Licence de mathématiques

Cahier-Cours et exercices

Mohamed Aqalmoun

Structures algébriques, polynômes et fractions rationnelles

Module *M*03

ENS-FES

Avant-propos

Ce cahier-cours (version $\frac{1}{2}$-cours) est destiné aux étudiants de première année de la licence d'éducation d'enseignement des mathématiques de l'école normale supérieure de Fès. Il propose un cours non complet (sans démonstrations) de structures algébriques (groupes, anneaux, polynômes et fractions rationnelles) correspondant au programme de la filière. Les champs pointés, correspondent aux détails (généralement les démonstrations et des exemples), font l'objet des séances du cours et ils seront complétés au fur et à mesure.

Table des matières

Chapitre 1

Structures usuelles

1.1 Loi de composition interne

Définition 1.1.

Soit G un ensemble non vide. On appelle loi de composition interne sur G toute application $* : G \times G \to G$. L'image d'un couple (x, y) sera noté $x * y$ et il est dit le composé de x par y.

Exemples :

1. L'addition $+$ et la multiplication $\times$ sont des lois de compositions internes sur $\mathbb{N}$,$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
2. Soit X un ensembles : l'intersection $\cap$, l'union $\cup$ et la différence symétrique Δ sont des lois de compositions internes sur $\mathscr{P}(X)$.
3. La multiplication est une loi de composition interne sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

Définition 1.2.

Soit $(G, *)$ un ensemble muni d'une loi de composition interne et A une partie de G. On dit que A est stable par la loi $*$ si : pour tous $x, y \in A$, $x * y \in A$.

Exemples :

1. $\mathbb{N}$ .....
2. $\mathbb{U} = \{z \in \mathbb{C} \ / \ |z| = 1\}$ .....

Définition 1.3. (loi induite)

Soit $(G,*)$ un ensemble muni d'une loi de composition interne et A une partie stable de G, l'application restreinte $A\times A\to A$; $(a,b)\mapsto a*b$ définie une loi de composition interne sur A, dite la loi induite sur A par $*$.

Exemple : .....

Définition 1.4.

Soit $(G,*)$ un ensemble muni d'une loi de composition interne.

1. *La loi $*$ est dite commutative sur G si : pour tous $x,y\in G$; $x*y=y*x$.*
2. *La loi $*$ est dite associative si : pour tous $x,y,z\in G$; $(x*y)*z=x*(y*z)$.*

Exemples :

1. L'addition + et la multiplication × sont .....
2. La soustraction est une loi de composition intenre sur .....

Notation : Soit $(G,*)$ un ensemble muni d'une loi de composition interne. Si $*$ est associative et $x,y,z\in G$, l'élément $(x*y)*z=x*(y*z)$ se note $x*y*z$.

1.1.1 Éléments particuliers

Définition 1.5.

Soit $(G,*)$ un ensemble muni d'une loi de composition interne. On dit que $e\in G$ est un élément neutre de $(G,*)$ si : pour tous $x\in G$; $x*e=e*x=x$.

Proposition 1.6. (Unicité de l'élément neutre)

Soit $(G,*)$ un ensemble muni d'une loi de composition interne. Si $(G,*)$ possède un élément neutre, alors celui-ci est unique.

Démonstration : .....

Exemples :

1. 0 est le neutre de .....
2. 1 est le neutre de .....

3. Soit X un ensemble. L'ensemble vide $\emptyset$ est le neutre .....
4. Soit X un ensemble. .....

Définition 1.7.

Soit $(G,*)$ un ensemble muni d'une loi de composition interne. On dit que $(G,*)$ est un monoïde, lorsque la loi $*$ est associative et possède un élément neutre.

Exemples : .....

Définition 1.8.

Soit $(G,*)$ un monoïde de neutre e. Un élément x de G est dit symétrisable, lorsqu'il existe $x' \in G$ tel que $x * x' = x' * x = e$.

Proposition 1.9. (et définition)

Soit $(G,*)$ un monoïde de neutre e et $x \in G$. Alors x est symétrisable si et seulement s'il existe un unique $x' \in G$ tel que $x * x' = x' * x = e$. Si c'est le cas, l'élément x' est appelé le symétrique de x et se note $\text{sym}(x)$ *; ainsi :*

$$x * \text{sym}(x) = \text{sym}(x) * x = e$$

Démonstration : .....

Exemples : .....

Proposition 1.10.

Soit $(G,*)$ un monoïde et $x, y \in G$.

