice	20

Objectifs

À la fin de cette leçon, vous serez capable de :

- **Identifier** la structure d'anneau
- Identifier la structure de corps
- Manipuler les opérations de base dans les anneaux
- Manipuler les opérations possibles dans les corps

Dans cette section, nous allons étudier deux nouvelles structures algébriques l'anneau et le corps. Contrairement aux groupes , ces structures possèdent deux lois de composition interne. Elles nous permettent de généraliser les notions d'addition et de multiplication dans des ensembles comme R en donnant une notation plus précise

A. Introduction aux Anneaux

Dans \mathbb{Z} , il existe une deuxième loi interne : la multiplication que nous noterons . Cette loi possède les propriétés (Commutativité, Associativité, Neutre) (le neutre étant 1), mais pas (Symétrie).

En effet, aucun entier relatif n'est solution, par exemple, de l'équation 3x = 1. (Ceci nécessite la création d'un ensemble "plus grand" contenant $\mathbb Z$; Il s'agit de l'ensemble des nombres rationnels).



Définition

Soit E un ensemble muni de deux lois de composition internes • et T. On dit que **T est distributive** par rapport à • si

 $\forall x \in E, \forall y \in E, \forall z \in E, xT(y \cdot z) = (xTy) \cdot (xTz) \text{ et } (yTz) \cdot x = (yTx) \cdot (zTx).$



Exemple

Lorsque, dans un ensemble il existe deux lois, on peut les faire opérer l'une avec l'autre :

Ainsi, vous savez que $(2+3) \times 5 = (2 \times 5) + (3 \times 5)$. Si ceci est vrai dans tous les cas, on parle alors de distributivité à droite de la multiplication par rapport à l'addition.

De même, il existe la distributivité à gauche. Dans l'exemple précédent, on écrirait $5 \times (2+3) = (5 \times 2) + (5 \times 3)$.

Si la deuxième loi est distributive à droite et à gauche par rapport à la première loi, on dit simplement qu'il y a distributivité, propriété notée (D).



Définition

Soit A un ensemble muni de **deux lois de composition internes** + et *. On dit que (A, +, *) **est un anneau** si

- (A,+) est un groupe commutatif;
- la loi * est associative ;
- la loi * est **distributive** par rapport à la loi +.

Si de plus, la loi * est commutative, on dit que (A, +, *) est un anneau commutatif.



Complément

On note 0_A ou plus simplement 0 l'élément neutre pour la loi +.

Alors 0 est un élément absorbant de A : $\forall x \in A, x * 0 = 0 * x = 0$.

On note 1_A ou plus simplement 1 l'élément unité pour la loi * .

Alors: $\forall x \in A, x * 1 = 1 * x = x$.

Un anneau est dit **unitaire** s'il possède un unique élément unité pour la loi * .



Exemple

- $(Z,+,\times)$ et $(Z/nZ,+,\times)$ sont des anneaux commutatifs
- Si pour $n \in N\setminus\{0\}$ on note G l'ensemble des endomorphismes du groupe (Rn, +), alors $(G,+, \cdot)$ est un anneau non commutatif.
- $(F(R, R), +, \times)$ l'ensemble des applications de R dans R est un anneau commutatif.



Fondamental

Soit (A,+,*) un anneau. On dit que c'est un **anneau intègre** si $\forall x \in A, \forall y \in A, x*y = 0 \Rightarrow x = 0$ ou y = 0.



Exemple

Z est un anneau intègre



Conseil

Lorsqu'on travaille dans un anneau, de nombreux calculs se passent "comme dans R". Cela dit, il faut faire attention par exemple à ne pas diviser. Le meilleur moyen

ANNEAUX ET CORPS

pour ne pas se tromper consiste en fait à "faire comme dans Z".



Attention

Il est nécessaire d'imposer la distributivité à droite et à gauche.

Par exemple, $(F(R,R), +, \circ)$ n'est pas un anneau : on a bien $(f + g) \circ h = f \circ h + g \circ h$ pour tout f, g, h, mais pas nécessairement $f \circ (g + h) = f \circ g + f \circ h$.

B. Exercice

[Solution n°2 p 23]

Exercice

L'ensemble (N, +, .) des entiers naturels est :

- un anneau commutatif
- un anneau intègre.
- n'est pas un anneau.
- o aucune des assertions précédentes n'est vraie

C. Exercice

Montrer que $(F(R, R), +, \times)$ l'ensemble des applications de R dans R est un anneau commutatif.

D. Sous-anneaux et morphisme d'anneaux



Définition

Soit (A, +, *) un anneau et $B \subset A$. On dit que B est un **sous-anneau** de A si les lois + et * lui confèrent une structure d'anneau :

B est un sous-groupe de (A,+);

 $\forall x \in B, \forall y \in B, x*y \in B$.



Exemple

Soient (A,+,*) et $(B,+,\times)$ des anneaux et f un morphisme entre ces anneaux. Alors Ker(f) est un sous-anneau de A et Im(f) est un sous-anneau de B.