1. *Si x est symétrisable, alors* $\text{sym}(x)$ *est symétrisable et on a* $\text{sym}(\text{sym}(x)) = x$.
2. *Si x et y sont symétrisables, alors $x * y$ est symétrisable et on a* $\text{sym}(x * y) = \text{sym}(y) * \text{sym}(x)$.

Démonstration : .....

1.1.2 Itéré d'un élément

Soit $(G,*)$ un monoïde de neutre e, et x un élément de G :
On pose $x^0 = e$ et pour $n \geq 1$,

$$a^n = a * a^{n-1} = \underbrace{a * a * \ldots * a}_{n\text{-fois}}$$

Proposition 1.11.

Soit $(G,*)$ un monoïde de neutre e, et $x \in G$.

1. *Pour tous $p,q \in \mathbb{N}$ on a ; $x^p * x^q = x^{p+q}$.*
2. *Pour tous $p,q \in \mathbb{N}$ on a ; $(x^p)^q = x^{pq}$.*

Démonstration : .....

Soit $(G,*)$ un monoïde de neutre e, et x un élément symétrisable de G, pour $n \in \mathbb{Z}\setminus\mathbb{N}$, on pose $x^n = (\text{sym}(x))^{-n}$, alors pour tous $p,q \in \mathbb{Z}$ on a :
$x^{p+q} = x^p * x^q$, $(x^p)^q = x^{pq}$, x^p est symétrisable et $\text{sym}(x^p) = x^{-p}$.

Notation additive et multiplicative :

- ☞ Un monoïde est dit noté additivement (respectivement multiplicativement) si sa loi est noté par + (respectivement ×).
- ☞ En notations additive, on utilise les conventions suivantes :
  - ✓ Le neutre de $(G,+)$ se note 0_G où 0.
  - ✓ Le symétrique d'un élément x (lorsqu'il existe) se note $-x$, dit **l'opposé** de x.
  - ✓ L'itéré d'ordre n de x se note nx.
  - ✓ Le composé $x_1 + x_2 * \ldots + x_n$ se note $\sum_{i=0}^{n} x_i$.
- ☞ En notation multiplicative, on utilise les conventions suivantes :
  - ✓ Le neutre de $(G,\times)$ se note 1_G ou 1.
  - ✓ Le symétrique d'un élément x (lorsqu'il existe) se note x^{-1} dit **l'inverse** de x.
  - ✓ L'itéré d'ordre n de x se note x^n.
  - ✓ Le composé $x_1 \times x_2 * \ldots \times x_n$ se note $\prod_{i=0}^{n} x_i$.

1.1.3 Loi produit

Définition 1.12.

Soient $(G,*)$ et $(G',.)$ deux ensembles muni de deux lois de compositions internes. On définit sur $G \times G'$ une loi de composition interne $\top$ en posant pour tous $(x,y),(x',y') \in G \times G'$, $(x,y) \top (x',y') = (x * x', y.y')$, la loi ainsi définie est dite la loi produit.

Proposition 1.13.

Soient $(G,*)$, $(G',.)$ deux monoïdes de neutres respectivement e et e'. Notons par $\top$ la loi produite. Alors $(G\times G',\top)$ est un monoïde de neutre (e,e').

Démonstration : .....

1.2 Groupes

1.2.1 Définitions et exemples

Définition 2.1.

Soit $(G,*)$ un ensemble muni d'une loi de composition interne. On dit que $(G,*)$ est un groupe si $(G,*)$ est un monoïde et tout élément de G est symétrisable.

Remarque : Dire que $(G,*)$ est un groupe signifie que :

1. $*$ est associative ; $\forall x,y,z\in G,\ x*(y*z)=(x*y)*z$,
2. G possède un élément neutre pour la loi $*$; $\exists e\in G$ tel que $\forall x\in G,\ x*e=e*x=x$,
3. Tout élément de G est symétrisable ; $\forall x\in G,\ \exists x'\in G$ tel que $x*x'=x'*x=e$.

Exemples : .....

Définition 2.2.

Un groupe $(G,*)$ est dit abélien ou commutatif, lorsque la loi $*$ est commutative.

Exemple : .....

Définition 2.3.

Un groupe $(G,*)$ est dit fini, lorsque l'ensemble G est fini, son cardinal est dit l'ordre du groupe et se note $O(G)$ ou $ord(G)$ ou $|G|$.

Exemple : .....

1.2.2 Groupe produit

Théorème 2.4. (et définition)

Soient $(G_1,*)$, $(G_2,.)$ deux groupes. Alors $G_1 \times G_2$ muni de la loi produite est un groupe, dit le groupe produit de $(G_1,*)$ et $(G_2,.)$.

Démonstration : .....

1.2.3 Sous-groupes

Définition 2.5.

Soit $(G,*)$ un groupe, H une partie de G. On dit que H est un sous groupe de G, si on a les deux propriétés suivantes :

1. *H est une partie stable de G,*
2. *H muni de la loi induite est un groupe.*

Exemple : .....

Théorème 2.6.

Soit H une partie d'un groupe $(G,*)$. Les propriétés suivantes sont équivalentes :

1. *H est un sous groupe de $(G,*)$,*
2. *H non vide, et $\forall x, y \in H$, $x * y \in H$ et $\text{sym}(x) \in H$.*

Démonstration : .....

Théorème 2.7.

Soit H une partie d'un groupe $(G,*)$, on a équivalence entre :

1. *H est un sous groupe de G,*
2. *H non vide, et $\forall x, y \in G$; $x * \text{sym}(y) \in H$.*

Démonstration : .....

Théorème 2.8. (Sous groupe de $\mathbb{Z}$)

Les sous groupe de $\mathbb{Z}$ sont les partie de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Démonstration : .....

Proposition 2.9.

Soit G un groupe et $(H_i)_{i\in I}$ une famille de sous groupes de G. Alors $\cap_{i\in I} H_i$ est un sous groupe de G. En particulier l'intersection de deux sous groupes est un sous groupe.

Démonstration : .....

Remarque : L'union de deux sous-groupes .....

1.3 Morphisme de groupes

Définition 3.1.

Soient $(G,*)$, $(G',.)$ deux groupes et $f : G \to G'$ une application. On dit que f est un morphisme de groupes si ; pour tous $x, y \in G$, on a $f(x*y) = f(x).f(y)$.

Exemples : .....

Propriétés 3.2.

Soit $f : G \to G'$ un morphisme de groupes. Alors

1. *$f(e) = e'$, où e (respectivement e') est le neutre de G (respectivement G').*
2. *Pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$.*

Démonstration : .....

Proposition 3.3.

Soit $f : G \to G'$ un morphisme de groupes.

1. *Si H est un sous groupe de G alors $f(H)$ est un sous groupe de G'.*
2. *Si K est un sous groupe de G' alors $f^{-1}(K)$ est un sous groupe de G.*

Démonstration : .....

Définition 3.4.

Soit $f : G \to G'$ un morphisme de groupes.

1. *L'ensemble $f^{-1}(\{e'\})$ est un sous groupe de G appelé le noyau de f*

et se note $\ker f$.

2. *L'ensemble* $f(G)$ *est un sous groupe de* G' *appelé image de* f *et se note* $\mathrm{Im}\, f$.

Remarque : Soit $f : G \to G'$ un morphisme de groupes.

1. $\ker f =$
2. $\mathrm{Im}\, f =$

Proposition 3.5.

Soit $f : G \to G'$ *un morphisme de groupes.*

1. f *injectif si, et seulement si,* $\ker f = \{e\}$.
2. f *est surjectif si, et seulement si,* $\mathrm{Im}\, f = G'$.

Démonstration :

Définition 3.6.

On dit que $f : G \to G'$ *est un isomorphisme de groupes si* f *est un morphisme de groupes bijectif.*

Exemple : .....

Proposition 3.7.

Soit $f : G \to G'$ *un isomorphisme de groupes. Alors* $f^{-1} : G' \to G$ *est aussi un morphisme de groupes.*

Démonstration : .....

Définition 3.8.

Un endomorphisme de G est un morphisme de G dans lui même.
Un automorphisme de G est un endomorphisme de G qui est bijectif.

Exemple : .....

1.4 Groupe symétrique

Théorème et définition 4.1.

Soit X un ensemble non vide. L'ensemble des applications bijectives de X vers X muni de la composition des applications est un groupe appelé groupe symétrique de X et se note $S(X)$. Un élément de $S(X)$ est appelé une permutation de X.

Notations : pour $n \geq 1$, on note S_n le groupe symétrique de $X = \{1, 2, \ldots, n\}$. Si $\sigma \in S_n$ avec $\sigma(i) = a_i$, alors σ se note $\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$, ainsi $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$

Remarque : S_n est fini et $\text{Card}(S_n) = n!$.

Exemple : S_2 et S_3 : .....

Exemple : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 5 & 4 & 1 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 3 & 1 \end{pmatrix}$:

$\sigma \circ \sigma'$ .....

σ^{-1} .....

Définition 4.2.