Définition

Soient (A,+, *) et $(B,+, \times)$ des anneaux. Soit $f \in F(A, B)$. On dit que f est un **morphisme d'anneaux** si

f est un morphisme de groupes entre (A,+) et (B,+):

$$\forall x \in A, \forall y \in A, f(x + y) = f(x) + f(y);$$

 $\forall x \in A, \forall y \in A, f(x * y) = f(x) \times f(y).$

Si f est de plus une bijection entre les ensembles A et B, on dit que f est un isomorphisme d'anneaux.



Définition

Soit (A,+,*) un anneau unitaire et soit $x \in A$. On dit que x est inversible s'il admet un inverse

pour la loi · :

 $\exists y \in A, x*y = y*x = 1_A$



Remarque

- 1_A et -1_A sont toujours des éléments inversibles
- Si x*y = 0, on peut conclure que x ou y est non inversible.
- Soit $(A,+,\cdot)$ un anneau unitaire, Alors l'ensemble des éléments inversibles de A est un groupe.

E. Exercice

[Solution n°3 p 23]

Exercice

Soit f un morphisme de l'anneau A dans l'anneau B. Laquelle des assertions suivantes est vraie ?

ANNEAUX ET CORPS
f(A) est un sous-anneau de A.
f(A) est un sous-anneau de B.
f-1(A) est un morphisme de l'anneau B dans l'anneau A.
f-1(A) est un sous-anneau de A.
Ker f est un sous-anneau de A.

F. Corps



Soit K un ensemble muni de deux lois de composition internes + et .

On dit que (K, +, .) est **un corps** si (K, +, .) est un *anneau unitaire commutatif* et si tout élément de K $\{0_K\}$ admet un inverse pour la loi .



Exemple

- **Exemple** $(Q, +, \times)$, $(R, +, \times)$, et $(C, +, \times)$ sont des corps.
 Si p est un nombre premier, $(Z/pZ, +, \times)$ est un corps.



Remarque

Autrement dit, $(K, +, \cdot)$ est **un corps** si (K, +, .) est un **anneau** et si $(K^*, .)$ est un groupe commutatif.

D'après la définition, un corps est en particulier un anneau intègre.

G. Exercice

[Solution n°4 p 24]

Exercice

Soit K I 'ensemble des nombres complexes: z = r+ is, r et s deux nombres rationnels.

	ANN	FΔI	IX	FT	()	R	PS
--	-----	-----	----	----	----	---	----

(K ,+) est un groupe non commutatif
(K, +, .) est un anneau intègre
(K,+, .) est un corps non commutatif
(K,+, .) est un corps commutatif
Aucune des assertions précédentes n'est vraie

H. Exercice

[Solution n°5 p 25]

Laquelle des assertions suivantes est vraie :		[501411011 11*5 p 25]
	Certain anneaux intègres ne sont pas des corps.	
	Tout anneau intègre est un corps.	
	Certain corps ne sont pas des anneaux intègres.	
	Tout corps est un anneau intègre.	
	Tout anneau intègre infini est un corps	



Conclusion

Cette leçon a introduit les notions de groupe , d'anneaux et de corps. Ces notions nous seront utiles pour tout le reste du cours et particulièrement pour la prochaine leçon.

Solution des exercices

> Solution n°1 (exercice p. 10)

Exercice

- La loi de composition interne T sur définie sur R par \forall x, y \in R (xTy)=xy+(x2 -1)(y2 -1) est commutative
- L'application T définie sur $R\setminus\{0 \times R \text{ par } (x, y)T(x',y') = (xx', xy' + y) \text{ est une loi de composition interne}$
- L'application T définie sur R\ $\{0\}$ ×R par (x, y)T(x', y') = (xx', xy' + y) est une loi de composition interne commutative

> Solution n°2 (exercice p. 17)

Exercice

- O un anneau commutatif
- un anneau intègre.
- o n'est pas un anneau.
- o aucune des assertions précédentes n'est vraie

> Solution n°3 (exercice p. 18)

Exercice

S	olution des exercices
	f(A) est un sous-anneau de A.
	f(A) est un sous-anneau de B.
	f-1(A) est un morphisme de l'anneau B dans l'anneau A.
5	f-1(A) est un sous-anneau de A.
5	Ker f est un sous-anneau de A.
Solution n°4 (exercice p. 19) Exercice	
	(K ,+) est un groupe non commutatif
	(K, +, .) est un anneau intègre
	(K,+, .) est un corps non commutatif
	(K,+, .) est un corps commutatif
	Aucune des assertions précédentes n'est vraie

> Solution n°5 (exercice p. 20)

 Solution des exercices
Certain anneaux intègres ne sont pas des corps.
Tout anneau intègre est un corps.
Certain corps ne sont pas des anneaux intègres.
Tout corps est un anneau intègre.
Tout anneau intègre infini est un corps



Bibliographie

- [1] F. Liret, D. Martinais, Algèbre Licence 1ère année MIAS-MASS-SM, éditions Dunod, 2002
- [2] François Liret, Maths en pratique à l'usage des étudiants Cours et exercices, éditions Dunod, 2006
- [3] Jean Romain Heu Cours d'Algèbre générale 2016
- [4] Claude Deschamps, André Warufsel, Mathématiques tout en un 1ière année, MPSI, PCSI, , éditions Dunod, 2003