Soit $n \geq 2$. Une transposition de S_n est une permutation de S_n qui échange deux éléments distincts de $[\![1, n]\!]$ et en fixant les autres éléments.
Soit $(i, j) \in [\![1,]\!]^2$ avec $i \neq j$. La transposition qui échange i et j se note τ_{ij}.
Elle est définie par : $\tau_{ij}(i) = j$ et $\tau_{ij}(j) = i$ et $\tau_{ij}(k) = k$, $\forall k \notin \{i, j\}$.

Proposition 4.3.

Soit $\tau \in S_n$ une transosition. Alors $\tau^2 = \text{Id}$ et $\tau^{-1} = \tau$.

Démonstration : .....

Définition 4.4.

Soit $\sigma \in S_n$. On appelle support de σ l'ensemble $\text{supp}(\sigma) = \{k \in [\![1, n]\!] / \sigma(k) \neq k\}$.

Exemples : .....

Définition 4.5.

Soit $\sigma \in S_n$. On dit que σ est un p-cycle s'ils existent $i_1, \dots, i_p$ deux à deux distincts tels que $\text{supp}(\sigma) = \{i_1, \dots, i_p\}$, *pour tout* $1 \leq k \leq p-1$, $\sigma(i_k) = i_{k+1}$ *et* $\sigma(i_p) = i_1$. *Dans ce cas σ se note* $\sigma = (i_1 \ i_2 \ \dots \ i_p)$.

Exemple : Dans S_8 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 6 & 5 & 8 & 7 & 1 \end{pmatrix}$ .....

Proposition 4.6.

Tout p-cycle est le produit de $p-1$ transpositions.

Démonstration : .....

Théorème 4.7.

Toute permutation est le produit de cycles à supports disjoints donc produit de transpositions.

Exemple : Décomosition en cycles disjoints .....

Définition 4.8.

Soit $\sigma \in S_n$. La signature de σ est le nombre noté $\epsilon(\sigma)$ défini par

$$\epsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Exemples : .....

Remarque : Pour $\sigma \in S_n$, $\epsilon(\sigma) \in \{-1, 1\}$. En effet on a $\{\sigma(1), \dots, \sigma(n)\} = \{1, \dots, n\}$, donc

Théorème 4.9.

La signature est un morphisme de groupes de S_n dans $(\{-1, 1\}, \times)$. Autrement dit $\epsilon(\sigma\sigma') = \epsilon(\sigma)\epsilon(\sigma')$.

Proposition 4.10.

1. *Pour toute transposition τ, $\varepsilon(\tau) = -1$.*
2. *Pour tout p-cycle σ, $\varepsilon(\sigma) = (-1)^{p-1}$.*

Exemple : .....

1.5 Anneaux et corps

1.5.1 Anneaux et sous anneaux

Définition 5.1.

Soit A un ensemble muni de deux lois de compositions internes $+$ et $\times$.
On dit que le triplet $(A,+,\times)$ est un anneau si :
• *$(A,+)$ est un groupe abélien (de neutre 0).*
• *La multiplication $\times$ est associative.*
• *$\times$ est distributive par rapport à $+$ c'est-à-dire ; pour tous $a,b,c \in A$, $(a+b)\times c = a\times c + b\times c$ et $a\times(b+c) = a\times b + a\times c$.*
Si de plus la loi $\times$ est commutative, on dit que $(A,+,\times)$ est un anneau commutatif.
Si $\times$ admet un neutre, on dit que A est unitaire.

Exemples :

1. $\mathbb{Z}$ .....
2. Pour X un ensemble non vide $\mathscr{F}(X,\mathbb{R})$ .....

Propriétés 5.2.

Soit A un anneau.

1. *Pour tout $a \in A$, $a.0 = 0.a = 0$,*
2. *Pour tous $a,b \in A$, $(-a)b = a(-b) = -ab$,*
3. *Pour tous $a,b,c \in A$, $a(b-c) = ab - bc$ et $(a-b)c = ac - bc$.*

Démonstration : .....

Proposition 5.3.

Soit A un anneau $a,b \in A$ tels que $ab = ba$ et $n \in \mathbb{N}^*$.

1. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.
2. $a^n - b^n = (a-b)\left(\sum_{k=0}^{n} a^k b^{n-1-k}\right)$.

Démonstration : Par récurrence sur n.

Définition 5.4.

Soit A un anneau et B une partie de A. On dit que B est un sous anneau de A si

1. *$(B,+)$ est un sous groupe de $(A,+)$.*
2. *B est stable par la multiplication c'est-à-dire $\forall a,b \in B,\ ab \in B$.*

Si de plus A est unitaire et $1 \in B$, on dit que B est un sous anneau unitaire de A.

Exemples : .....

Remarque : une partie non vide B est un sous anneau (unitaire) de A si, et seulement si, $\forall x,y \in B$, $x-y \in B$ et $xy \in B$ (et $1 \in B$).

Définition 5.5.

Soit A un anneau commutatif unitaire. On dit que A est intègre s'il est non nul et pour tout $x,y \in A$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$.

Exemple : .....

1.5.2 Groupe des unités

Définition 5.6.

Soit A un anneau unitaire. On dit que $x \in A$ est inversible, s'il existe $y \in A$ tel que $xy = yx = 1$.

Exemple :

Proposition 5.7.

Soit A un anneau unitaire et $x \in A$. Alors x est inversible si et seulement s'il existe un unique $y \in A$ tel que $xy = yx = 1$. L'élément y s'appelle l'inverse de x et se note x^{-1}.

Démonstration : .....

Proposition 5.8.

Soit A un anneau unitaire. L'ensemble des éléments inversibles dans A est un groupe pour la multiplication, appelé groupe des unités de A et se note $U(A)$.

Exemple : .....

1.5.3 Corps

Définition 5.9.

Un corps est un anneau unitaire A dans lequel tout élément non nul est inversible c'est-à-dire $U(A) = A \setminus \{0\}$. Un corps est dit commutatif si la multiplication est commutative.

Exemple : .....

Définition 5.10.

Soit K un corps. On dit que L est un sous corps de K si L est un sous anneau unitaire de K et pour tout élément non nul $x \in L$, $x^{-1} \in L$.

1.5.4 Idéaux

Définition 5.11.

Soit A un anneau commutatif unitaire et I une partie de A. On dit que I est un idéal de A si

1. *$(I,+)$ est un sous groupe de $(A,+)$,*
2. *$\forall a \in A, \forall x \in I, ax \in I$.*

Exemples : .....

Proposition 5.12.

Soit A un anneau commutatif unitaire.

1. *L'intersection d'une famille quelconque d'idéaux de A est un idéal de A.*
2. *Si I et J sont des idéaux de A alors $I+J := \{i+j \ / \ i \in I, j \in J\}$ est un idéal de A.*

Démonstration : .....

1.5.5 Morphismes d'anneaux

Définition 5.13.

Soient A et B deux anneaux unitaires et $f : A \to B$ une application. On dit que f est un morphisme d'anneaux (unitaires) si pour tout $x, y \in A$, $f(x+y) = f(x)+f(y)$, $f(xy) = f(x)f(y)$ et $f(1) = 1$.

Exemples : .....

Définition 5.14.

Soit $f : A \to B$ un morphisme d'anneaux. Le noyau de f est l'ensemble $\ker f = \{x \in A \ / \ f(x) = 0\}$ *. L'image de f est l'ensemble* $\operatorname{Im} f = f(A)$.

Proposition 5.15.

Si $f : A \to B$ est un morphisme d'anneaux alors $\ker f$ *est un idéal de A et* $\operatorname{Im} f$ *est un sous anneau de B.*

Démonstration :

1.5.6 Anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{Z}$. On considère sur $\mathbb{Z}$ la relation binaire R_n suivante : Pour $x, y \in \mathbb{Z}$, $xR_n y$ si, et seulement si, n divise $y-x$.
On vérifie facilement que R_n est une relation d'équivalence sur $\mathbb{Z}$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient $\mathbb{Z}/R_n$. Notons que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \{\overline{k} \ / \ 0 \leq k \leq n-1\}$.
On définit sur $\mathbb{Z}/n\mathbb{Z}$ deux lois de composition internes par : Pour tout $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{x}+\overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{xy}$.
Ces deux lois sont bien définies, en effet ; si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ alors n divise $x-x'$

et $y-y'$, autrement dit ils existent $k,l \in \mathbb{Z}$ tels que $x = x' + kn$ et $y = y' + ln$, donc $x+y = x'+y'+(k+l)n$ et $xy = x'y'+(ky'+lx'+kln)n$, ainsi $\overline{x+y} = \overline{x'+y'}$ et $\overline{xy} = \overline{x'y'}$.

Proposition 5.16.

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif et unitaire (d'unité $\overline{1}$).

Démonstration :

Théorème 5.17.

Un élément $\overline{m}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement si, $m \wedge n = 1$.

Démonstration :

Théorème 5.18.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Démonstration :